SECURONIX™

Securonix Threat Research:

Detecting WastedLocker Ransomware Using Security Analytics

Oleg Kolesnikov
Securonix Threat Research Team
Created on: July 28, 2020
Last Updated: August 18, 2020

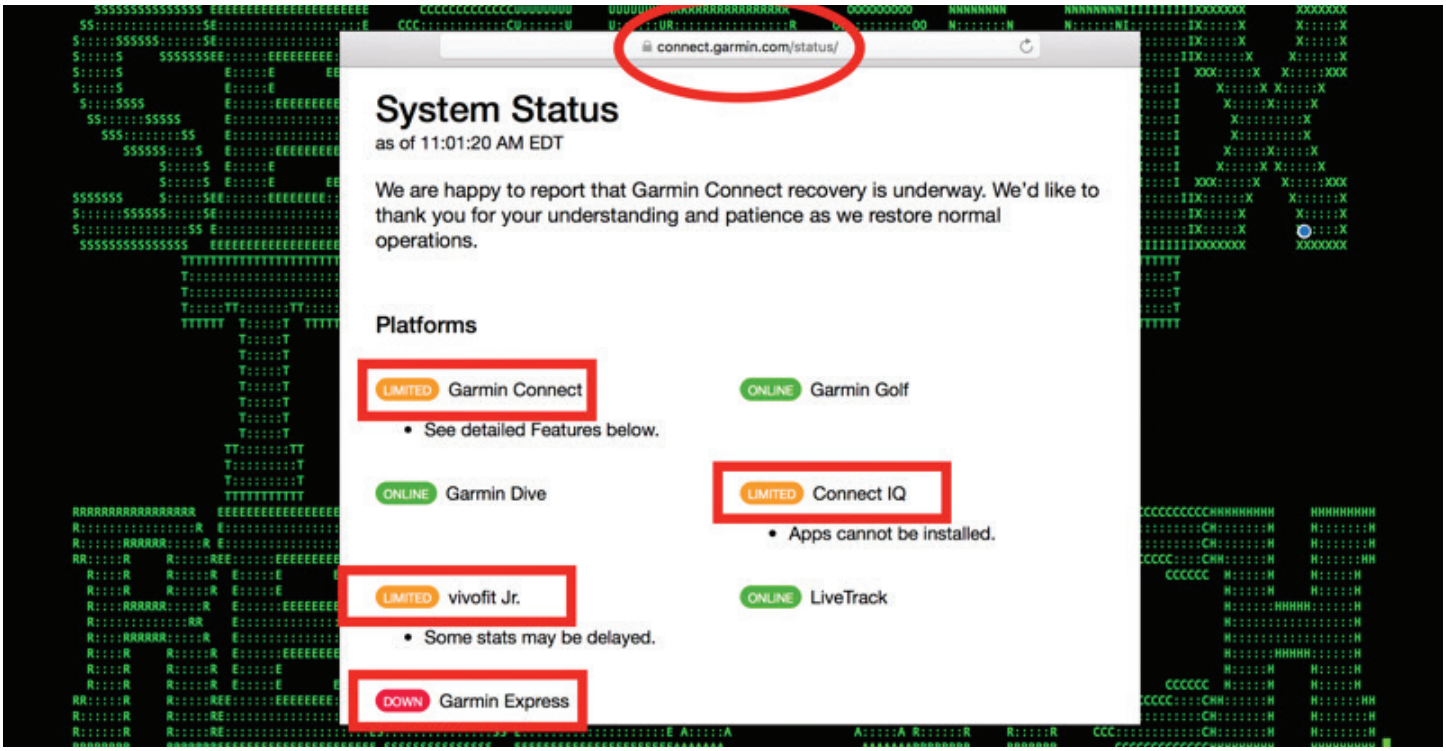

Figure 1: Victim's Systems Targeted by WastedLocker Unavailable (July 2020)

The Securonix Threat Research Team (STR) is actively investigating the details of the critical targeted Wastedlocker ransomware attacks that reportedly already exploited more than 31 companies, with 8 of the victims being Fortune 500 companies [1], to help our customers detect, mitigate, and respond to such attacks.

Here are some of the key technical details and our recommendations on possible Securonix predictive indicators/security analytics that can be used to detect the current and potentially future attack variants (these indicators may be updated as we receive more information.)

