Nevada Ransomware Campaign

February 2023

Cyberint

TABLE OF CONTENTS

Cyberint Copyright © All Rights Reserved 2023

EXECUTIVE SUMMARY

Over the weekend, a relatively new ransomware group named Nevada Ransomware initiated a first massive campaign, targeting any ESXi machine that is exposed to the internet.

The group seemed to compromise hundreds of servers over the weekend and caused major damage.

Although the scale of this campaign is one of the biggest we have seen, it might already have a solution.

WHO IS NEVADA?

Nevada group was first introduced to the cybercrime industry in December 10, 2021, as they published an announcement of recruiting new members to their Ransomware-as-a-Service plan (Figure 1).

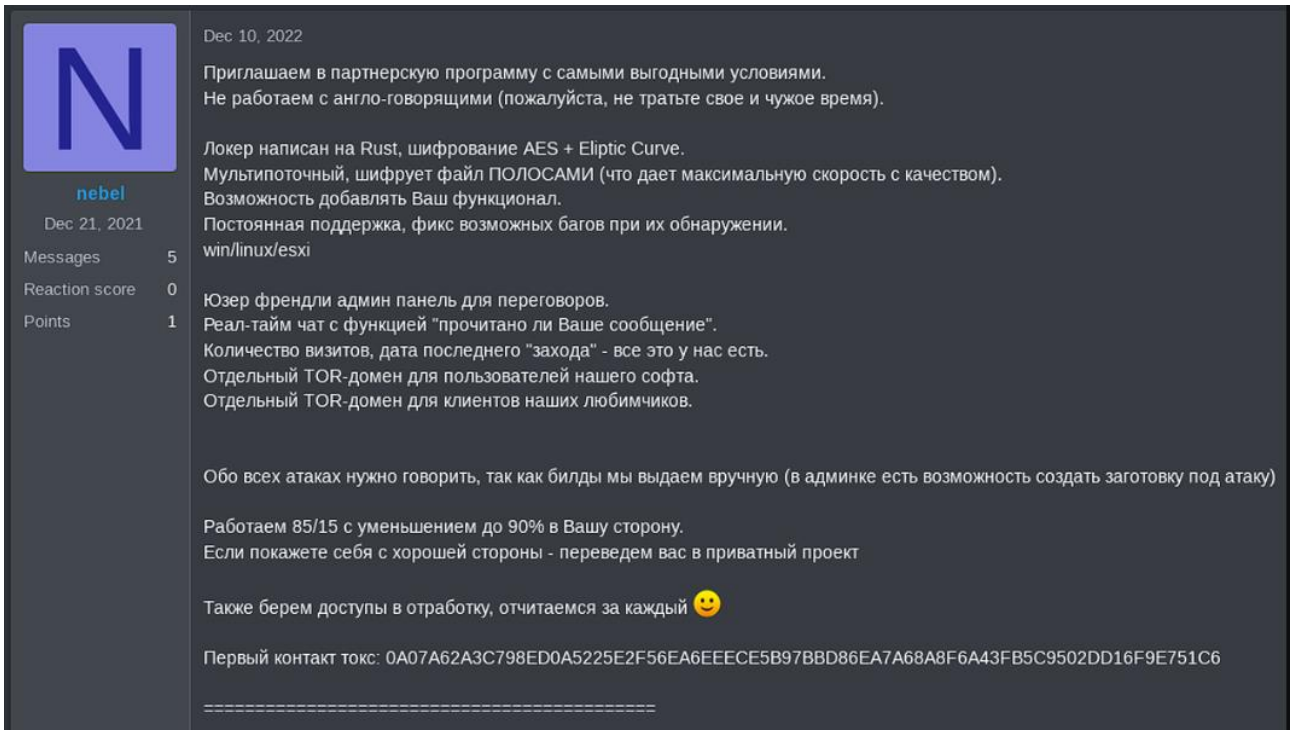


Figure 1: Nevada group's first recruiting announcement

The group works only with Russian and Chinese-speaking individuals.

Their encryption module is built in Rust and is currently still under development as the group claim they will target Windows and Linux machines in addition to ESXi.

As the group is still very new, there is a chance that this incident was merely an initial experiment for their products and a free PR they have received given the fact that any threat actor in the cybercrime industry knows their name.

