TLP WHITE: Threat Intelligence Report on The Current Threat Landscape February 6th 2024

This report was generated by Scot Terban using the ICEBREAKER A.I. Intel Analyst created by Scot Terban

This week’s threat landscape overview highlights several significant cybersecurity events and trends observed over the weekend, focusing on vulnerabilities, attacks targeting U.S. critical infrastructure, and CISA’s updated cyber incident scoring system to prioritize national-level risk effectively.

Trends:

In the evolving cyber threat landscape of 2024, two significant trends have been identified: the continued escalation of ransomware attacks and the emergence of new malware exploiting vulnerabilities in network infrastructure.

Ransomware attacks have notably worsened in 2023 compared to the previous year, with criminals shifting their focus towards data extraction rather than relying solely on encryption payloads. This shift indicates that ransomware threats are expected to continue increasing and evolving throughout 2024. A survey report by Delinea, which involved more than 300 U.S. IT and security decision-makers, revealed a significant increase in the number of ransomware victims, with a higher percentage of victims opting to pay the ransom, potentially influenced by the rise of cyberinsurance. The report highlights the challenges in cybersecurity practices, emphasizing the need for enhanced prevention and recovery measures to mitigate the impact of these attacks.

Adding to the complexity of the cyber threat environment, new malware has been identified targeting Ivanti VPN vulnerabilities. Google-owned Mandiant reported the employment of new malware by a China-nexus espionage threat actor known as UNC5221, among other groups, during post-exploitation activities. This malware includes custom web shells like BUSHWALK, CHAINLINE, FRAMESTING, and a variant of LIGHTWIRE, exploiting CVE-2023-46805 and CVE-2024-21887 to execute arbitrary commands with elevated privileges on affected devices. These vulnerabilities have been actively abused since early December 2023, highlighting the need for immediate action to secure network appliances against sophisticated espionage activities.

The cybersecurity outlook for 2024 also draws attention to the geopolitical landscape’s influence on cyber threats, with state-sponsored activities intensifying. Events such as the Paris 2024 Olympic Games are anticipated to attract the attention of cybercriminals, increasing the risk of cyber espionage, phishing attacks, DDoS attacks, and fraudulent activities. The landscape is further complicated by the activities of state-sponsored threat actors like APT28, APT29, Unit 61398, APT10, Lazarus Group, and APT33, which are driven by geopolitical events and military conflicts. These actors are involved in cyberespionage, sabotage, and disinformation campaigns, leveraging their government support and resources to conduct operations against political, economic, and military targets.

This comprehensive overview of the current cyber threat landscape underscores the critical need for vigilance and proactive cybersecurity measures. Organizations must stay informed about emerging threats and vulnerabilities to protect against sophisticated ransomware campaigns, espionage activities, and the exploitation of network infrastructure vulnerabilities. Collaboration between the public and private sectors is essential to enhance the collective cybersecurity posture and mitigate the risks posed by these evolving threats.

Vulnerabilities:

- **Linux Kernel Flaws:** Multiple vulnerabilities in the Linux kernel were reported, including null pointer dereference, use-after-free, and double free issues, posing risks for local privilege escalation and system crashes. These vulnerabilities, identified as CVE-2024-0841, CVE-2024-1085, and CVE-2024-1086, require immediate attention for patching to mitigate potential exploits.

- **Software Vulnerabilities:** The report also highlighted vulnerabilities in other software, such as Loom for macOS, allowing remote code execution (CVE-2024-23742), and various issues in MachineSense devices, including unchangeable credentials and unprotected APIs (CVE-2023-49617, CVE-2023-46706, CVE-2023-47867, CVE-2023-49610, CVE-2023-49115, CVE-2023-6221).

Critical Infrastructure Attacks & News:

- **DOJ and FBI Disrupt Chinese Botnet:** A significant enforcement action disrupted a botnet comprising hundreds of small office and home office routers infected by Volt Typhoon malware, sponsored by the People's Republic of China. This malware campaign targeted U.S. critical infrastructure, including communications, energy, transportation, and water sectors. This operation reflects the escalating nature of nation-state cyber threats aiming to pre-position themselves for potential physical harm to critical infrastructure.

CISA National Cyber Incident Scoring System (NCISS):

- CISA has updated its National Cyber Incident Scoring System to provide a standardized approach for evaluating the risk of cybersecurity incidents in a national context. This system considers the functional impact, information impact, recoverability, cross-sector dependency, and potential national impact of incidents to prioritize response and resources effectively. The scoring system helps in objectively assessing the severity of cybersecurity events and facilitating timely and coordinated responses.

Breaches:

Hewlett Packard Enterprise (HPE) Investigates New Breach: HPE is currently investigating a potential security breach after a threat actor claimed to have stolen data for sale on a hacking forum. This data allegedly includes HPE credentials among other sensitive information. HPE has not found any evidence of a breach or received any ransom demands but continues to investigate the claims. This incident is under scrutiny due to the sensitive nature of the stolen data, which could have significant implications if verified.

Recent Cybersecurity Incidents: The landscape of recent breaches reveals a variety of targets and impacts:

- **Hewlett Packard Enterprise (HPE)** is investigating a potential security breach after data allegedly containing HPE credentials and other sensitive information was put up for sale on a hacking forum. The company has not found any evidence of a security breach and is currently investigating the claims. This incident is notable for its potential impact on HPE's vast product and service ecosystem.

