

Prometheus: An Emerging Ransomware Group Using Thanos Ransomware to Target Organizations

 blog.cyble.com/2021/06/05/prometheus-an-emerging-apt-group-using-thanos-ransomware-to-target-organizations/

June 5, 2021



During our regular threat hunting operations, the Cyble Research team found a blog on the darkweb, hosted by the Prometheus ransomware group. This blog is a clear indication of the fact that the group is back in action these days.

In the blog, the group has affiliated itself with the REvil ransomware group, as shown in Figure 1.



Figure 1: Prometheus Blog

Name	Value	Type
[309]	[0x00013E0B, "llo6KlgL2dyYW50EV2ZXJ5b25lOikYgLI QgLOMgLE="]	System.Collections.Generic.KeyValuePair<int, string>
[310]	[0x000102B1, "10"]	System.Collections.Generic.KeyValuePair<int, string>
[311]	[0x00001383, "docx"]	System.Collections.Generic.KeyValuePair<int, string>
[312]	[0x00002CB, ".pdf"]	System.Collections.Generic.KeyValuePair<int, string>
[313]	[0x0000043E7, ".xlsx"]	System.Collections.Generic.KeyValuePair<int, string>
[314]	[0x00000F88, ".csv"]	System.Collections.Generic.KeyValuePair<int, string>
[315]	[0x00000258, ".1"]	System.Collections.Generic.KeyValuePair<int, string>
[316]	[0x00013E48, "WU9VUuBDT01QQU5ZIE5FVfDPUksgSEFTIEFRU4gSEFD50V..."]	System.Collections.Generic.KeyValuePair<int, string>
[317]	[0x00013E89, "QWxslHvdXgaw1wb3JOYW50IGZpbGVzJGhhdmUgYmVlbi..."]	System.Collections.Generic.KeyValuePair<int, string>
[318]	[0x0000F1A0, "LOGONISOFF"]	System.Collections.Generic.KeyValuePair<int, string>
[319]	[0x00014297, "mystartup.lnk"]	System.Collections.Generic.KeyValuePair<int, string>
[320]	[0x000142AC, "VGhhbm92"]	System.Collections.Generic.KeyValuePair<int, string>
[321]	[0x000142B9, "Debug_Log.txt"]	System.Collections.Generic.KeyValuePair<int, string>
[322]	[0x000142CE, "UserName="]	System.Collections.Generic.KeyValuePair<int, string>
[323]	[0x000142D8, "_MachineName="]	System.Collections.Generic.KeyValuePair<int, string>
[324]	[0x000142FD, "."]	System.Collections.Generic.KeyValuePair<int, string>
[325]	[0x000148F1, "win32_processor"]	System.Collections.Generic.KeyValuePair<int, string>
[326]	[0x00014906, "processorD"]	System.Collections.Generic.KeyValuePair<int, string>
[327]	[0x000142F5, "..."]	System.Collections.Generic.KeyValuePair<int, string>
[328]	[0x000142FE, "[ID-"]	System.Collections.Generic.KeyValuePair<int, string>
[329]	[0x00014307, "..."]	System.Collections.Generic.KeyValuePair<int, string>
[330]	[0x00014308, "..."]	System.Collections.Generic.KeyValuePair<int, string>
[331]	[0x0001496C, "..."]	System.Collections.Generic.KeyValuePair<int, string>
[332]	[0x00015249, "aHR0cCBhbmFseXplciBzdGFuZC1hbG9uZQ=="]	System.Collections.Generic.KeyValuePair<int, string>
[333]	[0x0001527A, "ZmlkZGxlcg=="]	System.Collections.Generic.KeyValuePair<int, string>
[334]	[0x0001528B, "ZWZmZXRlY2ggYHR0cCBzbmlmZmVy"]	System.Collections.Generic.KeyValuePair<int, string>
[335]	[0x00015284, "ZmlyZXNoZWVw"]	System.Collections.Generic.KeyValuePair<int, string>
[336]	[0x000152C5, "SUWXYXJjaCBQcm9mZXNzaW9uYWw="]	System.Collections.Generic.KeyValuePair<int, string>
[337]	[0x000152EE, "ZmlyZXNoZWVw"]	System.Collections.Generic.KeyValuePair<int, string>

Figure 3: Strings Used for Selecting File Types.

