New RedAlert Ransomware targets Windows, Linux VMware ESXi servers

bleepingcomputer.com/news/security/new-redalert-ransomware-targets-windows-linux-vmware-esxi-servers/

Lawrence Abrams

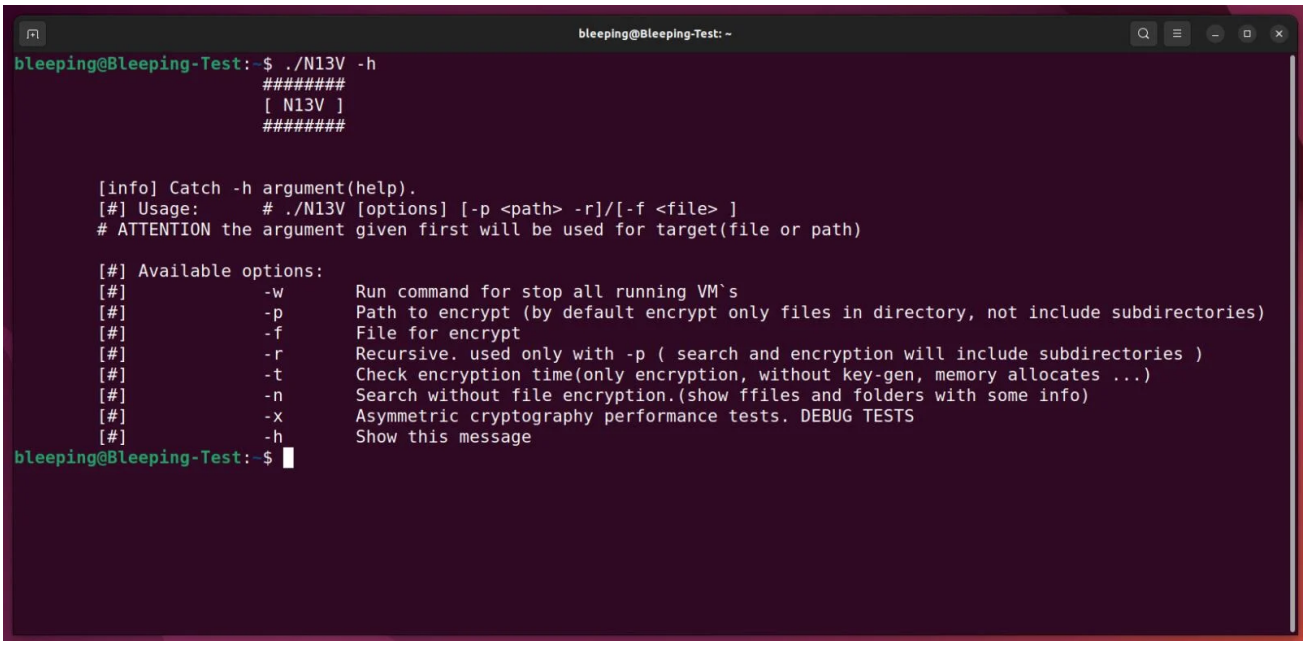
By
Lawrence Abrams

- July 5, 2022
- 06:20 PM
- 3

A new ransomware operation called RedAlert, or N13V, encrypts both Windows and Linux VMWare ESXi servers in attacks on corporate networks.

The new operation was discovered today by MalwareHunterTeam, who tweeted various images of the gang's data leak site.

The ransomware has been called 'RedAlert' based on a string used in the ransom note. However, from a Linux encryptor obtained by BleepingComputer, the threat actors call their operation 'N13V' internally, as shown below.



RedAlert / N13V ransomware command-line options

Source: BleepingComputer

The Linux encryptor is created to target VMware ESXi servers, with command-line options that allow the threat actors to shut down any running virtual machines before encrypting files.