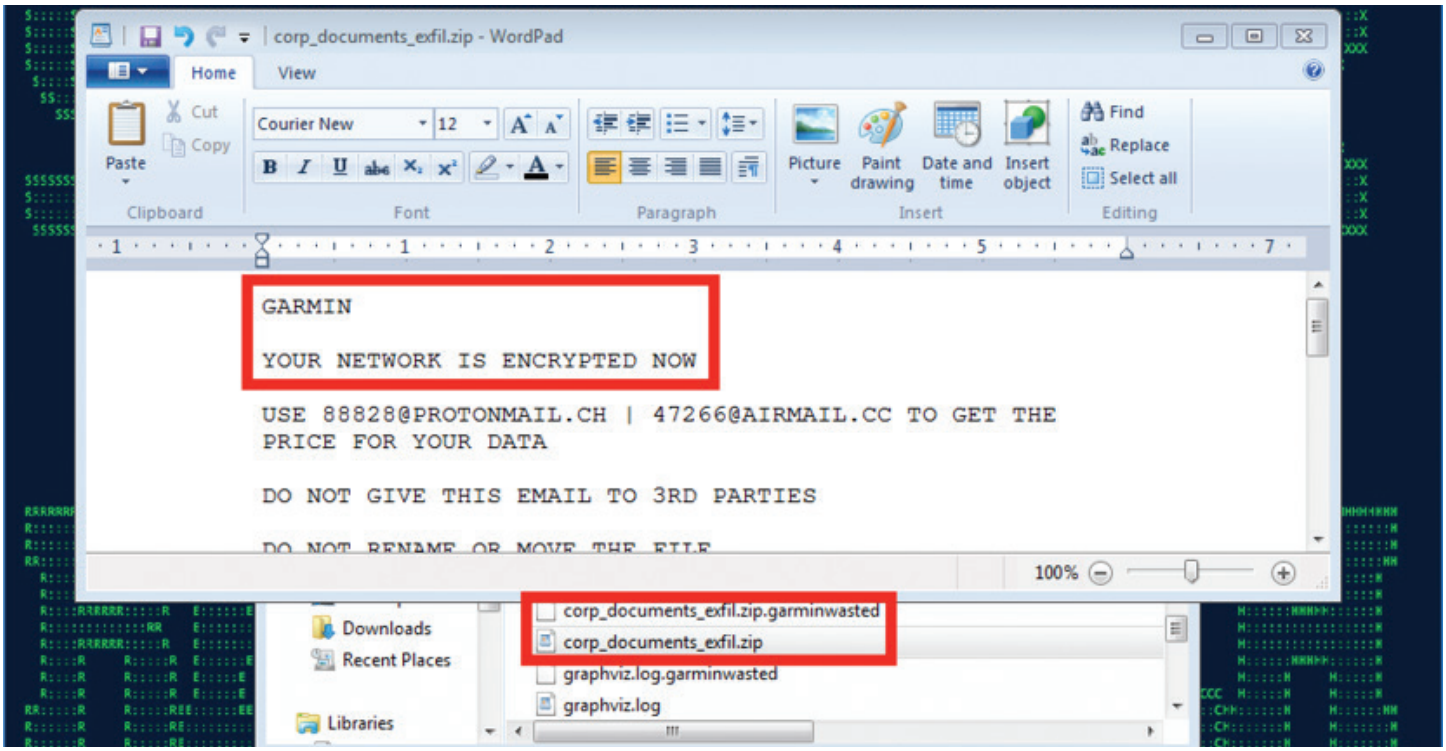

Figure 2: WastedLocker/EvilCorp Attack in Progress - Targeting a Victim Company in a Recent High-Profile Attack

Impact

Here are the key details regarding the impact of the high-profile WastedLocker ransomware attacks/ EvilCorp malicious cyber threat actor(s)(MTA) involved:

- The WastedLocker ransomware is a relatively new malicious payload used by the high-profile EvilCorp MTA, which previously used the Dridex trojan to deploy BitPaymer ransomware in attacks targeting government organizations and enterprises in the United States and Europe. (See Figure 1)
- This MTA currently focuses on targeted "big game hunting" (BGH) ransomware attacks with multiple industry victims in recent months, with Garmin as one of the latest high-profile victims attacked (officially confirmed by Garmin on July 27). (See Figure 2)
- The most recent ransom amount demanded was US$10M and appears to be based on the victim's financial data. Based on the available details, the ransom was likely paid [3]. (See Figure 3)
- To date, this MTA appears to have been using a mono-extortion scheme (data encryption only, with no or minimal data leakage) vs. other MTAs who use the threat of leaking a victim's data as part of a double-extortion scheme (such as, e.g. Netwalker, Maze, and others). However, based on our monitoring of this MTAs capabilities, this can likely be easily added in future attacks.