Cyberint Copyright © All Rights Reserved 2023

CONTROL PANEL

The group has a dashboard for each member to log in that grants access to private information about ongoing campaigns, chat with other members and so on (Figure 2).

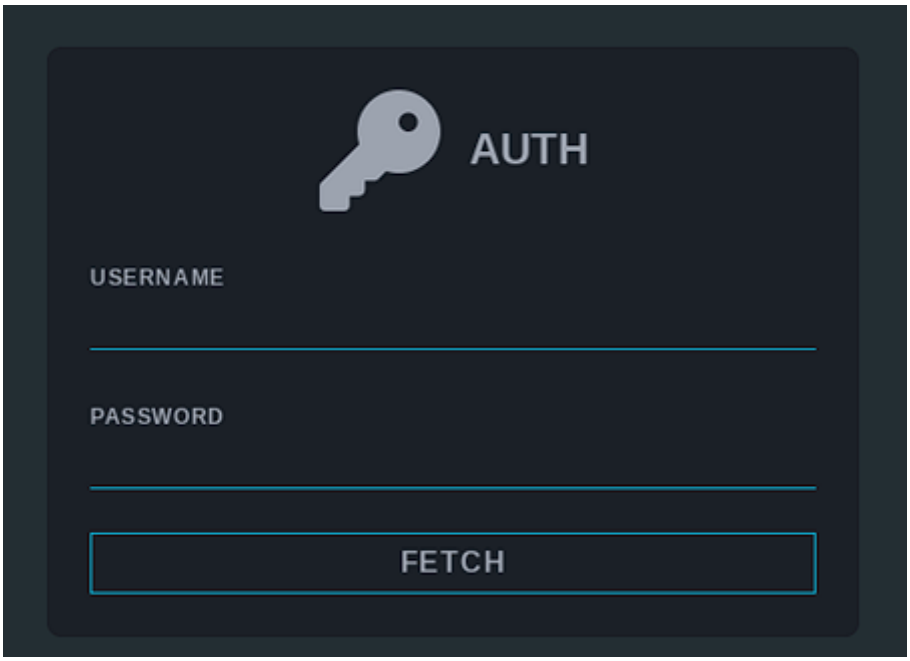


Figure 2: Nevada login page

VICTIMOLOGY

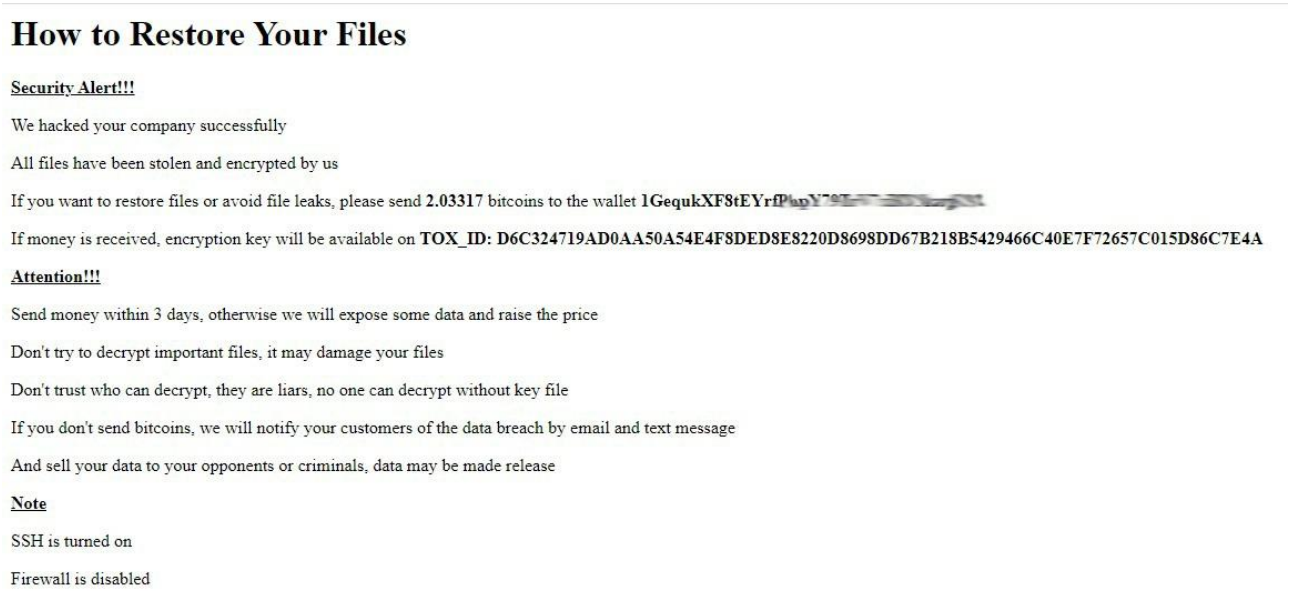
As mentioned, the group includes only Russian and Chinese speakers. Due to that, the group's encryption module does not target Russia, Albania, Hungary, Vietnam, Malaysia, Thailand, Turkey and Iran.

