EBOOK

A Hacker's Guide to Ransomware Mitigation and Recovery

By Hector Xavier Monsegur
and Andy Stone

PURESTORAGE®

EBOOK

Table of Contents

Executive Summary

Vaccinate your Data Against the Ransomware Pandemic

Even as highly effective vaccinations are starting to lift some nations out of the COVID-19 pandemic, a ransomware pandemic continues to rage across computer networks worldwide. In 2020, 51% of organizations were hit by a ransomware attack, according to a report by Sophos.[1] Recent ransomware attacks forced the Colonial Pipeline and JBS, the world's largest meat processor, to temporarily halt operations. The Washington Post reports that "Experts say continued ransomware threats are inevitable, calling on businesses and governments to ramp up efforts to secure their online networks."[2]

As a former "Black Hat" hacker, Hector Monsegur understands bad actors, their motivations, and how they operate. He now resides on the good side as an offensive security-focused "Red Team" researcher. He works with organizations to emulate how cybercriminals might attack defenses to help defense-focused "Blue Teams" better understand their risks, uncover, and address gaps in defenses, and prioritize future security investments. Andy Stone, Field CTO, Americas for Pure Storage, is a former CISO who focused on defensive cybersecurity.

In this ebook we will provide tips to help your organization prepare for ransomware attacks and safeguard your data by explaining:

- Why ransomware attacks are on the rise
- Attackers' modus operandi before an attack occurs
- What you should do in advance to prevent an attack or minimize data loss should one occur
- How to recognize an attack
- What to do if you detect an attack in-progress
- How to recover and restore your data after an attack

Introduction

The number of ransomware attacks has been increasing by leaps and bounds. Researchers at Check Point Research say that ransomware has impacted an average of more than 1,000 organizations each week since April of 2021. This represents a staggering 102% increase in the number of organizations affected by ransomware since the beginning of 2020.[3]

> The number of organizations impacted by ransomware leaped by 102% between 2020 and 2021.
>
> **THE NEW RANSOMWARE THREAT: TRIPLE EXTORTION | CHECK POINT SOFTWARE TECHNOLOGIES**

From the mid-2000s until the early 2010s, it was common for hacktivists to launch such attacks. But in recent years, hacktivists have cut back their activities significantly. Improved security postures at organizations have reduced the effectiveness of neophyte hackers who focus on low-hanging fruit. Arrests and prosecutions against members of Anonymous, LulzSec and other hacktivist groups have also had a significant deterrent impact.[4]

Now, state-sponsored hacker groups using off-the-shelf tools and open-source penetration testing tools carry out the vast majority of cyberattacks.[5] These nation-states often hire private sector offensive actors (PSOAs) who commercialize cyber threats and, like mercenaries, rent out their capabilities.[6] One such company, the NSO Group, has reportedly been involved in more than 100 abuse cases.[7] Nation-states find it cost effective to fund ransomware operations with the intention of causing disruptions to their targets without being directly involved.

Financial Motivations

With this shift in actors has come changing motivations for attacks. While hacktivists were typically motivated by political views, cultural or religious beliefs, national pride, or terrorist ideology, the key driver for ransomware attacks has become financial.

One factor that contributes to the recent ransomware uptick is the tendency for cyber insurance companies to give in to attacker's demands for ransom right away. I believe this response gives hackers more motivation to attack. For example, I consulted on one case where attackers researched how much insurance a target company had and then asked their victim to pay that amount. When the victim said they didn't have the money, the attackers pointed to the victim's insurance policy.

We're even starting to see attackers hack insurance companies to get this information. For example, in March of 2021, CNA, a leading US-based insurance company that provides cyber insurance policies was hit with a ransomware attack that disrupted its online services and business operations.[8] The company paid $40 million to regain control of its network.[9]

As long as organizations pay ransom, bad actors will continue to attack and find ways to exploit victims.

