Threat Hunting for REvil Ransomware

awakesecurity.com/blog/threat-hunting-for-revil-ransomware/

November 9, 2020

Summary

REvil (short for Ransomware Evil and also referred to as Sodinokibi) ransomware is in the ransomware-as-a-service(RaaS) business. The malware is handed over to the affiliates to infect users and extort money. In turn the original REvil developers take 20-30% of the amount that the affiliates receive. The ransomware developers say that they have made more than $100 million in one year by infecting users owning large businesses. Attacks attributed to REvil were first spotted in April 2019, soon after the shutdown of the Gandcrab ransomware family. In fact, the developers of REvil have admitted that they did not build from scratch, but instead used the Grandcrab code base. In this post we describe how security operations teams can hunt for REvil ransomware and the artifacts it produces / leaves behind.

Understanding REvil

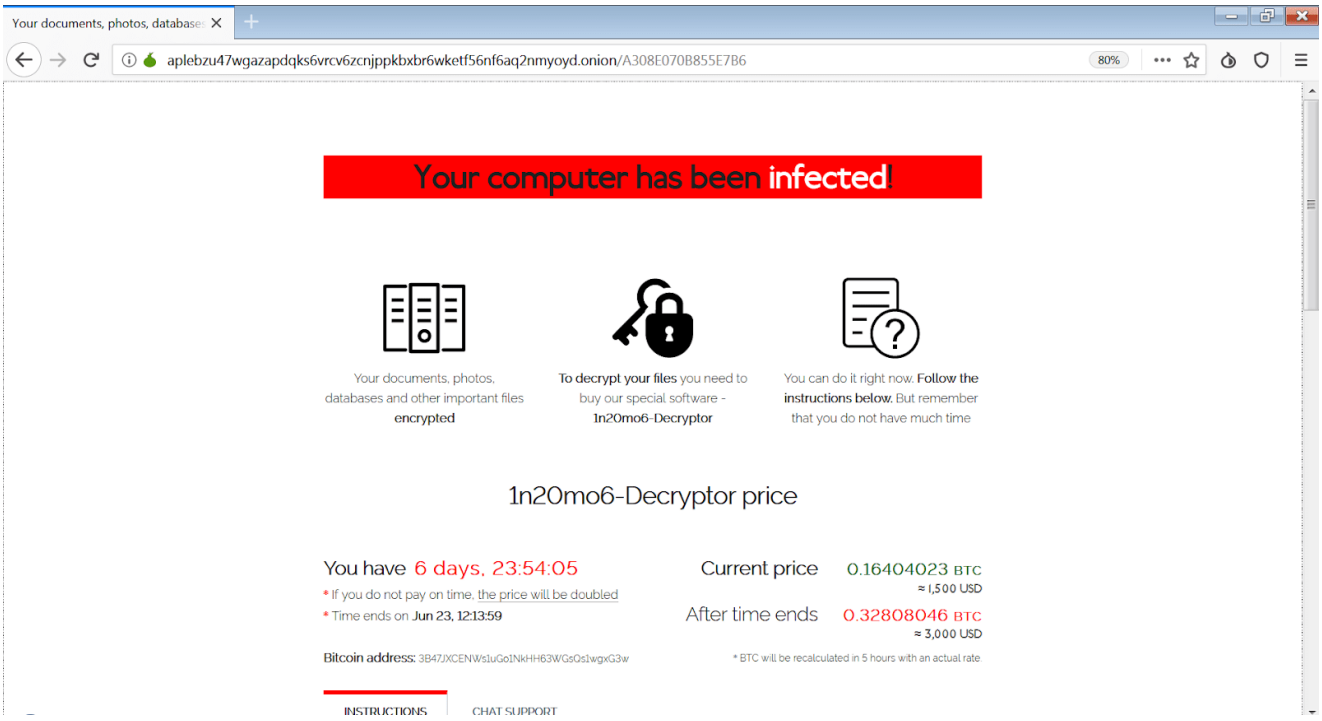

Figure 1: Tor Payment page from a REvil infected machine

To encrypt files, REvil uses elliptic curve cryptography(ECC). This allows smaller keys compared to other approaches without compromising on effectiveness of the encryption . Since its first appearance, this ransomware family has exploited vulnerabilities in software

such as Windows Servers like 2012, 2012 R2 etc, as well as more recently Remote Desktop Gateway (RD Gateway).

