Rewterz Threat Alert – Financially Motivated Aggressive Group Carrying Out Ransomware Campaigns – Active IOCs

rewterz.com/rewterz-news/rewterz-threat-alert-financially-motivated-aggressive-group-carrying-out-ransomware-campaigns-active-iocs

May 3, 2021

- Solutions

- Resources

Resources

December 25, 2023

December 25, 2023

Rewterz Threat Update – Xfinity Data Leak Affects More Than 35 Million Users

Severity High Analysis Summary Comcast Cable Communications, operating as Xfinity, has reported a data breach impacting over 35 million individuals. Discovered during a routine cybersecurity exercise […]

December 25, 2023

December 25, 2023

[Rewterz Threat Alert – New Stealthy KV-Botnet Attacks Cisco, Fortinet, and DrayTek Devices – Active IOCs]

Severity High Analysis Summary A new bot made of firewalls and routers from Cisco, Fortinet, NETGEAR, and DrayTek has been discovered being used as a covert […]

December 25, 2023

December 25, 2023

Rewterz Threat Alert – GuLoader Malware’s Newest Anti-Analysis Techniques Uncovered by Researchers – Active IOCs

Severity High Analysis Summary Cybersecurity researchers unveiled the latest techniques used by a malware strain dubbed GuLoader. These continuous updates in GuLoader’s obfuscation techniques make it […]

Get in Touch

- Solutions

- Resources

Resources

December 25, 2023

December 25, 2023

Rewterz Threat Update – Xfinity Data Leak Affects More Than 35 Million Users

Severity High Analysis Summary Comcast Cable Communications, operating as Xfinity, has reported a data breach impacting over 35 million individuals. Discovered during a routine cybersecurity exercise […]

December 25, 2023

December 25, 2023

[Rewterz Threat Alert – New Stealthy KV-Botnet Attacks Cisco, Fortinet, and DrayTek Devices – Active IOCs]

Severity High Analysis Summary A new bot made of firewalls and routers from Cisco, Fortinet, NETGEAR, and DrayTek has been discovered being used as a covert […]

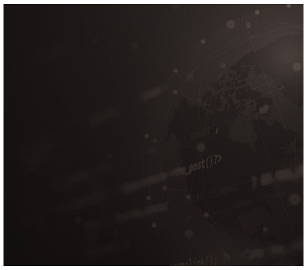
December 25, 2023

December 25, 2023

[Rewterz Threat Alert – GuLoader Malware’s Newest Anti-Analysis Techniques Uncovered by Researchers – Active IOCs]

Severity High Analysis Summary Cybersecurity researchers unveiled the latest techniques used by a malware strain dubbed GuLoader. These continuous updates in GuLoader’s obfuscation techniques make it […]

Get in Touch

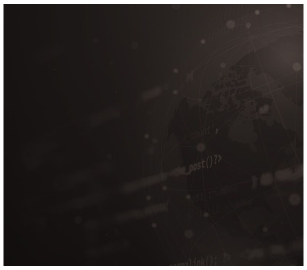


Rewterz Threat Advisory – CVE-2021-1223 – Multiple Cisco Products Snort HTTP Detection Engine File Policy Bypass Vulnerability

May 3, 2021

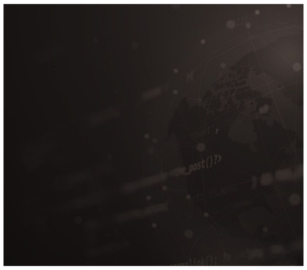
Rewterz Threat Alert – Kimsuky APT group – IOCs

May 3, 2021



Rewterz Threat Advisory – CVE-2021-1223 – Multiple Cisco Products Snort HTTP Detection Engine File Policy Bypass Vulnerability