The Staggering Cost of Ransomware Attacks

The recent rash of ransomware attacks have had tremendous costs. A recent survey[10] found that the average cost to recover from a single ransomware attack—considering downtime, people time, device costs, network cost, lost opportunity, ransom paid, and so on) was $1.85 million in 2021, more than double the $761,106 in cost in 2020. Analysts conservatively estimate that the total financial damage from ransomware operations worldwide amounts to more than $1 billion.[11]

Low Risks for Attackers

From the attackers' perspectives, moreover, crypto currencies have made ransom demands relatively low risk. For example, JBS allegedly paid $11 million (using Bitcoin) as ransom to get back online after its recent ransomware attack. Analysts say that Bitcoin and other cryptocurrencies such as Monero and Zcash make it possible to extort huge ransoms from large companies. Because these transactions are anonymous, there's little chance of getting caught.[12]

The Ransomware Task Force, an international coalition of government officials, private-sector technologists and law enforcement recently reported that crypto currencies add to the challenge of tracking down ransomware criminals because of the borderless nature of these types of digital money.[13] On the other hand, Bitcoin may not be foolproof—on June 7, 2021 the U.S. Justice Department and the FBI announced that they had recovered 63.70 bitcoin (worth roughly $2.3 million) of the $4.4 million that the Colonial Pipeline sent to hackers.[14]

Inadequate Cybersecurity Measures

Another key contributor to the proliferation of ransomware attacks is the fact that organizations have few defenses. Many have failed to address obvious security gaps. IT teams often focus on sexy new security technology, but don't practice good security hygiene, such as password authentication, identity management, backup policies, and incident management. These hygiene lapses make life easy for attackers, who typically focus on finding the easiest, most cost-effective way to get into your organization's systems.

Threat Patterns and Analysis

85%

85% OF BREACHES INVOLVED A HUMAN ELEMENT IN 2021*

61%

61% OF BREACHES INVOLVED USER CREDENTIALS IN 2021*

*SOURCE: 2021 VERIZON DATA BREACH INVESTIGATIONS REPORT | VERIZON

Don't Overlook the Human Factor

Cybersecurity measures also often fail to account for human psychology. Of all the attacks we've seen, only a small percentage were technical ones that used exploits, zero-day attacks, or direct compromise of services. Most attacks start with a human. Such attacks use phishing emails, vishing, or some other interaction between the attacker, their automated systems or tools, and the victim that enable the attacker to steal a user's login credentials. Attackers then use these credentials to login the network just like any other user.

Humans fall prey to these attacks for many psychological reasons. They may not be adequately trained. They may want to help people. They may be afraid of looking incompetent. They may fear losing their job. For all these reasons, if they see a link from their CEO, they click on it. If launching a social engineering campaign will get attackers inside a billion-dollar company after just a few days of setup and $100 or less in setup costs, that's a huge win.

Another concern is insider threats. We've seen nation states or other attackers bribe employees and pay them to set up ransomware inside the organization.

Thus, the combination of inadequate security measures, bribery, and human psychology, where employees surrender their access credentials to phishing attacks, results in successful compromises that enable attackers to move laterally across the internal network and ultimately to ransomware attacks.

The Three Pillars of Ransomware Protection

With ransomware attacks happening every day, your organization needs to be prepared. You should educate yourself on how hackers operate and develop a plan that spells out what you should do before, during, and after a ransomware attack. The following are specific recommendations based on my experiences both as an attacker and as a consultant working with organizations to defend against attacks.

> "Of organizations that were not hit by ransomware last year and don't expect to be hit in the future, the #1 reason for this confidence is having trained IT staff who are able to stop attacks."
>
> **THE STATE OF RANSOMWARE 2021 | SOPHOS**

Pillar 1—Before an Attack

Before they attack, cybercriminals perform reconnaissance to identify targets. They might look for companies with cyber insurance who are more likely to pay the ransom. They will surely have a methodology for sizing up a target's attack surface, looking for weaknesses in that attack surface and creating an appropriate attack path.

For example, say the attacker finds a target that's a small ISP who works with multi-billion-dollar corporations. The attacker might uncover potential entry ways to that ISP by determining:

- Does the company have support staff they can social engineer?
- Is there a particular human they should interact with?
- What kinds of services, tools, or software does the ISP use and how broad is their attack surface?
- Can they identify internal host names from published SSL certificates?
- Are their DNS names or host names pointing to hijackable resources?

Once an attacker gains entry to an ISP, they can access the larger corporation.

What You Should Do Before an Attack Occurs

To thwart these reconnaissance efforts and prevent a potential attack, it's critical to be proactive and preemptive. Put in place a cybersecurity plan before anything happens.

