SECURONIX™

Securonix Threat Research:

Detecting LockerGoga Targeted IT/OT Cyber Sabotage/Ransomware Attacks

Oleg Kolesnikov and Harshvardhan Parashar
Securonix Threat Research Team

LAST UPDATED: APRIL 30, 2019

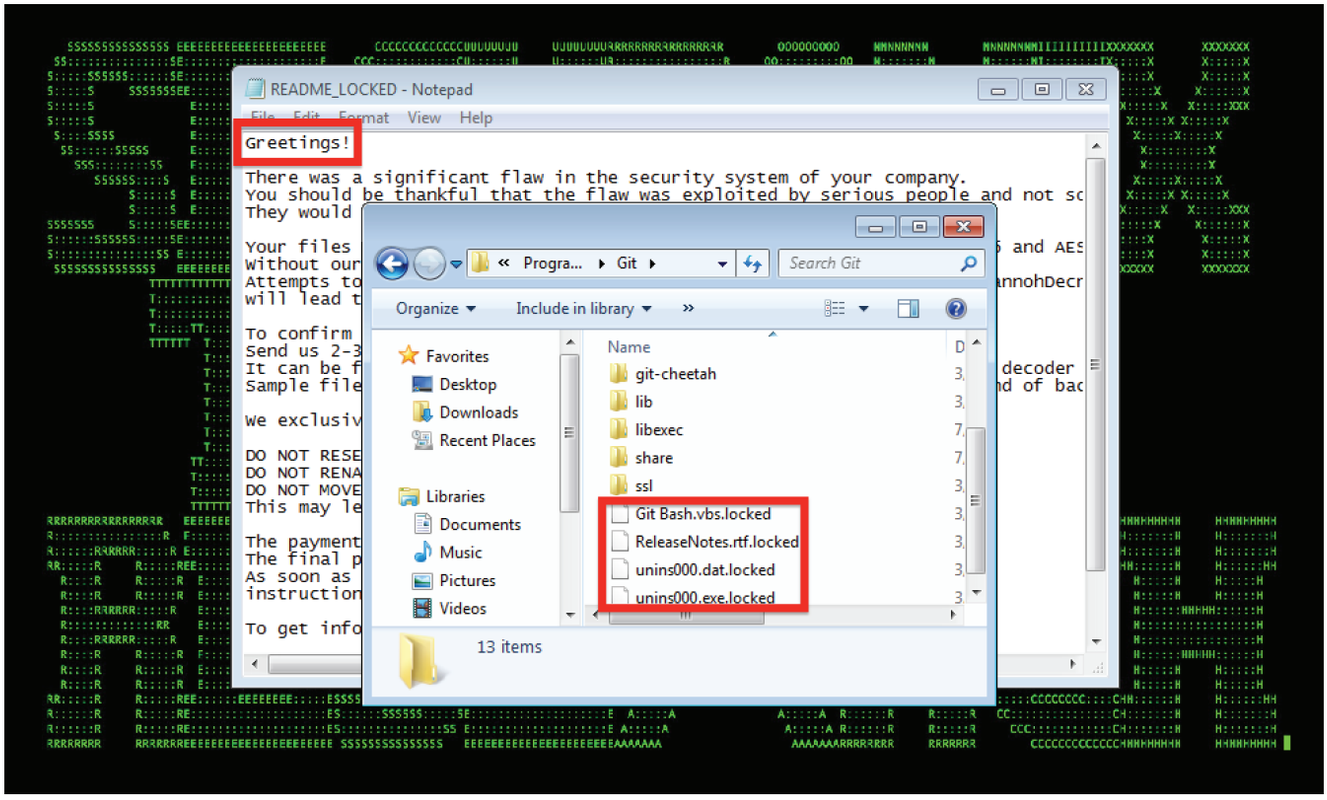


Figure 1: LockerGoga Targeted Malicious Cyber Sabotage/Ransomware Implant in Action

Introduction

The Securonix Threat Research Team has been closely monitoring the LockerGoga targeted cyber sabotage/ransomware (TC/R) attacks impacting Norsk Hydro (one of the largest aluminum companies worldwide), Hexicon/Momentive (a chemical manufacturer), and other companies' IT and operational technology (OT) infrastructure, causing over US$40 million in damages [1][2].

In this report is a summary of what we currently know about these high-profile attacks and our recommendations for some Securonix predictive indicators and security analytics to use to increase your chances of detecting such attacks targeting industrial operations and operational technology companies.

