Spook Ransomware | Prometheus Derivative Names Those That Pay, Shames Those That Don’t

By Jim Walter

Published: 2021-10-28 · Archived: 2026-04-05 22:20:06 UTC

By Jim Walter and Niranjan Jayanand

Executive Summary

- Spook Ransomware is an emerging player first seen in late September 2021
- The operators publish details of all victims regardless of whether they pay or not
- Targets range across several industries with an emphasis on manufacturing
- Analysis shows a significant degree of code sharing between Spook and the Prometheus and Thanos ransomware families

Overview

Spook ransomware emerged onto the scene in late September 2021 and follows the multi-pronged extortion model that is all too common these days. Victims are hit with the threat of data destruction as well as public data leakage and the associated fallout. In this report, we explore how the malware shares certain similarities with earlier ransomware families, and describe its main encryption and execution behaviour.

Spook and Prometheus

There is some indication that Spook is either linked to, or derived from, Prometheus ransomware. Prometheus is itself an evolution of Thanos ransomware. However, it is important to note that since Thanos ransomware had a builder which was leaked, any real attempts at attribution based solely on the malware’s code is somewhat futile. Even so, there are a few notable similarities between Spook, Prometheus, and ultimately Thanos.

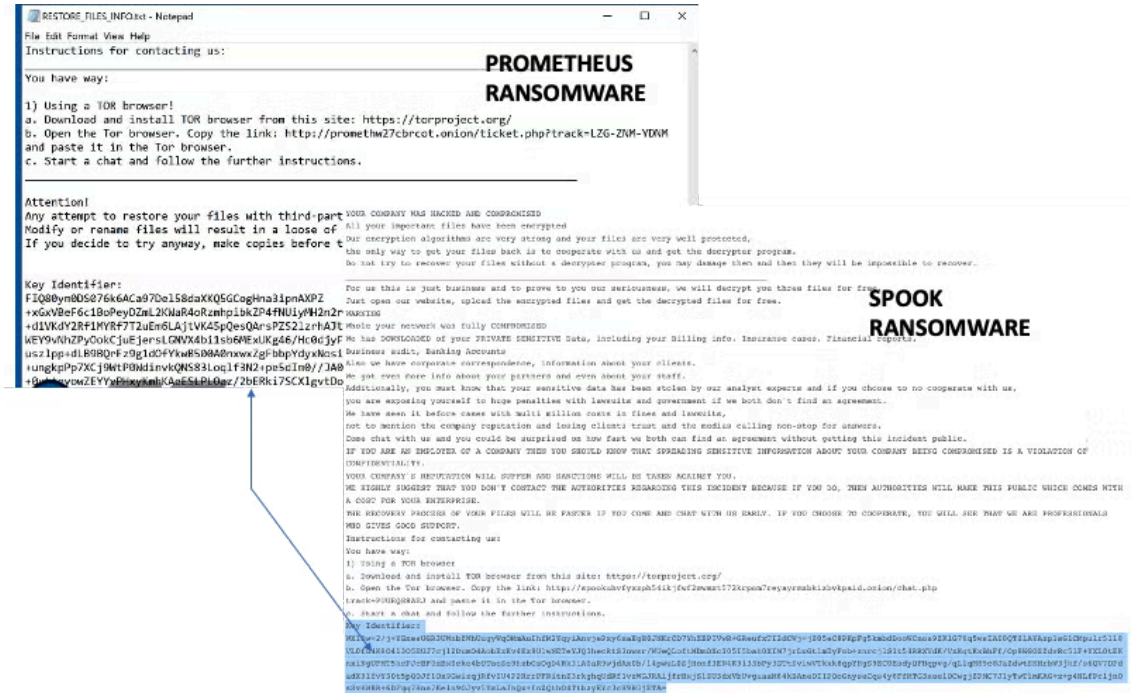
The .NET binary in the following sample, first seen in VirusTotal on 02 October, provides a glimpse into some of these similarities, with artifacts from the Thanos builder also apparent.