To create your plan, take the following steps:

Get visibility

Start by gaining technical, operational, and organizational visibility.

- Technical visibility. Technical visibility is an understanding of what connected devices you have on your network, where they are vulnerable, and the threats to them. Make sure you put logging tools in place to get visibility into your system so you can identify anomalies.
- Operational visibility. Because phishing attacks that exploit your employees make up the majority of cybersecurity incidents, you need operational visibility into how and why people are accessing data as well as what cybersecurity training you're providing.
- Organizational visibility. Lost business due to damaged reputation is the largest contributing factor to data breach costs. Having organizational visibility enables you to assess the extent to which an attack could damage your company's brand, reputation, or intellectual property.

Get control

Once you know what you have on your network, eliminate obvious holes in your attack surface by performing all necessary security hygiene. For example, make sure routers and firewalls are properly configured, keep your IT systems patched, upgrade to the latest versions, keep whitelists and blacklists updated, enforce strong password rules and Multi-Factor Authentication (MFA).

Reduce the surface area of your environment

Safeguarding your network is easier with a smaller attack surface. Reducing your surface area is about eliminating duplication. For example, having fewer versions of Windows or Linux makes them easier to manage and maintain in a consistent manner.

Increase the cost of the attack

Most attackers seek easy avenues for access. When I was an adversary, I placed an emphasis on targeting services and vectors I was intimately familiar with. So, to thwart attackers, you simply need to make it incrementally harder for an attacker to get into your environment than into that of the guy next door. To make life more difficult for attackers:

- Put in place the right tools, such as centralized logging and events
- Partner with your solution vendors to understand the features offered and to implement them properly
- Maintain good system hygiene

Create a response policy

Create a response playbook that spells out policies for how your organization should respond to an attack before one occurs. Such policies will be different for each company, but may include:

- Analyzing SIEM logs for events to identify potentially compromised systems and users
- Contacting the incident response team and incident response vendors
- Shutting down connections to the Internet
- Turning off machines
- Communicating with law enforcement
- Preparing an incident report for the C-suite and the board

Provide proper training

Make sure the IT staff who monitor your security tools understand what the logs mean and how to react when anomalies are detected.

Build a comprehensive business continuity and disaster recovery (BCDR) plan

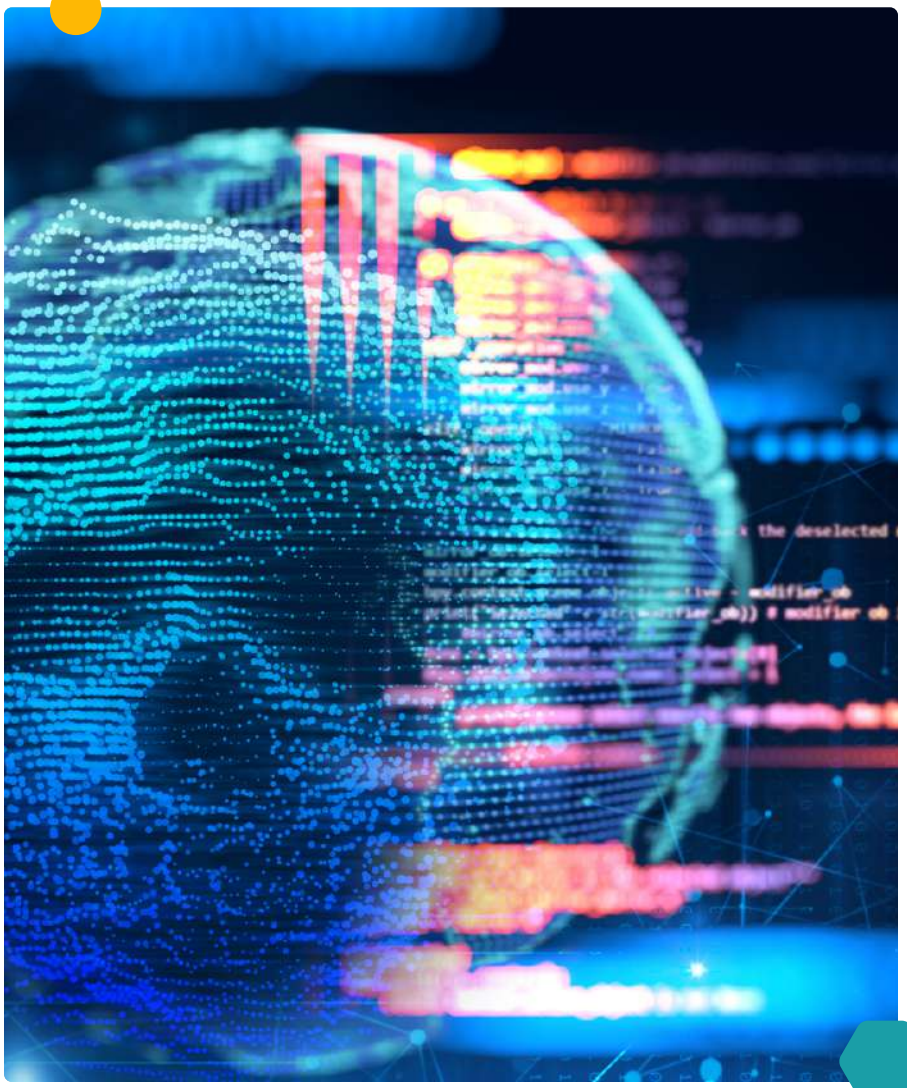
Despite all your planning, an attack can still shut you down. You need to be prepared to recover as quickly as possible by creating a comprehensive BCDR strategy.