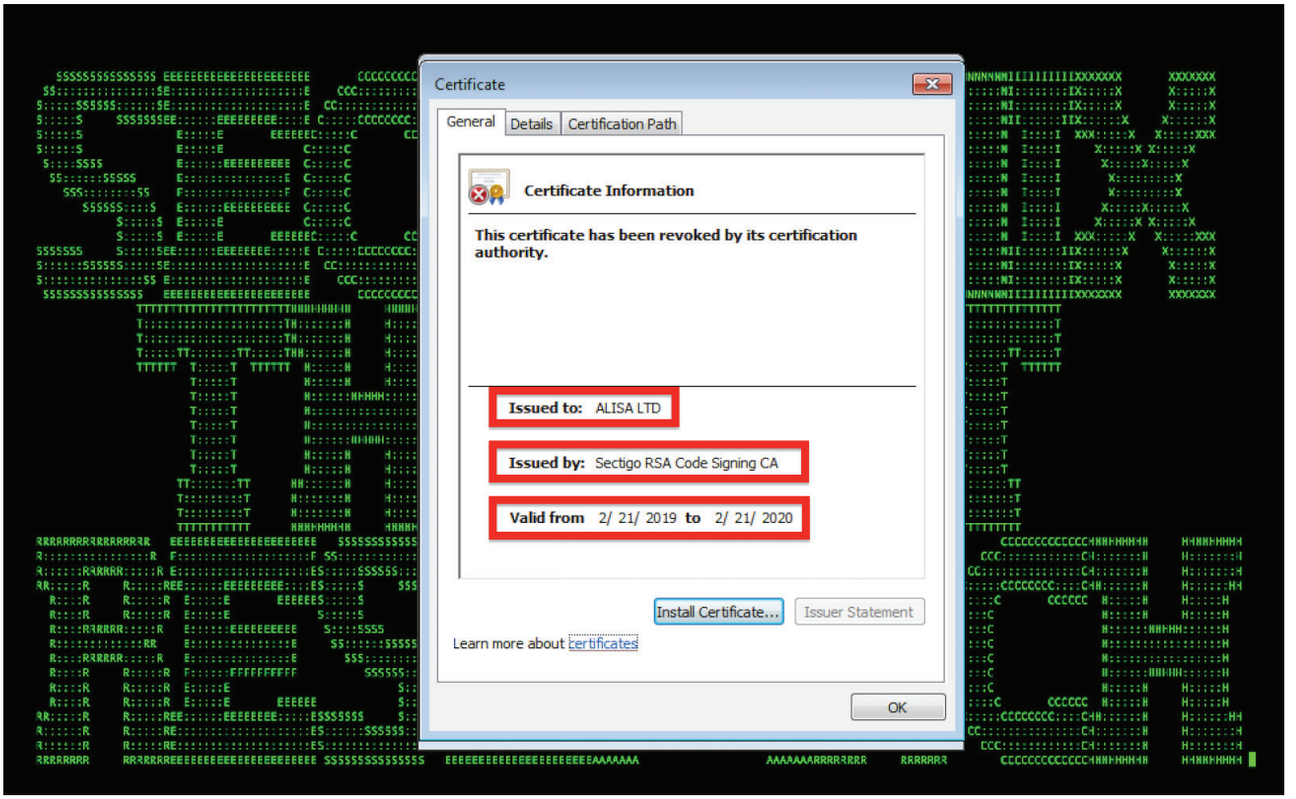


Figure 2: LockerGoga Digital Certificate Used to Evade EDR Detection

Summary

Here is a summary of some of the key details about some of the LockerGoga TC/R attack attacks we have been observing:

Impact

Caused the temporary shutdown of production networks, forcing companies to switch to manual operations and procedures. The financial impact for one of the largest targets, Norsk Hydro, is estimated to be between US$35 million and $41 million [5].