Over the weekend, the group targeted any front-facing ESXi machine that could find and exploited multiple related vulnerabilities. A big part of the victims' count is focused on France.

The group encrypts the configuration files of the ESXi systems instead of encrypting the vmdk disks themselves.

Then, a ransomware note (Figure 3) is left for the victim with contact information for negotiations.

Cyberint Copyright © All Rights Reserved 2023



How to Restore Your Files

Security Alert!!!

We hacked your company successfully

All files have been stolen and encrypted by us

If you want to restore files or avoid file leaks, please send **2.03317** bitcoins to the wallet **1GequkXF8tEYrf**[redacted]

If money is received, encryption key will be available on **TOX_ID: D6C324719AD0AA50A54E4F8DED8E8220D8698DD67B218B5429466C40E7F72657C015D86C7E4A**

Attention!!!

Send money within 3 days, otherwise we will expose some data and raise the price

Don't try to decrypt important files, it may damage your files

Don't trust who can decrypt, they are liars, no one can decrypt without key file

If you don't send bitcoins, we will notify your customers of the data breach by email and text message

And sell your data to your opponents or criminals, data may be made release

Note

SSH is turned on

Firewall is disabled

Figure 3: Nevada ransomware note

A SUCCESS STORY?

At first glance, it seems like the ultimate success story for any new threat group out there - hundreds of victims in one weekend with only few weeks of operation.

The group was able to cause a lot of damage to its victims which is true, but currently it seems that not a lot of victims has paid the ransom.

When tracking the balance in the wallet addresses the group provided in their ransom notes it seems that there had 0.5BTC transferred to their wallets - not much for this scale of a campaign.

Overall, the group might still take this event as a major win and a massive debut both because of the number of victims that goes by the hundreds and the major PR the group has received as any criminal in the cybercrime industry knows who they are which might help in recruiting some talented people.

Cyberint Copyright © All Rights Reserved 2023

CONCLUSIONS

Nevada Ransomware group is a new and interesting group. comparing their debut to other new groups such as BianLian, Royal and BlackBasta on 2022, no one was able to obtain the victims' count Nevada did.

Overall, the group might consider their debut as very successful although it seems to have little profit in the matter of finance.

The group is at a very early stage and it will take a bit of time and effort to recruit and develop their modules in order to make some impactful campaigns, but the Cyberint Research Team is convinced that they might be a solid new threat in our landscape in the near future.

RECOMMENDATIONS

- What Nevada was relaying on in this campaign was exposed and front-facing ESXi interfaces. In many cases, there is no real need to expose your ESXi interfaces, and we recommend do it only when necessary.
- One vulnerability that Nevada claimed to use goes back to 2021. It is a great example of how version control and patching is a key factors that might help keep our infrastructure safe.
- One of the cyber security community members, @habib_karatas has published a solution that might help recover the encrypted config files:
  - Delete the encrypted configuration file
  - Create an empty virtual machine
  - Open the config file on the new machine and put it in the directory of your encrypted machines.
  - Replace the information in the config file with the encrypted machine names.
  - Go to the VMWare screen and "register VM"

IOCS

- 104.152.52.55
- 43.130.10.173

Cyberint Copyright © All Rights Reserved 2023

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

USA - NY

Tel: +1-646-568-7813
368 9th Ave, Suite 11-108, New York, NY 10001

USA - MA

Tel: +1-646-568-7813
22 Boston Wharf Road Boston, MA 2210

UNITED KINGDOM

Tel: +44-203-514-1515
6 The Broadway, Mill Hill NW7 3LL, London

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

Cyberint Copyright © All Rights Reserved 2023