- Define what applications and systems you have in your environment and which ones are most critical.
- Work with your line of business (LOB) teams to understand how quickly they need and expect to have data back online so you can put in place the right systems and controls to meet SLAs.
- Implement the right architecture for backing up your data and building tiers of recoverability.
- Sit down with your backup vendors to understand what your products do and how to properly implement them.
- Test everything to be sure you can recover quickly should unplanned downtime occur, regardless of the cause.
- Beware that attackers will target your critical infrastructure. If they do, you won't be able to access your core systems or use remote access tools or even email. You'll therefore need to plan for how to get the right people to the right places. You'll need to specify who to call, in what order, where they should go, and what they need to do there.

Pillar 2—During the Attack

During an attack, cybercriminals begin exploiting weaknesses in your company's attack surface. For example, say that during surveillance, an attacker found a DNS hostname that points to a vulnerable WordPress blog.[15] The attacker might now compromise that instance to get access to the server hosting it. They might then start a phishing campaign that uses that URL with the host name included to convince employees to click on a link to a false webpage where they request the user's credentials for the company's internal network or VPN.

Once the attacker uses these stolen credentials to get on the network, the attacker can then move laterally, accessing servers to exfiltrate data, steal intellectual property, or launch a ransomware campaign. These attacks can work very quickly, potentially spreading across your enterprise in 30-40 minutes, while going into your backups and deleting them and/or changing your credentials so you can't get in. Alternatively, after the initial entry, the attacker may sit there for weeks or months, monitoring the network to see how you'll respond and then creating an attack plan or strategy and deploying the ransomware. Thus, just because the network is quiet doesn't mean an attacker isn't lurking on it.



What Should You Do During an Attack?

Assuming that you have all the proper network monitoring tools in place, such as SEIMs and Logs, a well-trained staff looking for anomalies and events will be able to identify an attack in action. When it does, it's time to leap to action.

Identify the attack

You identify an attack by finding anomalies in events, network traffic types, or protocols being used.

Anomalies are simply events that don't make sense. For example, you might see an employee logging into the domain controller, or a secretary logging into the backup server. These activities indicate a lateral move where the attacker has compromised the user's credentials and is using them to log into systems they shouldn't be logging into.

Another tipoff to an attack is the kind of traffic on the network. For example, IPv6 traffic on the internal network is often used to bypass security products implemented to monitor IPv4 traffic, so seeing this type of traffic on a network with zero IPv6 use may be an indicator of compromise. It should be noted that Windows systems may send out DHCPv6 requests looking for connectivity and DNS details that can be supplied by an adversary without much privilege beyond listening and responding to broadcast requests.

Further indications of attack can come from broadcast communications like LLMNR and NBT-NS. These protocols broadcast name translation requests. If a server responds back to such broadcast requests with arbitrary hosts, it's a dead giveaway for defenders that an attacker is in the network. Attackers also commonly use low-hanging fruit attacks on internal Windows networks.

