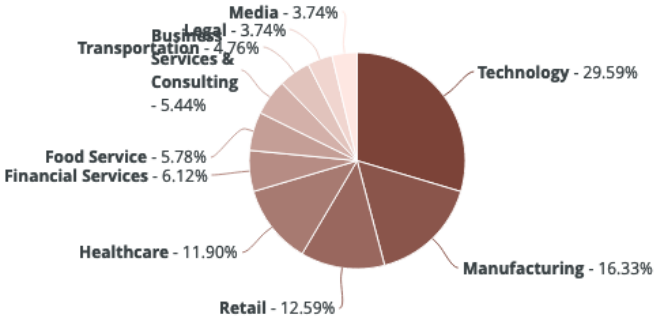
THE TEXAS A&M UNIVERSITY SYSTEM

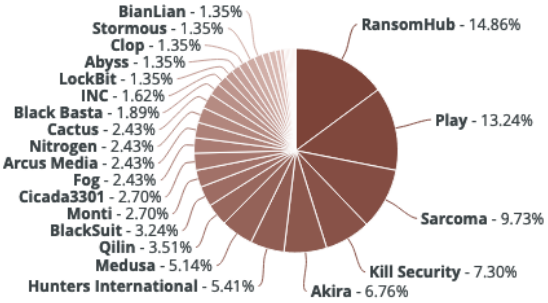
CYBERSECURITY

Weekly Cyber Threat Intelligence Standup

Top Ten Targeted Industries



Ransomware Groups by Percentage of Public Victims



[Cisco Takes DevHub Portal Offline After Hacker Publishes Stolen Data (BleepingComputer)]

Target audience: Authentication Teams, CISO, CIO, Fraud Teams, Incident Response, Security Engineers, Security Ops, Threat Intel/CTI

Summary:

Cisco confirmed today that it took its public DevHub portal offline after a threat actor leaked "non-public" data, but it continues to state that there is no evidence that its systems were breached. Cisco says there are no indications that personal information or financial data was stolen but is continuing to investigate what data may have been accessed. This statement comes after a threat actor known as IntelBroker claimed to have breached Cisco and attempted to sell data and source code stolen from the company. BleepingComputer spoke to IntelBroker about the alleged breach, who said he gained access to a Cisco third-party developer environment through an exposed API token. During Cisco's investigation, IntelBroker grew increasingly frustrated when the company would not acknowledge a security incident, sharing screenshots with BleepingComputer to prove he had access to a Cisco developer environment. These screenshots and files, which we also shared with Cisco, showed that the threat actor had access to most, if not all, of the data stored on this portal. This data included source code, configuration files with database credentials, technical documentation, and SQL files. It is unclear what customer data was stored on these servers, and none was shared with us.

Analyst comment:

Although Cisco asserts that its core systems remain uncompromised, the access gained by "IntelBroker" to a third-party developer environment raises concerns about the security of publicly exposed developer tools and resources. The leaked data could expose Cisco and its customers to further risks, especially if this information is exploited to find vulnerabilities in software or infrastructure. The hacker's access, if proven legitimate, highlights a supply chain

vulnerability

i Ransomware data is gathered within the last 30 days from posted public releases on Ransomer's "Leak" sites.

in which third-party developer environments can become a weak point in an organization's security perimeter. IntelBroker's willingness to expose the breach without extortion attempts suggests this may be more about selling sensitive data than monetary ransom. The leaked data being offered for sale could expose customers using Cisco's DevHub resources to downstream attacks if vulnerabilities are identified in the leaked materials.

North Korean APT Exploited IE Zero-Day in Supply Chain Attack (SecurityWeek)

Target audience: Authentication Teams, Incident Response, Security Ops, Threat Intel/CTI

Summary:

A North Korean threat actor has exploited a recent Internet Explorer zero-day vulnerability in a supply chain attack, threat intelligence firm AhnLab and South Korea's National Cyber Security Center (NCSC) say. Tracked as CVE-2024-38178, the security defect is described as a scripting engine memory corruption issue that allows remote attackers to execute arbitrary code on target systems that use Edge in Internet Explorer Mode. Patches for the zero-day were released on August 13, when Microsoft noted that successful exploitation of the bug would require a user to click on a crafted URL. According to a new report from AhnLab and NCSC, which discovered and reported the zero-day, the North Korean threat actor tracked as APT37, also known as RedEyes, Reaper, ScarCruft, Group123, and TA-RedAnt, exploited the bug in zero-click attacks after compromising an advertising agency.

Analyst comment:

This attack highlights the persistent risk posed by legacy software components—in this case, the jscript9.dll from Internet Explorer—despite the official end of IE support. APT37's exploitation of the ad supply chain as an attack vector exemplifies sophisticated zero-click tactics, allowing malware to be delivered without any user interaction. The targeting of South Korean individuals and groups critical of North Korea underscores APT37's alignment with espionage and cyberwarfare goals. This vulnerability's exploitation through an ad platform emphasizes the necessity of securing supply chain systems, particularly those relying on outdated or vulnerable software components.

See also:

AhnLab and NCSC Release Joint Report on Microsoft Zero-Day Browser Vulnerability (CVE-2024-38178)

Mirai-Inspired Gorilla Botnet Hits 0.3 Million Targets Across 100 Countries (HackRead)

Target audience: Fraud Teams, Security Engineers, Security Ops, Threat Intel/CTI

Summary:

A new Gorilla Botnet has launched massive DDoS attacks, targeting over 100 countries, according to cybersecurity firm NSFOCUS. This botnet, which utilizes Mirai botnet source code and advanced techniques, poses a growing and global threat. Gorilla Botnet leverages a network of compromised IoT devices like an army to launch large-scale DDoS attacks. These attacks flood targeted systems with traffic, crippling their access to users. What makes Gorilla Botnet particularly dangerous is its use of encryption to obscure key data, ensuring long-term control over compromised devices and supporting various CPU architectures, making it compatible with a wide range of devices. Gorilla Botnet uses a distributed C&C network to manage its operations and offers a variety of DDoS attack methods, including UDP Flood, ACK Bypass Flood, and VSE Flood. Additionally, it utilizes connectionless protocols like UDP to spoof IP addresses and further hide its origin.

Analyst comment:

The "Gorilla Botnet" represents a significant evolution of previous botnets, such as "Mirai," with enhanced persistence, encryption, and multi-platform support. Encryption to obscure key data complicates detection and mitigation efforts, while its ability to exploit vulnerabilities such as Apache Hadoop YARN RPC ensures it remains entrenched in compromised systems. By targeting critical infrastructure, the botnet could cause widespread disruption. Its use of connectionless protocols such as UDP to spoof IP addresses also makes tracking and shutting down its origin challenging, showing a level of sophistication typically associated with advanced threat groups such as "Keksec."

See also:

Over 300,000! GorillaBot: The New King of DDoS Attacks (NSFOCUS)