MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Security Primer
March 2019 • SP2019-0611

LockerGoga

Please Note: The information in this security primer is current as of March 28, 2019.

Overview

LockerGoga is a ransomware recently making headlines due to its disruptive effects on industrial and manufacturing firms' networks. Its recent victims include the Norwegian aluminum manufacturer Norsk Hydro, French engineering consulting firm Altran, and U.S. chemical companies Hexion and MPM Holdings (Momentive). The ransomware does not target or infect ICS systems, but its debilitating effects on the business and production networks tied to these industrial systems results in costly production down time. In the Norsk Hydro case, this involved temporarily moving to manual production. LockerGoga reportedly targets other sectors, although a disproportionate amount of victims reside in the industrial/manufacturing sector.

MalwareHunterTeam named the malware LockerGoga after discovering the name in a file path used for compiling source code into an executable. It also uses a .locked file extension for encrypted files.

```
X:\work\Projects\LockerGoga\cl-src-last\cryptopp\src\rijndael_simd.cpp
```

At this time, the initial intrusion vector is unknown. The ransomware's code is digitally signed using valid certificates which could let it evade security tools and get on systems. The certificates used in known attacks were revoked. The CTAs reportedly use Metasploit and Cobalt Strike to move laterally across a network. They also reportedly use the Mimikatz tool to pull passwords out of memory to compromise other accounts, including those with higher privileges. It is believed that they then use admin level credentials to target an organization's Active Directory for widespread ransomware deployment. LockerGoga reportedly does not have any self-propagation mechanisms, meaning that the malware itself cannot spread across the network and needs to be manually deployed. However, Palo Alto Networks Unit 42 reports they observed "LockerGoga moving around a network via the server message block (SMB) protocol, which indicates the actors simply manually copy files from computer to computer."

The malware is dropped in the %TEMP% folder with random number extensions, such as the following:

- %TEMP%\svc{random}.{randomnumber}.exe
- executed as %TEMP%\svc{random}.{random number}.exe -{random} -{random} {random}
- Example: %TEMP%\tgytutrc{4 Random Numbers}.exe

After execution, the malware moves itself to the directory %TEMP% in order to cover the malicious activity. LockerGoga then attempts to clear the Windows event logs, creates the ransom note, and begins the encryption process.

Security researches discovered a few LockerGoga idiosyncrasies affecting the ransomware's execution and the ability for victims to access the ransom note.

Cybersecurity vendor Alert Logic reports that there is currently a flaw in some LockerGoga variants where the ransomware will not encrypt anything if it comes across a .lnk file. LNK is a file extension for a Microsoft Windows shortcut file to point to an executable file. Since this discovery is public knowledge, it is highly likely that the malware authors are aware and will resolve the issue in future variants.

Cisco's Talos group observed that some LockerGoga variants forcibly log victims off their devices. They are then unable to log back onto the device, which also means they may not see the ransom note. Furthermore, in some cases the network interface on each system was disabled and the local user account passwords were changed. This can cause confusion on the victim's end as to their issue's root cause. If this is an intentional feature, then it is possible that the CTAs have both financial and destructive motivations.

Additionally, LockerGoga reportedly does not use a command-and control (C2) infrastructure for communication nor to generate encryption keys. This is a novel feature and the purpose might be to evade security tools that look for malicious C2 traffic.

The CTA's ransom note readme file does not list an extortion amount and only provides email addresses, which can be contacted to negotiate a ransom amount.

RECOMMENDATIONS

The most important proactive step an organization can take for ransomware is the ability to recover from their backups. Use a backup system that allows multiple iterations of the backups to be saved and stored offline, in case the backups include encrypted or infected files. Routinely test backups for data integrity and to ensure you can recover from them.

Please visit the MS-ISAC Ransomware Security Primer for more information on ransomware, including further recommendations.

The *MS-ISAC* is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance is available at 866-787-4722, *SOC@cisecurity.org*. The MS-ISAC is interested in your comments - an anonymous feedback *survey* is available.