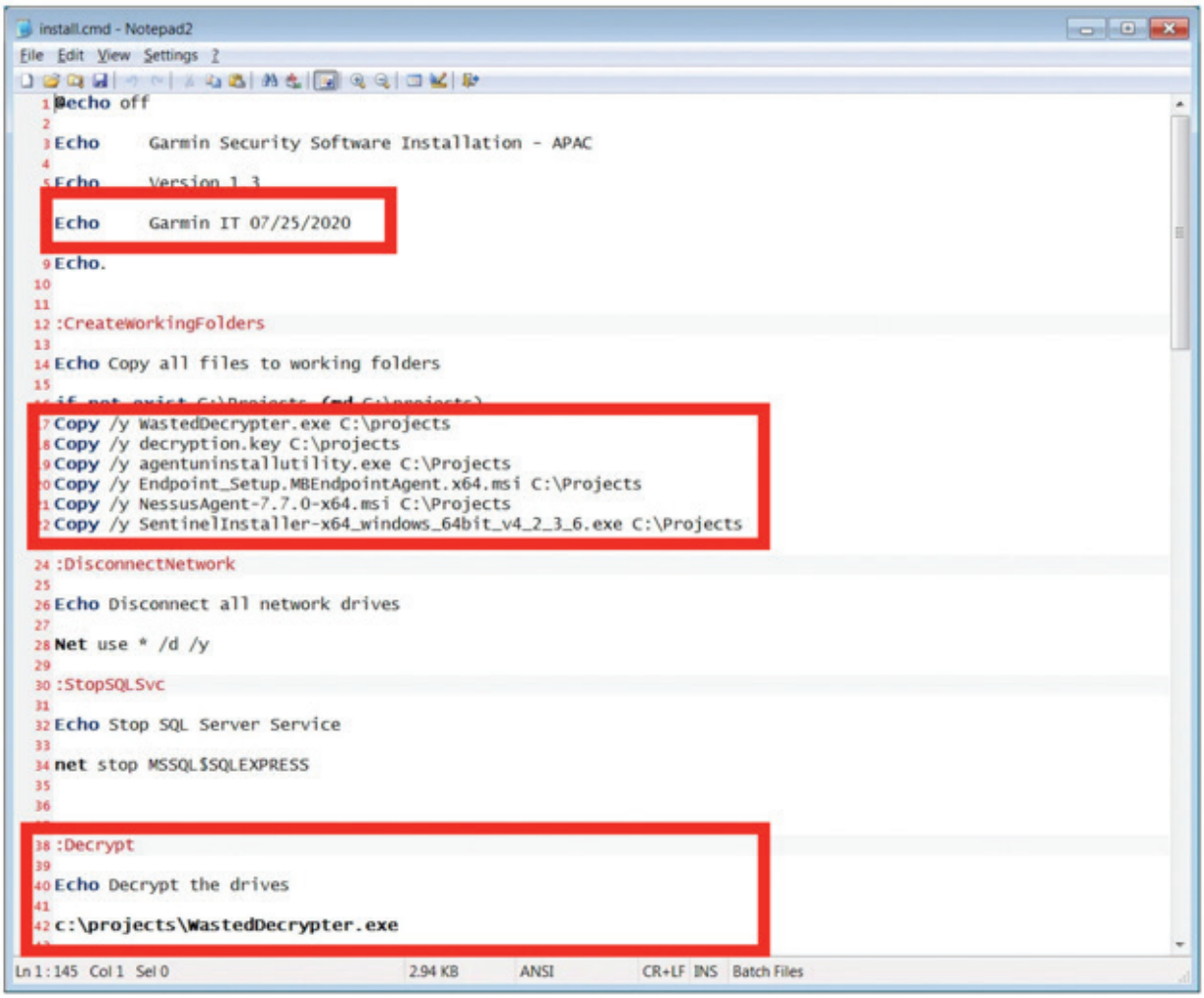

Figure 3: Victim Systems' Recovery Using Custom Utility & Decryption Key After Reported Ransom Payment to WastedLocker/EvilCorp [3]

Some Examples of Observed ATT&CK Techniques

- T1082 - System Information Discovery
- T1018 - Remote System Discovery
- T1003 - OS Credential Dumping
- T1089 - Disabling Security Tools
- T1127 - Trusted Developer Utilities Proxy Execution
- T1113 - Screen Capture
- T1189 - Drive-by Compromise
- T1500 - Compile After Delivery
- T1035 - Service Execution
- T1098 - Account Manipulation
- T1086 - PowerShell

- T1214 - Credentials in Registry
- T1047 - Windows Management Instrumentation
- T1057 - Process Discovery
- T1070 - Indicator Removal on Host
- T1077 - Windows Admin Shares
- T1087 - Account Discovery
- T1564 - Hidden Files and Directories/NTFS File Attributes
- T1569 - Service Execution
- T1548 - BypassUAC
- T1106 - Native API
- T1490 - Inhibit System Recovery
- T1059 - Command and Scripting
- T1222 - Permissions Modification
- T1486 - Data Encrypted for Impact

and others.

