

New RedAlert Ransomware targets Windows, Linux VMware ESXi servers

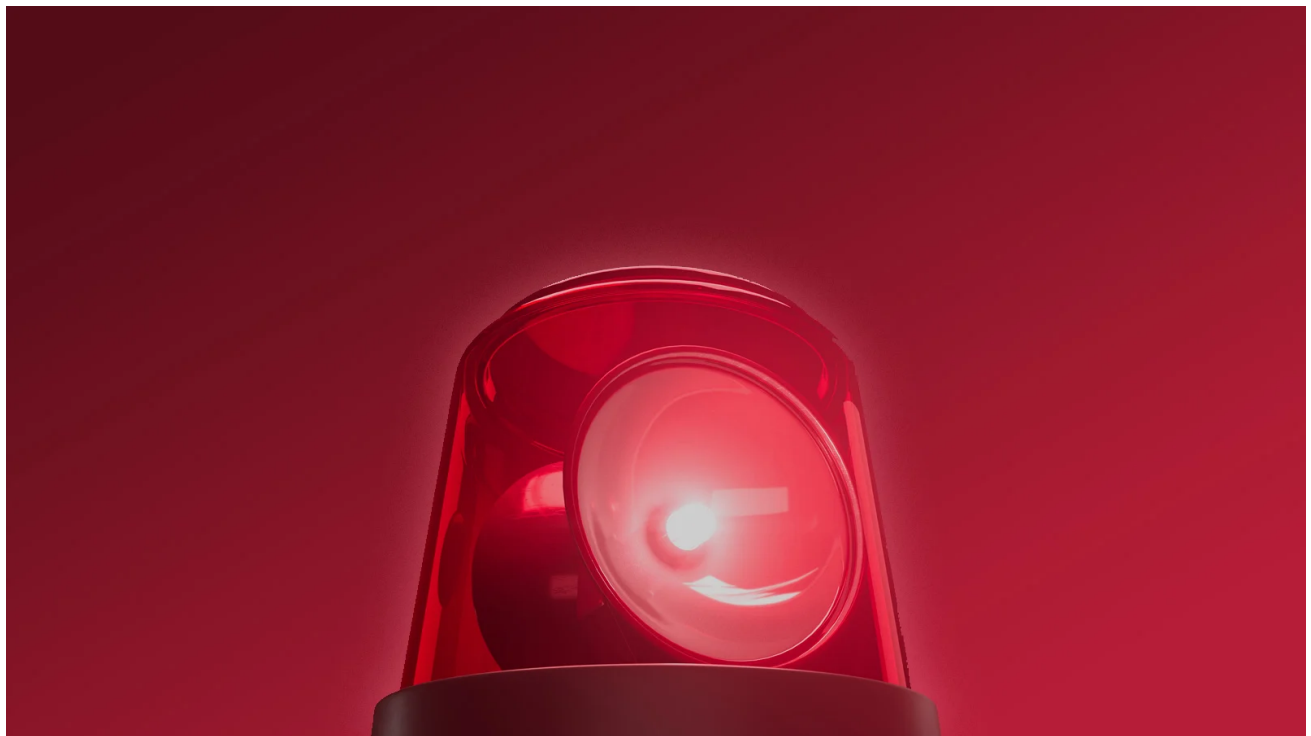
bleepingcomputer.com/news/security/new-redalert-ransomware-targets-windows-linux-vmware-esxi-servers/

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.

```
bleeping@Bleeping-Test: ~$ ./N13V -h
#####
[ N13V ]
#####

[info] Catch -h argument(help).
[#] Usage:      # ./N13V [options] [-p <path> -r]/[-f <file> ]
# ATTENTION the argument given first will be used for target(file or path)

[#] Available options:
[#]      -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
bleeping@Bleeping-Test: ~$
```

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](#).

```
bleeping@Bleeping-Test: ~  
bleeping@Bleeping-Test:~$ ./N13V -x  
#####  
[ N13V ]  
#####  
  
[info] Catch -x . Asymmetric cryptography performance testing.  
EES401EP1 keygen 147µs=6776/sec enc 26µs=38252/sec dec 31µs=31540/sec  
EES449EP1 keygen 181µs=5503/sec enc 28µs=34567/sec dec 38µs=26193/sec  
EES677EP1 keygen 372µs=2687/sec enc 45µs=21814/sec dec 61µs=16226/sec  
EES1087EP2 keygen 834µs=1197/sec enc 48µs=20409/sec dec 69µs=14291/sec  
EES541EP1 keygen 214µs=4666/sec enc 15µs=64775/sec dec 21µs=46783/sec  
EES613EP1 keygen 270µs=3702/sec enc 18µs=55145/sec dec 24µs=40038/sec  
EES887EP1 keygen 520µs=1922/sec enc 28µs=34562/sec dec 43µs=23188/sec  
EES1171EP1 keygen 902µs=1108/sec enc 44µs=22324/sec dec 65µs=15237/sec  
EES659EP1 keygen 296µs=3371/sec enc 15µs=66227/sec dec 21µs=46935/sec  
EES761EP1 keygen 387µs=2580/sec enc 16µs=58964/sec dec 24µs=40916/sec  
EES1087EP1 keygen 755µs=1323/sec enc 30µs=33056/sec dec 43µs=23026/sec  
EES1499EP1 keygen 1393µs=717/sec enc 44µs=22332/sec dec 66µs=14971/sec  
EES401EP2 keygen 125µs=7982/sec enc 9µs=102627/sec dec 12µs=82074/sec  
EES439EP1 keygen 142µs=7031/sec enc 11µs=90151/sec dec 14µs=71075/sec  
EES443EP1 keygen 145µs=6852/sec enc 10µs=94064/sec dec 13µs=72721/sec  
EES593EP1 keygen 251µs=3968/sec enc 16µs=62496/sec dec 20µs=47991/sec  
EES587EP1 keygen 247µs=4041/sec enc 17µs=56312/sec dec 21µs=45487/sec  
EES743EP1 keygen 368µs=2715/sec enc 20µs=49778/sec dec 27µs=36182/sec  
Test successfully finished.  
bleeping@Bleeping-Test:~$
```

