CYBER SECURITY INGEST

APRIL 24, 2022

Analysis from

PurpleSec's Security Experts

LEARN CYBER SECURITY

No matter where your cyber security maturity lies today, this guide will help you learn to build a more secure business.

Access 9 different domains of security for **FREE**.

LEARN WITH US

CONTENTS

CYBER SECURITY STATISTICS

Every week we share a handful of cyber security statistics across the industry that we think you might be interested in. From the cost of cybercrime to the rise of supply chain attacks, our library of expertly curated security statistics has you covered:

Cybercrime growth since the beginning of the pandemic: **600%**

THE TOP NUMBER OF BREACH INCIDENTS (SOCIAL ENGINEERING)

Number of cyber attacks per day

80,000

Cost of ransomware damage in 2019

$11.5B

Malicious mobile apps blocked every day

24,000

RECENT CYBER ATTACKS & DATA BREACHES

As data breaches become more pervasive in our interconnected world so must our understanding of modern day cyber attacks.

In this series, we sit down with cyber security experts and get their take on the most recent and relevant cyber attacks and breaches.

In this week's issue we cover:

- ZLoader malware takedown

ZLOADER MALWARE TAKEDOWN

Analysis by: Josh Allen

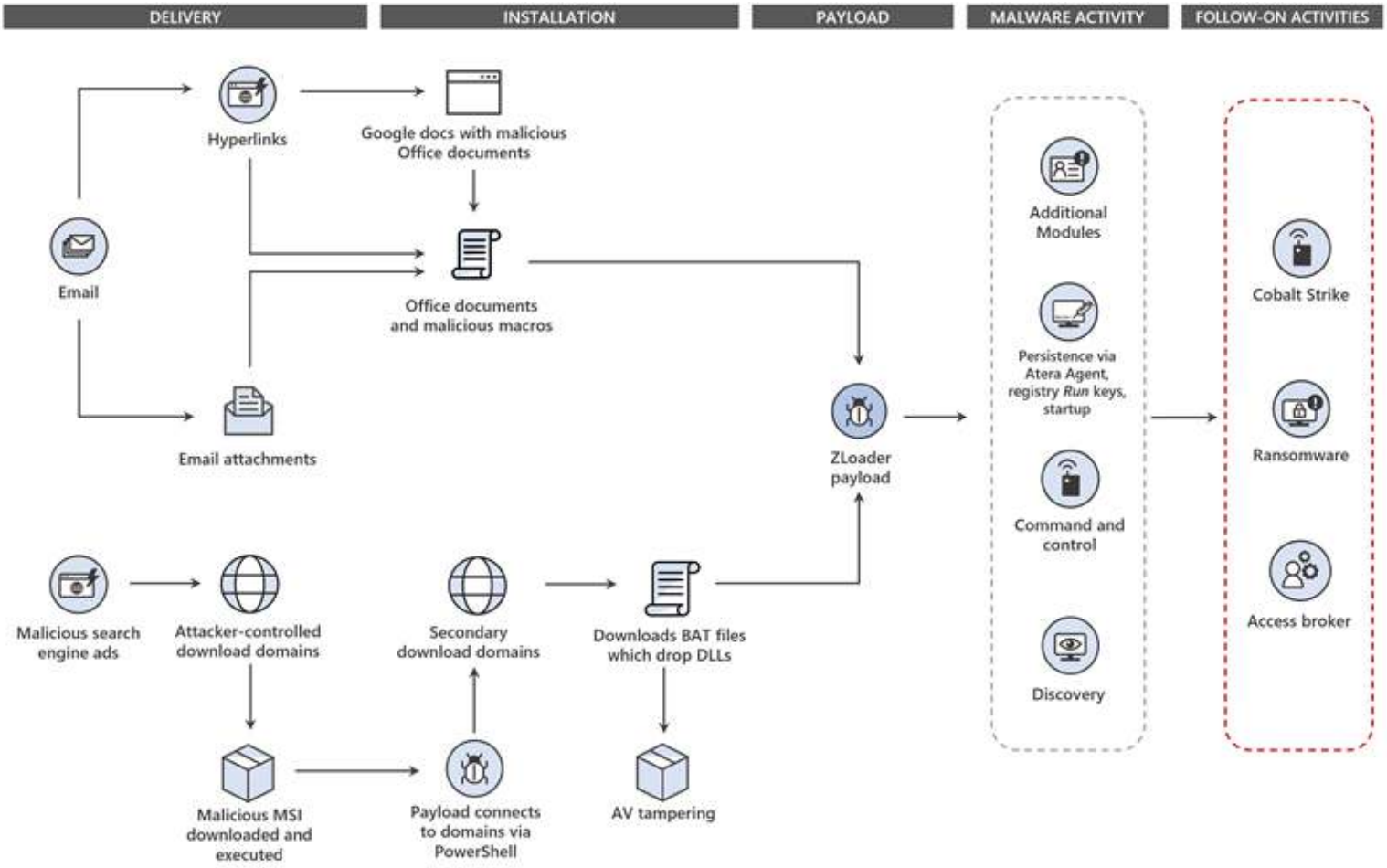

Image credit: *Microsoft Security Blog*

- Microsoft DCU partnered with other security companies to conduct a takedown of the botnet running ZLoader malware.
- Using Threat Intelligence, Data Science, Reverse Engineering, and cooperation, the task force captured over 300 domains registered for the botnet.
- ZLoader's origin is a trojan, but it has evolved into a Ransomware as a Service platform.
- ZLoader is the primary distributor of the Ryuk healthcare ransomware.

ZLOADER MALWARE TAKEDOWN

Analysis by: Josh Allen

On April 13, 2022, Microsoft announced that their Digital Crimes Unit (DCU) - in a joint effort with ESET, Black Lotus Labs, Palo Alto Networks, Health-ISAC, and Financial Services-ISAC – has successfully disrupted the botnet distributing the ZLoader trojan.

ZLoader is a malware derived from a banking trojan discovered in 2007 called Zeus, at one time called DELoader because it was seen in 2016 targeting German language systems. More than just a trojan, ZLoader has evolved over the years to do many things, with different goals.

