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.

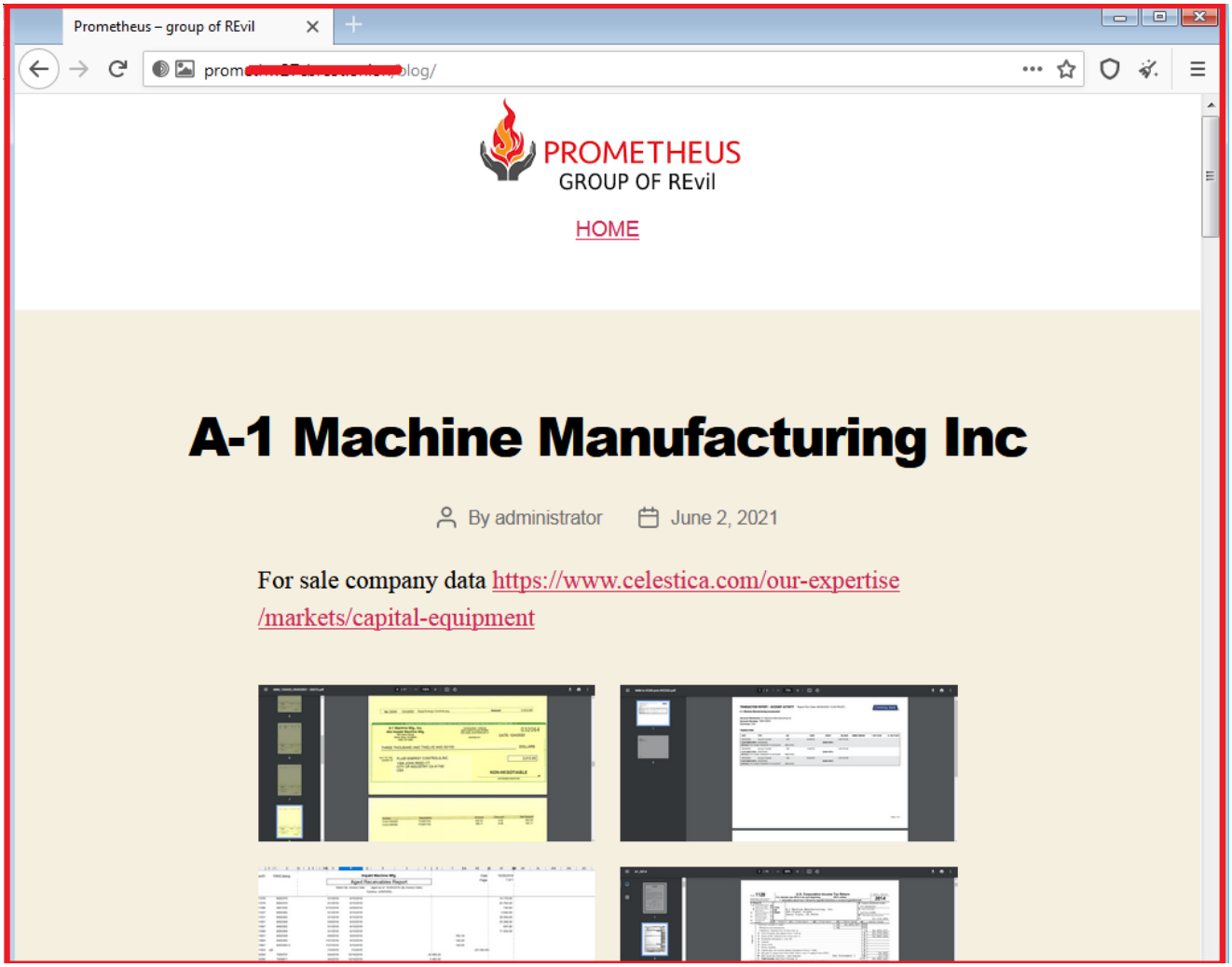

Figure 1: Prometheus Blog

Based on our research, Cyble researchers have found a sample of the Thanos ransomware being used by the Prometheus group for a recent ransomware attack. The technical analysis we have performed on the file has been shared below:

TECHNICAL ANALYSIS:

The Thanos ransomware is a 32-bit .NET executable file that is highly obfuscated. On decompiling it, we saw that the file has non-readable codes that made it difficult to reverse the file. We used a de-obfuscation tool to read the contents of the file, but complete code was not de-obfuscated. While decompiling, we also found a data object that contained a list of base64 encoded strings and several other plain strings. These strings helped us check the possible activities performed by the ransomware.

