



# SPYWARE STEALER LOCKER WIPER:

| LOCKERGOGA REVISITED

AUTHOR

Joe Slowik | Dragos, Inc.

MARCH, 2020

# EXECUTIVE

## SUMMARY

---

**LOCKERGOGA RANSOMWARE SEVERELY IMPACTED THE NORWEGIAN METALS GIANT, NORSK HYDRO, AND PROVIDES A BLUEPRINT FOR MALICIOUS ENTITIES TO WEAPONIZE RANSOMWARE VARIANTS FOR DISRUPTIVE PURPOSES.**

Ransomware has lived in various forms as a threat to computer operations for decades, even if it has only risen to prominence in recent years. Throughout the evolution and spread of ransomware, events have shifted from focused targeting, to near indiscriminate wormable propagation, to “big game hunting” of large enterprises through widespread compromise. Underneath these trends, a space has developed where state-sponsored, as opposed to criminal, elements can weaponize ransomware (or ransomware-like) functionality.

Beginning with a clumsy monetization effort by North Korea through WannaCry, ransomware-as-disruptor seemed to establish itself with the NotPetya event taking place only a few months later in 2017. Yet this event, while significantly disruptive and harmful, showed immaturity by being too obviously related to disruptive intentions as opposed to financial gain.

A new version of the LockerGoga ransomware impacted Norsk Hydro later. While superficially similar to other industrial-targeted ransomware events around the same time, the Hydro event incorporated unique disruptive characteristics calling into question whether the attackers ever intended to decrypt systems after infection.

Nevertheless, insufficient data exists to adequately disposition Hydro as a state-sponsored disruption event instead of a financially motivated criminal exercise. Given poor public-private information sharing due to mistrust and similar friction, combined with perverse financial incentives from lawsuits through denied insurance claims, victims have little reason to come forward with necessary data to disposition disruptive events between criminal ransomware and likely state-sponsored disruption. Only by resolving these issues and providing political and financial security to victims will governments be able to muster not only the cooperation, but even the information necessary to identify such threats – let alone combat them.

# CONTENT

<b>EXECUTIVE SUMMARY</b>	2
<b>INTRODUCTION</b>	4
<b>REVIEW OF LOCKERGOGA</b>	6
<b>THE NORSK HYDRO INCIDENT</b>	9
EVENT CHARACTERISTICS AND ATTACK PATH	10
LOCKERGOGA FUNCTIONALITY DIFFERENCES IN NORSK HYDRO	12
POSSIBLE ADDITIONAL VICTIMS AND WIDER EVENT TARGETING	14
NORSK HYDRO, LOCKERGOGA, AND FIN6	16
LOCKERGOGA SINCE NORSK HYDRO	17
LOCKERGOGA AND MEGACORTEX	19
<b>RANDOMWARE AS DISRUPTIVE CAPABILITY</b>	21
NOTPETYA AS RANSOMWARE-LIKE DESTRUCTIVE ATTACK	22
NOTPETYA LESSONS LEARNED AND ATTACKER EVOLUTION	23
<b>INFORMATION OPERATIONS AND DISRUPTIVE IMPLICATIONS OF REPURPOSED RANSOMWARE</b>	26
DENIABLE OPERATIONS BY MIMICKING CRIMINAL ACTIVITY	27
VICTIM REPORTING CONCERNS WITH POSSIBLE STATE-SPONSORED INVOLVEMENT	28
<b>CONCLUSIONS</b>	30
<b>APPENDICES</b>	32
APPENDIX A: LOCKERGOGA SAMPLES	32
APPENDIX B: APPROXIMATE RANSOMWARE TIMELINE	34

# INTRODUCTION

Ransomware has a surprisingly long history in information security, with the first publicly known instance being a floppy disk-distributed worm provided to AIDS researchers at a World Health Organization conference in 1989.<sup>1</sup>

---

After a lull with some periods of identified activity, like the GPCoDe virus,<sup>2</sup> ransomware returned to focus with the emergence of CryptoLocker in 2013.<sup>3</sup> In the years since, ransomware has rapidly proliferated, with over 20 distinct families emerging between 2013 and 2016.<sup>4</sup> In that time, ransomware grew into one of the most disruptive and financially-damaging types of computer security events, resulting in not only increasing financial costs but also availability impacts often lasting weeks or months during recovery operations.<sup>5</sup>

A turning point in ransomware arrived in 2017 with the WannaCry outbreak.<sup>6</sup> While unprecedented for the sheer speed with which it spread around the globe on release, WannaCry is also interesting as it subsequently proved the ransomware was not the work of ordinary criminal, extortion-minded entities. Instead, WannaCry's origins lay with state-sponsored cyber activity, specifically entities working on behalf of the Democratic People's Republic of Korea (DPRK).<sup>7</sup> Although featuring several functionality issues in terms of recovery following a ransom payment,<sup>8</sup> WannaCry at least appeared to be designed as a vast monetization scheme in support of DPRK interests – a “first” given available information.

Ransomware moved from a primarily criminal problem to one suddenly involving state-sponsored activity. Such shifts became even more apparent a few months later when what initially appeared to be a variant of Petya ransomware swept across the globe with even greater disruption than WannaCry.<sup>9</sup> Subsequent investigation, including government-sponsored reporting, identified the malware, now known as NotPetya, as a wiper masquerading as ransomware with the intention of causing massive, unrecoverable disruption on victim IT systems.<sup>10</sup>

Since the WannaCry and NotPetya events of 2017, ransomware has continued to rage globally, impacting entities including government agencies, schools, hospitals, and large corporations. However, the events of 2017 should not be lost even as an ever-greater number of ransomware variants emerge to hold networks hostage for payment. While continued ransomware events indicate monetary success for criminal entities, the two largest outbreaks recorded demonstrate a playbook for non-criminal actors. Ransomware’s disruptive capacity combined with its ubiquity may provide state-sponsored or -controlled entities with a unique, deniable tool to achieve large-scale network disruption.

NotPetya’s functionality, as described by multiple researchers, made it apparent the malware ultimately served as a “wiper”, functionally destroying infected machines rather than a true ransomware variant where decryption and recovery is (presumably) possible. NotPetya’s indiscriminate spread, beginning with a supply chain compromise at an accounting software company serving Ukraine then encompassing entities worldwide,<sup>11</sup> resulted in impacts likely far beyond the responsible entity’s desires – including significant impacts in Russia, believed by multiple government and private entities to be the likely source of the malware. An adversary paying attention to these events, as well as following the evolution of “typical” ransomware since 2017, could therefore design a less virulent infection method enabling greater control over propagation while avoiding the obviously destructive aspects of NotPetya to embrace legitimate encryption operations. An entity with no intention of ever providing or revealing a key can achieve the same functional goal of rendering victim machines unusable and data unrecoverable.

GIVEN THE CONTINUED WIDESPREAD, DISRUPTIVE NATURE OF CRIMINAL RANSOMWARE AT THE TIME OF THIS WRITING, ACCURATELY AND CONFIDENTLY DETECTING SUCH A WEAPONIZATION OF RANSOMWARE WOULD PROVE DIFFICULT IF IT OCCURRED, IF NOT OUTRIGHT IMPOSSIBLE.



## A NOTE ON METHODOLOGY

The following analysis relies almost entirely on publicly available reporting and analysis, with only a few exceptions that were sourced from multiple entities. As a result, some entities may disagree with analysis or details as a result of having additional, non-public and undisclosed information on events below. Organizations or entities possessing data that can significantly alter or dispute the below analysis are strongly encouraged to make available any relevant data to ensure greater accuracy. Since initial coverage of LockerGoga in general and the Norsk Hydro event in particular, few parties have made any substantial new information available beyond scattered media interviews and high-level conference talks, which are all included below.

# REVIEW OF LOCKERGOGA

LockerGoga first emerged in January 2019 with a ransomware event at French engineering company Altran Technologies.<sup>12</sup>

Subsequent reporting from the French government confirmed that LockerGoga was responsible for the event, while ensuing CERT-FR reporting added additional details.<sup>13</sup> Unlike many other ransomware variants that possessed some built-in mechanism for self-spreading, LockerGoga contained no such propagation features whatsoever.

Table 1: Probable Altran-Related LockerGoga Samples

SHA256	SIZE	COMPILE TIME	FIRST OBSERVED COUNTRY	FILE NAME	SIGNED	SIGNER	POS-SIBLE EVENT	FUNCTION-ALITY
14E8A8095426245633CD6C3440AF-C5B29D0C8CD4ACEFD10E16F82EB-3295077CA	1.21 MB	1/28/2019 18:13	ES	WORK-ER32	MIKL LIMITED	COMODO RSA	ALTRAN	ENCRYPT ONLY
6E69548B1AE61D951452B65D-B15716A5EE2F9373BE05011E897C-61118C239A77	1.21 MB	1/25/2019 16:30	NL	WORK-ER32	MIKL LIMITED	COMODO RSA	ALTRAN	ENCRYPT ONLY
BDF36127817413F625D-2625D3133760AF724D6AD-2410BEA7297DDC116ABC268F	1.21 MB	1/23/2019 22:42	RO	WORK-ER32	MIKL LIMITED	COMODO RSA	ALTRAN	ENCRYPT ONLY
8CFBD38855D2D6033847142FD-FA74710B796DAF465AB94216FBB-BE85971AEE29	1.22 MB	1/16/2019 19:27	NL	WORK-ER32	MIKL LIMITED	COMODO RSA	ALTRAN	ENCRYPT ONLY
5B0B972713CD8611B-04E4673676CDF70345AC7301B2C-23173CDFEAF564225C	1.22 MB	1/16/2019 1:23	RO	WORK-ER32	MIKL LIMITED	COMODO RSA	ALTRAN	ENCRYPT ONLY





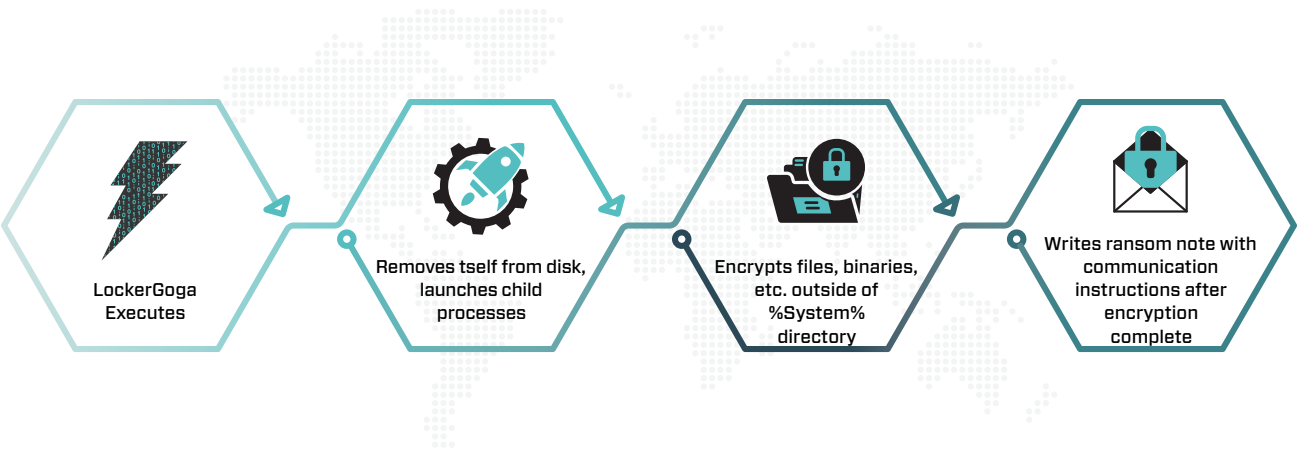
Instead of introducing a self-propagating file into the network, the Altran incident involved an extensive, interactive breach by an unknown entity leveraging publicly and commercially available tools, such as Metasploit, PowerShell Empire, Cobalt Strike, and PSEXec, to move laterally through the network. As stated in CERT-FR reporting, “Cette exécution est réalisée plusieurs semaines (voire plusieurs mois) après la compromission effective de la cible” – essentially, the attackers were in the network weeks or months prior to the execution of LockerGoga to prepare for and enable the ransomware event. While a precise mechanism for distribution was not identified, a combination of scripts and interactive logons appeared to disable security tools and prepare for the ransomware execution within the environment.