Once it has been loaded onto a victim's computer the attacker is given persistent command and control of that system, as well as a toolset for discovering more potential victims and the ability to load custom modules. The capabilities of ZLoader can be highly customized for specific goals, but at a high level, it is able to deliver Cobalt Strike, various Ransomware, and remote desktop access through VNC. Eventually, the creators even added the ability to disable many popular consumer antivirus and other software.

The primary goal of ZLoader campaigns historically was financial theft; stealing information to be then used to steal money directly from victim accounts.

However, the creators of ZLoader shifted their focus around 2020 to primarily offer Malware as a Service, or Ransomware as a Service (RaaS) through the botnet which acts as the support platform for ZLoader. What they built became like a malicious AWS cloud specially crafted to support and run ransomware campaigns for anyone willing to pay for it.

To disrupt the ability of the botnet to distribute and control malware, Microsoft and its allies used data and threat intelligence to form a legal case and obtained a court order from the United States District Court for the Northern District of Georgia which allowed them to take control of 65 actively used domains that the ZLoader botnet used for command and control.

It was also discovered through reverse engineering that ZLoader also contains code to generate new domains as backup or scaling the communication channels; these 319 registered domains were also taken over by the Microsoft DCU taskforce. Once they had control of the domains, Microsoft redirected them to sinkholes – domains that Microsoft controls and have no content – effectively crippling ZLoader's ability to call back to the botnet and ultimately the attacker, and its ability to switch to backup domains after the initial takedown.

ZLOADER MALWARE TAKEDOWN

Analysis by: Josh Allen

This is a big win for Blue Teams everywhere. The ZLoader RaaS has been used many times to distribute the infamous Ryuk ransomware which is well known for wreaking havoc on several healthcare institutions, extorting money while putting the health and lives of patients at risk.

It is also a great example of collaborative cyber security and the kind of accomplishment many of us in cyber security hope to achieve one day. The task force was also able to identify one of the creators, Denis Malikov, and publicly identified his name and location as a statement against other ransomware operators.