Figure 2 shows the list of base64 encoded strings.

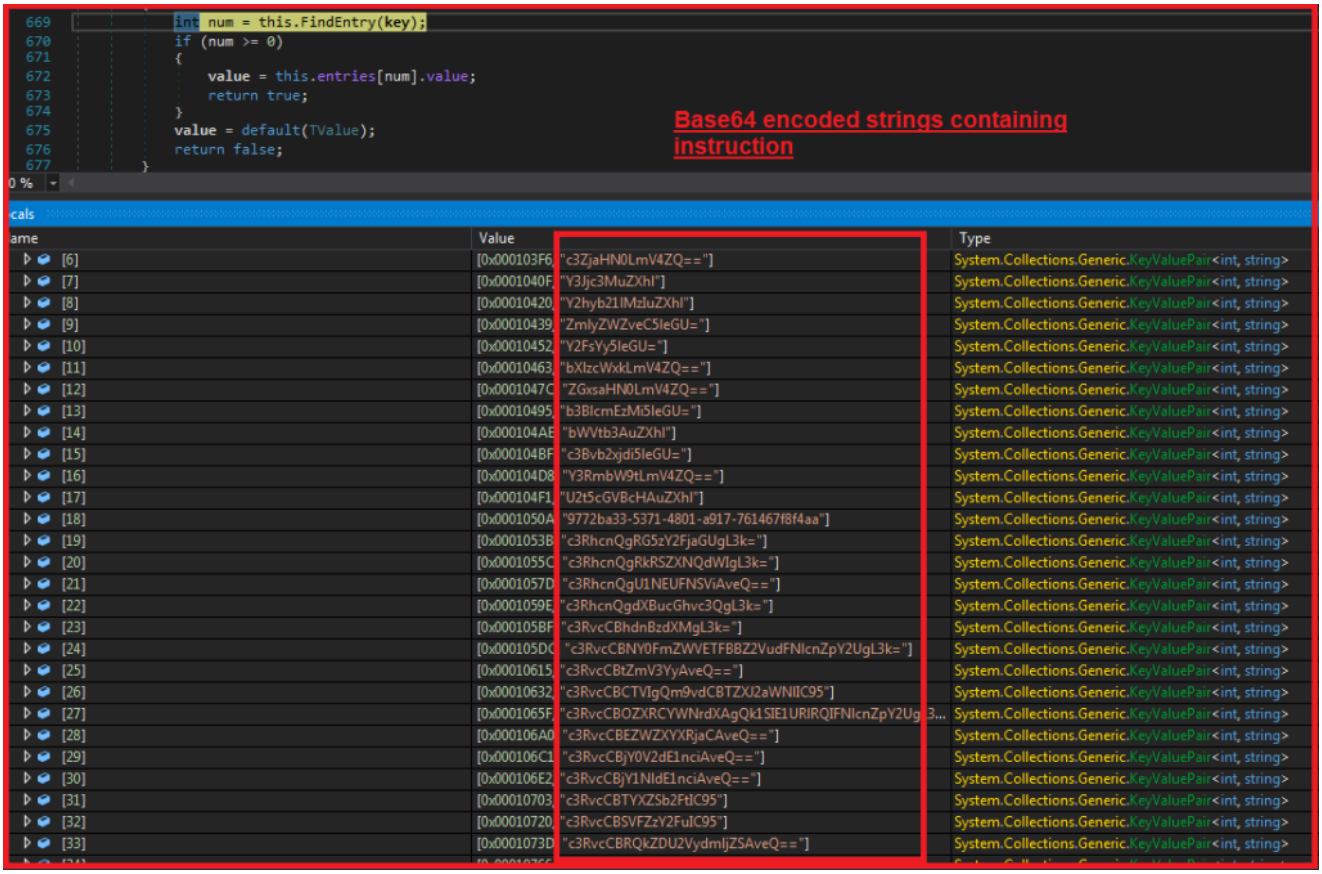

Figure 2: Base64 Encoded Strings

Apart from the base64 encoded strings, the modified
Thanos ransomware sample contained additional interesting strings related to document file extensions, link file name for persistence, system information, and extensions of various database files. On running the program, we found that only document files and database file extensions are being encrypted by the ransomware. Figure 3 shows the additional types and extracted information for selecting filetypes for encryption.