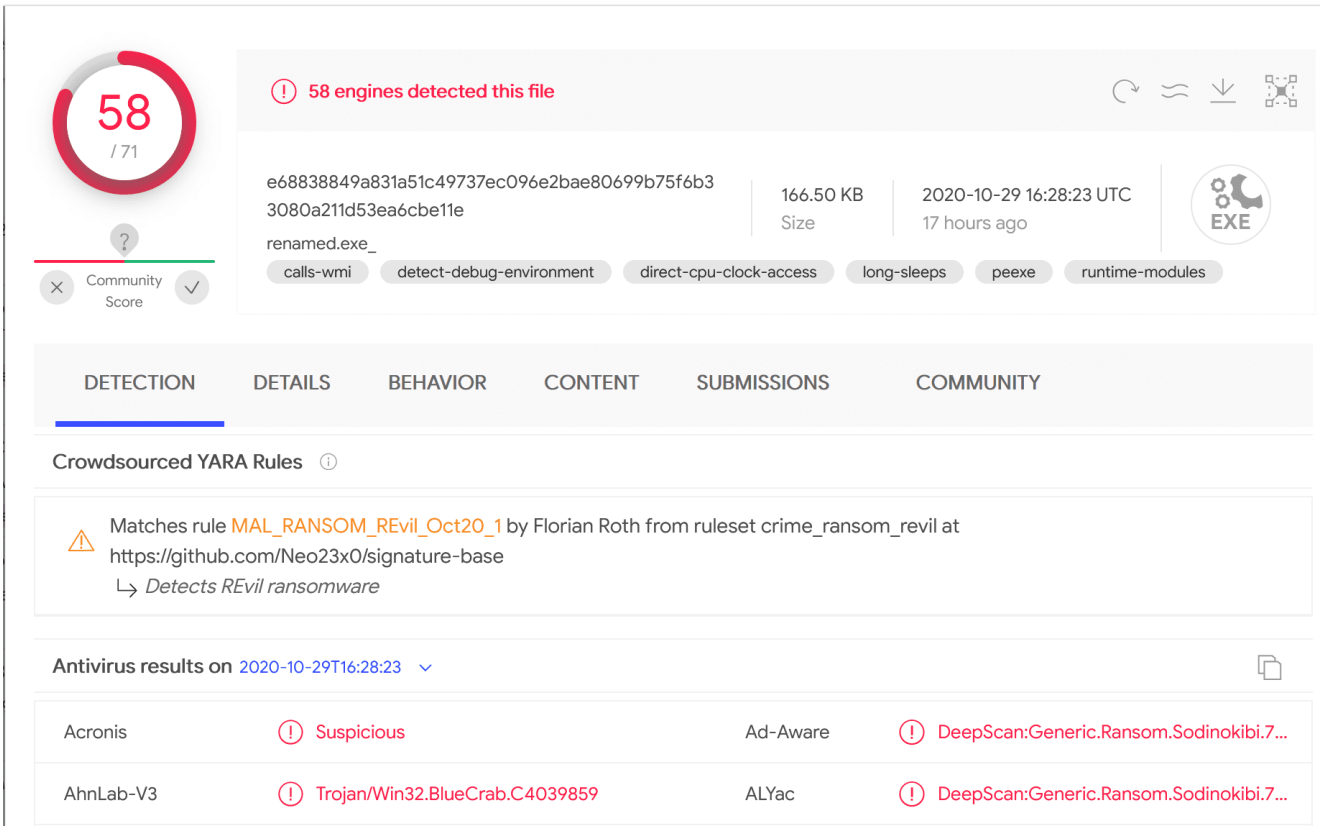

Figure 2: REvil result from Virustotal

The configuration that the malware reads is a JSON file and it is stored in a special section of the malware binary called **.iyaw** in this case (Figure 3). The name changes with every new sample and the configuration is RC4 encrypted.