The full list of command-line options can be seen below.

```
-w       Run command for stop all running VM`s
-p       Path to encrypt (by default encrypt only files in directory, not include
subdirectories)
-f       File for encrypt
-r       Recursive. used only with -p ( search and encryption will include
subdirectories )
-t       Check encryption time(only encryption, without key-gen, memory allocates
...)
-n       Search without file encryption.(show ffiles and folders with some info)
-x       Asymmetric cryptography performance tests. DEBUG TESTS
-h       Show this message
```

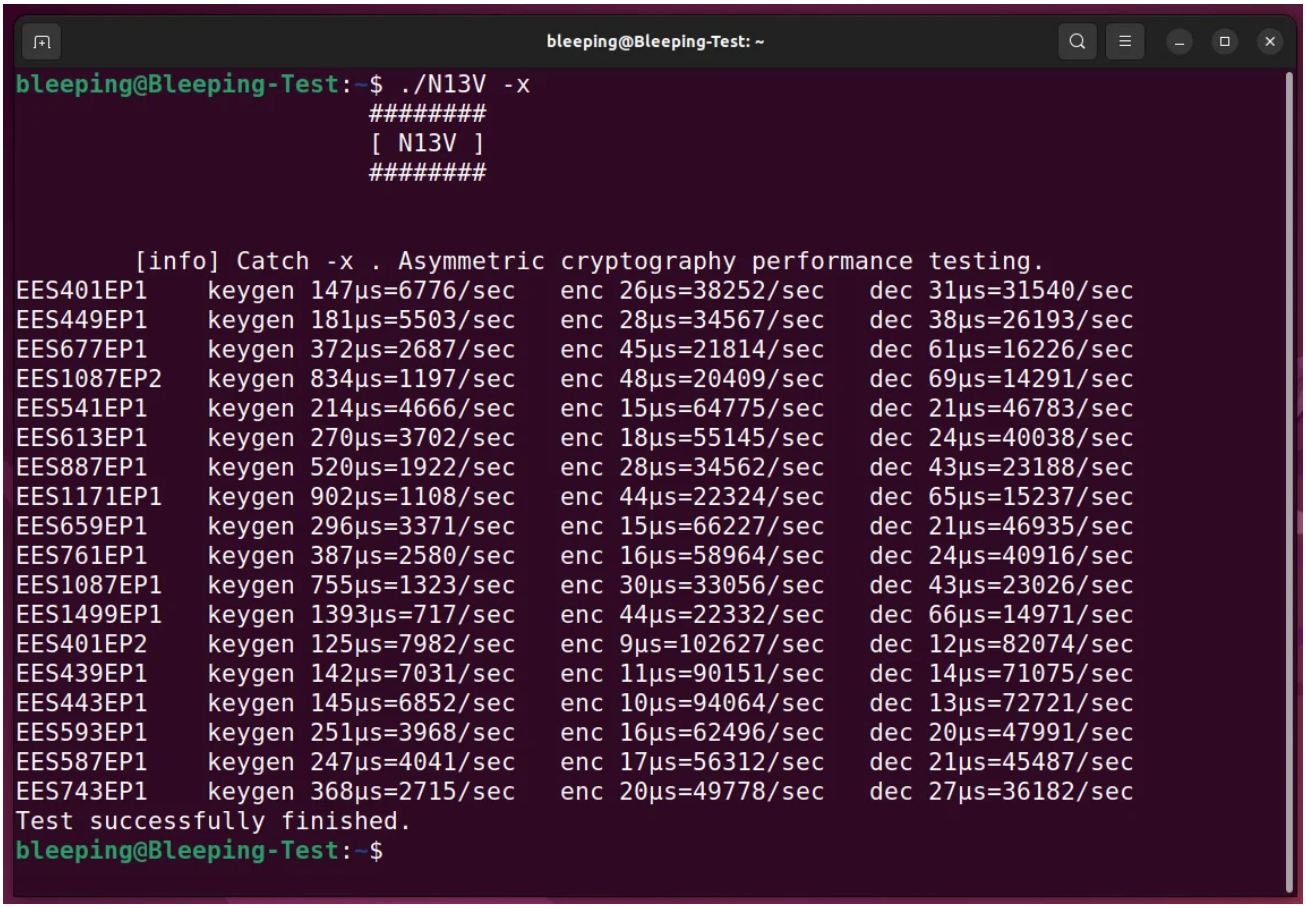
When running the ransomware with the '`-w`' argument, the Linux encryptor will shut down all running VMware ESXi virtual machines using the following esxcli command:

```
esxcli --formatter=csv --format-param=fields=="WorldID,DisplayName" vm process list
| tail -n +2 | awk -F $',' '{system("esxcli vm process kill --type=force --world-
id=" $1)}'
```