Infiltration Vector(s)

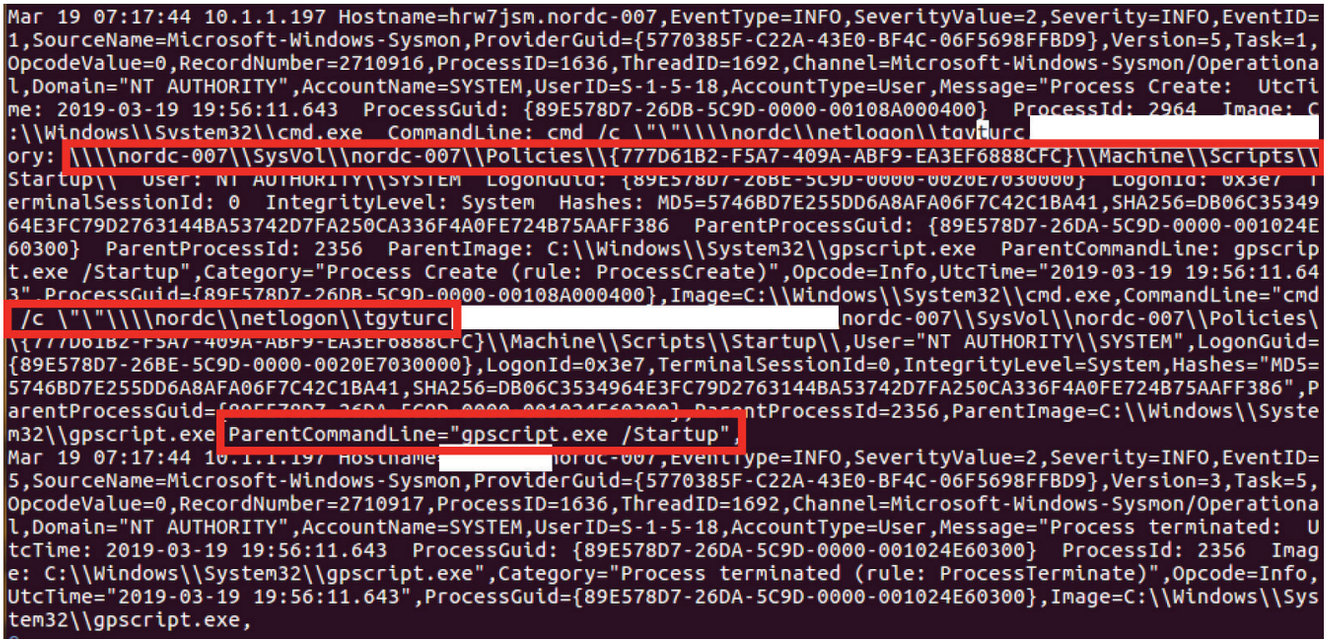
Unconfirmed; possibly a phishing email campaign containing specially crafted Microsoft Word documents or RTF attachments with macro/OLE content.

Attribution

LockerGoga is currently attributed to the FIN6 malicious threat actor [13]. In addition to industrial/manufacturing companies, the malicious threat actor is also known to target healthcare and insurance companies in the US and Asia [15].

Defense Evasion

LockerGoga payloads are signed with a valid digital certificate issued by multiple certificate authorities (CA) – namely Alisa Ltd., Kitty Ltd., and Sectigo and Mikl Limited – which allowed the LockerGoga TC/R attacks to evade detection. Some LockerGoga variants are also known to leverage the 'taskkill' command to disable antivirus (AV) and endpoint detection processes [6]. Some variants of the LockerGoga TC/R attack are capable of deleting windows event logs using wevtutil.exe [3].



Propagation

Most likely required operator placement, with the LockerGoga malicious threat actors observed moving the payload around the network using SMB [7]. In some incidents, the actors have also been using Active Directory management services to distribute the payload in the network. Specifically, the malicious binaries were believed to be distributed using the NETLOGON directory of the Domain Admin Group account which allowed the binaries to automatically propagate (more details below) [11].

Observed Artifacts

Hash Values (SHA-256) [7]