`a63a5de26582af1438c9886cfb15c4baa08cce2e`

```
SearchFiles
WalkDirectoryTree
<Main>b__4
Process
<IsDriveNTFS>b__17
DriveInfo
<Crypt>b__20
<Crypt>b__21
<Crypt>b__22
<WorkerCrypter2>b__2f
<WorkerCrypter2>b__32
<WorkerCrypter2>b__30
<WorkerCrypter2>b__31
<WorkerCrypter2>b__33
<WorkerCrypter2>b__34
<Encrypt2>b__44
<Encrypt2>b__45
```

Shared code block with Thanos

Our analysis suggests that there is an overlap of between 29-50% of shared code between Spook and Prometheus. Some of this overlap is related to construction of the ransom notes and key identifiers.



Ransom note similarity example (Prometheus vs Spook)

In addition to shared code artifacts, there are similarities with regards to the layout and structure of the Spook and Prometheus payment portals.

Below are the similarities between the leak data URLs hosted by both the groups

- Spook ransomware:
  `hxxp[:]//spookuhv****.onion/blog/wp-content/uploads/2021/05/1-15.png`

- Prometheus ransomware:
  `hxxp[:]//promethw****.onion/blog/wp-content/uploads/2021/05/1-15.png`

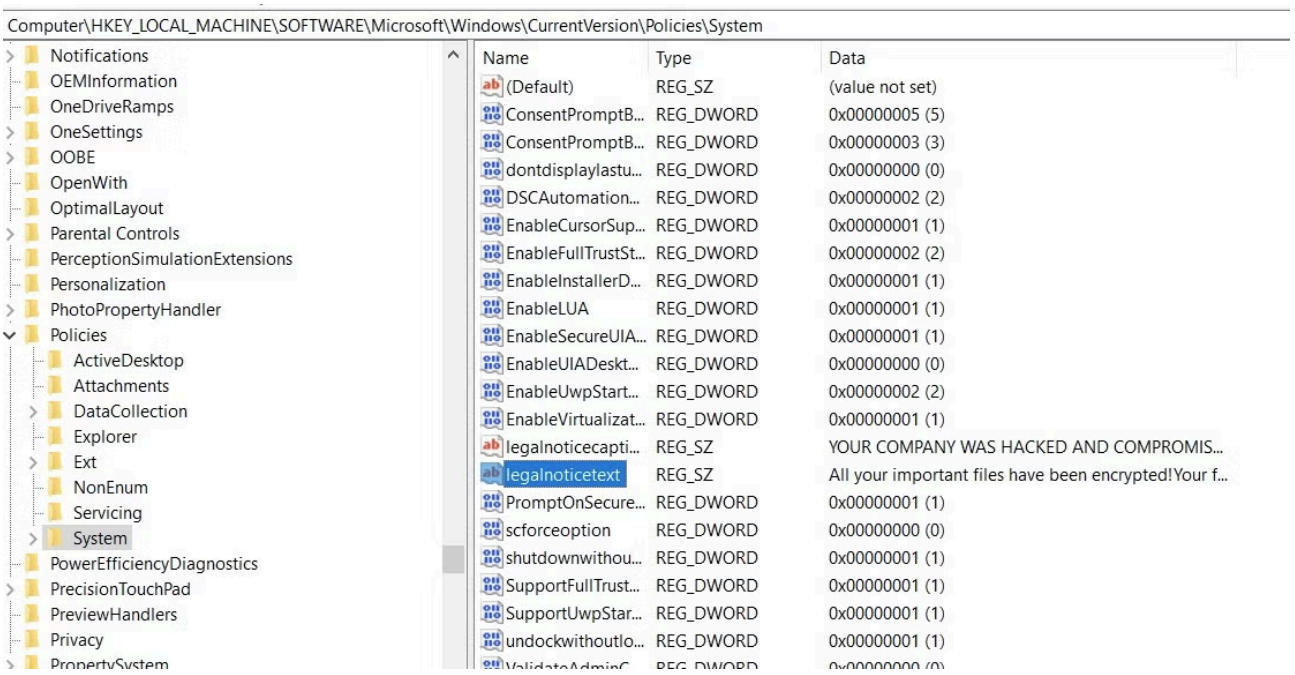
Offline Encryption and Process Manipulation

