Quorum Cyber

Threat Intelligence Nevada Ransomware Report

TLP Status: Green

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft Solutions Partner

Table of Contents

Document Control

Revision History

Version	Date	Summary of Changes
1.0	03/02/2023	Initial Report
1.1	06/02/2023	PDF Formatting

Related Documents

The following documents are either referenced within, or are related to, the content of this document:

Document Name	Date	Version
-	-	-

Nevada Ransomware Analysis

Overview

A ransomware operation, known as 'Nevada', has been detected targeting Windows and VMware ESXi systems, and is distributed via infected email attachments (macros), torrent websites and malicious advertisements.

The associated ransomware group was reported on the RAMP darknet forums, dating back to 10th December 2022. The group operates within the context of a Ransomware-as-a-Service (RaaS) model distribution and has invited Russian and Chinese threat actors to collaborate with their attack efforts, for a ransom cut of 85%. RaaS is a particularly dangerous model as it provides threat actors that lack sufficient tooling and infrastructure with the ability to carry out sophisticated attacks, thereby making the ransomware more widespread.

Nevada ransomware group operates within the confines of a 'Rust-based locker' feature, containing a real-time interactive messaging portal and the implementation of separate domains within the Tor network with regards to the affiliates and victims. Additional ransomware variants that are known to have adopted the Rust feature in recent months include BlackCat, Hive, Luna, Nokoyawa, RansomExx, and Agenda.

The ransomware group appears to have explicitly excluded English-speaking threat actor affiliates. However, they remain open to conducting business with brokers from any location. One unique feature of the Nevada ransomware group pertains to the list of target locations that they exclude from their encryption process. An emerging trend amongst ransomware groups, in general, is that they tend to avoid targeting potential victims inside Russia or the Commonwealth of Independent States (CIS) member list. However, the Nevada ransomware group has extended that list to the following nation states: Albania, Hungary, Vietnam, Malaysia, Thailand, Turkey and Iran.

Two variants of the Nevada ransomware strain currently exist. One directly affects Windows operating systems, whereas the other applies to Linux/ VMware ESXi systems. Both variants support a set of flags that provides the operators with control over the target system.

Cyber security researchers from Resecurity have identified similarities between this form of the Nevada ransomware variant and that of Petya ransomware[1]. The significance being that both of these ransomware variants possess a potential weakness that could allow the private key to be recovered, thus allowing the data to be retrieved without handing over the demanded ransom payment.

The Nevada ransomware group applies a double extortion technique, meaning that not only does the group encrypt the private data of the victim and demand a ransom for the keys, but they also threaten the victim with the publication of the data on their own dark webpage. This is likely designed to increase pressure on the victim and increase the chances of payment.

Impact

Successful exploitation by Nevada ransomware will almost certainly result in the encryption and exfiltration of significant quantities of data held on the compromised system, prior to a ransom of a predetermined value being issued. The ransom amount demanded will almost certainly depend on the estimated value of the compromised organisation. Furthermore, such a compromise of data will also result in the organisation incurring a negative reputational impact. Encrypted data may include private customer data, corporate finance data and system credentials that if released can assist threat actors with future attacks.

[1] https://resecurity.com/blog/article/nevada-ransomware-waiting-for-the-next-dark-web-jackpot

Due to the locker being written in Rust, execution through the console will result in encryption of selected files and directories, self-deletion, deletion of shadow copies, loading of hidden drives, self-mode encryption, and discovery and encrypting network shares.

Incident Detection

A comprehensive endpoint detection and response (EDR) solution such as Microsoft Defender can provide additional protection against ransomware threats like that implemented by the Nevada ransomware group. EDR solutions can alert system users of potential breaches and stop further progress before the malware can do significant damage.

If an EDR solution is not being used, the first instance of detection is likely to be the ransom note. The note will be labelled with the following file extension: readme.txt.

A copy of a Nevada ransom note is shown below:

Ransom note:

Greetings! Your files were stolen and encrypted.

You have two ways:

-> Pay a ransom and save your reputation.

-> Wait for a miracle and lose precious time.

We advise you not to wait.

After 2 days of your silence we will make a call your superiors and notificate them about what's happened.

After another 2 days all your competitors will be informed about your decision.

Finally, after 3 days we will post your critical data on our TOR-website.

If you are going to recover your files from backups and forget this like a nightmare, we are hurry to inform you – you can't prevent a leak.

Recommendations:

->Don't delete/rename encrypted files

->Don't use any public "decryptor", they contain viruses.

You have to download TOR browser.

To contact with us your can use the following link:

##[LINK NOT INSERTED FOR SECURITY PURPOSES]##

The cat is out of the bag.

Affected Products

The Nevada ransomware has the potential to impact the following products:

- Windows Operating System
- Linux /VMware ESXi systems

Containment, Mitigations & Remediations

It is recommended that employees receive training on how to spot signs of phishing emails. A common initial ingress mechanism utilised by the Nevada ransomware group is the distribution of phishing emails with malicious attachments. Whilst user awareness, through the utilisation of regular phishing training, would assist in reducing the likelihood of successful exploitation, in-house training will not be able to prevent attacks led by threat actors with stolen credentials obtained via stealware. Additional technical controls should also be explored. These controls could encompass the implementation of the multi-factor authentication (MFA) requirement for all users, conditional access policies and web proxies filtering on low- or non-reputation domains.