Some Examples of Observed Attack Artifacts/Payloads

In addition to the relatively wide range of technical attack capabilities/techniques employed by MTA, there are also a large number of attack/artifact variants associated with the EvilCorp MTA attacks, and new variants appear regularly, particularly because of the focus on defense evasion. Some of the artifacts observed to date include:

905ea119ad8d3e54cd228c458a1b5681abc1f35df782977a23812ec4efa0288a
3dfb4e7ca12b7176a0cf12edce288b26a970339e6529a0b2dad7114bba0e16c3
c786e4de11e64be8d4118cf8ba6b210e3396e3bb579f3afd4bf528c35bab4a6b
7a45a4ae68992e5be784b4a6da7acd98dc28281fe238f22c1f7c1d85a90d144a
bcdac1a2b67e2b47f8129814dca3bcf7d55404757eb09f1c3103f57da3153ec8
91b2bf44b1f9282c09f07f16631deaa3ad9d956d
70c0d6b0a8485df01ed893a7919009f099591083
2000de399f4c0ad50a26780700ed6cac
db908077689613c483bcdf037f211d0e3369ff12
5e5e62ff09ee59fd7d17f79ef2c726ed1c1fc26f
31a57376158d926ae4cfa0574143d7ee
2b3efa7882c674f4ae57dea991ff5014
83710bbb9d8d1cf68b425f52f2fb29d5ebbbd05952b60fb3f09e609dfcf1976c
JA3: d124ae14809abde3528a479fe01a12bd
advokat-hodonin.info
cofeedback.com

net-giftshop.info
msoftwares.info
websitesbuilder.info
rostraffic.com
consultane.com
feedbackgive.com
penaz.info
traffichi.com
mwebsoft.com
typiconsult.com
lgrarcosbann.club
dns.proactiveads.be
https://szn.services/1.exe
http://transvil2.xyz/index.php
http://lendojekam.xyz/index.php
https://utenti.live/1.exe
https://utenti.info/1.exe
https://triomigratio.xyz
https://uplandcaraudio.xyz
https://guiapocos.xyz
http://flablenitev.site/index.php
https://woofwoofacademy.xyz
https://respondcritique.xyz
http://paiolets.com/install.exe
https://ludwoodgroup.xyz
https://devicelease.xyz
http://lpequdeliren.fun/index.php
respondcritique.xyz
devicelease.xyz

and many others.

(A comprehensive list of static artifacts, including [imp]hashes, can be found in other researchers' work [3, 4, 5], and is out of scope for this advisory.)

