Cybersecurity Open Source Intelligence Weekly Wrap-Up
Wednesday, September 1, 2021

Ransomware

FBI Shares Technical Details for Hive Ransomware

The Federal Bureau of Investigation (FBI) has released some technical details and indicators of compromise associated with Hive ransomware attacks. In a rare occurrence, the FBI has included the link to the leak site where the ransomware gang publishes data stolen from companies that did not pay. Hive ransomware relies on a diverse set of tactics, techniques, and procedures, which makes it difficult for organizations to defend against its attacks, the FBI says. Among the methods that the gang uses to gain initial access and to move laterally on the network, there are phishing emails with malicious attachments and the Remote Desktop Protocol (RDP).
https://www.bleepingcomputer.com/news/security/fbi-shares-technical-details-for-hive-ransomware/

How to Stay Secure from Ransomware Attacks this Labor Day Weekend

Labor Day weekend is just around the corner and, believe it or not, cybercriminals are likely just as excited as you are! Ransomware gangs have nurtured a nasty habit of starting their attacks at the least convenient times: When computers are idle, when employees who might notice a problem are out of the office, and when the IT or security staff who might deal with it shorthanded. They like to attack at night and at weekends, and they love a holiday weekend. Indeed, while many people are looking forward to catching up with friends and family this Labor Day weekend, cybercrime gangs are likely huddling, too, planning to attack somebody. On the last big holiday weekend, Independence Day, attackers using REvil ransomware celebrated with an enormous supply-chain attack on Kaseya, one of the biggest IT solutions providers in the US for managed service providers (MSPs). Threat actors used a Kaseya VSA auto-update to push ransomware into more than 1,000 businesses.
https://blog.malwarebytes.com/101/how-tos/2021/08/how-to-stay-secure-from-ransomware-attacks-this-labor-day-weekend/

How Ransomware Runs the Underground Economy

The unwanted attention attracted by ransomware attacks recently have caused several of the top cybercrime forums to ban ransomware discussions and transactions on their platforms earlier this year. While some hoped this might have a significant impact on the ability of ransomware groups to organize themselves, the bans only pushed their activity further underground, making it harder for security researchers and companies to monitor it. If anything, the attacks in the months that followed the forum bans then have been more potent and audacious than ever. The truth is that ransomware is the life blood of the cybercrime economy and it will take extraordinary measures to put an end to it. The groups coordinating the attacks are highly professionalized and in many ways resemble modern corporate structures with development teams, sales and PR departments, external contractors and service providers that all get a cut from the illegal proceeds. They even use business lingo in their communications with victims, referring to them as clients who buy their data decryption services. https://www.csoonline.com/article/3631534/how-ransomware-runs-the-underground-economy.html

Threats/Vulnerabilities

Cold Wallet, Hot Wallet, or Empty Wallet? What is the Safest Way to Store Cryptocurrency?

In August of 2021, a thief stole about $600 million in cryptocurrencies from The Poly Network. They ended up giving it back, but not because they were forced to. Slightly more than one week later, Japanese cryptocurrency exchange Liquid was hacked and lost $97 million worth of digital coins. These examples of recent news about hacked cryptocurrency exchanges left many investors wondering whether it was still smart to invest in cryptocurrencies and how to keep them safe. We can't answer the first question for you. I wish I knew. But we can explain the terminology, the methods, and the risks. So you can decide which would be best for you. Full Article: https://blog.malwarebytes.com/crypto/2021/08/cold-wallet-hot-wallet-or-empty-wallet-what-is-the-safest-way-to-store-cryptocurrency/

CISA Adds Single-Factor Authentication to the List of Bad Practices

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added single-factor authentication to the short list of "exceptionally risky" cybersecurity practices that could expose critical infrastructure as well as government and the private sector entities to devastating cyberattacks. Single-factor authentication is a method of signing in users to websites and remote systems by using only one way of verifying their identity, typically a combination of username and password. It's considered to be of low-security, since it heavily relies on "matching one factor — such as a password — to a username to gain access to a system." But with weak, reused, and common passwords posing a grave threat and emerging a lucrative attack vector, the use of single-factor authentication can lead to unnecessary risk of compromise and increase the possibility of account takeover by cybercriminals. https://thehackernews.com/2021/08/cisa-adds-single-factor-authentication.html