After finding the base64 encoded strings we de-obfuscated them and observed that the strings were enumerated by the ransomware at the runtime to check the running processes, as shown in figure 4.

1	lsass.exe
2	svchst.exe
3	crccss.exe
4	chrome32.exe
5	firefox.exe
6	calc.exe
7	mysqld.exe
8	dllhst.exe
9	opera32.exe
10	memop.exe
11	spoolcv.exe
12	ctfmom.exe
13	SkypeApp.exe

Processes enumerated

Figure 4: Processes Enumerated by the Ransomware

Our observations also indicated that the ransomware started and stopped various services and programs after enumerating the processes. The services started are described in following table:

Services	Description
Dnscache	Used for client-side DNS resolution for faster DNS query.
FDRsePub	Makes computer and resources visible in the network.
SSDPSRV	Discovers networked devices.
upnphost	Discovering universal plug and play devices.

Table: Services Started by the Ransomware

The services started and stopped by the Prometheus ransomware are shown in Figure 5. The first 4 services are started by the ransomware, while the remaining are stopped.

```
14 start Dnscache /y
15 start FDResPub /y
16 start SSDPSRV /y
17 start upnphost /y
18 stop avpsus /y
19 stop McAfeeDLPAgentService /y
20 stop mfewc /y
21 stop BMR Boot Service /y
22 stop NetBackup BMR MFTFP Service /y
23 stop DefWatch /y
24 stop ccEvtMgr /y
25 stop ccSetMgr /y
26 stop SavRoam /y
27 stop RTVscan /y
28 stop QBFCService /y
29 stop QBIDPService /y
30 stop Intuit.QuickBooks.FCS /y
31 stop QBCFMonitorService /y
32 stop YooBackup /y
33 stop YooIT /y
34 stop zhudongfangyu /y
35 stop stc_raw_agent /y
36 stop VSNAPVSS /y
37 stop VeeamTransportSvc /y
38 stop VeeamDeploymentService /y
39 stop VeeamNFSSvc /y
40 stop veeam /y
41 stop PDVFSService /y
42 stop BackupExecVSSProvider /y
43 stop BackupExecAgentAccelerator /y
44 stop BackupExecAgentBrowser /y
45 stop BackupExecDiveciMediaService /y
46 stop BackupExecJobEngine /y
47 stop BackupExecManagementService /y
48 stop BackupExecRPCService /y
49 stop AcrSch2Svc /y
50 stop AcronisAgent /y
51 stop CASAD2DWebSvc /y
52 stop CAARCUUpdateSvc /y
53 stop sophos /y
```

Services Stopped

Figure 5: Services Started and Stopped by the Ransomware.