May 3, 2021



Rewterz Threat Alert – Kimsuky APT group – IOCs

May 3, 2021

Severity

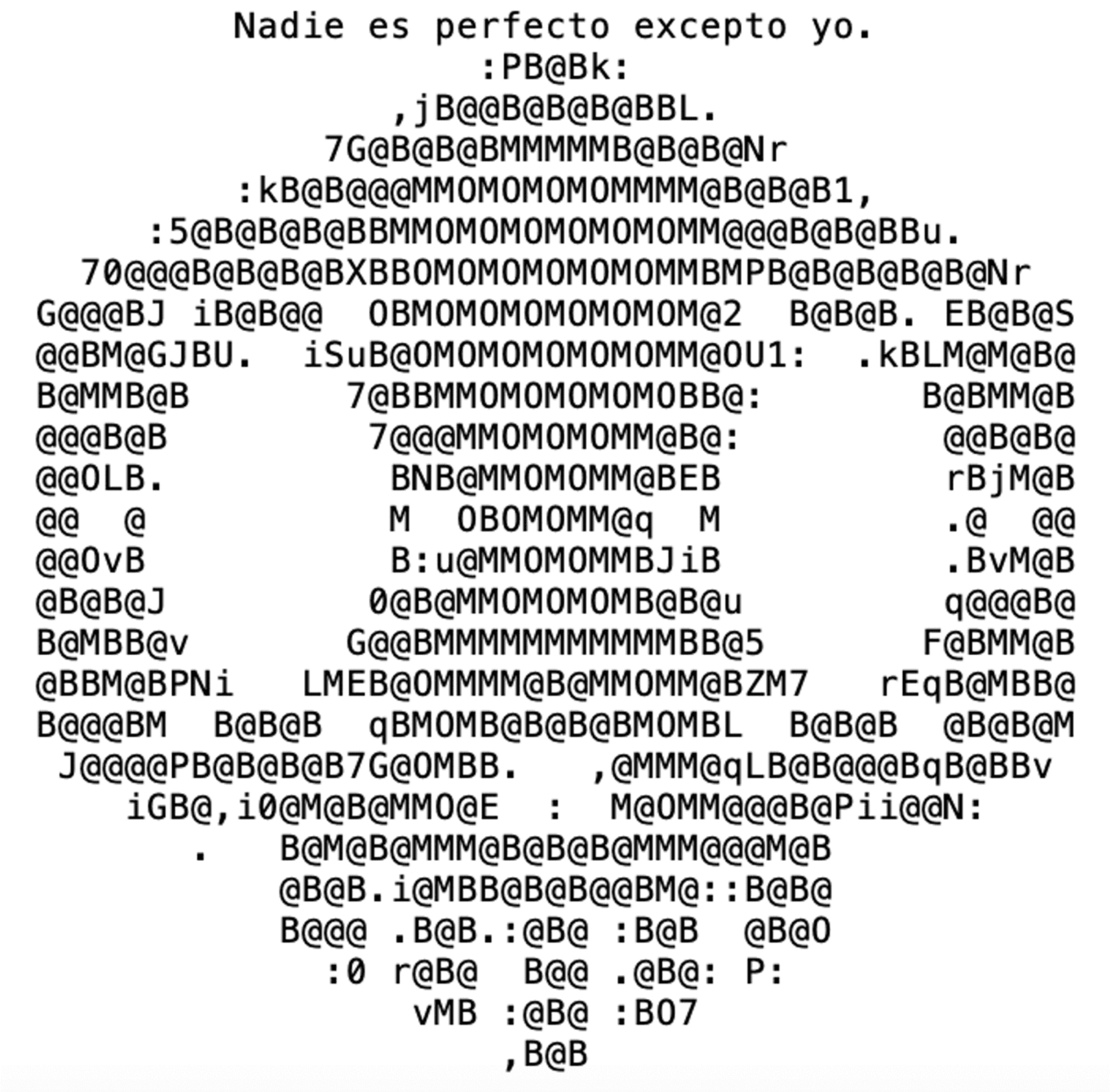
High

Analysis Summary

The group recognized as UNC2447 is found exploiting the SonicWall VPN zero-day vulnerability since a patch has not rolled out for the exploit yet. The malware being deployed was previously prevalent with the name “SOMBRAT.” SOMBRAT is being used for ransomware – which was not previously reported.

FIVEHANDS ransomware is first used by the group and later on the victims are extorted through media attention and data sale threats. The group targets organizations in Europe and North America. They have also displayed advanced capabilities of evading detection and minimize post-intrusion forensics.