This first sample of LockerGoga associated with a publicly known incident is interesting for several reasons. First, it is signed with a likely fraudulent code signing certificate issued by COMODO (now Sectigo).<sup>14</sup> Although not unique

for malware, signed binaries can assist in evading security products or operating system controls for execution. Second, LockerGoga uses the Boost C++ libraries for multiple purposes, including for file renaming, parent-child process communication, and file deletion routines.<sup>15</sup> Third, actual encryption routines rely on another publicly-available C++ library called Crypto++ instead of native Windows libraries or coded encryption routines.<sup>16</sup> Fourth, after initial execution on a victim host, multiple “worker” instances of the malware are launched which then encrypt files on the host machine. This is a cumbersome and high-overhead process, but also one where failure to stop or kill the “root” process means defensive software or interactive use will likely fail to halt the encryption routine. Of note given likely spreading and installation methodology, the parent-child encryption process, which takes more time than other mechanisms, is ideally suited to an infection pushed or scheduled after typical working hours like a malicious group policy change or widely-scripted execution event.

Based on binary strings, encryption appears to target a standard list of document and related file types ranging from Microsoft Office Word documents to PDF files. However, in practice, LockerGoga encrypts all files outside Program Files and operating system directories. The ransomware note that provides contact instructions to negotiate payment is written last. An overview of LockerGoga’s behavior and execution sequence can be found in Figure 1.

Figure 1: LockerGoga process flow



The network decryption and negotiation approach represents a slight shift in ransomware, also observed in Ryuk and later ransomware variants. Attackers can work to 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. LockerGoga (along with the contemporaneous ransomware variant Ryuk) appeared to inaugurate an enterprise-targeting shift within ransomware. Items such as payment instructions or a wallet ID for cryptocurrency are unnecessary because victims negotiate to unlock their entire network with the attackers.





**THE NORSK**

# HYDRO INCIDENT

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 cyber attack.<sup>17</sup>

---

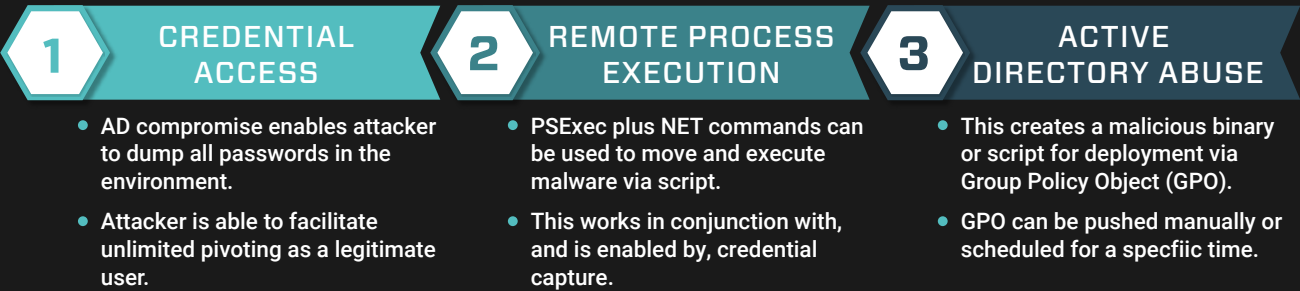
Based on public reporting and continued company updates, Hydro was able to resume reduced operations by placing impacted industrial and production systems in manual operations mode. Hydro reporting did not provide any technical observations or if the attack constituted a ransomware event. Subsequent analysis of publicly available information and sample correlation to company statements later indicated the event was the work of LockerGoga, but was a variant that featured additional functionality not observed in previous versions.

# EVENT CHARACTERISTICS AND ATTACK PATH

THE FIRST DETAILED REPORTING ON THE HYDRO EVENT CAME VIA INDEPENDENT SECURITY RESEARCHERS, MOST NOTABLY A LENGTHY OVERVIEW FROM KEVIN BEAUMONT.<sup>18</sup>

Follow-on reporting from the Norwegian CERT indicated LockerGoga spread and execution was enabled by a widespread compromise of Hydro’s Windows Active Directory (AD) instance.<sup>19</sup> With this level of compromise, attackers have access and control over the victim’s Windows environment, enabling a host of options including the placement and timing of malware execution throughout the enterprise. Examples of this timing are provided in Figure 2.

Figure 2: Active Directory Compromise Options

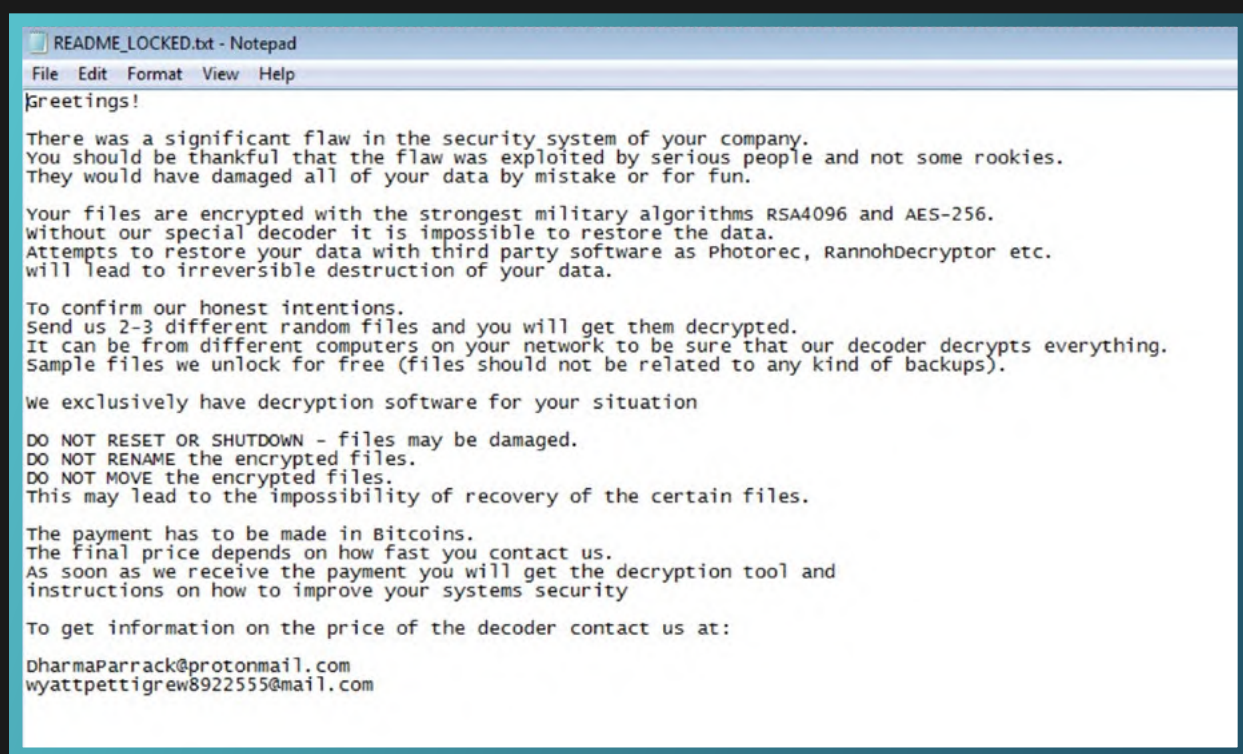


Precisely how the unknown attackers managed this level of penetration was unclear until follow-on reporting in the summer of 2019 from multiple media outlets. It was then revealed that Hydro was initially breached via phishing. Unknown entities managed to spoof legitimate communication with a Hydro customer and used this to deliver a malicious attachment matching expected communication with Hydro itself.<sup>20</sup> Although superficially similar to techniques such as Business Email Compromise

(BEC), the additional inclusion of what is described as a forged or modified legitimate document matching expected communication appears different from known BEC activity. Adequately dispositioning and evaluating the phishing vector is not possible due to a lack of technical details and further information. Subsequent actions resulted not in the attacker attempting to prompt a wire transfer, but to worm their way into Hydro’s network to gain complete control of the AD environment.

Although an official time-estimate of how far in advance Hydro was breached before the LockerGoga incident is unknown, estimates range from weeks to months.<sup>21</sup> Previous LockerGoga incidents are alleged to have involved extensive use of tools such as Metasploit and Cobalt Strike for lateral movement,<sup>22</sup> but no public evidence emerged from the Hydro event to support this claim. Some statements and conference discussions indicated possible use of Cobalt Strike, but no additional technical details were provided or are available. Later discussions with several sources indicated the attacker may have used a then-zero day, CVE-2019-0859, as a privilege escalation mechanism to enable penetration of the Hydro environment.<sup>23</sup> The attackers were able to widely distribute LockerGoga on Windows terminals throughout Hydro for coordinated execution, potentially via a malicious Group Policy Object push, to copy and execute the malware on 19 March 2019.

Figure 3: Norsk Hydro LockerGoga Variant Ransom Note





# LOCKERGOGA FUNCTIONALITY DIFFERENCES IN NORSK HYDRO

While the above is superficially similar to how Altran was likely breached and matches subsequent reporting on other ransomware families distributed via interactive compromise of a victim’s AD infrastructure,<sup>24</sup> other elements of the Hydro event were different than seen before. Initially noted by researchers at Cisco Talos, the LockerGoga variant most-likely associated with events at Hydro features additional functionality not found in previous variants,<sup>25</sup> either those identified at publicly known incidents or additional samples retrieved from commercial databases of malware samples.<sup>26</sup>

Table 2: Probable Norsk Hydro Related LockerGoga Samples

SHA256	SIZE	COMPILE TIME	FIRST OBSERVED COUNTRY	FILE NAME	SIGNED	SIGNER	POS-SIBLE EVENT	FUNCTIONALITY
65D5DD067E5550867B-532F4E52AF47B320BD31B-	1.21 MB	3/18.2019 9:07	NO	TGYTUTRC	ALISA	SECTIGO	NORSK HYDRO	ENCRYPT, CHANGE ACCOUNT PASS-WORDS, DIS-ABLE NETWORK ADAPTER
88D149F3E47DC337695D-76DA52B25660E3A454768AF-0D7E59C913995AF496A0F	1.21 MB	3/18.2019 9:07	NO	TGYTUTRC	ALISA	SECTIGO	NORSK HYDRO	ENCRYPT, CHANGE ACCOUNT PASS-WORDS, DIS-ABLE NETWORK ADAPTER



## SPYWARE STEALER LOCKER WIPER: LOCKERGOGA REVISITED

LockerGoga samples outside of those associated with Hydro followed the same functionality as the samples associated with the Altran event described earlier, focusing on file encryption using multiple processes. The samples associated with Hydro add significant new and disruptive functionality described below:



**Local user account passwords were changed to a hard-coded value.**



**Local administrator account passwords were changed to the same hard-coded value.**



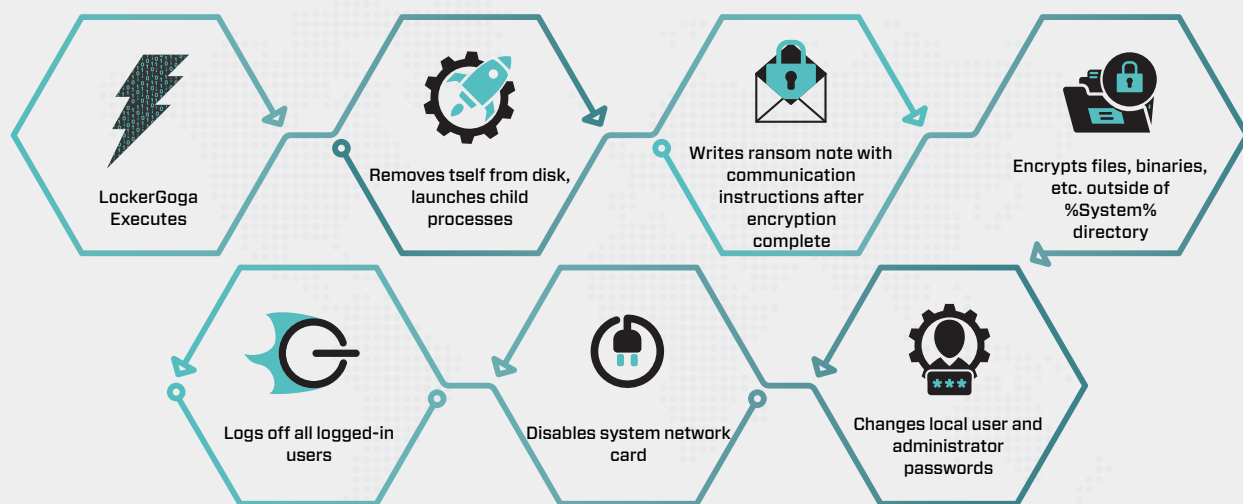
**The system network card was disabled.**



**All logged-in users to a machine were forcibly logged off.**

As noted by researchers at Talos, the above adds not only significantly more disruptive aspects to the event but appears also to work at cross-purposes to monetize the infection. The above chain of events means that systems were not only encrypted, but become inaccessible given changed local passwords and lack of network connectivity for remote and domain logons. In this scenario, even viewing the ransom note associated with the event would require additional work, such as forensically imaging the machine to recover the note from disk or analyzing the malware. This is especially true given that the ransom note was written at the end of the encryption process, just before local and remote access to the host was removed. While viewing ransom information is certainly possible, such items seem curious and counterproductive for efficient monetization.

