SCADAfence

WHITE PAPER

Norsk Hydro's LockerGoga Ransomware Propagation Detection & Mitigation

Mar 2019

By: Ofer Shaked

Co-Founder & CTO at SCADAfence

March 21st - Initial release of this report

March 22nd - Added our analysis results regarding the UK-based companies that were used to sign the ransomware executables.

March 24th - According to Motherboard, two additional US chemical companies (Hexion & Momentive) have been hit two weeks ago by LockerGoga. According to researcher Kevin Beaumont, a total of 8 unique samples of LockerGoga are currently known to the public, while we only know about 4 organizations who were attacked.

March 26th: $40M is the cost of the first week of LockerGoga @ Norsk Hydro.

April 5th update: FireEye has attributed the attack to the same attacker in the Ryuk malware: FIN6, a Russian crime Enterprise.

Yet another ongoing ransomware attack that happened this week in Norsk Hydro, a leading Norwegian aluminum manufacturer, severely affected the company IT and Production systems. Very few technical details have been published about the attack, and as a result of the panic - a lot of speculations have been posted online.

SCADAfence Research Team has conducted a research of what are the currently known facts, including possible propagation scenarios and mitigation of the malware. We will update this post as more details will be revealed by our team.

What do we know for certain?

1. Based on NorCERT's (Norwegian CERT) report to NRK (Norwegian government-owned broadcast network), a ransomware called LockerGoga attacked the Norsk Hydro IT and production systems, propagating through Microsoft Active Directory services. Later, however, Mr. Håkon Bergsjø, head of NorCERT, said he doesn't want to confirm it was an Active Directory attack.

2. According to the March 20th update from Norsk Hydro's CFO, they only found out about the attack on Tuesday (March 19th) after midnight, a short period of time before the publication of the attack.

3. According to the March 21st update from Norsk Hydro's Head of Information Systems, they're working with Microsoft and other vendors to get operations back to normal, which might indicate that the attack was indeed propagated using Microsoft Active Directory services.

4. This ransomware is similar to the one used at the end of January this year, against the French engineering company Altran, and apparently against 2 US chemical companies, Hexion and Momentive.

5. The ransomware is minimalistic, with only the capabilities you'd expect from a plain ransomware – encrypting local and shared files, and shutting down network interfaces, without any propagation mechanisms, C&C, or other, more advanced features.

6. What's special about this ransomware? At the time of the attack on Altran, it had a valid certificate (currently revoked by issuer), allowing it to evade detection from Endpoint detection products. Moreover, we found one sample of the ransomware that went undetected by 100% of security products on VirusTotal (0% detection rate out of 67 products) from 2 weeks ago (March 8th 2019). We can estimate that at the time of the attack, the ransomware could've been detected, regardless of which Endpoint security product Norsk Hydro had used. It also used multithreading and optimization of the RSA-1024 algorithm in order to speed up the encryption process. The code however was sloppy, and cause instability of the running hosts while encrypting the files.

Questions that are still open:

1. Who are the attackers and what is their motive?

2. How did the attackers get in the network in the first place?

3. How did the attackers propagate through the network?

4. How can companies prevent such incidents?

We put the SCADAfence Research Team to the task of answering those questions with the little currently available information, taking into account experience with similar attacks and general information about industrial network security.

Who is behind LockerGoga?

LockerGoga is a relatively new ransomware, similar to the one used in the attack on Altran, a French Engineering company. On the Altran attack, we know that the ransomware executable was cryptographically signed by "MIKL Limited", a UK-based IT consultancy firm registered in 2014. Some speculations have been made, that this IT firm is in fact a shell company, but it has yet to be confirmed. However, newer samples, possibly those that took part in the Norsk Hydro attack, were signed by a different company, Alisa LTD, which is related to women's clothing. A 3rd company, Kitty's LTD, registered with a virtual office address in London has been discovered in two older samples [1] [2]. Those companies look like shell companies, all employing few employees with little to no online presence. Usually, further investigations of shell companies ultimately leads to fake or stolen identities.