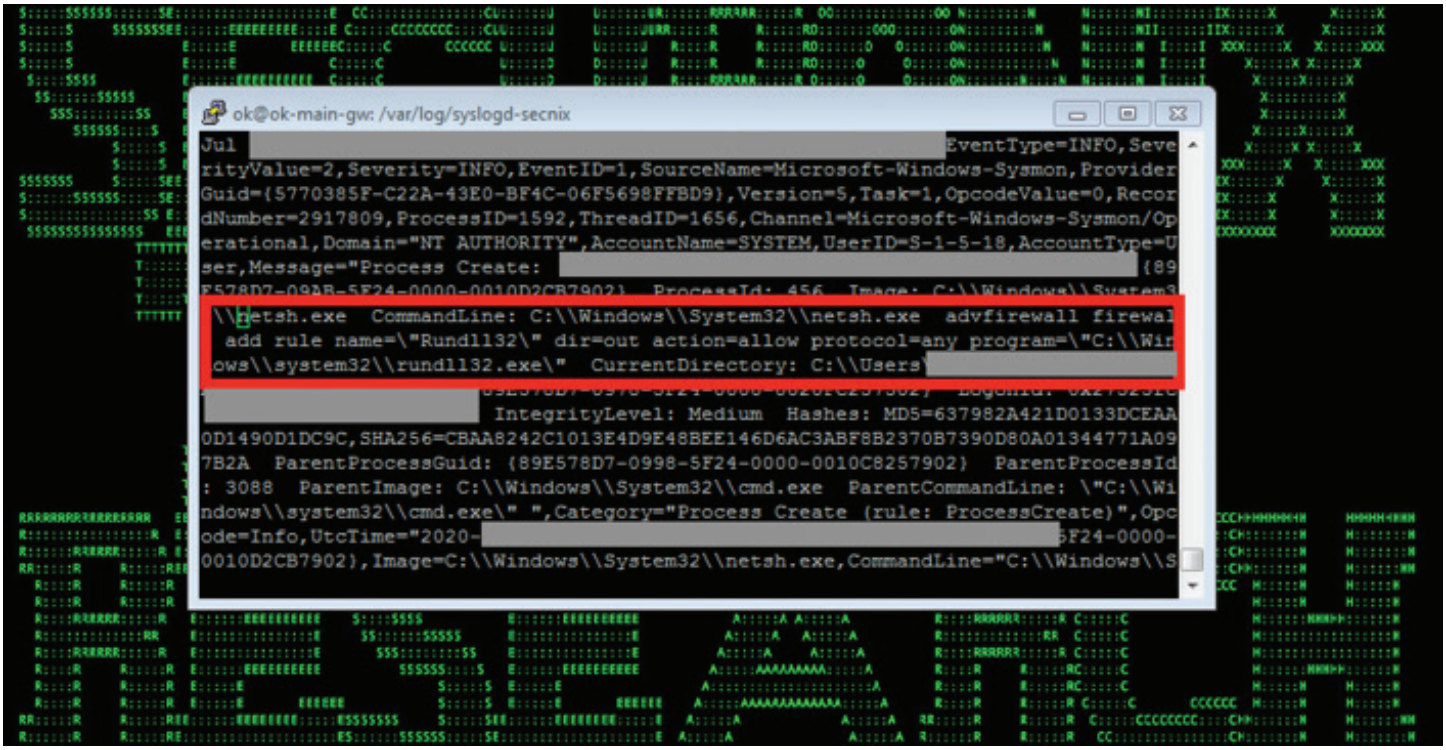

Figure 4: Example of WastedLocker/EvilCorp Malicious Activity (New Firewall Rule Creation) in Logs

WastedLocker/EvilCorp - Some Common Attack Progression/Behaviors Highlights

Following the initial compromise, one of the early steps commonly taken by the malicious operators observed is to perform internal discovery and disable security/AV vendor tools such as Cisco AMP and/or Windows Defender (ATT&CK T1089) [4]. Often this involves variations of the following commands:

- reg save HKLM\SAM C:\programdata\SamBkup.hiv
- reg save HKLM\SYSTEM C:\programdata\FileName.hiv
- C:\Windows\System32\cmd.exe /C whoami /all
- C:\Windows\system32\taskkill.exe /F /IM sfc.exe
- :\Program Files\Windows Defender\MpCmdRun.exe -RemoveDefinitions -All Set-MpPreference -DisableIOAVProtection $true
- C:\Windows\system32\cmd.exe /C C:\Program Files\Cisco\AMP\7.2.7\sfc.exe -stop
- C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\14.2.5323.2000.105\Bin\Smc.exe -disable -sep
- C:\Windows\system32\taskkill.exe /F /IM sfc.exe

and others.