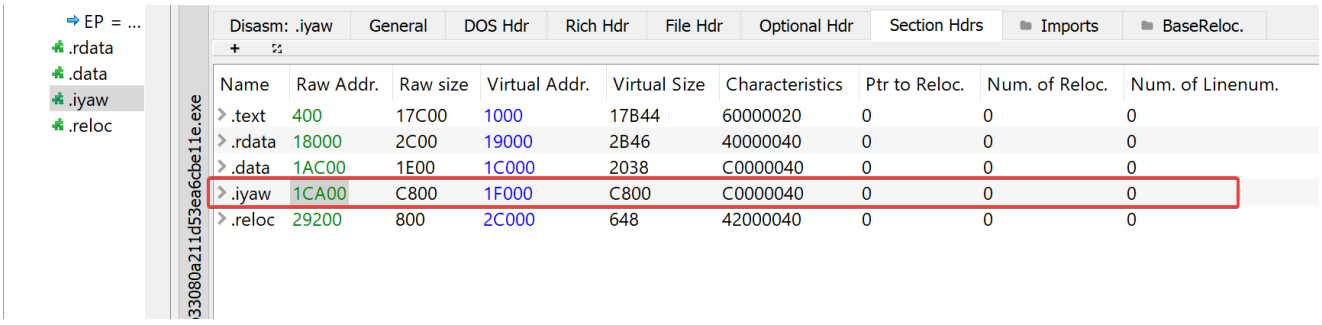

Figure 3: Section header containing ransomware configuration

The configuration defines the files to be excluded from encryption as well as the ransom note to be displayed. The sample configuration after being decrypted is shown in Figure 4.

```
{"pk":"M4O6efUNv8nZ38UjEZa5t0O4JprZSEOksh1dmd1lC1c=",
"pid":"21",
"sub":"707",
"dbg":false,
"fast":true,
"wipe":false,
"wht":{
    "fld":["windows.old","system volume information","$windows.~ws","google","boot","tor browser","programdata","
        $windows.~bt","program files (x86)","program files","windows","intel","msocache","$recycle.bin","mozilla","
        perflogs","appdata","application data"],

    "fls":["desktop.ini","ntuser.dat","autorun.inf","ntldr","boot.ini","ntuser.ini","iconcache.db","ntuser.dat.log",
        "bootfont.bin","thumbs.db","bootsect.bak"],

    "ext":["rom","ani","cab","mpa","diagpkg","drv","exe","bat","key","shs","idx","msc","wpx","cpl","ps1","nls","
        diagcfg","ics","lnk","cur","sys","com","scr","mod","msi","adv","msstyles","hta","ldf","lock","themepack","
        msu","spl","nomedia","rtp","386","bin","icns","cmd","ocx","diagcab","ico","prf","hlp","theme","msp","dll","
        deskthemepack","icl"]},
"wfld":["backup"],
"prc":["ocomm","excel","dbsnmp","onenote","firefox","xfssvccon","infopath","wordpa","isqlplussvc","dbeng50","mspub",
    "mydesktopqos","ocautoupds","thunderbird","encsvc","outlook","oracle","mydesktopservice","thebat","agntsvc","
    steam","ocssd","sql","tbirdconfig","synctime","visio","sqbcoreservice","winword","msaccess","powerpnt"],
"net":true,
"svc":["backup","mepocs","memtas","veeam","svc$","vss","sophos","sql"],
"exp":false,
```


Figure 4: Decrypted REvil configuration (Source: cybereason)

After encryption the wallpaper changes (Figure 5) to display that all files have been encrypted and all the instructions are in a text file (Figure 6).