When encrypting files, the ransomware utilizes the NTRUEncrypt public-key encryption algorithm, which support various 'Parameter Sets' that offer different levels of security.

An interesting feature of RedAlert/N13V is the '-x' command-line option that performs 'asymmetric cryptography performance testing' using these different NTRUEncrypt parameter sets. However, it is unclear if there is a way to force a particular parameter set when encrypting and/or if the ransomware will select a more efficient one.

The only other ransomware operation known to use this encryption algorithm is FiveHands.



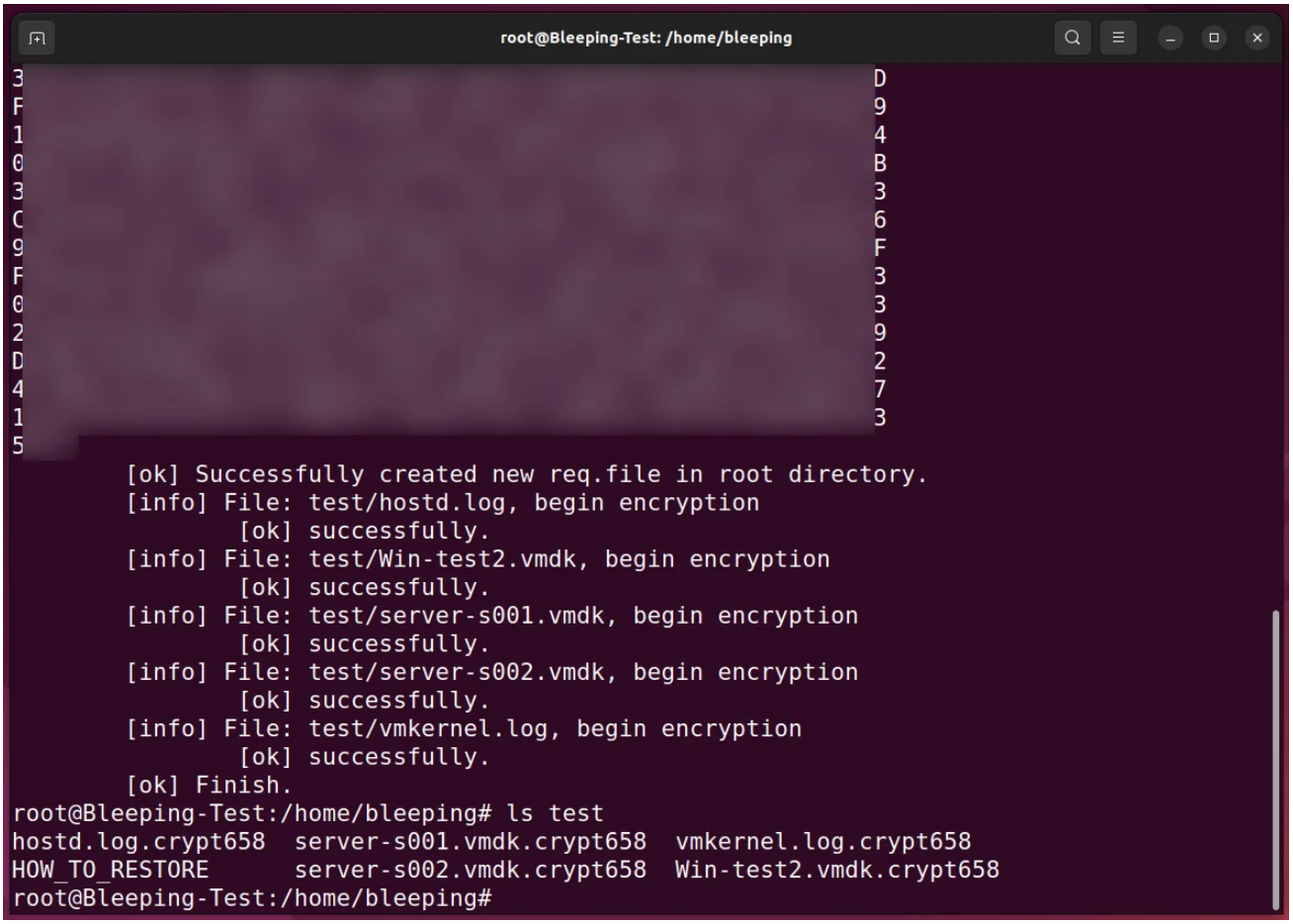
NTRUEncrypt encryption speed test

Source: BleepingComputer

When encrypting files, the ransomware will only target files associated with VMware ESXi virtual machines, including log files, swap files, virtual disks, and memory files, as listed below.

```
.log
.vmdk
.vmem
.vswp
.vmsn
```

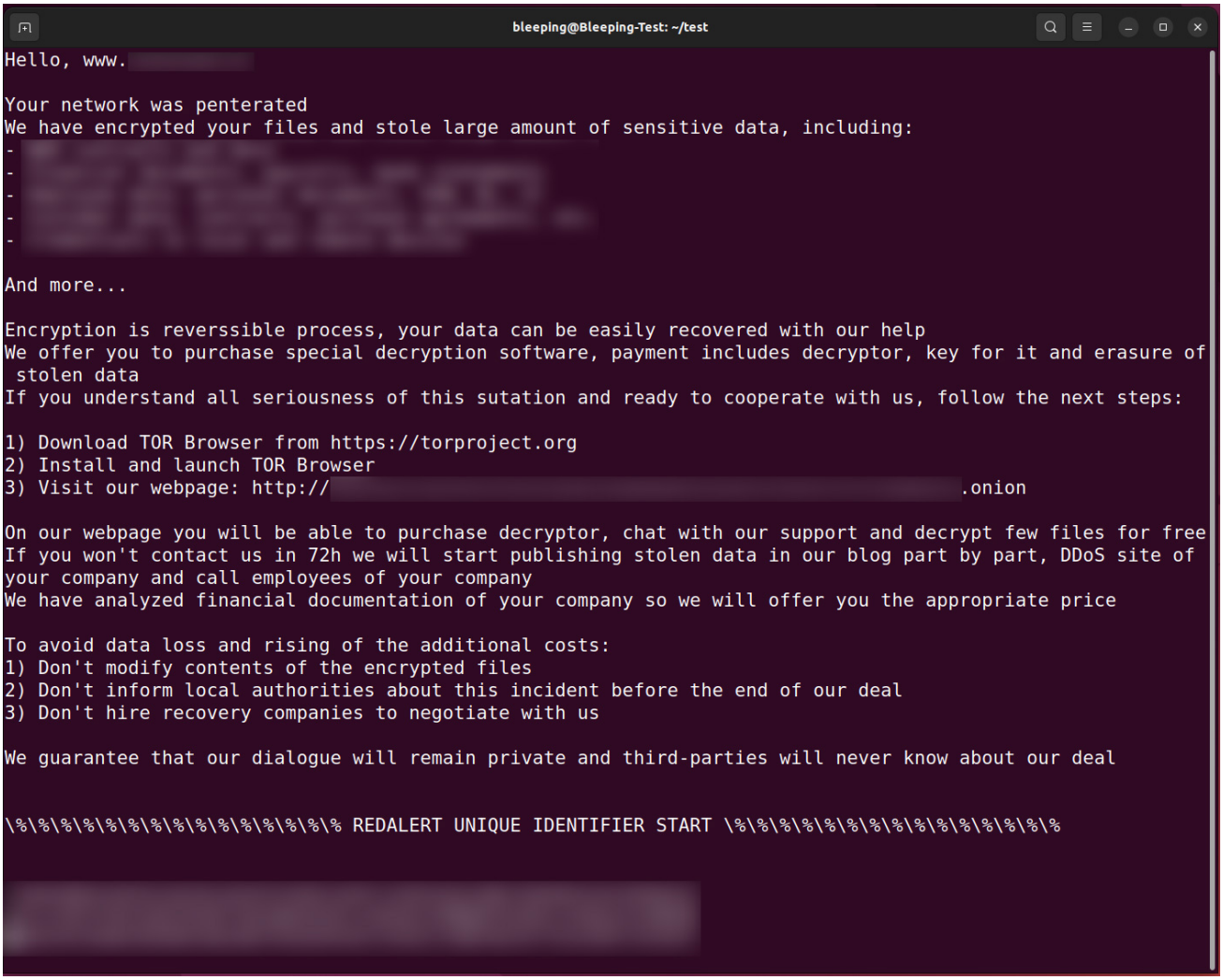
In the sample analyzed by BleepingComputer, the ransomware would encrypt these file types and append the **.crypt[number]** extension to the file names of encrypted files.