The ransomware stops several services that are critical for various purposes. This includes antivirus, system backup and restoring, database backup and restoring, and reporting tools. The purpose behind stopping the services is to block the backup and restoring operations, which has the potential to facilitate the data recovery in future. Figure 6 shows additional services which are terminated.

```

54 stop "Acronis VSS Provider" /y
55 stop MsDtsServer /y
56 stop IISAdmin /y
57 stop MExchangeES /y
58 stop "Sophos Agent" /y
59 stop EraserSvc11710 /y
60 stop "Enterprise Client Service" /y
61 stop "SQL Backups" /y
62 stop MsDtsServer100 /y
63 stop NetMsmqActivator /y
64 stop MExchangeIS /y
65 stop "Sophos AutoUpdate Service" /y
66 stop SamSs /y
67 stop ReportServer /y
68 stop "SQLsafe Backup Service" /y
69 stop MsDtsServer110 /y
70 stop POP3Svc /y
71 stop MExchangeMGMT /y
72 stop "Sophos Clean Service" /y
73 stop SMTPSvc /y
74 stop ReportServer$SQL_2008 /y
75 stop "SQLsafe Filter Service" /y
76 stop msftesql$PROD /y
77 stop SstpSvc /y
78 stop MExchangeMTA /y
79 stop "Sophos Device Control Service" /y
80 stop ReportServer$SYSTEM_BGC /y
81 stop "Symantec System Recovery" /y
82 stop MSOLAP$SQL_2008 /y
83 stop UIODetect /y
84 stop MExchangeSA /y
85 stop "Sophos File Scanner Service" /y
86 stop ReportServer$TPS /y
87 stop "Veeam Backup Catalog Data Service" /y
88 stop MSOLAP$SYSTEM_BGC /y
89 stop W3Svc /y
90 stop MExchangeSRS /y
91 stop "Sophos Health Service" /y
92 stop ReportServer$TPSAMA /y
93 stop "Zoolz 2 Service" /y
94 stop MSOLAP$TPS /y
95 stop "aphidmonitorservice" /y
96 stop msexchangeadtopology /y
97 stop "Sophos MCS Agent" /y

```

More Services Stopped

Figure 6: Additional Services Stopped

In addition to starting and stopping services, the Thanos ransomware also uses SC (Service Control) command to permanently change service configuration. Figure 7 shows the parameters passed to SC to permanently change shared network and device services.

```

230 config Dnscache start= auto
231 config FDResPub start= auto
232 config SSDPSRV start= auto
233 config upnphost start= auto
234 config SQLTELEMETRY start= disabled
235 config SQLTELEMETRY$ECWDB2 start= disabled
236 config SQLWriter start= disabled
237 config SstpSvc start= disabled

```

Configuration changed

Figure 7: SC Changing configuration.

The ransomware also terminates multiple processes running in the system for faster operation using taskkill.exe. As these programs are resource intensive and can lock the files targeted by the ransomware. Some of these programs are excel.exe, steam.exe,

sqlwriter.exe, thunderbird .exe, and msaccess.exe etc. The list of targeted programs is listed in Figure 8.

```
238 /IM mspub.exe /F
239 /IM mydesktopqos.exe /F
240 /IM mydesktopservice.exe /F
241 /IM mysqld.exe /F
242 /IM sqbcoreservice.exe /F
243 /IM firefoxconfig.exe /F
244 /IM agntsvc.exe /F
245 /IM thebat.exe /F
246 /IM steam.exe /F
247 /IM encsvc.exe /F
248 /IM excel.exe /F
249 /IM CNTAoSMgr.exe /F
250 /IM sqlwriter.exe /F
251 /IM tbirdconfig.exe /F
252 /IM dbeng50.exe /F
253 /IM thebat64.exe /F
254 /IM ocomm.exe /F
255 /IM infopath.exe /F
256 /IM mbamtray.exe /F
257 /IM zoolz.exe /F
258 /IM thunderbird.exe /F
259 /IM dbnmp.exe /F
260 /IM xfsvcon.exe /F
261 /IM Nrtscan.exe /F
262 /IM isqlplusvc.exe /F
263 /IM onenote.exe /F
264 /IM PccNTMon.exe /F
265 /IM msaccess.exe /F
266 /IM outlook.exe /F
267 /IM tmlisten.exe /F
268 /IM msftesql.exe /F
269 /IM powerpnt.exe /F
270 /IM visio.exe /F
271 /IM winword.exe /F
272 /IM mysqld-nt.exe /F
273 /IM wordpad.exe /F
274 /IM mysqld-opt.exe /F
275 /IM ocautoupds.exe /F
276 /IM ocspd.exe /F
277 /IM oracle.exe /F
```

Arguments Passed to taskkill.exe

Figure 8: Processes Terminated by taskkill.exe.