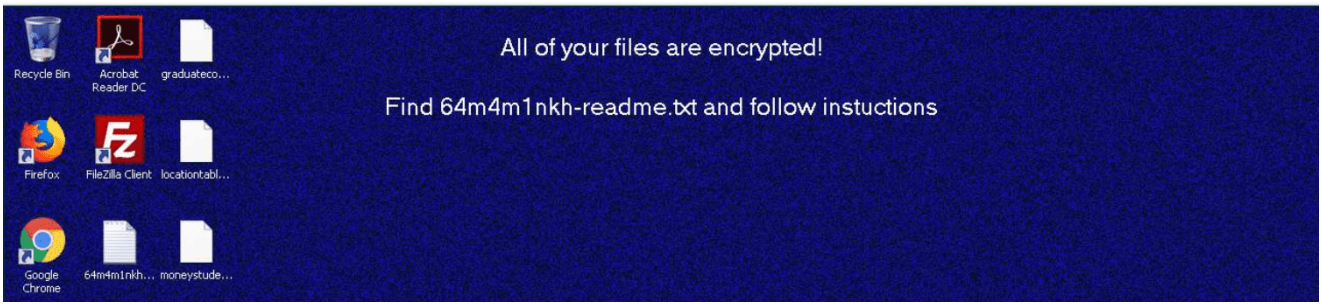

Figure 5: Wallpaper changed after REvil infection

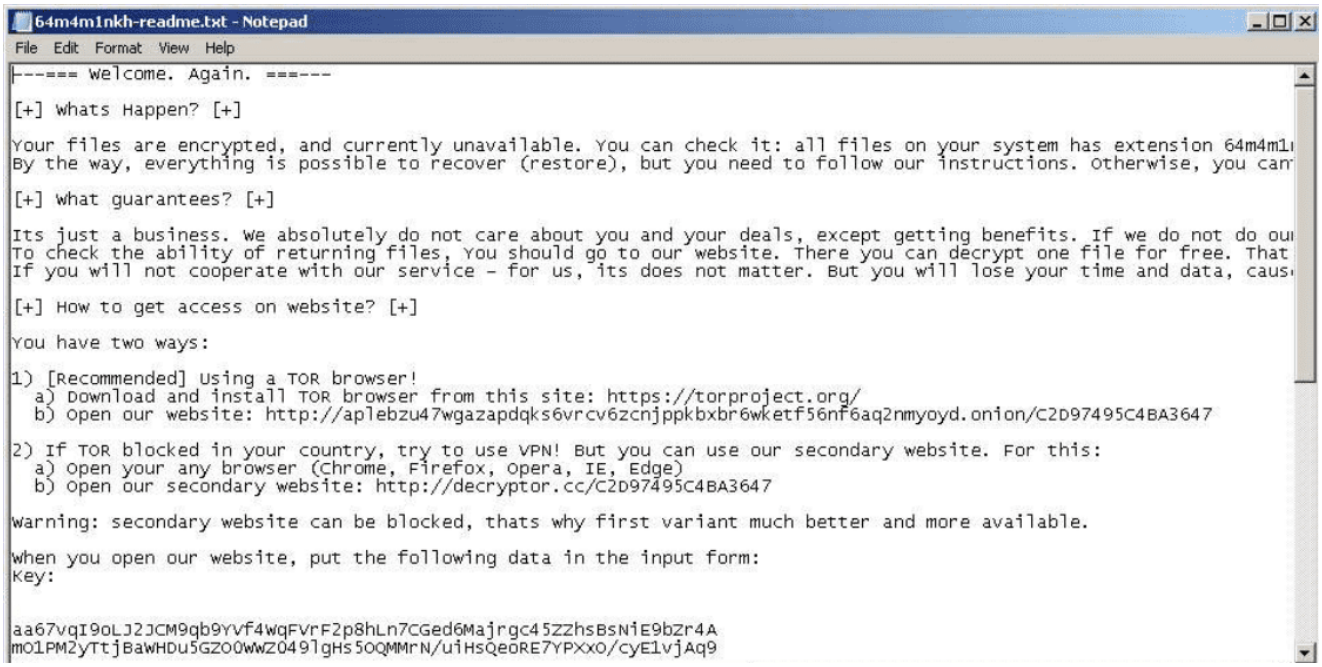

Figure 6: Note containing instruction for ransom payment

Process Cooldown

The configuration file (Figure 4) contains **prc** and **svc** fields which are process names and services that would be killed before the encryption process begins. REvil also deletes Volume Shadow Copies (VSS) using the PowerShell command shown in Figure 7.