- **AnyDesk**, the Germany-based developer of remote access software, informed customers about a security breach affecting its production systems. The breach led to the revocation of security-related certificates and passwords as a precautionary measure. AnyDesk has engaged CrowdStrike to assist with investigating and remediating the incident. Although the specifics of the attack have not been disclosed, the incident underscores the vulnerabilities associated with remote access software and the potential for supply chain attacks.
- **Cloudflare** detailed a security breach that occurred in November, where nation-state attackers targeted the company's internal Atlassian server, accessing documentation and a limited amount of source code. Cloudflare responded with a company-wide remediation effort dubbed "Code Red," assisted by Crowdstrike, to assess the damage and reinforce security measures. The attackers were expelled by November 24, 2023, but the incident highlights the ongoing threat posed by nation-state actors to global network infrastructure.

JCDC Instability:

Cyber Pros Are Giving Up On A Key Government Program

The Joint Cyber Defense Collaborative (JCDC) initiative, launched in 2021, was envisioned as a pivotal strategy by the Cybersecurity and Infrastructure Security Agency (CISA) to bolster the United States' defense against increasing cyber threats through collaboration between the government and the private sector. However, recent reports suggest that this initiative is encountering significant challenges that could adversely impact U.S. security.

According to Politico, there's a growing discontent within the JCDC, as key cybersecurity professionals have begun stepping back from the initiative. Experts have voiced concerns over the JCDC's management and the fear of becoming entangled in conservative criticism directed at CISA. The reduced participation from the private sector is particularly troubling as the U.S. heavily relies on these external entities for protecting government and critical infrastructure. This withdrawal could potentially weaken the country's defense against cyber threats, especially at a time when Chinese hackers are aggressively targeting American systems. CISA has acknowledged these challenges and expressed a commitment to addressing them, highlighting the JCDC's crucial role in combating sophisticated cyber threats.

Moreover, Alliant Cybersecurity emphasizes the JCDC's foundational goal of unifying efforts across public and private sectors to combat cyber threats more effectively. The initiative was a response to the severe consequences of ransomware attacks on public services and infrastructure, demonstrating the federal government's intent to protect its infrastructure from such cyberattacks. The diverse committee makeup of the JCDC, including tech giants and various governmental agencies, was aimed at fostering a collaborative environment to strengthen the United States' cybersecurity posture.

On a broader scale, the cybersecurity landscape in 2024 is becoming increasingly complex, with advanced threats such as AI-powered attacks and phishing at the forefront. Tech Wire Asia reports an escalation in cybersecurity challenges, with significant incidents like the breach at Hewlett Packard Enterprise highlighting the severity of the situation. The evolving threat landscape underscores the importance of initiatives like the JCDC, as collaboration and sharing of intelligence and resources among various stakeholders are critical to defending against sophisticated cyber threats.

The potential failure or weakening of the JCDC due to internal and external pressures could have far-reaching implications for U.S. national security. It could impair the country's ability to respond effectively to cyber threats, leaving critical infrastructure and sensitive government networks more vulnerable to attacks. This situation highlights the need for a cohesive and supported approach to cybersecurity, emphasizing the importance of overcoming the current challenges facing the JCDC to ensure the continued protection of the United States' digital and physical assets.

Conclusions:

In this week's cybersecurity threat intelligence report, we've observed a series of significant cybersecurity events and trends that underline the evolving and sophisticated nature of threats facing the U.S. The discovery of multiple vulnerabilities within the Linux kernel, along with software vulnerabilities in applications like Loom for macOS and MachineSense devices, poses a considerable risk for local privilege escalation and system crashes, necessitating immediate patching actions to mitigate potential exploits.

The disruption of a Chinese-sponsored botnet targeting U.S. critical infrastructure by the DOJ and FBI, alongside CISA's efforts to refine the National Cyber Incident Scoring System (NCISS), emphasizes the ongoing battle against nation-state cyber threats. These efforts are crucial in protecting the nation's critical infrastructure and maintaining national resilience against aggressive cyber campaigns.

However, the potential instability within the Joint Cyber Defense Collaborative (JCDC) poses a significant concern. The initiative, designed to enhance collaboration between the government and the private sector to combat cyber threats, faces challenges from internal discontent and external political pressures. This discontent threatens to undermine the collaborative efforts essential for defending against sophisticated cyber threats, highlighting the need for a cohesive approach to cybersecurity.

The JCDC's issues, combined with recent significant breaches such as the investigation into a potential security breach at Hewlett Packard Enterprise and the security breach affecting AnyDesk's production systems, illustrate the critical importance of robust cyber defenses. These incidents not only reveal the technical aspects of cybersecurity challenges but also the strategic and organizational hurdles that must be overcome to ensure effective defense mechanisms are in place.

Conclusively, the current landscape of cybersecurity threats and challenges underscores the imperative for continuous improvement in threat intelligence, vulnerability management, and collaborative defense strategies. The evolving nature of cyber threats, characterized by advanced techniques such as AI-powered attacks and phishing, requires a dynamic and proactive response to secure the digital and physical assets of the United States. As the cybersecurity landscape continues to change, initiatives like the JCDC must adapt and overcome internal and external pressures to fulfill their vital role in national security. The collective effort and commitment to cybersecurity resilience remain pivotal in navigating the complexities of today’s cyber threat environment.