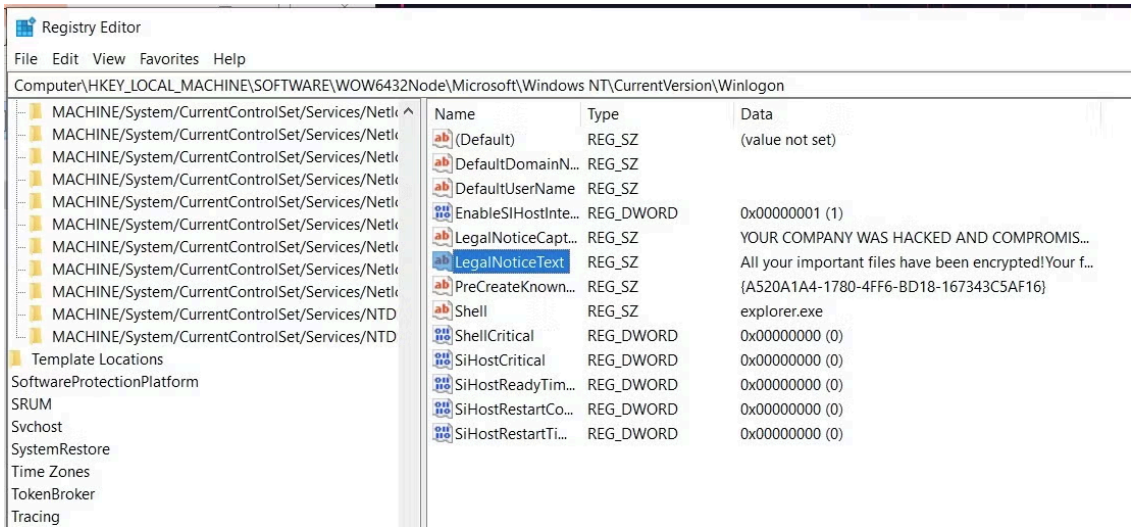
Spook, mirroring the manifestos of others, boasts “very strong (AES) encryption” along with the threat of leaking victim data to the public. The malware has the ability to encrypt target machines without requiring internet connectivity. Encryption of a full disk can occur within just a few minutes, at which point the ransom note is displayed on the desktop (`RESTORE_FILES_INFO.HTA`) along with numerous other system notifications.

The malware also makes a number of changes to ensure that the ransom notifications are displayed prominently after reboot (via Start Menu lnk, Reg).

`WinLogon` is modified (via registry) to display the Ransom Note text upon login:

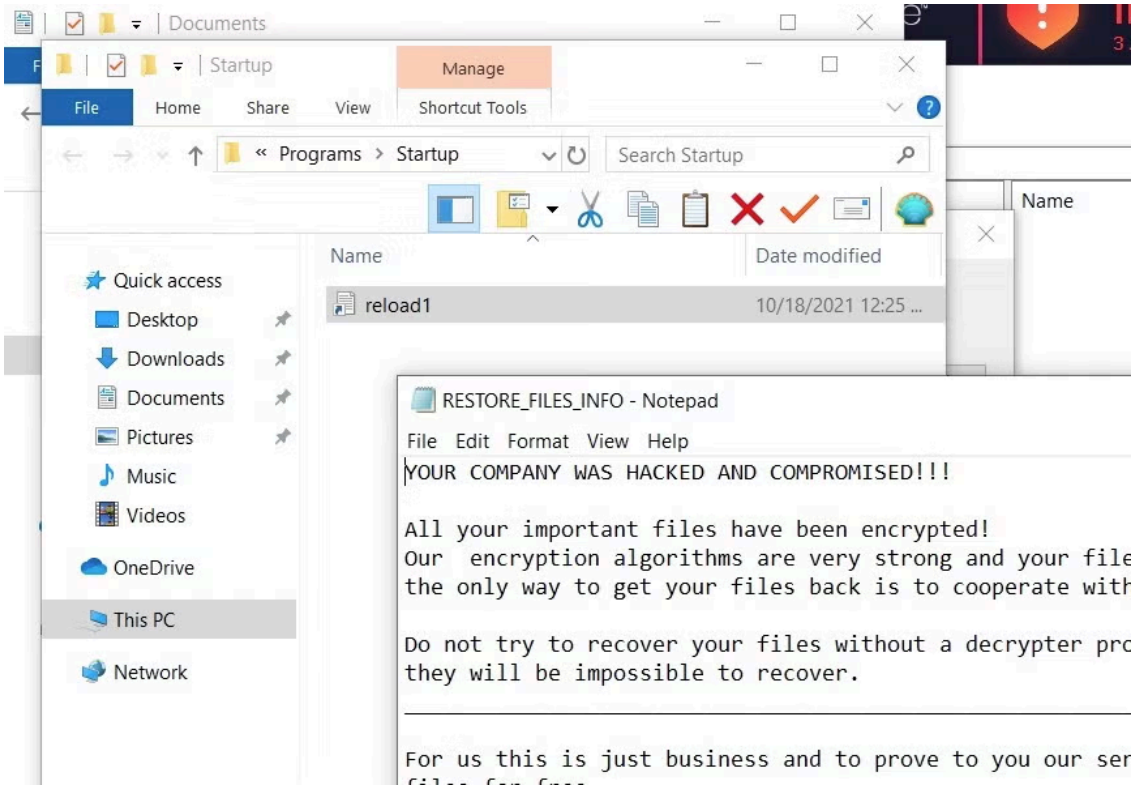
```
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon
Str Value: LegalNoticeCaption/Text
```