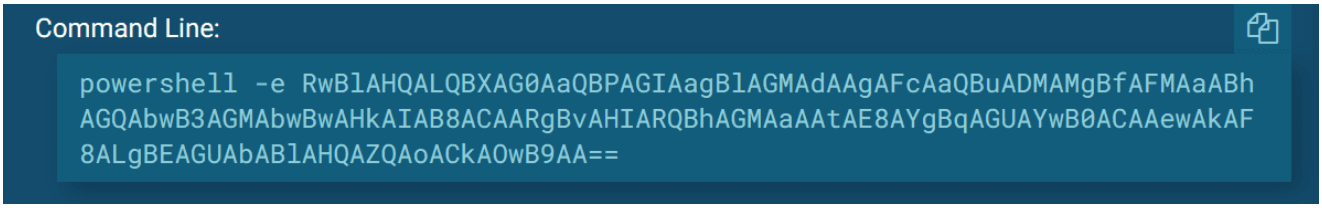

Figure 7: Encoded Powershell command to delete VSS

Decoding the command reveals the actual command (Figure 8).

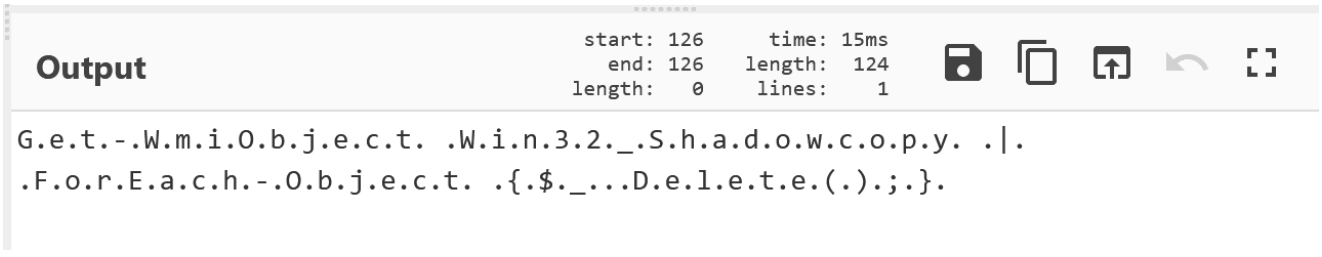

Figure 8: Decoded Powershell command

Threat Hunting for REvil

With that background, how does a security analyst uncover REvil, ideally before significant impact across the organization? After the files have been encrypted, the ransomware reaches out to over a 1000 domains generated based on information from the configuration file. Each URL contains the following pattern:

https://<domain>/<path1>/<path2>/<filename>.<ext>

Out of these 1000 domains, many are legitimate while others are C2 servers owned by the REvil operators which receive information from the infected machine. This technique allows the attackers to hide the real attacker servers. All the communication happens in TLS and the SNI can be seen in Figure 9.