This variant of the Thanos ransomware checks for various security tools used by malware researchers for reversing the malware. These tools are listed below.

```

322  http analyzer stand-alone
323  fiddler
324  effetech http sniffer
325  firesheep
326  IEWatch Professional
327  dumpcap
328  wireshark
329  wireshark portable
330  sysinternals tcpview
331  NetworkMiner
332  NetworkTrafficView
333  HTTPNetworkSniffer
334  tcpdump
335  interceptor
336  Interceptor-NG
337  ollydbg
338  x64dbg
339  x32dbg
340  dnspy
341  dnspy-x86
342  de4dot
343  ilspy
344  dotpeek
345  dotpeek64
346  ida64
347  RDG Packer Detector
348  CFF Explorer
349  PEiD
350  protection_id
351  LordPE
352  pe-sieve
353  MegaDumper
354  UnConfuserEx
355  Universal_Fixer
356  NoFuserEx

```

decoded base64 strings
showing name of the tools

Figure 9: List of Security Tools

The Thanos ransomware uses an interesting technique for obfuscation. At runtime, it loads the reversed base64 encoded string containing the registry information, as shown in Figure 10.

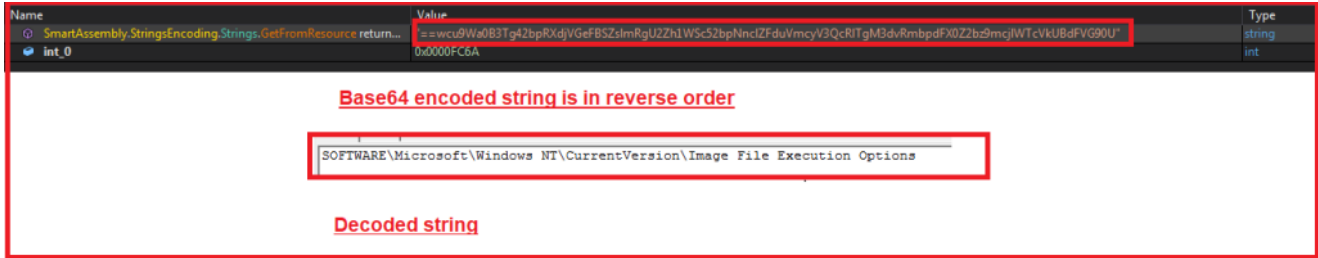


Figure 10: Obfuscation Used by the Ransomware

For network operations, the ransomware changes the Firewall rules to open various ports and allows outbound connection from other systems.

Figure 11 shows the registry entries for allowing inbound connections on various ports.


```

1554 KLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-UPnFHost-Out-TCP-NoScope: *v2.30|Action=Allow|Active=TRUE|Dir=Out|Protocol=TCP|Priority=1000
1555 KLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-NB_Name-In-UDP-NoScope: *v2.30|Action=Allow|Active=FALSE|Dir=In|Protocol=UDP|Priority=1000
1556 KLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-NB_Name-In-UDP-NoScope: *v2.30|Action=Allow|Active=TRUE|Dir=In|Protocol=UDP|Priority=1000
1557 KLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-NB_Name-Out-UDP-NoScope: *v2.30|Action=Allow|Active=FALSE|Dir=Out|Protocol=UDP|Priority=1000
1558 KLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-NB_Name-Out-UDP-NoScope: *v2.30|Action=Allow|Active=TRUE|Dir=Out|Protocol=UDP|Priority=1000
1559 KLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules\NETDIS-NB_Datagram-In-UDP-NoScope: *v2.30|Action=Allow|Active=FALSE|Dir=In|Protocol=UDP|Priority=1000

```

Ransomware changing firewall rules

Figure 11: Firewall Entries Edited.