References:

- Hogan-Burney, Amy. “Notorious Cybercrime Gang’s Botnet Disrupted.” Microsoft On The Issues." 13 Apr. 2022, https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine
- Microsoft 365 Defender Threat Intelligence Team. “Dismantling ZLoader: How Malicious Ads Led to Disabled Security Tools and Ransomware.” Microsoft On The Issues, 13 Apr. 2022, https://www.microsoft.com/security/blog/2022/04/13/dismantling-zloader-how-malicious-ads-led-to-disabled-security-tools-and-ransomware
- Malpedia. “ZLoader.” Malpedia, https://malpedia.caad.fkie.fraunhofer.de/details/win.zloader

GOVERNMENT POLICY & REGULATION

Many of the toolkits, processes, strategies, and technologies that enter the commercial sectors come down from the U.S. government and its military branches.

Our experts, Rich Selvidge and Josh Allen have over 30 years of combined experience working firsthand for U.S. Cyber Command, DoD, Special Operations, and Defense Industries to bring their analysis on the latest regulations, departments, and techniques that you should need to know.

In this week's issue we cover:

- Enterprise Patch Management
- Bureau of Cyberspace and Digital Policy (CDP) is established

ENTERPRISE PATCH MGMT

Analysis by: Rich Selvidge, CISSP

The National Institute of Standards and Technology's (NIST) National Cybersecurity Center of Excellence (NCCoE) issued final recommendations on enterprise patch management to assist enterprises in preventing vulnerabilities and exploitation of their IT systems.

Patching and preventative maintenance should be prioritized in order to minimize data breaches and operational interruptions, according to the two publications (SP-800-40 and SP 1800-31).

SP-800-40 is a planning reference for enterprise patch management, whereas SP-1800-31 looks at use cases and strategies for enhancing corporate patching processes for general IT systems.

Threat actors can easily get access to a network through unpatched devices and systems. Due to its mobility and the fact that enterprises may not know how many devices are on their networks at any given moment, medical devices in particular can be challenging to patch.

NCCoE's advice was aimed at chief information officers, cybersecurity directors and managers, chief information security officers (CISOs), and anyone else who would be in charge of software risk management.

“Once a new vulnerability becomes publicly known, risk usually increases because attackers are more likely to develop exploits that target the vulnerable software.”

Although immediate patching is desired, the document stated that in some cases, immediate patching is unrealistic. To manage vulnerability patching, it is critical to understand how to appropriately assess risk. Asset inventories should be kept, and organizations should learn how emerging vulnerabilities may affect their most vital assets.

Organizations should plan patch deployment, evaluate the patch, and confirm it via automation before delivering it. It is critical that IT teams monitor the fixes that have been applied after they have been implemented, according to the magazine.

"How dynamic and distributed computer assets are, as well as the sheer quantity of deployed software components to patch, has made corporate patch management more difficult recently."

Furthermore, depending on the kind of asset (e.g., OT, IoT, mobile, cloud, conventional IT, virtual machines, containers), patch management methods and technologies assume varied shapes," according to the paper.

As a result, many companies are finding it difficult to keep up with patching. Patching has a tendency to become reactive (i.e., swiftly release a patch when a serious vulnerability is widely exploited) rather than proactive (i.e., fast deliver patches to address numerous vulnerabilities before they are likely to be exploited).

"Reactive patching may leave systems vulnerable to threat actors. However, due to the persistent cyber security talent scarcity, many firms are operating with understaffed security teams that have less time to dedicate to proactive and preventative security measures. Nonetheless, putting in place reaction plans and risk management methods ahead of time can save time overall."

The report also advised businesses to depend on automation to reduce workloads and to plan for security disasters.

"To enhance enterprise patch management, businesses must modify their culture so that employees are prepared to confront problems when they occur, rather than dreading them and so postponing risk responses," according to the NCCoE.

"The company must become more robust, and everyone inside it must recognize that patching difficulties are a necessary nuisance that helps prevent big compromises."

Using automated methods to monitor the efficiency of imposed technological controls in real time can give a far more dynamic perspective of the controls' effectiveness and the organization's security posture.

All installed security controls, including management and operational controls, must be frequently reviewed for efficacy as part of any complete information security program, even if monitoring of such controls cannot or is difficult to automate.

ENTERPRISE PATCH MGMT

Analysis by: Rich Selvidge, CISSP

What you should do.

