Cyble Chronicles: Feb 1 Cybersecurity Insights

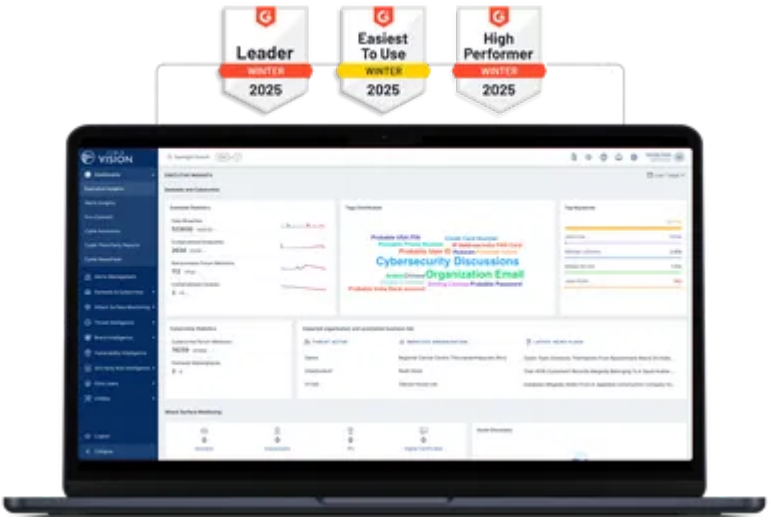
Published: 2024-02-01 · Archived: 2026-04-05 15:39:35 UTC

Uncovering Atomic Stealer (AMOS) Strikes and the Rise of Dead Cookies Restoration

Cyble Research and Intelligence Labs (CRIL) has recently uncovered a series of phishing websites masquerading as popular Mac applications, which are distributing the Atomic Stealer (AMOS), a potent InfoStealer malware. Despite being identified, these deceptive sites remain active, posing a significant threat to unsuspecting users. AMOS is noted for its rapid evolution and frequent updates, showcasing the developers' dedication to enhancing its malicious capabilities. Among its latest advancements is the ability to rejuvenate expired Google Chrome cookies, marking a concerning development in the InfoStealer arena.

This innovation in AMOS's functionality coincides with the discovery of a free code on a cybercrime forum capable of reviving "dead" cookies—a technique that was rumored to be sold for $500 as of October 2023. This revelation has catalyzed a new trend among InfoStealers to adopt this cookie revival feature. For instance, the Xehook Stealer, launched on January 20, 2024, quickly incorporated this feature within days, highlighting a swift adaptation among Threat Actors (TAs). Furthermore, the Command and Control (C&C) centers utilized by AMOS payloads were discussed in a report from early January, suggesting a broader network of connected campaigns or TAs exploiting this technique.

World's Best AI-Native Threat Intelligence



Read Cyble's detailed analysis of this here.

Active Exploitation of Atlassian Confluence RCE Vulnerability (CVE-2023-22527)

On January 26, 2024, Cyble's Global Sensor Intelligence (CGSI) network detected scanning attempts targeting a critical vulnerability in Atlassian Confluence, identified as CVE-2023-22527. This vulnerability, disclosed by Atlassian on January 16, 2024, affects outdated versions of Confluence Data Center and Server. It involves an Object-Graph Navigation Language (OGNL) injection, rated with a maximum CVSS score of 10, indicating its severe impact. OGNL injection vulnerabilities arise when applications like Atlassian Confluence fail to properly validate and sanitize user input before its incorporation into OGNL expressions, allowing Threat Actors (TAs) to execute remote code on the affected systems.

The CGSI network observed these exploitation attempts across various countries, highlighting the global interest of attackers in exploiting this vulnerability. Additionally, Cyble ODIN's scanners have identified over 4,000 internet-exposed instances of Confluence in the past three months, with a significant concentration in the United States, Germany, China, and Russia. This vulnerability, resulting from a template injection flaw in specific Confluence versions, allows unauthenticated attackers to achieve remote code execution. ProjectDiscovery's research further underscores the technical nuances of exploiting this vulnerability, including methods to bypass the 200-character limit in OGNL expressions. This situation underscores the critical need for organizations to promptly address and secure their systems against such vulnerabilities to protect against unauthorized access and potential compromise.

Read CRIL's detailed findings here.

GhostSec Continues to Extend their Support for Cyber Threat Actors and Hacktivists

Cyble Research and Intelligence Labs (CRIL) has raised alarms about the increasing activities of the hacktivist group GhostSec, particularly their recent initiative aimed at enhancing the anonymity of threat actors and hacktivists. GhostSec's new project, dubbed Low-Cost-Database, seeks to gather funds to assist activists and hacktivists in concealing their identities, especially those operating under false identities or seeking asylum for their actions, which they justify as fighting for noble causes. This initiative is significant because the group claims to source databases from collaborators, rather than relying on publicly leaked ones and has even set up a Telegram handle for coordination.

The project has gained traction quickly, with the Telegram channel amassing 2,676 subscribers and offering 28 datasets for sale, impacting organizations across multiple countries. This move is part of a broader trend of GhostSec's involvement in supporting hacktivism and online anonymity. Previous projects include NewBlood, aimed at educating newcomers on hacking skills, and WeFreeInternet, which provided free VPN services to Iranian activists, with plans to expand to other countries facing internet restrictions by their governments.