The ransomware starts encryption after stopping all the backup and restoring services, disabling security software, and changing the network state. The modified sample of the Thanos ransomware uses the AES encryption technique, and after encrypting files, it appends a custom extension that is unique for every malware file, unlike most other ransomware that typically append extensions based on the system. Figure 12 shows the encrypted files with the extension.

jadx-gui-1.2.0-with-jre-win.zip.[LZG-ZNM-YDNM]	6/3/2021 1:27 AM	[LZG-ZNM-YDNM]	42,411 KB
pestudio.zip.[LZG-ZNM-YDNM]	6/3/2021 1:27 AM	[LZG-ZNM-YDNM]	957 KB
sample.bin.[LZG-ZNM-YDNM]	6/3/2021 1:27 AM	[LZG-ZNM-YDNM]	1,293 KB
sample.bin.zip.[LZG-ZNM-YDNM]	6/3/2021 1:27 AM	[LZG-ZNM-YDNM]	696 KB
027119161d11ba87acc908a1d284b93a6bcdfcc012e52ce390ecb9cd745bf27_ANY.RUN - Free Malware Sandbox Online.pdf.[LZG-ZNM-YDNM]	6/3/2021 1:27 AM	[LZG-ZNM-YDNM]	505 KB
bintext303.zip.[LZG-ZNM-YDNM]	6/3/2021 1:27 AM	[LZG-ZNM-YDNM]	17 KB
c04433797667c205da21d0b783bdbbbd6ba3ca3d62f43f6e7e911ccd09007cb_ANY.RUN - Free Malware Sandbox Online.pdf.[LZG-ZNM-YDNM]	6/3/2021 1:27 AM	[LZG-ZNM-YDNM]	497 KB
c04433797667c205da21d0b783bdbbbd6ba3ca3d62f43f6e7e911ccd09007cb.zip.[LZG-ZNM-YDNM]	6/3/2021 1:27 AM	[LZG-ZNM-YDNM]	269 KB
Reqsht-1.9.0.7;.[LZG-ZNM-YDNM]	6/3/2021 1:27 AM	[LZG-ZNM-YDNM]	156 KB

Figure 12: Encrypted Files

While encrypting the files, the ransomware drops the ransom file containing the ransom note in hta and text format. Figures 13 and 14 show the dropped files and the ransom note.

6066299859664896	6/3/2021 1:30 AM	File folder	
010 Editor.Ink.[LZG-ZNM-YDNM]	6/3/2021 1:27 AM	[LZG-ZNM-YDNM] File	2 KB
5973954394882048.zip.[LZG-ZNM-YDNM]	6/3/2021 1:27 AM	[LZG-ZNM-YDNM] File	3,648 KB
6066299859664896.zip.[LZG-ZNM-YDNM]	6/3/2021 1:27 AM	[LZG-ZNM-YDNM] File	129 KB
aaa.exe	4/26/2021 11:11 PM	Application	391 KB
RESTORE_FILES_INFO.hta	6/3/2021 1:30 AM	HTML Application	23 KB
RESTORE_FILES_INFO.txt	6/3/2021 1:30 AM	Text Document	4 KB

Figure 13: Dropping Ransom Note



YOUR COMPANY NETWORK HAS BEEN HACKED

All your important files have been encrypted!

Your files are safe! Only modified.(AES)
No software available on internet can help you.
We are the only ones able to decrypt your files.

We also gathered highly confidential/personal data.
These data are currently stored on a private server.
Files are also encrypted and stored securely.

As a result of working with us, you will receive:

- Fully automatic decryptor, all your data will be recovered within a few hours after itâ€™s installation.
 - Server with your data will be immediately destroyed after your payment.
 - Save time and continue working.

*You will can send us 2-3 non-important files and we will decrypt it
for free to prove we are able to give your files back.*

If you decide not to work with us:

- All data on your computers will remain encrypted forever.
 - **YOUR DATA ON OUR SERVER AND WE WILL RELEASE YOUR DATA TO PUBLIC OR RE-SELLER!**
So you can expect your data to be publicly available in the near future..
 - The price will increase over time.
-

It doesn't matter to us what you choose pay us or we will sell your data.
We only seek money and our goal is not to damage your reputation or prevent your business from running.
Write to us now and we will provide the best prices.