- Reassess your patch management program, is it providing adequate coverage or are there gaps?
- If you do not have the staff or talent look for a provider who specializes in vulnerability management strategies. Anyone can point a scanner at your enterprise and call it a program.
- Update software regularly, unpatched software opens your network to multiple attack vectors.

References:

- https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf
- https://www.nccoe.nist.gov
- https://hbr.org/2012/06/managing-risks-a-new-framework
- https://healthitsecurity.com/news/nist-highlights-enterprise-patch-management-in-latest-guidance

ESTABLISHMENT OF CDP

Analysis by: Josh Allen

Image credit: *US Department Of State*

The United States Department of State announced on April 4, 2022, the creation of the Bureau of Cyberspace and Digital Policy (CDP). The CDP will serve as an important piece of national security in cyberspace.

Its mission is to lead and coordinate the Department of State's activities in cyberspace and advance policies to protect the integrity and security of the internet's infrastructure. Multiple units of the CDP will be dedicated to different missions which together will bring about more security, neutrality, and privacy on the internet.

With the recent announcement of the creation of the Bureau of Cyberspace and Digital Policy (CDP) comes a lot of potential for US privacy and cyber security laws to advance. US consumer data privacy laws have long dragged behind trends and technology, as well as lagging the EU and UK.

ESTABLISHMENT OF CDP

Analysis by: Josh Allen

One of the largest and most popularly used privacy laws in the United States is the Privacy Act of 1974. This fifty-year-old legislation governs the collection, maintenance, use, and dissemination of Personally Identifiable Information (PII); but it only applies to federal agencies.

The most recent win for privacy legislation was the passing of the California Consumer Privacy Act (CCPA) in June of 2018. While the state statute aimed to protect the personal data of typical home users and to give them some control of their data's use, it is much too limited in scope to be an effective data privacy law for Americans because it is limited to companies with revenues in excess of $25 billion; clearly aimed at companies like Facebook and Twitter.

California and other states have been leading the way in this arena very slowly up until now. The CDP's mission will hopefully accelerate the creation and adoption of Federal level consumer privacy laws that are relevant to the modern age and which apply to all people living in the US.

To accomplish this goal, the CDP has set up three departments, which it calls Policy Units, each with its own set of goals and focus.

- **International Cyberspace Security** – They will focus on the CDP's efforts to promote cyberspace stability and security to protect US national security interests in cyberspace. This unit will work with other nations to respond to malicious cyber activity.
- **International Information and Communications Policy** – This team will work to secure systems that are critical to our economies such as 5G, telecom services, supply chain security, and infrastructure. To promote a secure and fair digital economy, they will team up with multiple stakeholders in industry and government to develop internet governance and technical standards.
- **Digital Freedom Unit** – The DFU will be the nexus of the CDP's work on privacy, security, content moderation policy, tech platform regulation, human rights, and civic engagement. The DFU's goal is to protect the internet from repressive and authoritarian practices.

Heading up the department are five senior officials with various experiences in diplomacy, policy, telecommunications, and human rights.

You can learn more about the CDP and their efforts on Promoting Stability and Security, Advancing the Digital Economy, Advancing Digital Freedom, and Building Global Cyber and Digital Capacity by visiting the Department of State's website at https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/

HEALTHCARE SECURITY

Get thought leadership analysis and actionable steps you can take to better secure your organization from cyber attacks. Led by our in house expert, Rich Selvidge, we'll get you up to date on the latest breaches and regulations in healthcare security.

In this week's issue we cover:

- Mailchimp compromised
- BakerHostetler lawsuits
- Hive ransomware group

MAILCHIMP COMPROMISED

Analysis by: Rich Selvidge, CISSP

Image credit: *HHS Cybersecurity Program*

A breach affecting a reputable email marketing platform that has been used to send phishing emails has been discovered by the Health Sector Cybersecurity Coordination Center (HC3).

While the unlawful access was used to target users in the cryptocurrency and financial sectors, it's feasible that the unauthorized access may be used to target users in the Healthcare and Public Health (HPH) sector as well. These businesses should be aware of the threat and take the necessary precautions.