Encrypting files in Linux with RedAlert

Source: BleepingComputer

In each folder, the ransomware will also create a custom ransom note named **HOW_TO_RESTORE**, which contains a description of the stolen data and a link to a unique TOR ransom payment site for the victim.

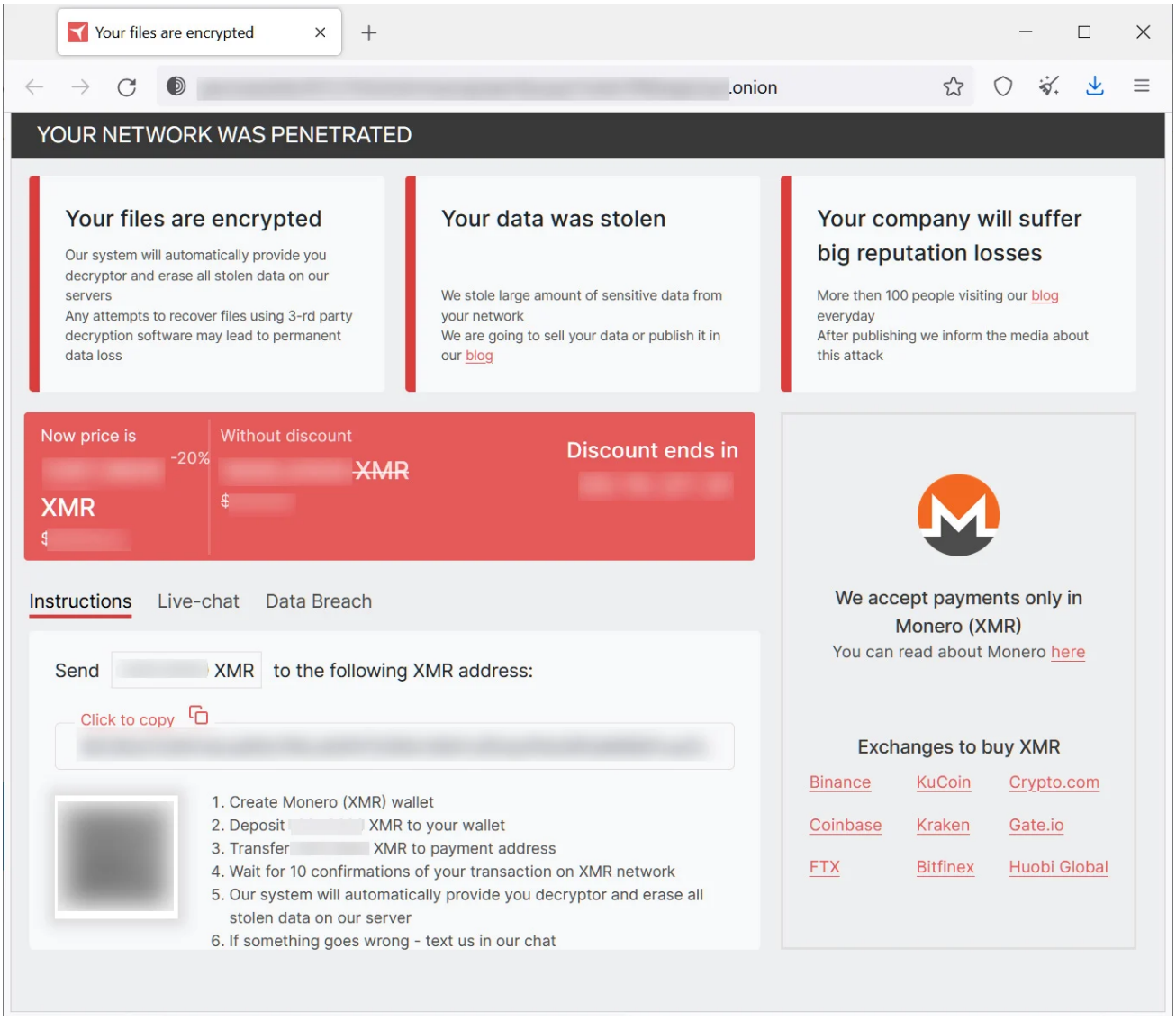


Red Alert / N13V ransom note

Source: BleepingComputer

The Tor payment site is similar to other ransomware operation sites as it displays the ransom demand and provides a way to negotiate with the threat actors.

However, RedAlert/N13V only accepts the Monero cryptocurrency for payment, which is not commonly sold in USA crypto exchanges because it is a privacy coin.