Instructions for contacting us:

- **You have way:**
- **1) Using a TOR browser!**
 - a. Download and install TOR browser from this site: <https://torproject.org/>
 - b. Open the Tor browser. Copy the link: <http://promethw27cbrcot.onion/ticket.php?track=LZG-ZNM-YDNM> and paste it in the Tor browser.
 - c. Start a chat and follow the further instructions.

Attention!

Any attempt to restore your files with third-party software will corrupt it.
Modify or rename files will result in a loose of data.
If you decide to try anyway, make copies before that

Figure 14: Ransomware Note

It is evident that more ransomware groups will emerge in the near future. Most of the time these groups use existing ransomware with slight modifications for evading detections. We recommend these best practices for ensuring the security of sensitive data in order to mitigate losses from ransomware attacks.

Indicators of Compromise (IoC):

Here's the list of sha256 of the files related to the recent Thanos ransomware attacks:

Sha256

779db1c725f71e54d4f31452763784abe783afa6a78cc222e17796b0045f33fc

a787997af509035b1e84f3cde7f8d62c1e02e8cc368fb95402783a0ed50f33f8

3605b9af44b153ef39a5bbe6d98ab8e6ef58b1f0f1c76eca4a3fb9b9a4042605

c2a01ef5115f2d41dff1b1a697d1d05b2b9532a70552473aab36d8e4dda7928

d662580e70711ba15f0bc65096a2298801ee7bc373ced3eb59582a637aeeb5fd

e9388ca092c87f310a159e03d3dd97b3ce79cd6cc642a7f3b057d0fa3dcde42c

5c66963cf7d417ffe475afdf18906df5c6dcd8dbbb1462918f197323dabb6f19

e15f9169021b5e11381547d57a952b98e06f6366161d56083ff9be69fc43e9bf

fdf8c15f27cfbf534cbc9771e3d4e42632a5993bb4b08f444111147ec540e273

c76825aeaa7960e44bda9786efbcb6e7865ef9f27fa6931e566aa44d88ad9cd

27ba35dbeb5324bd780ae6a95c5aae93fcb47c5aa8f48b1c21f83000a55de2da

785fdf2e6765a7b8870bd0b40d3e944536315604babfe30a7ca3466c02e411fe

779db1c725f71e54d4f31452763784abe783afa6a78cc222e17796b0045f33fc

2eb10ec6fa0d6d3f02a362ad5cbd55da6df47d23cfbacc3bc5a549e761cef7c8

b6f774f46949d54a060dabf2d7d08eef9fd390091f419ce1a2b555bcd58b2d32

e56cbdd422dda00fe75d80d0491195a3c42bade324ffebd913dcab29f741b9f6

0033c6e1db4b59f95b5261ecef244981e068c765f32616b26e23eddf99986454

e5211ef62f023a71cd5aa493f788198c2b97d6f79854f6e5f399893430e5ad0e

ef97bf49a9bd00a994143852590cc3a2d20227e510dc2b5968704d8f100b4d3c

8c723af5c826adea162ef3f2e37a1cca7b43d549c9a5fab7c9ff17f65eb5d8e7

9d9897d274e7a9ba3037d450dc6833c679e9ef8d125bd9d8b0329213df45b9e3

9d85a74f073c4403e3a91017b6757e0368139e672498a2f84f5efaad0d1b573b

ba6fbc352cc9a89771ca33901729dff8d1181a76f711ab74a61fb35df3bf8a19

1d4db8733c5f11ee8fca530aeb4a91069de04b1af64cbe1fa3ae2d3572a6e554

1c4b55fefcd78623a6724bb6c7779d0ef02ac20a6069cb9dbd91d753386606bb

48be948c3345e8c8b10c612a88eeee6bd1bf8af076092cf88268a268e889e698

1136907e76399f1d76694ee9c540b387ed6a5b12340b60f3fabfc183bca457df

714f630043670cdab4475971a255d836a1366e417cd0b60053bf026551d62409

a0e20c580e8a82f4103af90d290f762bd847fadd4eba1f5cd90e465bb9f810b7

e1c46a96effc5df063cea2fae83306ae1f0e2f898b0d2ada86c48052be5fe8d3

20d9efe472c01a0a23c9764db679b27a4b6a4d72e697e3508e44f218b8b952f5

aa3e530d4567c1511126029fac0562ba8aa4ead0a01aceea169ade3e38a37ea7