MAILCHIMP COMPROMISED

Analysis by: Rich Selvidge, CISSP

Mailchimp, an email marketing platform company, revealed a compromise affecting one of its internal technologies used by its customer service and account management staff on April 4, 2022. Although Mailchimp disabled the compromised employee accounts upon the breach's discovery, threat actors were still able to see about 300 Mailchimp user accounts and gain audience data from 102 of them, according to the company's CISO.

Additionally, threat actors gained access to an unspecified number of customers' API keys, which enabled attackers to develop custom email campaigns, such as phishing campaigns, and send them to mailing lists without logging into the MailChimp client interface.

While HC3 is currently aware of only one phishing campaign that exploited this unauthorized access to send phony data breach notification emails to users in the cryptocurrency and finance sectors (which was reportedly carried out with exceptional sophistication and planning), the Healthcare and Public Health (HPH) sector should remain vigilant for suspicious emails originating from legitimate email marketing platforms such as MailChimp.

It's critical to remember that APT groups have previously used legitimate mass-mailing providers to launch malicious email campaigns against a diverse range of businesses and industry verticals.

MAILCHIMP COMPROMISED

Analysis by: Rich Selvidge, CISSP

- User awareness training continues to be one of the most effective defenses against phishing attempts, which are a type of social engineering, particularly in this campaign, which used emails from a reputable source.
- Additional mitigation measures include the implementation of antivirus and network intrusion prevention systems, as well as the restriction of web-based information that is not required for business operations.
- A Vulnerability Management system that keeps workstations continually patched can help to mitigate any vulnerabilities that an attacker would use to gain a foothold in your network is vital.
- Anti-spoofing and email authentication technologies can also be used to filter communications based on the sender domain's authenticity (through SPF) and the message's integrity (using DKIM).
- Enabling these processes within an organization (through policies such as DMARC) may enable recipients to undertake comparable message filtering and validation (both intra- and cross-domain).

References:

- 9to5Mac: "PSA: Watch out for phishing emails from genuine mailing lists, following Mailchimp hack" April 05, 2022. https://9to5mac.com/2022/04/05/mailchimp-hack-phishing-alert/
- HC3. “Malicious Use of Email Marketing Services,” February 11, 2021. https://www.hhs.gov/sites/default/files/threat-posed-by-bulk-email-services.pdf
- HC3. “Phishing Campaigns Demonstrate Importance of User Training and Awareness,” September 02, 2021. https://www.hhs.gov/sites/default/files/phishing-analyst-note-tlpwhite.pdf

BAKERHOSTETLER LAWSUITS

Analysis by: Rich Selvidge, CISSP

BakerHostetler saw an uptick in data breach lawsuits in the weeks following incident notification, especially against healthcare organizations.

- Limit access to your most valuable data, develop data classification policies and protect accordingly.
- Third-party vendors must comply with your data protection policies.
- Conduct employee security awareness training, employee mistakes account for over 80% of breaches.
- Update software regularly, unpatched software opens your network to multiple attack vectors.
- Develop a cyber breach response plan, know how to respond in the event of a breach.

As healthcare data breaches continue to wreak havoc on small and large businesses around the country, data breach lawsuits are becoming more widespread. According to the latest data security incident report from legal firm BakerHostetler, there has been a spike in duplicative litigation, which typically result in high defense and settlement costs.

BakerHostetler looked at over 1,200 data security events that its Digital Assets and Data Management Practice Group employees assisted clients with between 2021 and 2022. The occurrences affected a wide range of industries, but the data indicated that healthcare was the most heavily impacted, accounting for 23% of all incidents studied.

According to the research, twenty-three of the occurrences resulted in at least one lawsuit. While this may not appear to be a large amount, the twenty-three instances resulted in over fifty-eight lawsuits.

"*There was always the danger of multidistrict litigation following significant data breaches in the past.*"

However, we increasingly see many cases filed in the same federal court after an event is reported. Alternatively, we observe a handful of instances in one federal court and another handful of cases in a state forum," according to the paper.

"Due to the number of plaintiffs' attorneys participating, this duplicative litigation tendency is increasing the 'race to the courthouse' filings, as well as the initial lawsuit defense expenses and the eventual settlement cost."

