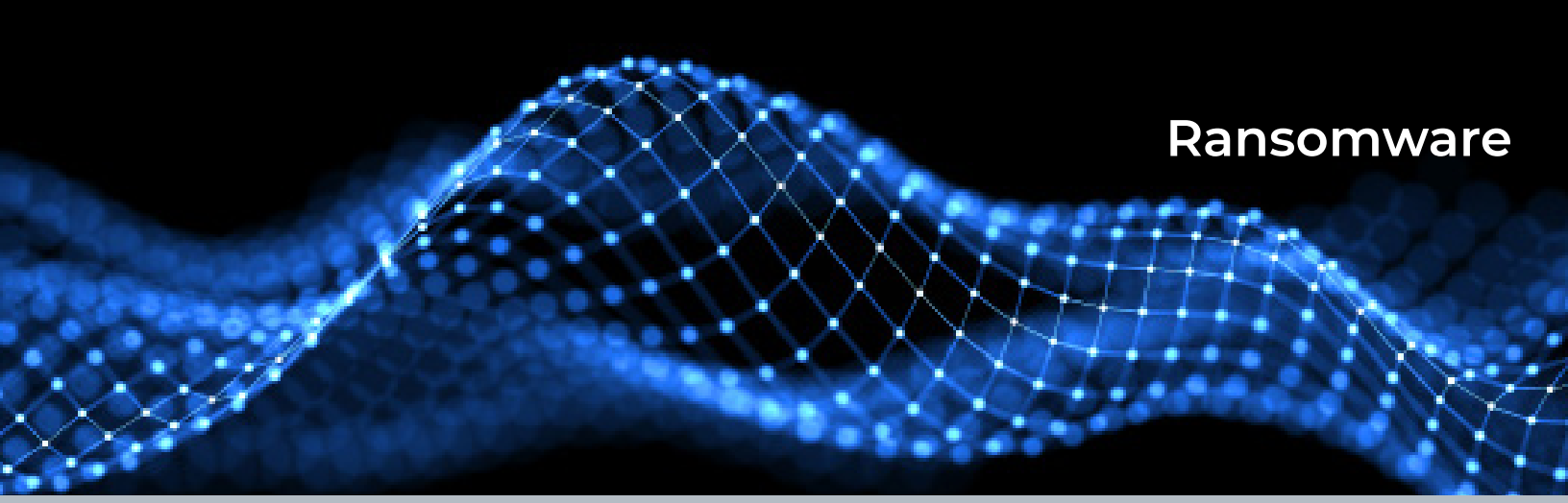

Sodinokibi Labels Keys with "Black Lives Matter"

Background

In June 2020, Arete released an article concerning Sodinokibi attacks against the education sector which included statistics about attacks observed up to that point[1]. In August and September 2020, Arete Incident Responders continued to work DFIR engagements involving Sodinokibi\REvil. In these instances, the ransomware attack occurred against targets in the Manufacturing, and Professional Services sectors.

In our analysis of the Sodinokibi malware, we observed the threat actors touting the Black Lives Matter (BLM) movement by saving their configuration data in BLM labeled registry keys. The following are examples of the Sodinokibi registry changes:

- HKLM**\SOFTWARE\BlackLivesMatter**Hv4 = E5 62 93 47 69 B2 AB D8 0C E0 5C 96 80 0B DB 81
- HKLM\SOFTWARE\BlackLivesMatter\KxGe = 50 C6 9A CB 34 91 22 C8 E1 B0 82 1E E7 A1 5B A5
- HKLM\SOFTWARE\BlackLivesMatter\I0sZQ = 21 A3 0C B5 A7 EA 57 73 6B 10 94 22 EC EF D0 7F
- HKLM\SOFTWARE\BlackLivesMatter\Z2iI9s = 3D 73 12 96 73 0A 17 6E 18 A4 EF B1 FF 16 34 EA
- HKLM\SOFTWARE\BlackLivesMatter\SaDZyFI = .591d1k-9jw

In a separate engagement, we saw slightly different registry key artifact like the above:

- HKLM**SOFTWARE\WOW6432Node\BlackLivesMatter**SaDZyFI = .7t9o0t9f

OSINT shows that the Trickbot ransomware precursor has also taken advantage of the Black Lives Matter theme in phishing email lures during e-voting campaigns, with malicious MS Office documents that run a macro to download and execute the Trickbot DLL.

Arete's Sodinokibi Threat Statistics

The information listed below is based on our statistics for the month of September 2020. Our IR and Data Analytics practices work hand-in-hand to track key data points for every ransomware engagement. The IR practice tracks data points on the ransomware variant and collects statistics based on handled engagements:

- The average ransom demand paid in US dollars has been $174,399.29
- The maximum ransom demand paid in US dollars has been $759,835.29
- The minimum ransom demand paid in US dollars has been $4,550.98
- Percentage of times the ransom paid is 60.22%
- The average business downtime is 7.46 days
- Threat actors have provided the decryption key 100% of the time
- Data exfiltration has occurred in 12.96% of the engagements
- The major infection vector has been Remote Access (RDP)

Additional Indicators

Ghost

In one of the Arete's Sodinokibi incidents, the attackers used an application known as "ghost" to create a tunnel, encrypting their network traffic connection to hide their communication (ref: https://github.com/ginuerzh/gost).

1 https://areteir.com/wp-content/uploads/2020/07/Arete_Insight_Sodino-Ransomware_June-2020.pdf

Sodinokibi file information

```
File Name:  serig.exe
File Size:  119808 bytes
MD5:        100cc792983e1a015e6c1509c6e0ae54
SHA1:       2f375a1a054e0d7a8f379942f75c4b09d4131c88
SHA256:     b619624078f2e0dbba5e421a9a2cd63a515e720f6d5a5bc3894a9458011cfce0
PE Time:    0x5F3E6BAA [Thu Aug 20 12:25:14 2020 UTC]
Sections (5):
  Name      Entropy  MD5
  .text     6.53     8e022997a2d930e7fef8e09973ad89d5
  .rdata    7.81     e212a9e510fd4c97da54813c0f43c809
  .data     7.47     ea9a0a525907145c83d3727e18ffe786
  .gwsp16   5.63     3771db0f8834f902ffc9aa2af849c69b
  .reloc    6.0      da875f4a1a782f7fd7be673e826952ad
```

Ransom Note

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on your system has extension 591d1k9jw.

By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.

To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.

If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key. In practice - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
 a) Download and install TOR browser from this site: https://torproject.org/
 b) Open our website:
http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/[removed_by_analyst]

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
 a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
 b) Open our secondary website: http://decryptor.cc/[removed_by_analyst]

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:

fn1[removed_by_analyst]fP

!!! DANGER !!!
DONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus solutions - its may entail damage of the private key and, as result, The Loss all data.
!!! !!! !!!
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) make everything for restoring, but please should not interfere.

References

https://areteir.com/wp-content/uploads/2020/07/Arete_Insight_Sodino-Ransomware_June-2020.pdf

https://www.bleepingcomputer.com/news/security/fake-black-lives-matter-voting-campaign-spreads-trickbot-malware/

https://nakedsecurity.sophos.com/2020/06/11/crooks-hijack-black-lives-matter-to-spread-zombie-malware