Registry Modifications for Persistence

Ransom notes are also displayed upon login via a Shortcut placed in the Startup directory



Startup Folder Shortcut

In addition, Spook will attempt to terminate processes and stop services of anything that may inhibit the encryption process.

Here again there is overlap between Spook, Prometheus, and Thanos with regards to process discovery and manipulation, especially with regards to checking for and killing the Raccine anti-ransomware process that some organizations deploy in an effort to protect shadow copies.

`TASKILL.EXE` is used to force the termination of the following processes if found:

```
agntsvc.exe
CNTAoSMgr.exe
dbeng50.exe
dbsnmp.exe
encsvc.exe
excel.exe
firefoxconfig.exe
hunderbird.exe
infopath.exe
isqlplussvc.exe
mbamtray.exe
msaccess.exe
msftesql.exe
mydesktopqos.exe
mydesktopservice.exe
mysqld-nt.exe
Mysqld-opt.exe
Mspub.exe
mysqld.exe
Ntrtscan.exe
ocautoupds.exe
ocomm.exe
ocssd.exe
onenote.exe
oracle.exe
outlook.exe
PccNTMon.exe
Powerpnt.exe
RaccineSettings.exe
sqbcoreservice.exe
sqlagent.exe
sqlbrowser.exe
sqlservr.exe
Sqlwriter.exe
synctime.exe
steam.exe
tbirdconfig.exe
thebat.exe
thebat64.exe
tmlisten.exe
visio.exe
winword.exe
wordpad.exe
xfssvccon.exe
zoolz.exe
```

```
taskkill.exe /IM ocomm.exe /F
```

The Raccine product is specifically targeted with regards to disabling the products' UI components and update features. These are carried out via basic OS commands such as `reg.exe` and `schtasks.exe`.

```
taskkill.exe /F /IM RaccineSettings.exe
reg.exe (CLI interpreter) delete "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "Ra
reg.exe (CLI interpreter) delete HKCU\Software\Raccine /F
schtasks.exe (CLI interpreter) /DELETE /TN "Raccine Rules Updater" /F
```

In addition, `sc.exe` is used to disable specific services and components:

```
sc.exe config Dnscache start= auto
sc.exe config SQLTELEMETRY start= disabled
sc.exe config FDResPub start= auto
sc.exe config SSDPSRV start= auto
sc.exe config SQLTELEMETRY$ECWDB2 start= disabled
sc.exe config SstpSvc start= disabled
sc.exe config upnphost start= auto
sc.exe config SQLWriter start= disabled
```

With various processes out of the way and the system in an optimal state for encryption, the malware proceeds to enumerate local files and folders, along with accessible network resources.