1477	2020-10-12 10:47:20.126690	192.168.100.174	123.176.96.19	TLSv1	172	321play.com.hk	Client Hello
465	2020-10-12 10:45:48.104246	192.168.100.174	216.194.169.74	TLSv1	185	antiaginghealthbene…	Client Hello
1668	2020-10-12 10:47:25.416946	192.168.100.174	151.139.128.10	TLSv1	178	artotelamsterdam.com	Client Hello
356	2020-10-12 10:45:44.112997	192.168.100.174	221.121.148.69	TLSv1	171	ausair.com.au	Client Hello
416	2020-10-12 10:45:46.996738	192.168.100.174	192.0.78.12	TLSv1	190	beyondmarcomdotcom.…	Client Hello
1748	2020-10-12 10:47:41.955936	192.168.100.174	128.140.223.200	TLSv1	179	bierensgebakkramen.…	Client Hello
991	2020-10-12 10:46:31.579423	192.168.100.174	104.131.178.218	TLSv1	174	brawnmediany.com	Client Hello
445	2020-10-12 10:45:47.354613	192.168.100.174	50.31.188.30	TLSv1	187	consultaractadenaci…	Client Hello
485	2020-10-12 10:45:48.903346	192.168.100.174	136.144.215.188	TLSv1	176	corendonhotels.com	Client Hello
1010	2020-10-12 10:46:32.544144	192.168.100.174	139.99.18.146	TLSv1	168	devok.info	Client Hello
1358	2020-10-12 10:47:08.746065	192.168.100.174	87.230.47.243	TLSv1	168	dlc.berlin	Client Hello
793	2020-10-12 10:45:56.235956	192.168.100.174	104.27.185.189	TLSv1	173	faizanullah.com	Client Hello
1688	2020-10-12 10:47:25.630664	192.168.100.174	85.232.241.218	TLSv1	170	galserwis.pl	Client Hello
1036	2020-10-12 10:47:02.799338	192.168.100.174	66.45.228.160	TLSv1	173	houseofplus.com	Client Hello
376	2020-10-12 10:45:45.554258	192.168.100.174	157.7.44.169	TLSv1	169	ihr-news.jp	Client Hello
1589	2020-10-12 10:47:21.833693	192.168.100.174	213.184.85.12	TLSv1	170	koko-nora.dk	Client Hello
837	2020-10-12 10:45:57.145111	192.168.100.174	66.235.200.145	TLSv1	178	marchand-sloboda.com	Client Hello
1135	2020-10-12 10:47:05.930686	192.168.100.174	206.189.37.221	TLSv1	173	myhealth.net.au	Client Hello
1016	2020-10-12 10:47:02.479240	192.168.100.174	217.160.0.62	TLSv1	174	parebrise-tla.fr	Client Hello
1096	2020-10-12 10:47:03.785202	192.168.100.174	142.93.206.89	TLSv1	177	pawsuppetlovers.com	Client Hello
169	2020-10-12 10:45:40.746936	192.168.100.174	213.186.33.2	TLSv1	174	peterstrobos.com	Client Hello
1378	2020-10-12 10:47:11.328654	192.168.100.174	213.239.249.207	TLSv1	173	pocket-opera.de	Client Hello
967	2020-10-12 10:46:30.330402	192.168.100.174	82.165.100.100	TLSv1	181	presseclub-magdebur…	Client Hello

Figure 9: SNIs reached by REvil

From having looked at multiple REvil samples, it appears that the TLS cipher suites (Figure 10) are always constant for any domain accessed by the ransomware.

