DeepSeas Threat Intel Report

*The DeepSeas monthly threat intelligence report is a collection of the top reports, threat actor activity, and malware from the month of **April 2025**. Find out how you can get even more curated intelligence reporting by emailing CyberDefense@deepseas.com.*

Malware

NEPTUNE RAT: An Advanced Windows RAT with System Destruction Capabilities and Password Exfiltration from 270+ Applications

CYFIRMA recently announced on its blog an update to Neptune RAT which contains features that make the malware more evasive and damaging to victims. Hosted on GitHub, Neptune RAT is a VBScript file that now contains direct PowerShell commands, uses the catbox.moe API to host malicious payloads, and features new obfuscation techniques, VM detection, and persistence methods. The RAT also comes packaged with other dangerous capabilities, such as ransomware functionality, a crypto clipper, a password grabber, live desktop monitoring, AV deactivation, and more.

Analysis from DeepSeas: The DeepSeas TIDE has observed that the publicly facing GitHub this RAT was hosted on (run by the "MasonGroup" or "FreeMasonry") has been taken down by GitHub. The wide-scale improvements made to the malware show, however, that activity from MasonGroup is not likely to stop anytime soon, especially with so much development time invested into Neptune RAT. We suspect more activity from MasonGroup to occur in the future.

Variant Identified: ResolverRAT Enters the Maze

Morphisec Threat Labs explained in a recent blog post that their discovery of "ResolverRAT" was due to its use of runtime resolution mechanisms and dynamic resource handling for evasion purposes. The RAT, loaded using reflective DLL loading, can perform many unique actions, including .NET resource resolver hijacking and control flow flattening, certificate pinning, code obfuscation, and timer-based connection management. For persistence, the RAT uses the registry and the file systems to hide in a victim's environment.

Analysis from DeepSeas: The unknown group's approach to initial access (targeting companies indiscriminately about vague legal troubles), along with phishing lures with multiple languages, shows a strategy that focuses on financial gain no matter the victim. In addition, due to overlaps with varying aspects of the CopyRh(ight)adamantys campaign, such as payload delivery mechanisms, artifact reuse, and lure themes, it is possible that both groups may collaborate or in fact, be one in the same.

Sapphire Werewolf Refines Amethyst Stealer to Attack Energy Companies

BI.ZONE Threat Intelligence has made headlines regarding a new variant of Amethyst, an information stealer used by the threat group Sapphire Werewolf. One of the new features available to this updated variant includes advancements in VM detection, specifically looking for VMware, and VirtualBox. The malware can also now collect from the registry, files, hardware manufacturing data, BIOS, disk, connected IoT devices, services, and more. Amethyst stealer also now uses the Triple DES symmetric algorithm for self-encryption.

Analysis from DeepSeas: The data Sapphire Werewolf was trying to steal consisted of sensitive documents, including plug and play devices like USB drives, along with credentials from web browsers such as Google Chrome, Opera, Yandex, Brave, Orbitum, Atom, Kometa, and Edge Chromium. They also attempted to exfiltrate Telegram data, as well as FileZilla and configuration files from remote desktops and VPN clients. Sapphire Werewolf was believed to

be espionage-focused in past, targeting Russia. This change in activity shows, perhaps, a change in modus operandi by the group.

Vulnerability

Reconnaissance Campaign Against Vulnerable Palo Alto Network Devices

GreyNoise security researchers uncovered a large scale campaign impacting Palo Alto Networks PAN-OS GlobalProtect portal. The campaign consists of scanning from over 24,000 IP addresses. The activity from these IPs has been primarily seen originating from the United States, Canada, Finland, Netherlands, and Russia, while directing their attacks towards countries such as the United States, the United Kingdom, Ireland, Russia, and Singapore.

Analysis from DeepSeas: Threat actors have targeted Palo Alto Networks PAN-OS vulnerabilities and vulnerabilities in other edge devices with more aggression over the last 12 to 18 months. This type of scanning activity generally denotes that threat actors are targeting old vulnerabilities but has also been an indication that new vulnerabilities will be released within 2-4 weeks from the scanning activity. It is unknown whether the threat actors are developing a zero-day exploit or if they are attempting to discover a zero-day exploit with this activity.

Nation-State

UNC5174's Evolution in China's Ongoing Cyber Warfare: From SNOWLIGHT to VShell

After a year of operating under the radar, the Sysdig Threat Research Team (TRT) identified a new campaign from Chinese state-sponsored threat actor UNC5174. It was found that the threat actor used a new open-source tool and command and control (C2) infrastructure in late January 2025. First discovered was a malicious bash script that downloaded multiple executable files for persistence. One of the binaries downloaded was a variant of UNC5174's SNOWLIGHT malware, previously identified by Mandiant in a campaign against F5 devices

and recently mentioned in the French Cyber Threat Overview report released in March 2025 by the French National Agency for Information Systems Security (ANSSI).

Analysis from DeepSeas: UNC5174 is likely a subset of a larger Chinese threat actor. They may be the unit responsible for initial access to victims, and then the victims are passed to a different threat group for exploitation. The use of an open-source C2 infrastructure is likely for obfuscation among other threat groups and cyber-criminals.

Renewed APT29 Phishing Campaign Against European Diplomats

Starting in January 2025, Check Point Research (CPR) has been tracking a wave of targeted phishing attacks aimed at European governments and diplomats. The techniques, tactics, and procedures (TTPs) observed in this campaign align with the WINELOADER campaigns that were attributed to APT29, a Russia-linked threat group. APT29, also commonly referred to as Midnight Blizzard or Cozy Bear, is known for targeting high-profile organizations, including government agencies and think tanks. Their operations vary from targeted phishing campaigns to high-profile supply chain attacks that utilize a large array of both custom and commercial malware. The threat group is also associated with the SolarWinds supply chain attack. In this current wave of attacks, the threat actors impersonate a major European Ministry of Foreign Affairs to send out invitations to wine tasting events, prompting targets to click a web link leading to the deployment of a new backdoor called GRAPELOADER. This campaign appears to be focused on targeting European diplomatic entities, including non-European countries' embassies located in Europe.

Analysis from DeepSeas: APT29 has focused most of its efforts on NATO and the war in Ukraine. Its operations have been centered on intelligence gathering and strategic information regarding diplomatic and military efforts involving Russia. Russia will likely continue to target governments and organizations that provide strategic information.

Cyber Crime

Newly discovered cyber-criminal groups

- Bert
- Crypto24
- Silent
- Gunra