28th November– Threat Intelligence Report

By lorenf

Published: 2022-11-28 · Archived: 2026-04-17 02:00:51 UTC

November 28, 2022

For the latest discoveries in cyber research for the week of 28th November, please download our Threat Intelligence Bulletin.

Top Attacks and Breaches

- The European Parliament website has been attacked following a vote declaring Russia a state sponsor of terrorism. The pro-Russian hacktivist groups Anonymous Russia and Killnet, have claimed responsibility for the attack, causing an ongoing DDoS (Distributed Denial of Service).
- Ukrainian organizations have been a victim of ransomware attacks that have been linked to the Russian military cyber-espionage group Sandworm (AKA Redmond, IRIDIUM). The group has used a new malware dubbed 'RansomBoggs', distributed by a PowerShell script from the domain controller. 'RansomBoggs' encrypts files using AES-256 in CBC mode using a random key, and adds a '.chsch' extension to the encrypted files.
- The Ragnar Locker ransomware gang has published stolen data belonging to Zwijndrecht police, a local police unit in Antwerp, Belgium. The data, which was initially attributed to the municipality of Zwijndrecht, contains a large amount of personal information including thousands of car plate numbers, fines, crime report files, investigation reports, and more.
- The Sports betting company DraftKings has been breached, causing the loss of approximately $300K of funds from active user accounts. The threat actors managed to change user passwords, and enabled two-factor authentication on a different phone number which led them to gain personal bank account information.
- Several American colleges, including Cincinnati State College, have been the victims of ransomware attacks over the Thanksgiving holiday. The threat actors shut down the colleges' financial aid services, network printing, VPN tools, admission application platforms, transcript exchanges, grading tools and more. Ransomware attacks targeting educational institutions are a part of on-going recently observed trend.

Check Point Threat Emulation provides protection against this threat (Trojan.Win.ViceSociety.)*

- Black Basta ransomware group is running a campaign targeting organizations in the United States, Canada, United Kingdom, Australia, and New Zealand. The group uses QakBot (AKA QBot, Pinkslipbot) banking Trojan to infect an environment and install a backdoor allowing it to drop the ransomware. Successful

exploitation will allow the ransomware group to steal victims' financial data, including browser information, keystrokes, and credentials.

Check Point Threat Emulation provides protection against this threat (Trojan.Wins.Qbot; Banker.Wins.Qbot)

Vulnerabilities and Patches

- Google has released an update for the Chrome web browser to patch a new, actively exploited zero-day vulnerability. Tracked as CVE-2022-4135, the vulnerability resides in the GPU component, as a heap-based buffer overflow bug that could be used to crash a program or execute arbitrary code, leading to unintended behavior.
- Researchers have observed a recently patched SQL injection vulnerability in Zoho ManageEngine products. Tracked CVE-2022-40300, the flaw will let threat actors send a crafted request to the target server, which could lead to arbitrary SQL code execution in the security context of the database service, which runs with SYSTEM privileges.
- Microsoft has tied an attack on seven facilities managing the electricity grid in Northern India to a vulnerable component, Boa web server, used by vendors across a variety of IoT devices and popular software development kits (SDKs). Successful exploitation could allow attackers to silently gain access to networks by collecting information from files.

Threat Intelligence Reports

- Researchers have investigated the Luna Moth ransomware campaign that has extorted hundreds of thousands of dollars from several victims in the legal and retail sectors, by using callback phishing and telephone-oriented attack delivery (TOAD).
- A technical analysis of a new Go-based information stealer named 'Aurora' has been published. The malware steals sensitive information from browsers and cryptocurrency apps, exfiltrates data directly from disks, and loads additional payloads.
- Researchers dived into a new ransomware tool called 'AXLocker', which encrypts several file types and make them unusable, steals Discord tokens from the victim's machine, and demands a ransom payment to recover the encrypted files.

Check Point Threat Emulation provides protection against this threat (Ransomware.Win.TouchTrapFiles.A)

- Researchers have discovered a new variant of the 'RansomExx' ransomware, primarily designed to run on Linux operating system. The ransomware, operated by the DefrayX threat actor group, encrypts files using AES-256, with RSA used to protect the encryption keys.

Check Point Threat Emulation provides protection against this threat (Ransomware.Wins.Ransomexx)

- An information-stealing Google Chrome browser extension named 'VenomSoftX' is being deployed by Windows malware to steal cryptocurrency and clipboard contents as users browse the web. The Chrome extension is being installed by the ViperSoftX Windows malware, which acts as a JavaScript-based RAT and cryptocurrency hijacker.

BLOGS AND PUBLICATIONS

- Check Point Research Publications
- Global Cyber Attack Reports
- Threat Research

February 17, 2020

“The Turkish Rat” Evolved Adwind in a Massive Ongoing Phishing Campaign

---