Figure 4: LockerGoga Execution Sequence, Norsk Hydro Variant



One possibility based on reporting and available information is that multiple samples of LockerGoga were present in the Hydro environment. Multiple media reports and Hydro press releases included copies of the ransom note dropped by the more disruptive samples indicating these had to be recovered somehow. Multiple versions of LockerGoga may have been active in the Hydro environment simultaneously, including variants similar to the previous types performing encrypt-only operations.

Irrespective of the above multiple variant possibility, reporting on Hydro recovery efforts included a quote from company personnel about the desire to detect rapid password changes in the environment using an unspecified artificial intelligence solution after the LockerGoga event.<sup>27</sup> Based on this observation, a reasonable conclusion is that at minimum the more-disruptive LockerGoga variant was definitely active in Hydro's network.



## POSSIBLE ADDITIONAL VICTIMS AND WIDER EVENT TARGETING

ADDITIONAL DETAILS EMERGED OVER THE COURSE OF 2019 CONCERNING THE HYDRO EVENT THAT CAST FURTHER UNCERTAINTY ON EVENTS.

First and immediately obvious, the attack itself took place the day after Hydro announced its existing CEO was stepping down to be replaced by an internal candidate.<sup>28</sup> Although a review of the announcement indicates the change in leadership would be effective several months later, the timing is nonetheless suspicious. One possibility is an attacker could view the announcement as indicating a shakeup of internal leadership (oblivious to the future change-over date) and thus an attack coinciding with the announcement could take advantage of perceived unsettled communications and unclear leadership to maximize disruption.

Reporting in the summer of 2019 revealed additional institutions were also targeted by the same entity responsible for the Hydro incident.<sup>29</sup> As

one would expect a criminal gang intent on monetizing its ransomware capability to continue activity, subsequent details on timing and possible geographic focus made circumstances appear different. 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 Hydro with Norwegian authorities.<sup>30</sup> Press reporting is unclear as to whether entities outside Norway were also targeted

with the disruptive LockerGoga variant. Specific timing of any follow-on attacks and questions surrounding subsequent activities planned together or separate from events at Hydro are also lacking.

The fact that ransomware infections are on the rise and increasingly disruptive is no surprise. Subsequent media reporting indicates multiple efforts in the European Union to identify and prosecute entities responsible for recent ransomware events against multiple industrial institutions.<sup>31</sup> The possibility the disruptive variant of LockerGoga was used specifically against multiple Norwegian businesses roughly simultaneously with the Hydro event is concerning. First, such intrusions are relatively labor-intensive and require entities to compromise entire networks to achieve full AD compromise for malware distribution. This indicates a well-resourced team able to execute multiple compromises simultaneously.



Second, if all the entities involved were targeted by a group utilizing the same version of LockerGoga, the potential for economic disruption within Norway (or any similarly-sized economy) would be quite significant.

Based on this information, the LockerGoga variant deployed at Norsk Hydro, and potentially also deployed against other companies in Norway, looks very suspicious. The capability to render victim networks functionally unusable means the possibility for cascading economic shock is high. Executed in multiple commercial environments, industrial or otherwise, such a ransomware incident could grind an economy to a halt provided it impacted a sufficient number of organizations. In the case of Norway specifically, where a large part of economic activity (especially in the form of exports) is tied to extractive and manufacturing industries represented by a relatively small number of firms,<sup>32</sup> disruption at only a few of these entities could result in profound economic consequences.

The Norsk Hydro-associated LockerGoga variant, if also targeting additional entities in the Norwegian economy, evolves from a critical concern for a single company to an item of near-existential risk for an entire country. Absent firm details on additional, potential victims of the disruptive LockerGoga variant make a definitive assessment impossible. Yet the possibility of essentially crippling a country through perceived criminal tools while avoiding collateral and unintended damage, as with NotPetya, represents a profound learning opportunity for malicious actors.

Two U.S. chemical companies also were identified as LockerGoga victims just prior to the events at Hydro: Hexion and Momentive.<sup>33</sup> The intrusions at these chemical companies appeared to identify a theme in LockerGoga events, with a focus on various industrial enterprises. While public disclosure of events at Hexion and Momentive occurred after the Hydro incident became known, all evidence and reporting indicate the two chemical companies were affected prior to Hydro between 9 and 12 May 2019. Furthermore, the malware samples most likely associated with these companies feature the same characteristics as the earlier Altran event, and do not include the additional disruptive features identified at Hydro. As a result, these events appear to be noticeably different from the Hydro incident.

**Table 3: LockerGoga Samples Possibly Associated with U.S. Chemical Company Events**

SHA256	SIZE	COMPILE TIME	FIRST OBSERVED COUNTRY	FILE NAME	SIGNED	SIGNER	POSSIBLE EVENT	FUNCTIONALITY
7BCD69B3085126F7E-97406889F78AB74E87230C11812B-79406D723A80C08DD26	1.19 MB	3/9/2019 17:50	NL	ZZBDRIMP	ALISA	SECTIGO	HEXION OR MOMENTIVE	ENCRYPT ONLY
BA15C27F26265F4B063B65654E9D-7C248D0D651919FAFB68CB-4765D1E057F93F	1.19 MB	3/9/2019 17:48	CA	IMTVKN-QQ	ALISA	SECTIGO	HEXION OR MOMENTIVE	ENCRYPT ONLY

# NORSK HYDRO, LOCKERGOGA, AND FIN6

APPROXIMATELY ONE MONTH AFTER THE HYDRO EVENT, INDICATIONS EMERGED THAT LOCKERGOGA INTRUSIONS MIGHT BE TIED TO A SINGLE ENTITY, FIREEYE-DESIGNATED FIN6, ALSO RESPONSIBLE FOR SOME RYUK RANSOMWARE EVENTS.<sup>34</sup>

As noted in public reporting, this link appeared out of place because prior FIN6 activity exclusively focused on payment card theft and related operations.<sup>35</sup>

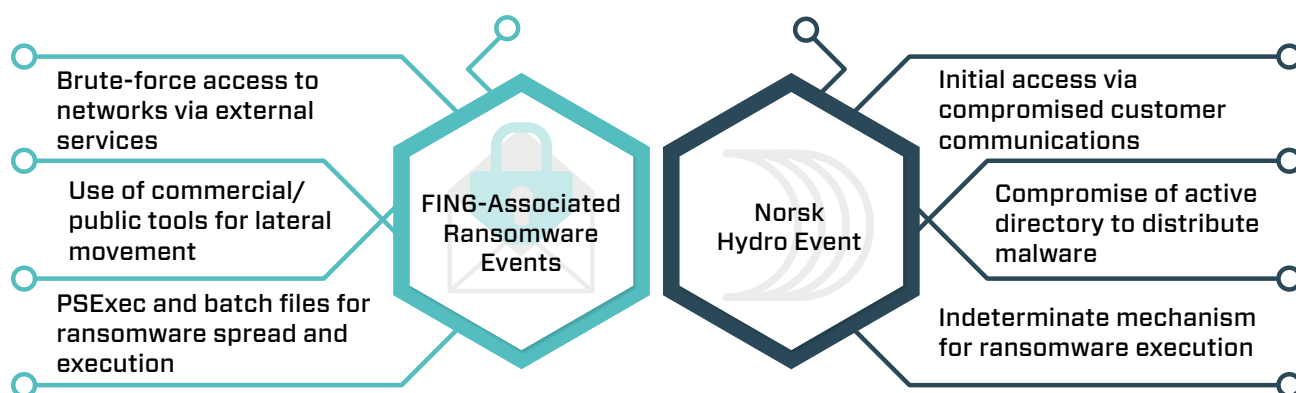
Examination indicates the link to FIN6 appears to be a replication or extension of previously cited work surrounding criminal activity deploying

LockerGoga and Ryuk by the French CERT.<sup>36</sup> The French CERT reporting mirrors subsequent analysis from FireEye in April 2019, demonstrating similar infection and lateral movement behaviors. Most critically for this analysis, both reports also exclusively cover LockerGoga variants performing encryption-only operations, instead of the more disruptive variant at Hydro.

Initial access techniques described in both reports focused on external service compromise or brute force access of remote access mechanisms. Ensuing activity focused on the use of commercial and publicly available tools for lateral movement, which may align with the Hydro event. These reports also emphasize the use of scripts and PSEXec for ransomware distribution as opposed to the possibility of AD-related malicious GPO creation.

Based on available data and analysis, it is possible that non-Hydro LockerGoga incidents are aligned with changes in FIN6 activity as publicly reported by FireEye and earlier indicated by the French CERT. However, available contextual information on the Hydro incident, such as initial access via highly targeted phishing and full AD compromise for likely distribution, indicate a separate entity was almost certainly involved in the more disruptive event.

Figure 5: Comparing FIN6 and Norsk Hydro Event



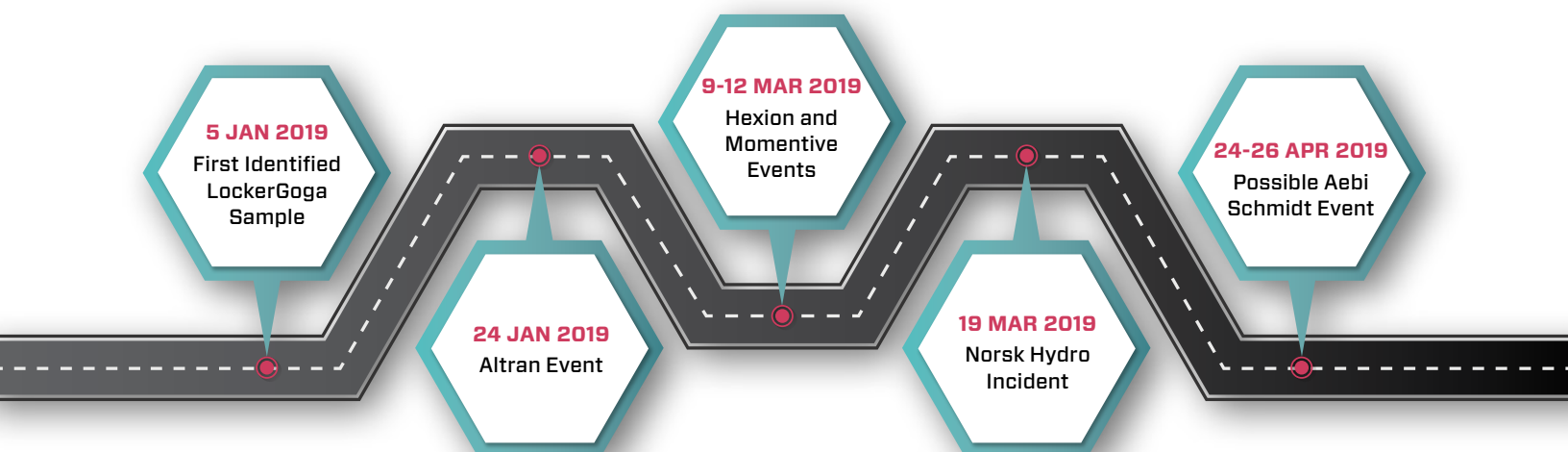
## LOCKERGOGA SINCE NORSK HYDRO

Following the Norsk Hydro event, LockerGoga seemed to disappear. While several security companies claimed they responded to multiple LockerGoga incidents around the time of the Norsk Hydro event,<sup>37</sup> no public reporting emerged providing additional information around these claims. While additional, unrelated LockerGoga events in conjunction with Norsk Hydro are certainly possible (i.e., outside of the possible coordinated economic disruption scenario discussed previously), it is equally probable that the events in question mirrored the ransomware-specific activity at Hexion and Momentive, and not the more disruptive variant deployed at Hydro.