Here's our analysis of the three UK-based companies:

Alisa LTD - The newest entity used to sign LockerGoga executables, possibly those that were in use during the attack on Norsk Hydro. Apparently this is the UK entity of Alisa Wedding Dresses. It looks like a legitimate wedding dresses business from Poland. We found more information about this business that we chose not to publish, because we believe it's unrelated to the cyber attack on Norsk Hydro. We will be able to share this information with the authorities if required.

Kitty's LTD - Registered to 2 Kenyan citizens who are UK residents. No reports about any financial activity.

MIKL LIMITED - Used in the Altran attack, is an IT consultancy, with minor financial activity.

Since Alisa LTD looks like a legitimate business, we can conclude one that one of the following options is true:

1. The company used to issue the code signing certificates made inadequate authenticity checks during the purchase of the certificates.
2. The attackers somehow got privileged information about the companies, allowing them to pass authentication during the purchase of the code signing certificates.

What was the propagation method?

According to the 1st update by Norsk Hydro, the attack started in the United States, propagating from there to plants in Europe. However, when we inspected the executables, we revealed that the ransomware doesn't have any propagation mechanisms, or even networking mechanisms, meaning it has no way to move by itself from machine to machine. Therefore, it needs an external tool or human intervention in order to propagate so fast between regions. Combining this with NorCERT's reply about the involvement of Microsoft

Active Directory in the attack, might indicate that Microsoft AD was used as the propagation mechanism. According to the 3rd update from Norsk Hydro's Head of Information Systems, they're working with Microsoft and other vendors to get operations back to normal, which might indicate that the attack was indeed propagated using Microsoft Active Directory services.

Attacks leveraging Microsoft AD are well known and have been used for years, but require more sophistication and human intervention (more about this later) than an automated exploitation of a known vulnerability, an attack method originating in the first computer worms in the 80s and 90s.

Was this a targeted attack?

Ransomwares are generally considered to be non-targeted attacks, not targeting a specific organization and requiring relatively a low effort to execute. However, due to the probable propagation method and attack tactics used, we believe that the attack on Norsk Hydro to be a coordinated, targeted effort.

Inspecting the ransomware executables, the SCADAfence Research Team has defined the capabilities used in it as requiring only medium technical abilities. It didn't require usage of any advanced technologies or vulnerabilities, yet it's simple and effective, and wasn't picked up by Endpoint protection products perhaps due to the signed executable.

What was the initial attack vector?

Currently, little is known about the initial attack vector. There's no indication that a newly discovered attack vector has been used in this attack. The attackers could have used any of the common attacks vectors which include spear phishing email, attack on an externally facing service, waterholing, man in the middle and others.

How can companies protect against LockerGoga and similar attacks?

Protection against such attacks can be split into the following categories:

1. Detect & respond
2. Backup & restore (if such an option exists)
3. Prevention (protecting against initial infection)
4. Prevent propagation
5. Protect against the encryption process

Detect & Respond

According to the March 20th update from Norsk Hydro's CFO, they only found out about the attack on Tuesday (March 19th) after midnight, a short period of time before the publication of the attack, probably when systems have stopped working as a result of the ransomware execution.

According to the compilation time of some of the samples labelled as LockerGoga, some executables have been compiled as late as 2019-03-18 09:07:54, only a few hours before the attack started. It's unknown how long the attackers have been in the network prior to the attack, preparing the ground for global infection. Could be days, could be weeks or even months.

Industrial network monitoring systems, such as those offered by SCADAfence, allows early detection of cyberattacks and malware propagation using multiple methods. It can also detect risks that can be used for initial infection. SCADAfence Platform integrates with firewalls, Network Access Control and other products to automate incident response.

For example, Norsk Hydro mentioned in their 1st update that they're working to isolate the plants, to prevent further infection. An automated incident response scenario can include automatic isolation of the infected plant, limiting infection to a defined area.

Backup & Restore procedures

Enough has been said about backup & restore procedures. Norsk Hydro say they have multiple systems for on-site and off-site backup and restore. Having such systems in place, with the right procedures and employee training, can greatly limit the impact of a ransomware attack, but not completely prevent it.