As previous instances have demonstrated, plaintiffs' success in healthcare data breach litigation is tough. This is in part due to the Supreme Court's decision in Ramirez v. TransUnion, which said that data breach victims must show real damages and prove that the defendant's actions caused the damage.

BAKERHOSTETLER LAWSUITS

Analysis by: Rich Selvidge, CISSP

The June 2021 decision marked a fundamental shift in the way data breaches are dealt with in court. To establish Article III standing, plaintiffs must now show that they have experienced tangible damage.

For example, a court recommended dismissing a class-action lawsuit against medical management business Practice first in February 2022, claiming a lack of proof of actual injury caused by a December 2020 breach.

"*There have been very few published class certification judgments after data events over the last decade," BakerHostetler stated, "yet the majority of those that did exist were beneficial to the defense."*

"However, two significant class certification judgments in 2020 and 2021 are emboldening plaintiffs' firms, both in terms of the volume of lawsuits they file and their negotiating techniques during mediations."

In addition to legal insights, the research stated that ransomware will be responsible for 37% of events in 2021, up from 27% in 2020. Hackers were also seen utilizing double or triple extortion techniques to put further pressure on victims, according to the business.

In a press release, Craig Hoffman, co-leader of BakerHostetler's national digital risk advisory and cybersecurity team, said that:

"A key difference between organizations that had meaningful ransomware events and those that did not was the use of an endpoint detection and response (EDR) tool that was set in enforcement mode with the anti-uninstall feature enabled."

***References**:*

- Bakerlaw: "Lynn Sessions Talks about Data Security Incident Response Report and Healthcare Industry." April 12, 2019. https://www.bakerlaw.com/news/lynn-sessions-talks-about-data-security-incident-response-report-and-healthcare-industry
- Reuters: "Plaintiffs' lawyer trio tapped as leads in T-Mobile data breach litigation." February 25, 2022. https://www.reuters.com/legal/litigation/plaintiffs-lawyer-trio-tapped-leads-t-mobile-data-breach-litigation-2022-02-25/
- Seyfarth Shawl LLP: "Annual Workplace Class Action Litigation Report" https://www.seyfarth.com/dir_docs/publications/2022_WCAR_Executive_Summary.pdf
- DR Journal: "BakerHostetler Launches 2022 Data Security Incident Response Report — Resilience and Perseverance." April 07, 2022. https://drj.com/industry_news/bakerhostetler-launches-2022-data-security-incident-response-report-resilience-and-perseverance/

HIVE RANSOMWARE GROUP

Analysis by: Rich Selvidge, CISSP

Image credit: *Getty Images*

HHS's Health Sector Cybersecurity Coordination Center (HC3) issued an analyst note regarding the Hive ransomware group, the notorious cybercrime group responsible for multiple attacks against the healthcare sector.

"Hive is an exceptionally aggressive, financially-motivated ransomware group known to maintain sophisticated capabilities who have historically targeted healthcare organizations frequently," the note warned.

"HC3 recommends the Healthcare and Public Health (HPH) Sector be aware of their operations and apply appropriate cybersecurity principles and practices found in this document in defending their infrastructure and data against compromise."

HIVE RANSOMWARE GROUP

Analysis by: Rich Selvidge, CISSP

Hive claimed responsibility for an August 2021 attack against Memorial Health System that impacted 215,000 individuals and resulted in data exfiltration. Hive was also tied to a September 2021 cyberattack at Missouri Delta Medical Center, and HC3 identified the group as one of the top US healthcare ransomware threats in Q3 2021.

In March 2022, Hive claimed responsibility for stealing 850,000 records containing personally identifiable information (PII) from Partnership HealthPlan of California.

According to HC3, Hive uses the ransomware as a service (RaaS) concept to gain access to victim infrastructure as well as their affiliates.

The business uses Golang as a malware programming language, and RDP and VPN infiltration, as well as phishing, are frequently used. The group is well-known for examining target PCs for data backup processes and then deleting shadow copies and system snapshots to interrupt them.

"Hive removed Tor negotiation URLs from their encryptor to prevent security researchers from retrieving the ransom message and listening in on chats," HC3 observed.

