March 13, 2024

CYBERFORCE|Q

FEBRUARY 2024 MONTHLY BULLETIN

CyberForce|Q continues to work diligently to detect the latest threats of the cyber landscape. Our monthly bulletin covers the most prominent security incidents of the past month and provides insights into emerging trends and tactics used by threat actors, so you can stay informed.

Key Takeaways

- A potentially unwanted application (PUA) is a non-malicious software that poses security risks through bundled installations and unwanted features like data collection and keylogging.
- ConnectWise addressed two vulnerabilities in ScreenConnect that can allow threat actors to comprimise sensitive data.
- Staying informed about critical security vulnerabilities in widely used tools and taking immediate action, will greatly help protect against new and emerging threats.

Case Study

ClearBrowser and ClearBar: Top PUA's in February

A potentially unwanted application (PUA) is a type of software that can negatively affect a user's privacy or security. Although PUAs are not classified as malware, they can still pose a security risk to users. PUAs can be bundled with other software and often include unwanted additional features that may compromise the user's privacy and security. Some of these features include data collection, keylogging, adware, and browser hijacking.

Two of the most observed PUAs in our participants' environments in February were ClearBrowser and ClearBar. Clear enhances the desktop experience by offering users an easy-to-use integration for web searches, access to curated content, utilities, and other features. However, it's important to note that both ClearBrowser and ClearBar have been flagged for aggressive data collection practices. This can potentially expose users to unnecessary privacy risks.

Steps To Mitigate Risk

- Ensure employees are aware of the risks of downloading and installing software from unreliable sources. Advise them to only install software from trusted sources.
- Implement application allowlisting to restrict the execution environment and set up allowlisting for business roles.
- Consider creating an inventory of existing configurations, policies, and installed software on each host. If the host does not require a specific piece of software, uninstall it to limit the tools available.

How CyberForce|Q Can Help

For over 27 years, CyberForce|Q has been a trusted name in advancing cybersecurity programs. Our expertise lies in designing and executing measurable cybersecurity strategies tailored to organizations of all sizes. With a track record of proven results, we offer services such as customized security assessments, robust security operations centers, and comprehensive strategic guidance. Let us assist your organization in prioritizing its goals, elevating your cybersecurity capabilities, and providing meaningful measurements of progress. Our participants are innovative leaders who share optimal strategies to implement and advance a proven cybersecurity program. CyberForce|Q together with our participants protecting the cyber realm.

External Trend

ConnectWise Addresses Critical Vulnerabilities in ScreenConnect, Urges Immediate Action for On-Premise Partners

ConnectWise ScreenConnect, previously known as ConnectWise Control, is a popular remote desktop software solution utilized by managed services providers, businesses, and help desk teams. However, it is also favored by tech support scammers and cybercriminals, including ransomware groups.

The company recently addressed two vulnerabilities (CVE-2024-1709 and CVE-2024-1708) in ScreenConnect that could potentially allow threat actors to execute remote code or compromise sensitive data and critical systems. These vulnerabilities have been exploited to deliver various threats, including LockBit ransomware, Cobalt Strike, SSH tunnels, remote management tools, various info-stealers, AsyncRAT, and cryptocurrency miners.

Immediate action is advised for on-premise partners to mitigate the identified security risks. They are advising self-hosted or on-premise partners to promptly update their servers to version 23.9.8, which includes a patch for these vulnerabilities. ConnectWise will also provide updated versions of releases 22.4 through 23.9.7 for addressing the critical issue, but upgrading to ScreenConnect version 23.9.8 is strongly recommended.

Contact Us For More Information

248-837-1400 • solutions@cyberforceq.com