Cybersecurity Open Source Intelligence Weekly Wrap-Up
Wednesday, August 25, 2021

Ransomware

CISA Shares Guidance on How to Prevent Ransomware Data Breaches

The US Cybersecurity and Infrastructure Security Agency (CISA) has released guidance to help government and private sector organizations prevent data breaches resulting from ransomware double extortion schemes. CISA's fact sheet includes best practices for preventing ransomware attacks and protecting sensitive information from exfiltration attempts. The federal agency issued these recommendations in response to most ransomware gangs using data stolen from their victims' networks as leverage in ransom negotiations under the threat of publishing the stolen info on dedicated leak sites. https://www.bleepingcomputer.com/news/security/cisa-shares-guidance-on-how-to-prevent-ransomware-data-breaches/

Device Complexity Leaving Schools at Heightened Risk of Ransomware Attacks

Absolute Software announced a research revealing the significant management and security challenges faced by K-12 education IT teams with the rise in digital learning and widespread adoption of 1:1 device programs. The report underscores how increased device mobility and complexity are leaving schools increasingly vulnerable to security risks and potential attacks. As devices quickly became the primary mode of learning and connection for students and staff, school districts raced to expand their fleets; data shows that the total number of devices deployed across K-12 environments increased 74 percent from 2019 to 2020. At the same time, the disruption caused by digital learning – and the flurry of new technologies needed to support it – opened up new potential attack vectors for cybercriminals. https://www.helpnetsecurity.com/2021/08/19/schools-ransomware-attacks/

Ransomware Attacks are Now the Second Most Commonly Reported Security Incident

Analysis by CybSafe of incidents reported to the UK's Information Commissioner's Office (ICO) shows that ransomware attacks made up 22 percent of all reported cyber security incidents in the first half of 2021. This is up from 11 percent in the first half of 2020. Phishing still leads, accounting for 40 percent of all cybersecurity cases reported to the ICO, slightly down from 44 percent the year before, but ransomware has now edged into second place. Education is the sector hardest hit, with ransomware accounting for 32 percent of attacks in the first half of 2021 compared to just 11 percent the year before. With many schools rushing to transition to remote learning, increased attacks have resulted in schools losing coursework, financial records and COVID-19 testing data. https://betanews.com/2021/08/19/ransomware-second-most-common-security-incident/

Researchers Warn of 4 Emerging Ransomware Groups That Can Cause Havoc

Cybersecurity researchers on Tuesday took the wraps off four up-and-coming ransomware groups that could pose a serious threat to enterprises and critical infrastructure, as the ripple effect of a recent spurt in ransomware incidents show that attackers are growing more sophisticated and more profitable in extracting payouts from victims. “While the ransomware crisis appears poised to get worse before it gets better, the cast of cybercrime groups that cause the most damage is constantly changing,” Palo Alto Networks’ Unit 42 threat intelligence team said in a report shared with The Hacker News. “Groups sometimes go quiet when they’ve achieved so much notoriety that they become a priority for law enforcement. Others reboot their operations to make them more lucrative by revising their tactics, techniques and procedures, updating their software and launching marketing campaigns to recruit new affiliates.” https://thehackernews.com/2021/08/researchers-warn-of-4-new-ransomware.html

Threats/Vulnerabilities

Small Companies Make Good Targets for Cybercriminals

"Cybersecurity doesn’t apply to me because my business is too small to matter", and "Cybercriminals would never bother hacking us because we don’t have valuable data or many financial assets." If these comments sound familiar, that’s because it is unfortunately the view held by a large majority of the SMB community. Small to medium sized businesses are slowly jumping on the cybersecurity bandwagon, but must first leave this 'it would never happen to me' mentality behind. It is understandable why small businesses would struggle to see why they would need to be protected from cyber attacks when our news outlets are littered each day with the latest breaches of multinational organizations. It seems like cyber crime belongs to the world of large enterprises and is not a concern for the average SMB. However, it is this false impression that only exacerbates the problem and helps to make small businesses an even better target for cybercriminals. https://betanews.com/2021/08/17/small-companies-targets-for-cybercrime/

Evanina: Combating China’s ‘Existential’ Cyber, Influence Threats Requires Post-9/11 Intensity

Battling in “the new frontier” of malign foreign influence requires finding ways to fill “a vast gaping hole” in helping Americans identify vulnerabilities and influence ops “every day living in technology but also with elections in the future,” the former director of the National Counterintelligence and Security Center said, adding that the Department of Homeland Security could fill that domestic engagement role. Bill Evanina told the Senate Intelligence Committee at an Aug. 4 hearing that “the holistic and comprehensive threat to the United States posed by the Communist Party of China is an existential threat, and it is the most complex, pernicious, aggressive, and strategic threat our nation has ever faced.” The private sector and academia “have become the geopolitical battle space for China” as leader Xi Jinping “has one goal: to be the geopolitical, military, and economic leader in the world, period.” https://www.hstoday.us/subject-matter-areas/infrastructure-security/evanina-combating-existential-cyber-influence-threats-from-china-requires-post-9-11-intensity/

Critical Infrastructure Attack Trends: What Business Leaders Should Know

Amateur threat actors have been able to compromise critical infrastructure like industrial control systems (ICS) and other operational technology (OT) assets more often lately. Compromises of exposed OT assets rose over the past 18 months, according to threat researchers at Mandiant, with attackers using readily-available tools and common techniques to gain access to the systems. Attackers can get into those because they’re often connected to the internet without authentication and visible via connected-device search engines, like Shodan. Why else is this happening more now? And what can businesses with a lot of OT involved in their critical infrastructure do against attacks like this? https://securityintelligence.com/articles/critical-infrastructure-attack-trends-business-leaders/

BlackBerry software flaw could impact cars, medical devices - U.S. agencies

A cybersecurity flaw in a software designed by BlackBerry Ltd could put at risk cars and medical equipment that use it and expose highly sensitive systems to attackers, the U.S. drugs regulator and a federal agency said on Tuesday. The warning came after the Canadian company disclosed that its QNX Real Time Operating System has a vulnerability that could allow an attacker to execute an arbitrary code or flood a server with traffic until it crashes or gets paralyzed. The software is used by automakers including Volkswagen, BMW and Ford Motor in many critical functions including the Advanced Driver Assistance System. https://cio.economictimes.indiatimes.com/news/corporate-news/blackberry-software-flaw-could-impact-cars-medical-devices-u-s-agencies/85418837

Rockwood School District Provides Notice of Ransomware Incident

EUREKA, Mo.,— Rockwood School District (the "District") today is providing information about a recent event that may impact the privacy of some personal data related to current and former employees and students. The confidentiality, privacy, and security of information in the District's care is one of its highest priorities and the District takes this incident very seriously. Although the District has not received any reports of actual or attempted misuse of the impacted information, the District is providing this notice in an abundance of caution. What Happened? https://app.hacknotice.com/#/hack/611fa8aff5526f40fc032160?utm_source=dlvr.it

Malware

ShadowPad Malware is Becoming a Favorite Choice of Chinese Espionage Groups

ShadowPad, an infamous Windows backdoor that allows attackers to download further malicious modules or steal data, has been put to use by five different Chinese threat clusters since 2017. "The adoption of ShadowPad significantly reduces the costs of development and maintenance for threat actors," SentinelOne researchers Yi-Jhen Hsieh and Joey Chen said in a detailed overview of the malware, adding "some threat groups stopped developing their own backdoors after they gained access to ShadowPad." The American cybersecurity firm dubbed ShadowPad a "masterpiece of privately sold malware in Chinese espionage." https://thehackernews.com/2021/08/shadowpad-malware-is-becoming-favorite.html

Hacks/Breaches

Does a VPN Protect You from Hackers?

A virtual private network (VPN) is the perfect solution for a lot of issues you might experience online- accessing blocked sites, hiding your browsing activity, getting rid of internet throttling, finding better deals, and much more. But does a VPN protect you from hackers? Is your private information and files safer on the internet with a VPN? How much of a difference does it make in terms of data protection? The answer to these questions isn't as simple as Yes or No. So, keep reading to find out. You should definitely use a VPN on a public network or your home wi-fi because it significantly protects your privacy. But a VPN can't simply protect you from every single type of cyber attack. Some attacks are very sophisticated and complex, which even a VPN can't prevent. https://thehackernews.com/2021/08/does-vpn-protect-you-from-hackers.html

Iranian Hackers Target Several Israeli Organizations With Supply-Chain Attacks

IT and communication companies in Israel were at the center of a supply chain attack campaign spearheaded by an Iranian threat actor that involved impersonating the firms and their HR personnel to target victims with fake job offers in an attempt to penetrate their computers and gain access to the company's clients. The attacks, which occurred in two waves in May and July 2021, have been linked to a hacker group called Siamesekitten (aka Lyceum or Hexane) that has primarily singled out oil, gas, and telecom providers in the Middle East and in Africa at least since 2018, researchers from ClearSky said in a report published Tuesday. https://thehackernews.com/2021/08/iranian-hackers-target-several-israeli.html

North Korean Hackers Use Browser Exploits to Drop Malware

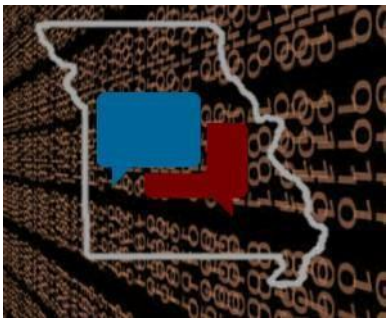
Researchers say they have spotted North Korea-linked hacking group "InkySquid" (ScarCruft, APT37) conducting a strategic web compromise attack targeting a limited number of victims in order to infect targeted systems with malware. According to Veloxity researchers, in the attacks, InkySquid exploited an Internet Explorer vulnerability from 2020, which allowed it to load obfuscated JavaScript code that was hiding within legitimate code. Reports indicate that InkySquid similarly targeted Microsoft's Edge browser with a more recent exploit that can also work against Internet Explorer. In attacks targeting both browsers, the loaded JavaScript code was decrypted into a stager version of the "Cobalt Strike" penetration tool, closely followed by a new, secondary payload, which Veloxity has dubbed "Bluelight." According to Veloxity researchers, BLUELIGHT is a new reconnaissance tool and information stealer that can be set up by attackers to leverage different cloud providers for command and control (C&C). Veloxity adds that as part of the Korean attacks, attackers were using a Microsoft Graph application programming interface (API) for Microsoft 365, Office, and other servers as part of their Bluelight operations. https://www.itnews.com.au/news/north-korean-hackers-use-browser-exploits-to-drop-malware-568734

The State Department Has Reportedly Been Hacked

The U.S. State Department was purportedly the victim of a serious cyber attack in recent weeks, according to a Fox News report published on Saturday. The extent of breach and when it was discovered are currently unknown. Citing an unnamed source, the outlet stated that the Department of Defense's Cyber Command had issued notifications of a possibly serious breach. Although it's unclear whether the State Department's operations have been affected by the attack, Fox reported that the department's work to evacuate thousands of Americans and Afghans from Kabul, Afghanistan amid the withdrawal of U.S. forces had not been affected. https://gizmodo.com/the-state-department-has-reportedly-been-hacked-1847536299

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