ae7e9839b7fb750128147a9227d3733dde2faacd13c478e8f4d8d6c6c2fc1a55
f474a8c0f66dee3d504fff1e49342ee70dd6f402c3fa0687b15ea9d0dd15613a
ffab69deafa647e2b54d8daf8c740b559a7982c3c7c1506ac6efc8de30c37fd5
c1670e190409619b5a541706976e5a649bef75c75b4b82caf00e9d85afc91881
65d5dd067e5550867b532f4e52af47b320bd31bc906d7bf5db889d0ff3f73041
31fdce53ee34dbc8e7a9f57b30a0fbb416ab1b3e0c145edd28b65bd6794047c1
32d959169ab8ad7e9d4bd046cdb585036c71380d9c45e7bb9513935cd1e225b5
e00a36f4295bb3ba17d36d75ee27f7d2c20646b6e0352e6d765b7ac738ebe5ee
6d8f1a20dc0b67eb1c3393c6c7fc859f99a12abbca9c45dcbc0efd4dc712fb7c
79c11575f0495a3daaf93392bc8134c652360c5561e6f32d002209bc41471a07
050b4028b76cd907aabce3d07ebd9f38e56c48c991378d1c65442f9f5628aa9e
1f9b5fa30fd8835815270f7951f624698529332931725c1e17c41fd3dd040afe
276104ba67006897630a7bdaa22343944983d9397a538504935f2ec7ac10b534
88d149f3e47dc337695d76da52b25660e3a454768af0d7e59c913995af496a0f
c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15
06e3924a863f12f57e903ae565052271740c4096bd4b47c38a9604951383bcd1
a845c34b0f675827444d6c502c0c461ed4445a00d83b31d5769646b88d7bbedf
7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d723a80c08dd26
ba15c27f26265f4b063b65654e9d7c248d0d651919fafb68cb4765d1e057f93f
eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0
7852b47e7a9e3f792755395584c64dd81b68ab3cbcdf82f60e50dc5fa7385125
14e8a8095426245633cd6c3440afc5b29d0c8cd4acefd10e16f82eb3295077ca
47f5a231f7cd0e36508ca6ff8c21c08a7248f0f2bd79c1e772b73443597b09b4
f3c58f6de17d2ef3e894c09bc68c0afcce23254916c182e44056db3cad710192
9128e1c56463b3ce7d4578ef14ccdfdba15ccc2d73545cb541ea3e80344b173c
c3d334cb7f6007c9ebee1a68c4f3f72eac9b3c102461d39f2a0a4b32a053843a
6e69548b1ae61d951452b65db15716a5ee2f9373be05011e897c61118c239a77
8cfbd38855d2d6033847142fdfa74710b796daf465ab94216fbbbe85971aee29
bdf36127817413f625d2625d3133760af724d6ad2410bea7297ddc116abc268f
5b0b972713cd8611b04e4673676cdff70345ac7301b2c23173cdfeaff564225c
c7a69dcfb6a3fe433a52a71d85a7e90df25b1db1bc843a541eb08ea2fd1052a4

LockerGoga T/CR Attacks: High-Level Behaviors

Ransomware

At a high level, the LockerGoga TC/R attacks aim at encrypting files with the extensions: .doc, .dot, .docx, .docb, .dotx, .wkb, .xlm, .xml, .xls, .xlsx, .xlt, .xltx, .xlsb, .xlw, .ppt, .pps, .pot, .ppsx, .pptx, .posx, .potx, .sldx, .pdf, .db, .sql, .cs, .ts, .js, and .py. The attacks use the embedded RSA-1024 public key in the binaries to encrypt the AES-256 key used to encrypt the individual files. The encrypted files are stored with extension *.LOCKED.

Cyber Sabotage

Besides encrypting files, some LockerGoga variants include code that actually made it harder for the victims to pay ransom. This is done by changing administrator passwords and logging users off using logoff.exe (see below). This indicates that the attackers objectives' may have included additional goals that are not part of a traditional ransomware modus operandi, such as cyber sabotage.

Lateral Movement

While the known variants of LockerGoga do not appear to include code to enable lateral movement, according to NorCert, the threat actors were able to move laterally, infecting the entire organization. The most likely attack progression was that an initial compromise was followed by manual operator placement and modification of one of the existing logon script entries in the Netlogon directory on an AD resource, for example \WINDOWS\sysvol\sysvol\<DOMAIN>\scripts, which allowed the binary to automatically propagate and be executed by users within the organization during a logon session. It is also possible that the threat actors created a new logon script and added a new logon GPO entry to execute the binary on all of the systems applying the logon script to the organizational unit or the complete organization (see Figure 4).