One entity that may have suffered a ransomware event at the hands of LockerGoga following Hydro is the Swiss-based manufacturing company Aebi Schmidt. This company suffered a ransomware event in late April 2019 that some sources linked to LockerGoga, but no compelling public evidence ever emerged to tie the events together.<sup>38</sup>



Figure 6: Timeline of Known LockerGoga Activity



LockerGoga featured an effective lifespan of only three or four months. The ransomware family emerged in January 2019 with the Altran event then largely disappeared after the Norsk Hydro event in March 2019. Additional samples of LockerGoga have appeared in various repositories, but in all cases seem to be researcher modifications to existing samples and do not appear linked to any publicly known ransomware incident. While ransomware families are quite fluid, their function as monetizing instruments mean they typically persist for longer than a few months. Looking at LockerGoga specifically, there is an easily-observable development lifecycle and versioning reflected in the binaries from pre-Altran through Norsk Hydro, shown in Table 4.

Table 4: Observed LockerGoga Versions

LOCKERGOGA VERSION NUMBER	FIRST OBSERVED COMPILATION TIME	FUNCTION
0.9.9.0	05 JANUARY 2019	ENCRYPT ONLY
1.0.1.0	16 JANUARY 2019	ENCRYPT ONLY
1.0.2.0	16 JANUARY 2019	ENCRYPT ONLY
1.1.0.0	23 JANUARY 2019	ENCRYPT ONLY
1.1.1.0	25 JANUARY 2019	ENCRYPT ONLY
1.2.0.0	03 FEBRUARY 2019	ENCRYPT ONLY
1.3.2.0	02 MARCH 2019	ENCRYPT ONLY
1.4.4.0	09 MARCH 2019	ENCRYPT ONLY
1.4.4.1	10 MARCH 2019	ENCRYPT ONLY
1.5.1.0	18 MARCH 2019	ENCRYPT, CHANGE PASSWORDS, DISABLE NETWORK ADAPTERS, LOGOFF USERS

LockerGoga featured a very active development period from January through March 2019. Following the Norsk Hydro incident, the malware family appeared to be abandoned. The dramatic change in functionality from the 1.4 versions to the 1.5 variant at Hydro indicated a significant shift in intention and capability after several months of the malware focusing exclusively on encryption operations.

From an economic and resource-focused view, a criminal or related entity investing development resources into designing and deploying a new type of ransomware would presumably desire to draw as much value from that malware as possible. This is observed in the long lifecycles in almost every major ransomware variant, as described in Appendix B of this document.



While responses at Momentive and Hexion to likely LockerGoga variant infections are not publicly known, all public indications suggest that neither Altran nor Hydro paid the ransom associated with their events. In this respect, LockerGoga would appear to have a poor success rate in generating funds, and since it disappeared so suddenly appears inefficient from a monetization perspective. Given all this information, and the sudden shift from versions performing fairly non-descript network encryption operations to the more disruptive malware involved at Hydro, the evolution of available LockerGoga samples indicates a tool that was potentially modified for one-time, spectacular disruptive purposes before being retired.

## LOCKERGOGA AND MEGACORTEX

---

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.

This theory is supported by media reporting in May 2019 that identified unusual links between LockerGoga and a newly-emerged ransomware family called MegaCortex.<sup>39</sup> Links between the two focus on support items, specifically similar batch files for security process and related process kill actions, and a shared IP address identified in compromises. As noted in the public technical report by researchers from Sophos, the IP address in question is associated with multiple, unspecified malware activity and is not a definitive indicator of links given widespread use.<sup>40</sup> Other observables, such as both malware families using Boost libraries (although MegaCortex appears to only use Boost for inter-process communication, while LockerGoga relies on Boost for additional file

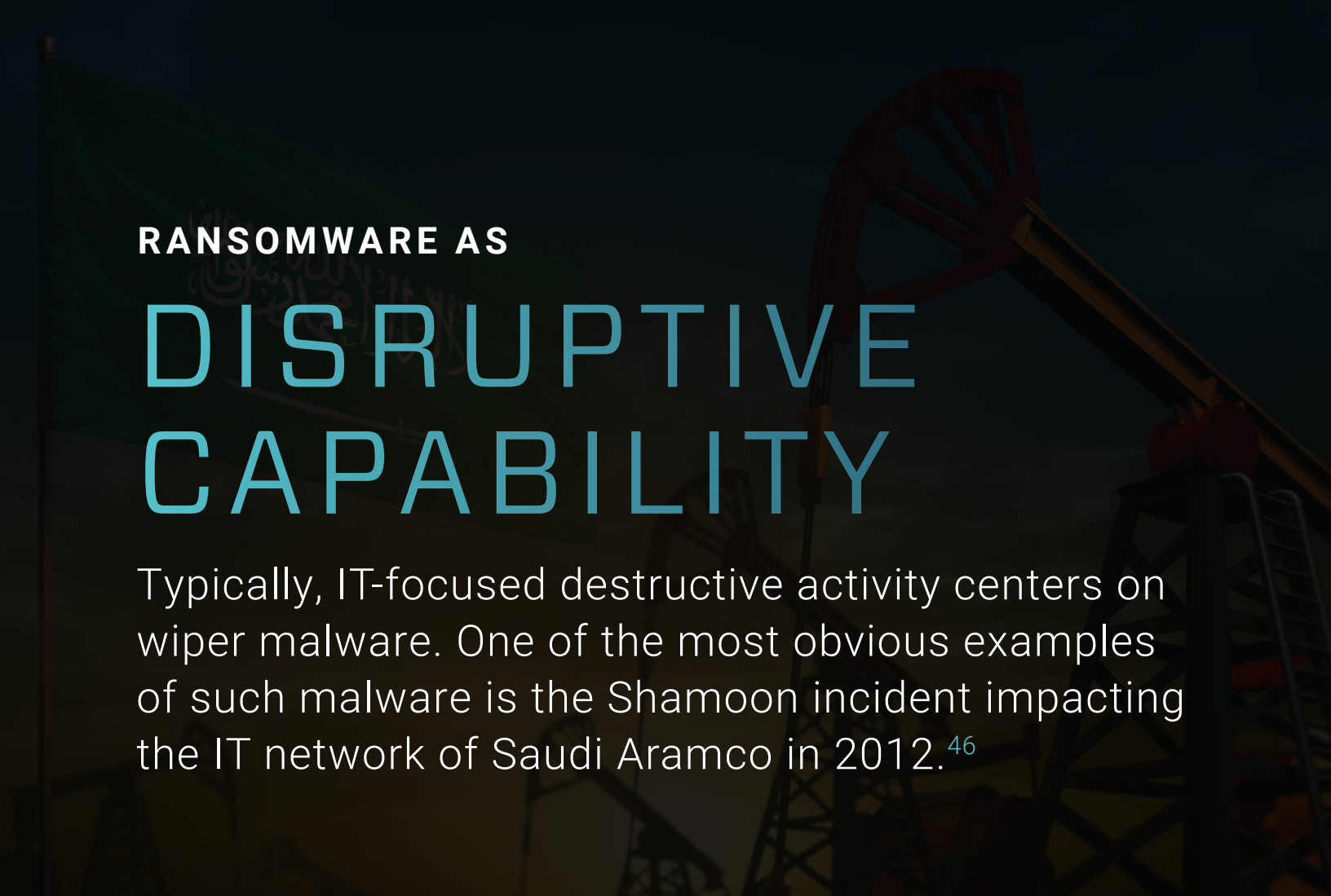
modification purposes) and parent-child process behavior can be seen as coincidences, and are noted as such by Sophos.

While there are superficial similarities between the malware families, and they have been referenced together in public alerts on ransomware activity,<sup>41</sup> available evidence supports only a tangential connection at best between the two. Given "core" LockerGoga functionality emerged in January 2019 while MegaCortex first came to light in May 2019, it is very possible that MegaCortex's design is based off review and analysis of LockerGoga functionality following the Altran event. Additionally, MegaCortex has not displayed the disruptive capabilities associated with the LockerGoga variant involved in the Hydro incident.

One final consideration on this topic concerns a new variant of MegaCortex from summer 2019,<sup>42</sup> and a further variant of this malware called “EKANS” from December 2019.<sup>43</sup> In both cases, observed malware featured an extensive list of processes to terminate as part of the encryption process. While most of the processes identified in the MegaCortex variant were security products, a subset related to industrial control system (ICS) software existed within the binary. This subset was ported together with the later EKANS variant. While some reporting around EKANS highlighted this event as a possible state-sponsored disruptive event,<sup>44</sup> all available evidence and malware functionality strongly suggest otherwise.<sup>45</sup>

While the two malware variants target processes for termination, the most likely explanation for doing so is to free files “locked” by them to further spread encryption of vital resources. The targeted processes focus on data storage, analysis platforms, and licensing servers, and appear to support this conclusion. While the ransomware encrypts significant portions of the victim machine, it does not perform disruptive actions like password changes and network card disabling associated with LockerGoga, or the filesystem encryption activity from NotPetya (discussed in detail below). These items appear to represent an evolution in likely criminal ransomware development, as opposed to a potential disruptive capability masquerading as such.





RANSOMWARE AS

# DISRUPTIVE CAPABILITY

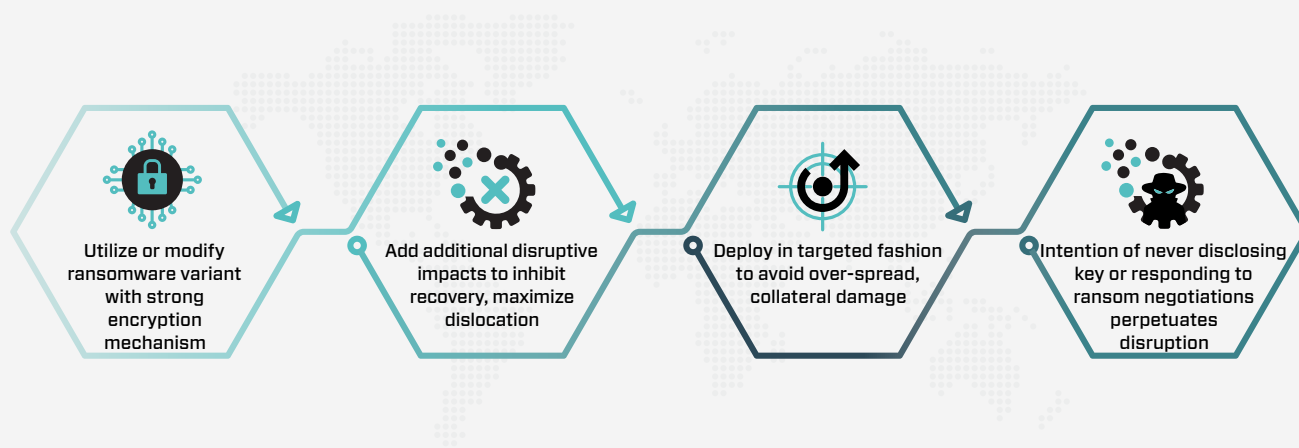
Typically, IT-focused destructive activity centers on wiper malware. One of the most obvious examples of such malware is the Shamoon incident impacting the IT network of Saudi Aramco in 2012.<sup>46</sup>

Multiple rounds of disruptive malware have followed,<sup>47</sup> from follow-on Shamoon variants to the use of KillDisk in the 2015 Ukraine power event.<sup>48</sup> Yet in all these cases, the intention of the malware involved is clear based on technical analysis: to irrevocably wipe and render IT systems unusable within the victim environment. These events can be clearly positioned as the actions of an entity motivated by reasons other than financial gain, whether state-sponsored geopolitical activity or potentially, although never proven in actual events, a politically motivated independent actor (e.g., “hacktivist”). The fingerprints for a wiper make assessing adversary intent, and given other observables, adversary identity somewhat clear.