83e2ba9faf075547be65d2b6dbd13e190a0b1c1cf626788cb756ab7a3c770dcb

4e747c7024d9a76e22a31d38aee9408749023fc65b917c6d9ac05dd3afc3f36f

9e573ba20b55f6149d801491c0ebb51c9f1c954b956a2f6cea6f18af68f0164b

6e016c4d1db409b5e499289f31bcb6b87b5c46b29d4fcb4a50a7b68d733b93e

8b55f596d8179b043f050f42bc7c079d07be918fe321805aff1a00f88dd8f06d

b9acf82471bc22c7ce444684759d7506d407286989141028a2621a0b0f535094

ea55c78b15e2045f26ea39db122acb9a5cca84ba97625f444054f3efa331b386

113230f881d7008fad3d62e34ce79f1b9273f604303f1b5c1450cff6481655de

a88db6dc88a37a79056f466c6e0878569715409c5387be4947789cc924a97b92

3caa5163083177d40dd9ec2c3b84d0b37c82e2ee9807a50338af89f132a354d9

5d40615701c48a122e44f831e7c8643d07765629a83b15d090587f469c77693d

0cfed709f1954141a3c5a363e4e95d7e5b546ef310cfb9a63f0ca20ccc6ed152

2033194ab3c2602eb9d3b31eeb5432514c423eac213f1219e5865dfec371ed58

a5a544ef213bc2e02937fa7e0967a4b6ba926b9f5b3485dd108e232521155bf7

5fb35d559259cd85537265346901bb52083090489266608cef0a1c85de214aed

ad6b792c1e886156cd81586205a81aa92b9f256bd57cbcc527d194ae3f1b53d0

52f7f9e8369a3e89899d40e89766c9642b137b25bfd58a2b564dac67a40445f3

899f48bad035165acf8869af63922619f8a901bbeb8a7fc13919ba90dd9e7768

2d3d1b83067859ebb118ff1a99ac098806b65f566df094fad9a4debef4da911d

f4773540eb06fbde9a23f03424b3722999d0e6efabf5009c94c1bb0911626ada

b3b1cfa71b1cc572dace69e0996d537f41632ec4bab5b1f376d66aa765928b5f

67c29db79904510822a97c5e887606676c5cf77f5c31d60420d1d0ce9403daa3

8d268be58a27d2c980b807ffe703ea28b0fd0cd1ba2e455902faebe9ec17c52e

d7f7ea6cb92e1f01e815007fdcdf2455680e739077aff7e3eaf51311cf3388a5

5eedadeabe3b12131cdbc04c7af3927bd3d09add1d0725bce5db024d5102fb96

02665fcf9c0ddfb2cd3e04d254f60c5a4453947f7c3df5480316a040c0c8686f

Organizations should implement the following best practices to strengthen the security posture of their organization's systems.

- Check for instances of standard executables executing with the hash of another process.
- Implement multi-factor authentication (MFA), especially for privileged accounts.
- Use separate administrative accounts on different administration workstations.
- Employ Local Administrator Password Solution (LAPS).
- Allow the least privilege to employees on data access.
- Use MFA to secure Remote Desktop Protocol (RDP) and "jump boxes" for access.
- Secure your endpoints by deploying and maintaining endpoint defense tools.
- Always keep all software up-to-date.
- Keep antivirus signatures and engines up-to-date.
- Avoid adding users to the local administrators' group unless required.
- Implement a strong password policy and enforce regular password changes.
- Configure a personal firewall on organization workstations to deny unwanted connection requests.
- Deactivate unnecessary services on organization workstations and servers.

About Cyble

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the darkweb. Cyble's prime focus is to provide organizations with real-time visibility into their digital risk footprint. Backed by Y Combinator as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Startups To Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com.