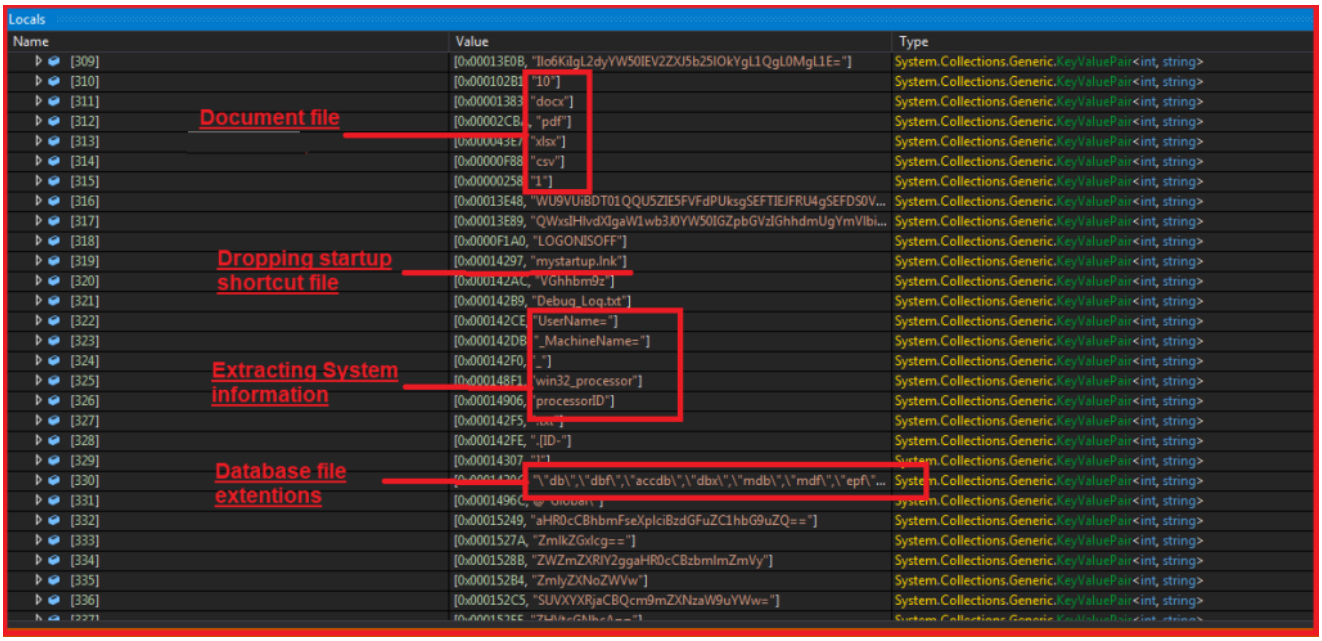

Figure 3: Strings Used for Selecting File Types.

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.