Execute your plan

Once you've confirmed that you're under attack, it's time to execute the response plan you've mapped out previously. Following your incident response plan and recovery procedures is extremely important. Otherwise, network and systems administrators are left using their own judgement to neutralize the threat, which in my experience is usually ineffective or even disastrous.

Prepare for investigations

Contact those in charge of incident response, communicate with your leadership and legal teams, and prepare your environment for investigations down the line with your vendors or law enforcement.

If you've brought in a company to do an investigation, make sure there's a handoff between them and law enforcement.

Should You Pay Ransom?

As a general rule, I don't think organizations should pay the ransom as it only encourages attacks. For example, a report by Cybereason found that 80% of organizations that paid the ransom were hit again.[16]

But there are many variables involved. For example, if you are an intensive care hospital and physicians won't be able to treat patients without these systems, you might need to pay the ransom immediately. Evaluate ransom payment on a case-by-case basis.

And whatever you do, beware that attackers may double or triple dip. Not only do the attackers encrypt the data and get you to pay, but they may also then extort you to pay even more, or they'll post your data online. Finally, they will threaten to tell the media to make sure your customers know about the attack. This disclosure can lead to additional legal costs, shareholder lawsuits and the need for regulatory compliance filings.

What Happens If You Don't Have a Security Plan?

Many organizations don't have a security and recoverability plan in place due to constraints that include lack of budget or manpower. If the organization has a security team, individual roles may not be properly defined.

If you don't have a response plan, things will get dicey because your security team won't know what to do. If a security engineer, analyst, incident responder identifies the attack without having a policy to give them a structure to work with, the organization could end up in total confusion. You may not understand the full scope of the compromise. They might take systems offline that don't need to be offline. You may be unable to provide your incident response vendor or internal team enough information to pass on to help with the scenario.

More Victims are Paying Ransom[17]

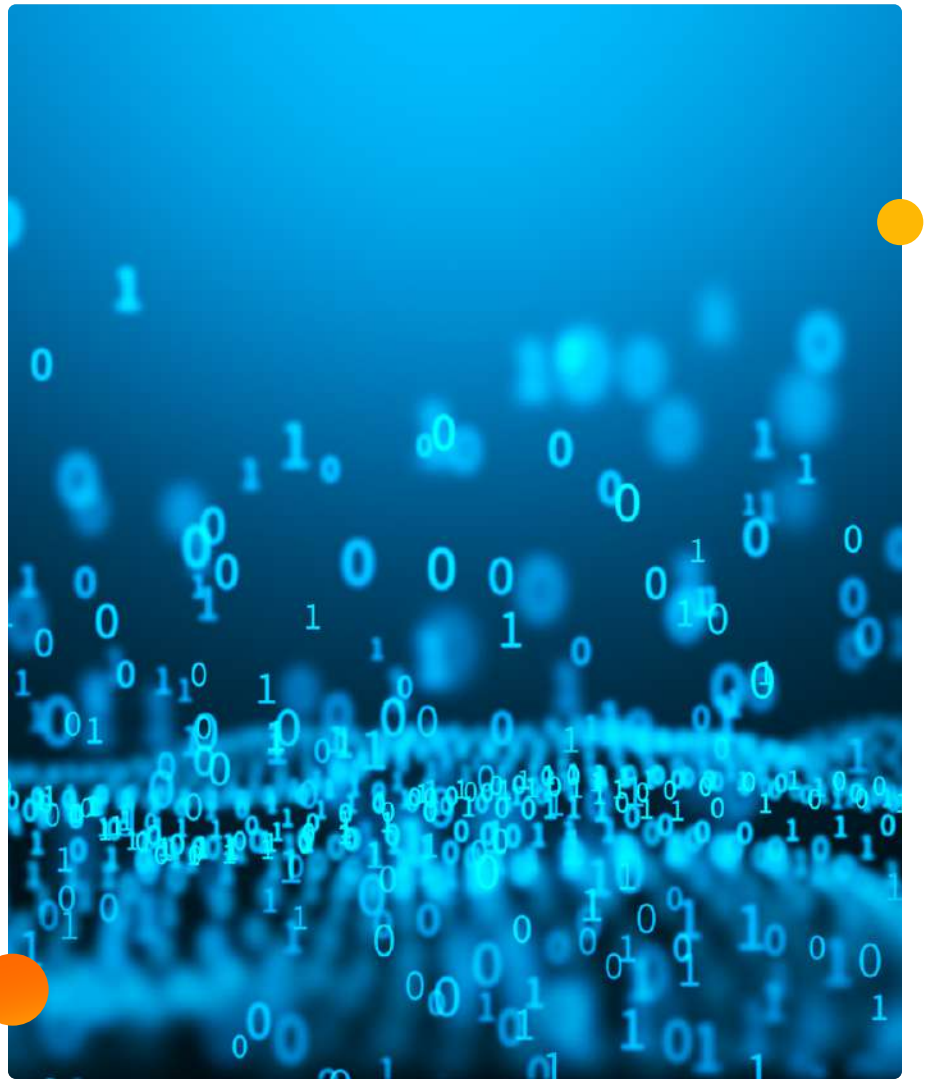
2020	2021	
26%	**32%**	**Paid Ransom to Get Data Back**
56%	**57%**	Used Backups to Get Data Back
12%	**8%**	Used Other Means to Get Data Back
94%	**96%**	Total That Got Data Back