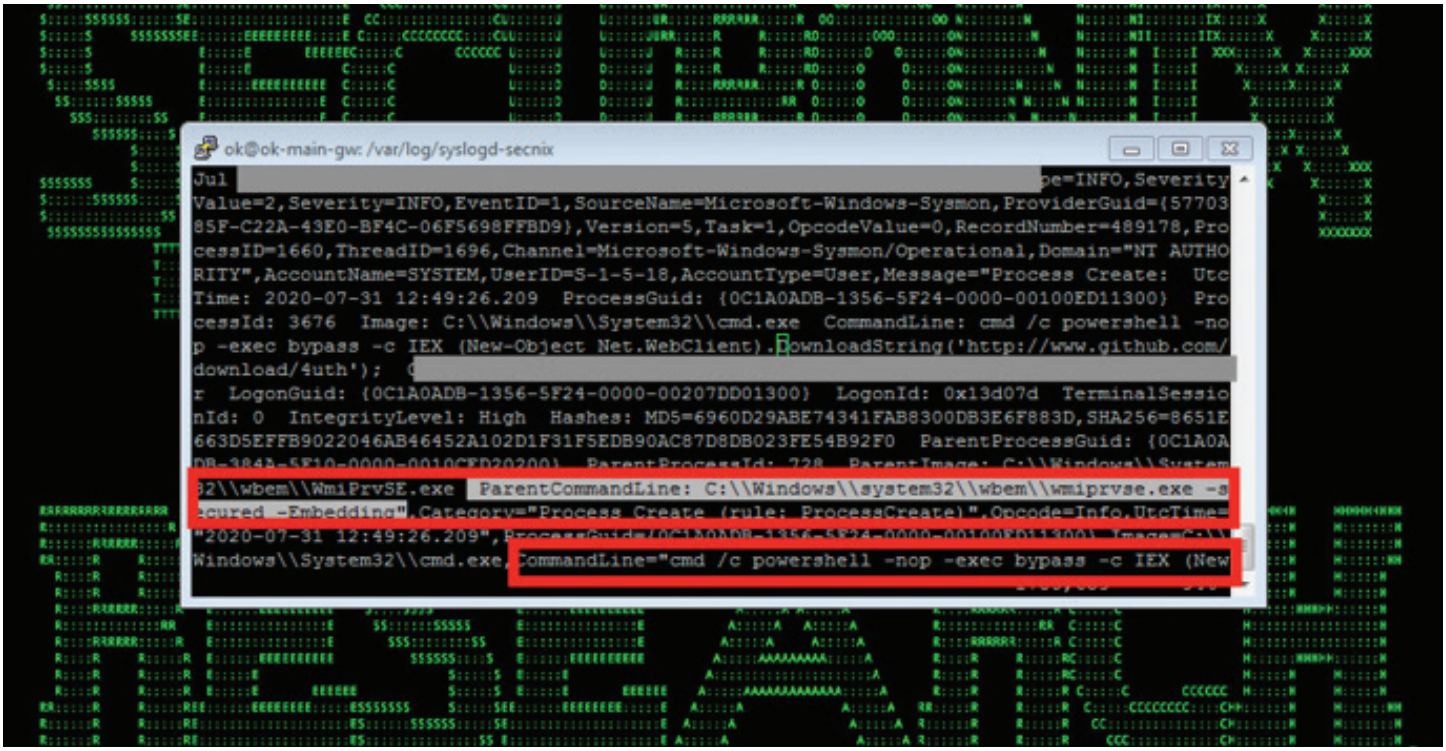

Figure 5: Example of WastedLocker/EvilCorp Malicious Activity (Lateral Movement Using WMI/Powershell) in Logs

Following the initial compromise and the internal discovery/disabling security tools steps mentioned above, the typical attack progression involves further defense evasion (for instance, using NTFS alternate data streams e.g. during threat hunting, one might see a 4688 event with a NewProcessName process named as - *\\AppData\\Roaming\\Wcncsvc:bin), UACBypass, firewall compromise/rule changes (see Figure 4), compiling targeted payloads on-the-fly using LOLBINS/cvc/cvtres, evasion using .NET injection, lateral movement ranging from trivial PSEXEC to basic staging via WMI/powershell (see Figure 5).

The final stage often involves disabling shadow copies and stopping some of the critical/backup/SQL services, e.g.

- stop NetBackup BMR MTFTP Service /y
- stop BMR Boot Service /y
- config SstpSvc start= disabled
- config SQLTELEMETRY start= disabled
- config SQLWriter start= disabled

and deploying the malicious ransomware implant (usually persistent as a service/registry),

performing some basic automated evasion/file attribute resets and encryption of the sensitive data. The resets are performed by the malicious ransomware implant service, e.g. using commands such as:

- cmd /c choice /t 10 /d y & attrib -h \"C:\\Windows\\SysWOW64\\Wcncsvc.exe\" & del \"C:\\Windows\\SysWOW64\\Wcncsvc.exe\""
- takeown, icacls.exe

and others.

The encryption process itself involves behaviors that aim at evading anti-ransomware solutions and optimizing performance, including using memory-mapped I/O as part of file encryption [6]. However, in our experience, the threat hunting/log detection artifacts associated with the ransomware encryption process and the associated file writes are typically still present and usually are detectable in the logs.

Detection - Sample Spotter Search Queries

Please find below some examples of the trivial Spotter queries to assist with initial threat hunting/identifying some possible attack behaviors based on the details above.

Note: Because of the rapidly changing attack landscape, the recommendation is not to rely on static IOAs/queries and to implement the use cases/predictive indicators for the best possible protection (see next section).

EDR Process Monitoring

Initial infiltration via fake update (many other vectors possible)

resourcegroupname = “Microsoft Sysmon” and deviceaction = “Process Create” and resourcecustomfield1 contains .js and resourcecustomfield1 contains wscript and resourcecustomfield1 contains “Chrome.Update”

FW hole punching

resourcegroupname = “Microsoft Sysmon” and deviceaction = “Process Create” and resourcecustomfield1 contains “dir=out action=allow protocol=any” and resourcecustomfield1 contains “firewall add rule”

AV tool disabling

resourcegroupname = “Microsoft Sysmon” and deviceaction = “Process Create” and resourcecustomfield1 contains “Set-MpPreference -DisableBehaviorMonitoring”

NTFS stream evasion

resourcegroupname = “windows” and baseeventid = 4688 and sourceprocessname contains “:bin”

Shadow copy disabling

resourcegroupname = “Microsoft Sysmon” and deviceaction = “Process Create” and resourcecustomfield1 contains “Delete Shadows /all /quiet”