More discrete tools and capabilities exist to deliver an equivalent impact while keeping

overall matters of intent, attribution, and perceived purpose murky. A ransomware event that encrypts an entire network and disables key functionality, provided the encryption schema is sound and not vulnerable to brute force or other attacks, delivers essentially the same impact as a network-wide wiper, in that systems are unusable and near impossible to recover. Such an event blends into an increasingly murky market of multiple actors deploying ransomware variants for perceived criminal gain. Even if the encryption mechanism proves faulty (in terms of file recovery), an actor attempting to “hide” a disruptive attack through ransomware can still blend in with similarly botched encryption implementations to make their irrecoverable file encryption appear a mistake as opposed to a deliberate action at making systems inaccessible.<sup>49</sup>

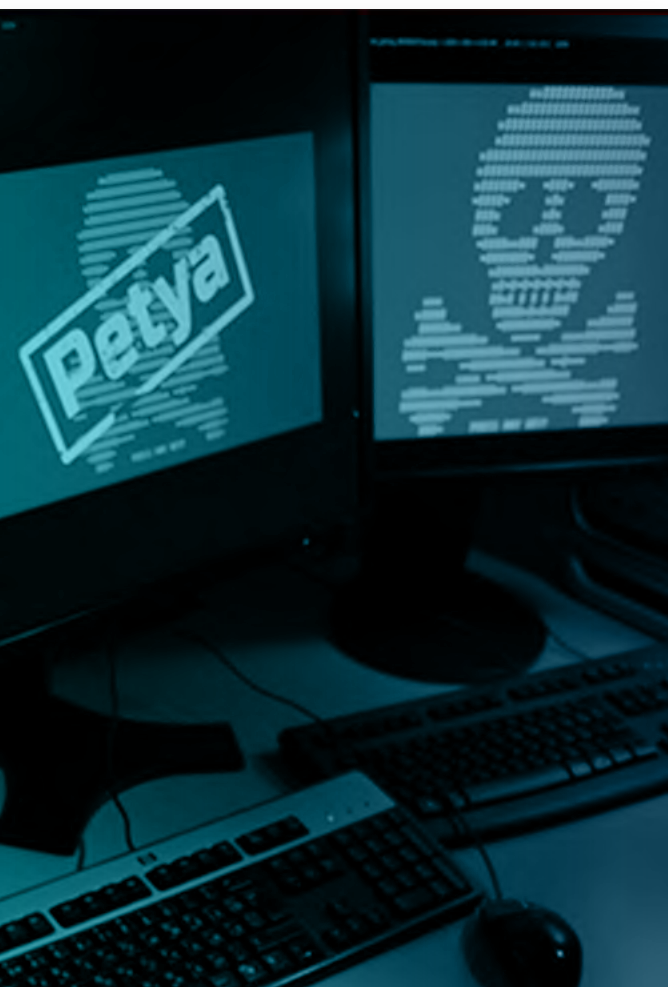
Figure 7: Ransomware-as-Disruptor Possible Attack Sequence



## NOTPETYA AS RANSOMWARE-LIKE DESTRUCTIVE ATTACK

NotPetya emerged as an especially virulent, widespread system encryption event months after WannaCry. Closer examination of NotPetya – from its initial delivery mechanism through its specific actions on victim systems – revealed a murkier picture indicating the malware was designed not as a tool for monetization, but rather a mechanism to render victim systems unusable.

The disruptive NotPetya worm has its origins in a ransomware variant that emerged in 2016 called Petya. Unlike other ransomware variants, Petya overwrites the victim machine's Master Boot Record (MBR) and encrypts the Master File Table (MFT), making the system functionally unusable without decryption.<sup>50</sup> While a concerning development in ransomware, actual implementation was faulty and led researchers to successfully identify ways to recover impacted systems without paying the ransom.<sup>51</sup>



A new strain of Petya, subsequently referred to as “NotPetya” given dramatically different intentions, emerged on 27 June 2017 and rapidly spread worldwide.<sup>52</sup> As noted previously, NotPetya appeared to start as a targeted attack on Ukrainian organizations given initial infection via a malicious update to Ukraine-specific accounting software. Using a combination of both the MS17-010 vulnerability (and accompanying EternalBlue exploit) and dynamic credential capture and re-use,<sup>53</sup> it spread globally quickly beyond its likely intended area of operations. As a result, NotPetya impacted entities likely beyond adversary intent – including significant impacts on Russian enterprises such as Rosneft, Evraz, and Sberbank.<sup>54</sup> Given subsequent attribution by multiple entities that the NotPetya attack originated with Russian state interests,<sup>55</sup> it would appear the malware spread almost too effectively resulting in domestic damage for its perpetrators.

Yet this last point underscores several interesting observations about NotPetya’s alterations from its predecessor. In addition to incorporating virulent self-propagating mechanisms, NotPetya’s encryption routine simply does not allow for recovery. As noted by researchers at Kaspersky and Matt Suiche of Comae, NotPetya generates the infection victim identifier – critical for determining the right decryption key – by creating random data.<sup>56</sup> Attackers would never be able to derive or recover the decryption key to unlock an infected system (or network), even if payment is made. NotPetya effectively “wipes” systems due to the combination of MBR/MFT attack (rendering the system inaccessible) and is intended to be a one-way encryption routine with no recovery.

**ATTACKERS ESSENTIALLY LOCKED SYSTEMS, THEN THREW AWAY THE KEY.**

## NOTPETYA LESSONS LEARNED AND ATTACKER EVOLUTION

---

Deploying ransomware (or ransomware-like functionality) without ever intending victim recovery presents a case where attackers can muddy reporting and potentially deflect blame while still executing devastating attacks. As noted by Matt Suiche, “The fact of pretending to be a ransomware while being in fact a nation state attack – especially since WannaCry proved that widely spread ransomware are [not] financially profitable – is in our opinion a very subtle way from the attacker to control the narrative of the attack.”<sup>57</sup>

At least initially, and especially emerging relatively soon after the global WannaCry outbreak, the desired narrative of highly virulent criminal ransomware seemed to hold. Technical analysis such as that mentioned above began to poke holes in this initial understanding with ultimate public attribution by several governments that NotPetya was a Russian destructive attack focused on Ukraine, ultimately settling nearly all reasonable debate.



Yet there were several problems with how NotPetya worked, especially since the desired story failed to hold over time. What appeared to be a Ukraine-centric event given the focus on the MEDoc accounting software as initial infection vector quickly became a globally disruptive phenomenon.<sup>58</sup> That the malware spread to key Russian companies was probably the least significant concern for a Russian-sponsored disruptive event, as cascading disruptions in Europe and the U.S. could have led to some degree of retaliation – a possibility since echoed in public comments by NATO Secretary General Jens Stoltenberg.<sup>59</sup>

**NotPetya appeared to have the following failings:**

1. The encryption routine and related processes destroyed any plausibility that the event could be construed as criminally motivated ransomware.
2. The attack was too effective in spreading, resulting in significant impacts outside the intended target (Ukraine), but hitting domestic (Russian) organizations and entities that might retaliate (U.S., Europe) as well.

The idea presented by NotPetya would be quite enticing to an adversary; the ability to execute a potentially crippling disruptive attack against an entity while severely undermining any ability to publicly identify the true responsible party. With adjustments in disabling methodology and spreading mechanisms, a more effective and controlled attack could be possible.

The evolution of ransomware after the NotPetya event provided many of the elements necessary to meet these goals. From a propagation standpoint, ransomware authors and those deploying such 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.<sup>60</sup> 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.



Figure 8: NotPetya Failures and Limitations



An attacker wishing to replicate the idea of NotPetya, but more effectively with greater control, could therefore breach the networks of organizations of interest in advance, seed these networks with ransomware that is somewhat more disruptive than normal (but not exceptionally so), and then simply “throw away the key” after execution. If cryptographically sound methods are used to deliver the attack, the possibility of recovery outside of complete system rebuild is very small. Given previous analysis and cited research above, the scenario of a more controlled, better implemented NotPetya begins to look close to something like the Norsk Hydro event and its unique variant of LockerGoga ransomware.

Although impossible to prove, an evaluation of publicly available data and related malware samples shows Norsk Hydro to be uniquely suited to follow a targeted and effective NotPetya model. When combined with other observations, such as potentially more widespread targeting of Norwegian companies, the situation becomes a part of a reasonably contained but locally widespread disruptive event. Available evidence cannot effectively disposition events toward either criminal activity or state-sponsored disruption, but given observations and the analysis above, the Hydro event at minimum provides an interesting and worryingly effective blueprint to state-sponsored entities on how to leverage seemingly criminal activity for disruptive purposes.



## INFORMATION OPERATIONS AND DISRUPTIVE IMPLICATIONS OF

# REPURPOSED RANSOMWARE

While NotPetya was certainly disruptive, it also represented a very blunt tool.

---

Widely targeted and quickly revealed as something other than criminal malware, it caused great damage but failed to take advantage of potential misdirection and misinformation items tied to its masquerade as ransomware. With some modifications, which coincidentally adhere closely to the evolution of the overall criminal ransomware environment, this activity can rapidly shift into a targeted, effective disruption mechanism. We typically examine cyber weapons through the lens of very complex, highly targeted examples such as Stuxnet. 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 quite effective in achieving an attacker's goals.

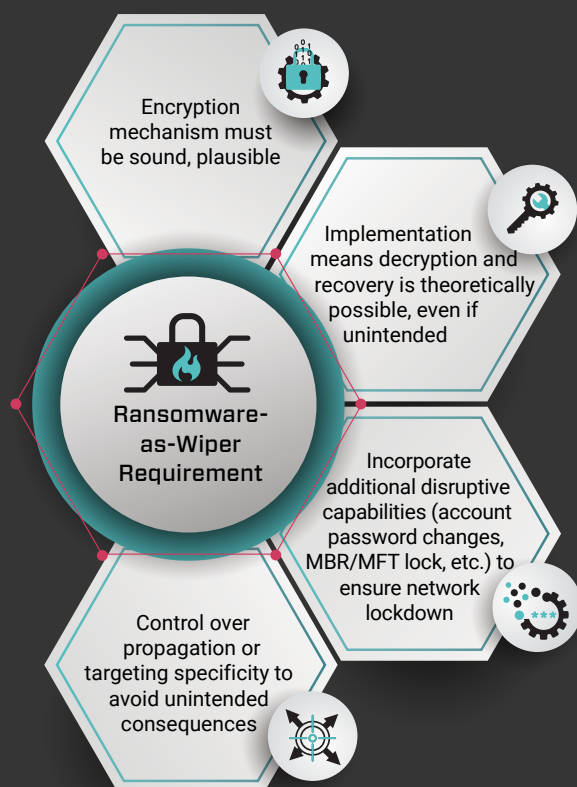
Repurposed ransomware offers an avenue to meet these objectives. The degree of alterations can be relatively minimal, requiring alterations to encrypt or disable systems (such as NotPetya's MBR/MFT capability, or the Hydro LockerGoga variant's forced after disabling network connectivity and changing credentials) to achieve disruptive goals. Another key point is access to software, especially source code, to facilitate modification while adhering closely to the profile of known, existing ransomware families. The relationships between criminal elements and state-sponsored cyber entities are close in many environments,<sup>61</sup> facilitating knowledge and capability transfer from criminal spaces for repurposing by state interests.