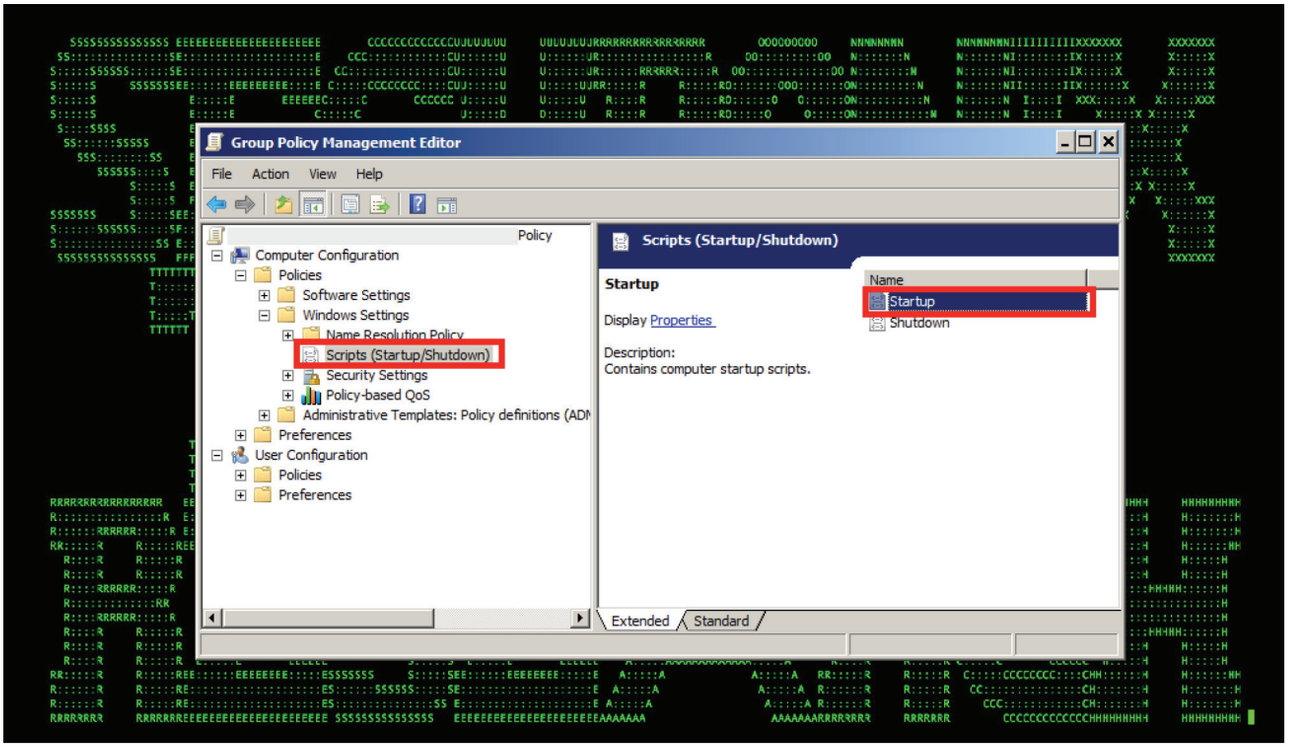


Figure 4: Logon Scripts Likely Utilized by LockerGoga for Lateral Movement

File Encryption

As soon as the endpoint is infected with the LockerGoga TC/R attack payload, the payload is moved to %TEMP% directory and executes a master/parent process which enumerates files on the endpoint and spawns slave/child processes to encrypt the individual files [8]. A high number of worker processes is known to be spawned by this threat in order to leverage additional CPU resources available on targets with multiple processors/cores.

Password Modification

LockerGoga variants are known to modify the password of the administrator accounts to HuHuHUHoHo283283@dJD and run logoff.exe in order to force a log off of the users and locking them out. LockerGoga also enumerates all the Ethernet and wireless interfaces on the endpoint and disables them using the CreateProcessW function via command line (netsh.exe interface set interface DISABLE) to isolate the endpoint [9].

Defense Evasion

Some LockerGoga variants are known to utilize trivial defense evasion techniques, including basic anti-VM and anti-sandbox mechanisms in a virtual environment, by leveraging functions like GetLastError(), IsDebuggerPresent, and OutputDebugStringA() [4]. As mentioned earlier, the LockerGoga binaries are signed by a valid certificate issued by a legitimate CA. Many variants use the 'taskkill' command to terminate AV-associated processes and also attempt to clear windows logs using the 'C:\Windows\system32\wevtutil.exe cl Microsoft-Windows-WMI-Activity/Trace' command [3].

Windows API Calls

LockerGoga is also known to use some undocumented Window API calls (NtQuerySection) and import WS2_32.dll to support process communications, which shows the level of sophistication of the actors [7].

Detection: Sample Securonix Spotter Search Queries

Here are some sample Securonix Spotter search queries to assist with detection of the existing infections.