Pillar 3—Restoring your Data After an Attack

Every minute your business is offline costs you money. According to Gartner, the average cost of IT downtime is $5,600 per minute. At the low end, downtime can cost as much as $140,000 per hour, $300,000 per hour on average, and as much as $540,000 per hour at the higher end.[18] And for a large company like Costco or Target or Walmart on Black Friday, the costs can easily rise to millions of dollars per minute.

A 2020 Coveware study reported that the average downtime for businesses as a result of a ransomware attack was 16.2 days.[19] And fully recovering from an attack takes even longer—an average of 287 days.[20]

With these high costs in mind, the shorter the duration of any breach the better. After the attack, you'll want to clean up and restore your systems as soon as possible.



Steps to Take After an Attack Has Occurred

Clean Up Your Systems

During the attack, your defense team should have isolated and disconnected compromised network systems. Once the attack is over, it's time to fully audit all the systems on your network to make sure no artifacts or malware remains. Otherwise, you might find yourself in a situation where you shut down multiple systems, do migrations, restore your data, and get the network back online only to have the automated ransomware reactivate. So, make sure you sanitize your environment before you restore data from your backups and go live.

Rapid Restore

Before you were attacked, you should have established proactive and preemptive recovery measures including implementing a BCDR plan. These plans should include having backups that you can restore from that were not deleted. You should also make sure you can recover quickly because every minute you're down costs you money. However, in order to effectively and rapidly restore, you must have a current or very recent point of recoverability. Without that, your recovery process will be slowed or even impossible. Ensuring your storage and backup solutions offer a degree of recoverability is absolutely critical. A good solution is to leverage modern storage technologies that prevent attackers from fully deleting your organization's data.

It is also important to have the appropriate sandbox environment available for forensic analysis of your snapshots and backup data. You can't just restore directly without performing a forensic review and cleansing to remove identified indicators of compromise left behind by the attacker. Having a solid logging environment in place that delivers the proper visibility will be critical through your restoration process as you seek to find "patient zero" in the attack.

Adapt, Recover, and Respond

After you're back up and running, it's important to review what happened, learn from that, and modify your systems and policies accordingly so you can move on in an educated manner. This postmortem evaluation should look not only at technology, but also at people and processes. For example, you may find that you need to educate users more comprehensively to recognize phishing attacks. By evaluating lessons learned and incorporating them into your plans and policies, you can continuously improve your readiness and response.

Conclusion

By understanding why and how ransomware attacks occur as well as what you should be doing before, during and after an attack occurs, you should be better prepared to prevent an attack or recover quickly. These actions should include putting in place the right tools, from the right vendor, with the proper implementation, and providing education for both your technical team and end users. You should also ensure that strong passwords are set and managed properly, as well as inventory your software and assets so you can protect them and minimize your attack surface.