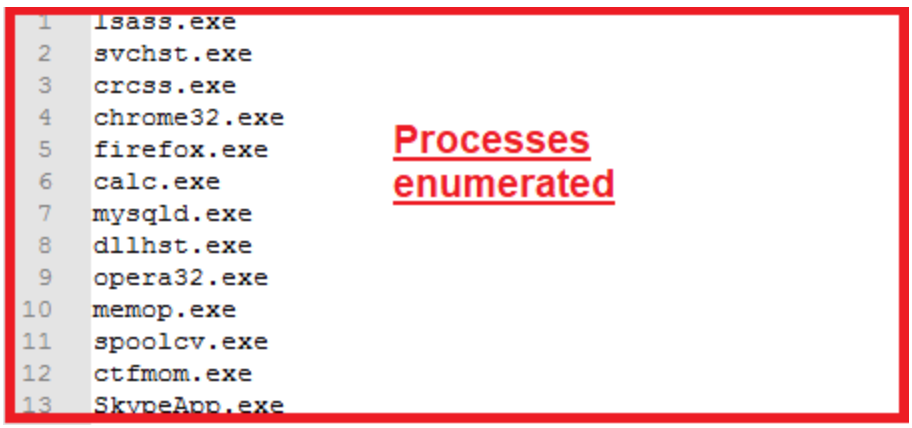

Figure 4: Processes Enumerated by the Ransomware

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.

```
start Dnscache /y
start FDResPub /y
start SSDPSRV /y
start upnphost /y
stop avpsus /y
stop McAfeeDLPAgentService /y
stop mfewc /y
stop BMR Boot Service /y
stop NetBackup BMR MTFTP Service /y
stop DefWatch /y
stop ccEvtMgr /y
stop ccSetMgr /y
stop SavRoam /y
stop RTVscan /y
stop QBFCService /y
stop QBIDPService /y
stop Intuit.QuickBooks.FCS /y
stop QBCFMonitorService /y
stop YooBackup /y
stop YooIT /y
stop zhudongfangyu /y
stop stc_raw_agent /y
stop VSNAPVSS /y
stop VeeamTransportSvc /y
stop VeeamDeploymentService /y
stop VeeamNFSSvc /y
stop veeam /y
stop PDVFSService /y
stop BackupExecVSSProvider /y
stop BackupExecAgentAccelerator /y
stop BackupExecAgentBrowser /y
stop BackupExecDiveciMediaService /y
stop BackupExecJobEngine /y
stop BackupExecManagementService /y
stop BackupExecRPCService /y
stop AcrSch2Svc /y
stop AcronisAgent /y
stop CASAD2DWebSvc /y
stop CAARCUpdateSvc /y
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.