One main method of reducing the threat of Nevada ransomware is to detect it in the early stages through the use of an effective and monitored EDR solution. An effective EDR tool such as the Microsoft Defender suite will block ransomware attempts once detected.

Organisations can also perform routine back-ups of sensitive data that is needed to run the business and to keep a copy offline in case back-ups are impacted by the attack[2]. Therefore, if a breach occurs and the business can no longer function, a back-up is ready to use, and the business can continue to operate with little disruption. However, this does not nullify the fact that customer and employee data may have also been lost, and potentially released as Nevada operates via double extortion.

Indicators of Compromise

Associated Nevada domain:

nevcorps5cvivjf6i2gm4uia7cxng5ploqny2rgrinctazjlnqr2yiyd[.]onion

Associated Nevada ransomware hashes (MD5):

- 709ba88e758454f097959c3e62997000
- 99549bcea63af5f81b01decf427519af
- 1396ab93e9104faaf138ac64211471ba
- f1f569c6e4f961007f7411fca131bbe0
- fb5dcf0b880b57b10a2093f164f2ed27

[2] https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world

Threat Group

The Nevada ransomware group operates on the basis of a double extortion technique. Not only does the group encrypt the private data of the victim and demand a ransom for the keys, but they also threaten the victim with the publishing of their data on their own dark webpage. This is likely designed to increase pressure on the victim and increase the likelihood of the desired payment. Despite the group's recent emergence, it is highly likely that they are composed of seasoned cybercriminals who have experience with ransomware extortion tactics, due to the application of the double extortion technique, as well as their related rise to notoriety.

A relative lack of specific detail exists with regards to this ransomware group and the correlating new ransomware variant. However, due to the Nevada ransomware group having been well presented on the RAMP underground forum, they have already been detected to be formulating initial collaboration efforts with both Russian and Chinese cyber threat actors. As such, it is highly likely that attack efforts, originating from the group, will continue to increase in frequency and prevalence.

Nevada Mitre Methodologies

Reconnaissance
T1590 - Gather Victim Network Information[3]

Resource Development
T1588.001 - Obtain Capabilities: Malware[4]

Persistence
T1547 - Boot or Logon Autostart Execution[5]
T1574.002 - Hijack Execution Flow: DLL Side-Loading[6]

Defence Evasion
T1027 - Obfuscated Files or Information[7]
T1070 - Indicator Removal[8]

Command and Control
T1105 - Ingress Tool Transfer[9]
T1573 - Encrypted Channel[10]

Impact
T1486 - Data Encrypted for Impact[11]

[3] https://attack.mitre.org/techniques/T1590/
[4] https://attack.mitre.org/techniques/T1588/001/
[5] https://attack.mitre.org/techniques/T1547/
[6] https://attack.mitre.org/techniques/T1574/002/
[7] https://attack.mitre.org/techniques/T1027/
[8] https://attack.mitre.org/techniques/T1070/
[9] https://attack.mitre.org/techniques/T1105/
[10] https://attack.mitre.org/techniques/T1573/
[11] https://attack.mitre.org/techniques/T1486/

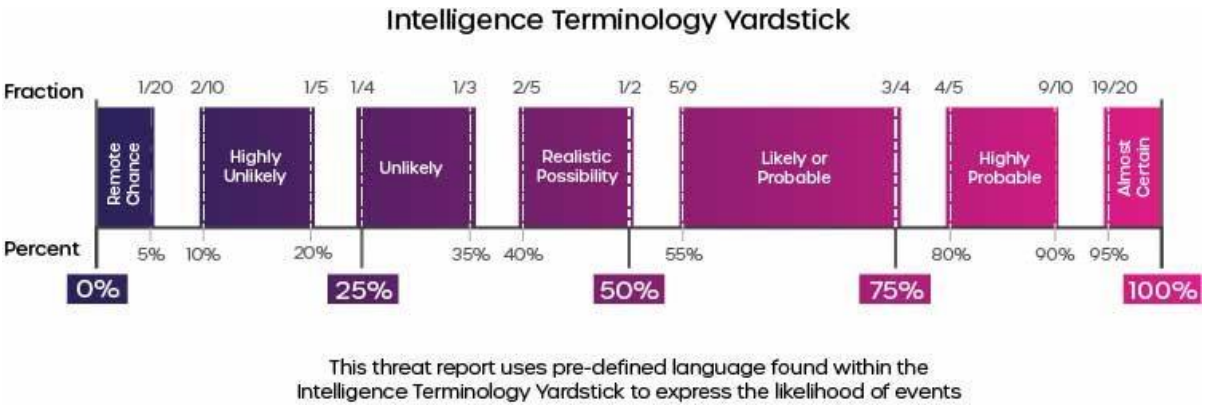
Additional Information

Nevada ransomware news article: SCMagazine

Nevada ransomware news article: BleepingComputer

Nevada technical blog: Resecurity

Intelligence Cut-off Date (ICoD): 06/01/2023 10:00 GMT



This threat report uses pre-defined language found within the Intelligence Terminology Yardstick to express the likelihood of events