The extensions .hive, and .key are widely used by Hive to end encrypted files. HC3 noted that *"many of Hive's actions are typical procedure among ransomware operators." "However, they have a set of unique powers that distinguish them."*

Hive employs a range of tactics, methods, and procedures (TTPs), as detailed in the FBI's August 2021 flash notice, making mitigation and defense challenging.

"There are common measures that should be followed while protecting against Hive or any other ransomware version." "The best method is always to prevent," said HC3.

MFA, strong passwords, and data backups should all be used by businesses. HC3 suggested that businesses use the 3-2-1 rule for data backups, which means that data should be backed up in three distinct locations, on two distinct types of media, and one of them should be maintained offline.

Along with endpoint security measures, continuous monitoring and a strong vulnerability management program are critical mitigation methods.

Hive has likely modified its techniques to remain a substantial and unpredictable threat to the US healthcare industry, according to HC3, which led organizations to a mechanism for obtaining the secret key for decryption uncovered by Cornell University researchers.

What can you do?

1. Patch Your Systems

Many IT executives concentrate their efforts fighting ransomware on preventing zero-day threats. But consider this: According to a recent study, over two-thirds of system vulnerabilities are due to defects discovered two years ago.

That indicates that if you make the effort to utilize accessible updates, the majority of your vulnerabilities are already fixed. Low-hanging fruit is a favorite of hackers. Allowing them to locate it on your machine is not a good idea. Get a vulnerability check done first, and then fill in the holes.

2. Actively Monitor Your Systems

If a ransomware actor manages to gain a foothold in your system, quickly detecting it allows you to stop the attack before it escalates. According to IBM, the typical breach is discovered after 280 days. You are capable of much more.

The most recent protection is a Managed Extended Detection and Response system that continuously monitors activity, use artificial intelligence to detect several diverse actions as a brewing attack, and actively intervenes to stop suspicious behavior.

3. Segment your systems

You can restrict how far ransomware hackers can get if they infiltrate one area of your network by efficiently isolating/air-gapping separate components of your system.

4. **Limit Each User's Access**

Similar to the previous point, implementing a policy of least-privileged access and Identity and Access Management means you keep hackers from getting into your entire system if they compromise one user's credentials.

4. Have a Robust Backup Strategy

Even if ransomware encrypts your data, you can swiftly restore operations provided you have a good backup. To verify that the backup is working properly, test it frequently.

5. Plan Ahead

When you get a warning that you have been affected by ransomware, a clear incident response strategy helps everyone know what to do to mitigate the damage. Companies who have an IR plan in place before a breach have 38 percent lower breach expenses.

References:

- https://www.infosecurity-magazine.com/news/hhs-issues-warning-us-healthcare/
- https://www.hhs.gov/about/agencies/asa/ocio/hc3/about/index.html
- https://www.weforum.org/agenda/2021/11/healthcare-cybersecurity/
- https://www.medtechdive.com/news/hhs-opens-cybersecurity-coordination-center-after-troubled-year/541034/

CRYPTO & BLOCKCHAIN

With the rise of cryptocurrency came the seemingly endless applications of blockchain technologies. One of the most interesting applications is in the cyber security space.

Our expert, Ken Thomas, brings forward his analysis on current trends in the crypto and blockchain community and attempts to demystify and explain its uses well beyond the marketing buzzwords.

In this week's issue we cover:

- Kraken warns users
- Centralized decentralization

KRAKEN WARNS USERS

Analysis by: Ken Thomas

Amidst growing privacy concerns Kraken CEO Jesse Powell took to Twitter warning users they would be forced to comply with the Canadian Emergencies Powers Act if asked to.

Jesse states *"If you're worried about it, don't keep your funds with any centralized/regulated custodian. We cannot protect you. Get your coins/cash out and only trade p2p."*

The Emergencies Powers Act was invoked on February 14, 2022, in response to on-going protests concerning mask mandates in Canada. Individuals and companies alike are potentially at risk if they use cryptocurrency, or lending platforms such as GoFundMe to support protest efforts.

On February 17, 2022, Deputy Prime Minister Chrystia Freeland stated *"The names of both individuals and entities as well as crypto wallets have been shared by the RCMP with financial institutions and accounts have been frozen and more accounts will be frozen."*

CENTRALIZED DECENTRALIZATION?