ETDR Process Monitoring (Process Hash Conditions)

(rg_category contains “Endpoint” OR rg_category contains “ips” OR rg_category contains “ids”) AND
(customstring3= ae7e9839b7fb750128147a9227d3733dde2faacd13c478e8f4d8d6c6c2fc1a55 or
customstring3= f474a8c0f66dee3d504fff1e49342ee70dd6f402c3fa0687b15ea9d0dd15613a or
customstring3= ffab69deafa647e2b54d8daf8c740b559a7982c3c7c1506ac6efc8de30c37fd5 or
customstring3= c1670e190409619b5a541706976e5a649bef75c75b4b82caf00e9d85afc91881 or
customstring3= 65d5dd067e5550867b532f4e52af47b320bd31bc906d7bf5db889d0ff3f73041 or
customstring3= 31fdce53ee34dbc8e7a9f57b30a0fbb416ab1b3e0c145edd28b65bd6794047c1 or
customstring3= 32d959169ab8ad7e9d4bd046cdb585036c71380d9c45e7bb9513935cd1e225b5 or
customstring3= e00a36f4295bb3ba17d36d75ee27f7d2c20646b6e0352e6d765b7ac738ebe5ee or
customstring3= 6d8f1a20dc0b67eb1c3393c6c7fc859f99a12abbca9c45dcbc0efd4dc712fb7c or
customstring3= 79c11575f0495a3daaf93392bc8134c652360c5561e6f32d002209bc41471a07 or
customstring3= 050b4028b76cd907aabce3d07ebd9f38e56c48c991378d1c65442f9f5628aa9e or
customstring3= 1f9b5fa30fd8835815270f7951f624698529332931725c1e17c41fd3dd040afe or
customstring3= 276104ba67006897630a7bdaa22343944983d9397a538504935f2ec7ac10b534 or
customstring3= 88d149f3e47dc337695d76da52b25660e3a454768af0d7e59c913995af496a0f or
customstring3= c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15 or
customstring3= 06e3924a863f12f57e903ae565052271740c4096bd4b47c38a9604951383bcd1 or
customstring3= a845c34b0f675827444d6c502c0c461ed4445a00d83b31d5769646b88d7bbedf or
customstring3= 7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d723a80c08dd26 or
customstring3= ba15c27f26265f4b063b65654e9d7c248d0d651919fafb68cb4765d1e057f93f or
customstring3= eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0 or
customstring3= 7852b47e7a9e3f792755395584c64dd81b68ab3cbcdf82f60e50dc5fa7385125 or
customstring3= 14e8a8095426245633cd6c3440afc5b29d0c8cd4acefd10e16f82eb3295077ca or
customstring3= 47f5a231f7cd0e36508ca6ff8c21c08a7248f0f2bd79c1e772b73443597b09b4 or
customstring3= f3c58f6de17d2ef3e894c09bc68c0afcce23254916c182e44056db3cad710192 or
customstring3= 9128e1c56463b3ce7d4578ef14ccdfdba15ccc2d73545cb541ea3e80344b173c or
customstring3= c3d334cb7f6007c9ebee1a68c4f3f72eac9b3c102461d39f2a0a4b32a053843a or
customstring3= 6e69548b1ae61d951452b65db15716a5ee2f9373be05011e897c61118c239a77 or
customstring3= 8cfbd38855d2d6033847142fdfa74710b796daf465ab94216fbbbe85971aee29 or
customstring3= bdf36127817413f625d2625d3133760af724d6ad2410bea7297ddc116abc268f or
customstring3= 5b0b972713cd8611b04e4673676cdff70345ac7301b2c23173cdfeaff564225c or
customstring3= c7a69dcfb6a3fe433a52a71d85a7e90df25b1db1bc843a541eb08ea2fd1052a4