RedAlert / N13V Tor negotiation site

Source: BleepingComputer

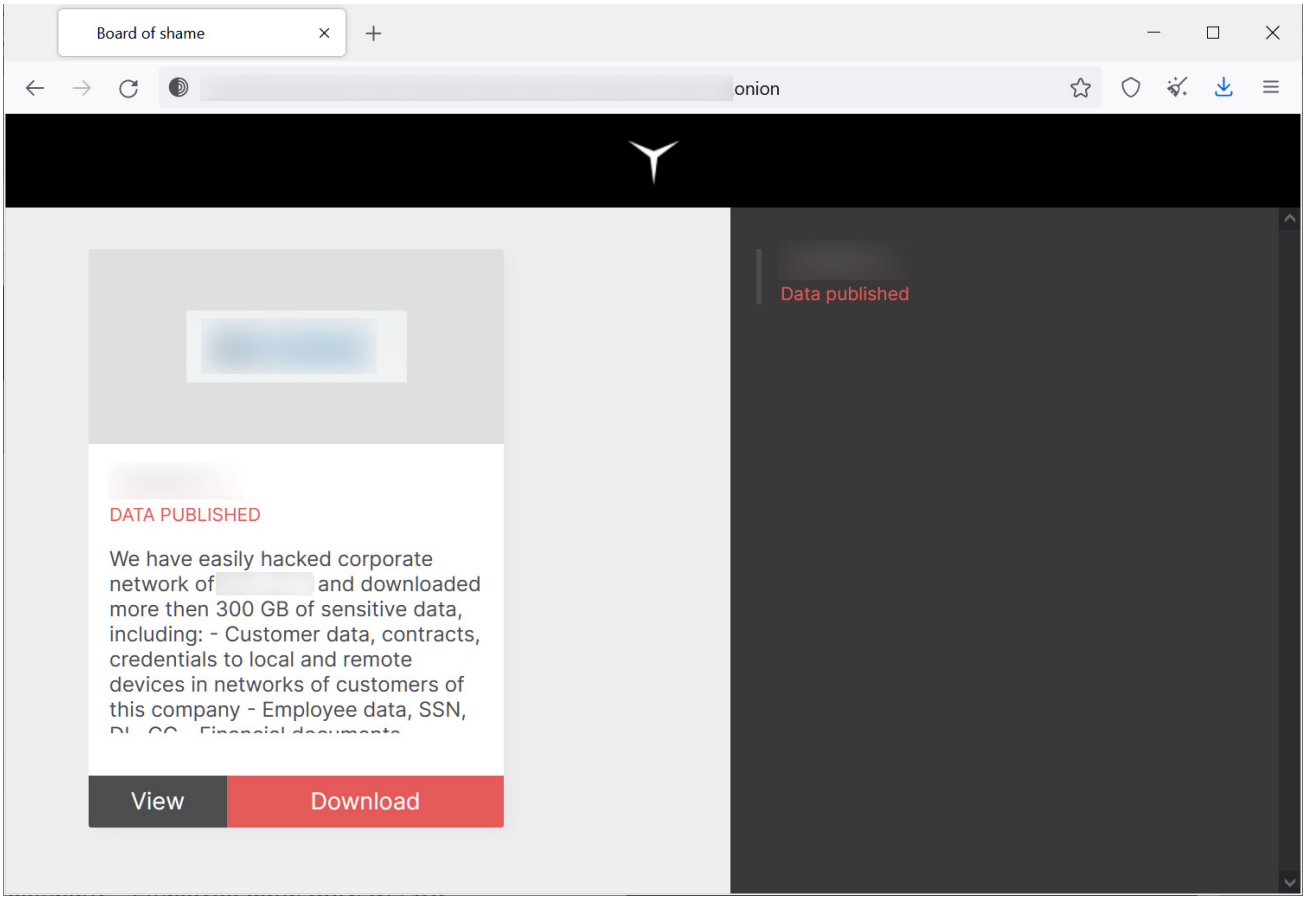
While only a Linux encryptor has been found, the payment site has hidden elements showing that Windows decryptors also exist.

"Board of Shame"

Like almost all new enterprise-targeting ransomware operations, RedAlert conducts double-extortion attacks, which is when data is stolen, and then ransomware is deployed to encrypt devices.

This tactic provides two extortion methods, allowing the threat actors to not only demand ransom to receive a decryptor but also demand one to prevent the leaking of stolen data.

When a victim does not pay a ransom demand, the RedAlert gang publishes stolen data on their data leak site that anyone can download.



RedAlert / N13V Data Leak Site

Source: BleepingComputer

Currently, the RedAlert data leak site only contains the data for one organization, indicating that the operation is very new.

While there has not been a lot of activity with the new N13V/RedAlert ransomware operation, it is one that we will definitely need to keep an eye on due to its advanced functionality and immediate support for both Linux and Windows.

Related Articles:

Microsoft Azure now has confidential VMs with ephemeral storage

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

Linux version of Black Basta ransomware targets VMware ESXi servers

New Windows Subsystem for Linux malware steals browser auth cookies

Malicious PyPI package opens backdoors on Windows, Linux, and Macs

- Linux
- N13V
- RedAlert

- Virtual Machine
- Vmware ESXi
- Windows

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

- 

  TsVk! - 1 week ago

  -
  -

  I'm surprised that more ransomware operators are not demanding Monero for payment.

- 

  Lawrence Abrams - 1 week ago

  -
  -

  Harder to get and more regulated due to it being a privacy coin.

- 

  TsVk! - 1 week ago

  -
  -

  Putting the onus on victims to do that leg work and find it seems like less work than trying to tumble or obscure the digital trail with Bitcoin though.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: