Ransomware or Wiper? LockerGoga Straddles the Line

blog.talosintelligence.com/lockergoga/

Nick Biasini March 20, 2019

By Nick Biasini

Wednesday, March 20, 2019 14:03

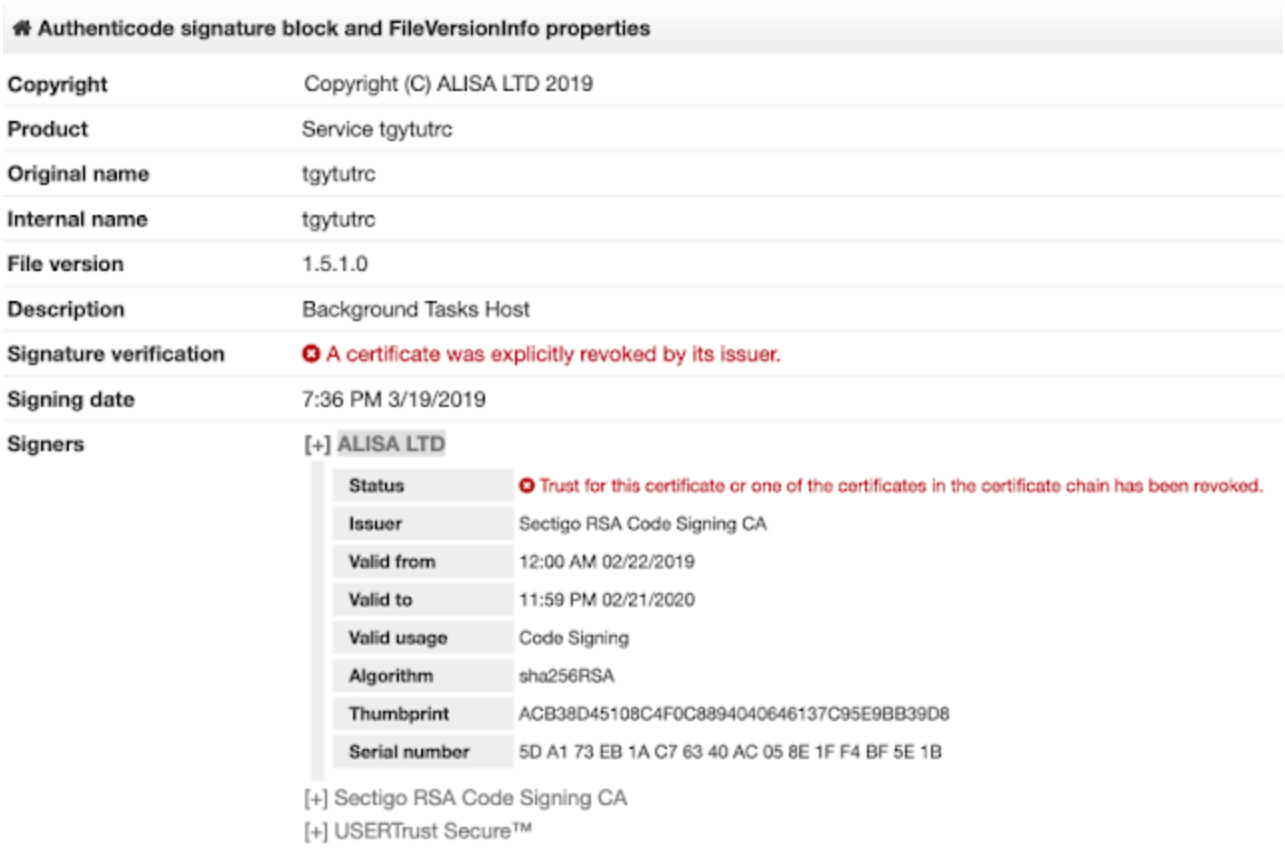
ransomware

Executive Summary Ransomware attacks have been in the news with increased frequency over the past few years. This type of malware can be extremely disruptive and even cause operational impacts in critical systems that may be infected. LockerGoga is yet another example of this sort of malware. It is a ransomware variant that, while lacking in sophistication, can still cause extensive damage when leveraged against organizations or individuals. Cisco Talos has also seen wiper malware impersonate ransomware, such as the NotPetya attack.

Earlier versions of LockerGoga leverage an encryption process to remove the victim's ability to access files and other data that may be stored on infected systems. A ransom note is then presented to the victim that demands the victim pay the attacker in Bitcoin in exchange for keys that may be used to decrypt the data that LockerGoga has impacted. Some of the later versions of LockerGoga, while still employing the same encryption, have also been observed forcibly logging the victim off of the infected systems and removing their ability to log back in to the system following the encryption process. The consequence is that in many cases, the victim may not even be able to view the ransom note, let alone attempt to comply with any ransom demands. These later versions of LockerGoga could then be described as destructive.

While the initial infection vector associated with LockerGoga is currently unknown, attackers can use a wide variety of techniques to gain network access, including exploiting unpatched vulnerabilities and phishing user credentials. Expanding initial access into widespread control of the network is facilitated by similar techniques with stolen user credentials being an especially lucrative vector to facilitate lateral movement. For example, the actors behind the SamSam attacks leveraged vulnerable servers exposed to the internet as their means of obtaining initial access to environments they were targeting.

LockerGoga Details Several of the LockerGoga samples observed in the wild appear to have been signed using a certificate that was issued to ALISA LTD by Sectigo:



This was likely an attempt by the malware author to minimize anti-malware detection, as executables that are signed using valid certificates may not be analyzed as rigorously as executables with no signature verification. The certificate has since been revoked by the issuer.