# DENIABLE OPERATIONS BY MIMICKING CRIMINAL ACTIVITY

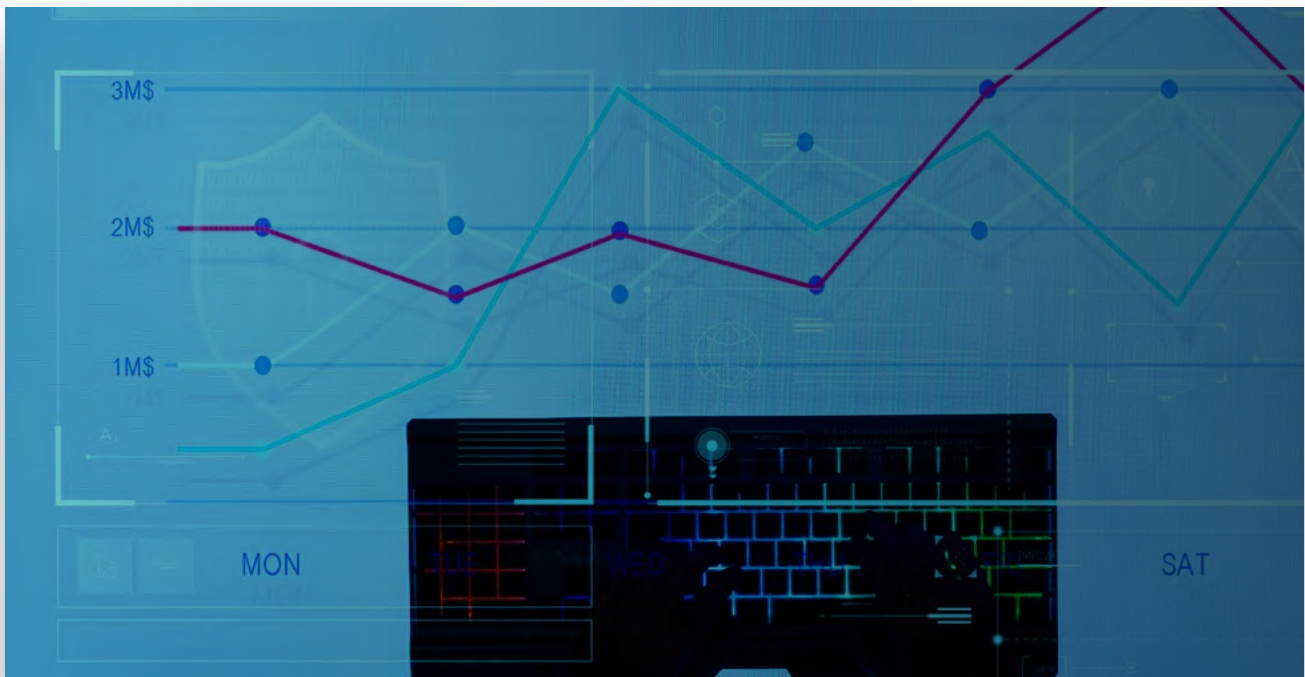
The field of cyberwarfare remains immature with still-fluid norms. As campaigns become more harmful and more brazen, governments are increasingly willing to publicly condemn attackers and impose a degree of cost on entities. Most consequences focus on legal remedies such as indictments or sanctions.<sup>62</sup> While legal approaches seldom result in actual arrests, although there are exceptions, the increasing willingness to issue significant punishments in terms of commercial restrictions or access to markets through sanctions has noticeable costs. Except entities completely divorced from the international system, like DPRK, sanctions have meaning. Avoiding them is preferential to having to deal with their consequences.

For disruptive operations outside of established or recognized conflict zones (such as Ukraine or the Gulf region), there is significant value in being able to generate enough uncertainty to avoid legalistic attribution. Repurposing already-disruptive criminal malware for disruptive means provides a simple and cheap avenue for doing so. Combined with institutional and cultural considerations around reporting and identification (discussed below), a state-sponsored or directed entity could launch an attack as effective as any of the Shamoon events while hiding behind the façade of possible criminal ransomware activity.

Figure 9: Ransomware-as-Wiper Requirements



Aside from avoiding obvious international criticism for the use of cyberattacks to disrupt civilian or commercial infrastructure, this approach also broadens the scope of areas where attacks can be used with relative impunity. For example, the various rounds of Russian-linked disruptive cyber activity in Ukraine, from two electric sector events to multiple additional campaigns, has resulted in no noticeable consequence to Russia.<sup>63</sup> Although better resourced and arguably more strategically valuable, the same can be said for multiple rounds of wiper malware impacting the Kingdom of Saudi Arabia, likely from Iranian entities, since the original Shamoon event. 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.



## VICTIM REPORTING CONCERNS WITH POSSIBLE STATE-SPONSORED INVOLVEMENT

---

When focused on civilian, non-government networks, the capabilities for deniability and hiding behind perceived criminal actions become more robust. Several items enter consideration at this stage, including continuing tension between private or commercial sector network defense and government interest in having access to incident data for investigation. 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 (or to perception in potentially important markets, such as those of the likely perpetrators of intrusion activity), the cooperation may be very shallow or effectively non-existent.

In a disruptive cyber event, additional perverse incentives exist that provide further room for malicious actors to hide their activities. A disruptive event by its very nature entails widespread dislocation of everyday business practices. Recovery operations take primary importance as impacted firms lose thousands (or millions) of dollars for each hour systems are unavailable. Given the trend toward network-wide, simultaneous encryption events in the criminal market, mirrored activity by state-sponsored entities mean similar challenges in attempting to perform meticulous, detailed forensic analysis and evidence recovery when the primary goal of the business is service restoration. Malicious behaviors and potential subtle differences between known criminal entities and other parties, can become masked or destroyed as systems are wiped, rebuilt, and restored as quickly as possible.



This is a common tension in computer network defense operations and is not unique. The implications of having, acknowledging, or admitting to a disruptive event emerging from state-directed or related activity can be turbulent. One especially interesting legal development in the aftermath of NotPetya concerned cyber insurance claims. While recovering from this disruptive event, 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.<sup>64</sup>

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. As explained previously, the NotPetya attack was almost certainly more widespread and damaging than intended, thus producing conditions prompting a firm, unequivocal response from impacted governments (even if only of the “name and shame” variety). More targeted events, such as a theoretical Norsk Hydro scenario where a company is impacted by a more deliberate event that also appears to be actual ransomware, avoids the massive impacts prompting government response. Given the limited scope of the event, any emerging information sharing would have to come from the impacted party itself or those responding to events on their behalf (all of whom are likely under strict nondisclosure agreements). 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 publicly. In observed NotPetya insurance claims, the potential costs to victims ranged from the hundreds of millions to billions of dollars.

While available reporting from LockerGoga and other ransomware events in Europe stress significant law enforcement involvement in attempting to identify perpetrators behind incidents, an ecosystem with financial incentives effectively penalizing companies for sharing information about their disruptions will lead to suboptimal results. When taken into consideration with existing concerns, such as the threat of lawsuits for negligence, failure to protect shareholder value, or damages from impacted customers or clients,<sup>65</sup> organizations are strongly incentivized to share as little information as possible.

Within this landscape, the necessary information to identify what appears at first glance to be another ransomware event is denied to those able to make such judgments. This set of perverse 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. Without significant changes in regulation, legal risk, and insurance language, private sector entities (who also control large amounts of critical infrastructure, to say nothing of overwhelming economic footprints) facing a targeted “wiper-as-ransomware” will have little reason to be cooperative or forthcoming with anything other than superficially useful data. The result is a poorer, less secure landscape for all organizations.



# CONCLUSIONS

THE NORSK HYDRO RANSOMWARE EVENT APPEARS AT ONCE BOTH STRAIGHTFORWARD AND INCREDIBLY CURIOUS.

While insufficient evidence exists to definitively determine that the 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.

While ransomware rages on through new families and an increasing array of victims, the sheer volume of such activity provides ample space for entities not focused on monetary gain to operate with more nefarious intentions. NotPetya may have served as an initial example of such activity, but a combination of poorly

implemented encryption functionality and over-zealous propagation made this event relatively easy to attribute to its state-based roots.

As ransomware has evolved from wildly propagating host-specific infections to more deliberate network compromise, malicious state-directed entities now have a new and valuable option for future disruptive operations. The combination of efficacy (when properly implemented), deniability (due to continued widespread criminal activity), and specificity (as self-propagation gives way to precise network compromise) enables selective and controlled targeting of entities for disruption and effective IT-based destruction.

While examples beyond NotPetya remain speculative, cases such as Norsk Hydro provide possibilities that adversaries can (and will) learn from, meaning defenders and policymakers must similarly pay close attention to such events. Current frameworks for responding to disruptive intrusion events that appear to be merely “criminal” push most responsibility to victims (and their incident response retainer vendors). Subsequent investigation under a law enforcement aegis means state-sponsored and directed elements have significant space, both technically and bureaucratically, to operate unimpeded given slow timelines, inadequate evidence collection, and disincentives towards unrestricted sharing of vital data.

To counter the risk of adversaries becoming savvier and the possibilities of masquerading as criminal entities for destructive purposes, a rethink is required in how network defense, information sharing, and cost sharing are conducted. First, defenders must move from a position where criminal and state-directed intrusion activity are bifurcated and instead recognize a continuum of behaviors and actions where the two can blend together for ambiguous results. Second, based on this recognition of indeterminate boundaries between criminal and state activity, organizations should be incentivized to share within trusted parties and relationships as much information about incidents and intrusions as possible, so as to facilitate the identification of trends and patterns indicative of coordinated operations associated with widespread disruptive campaigns. Lastly, current economic models do not accurately capture risk or correctly reward behaviors necessary for responding to an environment where criminal and state entities can blend together in action and immediate impact. Reforming such systems, providing alternative means of support for companies suffering from widespread network intrusion ransomware events, and using these changes to build more robust defense and detection will repel both criminal and state-nexus entities and produce a more robust security ecosystem for all involved stakeholders.



# APPENDICES

## APPENDIX A: LOCKERGOGA SAMPLES

SHA256	Compile Time	Country	Version	Associated Emails
2fe3c29913f66c255cb7aa5c34821ab182f889e7f96c25bad31267adc8a19e5b	3/18/2019 9:07	SG	1.5.1.0	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com
e7cd839c736b609bca04155aadb53a5e971459da1fff9b1c3ca4251d0d17107a	3/18/2019 9:07	SG	N/A	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com
808cf1f03ede512be8396f4be33122fddc2ec0bc5abc49792738bb7ea2daa01e	3/18/2019 9:07	FR	1.5.1.0	N/A
cc39fa68ba131e673ef7617e76af43a3094ca1379337339c21e6f687ebed177e	3/18/2019 9:07	DE	1.5.1.0	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com
b56ae7ae799c605f1113e8e4f1ba7b0133d0c64afd959d8162a7790ee64ee207	3/18/2019 9:07	IL	1.5.1.0	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com
4b3d9ffad989b659d264746e9346685fb8a7d27dc22592309a69fbc04996b834	3/18/2019 9:07	AR	1.5.1.0	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com
55d28e9c577d54732a546acb9b74a12e20cf25afab9636273abcabbb1a00e83d	3/18/2019 9:07	CZ	1.5.1.0	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com
974df521074fe3aba941e43e72f16882b9ea268c801ea3eea001fa39bad70525	3/18/2019 9:07	RO	1.5.1.0	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com
c2d44d4c92cdc0833b00128898a0cab00e9d2b97a455816be6e9ac8cdab4705e	3/18/2019 9:07	KR	1.5.1.0	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com
22972251517fd8d618f39ed5e5d26ef9276221724a5a5fad0372cc32afcce6de	3/18/2019 9:07	SE	1.5.1.0	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com
37e7b7a18b530ab4b7bfc55a446812159dddf40645811117ef5db5be2d61cc98	3/18/2019 9:07	SE	1.5.1.0	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com
dda454a53556047a82bbdf01cf97948a7ec5cac606884a2bc9d6cc6b80fd3460	3/18/2019 9:07	SE	1.5.1.0	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com
231132ca48b531f058fe6c7ed2200a8f2b65f19ae2f9d6c92da4aa651214abc7	3/18/2019 9:07	SE	1.5.1.0	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com
4ce29b6295eedd6b0d4fd9a1e9733f2d8ddfe8726b266a533543d12fbdd0274d	3/18/2019 9:07	US	1.3.3.7	mccrypt2019@yandex.com
e1985b06a9211a233843ca5edeb3b5a6b7435ba4ac48630187fedd5e90f8cd21	3/18/2019 9:07	FR	1.5.1.0	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com
0049d6b62cdf322b22ba6a398cda15b25f3440b76833fa24c3f4fccefa88432	3/18/2019 9:07	FR	1.5.1.0	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com
97b166566fe68e2e94cab8446b28b4b7153a239689570f9f8e6553e2574e7424	3/18/2019 9:07	US	1.5.1.0	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com
ffab69deafa647e2b54d8daf8c740b559a7982c3c7c1506ac6efc8de30c37fd5	3/18/2019 9:07	AE	1.5.1.0	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com
65d5dd067e5550867b532f4e52af47b320bd31bc906d7bf5db889d0ff3f73041	3/18/2019 9:07	NO	1.5.1.0	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com
88d149f3e47dc337695d76da52b25660e3a454768af0d7e59c913995af496a0f	3/18/2019 9:07	NO	1.5.1.0	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com
c97d9bbc80b573bdeeda3812f4d00e5183493dd0d5805e2508728f65977dda15	3/18/2019 9:07	FR	1.5.1.0	DharmaParrack@protonmail.com, wyattpettigrew8922555@mail.com