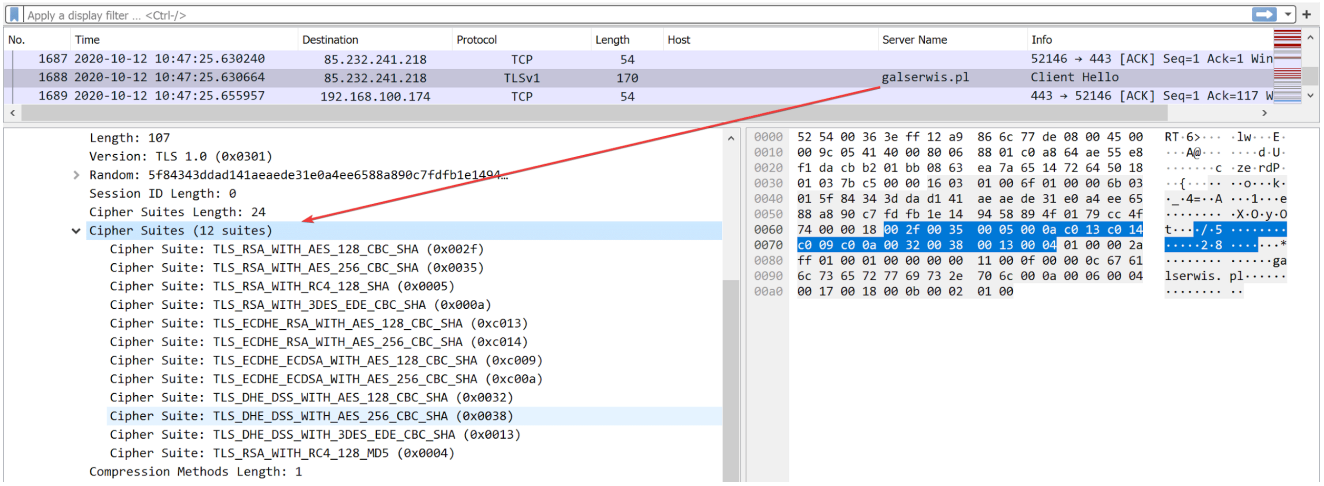

Figure 10: TLS cipher suites for domains accessed by REvil

Similarly, the TLS client extension codes also remain constant across all domains.

```
Compression Methods Length: 1
> Compression Methods (1 method)
Extensions Length: 49
v Extension: renegotiation_info (len=1)
    Type: renegotiation_info (65281)
    Length: 1
  v Renegotiation Info extension
      Renegotiation info extension length: 0
v Extension: server_name (len=24)
    Type: server_name (0)
    Length: 24
  > Server Name Indication extension
v Extension: supported_groups (len=6)
    Type: supported_groups (10)
    Length: 6
    Supported Groups List Length: 4
  > Supported Groups (2 groups)
v Extension: ec_point_formats (len=2)
    Type: ec_point_formats (11)
    Length: 2
```

Figure 11: TLS client extension codes for REvil C2 domains

The fact that the TLS fields are identical across all of the REvil session can be observed using TLS fingerprinting. This fact can be used with a technology like JA3 and can be fine tuned for true positives by using additional analytics. Specifically, the JA3 hash of the REvil traffic is **1d095e68489d3c535297cd8dffb06cb9.** However, simply relying on this hash is likely to lead to false positives**.** For instance, searching customer networks for the same JA3 hash showed *some* traffic that was clearly not ransomware (Figure 12).

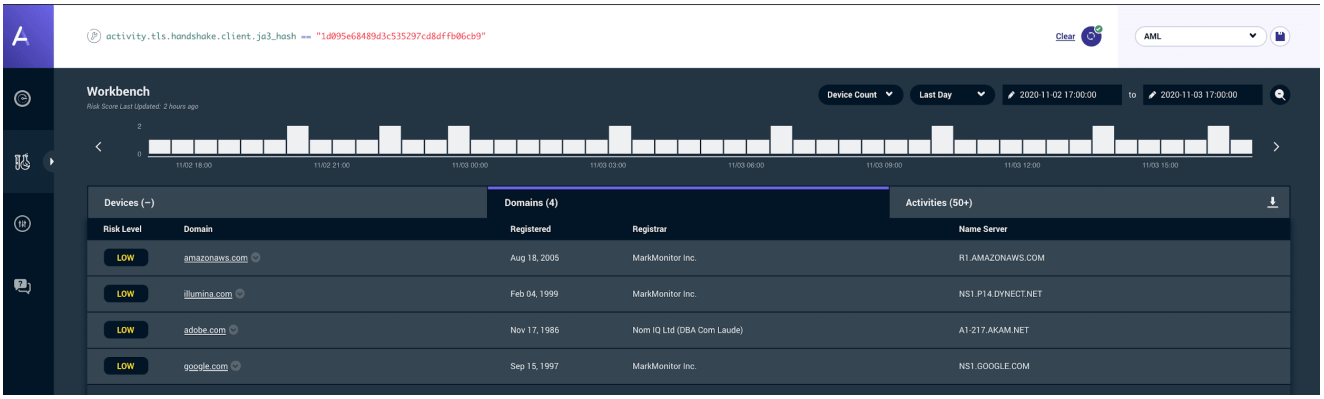

Figure 12: JA3 False Positive; Basespace AWS API Traffic

This is where deep security analytics can help. For instance, it is possible to identify devices within this list that have the behavior described above where thousands of different destinations are accessed in quick succession.