Pure Storage solutions can help with these efforts. Pure ensures your data is safe from encryption by ransomware attackers, that it's stored in a protected manner, and that it leverages an out-of-band, multi-factor authentication approach to ensure that even people or processes with administrative access cannot fully delete data without manual interaction and intervention from Pure support. Pure's solutions ensure you have a starting point for recoverability and provide the fastest recovery solution available to get your business back up and running quickly. To learn more about Pure Storage ransomware solutions, visit the Pure Storage Ransomware webpage.

Endnotes:

1 - The State of Ransomware 2021 | Sophos

2 - FAQ: What you need to know about ransomware attacks | The Washington Post

3 - Ransomware attacks surge in 2021, Triple Extortion threat comes to light | SecurityBrief New Zealand

4 - Hacktivism returns to its roots as a cyber warfare tool | The Daily Swig

5 - 2020 Cyber Threatscape Report I Accenture

6 - Protecting the enterprise against state-sponsored attacks | 2021-05-19 | Security Magazine

7 - NSO Group / Q Cyber Technologies: Over One Hundred New Abuse Cases | the Citizen Lab

8 - Insurance giant CNA fully restores systems after ransomware attack | Bleeping Computer

9 - CNA Financial Paid $40 Million in Ransom After March Cyberattack | Bloomberg

10 - Sophos Survey: Ransomware Recovery Costs Near $2M | Dark Reading

11 - The ransomware plague cost the world over $1 billion | Help Net Security

12 - How Bitcoin Has Fueled Ransomware Attacks | NPR

13 - Bitcoin extortion: How cryptocurrency has enabled a massive surge in ransomware attacks | Marketwatch

14 - Bitcoin Keys Cannot be Hacked: Skeptics Question the Official Colonial Pipeline Bitcoin Seizure Story | Bitcoin News

15 - Are WordPress Websites Really That Vulnerable? | WPSec.com

16 - Cybereason: 80% of orgs that paid the ransom were hit again | Venture Beat

17 - The State of Ransomware 2021 | Sophos

18 - The Cost of IT Downtime | The 20

19 - 10 Shocking data loss and disaster recovery statistics | Comparitech

20 - Combating Ransomware. A Comprehensive Framework for Action | Ransomware Task Force

Author Bios

Hector Xavier Monsegur

Hector Monsegur is an internationally recognized expert on global cyber security issues and a leading voice on cyber-attacks and cyber warfare. As Director of Research at Alacrinet, Monsegur works to secure clients in technology, healthcare, finance, government, and other industries. In his leadership role, his unmatched technical experience is shared to both educate other operators and guide technical research. Formerly known by his online alias "Sabu," Monsegur was once the technical expert behind the Anonymous/ LulzSec hacker collectives. As a "black hat hacker", he highlighted critical vulnerabilities in numerous organizations, including governments, military organizations, and cyber security firms. Later, in working with the US Government, Monsegur identified key vulnerabilities—and potential attacks—against major federal infrastructure, including the US military and NASA. Since working with US government and commercial security executives around the world, he has helped prevent upwards of 350 cyber-attacks against US government computer systems.

Andy Stone

Andy Stone joined Pure Storage in April 2019 as CTO – Americas where he supports go-to-market and internal, product development activities. Prior to joining Pure, Andy worked at PwC as US and Global Chief Technology Officer and Global Head of Security Technology and Engineering supporting the Firm's 160 global territories and nearly 300,000 users. At PwC, Andy implemented a number of global technology solutions to improve overall usability, scalability and security posture while enhancing overall IT services' performance. He also led efforts to virtualize PwC desktops to improve end-user usability and protect from outside attacks and internal data leakage. Prior to PwC, Andy was the Farmers CISO and Global Head of Security Engineering, Architecture, Technology and Strategy for Zurich Insurance where he led a global security transformation across 140+ countries. Andy has also worked for Accenture, leading the creation of multiple security offerings including Identity and Access Management and Application Security as well as the Power of 3 security alliance between Accenture, Avanade, and Microsoft. He also worked with numerous, Global Fortune 500 companies, where he provided thought leadership and helped design, implement and support a broad set of custom and commercial technology solutions. Andy holds a BS in Business – Information Systems from Indiana University, Bloomington and an MBA from the University of Southern California. Andy has been presented at numerous conferences and been published on several topics in security and other technologies. Lastly, Andy holds patents in the security space for various identity and access management technologies.

PS2102-01 07/2021