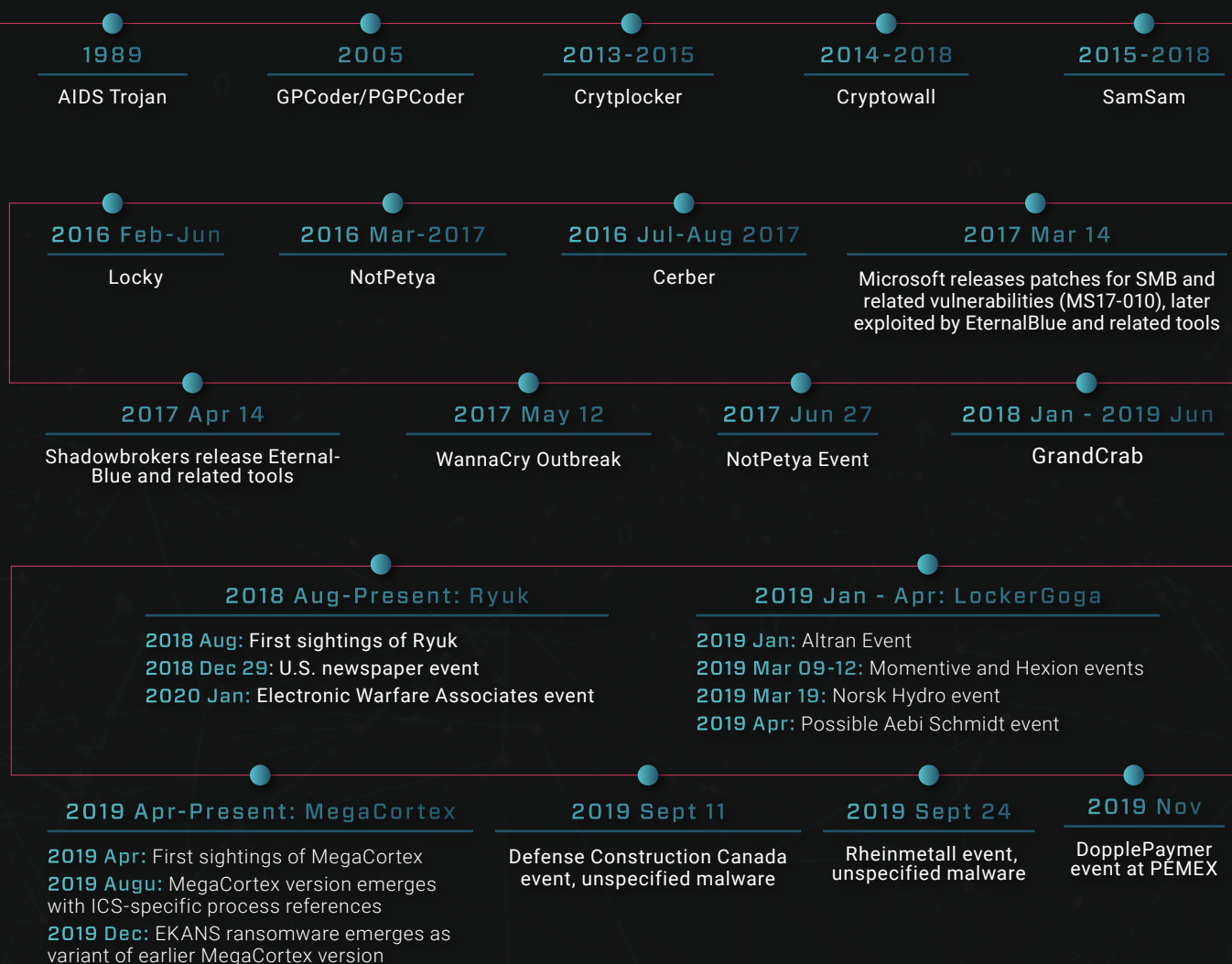


SHA256	Compile Time	Country	Version	Associated Emails
2ce4984a74a36dcdc380c435c9495241db4ca7e107fc2ba50d2fe775fb6b73ce	3/10/2019 22:43	NL	1.4.4.1	VernetEithan@protonmail.com, climprout1538818@mail.com
7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d723a80c08dd26	3/9/2019 17:50	NL	1.4.4.0	MayarChenot@protonmail.com, QicifomuEjijika@o2.pl
e78239849c9cfe1e1b9115d6ed05be3759cd91896a529992c8255e4bdf139f7a	3/9/2019 17:48	US	1.4.4.0	SayanWalsworth96@protonmail.com, RezawyreEdipi1998@o2.pl
ba15c27f26265f4b063b65654e9d7c248d0d651919fafb68cb4765d1e057f93f	3/9/2019 17:48	CA	1.4.4.0	SayanWalsworth96@protonmail.com, RezawyreEdipi1998@o2.pl
75ae842224d4b459ad3c94d48d0e6f24dda3fa2b0c76d9d8925bf7ebf872836d	3/2/2019 19:41	SE	1.3.2.0	SuzuMcpherson@protonmail.com, AsuxidOruraep1999@o2.pl
8e5abb9b44c93d946afe24f6cd4161a1593f94c06abc0c576f1f4609f2b6d0d	3/2/2019 19:41	SE	1.3.2.0	SuzuMcpherson@protonmail.com, AsuxidOruraep1999@o2.pl
ea3a76fe10d6ad2e19722f6360e8577279b8a98387b6e0171d39541192c71660	3/2/2019 19:41	SE	1.3.2.0	SuzuMcpherson@protonmail.com, AsuxidOruraep1999@o2.pl
f804dfcd78436fa325ba29d175830e239013a8bd44c1a0f8fe75ed356a526024	3/2/2019 19:41	CA	1.3.2.0	SuzuMcpherson@protonmail.com, AsuxidOruraep1999@o2.pl
eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0	3/2/2019 19:41	CH	1.3.2.0	SuzuMcpherson@protonmail.com, AsuxidOruraep1999@o2.pl
47f5a231f7cd0e36508ca6ff8c21c08a7248f0f2bd79c1e772b73443597b09b4	2/3/2019 17:48	DE	1.2.0.0	PhanthavongsaNeveyah@protonmail.com, AperywsQaroci@o2.pl
7852b47e7a9e3f792755395584c64dd81b68ab3cbcdf82f60e50dc5fa7385125	2/3/2019 15:32	US	1.2.0.0	RomanchukEyla@protonmail.com, Couwetlzofofo@o2.pl
14e8a8095426245633cd6c3440afc5b29d0c8cd4acefd10e16f82eb3295077ca	1/28/2019 18:13	ES	1.1.1.0	DutyuEnugev89@o2.pl, SchreiberEleonora@protonmail.com
2070304ea7328c6a4c0101baa48da8c219112b24b48e7f347e2265a3c9d6a856	1/28/2019 17:56	NL	1.1.1.0	QtuitihGaqij89@o2.pl, DrillockMorgen@protonmail.com
9128e1c56463b3ce7d4578ef14ccdfdba15ccc2d73545cb541ea3e80344b173c	1/25/2019 16:30	SE	N/A	N/A
b0b6d39accd2ba94f23bde9f76d0750f858d6d463e547357e6f2056e6e7689bf	1/25/2019 16:30	CA	N/A	N/A
c3d334cb7f6007c9ebee1a68c4f3f72eac9b3c102461d39f2a0a4b32a053843a	1/25/2019 16:30	NL	N/A	AbbsChevis@protonmail.com, ljuqodiSunovib98@o2.pl
6e69548b1ae61d951452b65db15716a5ee2f9373be05011e897c61118c239a77	1/25/2019 16:30	NL	1.1.1.0	AbbsChevis@protonmail.com, ljuqodiSunovib98@o2.pl
f3c58f6de17d2ef3e894c09bc68c0afcce23254916c182e44056db3cad710192	1/23/2019 22:42	FR	1.1.0.0	CottleAkela@protonmail.com, QyavauZehyco1994@o2.pl
bdf36127817413f625d2625d3133760af724d6ad2410bea7297ddc116abc268f	1/23/2019 22:42	RO	1.1.0.0	QyavauZehyco1994@o2.pl, CottleAkela@protonmail.com
8cfbd38855d2d6033847142fdfa74710b796daf465ab94216fbbbe85971aee29	1/16/2019 19:27	NL	1.0.2.0	AbbsChevis@protonmail.com, ljuqodiSunovib98@o2.pl
5b0b972713cd8611b04e4673676cdff70345ac7301b2c23173cdfcaff564225c	1/16/2019 1:23	RO	1.0.1.0	AbbsChevis@protonmail.com, ljuqodiSunovib98@o2.pl
ad587dc5b65ac52a6c62a141f2a86f5d39a38b1d39eb825cf496949d28f51eb2	1/5/2019 11:34	CH	0.9.9.0	kv8f6fx@protonmail.com, kv8f6fx@tutanota.com
1dcbcd1f86c658f262c44db3dc6bf933f29177c5e828e628a149e8d4f11e7b3c	1/5/2019 11:33	NL	0.9.9.0	N/A
97a2ab7a94148d605f3c0a1146a70ba5c436a438b23298a1f02f71866f420c43	1/5/2019 11:33	NL	0.9.9.0	N/A



## APPENDIX B: APPROXIMATE RANSOMWARE TIMELINE

The following provides a high-level overview of ransomware and related activity. The list is not meant to be comprehensive given the sheer volume of activity, especially within the past five years, and lifespans of certain ransomware variants are open to interpretation and the limitations of relying on public information and telemetry. There are multiple potential points of disagreement in the following timeline, but overall the purpose is to provide an overview of how ransomware and related activity has evolved.



## ENDNOTES

- 1 Ransomware: Unlocking the Lucrative Criminal Business Model – Palo Alto Unit42 ([https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en\\_US/resources/research/ransomware-report](https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/ransomware-report)); The Computer Virus that Haunted Early AIDS Researchers – Kaveh Waddell, The Atlantic (<https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/>)
- 2 Cracking the Code: The History of Gpcode – David Emm, Computer Fraud & Security (<https://www.sciencedirect.com/science/article/abs/pii/S1361372308701398>)
- 3 Ransomware: Unlocking the Lucrative Criminal Business Model – Palo Alto Unit42; CryptoLocker: Everything You Need to Know – Jeff Petters, Varonis (<https://www.varonis.com/blog/cryptolocker/>); A History of Ransomware
- 4 Ransomware Timeline – Carbon Black ([https://cdn.www.carbonblack.com/wp-content/uploads/2016/09/Ransomware\\_Timeline\\_Carbon\\_Black.jpg](https://cdn.www.carbonblack.com/wp-content/uploads/2016/09/Ransomware_Timeline_Carbon_Black.jpg))
- 5 ThreatList: Ransomware Costs Double in Q4, Sodinokibi Dominates – Lindsey O'Donnell, ThreatPost (<https://threatpost.com/threatlist-ransomware-costs-double-in-q4-sodinokibi-dominates/152200/>)
- 6 Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool – Nichole Perlroth and David E. Sanger, The New York Times (<https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html>); What You Need to Know about the WannaCry Ransomware – Symantec Security Response (<https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack>)
- 7 North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions – US Department of Justice (<https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and>); How US Authorities Tracked Down the North Korean Hacker behind WannaCry – Catalin Cimpanu, ZDNet (<https://www.zdnet.com/article/how-us-authorities-tracked-down-the-north-korean-hacker-behind-wannacry/>); WannaCry and LazarusGroup – The Missing Link? – Kaspersky GReAT, SecureList (<https://securelist.com/wannacry-and-lazarus-group-the-missing-link/78431/>)
- 8 The WannaCry Ransomware Hackers Made Some Real Amateur Mistakes – Andy Greenberg, Wired (<https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/>)
- 9 Cyberattack Hits Ukraine Then Spreads Internationally – Nicole Perlroth, Mark Scott, and Sheera Frenkel, The New York Times (<https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html>)
- 10 The Untold Story of NotPetya, the Most Devastating Cyberattack in History – Andy Greenberg, Wired (<https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>); New Petya/NotPetya/ExPetr Ransomware Outbreak – Kaspersky (<https://www.kaspersky.com/blog/new-ransomware-epidemics/17314/>); Statement from the Press Secretary – United States Office of the President (<https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/>); Petya Ransomware – US Department of Homeland Security Cyber-Infrastructure Security Agency (<https://www.us-cert.gov/ncas/alerts/TA17-181A>)
- 11 TeleBots are Back: Supply-Chain Attacks against Ukraine – Anton Cherepanov, ESET (<https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/>)
- 12 Altran Technologies: Update on the Cyber Attack – Altran (<https://www.globenewswire.com/news-release/2019/02/21/1738988/0/en/ALTRAN-TECHNOLOGIES-Update-on-the-cyber-attack.html>); New LockerGoga Ransomware Allegedly Used in Altran Attack – Ionut Ilascu, BleepingComputer (<https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/>)
- 13 Le Ransomware LockerGoga Identifié lors d'une Attaque contre Altran – L'Agence Française de la Santé

