Cybersecurity Open Source Intelligence Weekly Wrap-Up
Wednesday, September 8, 2021

Ransomware

Conti Ransomware Now Hacking Exchange Servers with Proxyshell Exploits

The Conti ransomware gang is hacking into Microsoft Exchange servers and breaching corporate networks using recently disclosed ProxyShell vulnerability exploits. ProxyShell is the name of an exploit utilizing three chained Microsoft Exchange vulnerabilities (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) that allow unauthenticated, remote code execution on unpatched vulnerable servers. These three vulnerabilities were discovered by Devcore's Orange Tsai, who used them as part of the Pwn2Own 2021 hacking contest. https://www.bleepingcomputer.com/news/security/conti-ransomware-now-hacking-exchange-servers-with-proxyshell-exploits/?&web_view=true

Revil Ransomware's Servers Mysteriously Come Back Online

The dark web servers for the REvil ransomware operation have suddenly turned back on after an almost two-month absence. It is unclear if this marks their ransomware gang's return or the servers being turned on by law enforcement. On July 2nd, the REvil ransomware gang, aka Sodinokibi, used a zero-day vulnerability in the Kaseya VSA remote management software to encrypt approximately 60 managed service providers (MSPs) and over 1,500 of their business customers. REvil then demanded $5 million from MSPs for a decryptor or $44,999 for each encrypted extension at the individual businesses. The gang also demanded $70 million for a master decryption key to decrypt all Kaseya victims but soon dropped the price to $50 million. After the attack, the ransomware gang faced increasing pressure from law enforcement and the White House, who warned that the USA would take action themselves if Russia did not act upon threat actors in their borders. https://www.bleepingcomputer.com/news/security/revil-ransomwares-servers-mysteriously-come-back-online/

Ransomware Attacks Soar 288% in First Half of 2021

The number of ransomware attacks surged by 288% between the first and second quarters of 2021 as double extortion attempts grew, according to the latest data from NCC Group. Analyzing incidents dealt with by its own Research Intelligence and Fusion Team (RIFT) throughout 2021, the firm claimed nearly a quarter (22%) of data leaks in the second quarter came from the Conti group. Conti typically gains initial network access to victim organizations via phishing emails, it claimed. Next came Avaddon, which accounted for 17% of incidents, although this variant is now thought to be inactive. Unsurprisingly, nearly half (49%) of victims with known locations in Q2 were based in the US, followed by 7% in France and 4% in Germany. https://www.infosecurity-magazine.com/news/ransomware-attacks-soar-half-2021/

This is a joint cybersecurity weekly product from the Missouri Information Analysis Center, St. Louis Fusion Center, Kansas City Regional Fusion Center and the Missouri Office of Homeland Security. All information in this product is open-source and may be shared without further permission. If any member of the public has pertinent information regarding the subject material contained within this Public Awareness Bulletin, they should contact the agency listed above directly. Any unauthorized alteration of any portion of this Public Awareness Bulletin is considered a violation and subject to legal prosecution.

FBI Warns Food and Agriculture Firms of Ransomware Threat

The FBI has issued a new alert warning companies in the food and agricultural sector that they are increasingly at risk of ransomware as their corporate attack surface expands. The Private Industry Notification, seen by Infosecurity, noted that the vertical is a critical infrastructure sector which, if impacted by such threats, could negatively impact the food supply chain. "Ransomware may impact businesses across the sector, from small farms to large producers, processors and manufacturers, and markets and restaurants," it continued. "Cyber-criminal threat actors exploit network vulnerabilities to exfiltrate data and encrypt systems in a sector that is increasingly reliant on smart technologies, industrial control systems and internet-based automation systems." Attacks may target larger organizations, deemed more likely to pay higher ransom demands, and smaller firms perceived as softer targets. For both, the increasing move to IoT may offer a new attack surface to target, the FBI warned. https://www.infosecurity-magazine.com/news/fbi-warns-food-agriculture-firms/

This Is the Perfect Ransomware Victim, According to Cybercriminals

Researchers have explored what the perfect victim looks like to today's ransomware groups. On Monday, KELA published a report on listings made by ransomware operators in the underground, including access requests -- the way to gain an initial foothold into a target system -- revealing that many want to buy a way into US companies with a minimum revenue of over $100 million. Initial access is now big business. Ransomware groups such as Blackmatter and Lockbit may cut out some of the legwork involved in a cyberattack by purchasing access, including working credentials or the knowledge of a vulnerability in a corporate system. When you consider a successful ransomware campaign can result in payments worth millions of dollars, this cost becomes inconsequential -- and can mean that cybercriminals can free up time to strike more targets. https://www.zdnet.com/article/this-is-the-perfect-ransomware-victim-according-to-cybercriminals/

Threats/Vulnerabilities

9 Notable Government Cybersecurity Initiatives of 2021

Cybersecurity has steadily crept up the agenda of governments across the globe. This has led to initiatives designed to address cybersecurity issues that threaten individuals and organizations. "Government-led cybersecurity initiatives are critical to addressing cybersecurity issues such as destructive attacks, massive data breaches, poor security posture, and attacks on critical infrastructure," Steve Turner, security and risk analyst at Forrester, tells CSO. "These initiatives provide consistent guidance on how organizations and consumers can protect themselves, provide services to companies that don't have the knowledge or monetary means to protect themselves, legislative levers that can be utilized, means of taking offensive actions against nation state adversaries, and most of all investigation of significant cyber incidents paired with critical information sharing during or after those incidents." Here are some of the most notable cybersecurity initiatives introduced by governments around the world in 2021.
https://www.csoonline.com/article/3630632/9-notable-government-cybersecurity-initiatives-of-2021.html

The Cybersecurity of Industrial Companies Remains Low, Potential Damage Can Be Severe

Positive Technologies released a research that examines information security risks present in industrial companies, the second-most targeted sector by cybercriminals in 2020. Among key findings, an external attacker can penetrate the corporate network at 91% of industrial organizations, and penetration testers gained access to the industrial control system (ICS) networks at 75% of these companies. Attack vectors for accessing critical systems can be simple, and the potential damage severe. Once criminals have obtained access to ICS components, they can shutdown entire productions, cause equipment to fail, trigger chemical spills and even industrial accidents that could cause series harm

This is a joint cybersecurity weekly product from the Missouri Information Analysis Center, St. Louis Fusion Center, Kansas City Regional Fusion Center and the Missouri Office of Homeland Security. All information in this product is open-source and may be shared without further permission. If any member of the public has pertinent information regarding the subject material contained within this Public Awareness Bulletin, they should contact the agency listed above directly. Any unauthorized alteration of any portion of this Public Awareness Bulletin is considered a violation and subject to legal prosecution.

to industrial employees or even death. Olga Zinenko, Senior Analyst at Positive Technologies, said: “Today, the level of cybersecurity at most industrial companies is too low for comfort. In most cases, internet-accessible external network perimeters contain weak protection, device configurations contain flaws, and we find a low level of ICS network security and the use of dictionary passwords and outdated software versions present risks.” https://www.helpnetsecurity.com/2021/09/02/industrial-companies-cybersecurity/

Security Risks to Your Mobile App and How to Avoid Them

Mobile devices, while convenient tools for communication and engagement, also come with their fair share of security risks — particularly when it comes to mobile applications. On the other hand, apps help improve communication, provide new ways to learn and be entertained, and keep us connected to the world. When produced correctly, they can be assets. When produced poorly, they become liabilities. Mobile app development companies are prioritizing the security of their apps now more than ever. Without security, they can lose trust in their consumers and risk becoming a liability themselves. Knowing how to navigate common security risks is an asset that allows developers to create apps that cater to what their audience needs while putting their minds at ease, knowing their private data remains secure. So what are the most significant security risks to your mobile app? We’ve explained them below to help you avoid making the same mistakes. https://www.hackread.com/security-risks-to-your-mobile-app/

Tech CEOs: Multi-Factor Authentication Can Prevent 90% of Attacks

The use of multi-factor authentication (MFA) could prevent as much as 80–90% of cyber-attacks, according to figures cited by the US national security cyber chief. Anne Neuberger, who’s deputy national security advisor for cyber and emerging technologies, said the stat was itself referenced by a number of the tech CEOs who attended a meeting with President Biden last week. MFA is one of the five key measures that Biden has mandated be rolled out across federal government by November, as part of his executive order on cybersecurity. Alongside MFA, she urged leadership teams at US organizations to implement four steps ahead of the holiday weekend. The others were strong passwords, prompt patching of all software, a review of incident response plans, and up-to-date backups which are segregated from the corporate network. Full Article: https://www.infosecurity-magazine.com/news/tech-execs-mfa-prevent-90-of/

39% of All Internet Traffic is from Bad Bots

Automated traffic takes up 64% of internet traffic – and whilst just 25% of automated traffic was made up by good bots, such as search engine crawlers and social network bots, 39% of all traffic was from bad bots, a Barracuda report reveals. These bad bots include both basic web scrapers and attack scripts, as well as advanced persistent bots. These advanced bots try their best to evade standard defences and attempt to perform their malicious activities under the radar. The report revealed that the most common of these persistent bots were ones that went after e-commerce applications and login portals. The report also included a breakdown of bad bot traffic by location. It revealed that North America accounts for 67% of bad bot traffic, followed by Europe (22%) and then Asia (7.5%). Full Article: https://www.helpnetsecurity.com/2021/09/07/bad-bots-internet-traffic/

Over 60,000 Parked Domains were Vulnerable to AWS Hijacking

Domain registrar MarkMonitor had left more than 60,000 parked domains vulnerable to domain hijacking. MarkMonitor, now part of Clarivate, is a domain management company that "helps establish and protect the online presence of the world's leading brands - and the billions who use them." The parked domains were seen pointing to nonexistent Amazon S3 bucket addresses, hinting that there existed a domain takeover weakness. (Sub)domain takeover refers to an unauthorized actor being able to serve the content of their choice on a domain they otherwise have no rights to or ownership of. This can occur, for example, if the domain name has a canonical name (CNAME) DNS entry pointing to a host that is not providing any content for it. https://www.bleepingcomputer.com/news/security/over-60-000-parked-domains-were-vulnerable-to-aws-hijacking/

This is a joint cybersecurity weekly product from the Missouri Information Analysis Center, St. Louis Fusion Center, Kansas City Regional Fusion Center and the Missouri Office of Homeland Security. All information in this product is open-source and may be shared without further permission. If any member of the public has pertinent information regarding the subject material contained within this Public Awareness Bulletin, they should contact the agency listed above directly. Any unauthorized alteration of any portion of this Public Awareness Bulletin is considered a violation and subject to legal prosecution.

SolarWinds

Hacked SolarWinds Software Lacked Basic Anti-Exploit Mitigation: Microsoft

Software vendor SolarWinds failed to enable an anti-exploit mitigation available since the launch of Windows Vista 15 years ago, an oversight that made it easy for attackers to launch targeted malware attacks in July this year. The missing mitigation was flagged by Microsoft in a post mortem of last month's zero-day attack that hit businesses using the SolarWinds Serv-U Managed File Transfer and Serv-U Secure FTP products. Microsoft originally shipped the mitigation -- called ASLR (Address Space Layout Randomization) in Windows Vista back in 2006 as part of a larger plan to make it more difficult to automate attacks against the operating system. However, according to Microsoft's newly minted Offensive Research & Security Engineering team, SolarWinds developers failed to enable ASLR compatibility in some modules. https://www.securityweek.com/microsoft-hacked-solarwinds-ftp-software-lacked-basic-anti-exploit-mitigation

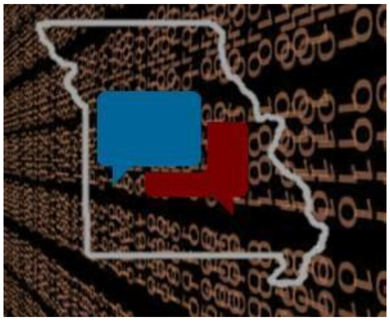
Phishing

Credential Phishing and Brute Force Attacks Continue to Surge

Financial and reputational aspects of organizations across the globe are taking a severe hit as they witness advanced email threats from unprecedented email attacks that continue to escalate, as per a recent report by Abnormal Security. Unsuspecting victims fall prey to the schemes which are devised to make the malicious emails land directly into their inboxes evading security mechanisms. As threat actors continue to work around various phishing techniques, cyber-attacks via credential phishing and brute force continue to remain effective attack vectors. Advanced email threats such as 'Business Email Compromise' attacks are designed to safely bypass secure email gateways and other conventional security infrastructure allowing the operators to steal in billions each year. Full Article: https://www.ehackingnews.com/2021/09/credential-phishing-and-brute-force.html

See Something/Say Something

if you
SEE
something
SAY
something™
If You See Something Say Something™ used with permission of the NY Metropolitan Transportation Authority.



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

This is a joint cybersecurity weekly product from the Missouri Information Analysis Center, St. Louis Fusion Center, Kansas City Regional Fusion Center and the Missouri Office of Homeland Security. All information in this product is open-source and may be shared without further permission. If any member of the public has pertinent information regarding the subject material contained within this Public Awareness Bulletin, they should contact the agency listed above directly. Any unauthorized alteration of any portion of this Public Awareness Bulletin is considered a violation and subject to legal prosecution.