Protection against initial infection

Industrial networks, such as the ones that were affected by the Norsk Hydro attack, are known to be more vulnerable to cyber attacks due to lack of patching and lack of basic security mechanisms.

Again, utilizing an industrial network monitoring platform can detect an initial infection and identify network vulnerabilities such as unpatched hosts, and design flaws such as direct connections to the internet or office network, which enables the company to resolve them. They can also detect violations of company cyber security regulations and deviations from best practices.

Employee training (e.g. how to identify spear phishing emails), hardening of hosts (removal of administrator credentials and other methods), updated endpoint protection software and other methods can also reduce the likelihood of an initial infection.

Protect against propagation

Based on NorCERT's (Norwegian CERT) report to NRK (Norwegian government-owned broadcast network), a ransomware called LockerGoga attacked the Norsk Hydro IT and production systems, propagating through Microsoft Active Directory services. Later, however, Mr. Håkon Bergsjø, head of NorCERT, said he doesn't want to confirm it was an Active Directory attack. According to the 3rd update from Norsk Hydro's Head of Information Systems, they're working with Microsoft and other vendors to get operations back to normal, which might indicate that the attack was indeed propagated using Microsoft Active Directory services.

Since there's no other propagation method that is discussed currently, and since the Active Directory method is the likely option, given the rest of the information currently available about the attack, we chose to refresh the guidelines regarding Active Directory risks and attack mitigation.

How to attack using Active Directory?

Following is a brief overview of common lateral movement techniques that can be achieved by abusing AD:

Pass the hash / pass the ticket - By dumping password hashes for the KRBTGT account of a domain (using tools like Mimikatz), it's possible to create forged Kerberos tickets (TGT) to request TGS tickets for any service on any computer in the domain. Golden ticket remains valid and is persistent to password changes and DC rebuild.

System Center Configuration Manager (SCCM) - Allows to package and deploy operating systems, software and updates. Abusing of SCCM can be in the form of hosting the payload on a SCCM server and using PowerShell to grab the payload from a network path and execute it, without dropping a file to the file-system.

Automated lateral movement - Complex attack paths can be identified automatically using a tool like BloodHound, which utilizes graph theory to reveal hidden and unintended relationships within an AD environment. For example, GoFetch is a tool that automatically exercise an attack plan by BloodHound.

How to protect against Active Directory attacks?

Some AD attacks can be detected by network security products. However, to assure secure AD Domain Services we recommend to work proactively and follow security guidelines:

- Limit use of powerful user accounts

  - Few users as possible
  - Limit permissions to the minimum required
  - For administrators: separate personal users and admin users.
  - Harden your Active Directory settings
  - Service accounts that are used to run applications on hosts managed by the AD, should be limited to the minimum required permissions.
  - Harden password requirements for privileged accounts and Service accounts.
  - Patching & updates – especially on Domain Controllers

- Remove local administrator accounts, and enforce unique passwords per local default admin account.
- Periodically monitor & cleanup admin group membership
- Isolate legacy systems and applications

A good resource for additional reading is Microsoft's Best Practices for Securing Active Directory.

Protect against the encryption process

Some endpoint protection products claim to be able to detect file encryption, using file entropy detection, usage of crypto APIs and other methods. However, according to VirusTotal, most endpoint protection products didn't detect the encryption process. In any case, if such solutions are production-ready, they can be a viable option for protecting against the encryption process. Since the encryption process is usually run locally, only an endpoint detection product can detect and respond to it after it has already started.

About SCADAfence

SCADAfence is the global technology leader in OT & IoT cybersecurity. SCADAfence offers a full suite of industrial cybersecurity products that provides full coverage of large-scale networks, offering best-in-class network monitoring, asset discovery, governance, remote access, and IoT device security. A Gartner "Cool Vendor" in 2020, SCADAfence delivers proactive security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAfence enables organizations in critical infrastructure, manufacturing, and building management industries to operate securely, reliably, and efficiently. To learn more, go to www.scadafence.com