UNC2447 was previously found using RAGNARLOCKER ransomware. HELLOKITTY and FIVEHANDS were used by the system and HELLOKITTY was being used from May 2020 to December 2020, and FIVEHANDS is being actively used since then.



```
         Nadie es perfecto excepto yo.
                    :PB@Bk:
                ,jB@@B@B@B@BBL.
             7G@B@B@BMMMMMB@B@B@Nr
         :kB@B@@@MMOMOMOMOMMMM@B@B@B1,
     :5@B@B@B@BBMMOMOMOMOMOMOMM@@@B@B@BBu.
  70@@@B@B@B@BXBBOMOMOMOMOMOMMBMPB@B@B@B@Nr
G@@@BJ iB@B@@  OBMOMOMOMOMOMOM@2  B@B@B. EB@B@S
@@BM@GJBU.  iSuB@OMOMOMOMOMOMM@OU1:  .kBLM@M@B@
B@MMB@B       7@BBMMOMOMOMOMOBB@:       B@BMM@B
@@@B@B         7@@@MMOMOMOMM@B@:         @@B@B@
@@OLB.          BNB@MMOMOMM@BEB          rBjM@B
@@  @           M  OBOMOMM@q  M          .@  @@
@@OvB           B:u@MMOMOMMBJiB          .BvM@B
@B@B@J         0@B@MMOMOMOMB@B@u         q@@@B@
B@MBB@v       G@@BMMMMMMMMMMBB@5        F@BMM@B
@BBM@BPNi   LMEB@OMMMM@B@MMOMM@BZM7   rEqB@MBB@
B@@@BM  B@B@B  qBMOMB@B@B@BMOMBL  B@B@B  @B@B@M
 J@@@@PB@B@B@B7G@OMBB.   ,@MMM@qLB@B@@@BqB@BBv
    iGB@,i0@M@B@MMO@E  :  M@OMM@@@B@Pii@@N:
       .   B@M@B@MMM@B@B@B@MMM@@@M@B
           @B@B.i@MBB@B@B@@BM@::B@B@
           B@@@ .B@B.:@B@ :B@B  @B@O
             :0 r@B@  B@@ .@B@: P:
                 vMB :@B@ :BO7
                     ,B@B
```

Impact

Files Encryption

Indicators of Compromise

Domain Name

- Cosarm[.]com
- Portalcos[.]com

MD5

- 87c78d62fd35bb25e34abb8f4caace4a
- 6382d48fae675084d30ccb69b4664cbb
- 39ea2394a6e6c39c5d7722dc996daf05
- f568229e696c0e82abb35ec73d162d5e
- 6c849920155f48d4b4aafce0fc49eb5b
- 22d35005e926fe29379cb07b810a6075
- 57824214710bc0cdb22463571a72afd0
- 87c0b190e3b4ab9214e10a2d1c182153
- 1b0b9e4cddcbcb02affe9c8124855e58
- 46ecc24ef6d20f3eaf71ff37610d57d1
- 1a79b6d169aac719c9323bc3ee4a8361
- a64d79eba40229ae9aaebbd73938b985

SHA-256

- 61e286c62e556ac79b01c17357176e58efb67d86c5d17407e128094c3151f7f9
- 99baffcd7a6b939b72c99af7c1e88523a50053ab966a079d9bf268aff884426e
- 61e286c62e556ac79b01c17357176e58efb67d86c5d17407e128094c3151f7f9
- 02a08b994265901a649f1bcf6772bc06df2eb51eb09906af9fd0f4a8103e9851
- c2498845ed4b287fd0f95528926c8ee620ef0cbb5b27865b2007d6379ffe4323
- dc007e71085297883ca68a919e37687427b7e6db0c24ca014c148f226d8dd98f
- 947e357bfdfe411be6c97af6559fd1cdc5c9d6f5cea122bf174d124ee03d2de8
- ef614b456ca4eaa8156a895f450577600ad41bd553b4512ae6abf3fb8b5eb04e
- bade05a30aba181ffbe4325c1ba6c76ef9e02cbe41a4190bd3671152c51c4a7b
- 52dace403e8f9b4f7ea20c0c3565fa11b6953b404a7d49d63af237a57b36fd2a
- a147945635d5bd0fa832c9b55bc3ebcea7a7787e8f89b98a44279f8eddda2a77
- 0e5f7737704c8f25b2b8157561be54a463057cd4d79c7e016c30a1cf6590a85c
- 7be901c5f7ffeb8f99e4f5813c259d0227335680380ed06df03fb836a041cb06

SHA1

- ffa5e945264288d4dec91d6871636f67624fd6ea
- 0b4aeaff91b347197310fcbd432e2fe06d583b57
- ca010ca1e7d5104049c09eefca128cc0e50729e1
- 71889fdf2d7616f366c38072ef3d24b021068ab8
- e8044ecd514574b71c353a9b640c8d6705a8051c
- a0181227dcb49b9417b468eeb38a2f8655553409

- dc8595989fc1bc784138b56cf32e8b194f425727
- 2c916c1c094e35577ca0b863168dee48991f1a2c
- 8fb41b6d5186cc996b4b92e812407a1adee8932f
- 2342cc02a5ac26fd78603ac82e2d90e1b54ff71f
- c4a1eb629133a63dbfc7bdae189bfa73168c260c
- e6e4f57df5c0db2aa0d64ca7b5fb65a4395e3b5f

Remediation

- Download and install the latest patches for browsers.
- Be vigilant while browsing the internet and do not open spam email.
- Beware of suspicious users and emails.