Cybersecurity Threat

May 2023 Newsletter

Threat Actors Zero-In On Healthcare IT

Hackers' growing appetite toward healthcare targets seems to have been confirmed this month, with threat actors moving from attacking healthcare facilities to IT services. The US Health Sector Cybersecurity Coordination Center (HC3) has alerted that hackers seek to exploit a known vulnerability in the Veeam Backup and Replication (VBR) software. VBR is used by many healthcare organizations, which is why it is targeted. The GoAnywhere MFT vulnerability is also popular among hackers to attack hospitals and clinics, often used by Clop and LockBit to drop ransomware. Flaws in PaperCut MF/NG, a popular print management system, are also being increasingly leveraged.

Ransomware Task Force: Mixed Results 2 Years On

In 2021, the international Ransomware Task Force, a cross-sector group created to combat ransomware globally, issued almost 50 recommendations to organizations to deter and disrupt ransomware attacks. Two years later, it is highlighting that ransomware could not be curbed in a major way. Although 2022 saw a decline in the success of ransomware attacks, 2023 saw threat actors become more inventive. Notably, the GoAnywhere MFT file transfer flaw has resulted in over 459 successful exploits in March alone – the highest of any month since 2020. In its 2023 report, the Task Force notes that small and medium organizations are lagging in the implementation of cybersecurity best practices and more needs to be done by way of incentives. Continued collaboration between the private sector and organizations is advised as states continue investments in cybersecurity.

Critical Infrastructure as a Growing Target

As geopolitical tensions flare up, we saw that state-backed APTs are intent on going after the critical infrastructure and services of countries they see as adversarial. This pattern was seen before Russia's invasion of Ukraine as Ukrainian and Georgian CI were taken offline in cyberattacks. It was confirmed as a tactic in last month's Vulkan leaks, which showed the GRU considering cyberattacks on hospitals as fair game.

Washington Steps Up CI Cybersecurity

American authorities seem to have taken these new developments seriously, as President Biden sets his sights on updating a decade-old directive on protecting critical infrastructure. The directive, known as PPD-21, has significant gaps for cybersecurity protection, including a lack of guidelines related to space and cloud computing. Directives such as PPD- 21 should be regularly updated per CISA's director Jen Easterly, who also mentioned the US CI's vulnerability to cyberattacks. Specifically brought up by Easterly were the 2021 Colonial pipeline attack and looming threats posed by Moscow and Beijing.

Exploits and Issued Patches

- CISA is raising the alarm on the active exploitation of severe Android and Novi Survey vulnerabilities. The Android flaws could lead threat actors to escalate privilege on devices running Android without getting additional execution privileges.

  Our Thoughts: Novi Survey has addressed the issue, while Android acknowledges the flaw is executed. We advise immediately patching the Android flaw.

- Illumina's DNA sequencing instruments have been identified by CISA as having multiple vulnerabilities. CISA's advisory highlights possible exposure of IP addresses, leading to eavesdropping, and remote code execution.

  Our Thoughts: Healthcare IT services cyberattacks are on the rise – fixes have been issued, immediate action is advised.

- Sophos has issued patches for a critical code execution vulnerability in its web security appliance.

  Our Thoughts: This vulnerability could be exploited without authentication – this is dangerous. Update to the Sophos Web Appliance 4.3.10.4 to stay safe.

- The PaperCut printing software has issued an advisory on vulnerabilities that could lead to remote code execution and information disclosure.

  Our Thoughts: These are serious vulnerability in a popular software. Immediate updates are advised.

- A Service Location Protocol (SLP) vulnerability could potentially be used to carry out massive DDoS amplification attacks. VMWare has weighted in, claiming that the issue only impacts unsupported older ESXi releases.

  Our Thoughts: Where possible, disable SLP for systems exposed to the internet or untrusted networks. Organizations can also configure firewalls to filter traffic on UDP and TCP port 427, the main entry points for malicious requests exploiting SLP.

Threat Actor Updates

- Solution bugs at Veritas Backup are being targeted by ALPHV/BlackCat ransomware affiliates. The affiliate, tracked as UNC4466, was able to gain footholds in targeted networks through these.

  Our Thoughts: This is worrisome, CISA has advised immediate patching – and we agree.

- ALPHV/BlackCat also successfully caused an outage at the National Cash Register, a US-based consulting company. Threat actors took down the NCR's Aloha point of sale platform, used by many restaurants across the US.

  Our Thoughts: We don't know what ransomware tools were used to carry out this attack – save from a snippet on BlackCat's blog. This reiterates the ongoing threat posed by ransomware.

- STYX Marketplace, a cybercriminal e- commerce platform specializing in fraud and money laundering, has been growing in popularity according to Resecurity.

  Our Thoughts: These are major news for threat hunters, this is a sophisticated platform that has tools to bypass anti-fraud filters.

- A new malware toolkit known as Decoy Dog has been targeting enterprise networks while remaining undetected.

  Our Thoughts: Decoy Dog domains are being tracked and are not used in a widespread manner for now. We advise careful monitoring.

- TrendMicro reports that ViperSoftX, and information-stealing malware, is going after password managers. It is also able to infect browsers other than Chrome now.

  Our Thoughts: Password managers are becoming ubiquitous and we're not surprised to see threat actors adapting. Be selective about the password manager you use.

SUBSCRIBE

Subscribe to our newsletter and stay updated.