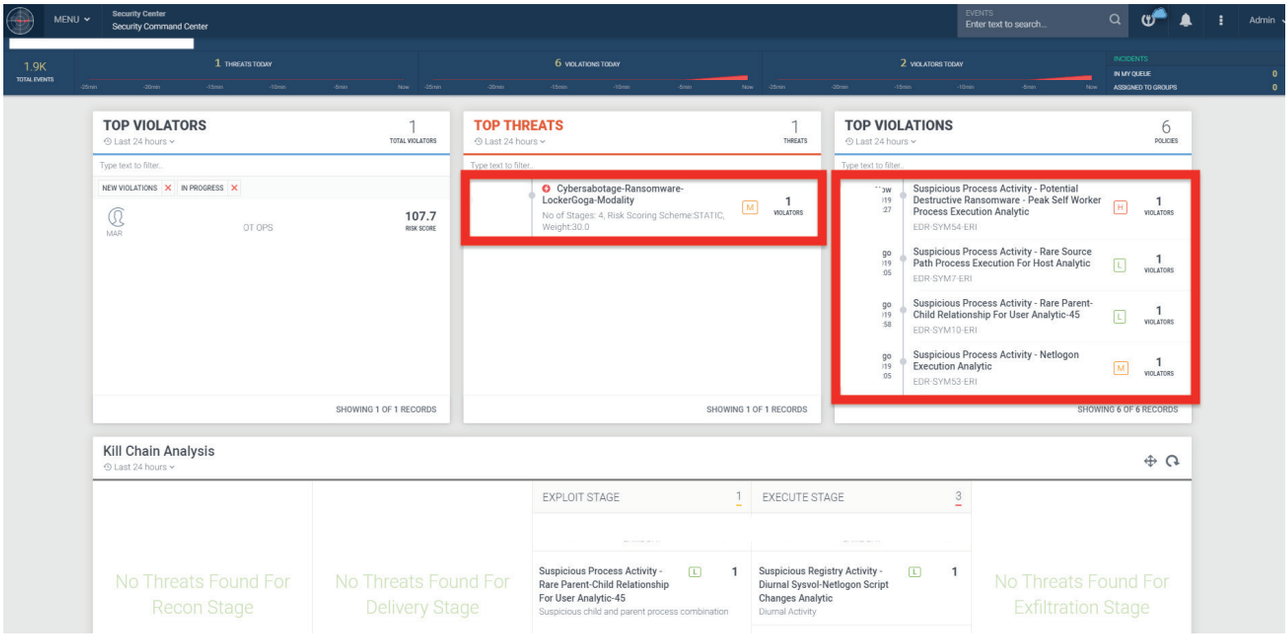


Figure 4: LockerGoga Malicious TC/R Implant Detection Using Securonix

ETDR Process Monitoring (Trivial Process Name Conditions)

(rg_category contains “Endpoint” OR rg_category contains “ips” OR rg_category contains “ids”) AND (sourceprocessname starts with tgytutrc)

Securonix Detection: Some Examples of Securonix Predictive Indicators

Some high-level examples of the relevant Securonix behavior analytics and predictive indicators that could help detect such attacks in your IT/OT environments are given below. Figures 4 and 5 show a practical example of the detection of the LockerGoga attacks using Securonix.

Suspicious Process Activity -
Potential Sysvol/Netlogon Lateral Movement Execution Analytic
This can be leveraged to detect the lateral movement of the malicious LockerGoga implants associated with netlogon, for example gpscript execution, to help cover both the current LockerGoga variants where operator placement is required and potentially future variants involving more automation.

Suspicious Process Activity - Peak Self Worker Process Execution Analytic
This can be used to help detect the encryption activity involving spawning a large number of worker processes to encrypt the files. The number of LockerGoga worker processes spawned depends on the number of processors/cores.

Suspicious Process Activity - Targeted - Potential Phishing Sequence II Malicious Payload Open Browser Modality Analytic
This can be used to detect the likely initial infiltration vectors used by the malicious LockerGoga attacks.

Suspicious Process Activity - Rare Parent-Child Relationship For Host Analytic
This can help detect the initial compromise and the behaviors associated with the operator placement required for lateral propagation.

Suspicious Process Activity - Peak Netsh Execution For User Analytic
This can be utilized to identify unusual activity associated with disconnecting the network interfaces on the targets using netsh disable.

Suspicious Registry Activity - Diurnal Sysvol/Netlogon Script Changes Analytic
This can help detect initial operator placement needed for lateral movement in the form of unusual GPO sysvol/scripts registry updates associated with the logon scripts GPO changes.

And a number of other Securonix behavioral analytics and predictive indicators, including: EDR-SYM5-ERI, EDR-SYM11-ERI, SST-SYM3-BPI, WEL-TAN1-BAI, EDR-SYM7-ERI, WEL-OTH1-RUN, EDR-SYM21-RUN, SST-SYM3-BPI et al.

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. Make sure that your backups are stored in a location that cannot be accessed/encrypted by the LockerGoga TC/R attack. For example, consider using remote write-only backup locations.

2. One of the possible ad hoc prevention or 'inoculation' methods for this particular threat could leverage an unhandled exception in the LockerGoga source code. While enumerating the target files, if the parent process encounters a malformed ".lnk" file (contains invalid network path and has no associated RPC endpoint) the process is terminated without any further encryption [10].