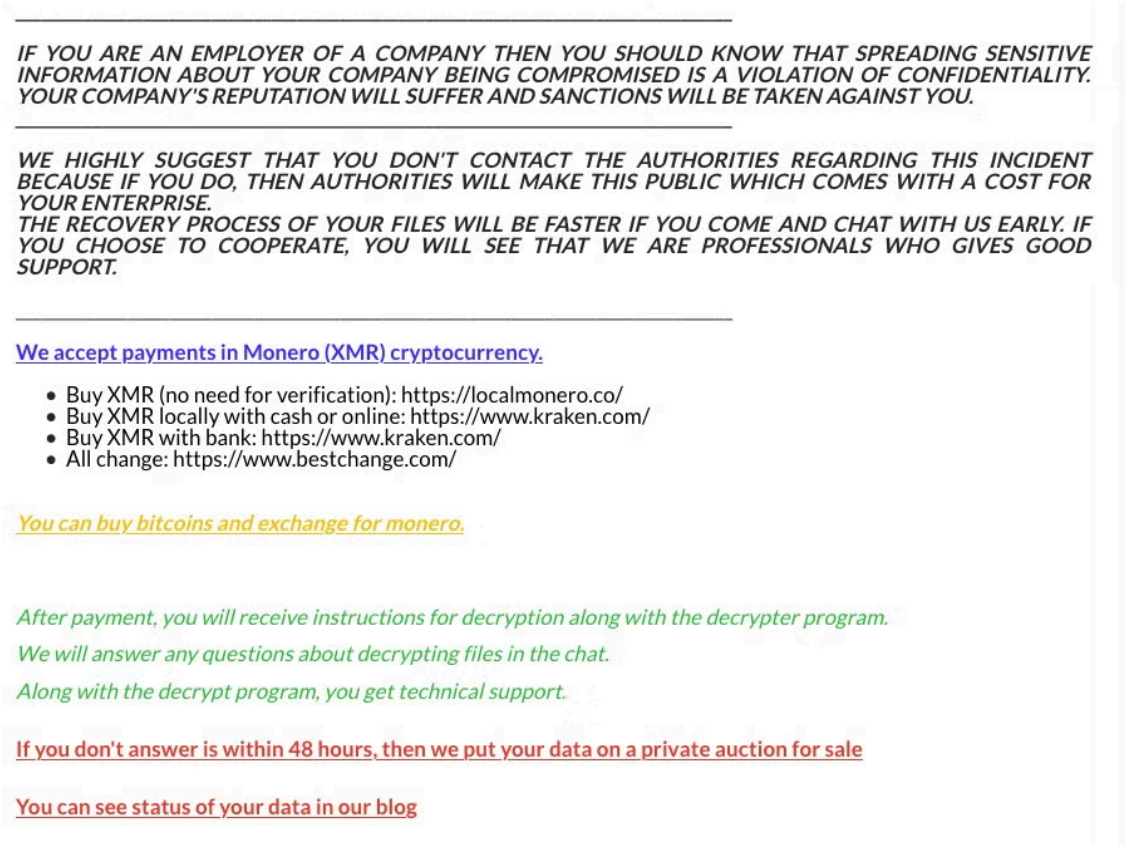
Given the Thanos pedigree, specifics around encryption can vary. The samples analyzed employ a random string at runtime as the passphrase for file encryption (AES). The string is subsequently encrypted with the attacker's public key and added into the generated ransom note(s). Recovery of encrypted data is, therefore, not possible without the corresponding private key.

Ransom Payment and Victimology

Upon infection, victims are instructed to proceed to Spook's TOR-based payment portal.

Spook Ransom Demand

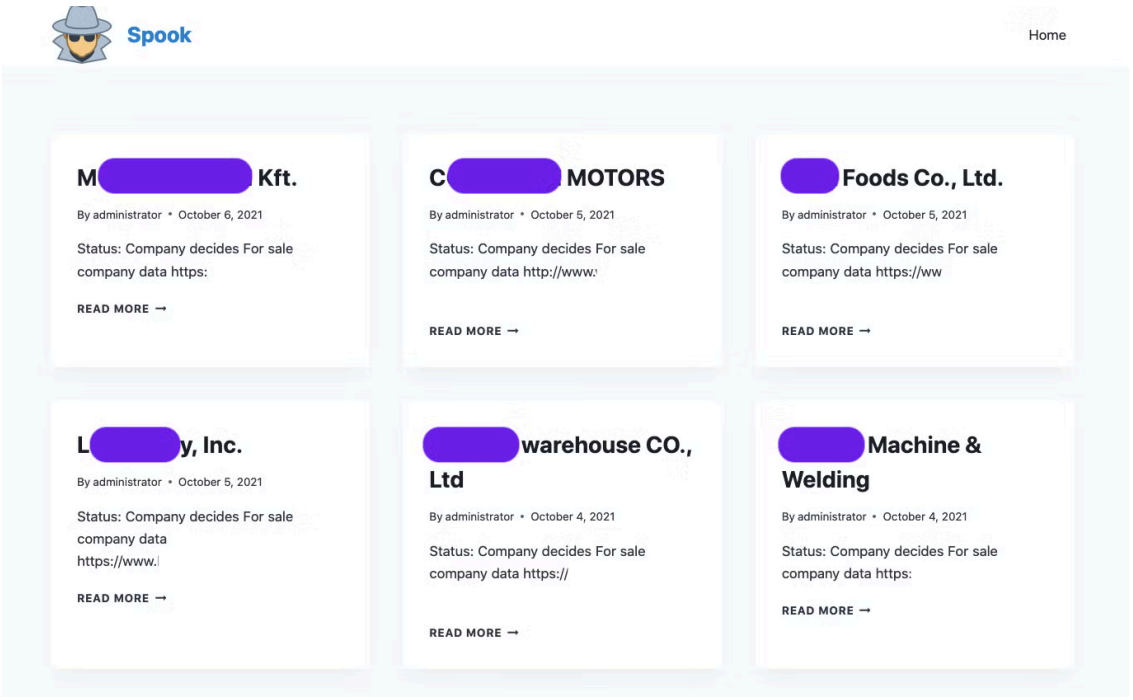
At the payment portal, the victim is able to interact with the attackers via chat to negotiate payment.