Cybersecurity Advisory: Top Routinely Exploited Vulnerabilities

This advisory provides details on the top 30 vulnerabilities—primarily Common Vulnerabilities and Exposures (CVEs)—routinely exploited by malicious cyber actors in 2020 and those being widely exploited thus far in 2021.
Cyber actors continue to exploit publicly known—and often dated—software vulnerabilities against broad target sets, including public and private sector organizations worldwide. However, entities worldwide can mitigate the vulnerabilities listed in this report by applying the available patches to their systems and implementing a centralized patch management
system. http://7thspace.com/headlines/1653370/cybersecurity_advisory__top_routinely_exploited_vulnerabilities.html?utm_campaign=cyber-daily&utm_medium=email&_hsmi=153316601&utm_content=153316601&utm_source=hs_email

File Upload Security Best Practices Rarely Implemented to Protect Web Applications

Despite a marked increase in concerns around malware attacks and third-party risk, only 8% of organizations with web applications for file uploads have fully implemented the best practices for file upload security, a report from OPSWAT reveals. Most concerning, one-third of organizations with a web application for file uploads do not scan all file uploads to detect malicious files and a majority do not sanitize file uploads with CDR to prevent unknown malware and zero-day attacks. "The hybrid workspace has been driving digital transformation and cloud migration initiatives for a while now, and the rise of cloud services, mobile devices, and remote workers has driven organizations to develop and deploy web applications that enhance the experience for their customers, partners, and employees," said Benny Czarny, CEO at OPSWAT. "Web applications for file uploads help to streamline their business by making it faster, easier, and less expensive to submit and share documents. Consequently, this adoption has also introduced new attack surfaces that organizations are not effectively protecting." https://www.helpnetsecurity.com/2021/08/30/file-upload-security/

Cyberattackers are Now Quietly Selling Off Their Victim's Internet Bandwidth

Cyberattackers are now targeting their victim's internet connection to quietly generate illicit revenue following a malware infection. On Tuesday, researchers from Cisco Talos said "proxyware" is becoming noticed in the cybercrime ecosystem and, as a result, is being twisted for illegal purposes. Proxyware, also known as internet-sharing applications, are legitimate services that allow users to portion out part of their internet connection for other devices, and may also include firewalls and antivirus programs. Other apps will allow users to 'host' a hotspot internet connection, providing them with cash every time a user connects to it. It is this format, provided by legitimate services including Honeygain, PacketStream, and Nanowire, which is being used to generate passive income on behalf of cyberattackers and malware developers. https://www.zdnet.com/article/cyberattackers-are-now-quietly-selling-off-their-victims-internet-bandwidth/

Cybercriminal sells tool to hide malware in AMD, NVIDIA GPUs

Cybercriminals are making strides towards attacks with malware that can execute code from the graphics processing unit (GPU) of a compromised system. While the method is not new and demo code has been published before, projects so far came from the academic world or were incomplete and unrefined. Earlier this month, the proof-of-concept (PoC) was sold on a hacker forum, potentially marking cybercriminals' transition to a new sophistication level for their attacks. https://www.bleepingcomputer.com/news/security/cybercriminal-sells-tool-to-hide-malware-in-amd-nvidia-gpus/

Hacks/Breaches

China's Microsoft Hack May Have Had a Bigger Purpose Than Just Spying

NPR's months-long examination of the attack — based on interviews with dozens of players from company officials to cyber forensics experts to U.S. intelligence officials — found that stealing emails and intellectual property may only have been the beginning. Officials believe that the breach was in the service of something bigger: China's artificial intelligence ambitions. The Beijing leadership aims to lead the world in a technology that allows computers to perform tasks that traditionally required human intelligence — such as finding patterns and recognizing speech or faces. "There is a long-term project underway," said Kiersten Todt, who was the executive director of the Obama administration's bipartisan commission on cybersecurity and now runs the Cyber Readiness Institute. "We don't know what the Chinese are building, but what we do know is that diversity of data, quality of data aggregation, accumulation of data is going to be critical to its success." https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying

T-Mobile Hack Involved Exposed Router, Specialized Tools and Brute Force Attacks

T-Mobile's CEO and an individual who claims to be behind the recent hacking of the mobile carrier's systems have shared some information about how the attack was carried out. In a statement issued on Friday, Mike Sievert, CEO of T-Mobile, said that while the company's investigation into the incident was "substantially complete," he could not share too many technical details due to the criminal investigation conducted by law enforcement. He did, however, share a high-level summary of the attack. "What we can share is that, in simplest terms, the bad actor leveraged their knowledge of technical systems, along with specialized tools and capabilities, to gain access to our testing environments and then used brute force attacks and other methods to make their way into other IT servers that included customer data," he said. "In short, this individual's intent was to break in and steal data, and they succeeded." https://www.securityweek.com/t-mobile-hack-involved-exposed-router-specialized-tools-and-brute-force-attacks

Phishing

DMARC 101: How to Keep Phishing Attacks Out of Your Inbox

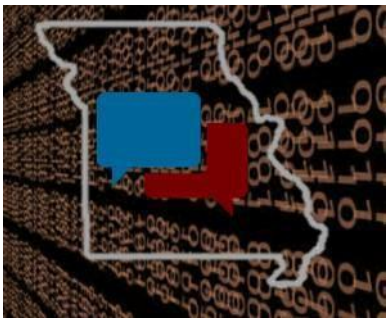
You have the latest antivirus program. The firewall is turned on. Passwords are strong and frequently updated. Now you can sleep at night knowing your organization is safe from cyberattacks, right? Well, at least until John from HR decides to log in from a link he received in an email. He probably knew not to click on suspicious emails, but what is considered suspicious? That email could have arrived from your own domain. Attackers can spoof your domain to trick employees or your customers into divulging confidential information or downloading a malicious file attachment. Phishing emails are arriving with smarter baiting tactics, becoming harder to identify. Defenses need to catch up as well. Security teams, especially those responsible for domain integrity, should make sure to correctly implement the three anti-phishing standards: SPF, DKIM, and DMARC. Full Article: https://www.darkreading.com/edge-articles/dmarc-101-how-to-keep-phishing-attacks-out-of-your-inbox

Increase in Credential Phishing and Brute Force Attacks Causing Financial and Reputational Damage

Abnormal Security released a report which examines the escalating adverse impact of socially-engineered and never-seen-before email attacks, and other advanced email threats—both financial and reputational—to organizations worldwide. The report surveyed advanced email attacks across eight major industry sectors, including retail and consumer goods; manufacturing; technology; energy and infrastructure services; medical; media and television; finance; and hospitality. 32.5% of all companies were targeted by brute force attacks in early June 2021; 137 account takeovers occurred per 100,000 mailboxes for members of the C-suite; 61% of organizations experienced a vendor email compromise attack this quarter; 22% more business email compromise attacks since Q4 2020; 60% chance of a successful account takeover each week for organizations with 50,000+ employees; 73% of all advanced threats were credential phishing attacks; 80% probability of attack every week for retail and consumer goods, technology, and media and television companies. https://www.helpnetsecurity.com/2021/08/31/increase-in-credential-phishing/

See Something/Say Something

The three Missouri Fusion Centers: the St. Louis Fusion Center, the Missouri Information Analysis Center, and the Kansas City Regional Fusion Center has teamed up with the Missouri Office of Homeland Security and P3 to create a Suspicious Cyber Activity Reporting Tool.



The Suspicious Cyber Activity Reporting Tool is accessible on the SafeNation App or go to https://www.p3tips.com/TipForm.aspx?ID=2600&TemplateID=129