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
```

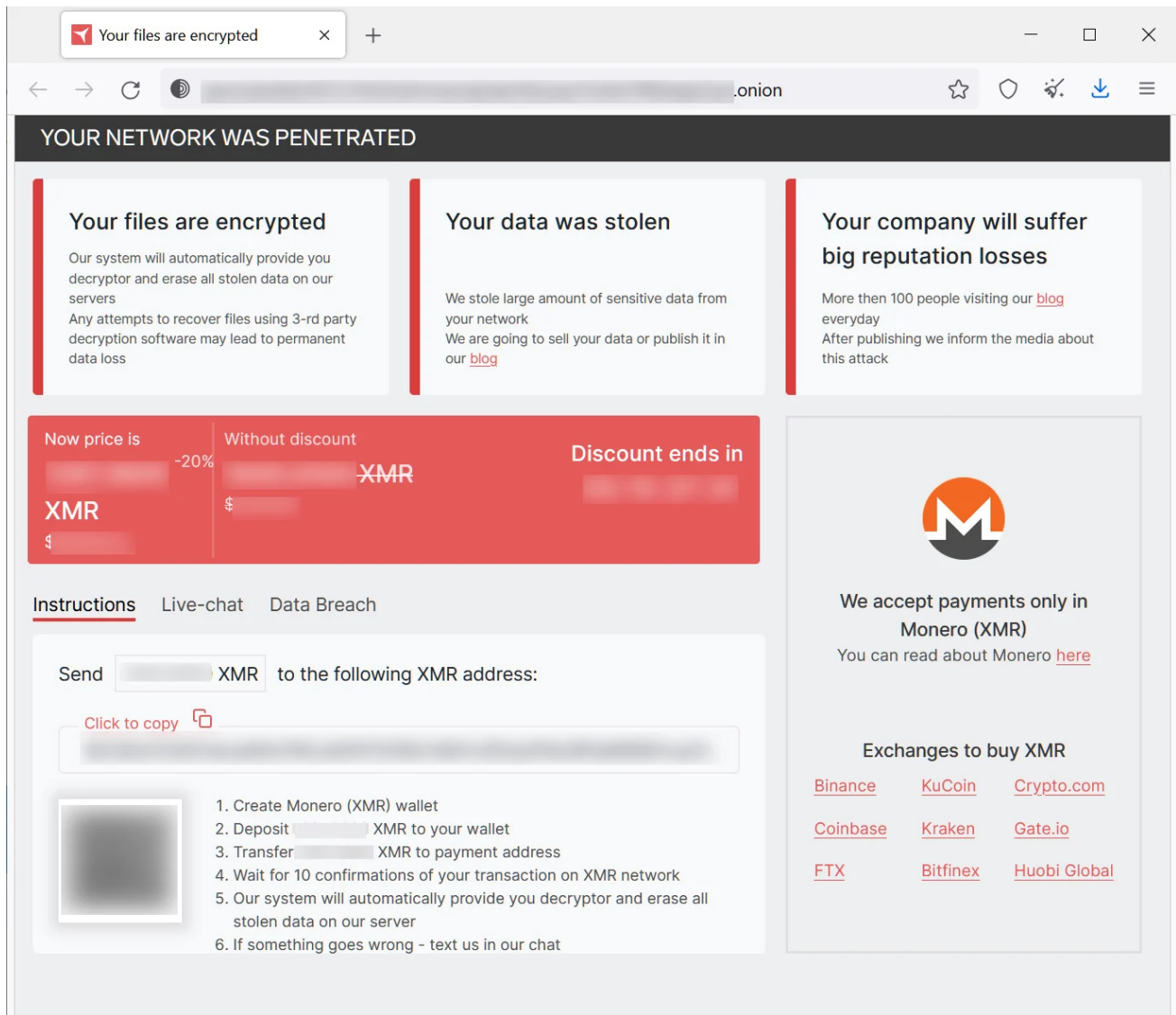
In the sample analyzed by BleepingComputer, the ransomware would encrypt these file types and append the **.crypt[number]** extension to the file names of encrypted files.