During the infection process, the LockerGoga executable is copied to the %TEMP% directory on the victim system and executed.

Talos has also observed versions of the LockerGoga ransomware that attempt to clear the Windows Event Logs using the following command syntax:

The ransomware then creates the ransom note and begins the encryption process. LockerGoga supports many of the common types of files that organizations typically use to store important data. As files are encrypted, the originals are deleted and replaced with the encrypted data, which is stored as files with the "*.LOCKED" file extension. Unlike many ransomware variants commonly observed, LockerGoga also encrypts the contents of the victim's Recycle Bin directory.

One other interesting aspect of the LockerGoga variant is that the files appear to be encrypted individually. When interacting with the sample, Talos observed commands being executed to encrypt each individual file, an example of which you can find below. This isn't commonly done since it's inefficient and creates overhead.

LockerGoga Ransom Note Following a successful infection, the LockerGoga ransomware writes a ransom note to the victim's desktop as a text file called "README_LOCKED.txt." Note that, in our research, we did find another campaign in January that was using a ransom note filename of "README-NOW.txt." Opening the ransom note with Notepad reveals the following:

Interestingly, unlike many of the more sophisticated ransomware variants seen in recent years, the ransom note does not include instructions for using a payment portal to process the ransom payment. It also does not include a Bitcoin or Monero wallet address and simply includes instructions for contacting the malware distributor via two email addresses that are included in the note. Talos has observed different emails listed across various samples that were analyzed.

There also does not appear to be a dedicated command and control (C2) structure set up to facilitate remote connectivity with the attackers. The attackers are also offering to decrypt a small number of encrypted files for free as a way to further convince victims of the

legitimacy of the operation and maximize the likelihood that the victim will pay the ransom demand. Additionally, Talos has observed no evidence to suggest that LockerGoga has the ability to self propagate across hosts on a network where an infection has taken place.

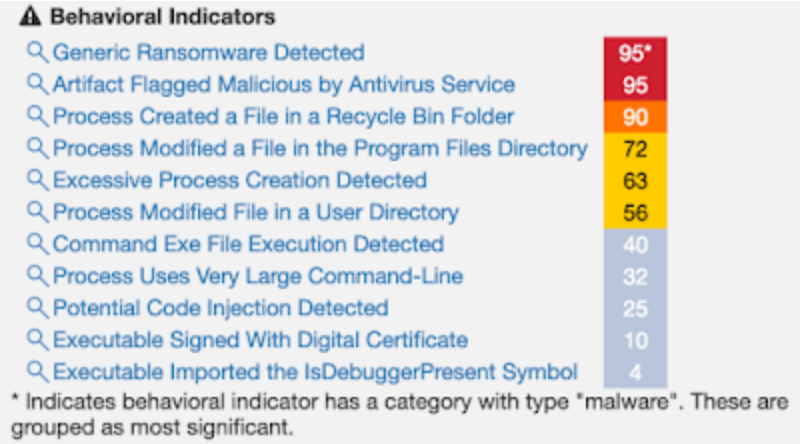
Conclusion Data is a valuable resource on all of our systems, whether that data is user photos or corporate documents. Therefore, ransomware continues to be a significant threat because it enables an attacker to steal that valuable data and hold it for ransom. Talos has seen financially motivated cybercriminals using ransomware in an attempt to generate a profit while other adversaries have used ransomware as a cover (such as the Not Petya attack) to disrupt the operation of the network, and hide their tracks by making forensic analysis more difficult.

Between using active exploitation, sending a threat via email or over the web, or even using stolen or bought credentials the possibilities are virtually endless. This is where some of the basic tenets of security come into play. Organizations increasingly need to have near real-time visibility into their endpoints in addition to the protective capabilities that products like AMP provide. Additionally, having multi-factor authentication (MFA) like Duo, enabled on systems can help prevent initial infection or slow its spread by limiting lateral access. Following established best practices with regard to network architecture and proper network segmentation can also help minimize operational disruption from threats such as ransomware, wiper malware, etc. Talos will continue to monitor this threat to ensure that customers remain protected from any evolutions that will inevitably occur.

Note: This blog post discusses active research by Talos. This information should be considered preliminary and will be updated as research continues.

Coverage LockerGoga is currently detected by Cisco security products which can be used by organizations to protect their environments from this and other ransomware attacks.

Example ThreatGrid Indicator Report:



Example AMP Detection:

Additional ways our customers can detect and block this threat are listed below.

Advanced Malware Protection(AMP) is ideally suited to prevent the execution of the malware used by these threat actors. Try AMP for free here.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Indicators of Compromise The following indicators of compromise have been observed to be associated with attacks leveraging the LockerGoga ransomware.

LockerGoga Executables (SHA256):

c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15
88d149f3e47dc337695d76da52b25660e3a454768af0d7e59c913995af496a0f
eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0
ba15c27f26265f4b063b65654e9d7c248d0d651919fafb68cb4765d1e057f93f
7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d723a80c08dd26
C3d334cb7f6007c9ebee1a68c4f3f72eac9b3c102461d39f2a0a4b32a053843a

---

Email Addresses from Ransom Notes MayarChenot@protonmail[.]com

DharmaParrack@protonmail[.]com
SayanWalsworth96@protonmail[.]com
DharmaParrack@protonmail[.]com
wyattpettigrew8922555@mail[.]com
SuzuMcpherson@protonmail[.]com
QicifomuEjijika@o2[.]pl
AsuxidOruraep1999@o2[.]pl
RezawyreEdipi1998@o2[.]pl

AbbsChevis@protonmail[.]com
IjuqodiSunovib98@o2[.]pl
RezawyreEdipi1998@o2[.]pl