AV tool disabling

resourcegroupname = “Microsoft Sysmon” and deviceaction = “Process Create” and resourcecustomfield1 contains “WinDefend start= disabled”

Locked file creation

resourcegroupname = “Microsoft Sysmon” and and deviceaction contains “File Create” and resourcecustomfield5 contains wasted | stats count by sourcehostname

ETDR Process Monitoring (Process Hash Conditions)

(rg_category contains “Endpoint” OR rg_category contains “ips” OR rg_category contains “ids”) AND (customstring3=905ea119ad8d3e54cd228c458a1b5681abc1f35df782977a23812ec4efa0288a or customstring3=3dfb4e7ca12b7176a0cf12edce288b26a970339e6529a0b2dad7114bba0e16c3 or customstring3=c786e4de11e64be8d4118cf8ba6b210e3396e3bb579f3afd4bf528c35bab4a6b or customstring3=7a45a4ae68992e5be784b4a6da7acd98dc28281fe238f22c1f7c1d85a90d144a or customstring3=bcdac1a2b67e2b47f8129814dca3bcf7d55404757eb09f1c3103f57da3153ec8 or customstring3=91b2bf44b1f9282c09f07f16631deaa3ad9d956d or customstring3=70c0d6b0a8485df01ed893a7919009f099591083 or customstring3=2000de399f4c0ad50a26780700ed6cac or customstring3=db908077689613c483bcdf037f211d0e3369ff12 or customstring3=5e5e62ff09ee59fd7d17f79ef2c726ed1c1fc26f or customstring3=31a57376158d926ae4cfa0574143d7ee or customstring3=2b3efa7882c674f4ae57dea991ff5014 or customstring3=83710bbb9d8d1cf68b425f52f2fb29d5ebbbd05952b60fb3f09e609dfcf1976c)

Mitigation and Prevention - Securonix Recommendations

Here are some of the Securonix recommendations to help customers prevent and/or mitigate the attack:

1. Review your backup version retention policies and make sure that your backups are stored in a location that cannot be accessed/encrypted by operator placed targeted ransomware, (e.g. consider remote write-only backup locations).
2. Implement an end user security training program, since end users are ransomware targets. It is important for them to be aware of the threat of ransomware and how it occurs.
3. Patch operating systems, software, and firmware on your infrastructure. Consider leveraging a centralized patch management system.
4. Maintain regular air-gapped backups of critical corporate/infrastructure data.
5. Implement security monitoring, particularly for high-value targets (HVT) in your environments, to detect possible malicious ransomware operator placement activities earlier.
6. For your Windows systems, consider enabling and auditing controlled folder access/turn on the protected folders feature – see https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/enable-controlled-folders-exploit-guard

