SECURITY ADVISORY

CYBER STASH

February, 2023

CVE-2020-3992 | CVE-2021-21974

Nevada Ransomware

Context

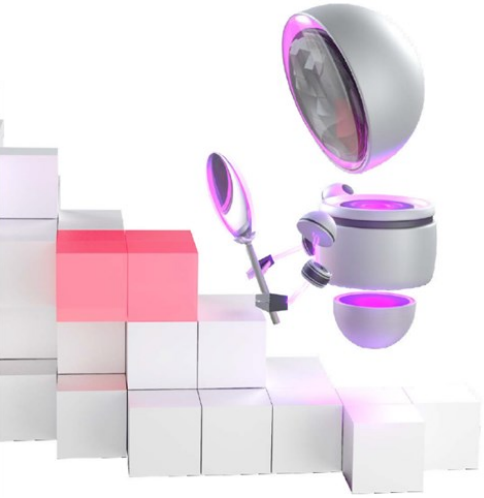
NEVADA is a ransomware that targets Windows and Linux operating systems, encrypting files and appending the ".NEVADA" extension to filenames. It also drops a ransom note in folders containing encrypted files. The security community has addressed the malware's initial access vector and variations, with investigations ongoing to determine which known vulnerabilities attackers may be exploiting.

As of February 3rd, 2023, Nevada ransomware is targeting VMware ESXi servers exposed to the Internet, and it's a growing Ransomware-as-a-Service with an affiliate network for both Russian and English-speaking entities. The new variant of ESXiArgs encrypts more data, making it challenging to recover, and the bitcoin wallet is no longer trackable. To counter the ongoing situation, it's essential to ensure that ESXi servers are updated with VMWare's provided patches for known vulnerabilities and not exposed to the Internet.

Mitigation

To reduce the chances of being affected by Nevada Ransomware, it is advised to implement the following measures for risk mitigation:

- Update ESXi servers with VMWare's provided patches for known vulnerabilities.
- Block inbound traffic with OpenSLP port 427 that's destined to exposed ESXi Servers or restrict access to the exposed service from trusted IP addresses.
- Restrict outbound traffic from ESXi Servers to only trusted infrastructures (domains and IP addresses).
- The U.S. Cyber Security and Infrastructure Agency (CISA) has released a script called ESXiArgs-Recover, used to recover VMware ESXi servers encrypted by the type of ransomware attack described above.



Technical Details

Tactics, Techniques and Procedures

The Nevada Ransomware uses various tactics, techniques, and procedures (TTPs) to infect and encrypt victims' files. Some of the common TTPs used by the Nevada Ransomware include:

- *T1192* - Phishing emails: The ransomware is often distributed through phishing emails that contain malicious attachments or links.
- *T1204* - Exploit kits: The ransomware can also be distributed through exploit kits that take advantage of vulnerabilities in software or operating systems.
- *T1076* - Remote Desktop Protocol (RDP) attacks: The ransomware can also be distributed through RDP attacks that exploit weak or default credentials.

Cyber Threat Intelligence

The ransomware is to distributed by a group of cybercriminals that operate on the dark web. According to their own cybercrime forum posts, Nevada provides affiliates with a "locker" (encryption) payload written in Rust that has support for Linux, Windows, and VMware ESXi hosts, the latter of which is the subject of this recent increase in vulnerability scanning and ransomware attacks.

Nevada ransomware started to be promoted on the RAMP darknet forums on December 10, 2022, inviting Russian and Chinese-speaking cybercriminals to join it for an 85% cut from paid ransoms. For those affiliates who bring in a lot of victims, Nevada say they will increase their revenue share to 90%.

Researchers at Zscaler ThreatLabz have discovered that the Nevada ransomware shares a significant amount of code with the Rust-based version of the Nokoyawa ransomware. Then, in January of 2023, ThreatLabz also found another version of Nokoyawa that was written in C and is similar to the original version. However, it uses the same configuration options as the Rust-based Nokoyawa 2.0, which are passed via the command-line.

References

Sandbox Report

- https://www.hybrid-analysis.com/sample/855f411bd0667b650c4f2fd3c9fbb4fa9209cf40b0d655fa9304dcdd956e0808/6401dca892a28b0ab20498a2
- https://www.virustotal.com/gui/file/855f411bd0667b650c4f2fd3c9fbb4fa9209cf40b0d655fa9304dcdd956e0808

Public Intelligence

- https://www.bleepingcomputer.com/news/security/new-nevada-ransomware-targets-windows-and-vmware-esxi-systems/
- https://www.pcrisk.com/removal-guides/25915-nevada-ransomware
- https://www.zscaler.com/blogs/security-research/nevada-ransomware-yet-another-nokoyawa-variant