```
stop "Acronis VSS Provider" /y
stop MsDtsServer /y
stop IISAdmin /y
stop MSExchangeES /y
stop "Sophos Agent" /y
stop EraserSvc11710 /y
stop "Enterprise Client Service" /y
stop "SQL Backups /y
stop MsDtsServer100 /y
stop NetMsmqActivator /y
stop MSExchangeIS /y
stop "Sophos AutoUpdate Service" /y
stop SamSs /y
stop ReportServer /y
stop "SQLsafe Backup Service" /y
stop MsDtsServer110 /y
stop POP3Svc /y
stop MSExchangeMGMT /y
stop "Sophos Clean Service" /y
stop SMTPSvc /y
stop ReportServer$SQL_2008 /y
stop "SQLsafe Filter Service" /y
stop msftesql$PROD /y
stop SstpSvc /y
stop MSExchangeMTA /y
stop "Sophos Device Control Service" /y
stop ReportServer$SYSTEM_BGC /y
stop "Symantec System Recovery" /y
stop MSOLAP$SQL_2008 /y
stop UI0Detect /y
stop MSExchangeSA /y
stop "Sophos File Scanner Service" /y
stop ReportServer$TPS /y
stop "Veeam Backup Catalog Data Service" /y
stop MSOLAP$SYSTEM_BGC /y
stop W3Svc /y
stop MSExchangeSRS /y
stop "Sophos Health Service" /y
stop ReportServer$TPSAMA /y
stop "Zoolz 2 Service" /y
stop MSOLAP$TPS /y
stop "aphidmonitorservice" /y
stop msexchangeadtopology /y
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.