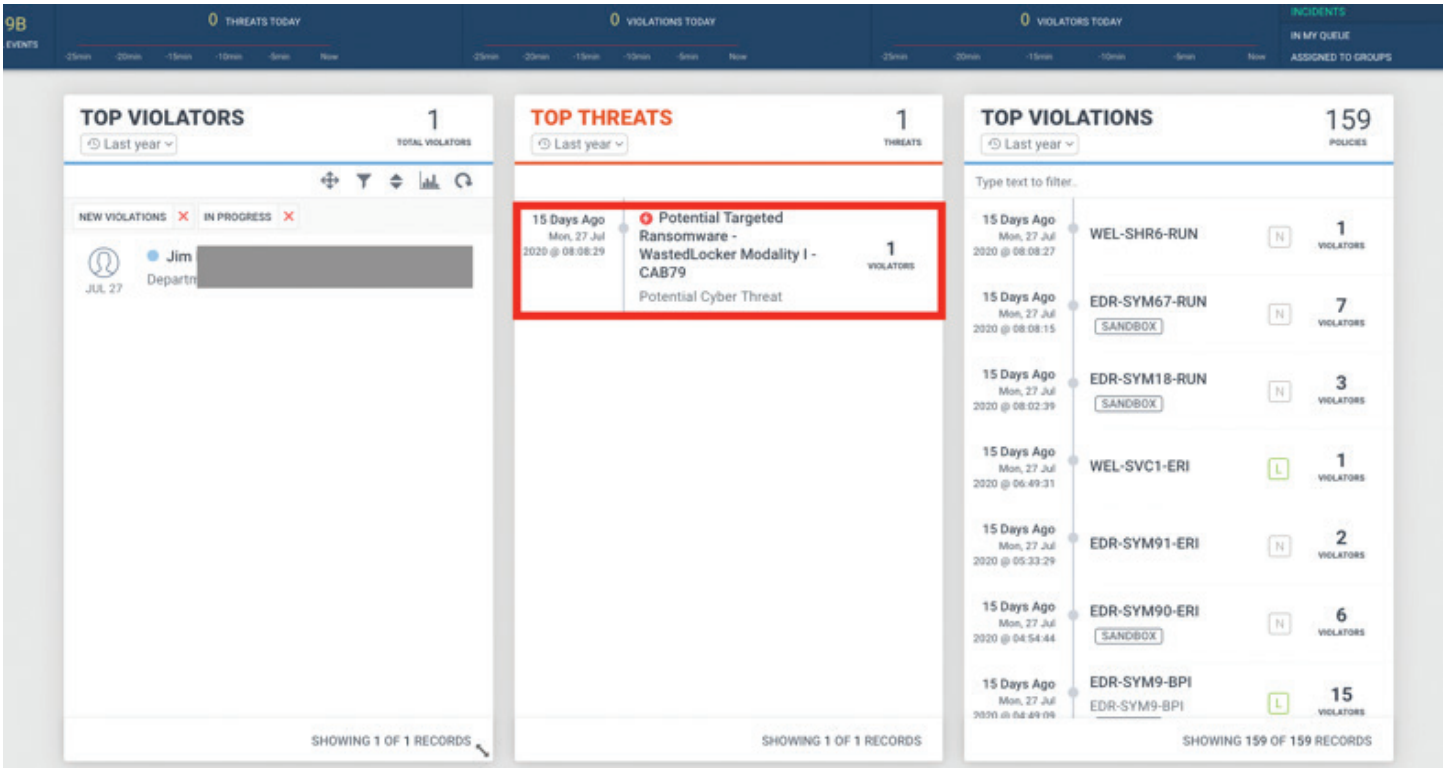

Figure 6: Example of the Malicious Threat Detection in Securonix Labs

Detection Using Security Analytics – Some Examples of Securonix Predictive Indicators

Here are some high-level examples of some of the relevant Securonix behavior analytics/predictive indicators to increase the chances of early detection of the malicious activity associated with the WastedLocker/EvilCorp MTA, and potentially other future variants of attacks:

- Possible Initial Infiltration Via Fake Chrome Update
- Rare Image For CLR Executable Load Potential Donut CLR Injection
- Potential PSEXEC Activity
- Rare WMI Exec Process Potential Lateral Movement
- NTFS File Attribute Hidden Artifact Executable Creation
- Rare Service Creation For User Analytic
- Potential Log Clearing
- Potential Defense Evasion Interference/Disabling Antivirus Tools
- Executable File/Script Creation Analytic

and a number of others, including AVI-WDF2-RUN, EDR-SYM9-BPI, EDR-SYM90-ERI, EDR-SYM91-ERI, WEL-SVC1-ERI, EDR-SYM18-RUN, EDR-SYM67-RUN, WEL-SHR6-RUN, EDR-SYM93-RUN, WEL-OTH1-RUN, WEL-PSH12-RUN, et al.

Some examples of successful detection of these real-world attacks in practice in Securonix Labs are shown in Figure 6.

References

[1] Garmin. Ransomware Outage Press Release. July 27, 2020. https://newsroom.garmin.com/newsroom/press-release-details/2020/Garmin-issues-statement-on-recent-outage/default.aspx

[2] Kolesnikov et al. Securonix Threat Research: Detecting High-Impact Targeted Cloud/MSP $14M+ Ryuk and REvil Ransomware Attacks. January 3, 2020. https://www.securonix.com/securonix-threat-research-detecting-high-impact-targeted-cloud-msp-14m-ryuk-and-revil-ransomware-attacks/

[3] Lawrence Abrams. BleepingComputer: Confirmed: Garmin received decryptor for WastedLocker ransomware. August 1, 2020. https://www.bleepingcomputer.com/news/security/confirmed-garmin-received-decryptor-for-wastedlocker-ransomware/.

[4] Ben Baker et al. WastedLocker Goes "Big-Game Hunting" in 2020. July 6, 2020. https://blog.talosintelligence.com/2020/07/wastedlocker-emerges.html.

[5] Jim Walter. WastedLocker Ransomware: Abusing ADFS and NTFS File Attributes. July 23, 2020. https://labs.sentinelone.com/wastedlocker-ransomware-abusing-ads-and-ntfs-file-attributes/

[6] 6 Labs. WastedLocker's techniques point to a familiar heritage. August 4, 2020. https://news.6.com/en-us/2020/08/04/wastedlocker-techniques-point-to-a-familiar-heritage/.

About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, SOAR, Security Data Lake, NTA, and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise, prioritizes high fidelity alerts, and detects and responds to advanced insider and cyber threats with behavioral analytics technology that pioneered the UEBA category.

Contact Securonix

www.securonix.com
info@securonix.com | (310) 641-1000

0820


SECURONIX™