Within the Awake Security Platform, Ava, performs this analysis automatically for you much like an experienced threat hunter. For instance, Ava will automatically connect the dots across the different behaviors we described above to triage and narrow down to just the trust positives. Ava can also account for threat intelligence and open source intelligence indicators to confirm the compromise and recommend next steps for investigation and response. Finally, Ava can trigger response actions by integrating with the rest of the organization's security and IT infrastructure. Especially when dealing with ransomware, speed of remediation is of the essence and the automated triage, investigation and response that Ava brings to this process helps mitigate impact.

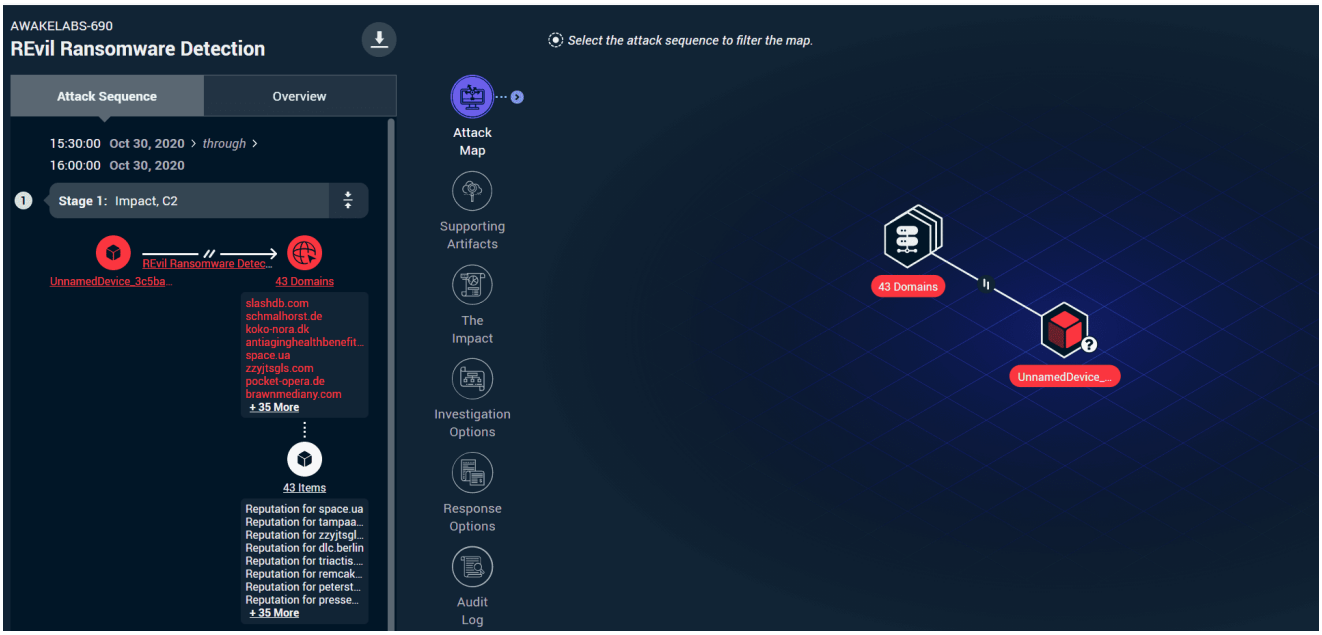

Figure 13: Awake Situation for REvil ransomware detection

Remediation

It is recommended to backup all important data to external drives or in the cloud for better security. Additionally, organizations should protect and monitor all the early vectors of ransomware. This includes protecting email and securely working with attachments especially from unknown sources as well as monitoring and protecting the entire attack surface e.g. externally exposed remote desktop or VPN services etc.. Finally, identify the sequence and patterns of communication we describe in this blog post and hunt for those to uncover the presence of REvil on your network.

References

Subscribe!

If you liked what you just read, subscribe to hear about our threat research and security analysis.

Ashish Gahlot

Threat Researcher

LinkedIn