```
config Dnscache start= auto
config FDResPub start= auto
config SSDPSRV start= auto
config upnphost start= auto
config SQLTELEMETRY start= disabled
config SQLTELEMETRY$ECWDB2 start= disabled
config SQLWriter start= disabled
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 flies 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.

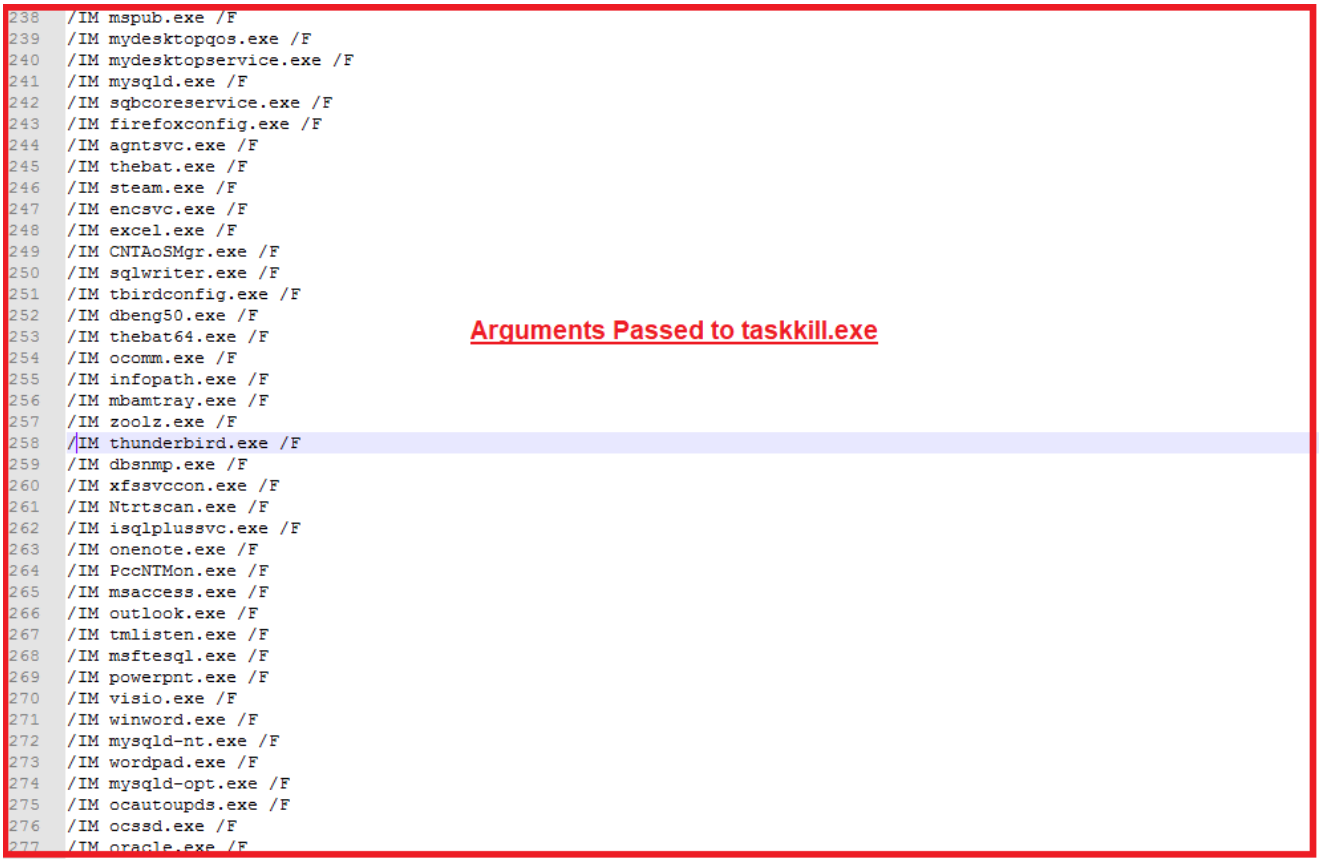

Figure 8: Processes Terminated by taskkill.exe.

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

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.

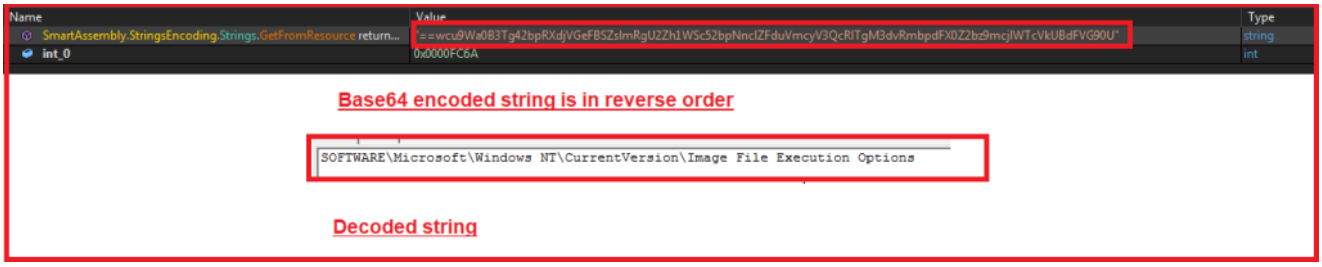

Figure 10: Obfuscation Used by the Ransomware

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.

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.

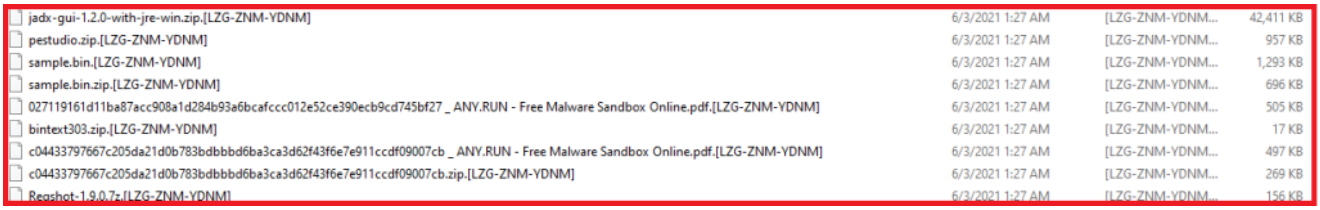

Figure 12: Encrypted Files

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.

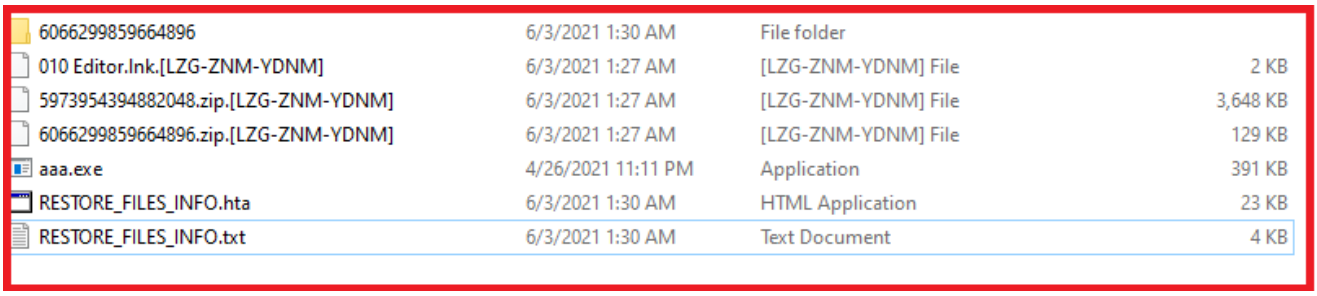

Figure 13: Dropping Ransom Note

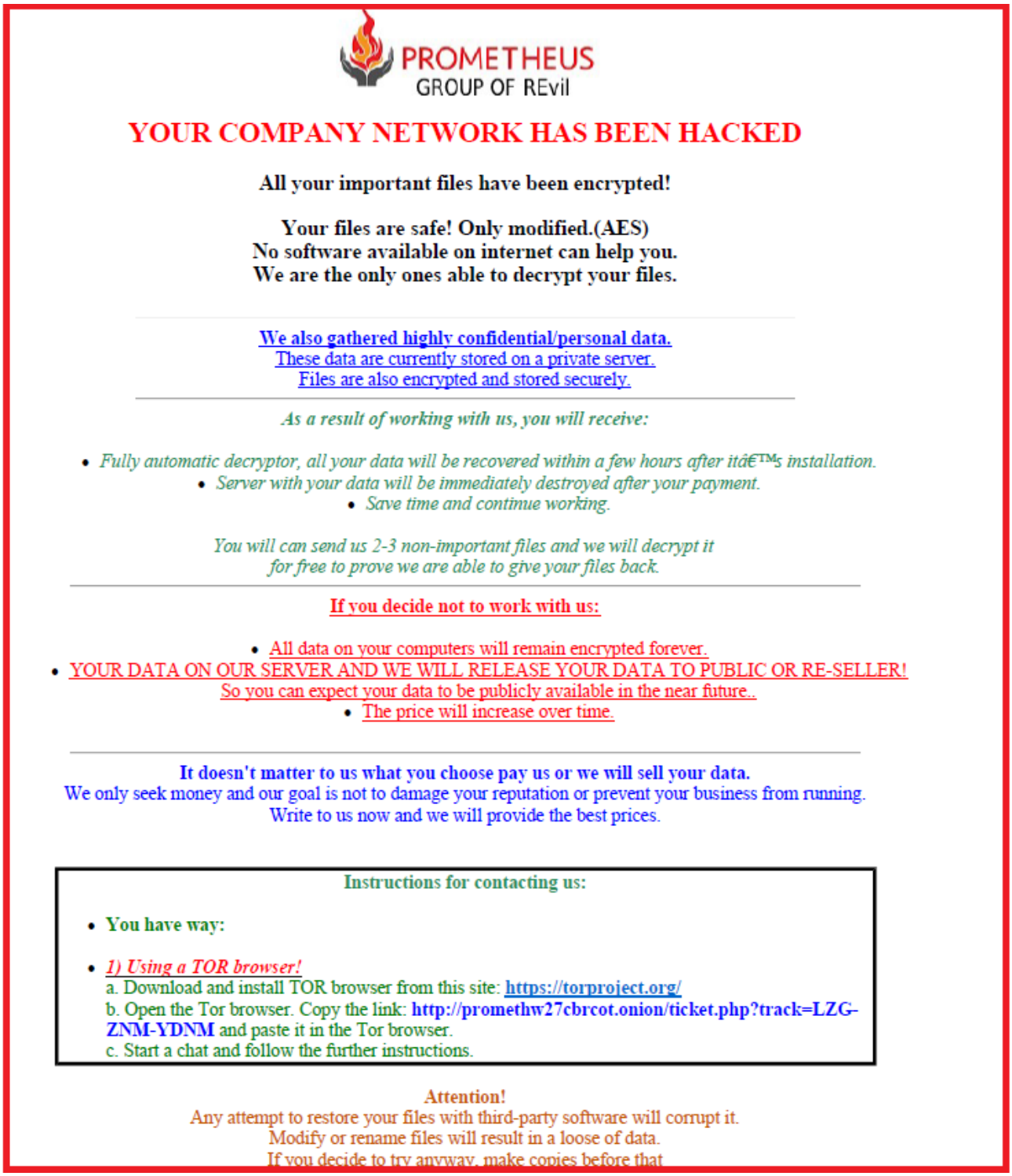

Figure 14: Ransomware Note

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
c2a01ef5115f2d41dffa1b1a697d1d05b2b9532a70552473aab36d8e4dda7928