Spook Payment Portal

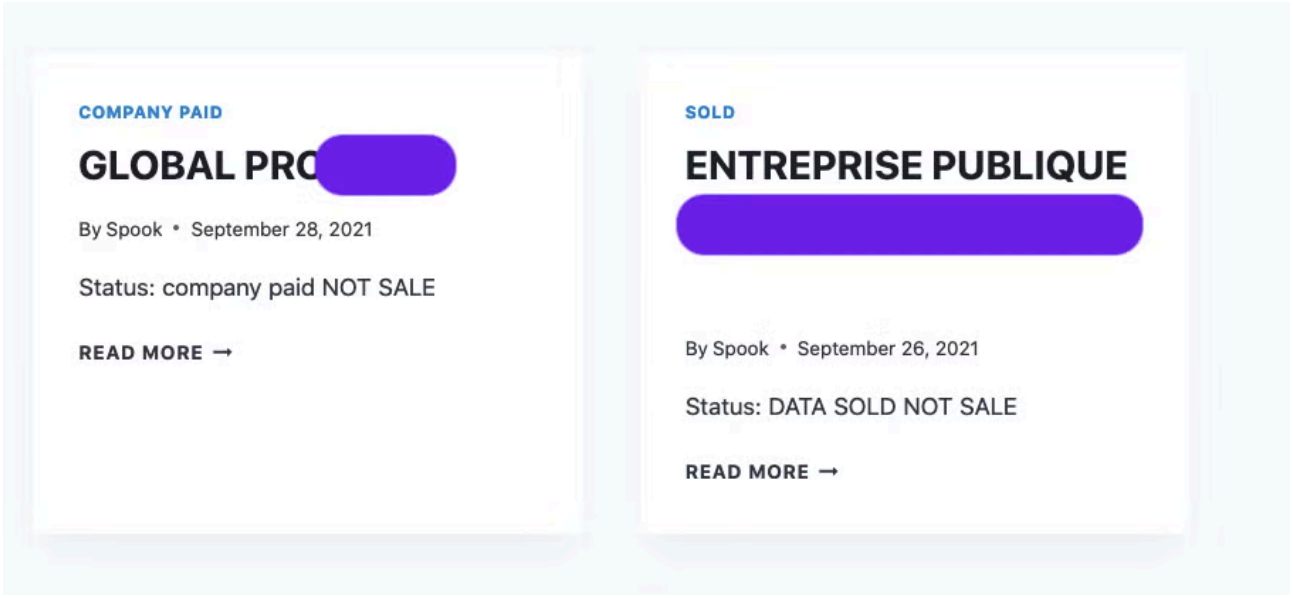
Spook has been leveraging attacks against high-value targets across the globe, with little to no discretion with regards to industry. Looking at the current cross-section of victims posted on the group's web site, however, the majority are in the manufacturing sector.