```
root@Bleeping-Test: /home/bleeping
3
F
1
0
3
C
9
F
0
2
D
4
1
5
D
9
4
B
3
6
F
3
3
9
2
7
3
[ok] Successfully created new req.file in root directory.
[info] File: test/hostd.log, begin encryption
      [ok] successfully.
[info] File: test/Win-test2.vmdk, begin encryption
      [ok] successfully.
[info] File: test/server-s001.vmdk, begin encryption
      [ok] successfully.
[info] File: test/server-s002.vmdk, begin encryption
      [ok] successfully.
[info] File: test/vmkernel.log, begin encryption
      [ok] successfully.
[ok] Finish.
root@Bleeping-Test:/home/bleeping# ls test
hostd.log.crypt658  server-s001.vmdk.crypt658  vmkernel.log.crypt658
HOW_TO_RESTORE     server-s002.vmdk.crypt658  Win-test2.vmdk.crypt658
root@Bleeping-Test:/home/bleeping#
```

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.



RedAlert / N13V Tor negotiation site

Source: *BleepingComputer*

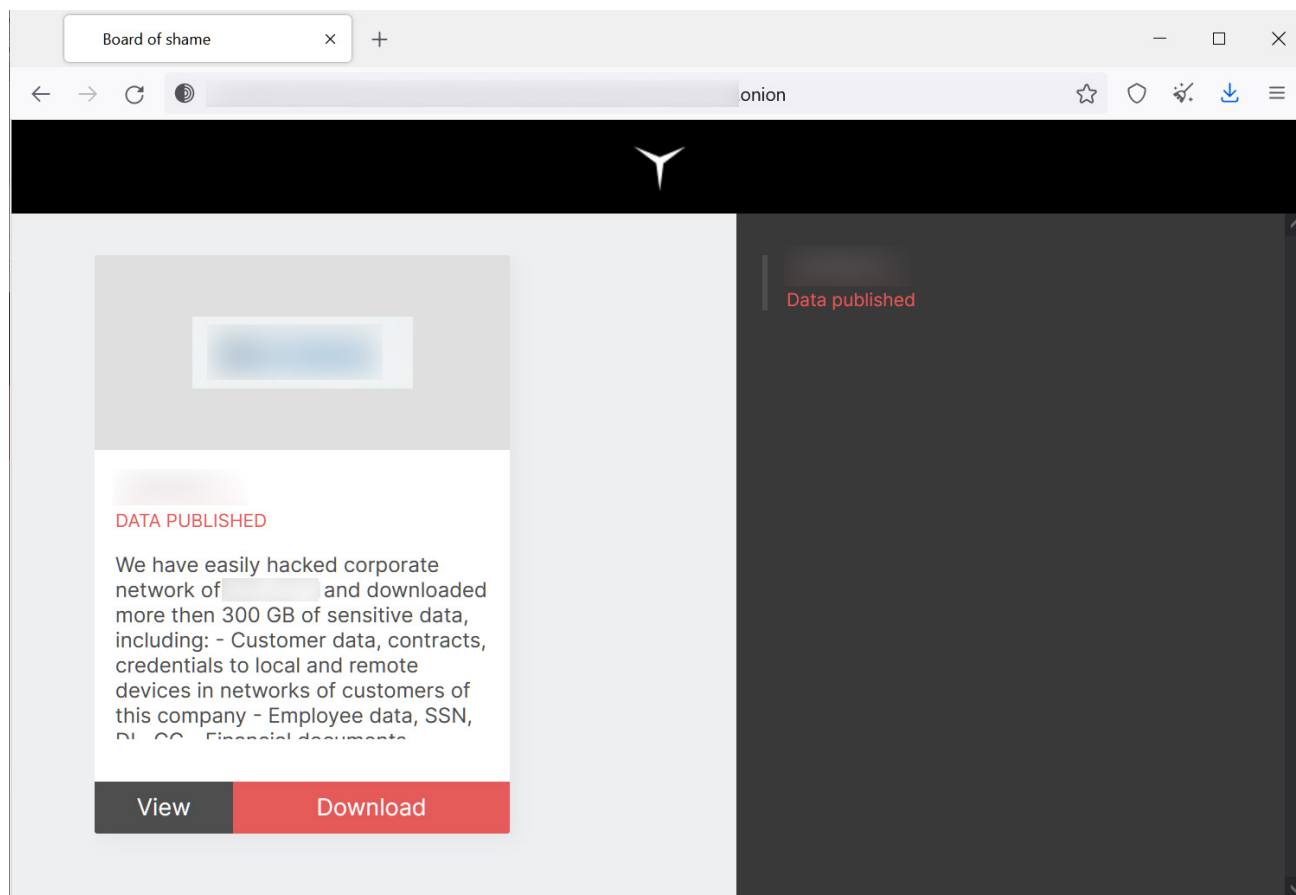
While only a Linux encryptor has been found, the payment site has hidden elements showing that Windows decryptors also exist.

"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



[TsVkl!](#) - 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:
