Cybersecurity Threat

July 2023 Newsletter

USA Is Playing Offense

The Biden administration definitely means business with its national cybersecurity strategy. Cybersecurity investments in 2025 will focus on offensive measures to stop hackers and cybercriminals, modernization of defenses, and zero-trust implementation. Per an internal notice circulated with department heads, "the Administration is committed to mounting disruption campaigns and other efforts that are so sustained, coordinated, and targeted that they render ransomware no longer profitable." This means that the DOJ's disbanding of Hive ransomware was not a one-off and that more will follow.

Meta Receiving Record-Breaking Fine

The EU has imposed a record-breaking fine of €1.2 billion on Facebook's Meta for violating the bloc's data protection rules, under the GDPR. This is the largest penalty ever issued by the European Data Protection Board (EDPB), which oversees the implementation of the General Data Protection Regulation (GDPR). The EDPB found that Meta failed to comply with several provisions of the GDPR, such as obtaining valid consent from users, providing transparent information about data processing, and ensuring data security and accountability. The EDPB also accused Meta of using deceptive practices to manipulate users into accepting its privacy policies and sharing their personal data with third parties.

The fine is a clear signal that the EU is serious about enforcing its data protection laws and protecting the rights and freedoms of its citizens. The EDPB said that the fine reflects the gravity and duration of Meta's infringements, as well as its global reach and impact on millions of users.

By imposing a hefty fine on Meta, the EU has set a strong tone for global privacy standards and expectations. The EU has shown that it will not tolerate any violations of its data protection rules, and that it will hold companies accountable for their actions. The EU has also demonstrated its leadership and influence in shaping the digital landscape and safeguarding the interests of its citizens. The EU's fine could serve as a catalyst for other countries to follow suit and enforce their own data protection laws with more rigor and determination. The EU's fine could also encourage users to demand more transparency and control over their personal data, and to exercise their rights more actively. The EU's fine could ultimately lead to a more privacy-respecting and trustworthy online environment for everyone.

Foreign Cyber Threats Abound

Recently published, CSE's annual report highlights that the agency has blocked over 2.3 trillion malicious actions between April 2022 and March 2023. This a substantial upshot from the two to five billion attacks highlighted in CSE's last yearly report. This echoes earlier warnings about foreign threats to critical infrastructure and governmental and private organizations. Although the main culprits are based in Russia, China is also furthering its cyberwarfare capacities. Recently, Chinese threat actors attacked Laurentian University with the aim of stealing intellectual property from researchers.

SEO Poisoning Reaches Healthcare

The US's Health Sector Cybersecurity Coordination Center (HC3) has released an analyst note on search engine optimization poisoning being leveraged against healthcare organizations. One common method involves typo-squatting, where attackers register domain names similar to legitimate URLs. A user might unknowingly click on a link with a misspelled URL, leading to a fake website prompting the download of malware-infected files. These websites often appear at the top of search results due to keyword stuffing, cloaking, and search ranking manipulation techniques used by threat actors.

Human Resources Lagging

In a new study, Legend, a research and analytics organization, has found that human resources have become increasingly important, particularly due to the COVID-19 pandemic. The study indicates that talent attraction and retention, including experienced CIOs, remains a major concern for organizations. Additionally, the pandemic has prompted individuals to exit their careers, further exacerbating the challenges faced by the Canadian job market. These human resource challenges adversely affect the management of complex IT projects, preventing organizations from achieving their objectives within specified timelines and budgets.

Real Impact of AI on Healthcare Cybersecurity

With the rise of artificial intelligence in 2023, HC3 has published a brief on potential threats made by AI against healthcare cybersecurity. HC3 advises healthcare organizations to look at frameworks such as publications from NIST to build a solid baseline but also to remain vigilant. As AI evolves, so will adversary tactics and organizations must define how they frame AI use and how they defend against it.

ENISA: Most Threats in Health are Ransomware

ENISA, the EU's cybersecurity agency, has released its first threat landscape for healthcare, showing that ransomware accounts for 54% of cybersecurity threats in healthcare. ENISA is highlighting patterns in Europe similar to those in North America, including slow adoption of patches, widespread incidents, cyberwarfare attacks, and healthcare being appetizing to ransomware.

Exploits and Issues Patches

- This month's biggest exploit has been Chinese hackers' theft of inactive consumer signing keys to breach Exchange Online and AzureAD. More concerning is that Microsoft still does not know how this took place.

  Our Thoughts: This news are worrisome, especially considering that the American Commerce Secretary was among those breached. We will be monitoring this one closely as its implications could be dire.

- Microsoft Word documents containing remote code execution flaws are used as phishing lures to drop LokiBot malware on compromised systems. LokiBot is one of the older and best known Trojans, but this malware iteration includes evasion techniques to check for debuggers.

  Our Thoughts: Microsoft products have been and will continue to be popular for hackers to deceive people. Make sure that users are trained and aware of phishing etiquette.

- Adobe is raising the alarm on a critical ColdFusion pre-authentication remote code execution vulnerability that is actively exploited in attacks. Adobe recommends that users "lockdown" ColdFusion installations, although researchers warned that the vulnerability can bypass lockdown mode.

  Our Thoughts: This is concerning news. If you are an Adobe shop and use ColdFusion, implement updates to the latest version to limit your attack surface.

- Apple has fixed and re-released security updates published to urgently address a WebKit zero-day vulnerability exploited in the wild. This was due to some websites not displaying properly because of initial patch implementations.

  Our Thoughts: Since early 2023, Apple has had to address a total of ten zero-days being actively exploited; patch.

- The BlackLotus UEFI bootkit source code has been leaked online, allowing a better understanding of the malware. BlackLotus is a Windows-targeting UEFI bootkit known for bypassing Secure Boot on fully patched

  Our Thoughts: This is good news for us. Anything that will put threat actors out of harm's way and contribute to a more secure cyber space is a win.

Threat Actor Updates

- A report from Mandiant outlines that malware being distributed via USB drives has tripled since early 2023. Two main campaigns have been observed, both related to Beijing, where infected USB devices have been distributed to conduct cyber espionage for geopolitical and industrial purposes.

  Our Thoughts: We have seen a surge in state-backed cyberattacks since the beginning of the year, and these should not be taken lightly. Make sure staff are trained not to pick up and plug unknown portable media.

- The RomCom threat actor group, a Russian-speaking gang, has been targeting NATO countries. RomCom was known to impersonate brands and create fake websites to ensnare its targets previously. This time, it was through phishing messages purporting to come from the Ukrainian World Congress which included a spoofed website.

  Our Thoughts: Advanced persistent threat groups are always dangerous because their pockets run deep. However, the most common infection vectors remain the same. Train, train, train.