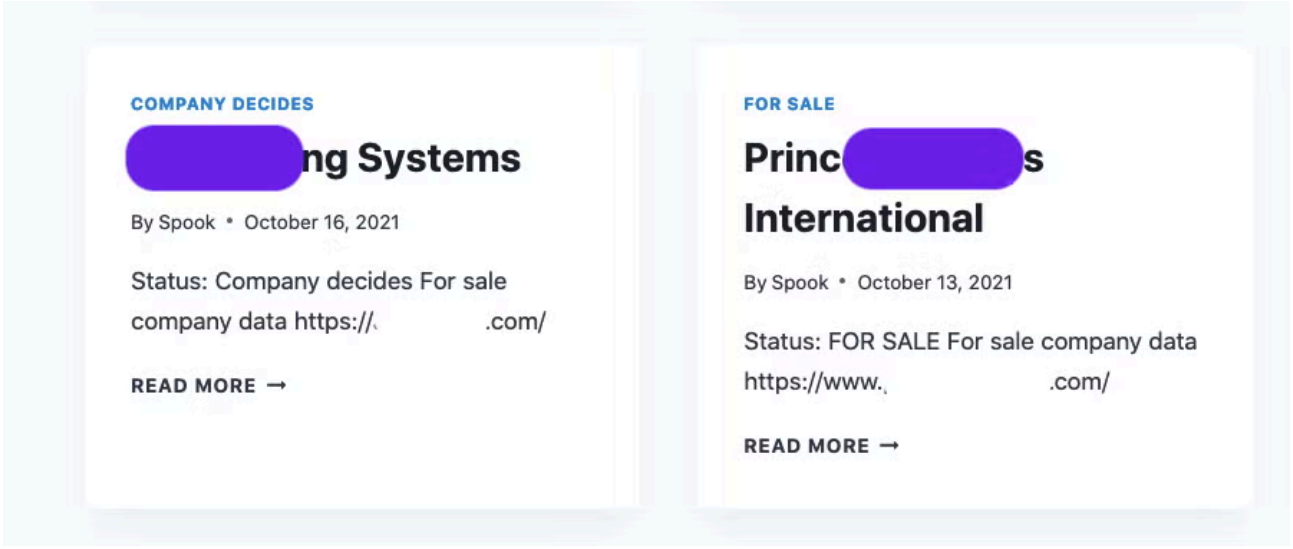
The public blog went live in early October 2021. At the time of writing, there are 17 victims posted on the Spook site.



Some of the victims named on the Spook blog site

Spook actually lists all attacked companies, regardless of whether or not they pay the ransom demand. Those victims that pay have their entry updated to indicate that the company's data is 'not for sale'. Those that have not paid are listed as having data that is "For Sale", while some victim entries, presumably the most recent or those that are in the process of negotiating, are listed as "Company Decides".





Conclusion

As these attacks continue to escalate and become more egregious, the need for true attack prevention is all the more critical. Spook's tactic of public outing victims even if they pay threatens reputational harm to any compromised company, even if they follow the attackers' payment demands.

This only continues to illustrate the importance of preventing attacks in the first place. Ransomware operators have moved beyond worrying about companies detecting after-the-fact and attempting to recover encrypted data.

Indicators of Compromise

SHA256

8dad29bd09870ab9cacfdea9e7ab100d217ff128aea64fa4cac752362459991c
e347fd231a543a5dfd53b01ff0bc67b2bf37593e7ddc036f15bac8ad92f0d707
d991aa2b1fad608b567be28e2d13d3d4f48eea3dea8f5d51a8e42aa9a2637426