Analysis by: Ken Thomas

An essential component of blockchain technology is decentralization, however, users of popular software from Consensys (Metamask, Infura) could find themselves unable to transact due to centralized efforts.

On March 3rd, 2022 Venezuelan users of MetaMask were unable to connect to the Ethereum network after an IP block intended for separatist regions in Ukraine. Infura apologized for the interruption on Twitter adding that *"MetaMask relies on Infura as the default endpoint, but this setting can be modified by users if desired, or in case of any service interruptions"*.

Users wishing to use RPC endpoints other than Infura may do so here - https://www.youtube.com/watch?v=8ruuz3u2V2E

- The browser is the primary vector of attack for crypto wallets such as MetaMask. Check your updates frequently and keep your browser free of zero days.
- Not your keys, not your crypto.
- Use custom RPC endpoints such as pokt.network or consider running your own node.

ABOUT PURPLESEC

PurpleSec is a veteran led cyber security company based outside of Washington, DC. Our cyber security experts have received extensive experience and training from operations serving in the U.S. Cyber Command, DoD, Special Operations, Defense and Private Industries.

Now we're bringing the best of breed practices to the commercial marketplace. Our team have decades of experience servicing complex, multifaceted IT Security needs in warfare, private industry, healthcare IT and government.

Our proven methods backed by experts with decades of experience at the Department of Defense work to seamlesslessly integrate security into your existing business processes.

FREE CONSULT

MEET OUR EXPERTS

Rich Selvidge, CISSP

Rich Selvidge is the CISO at PurpleSec with over 21 years of information technology and security risk management experience. Prior to joining PurpleSec, he was the Manager of Information Security Governance and Compliance at American Automobile Association national office.

Working at various offices within the Department of Defense, Rich was responsible for teams of information security professionals who provided information security risk prevention and deterrence services, globally.

He was simultaneously accountable for all information security controls outside of the United States within the DoD Research community covering forty-eight countries.

MEET OUR EXPERTS

Josh Allen

Joshua is a diversely-skilled cyber security professional with 10 years of Department of Defense cyber security experience. He currently serves as PurpleSec's Chief Product Officer responsible for creating and developing bleeding edge technologies and processes to service SMB and Enterprise clients.

Josh has recently served as a team lead for a Secure Operations (SOC) environment supervising a team in a fast-paced cloud security as a service company. Joshua’s skillsets include enterprise architecture hardening, penetration testing, web application firewall management, network security, data privacy and classification, and enterprise risk assessment.

MEET OUR EXPERTS

Seth Kimmel, OSCP

Seth is an accomplished cyber security professional with 10 years of proven experience leading teams and projects to successful completion for an enterprise company with over 700 employees. Seth is the co-founder and Chief Technology Officer of PurpleSec, as well as a military veteran having served 6 years in the United States Marine Corps.

Seth holds both a BS in Security Risk Analysis – Information and Cyber Security, from Pennsylvania State University, and the coveted Offensive Security Certified Professional (OSCP) certification. When Seth isn't building systems to defend against cyber attacks, you'll find him outdoors spending time with his Golden Retriever, Murphy, or wrapped up in a Hardcore History podcast.

MEET OUR EXPERTS

Kenneth Thomas

Kenneth Thomas is a Corporate Security Professional for the Oil & Gas industry with over 10 years of cyber security experience and the founder of Telegram web3 community '**meefs NFT Corner**'.

Kenneth specializes in enterprise cloud security, blockchain development, and community building. Kenneth has a passion for artificial intelligence, creating bespoke meta verse experiences, and cloud architecture.

MEET OUR EXPERTS

Jason Firch, MBA

Jason is a veteran IT operations manager and digital marketer with a decade of experience. He is also the co-founder of PurpleSec and services as both the CEO and CMO.

Throughout his career, Jason has developed, deployed and evaluated successful digital, inbound, paid, social media and content marketing initiatives in technology industries.

Jason holds both an MBA and BA with a focus on marketing from Bloomsburg University of Pennsylvania. He is a recipient of multiple sales awards and has been published in an international business journal. When he's not studying for his CISSP or contributing to the PurpleSec blog, you'll find Jason helping nonprofits with their online marketing.