# Spyware Stealer Locker Wiper: LockerGoga Revisited

By Dragos, Inc.

Published: 2020-03-17 · Archived: 2026-04-29 02:11:40 UTC

*This blog summarizes Principal Adversary Hunter Joe Slowik's whitepaper, "Spyware Stealer Locker Wiper: LockerGoga Revisited."*

LockerGoga ransomware severely impacted the Norwegian metals giant, Norsk Hydro, and provides a blueprint for malicious entities to weaponize ransomware variants for disruptive purposes. The Norsk Hydro event incorporated unique disruptive characteristics calling into question whether the attackers ever intended to decrypt systems after infection. Insufficient data exists to adequately disposition Norsk Hydro as a state-sponsored disruption event instead of a financially motivated criminal exercise. Ransomware has destructive capability, and repurposed ransomware may allow for nation-states to hide behind criminal activity and prevent victims from reporting incidents.

LockerGoga first emerged in January 2019 with a ransomware event at French engineering company Altran Technologies.

Instead of introducing a self-propagating file into the network, the Altran incident involved an extensive, interactive breach by an unknown entity leveraging publicly and commercially available tools, such as Metasploit, PowerShell Empire, Cobalt Strike, and PSExec, to move laterally through the network. LockerGoga encrypts all files outside Program Files and operating system directories. Attackers can hold an entire network hostage, negotiating for decryption of the entire victim space, rather than providing per-host decryption instructions through a set price and reference to a Bitcoin or related cryptocurrency wallet.

Following events at Altran, there were no recorded or public sightings of LockerGoga until 19 March 2019 when Norwegian power and aluminum company, Norsk Hydro, faced a crippling cyberattack. Norsk Hydro was able to resume reduced operations by placing impacted industrial and production systems in manual operations mode. Reporting from the Norwegian CERT indicated LockerGoga execution was enabled by a widespread compromise of Norsk Hydro's Windows Active Directory (AD) instance. Unknown entities managed to spoof legitimate communication with a Norsk Hydro customer and used this to deliver a malicious attachment matching expected communication with Norsk Hydro itself. Multiple versions of LockerGoga may have been active in the Hydro environment simultaneously, including variants similar to the previous types performing encrypt-only operations. The attack itself took place the day after Hydro announced its existing CEO was stepping down to be replaced by an internal candidate. Norwegian reporting indicated that multiple Norwegian companies were targeted by the same entity responsible for the Hydro event, and that these entities were able to thwart the attackers based on quick information sharing from Norsk Hydro with Norwegian authorities.

Approximately one month after the Norsk Hydro event, indications emerged that LockerGoga intrusions might be tied to a single entity, FireEye-designated FIN6, also responsible for some Ryuk ransomware events. Examination indicates the link to FIN6 appears to be a replication or extension of previously cited work surrounding criminal

activity deploying LockerGoga and Ryuk by the French CERT. Reports also exclusively cover LockerGoga variants performing encryption-only operations, instead of the more disruptive variant at Norsk Hydro. One possibility behind LockerGoga's sudden rise and equally sudden disappearance is that the entity behind the malware simply evolved or modified capabilities, especially after a very high-profile event such as Norsk Hydro. While there are superficial similarities between the malware families, and they have been referenced together in public alerts on ransomware activity, available evidence supports only a tangential connection at best between the two.

From a propagation standpoint, ransomware authors and those deploying malware in many cases shifted network compromise from the use of self-spreading tools to more deliberate, interactive compromise of victim environments. This trend is observed in the "big game hunting" type of intrusions associated with Ryuk, LockerGoga, and MegaCortex (among others), where attackers compromise the network then use the resulting access to seed ransomware for future coordinated execution. The shift from per-host victim encryption to per-network encryption schemas where entire organizations are impacted provides a means to achieve widespread disruption without having to "fake" the existence of a decryption mechanism.

Malware is a tool to obtain an objective, and when combined with concerns over attribution (and potential retaliation), an attack that is minimally complex while avoiding assignment of blame can be effective in achieving an attacker's goals. The degree of alterations can be relatively minimal, requiring alterations to encrypt or disable systems (such as NotPetya's MBR/MFT capability, or the Norsk Hydro LockerGoga variant's forced reboot after disabling network connectivity and changing credentials) to achieve disruptive goals. As campaigns become more harmful and more brazen, governments are increasingly willing to publicly condemn attackers and impose a degree of cost on entities. By providing a means to not only obfuscate attribution but to redirect blame to likely criminal elements, a ransomware-as-disruptor pattern is ideally placed to enable actions in locations such as the U.S. or Europe while avoiding likely consequences.

Organizations may publicly declare willingness to work with governmental partners, but when such cooperation comes with potential risks of leaks, disclosures, or impacts to reputation, the cooperation may be very shallow or effectively non-existent. Pharmaceutical giant Merck, food products manufacturer Mondelez, and other entities attempted to recoup losses via insurance policies which included coverage for cyber events. All claims were denied due to "act of war" provisions in the policies exempting such actions from coverage. In NotPetya-related cases, information enabled insurance companies to invoke war exemptions in policies derived from government reporting and condemnation of the event as a Russia-directed effort. In this environment, if a company has even the slightest thought that circumstances were brought about by a possible state-sponsored attack, financial incentives would argue for sharing as little technical and related information as possible that could be used to make such a case of state-sponsored attribution public. Incentives due to financial penalties or losses means a potential state-sponsored or directed actor has significant space to operate directly in view of government authorities (or commercial security vendors) charged with safeguarding entities under their control or protection.

While insufficient evidence exists to definitively determine that the Norsk Hydro event was truly a disruptive attack instead of another (if spectacular) ransomware event, details showcase items that forecast potential developments in the field of cyberwarfare. The combination of a modification of existing ransomware, increased disruptive impacts from such malware, and targeting and timing specification provide a blueprint for how a state-directed adversary could utilize criminal tooling to execute deniable, but effective, disruptive operations.

Source: https://www.dragos.com/blog/industry-news/spyware-stealer-locker-wiper-lockergoga-revisited/