SHA1

a63a5de26582af1438c9886cfb15c4baa08cce2e

bfd0ab7eec4b282cc5689a48e8f438d042c9d98f

e2b098d36e51d2b7405fadbd578cf9774433f85a

MITRE ATT&CK

TA0005 – Defense Evasion

T1486 – Data Encrypted for Impact

T1027.002 – Obfuscated Files or Information: Software Packing

T1007 – System Service Discovery

T1059 – Command and Scripting Interpreter

T1112 – Modify Registry

TA0010 – Exfiltration

T1018 – Remote System Discovery

T1082 – System Information Discovery

T1547.004 – Boot or Logon Autostart Execution: Winlogon Helper DLL

T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Spook Ransom Note Sample

```
YOUR COMPANY WAS HACKED AND COMPROMISED!!!

All your important files have been encrypted!
Our  encryption algorithms are very strong and your files are very well protected,
the only way to get your files back is to cooperate with us and get the decrypter program.

Do not try to recover your files without a decrypter program, you may damage them and then they will be impossible to
recover.
_____________________________________________________________________________

For us this is just business and to prove to you our seriousness, we will decrypt you three files for free.
Just open our website, upload the encrypted files and get the decrypted files for free.
_____________________________________________________________________________

 ! WARNING !
Whole your network was fully COMPROMISED!

We has DOWNLOADED of your PRIVATE SENSITIVE Data, including your Billing info, Insuranse cases, Financial reports,
Business audit, Banking Accounts! Also we have corporate correspondence, information about your clients.
We got even more info about your partners and even about your staff.

Additionally, you must know that your sensitive data has been stolen  by our analyst experts and if you choose to no
cooperate with us,
you  are exposing yourself to huge penalties with lawsuits and government if we both don't find  an agreement.
We have seen it before cases with multi million costs in  fines and lawsuits,
not to mention the company reputation and losing clients trust and  the medias calling non-stop for answers.
Come chat with us and you could  be surprised on how fast we both can find an agreement without getting this incident
public.
_____________________________________________________________________________

IF YOU ARE AN EMPLOYER OF A COMPANY THEN YOU SHOULD KNOW THAT SPREADING SENSITIVE INFORMATION ABOUT YOUR COMPANY BEING
COMPROMISED IS A VIOLATION OF CONFIDENTIALITY.
YOUR COMPANY'S REPUTATION WILL SUFFER AND SANCTIONS WILL BE TAKEN AGAINST YOU.
_____________________________________________________________________________

WE HIGHLY SUGGEST THAT YOU DON'T CONTACT THE AUTHORITIES REGARDING THIS INCIDENT BECAUSE IF YOU DO, THEN AUTHORITIES
WILL MAKE THIS PUBLIC WHICH COMES WITH A COST FOR YOUR ENTERPRISE.
THE RECOVERY PROCESS OF YOUR FILES WILL BE FASTER IF YOU COME AND CHAT WITH US EARLY. IF YOU CHOOSE TO COOPERATE, YOU
WILL SEE THAT WE ARE PROFESSIONALS WHO GIVES GOOD SUPPORT.

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://spookuhvfyxzph54ikjfwf2mwmxt572krpom7reyayrmxbkizbvkpaid.onion/chat.php?
track=PUUEQS8AEJ and paste it in the Tor browser.
c. Start a chat and follow the further instructions.


Key Identifier:
WX1Dw+2/
j+YGxesUGR3UWnbZWhUugyWqOMmAuIhfM2YqyiAnvjePxy6xaEgH0JNKrCD7YhZEPIVwR+GReufxTI2dCWj+jZ05eC8PKpFg5kmbdDooWCnoa9ZKlG76q5w
sIAI0QTZlAYAzp1sGlCMpulr51l8VL0fu4K8O4l3O5EUJ7cj1ZDumO4AobEzKv4Kz9U1wNETeYJQ1hecRtS3nwsr/
WUeQLoftMDmDXcI05I5bah0XIM7jrLuGt1mEyFob+znrcjlSlt54RRXVdK/VxKqtKxBhFf/
Op8WGOZZdvRc5lF+YXLOtEKnxiNgUFMT5kcPJcBF0zBx0cke4bOTaoZe9hzbOzOgD4Rk3iA0aR9wjdAx0b/
l4pwuL0SjHonf3EN4K9i33bPy3GTtSviwVTkxk8qpYHgS9EC0EsdyQFHqpvg/qLlqM89c8JaZdwtSKHrbW3jkf/
s6QV7DPdadX9lfvY30t5pQOJf1Ox9GwizqjRfvIU4P2RrrPFRitnZ3rkghqUdRf1vzWGJRAijfrHxjSlZU3dxVbUvguaaM64kBAneDI1PQoGnyseCqs4y6F
fMTG3xeelQCwgjZPMC7J1yTwTlmKAG+z+p4HLfPcljnOsSvKW8R+6DFqq7Rna7Keln9OJyv5YmLaJnQx+fnZQthO4TtbzyEYc3cH9R0jETA=
```

Source: https://www.sentinelone.com/labs/spook-ransomware-prometheus-derivative-names-those-that-pay-shames-those-that-dont/