3. Implement an end user security training program since end users are ransomware targets and it is important for them to be aware of the threat of ransomware and how it occurs.

4. Patch operating systems, software, and firmware on your infrastructure. Consider leveraging a centralized patch management system.

5. For your Windows systems, consider enabling and auditing controlled folder access/turn on the protected folders feature. https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/enable-controlled-folders-exploit-guard

References

[1] Altran Technologies, Stéphanie Bia. Press release- Information on a cyber attack. January 01, 2019. https://ml.globenewswire.com/Resource/Download/0663f8d4-0acf-4463-b0fd-bb05042d1373. Last Accessed: March 28, 2019.

[2] Norsk Hydro ASA. Update on cyber attacks March 21. March 21, 2019. https://www.hydro.com/nl-NL/media/news/2019/update-on-cyber-attacks-march-21/. Last Accessed: March 28, 2019.

[3] Nick Biasini. Ransomware or Wiper? LockerGoga Straddles the Line. March 20, 2019. https://blog.talosintelligence.com/2019/03/lockergoga.html. Last Accessed: March 28, 2019.

[4] Pierluigi Paganini. [SI-LAB] LockerGoga is the most active ransomware that focuses on targeting companies. March 21, 2019. https://securityaffairs.co/wordpress/82684/malware/lockergoga-ransomware-spreads.html. Last Accessed: March 28, 2019.

[5] Nerijus Adomaitis. Norsk Hydro's initial loss from cyber attack may exceed $40 million. March 26, 2019. https://www.reuters.com/article/us-norway-cyber/norsk-hydros-initial-loss-from-cyber-attack-may-exceed-40-million-idUSKCN1R71X9. Last Accessed: March 28, 2019.

[6] Andy Greenberg. A Guide To LockerGogoa, The Ransomware Crippiling Industrial Firms. March 25, 2019. https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms. Last Accessed: March 28, 2019.

[7] Mike Harbison. Born This Way? Origins of LockerGoga. March 26, 2019. https://unit42.paloaltonetworks.com/born-this-way-origins-of-lockergoga. Last Accessed: March 28, 2019.

[8] Khasaia.Analysis of LockerGoga Ransomware. March 27, 2019. https://labsblog.f-secure.com/2019/03/27/analysis-of-lockergoga-ransomware/. Last Accessed: March 28, 2019.

[9] Trend Micro™ Security. What You Need to Know About the LockerGoga Ransomware. March 20, 2019. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware. Last Accessed: March 28, 2019.

[10] Alert Logic. Halting the Lockergoga Ransomware. March 25, 2019. https://blog.alertlogic.com/halting-the-lockergoga-ransomware/. Last Accessed: March 28, 2019.

[11] Alessandro Di Pinto, Heather MacKenzie. Breaking Research: LockerGoga Ransomware Impacts Norsk Hydro. March 19, 2019. https://www.nozominetworks.com/blog/breaking-research-lockergoga-ransomware-impacts-norsk-hydro/. Last Accessed: March 28, 2019.

[12] Mike Harbison - Palo Alto Unit 42. Born this Way: Origins of LockerGoga. March 26, 2019. https://unit42.paloaltonetworks.com/born-this-way-origins-of-lockergoga. Last Accessed: March 28, 2019.

References

[13] Brendan McKeague et al. Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware. April 5, 2019. https://unit42.paloaltonetworks.com/born-this-way-origins-of-lockergoga. Last Accessed: April 17, 2019.

[14] Jasper Manuel et al.. LockerGoga: Ransomware Targeting Critical Infrastructure. April 11, 2019. https://unit42.paloaltonetworks.com/born-this-way-origins-of-lockergoga. Last Accessed: April 17, 2019.

[15] Cyware. Dissecting the activities and operations of FIN6 threat actor group. April 30, 2019. https://cyware.com/news/dissecting-the-activities-and-operations-of-fin6-threat-actor-group-ebc7df0a. Last Accessed: April 13, 2019.

ABOUT SECURONIX

Securonix is radically transforming all areas of data security with actionable security intelligence. Our purpose-built, advanced security analytics technology mines, enriches, analyzes, scores and visualizes customer data into actionable intelligence on the highest risk threats from within and outside their environment. Using signature-less anomaly detection techniques that track users, account and system behavior, Securonix is able to detect the most advanced insider threats, data security and fraud attacks automatically and accurately.

CONTACT SECURONIX

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

0419


SECURONIX™