d662580e70711ba15f0bc65096a2298801ee7bc373ced3eb59582a637aeeb5fd
e9388ca092c87f310a159e03d3dd97b3ce79cd6cc642a7f3b057d0fa3dcde42c
5c66963cf7d417ffe475afdf18906df5c6dcd8dbbb1462918f197323dabb6f19
e15f9169021b5e11381547d57a952b98e06f6366161d56083ff9be69fc43e9bf
fdf8c15f27cfbf534cbc9771e3d4e42632a5993bb4b08f444111147ec540e273
c76825aeaa7960e44bda9786efbcbb6e7865ef9f27fa6931e566aa44d88ad9cd
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
6e016c4d1db409b5e499289f31bcb6b87b5c46b29d4fcba4a50a7b68d733b93e
8b55f596d8179b043f050f42bc7c079d07be918fe321805aff1a00f88dd8f06d
b9acf82471bc22c7ce444684759d7506d407286989141028a2621a0b0f535094
ea55c78b15e2045f26ea39db122acb9a5cca84ba97625f444054f3efa331b386
113230f881d7008fad3d62e34ce79f1b9273f604303f1b5c1450cff6481655de
a88db6dc88a37a79056f466c6e0878569715409c5387be4947789cc924a97b92
3caa5163083177d40dd9ec2c3b84d0b37c82e2ee9807a50338af89f132a354d9
5d40615701c48a122e44f831e7c8643d07765629a83b15d090587f469c77693d
0cfed709f1954141a3c5a363e4e95d7e5b546ef310cfb9a63f0ca20ccc6ed152
2033194ab3c2602eb9d3b31eeb5432514c423eac213f1219e5865dfee371ed58
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.