The anonymity provided by groups like GhostSec poses significant challenges for law enforcement agencies and cybersecurity professionals in attributing and tracking contemporary threat activities. As threat actors may switch identities at any time, this complicates threat assessments and leaves organizations vulnerable to attacks. The support for concealing identities, as offered by well-funded hacktivist groups, exacerbates these challenges, potentially enabling malicious activities by state-sponsored groups and others. Addressing the anonymity of threat actors requires a concerted international effort from both law enforcement and the cybersecurity community to mitigate risks effectively.

Read Cyble's detailed breakdown of this Threat Actor here.

Greenbean: Latest Android Banking Trojan Leveraging Simple RealTime Server (SRS) for C&C Communication

Cyble has recently unveiled its analysis of "GreenBean," a new Android Banking Trojan that poses a significant threat to users of cryptocurrency, payment, and banking applications. This malware, spread through a phishing site promoting a cryptocurrency scheme, specifically targets five applications, with its activities predominantly focused on Android users in China and Vietnam. This regional specificity is deduced from the application's naming conventions and the presence of Chinese and Vietnamese characters within the target code.

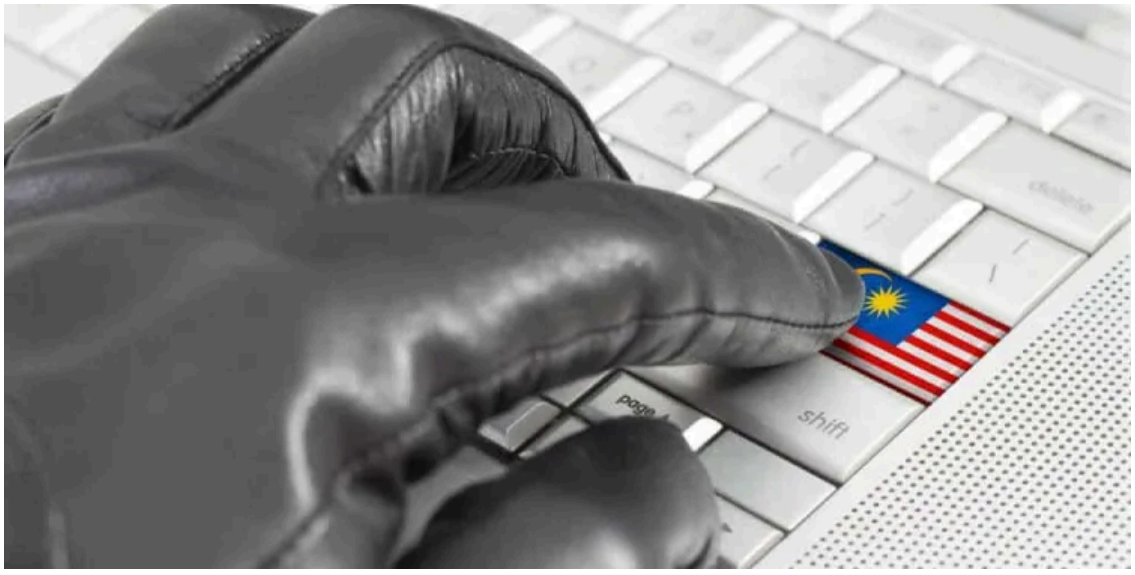
GreenBean exploits the Accessibility service on Android devices to harvest credentials from the targeted applications. A distinctive feature of this malware is its use of video streaming capabilities facilitated through WebRTC technology. This allows the attackers not only to collect data but also to potentially observe and record the screen of the infected device, adding a layer of sophistication to their espionage capabilities. Moreover, the malware employs an open-source project, the Simple Realtime Server (SRS), for its Command and Control (C&C) communications. This choice of C&C infrastructure is notable for its support of WebRTC streaming, indicating the malware developers' preference for leveraging robust and versatile technologies to manage their operations.

At the time Cyble published their findings, the phishing site used to disseminate GreenBean was still operational, signaling that the malware continues to be a live threat. The continued activity of this phishing site underscores

the importance of ongoing vigilance and the need for users to be cautious of phishing schemes, especially those promoting too-good-to-be-true cryptocurrency opportunities. This analysis by Cyble sheds light on the evolving landscape of Android banking Trojans and the increasing complexity of threats facing users in the digital finance space.

Read CRIL's detailed analysis of this here.

Malaysian Telecom Provider, Aminia Hit by Pro-Israeli Cyberattack, Website Inaccessible



The Malaysian telecom provider Aminia was recently targeted by the pro-Israeli hacktivist group R00TK1T ISC Cyber Team, marking their first attack against the company amidst threats to Malaysian internet infrastructure. The attack resulted in the internal defacement of Aminia's billing and Managed WiFi services portals, potentially indicating a data breach. Following the cyberattack, Aminia's website became inaccessible, showing an "Index of /" error, typical of cyberattack aftermaths where server settings are altered or files are deleted.

R00TK1T ISC Cyber Team's actions included leaving a warning message on the compromised portal and sharing screenshots exposing sensitive information from Aminia's systems. The group accused Malaysia of supporting cyber threats related to the Middle East conflict and threatened further exposures. This attack is part of a broader threat to target Malaysian organizations, as indicated by the group's explicit threats made on January 26. The hacktivists also exploited vulnerabilities in the Controlled Access Point System Manager (CAPsMAN) panel manufactured by MicroTik, revealing a critical security flaw (CVE-2023-41570). The incident raises significant concerns over the cybersecurity of Malaysian telecom networks and underscores the need for enhanced security protocols and vigilance.

Read The Cyber Express' detailed coverage here.