Numérique (<https://cyberveille-sante.gouv.fr/cyberveille/1166-le-ransomware-lockergoga-identifie-lors-dune-attaque-contre-altran-2019-02-01>); Rapport Menaces et Incidents du CERT-FR – CERT-FR (<https://www.cert.ssi.gouv.fr/cti/CERTFR-2019-CTI-001/>); Informations Concernant les Rancongiels LockerGoga et Ryuk – CERT-FR (<https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-ACT-005.pdf>)

14 Comodo CA is Now Sectigo – Sectigo (<https://sectigo.com/comodo>)

15 Analysis of LockerGoga Ransomware – F-Secure (<https://blog.f-secure.com/analysis-of-lockergoga-ransomware/>); Unlocking the LockerGoga Ransomware and What Makes it Unique – VIPRE Labs (<https://labs.vipre.com/unlocking-the-lockergoga-ransomware-and-what-makes-it-unique/>); LockerGoga: Ransomware Targeting Critical Infrastructure – Japser Manuel & Joie Salvio, Fortinet (<https://www.fortinet.com/blog/threat-research/lockergoga-ransomware-targeting-critical-infrastructure.html>)

16 Ransomware Behind Norsk Hydro Attack: LockerGoga Ransomware – Anton Ziukin, SentinelOne (<https://www.sentinelone.com/blog/lockergoga-ransomware-targets-industrial-companies/>); What You Need to Know about the LockerGoga Ransomware – TrendMicro (<https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware>)

17 Hydro Subject to Cyber Attack – Norsk Hydro (<https://www.hydro.com/en/media/news/2019/hydro-subject-to-cyber-attack/>); Cyber-attack on Hydro – Norsk Hydro (<https://www.hydro.com/en/media/on-the-agenda/cyber-attack/>); LockerGoga Ransomware Sends Norsk Hydro into Manual Mode – Ionut Ilascu, BleepingComputer (<https://www.bleepingcomputer.com/news/security/lockergoga-ransomware-sends-norsk-hydro-into-manual-mode/>); Nordic Metals Firm Hydro Restoring Systems after Cyber Attack – Nerijus Adomaitis and Terje Solsvik, Reuters (<https://www.reuters.com/article/us-norsk-hydro-cyber/hydro-still-working-to-restore-operations-after-cyber-attack-idUSKCN1R10PU>)

18 How LockerGoga Took Down Hydro – Ransomware Used in Targeted Attacks aimed at Big Business – Kevin Beaumont (<https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880>)

19 Skreddersydd dobbeltangrep mot Hydro – Henrik Lied, Peter Svaar, Dennis Ravndal, Anders Brekke, and Kristine Hirsti, NRK (<https://www.nrk.no/norge/skreddersydd-dobbeltangrep-mot-hydro-1.14480202>)

20 EXCLUSIVE: How the Norsk Hydro Cyberattack Unfolded – Andrea Hotter, Metal Bulletin (<https://www.metal-bulletin.com/Article/3890232/EXCLUSIVE-How-the-Norsk-Hydro-cyberattack-unfolded.html>)

21 IT-sjefen i Hydro om dataangrepet: – Man tror krisen blir stor, så blir den enda verre – Line Tomter & Martin Gundersen, NRK ([https://www.nrk.no/norge/it-sjefen-i-hydro-om-dataangrepet\\_-\\_man-tror-krisen-blir-stor\\_-sa-blir-den-enda-verre-1.14515043](https://www.nrk.no/norge/it-sjefen-i-hydro-om-dataangrepet_-_man-tror-krisen-blir-stor_-sa-blir-den-enda-verre-1.14515043))

22 Security Primer – LockerGoga – Center for Internet Security (<https://www.cisecurity.org/white-papers/security-primer-lockergoga/>); FBI Issues Alert for LockerGoga and MegaCortex Ransomware – Lawrence Abrams, BleepingComputer (<https://www.bleepingcomputer.com/news/security/fbi-issues-alert-for-lockergoga-and-megacortex-ransomware/>)

23 CVE-2019-0859 Win32k Elevation of Privilege Vulnerability – Microsoft (<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0859>)

24 Rolling Back Ryuk Ransomware – Sophos (<https://news.sophos.com/en-us/2019/10/04/rolling-back-ryuk-ransomware/>); Ryuk Ransomware Cripples MSP and Major Newspapers, Represents Dangerous Shift Toward Coordinated Attacks – Jonathan Crowe, Ninja RMM (<https://www.ninjarmm.com/blog/ryuk-ransomware-attacks-newspapers-msp-dataresolution/>)

25 Ransomware of Wiper? LockerGoga Straddles the Line – Cisco Talos (<https://blog.talosintelligence.com/2019/03/lockergoga.html>)

- 26 A list of all known LockerGoga samples is provided in Appendix A.
- 27 Norsk Hydro Tests AI in Cyber Defenses After Attack – Catherine Stupp, The Wall Street Journal (<https://www.wsj.com/articles/norsk-hydro-tests-ai-in-cyber-defenses-after-attack-11566207000>)
- 28 Hilde Merete Aasheim Appointed New CEO of Hydro – Norsk Hydro (<https://www.hydro.com/en/media/news/2019/hilde-merete-aasheim-appointed-new-ceo-of-hydro/>)
- 29 Investigators Warned Other Companies After Norsk Hydro Attack – Catherine Stupp, The Wall Street Journal (<https://www.wsj.com/articles/investigators-warned-other-companies-after-norsk-hydro-attack-11566552601>)
- 30 Hackerne i Hydro-saken planla flere cyberangrep – Aftenposten (<https://www.aftenposten.no/norge/i/b5o3yA/hackerne-i-hydro-saken-planla-flere-cyberangrep>); Kripes om Hydro-hackingen: Har potensielt forhindret angrep mot andre bedrifter – David Bach and Sigrid Moe, E24 (<https://e24.no/teknologi/i/9vG6R5/kripes-om-hydro-hackingen-har-potensielt-forhindret-angrep-mot-andre-bedrifter>)
- 31 Nederlandse bedrijven slachtoffer van geavanceerde gijzelsoftware – Joost Schellevis, NOS (<https://nos.nl/artikel/2312363-nederlandse-bedrijven-slachtoffer-van-geavanceerde-gijzelsoftware.html>); A Guide to LockerGoga, the Ransomware Crippling Industrial Firms – Andy Greenberg, Wired (<https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/>)
- 32 Business and Industry in Norway – The Structure of the Norwegian Economy – Norwegian Government (<https://www.regjeringen.no/en/dokumenter/Business-and-industry-in-Norway---The-structure-of-the-Norwegian-economy/id419326/>)
- 33 LockerGoga Ransomware Victims: Dozens of Industrial, Manufacturing Firms – DH Kass, MSSP Alert (<https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/lockergoga-victims/>)
- 34 Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware – Brendan McKeague, Van Ta, Ben Fedore, Geoff Ackerman, Alex Pennino, Andrew Thompson, and Douglas Bienstock, FireEye (<https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html>)
- 35 FIN6 – MITRE (<https://attack.mitre.org/groups/G0037/>)
- 36 Bulletin d'alerte du CERT-FR – CERT-FR (<https://www.cert.ssi.gouv.fr/alerte/CERTFR-2019-ALE-003>); Informations concernant les rançongiciels LockerGoga et Ryuk – CERT-FR (<https://www.cert.ssi.gouv.fr/uploads/CERTFR-2019-ACT-005.pdf>)
- 37 Ransomware Forces Two Chemical Companies to Order 'Hundreds of New Computers' – Lorenzo Franceschi-Bicchierai, Motherboard ([https://www.vice.com/en\\_us/article/8xyj7g/ransomware-forces-two-chemical-companies-to-order-hundreds-of-new-computers](https://www.vice.com/en_us/article/8xyj7g/ransomware-forces-two-chemical-companies-to-order-hundreds-of-new-computers)); A Guide to LockerGoga, the Ransomware Crippling Industrial Firms – Andy Greenberg, Wired (<https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/>)
- 38 Aebi Schmidt Latest Manufacturer Dealing with Cyberattack – Doug Olenick, SCMagazine (<https://www.scmagazine.com/home/security-news/malware/aebi-schmidt-latest-manufacturer-dealing-with-cyberattack/>)
- 39 LockerGoga, MegaCortex Ransomware Share Unlikely Traits – Kelly Sheridan, DarkReading (<https://www.darkreading.com/perimeter/lockergoga-megacortex-ransomware-share-unlikely-traits/d/d-id/1334696>)
- 40 MegaCortex, Deconstructed: Mysteries Mount as Analysis Continues – Andrew Brandt, Sophos (<https://news.sophos.com/en-us/2019/05/10/megacortex-deconstructed-mysteries-mount-as-analysis-continues/>)
- 41 FBI Issues Alert for LockerGoga and MegaCortex Ransomware – Lawrence Abrams, BleepingComputer (<https://www.bleepingcomputer.com/news/security/fbi-issues-alert-for-lockergoga-and-megacortex-ransomware/>); FBI Issues Alert on LockerGoga and MegaCortex Ransomware – Chris Brook, DigitalGuardian (<https://www.digitalguardian.com/news/fbi-issues-alert-on-lockergoga-and-megacortex-ransomware>)

[digitalguardian.com/blog/fbi-issues-alert-lockergoga-and-megacortex-ransomware](https://digitalguardian.com/blog/fbi-issues-alert-lockergoga-and-megacortex-ransomware))

42 New Version of MegaCortex Targets Business Disruption – Leo Fernandes, Accenture (<https://www.accenture.com/us-en/blogs/blogs-megacortex-business-disruption>); Technical Analysis of MegaCortex Version 2 Ransomware – Accenture ([https://www.accenture.com/\\_acnmedia/PDF-106/Accenture-Technical-analysis-MegaCortex.pdf](https://www.accenture.com/_acnmedia/PDF-106/Accenture-Technical-analysis-MegaCortex.pdf))

43 EKANS Ransomware and ICS Operations – Dragos (<https://dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/>)

44 Snake: Industrial-Focused Ransomware with Ties to Iran – Otorio (<https://www.otorio.com/blog/posts/snake-industrial-focused-ransomware-with-ties-to-iran>); Ransomware Linked to Iran, Targets Industrial Controls – Gwen Ackerman, Bloomberg (<https://www.bloomberg.com/news/articles/2020-01-28/-snake-ransomware-linked-to-iran-targets-industrial-controls>)

45 Getting the Story Right, and Why It Matters – Joe Slowik (<https://pylos.co/2020/01/28/getting-the-story-right-and-why-it-matters/>)

46 Shamoon the Wiper: Further Details – Dmitry Tarakanov, Kaspersky (<https://securelist.com/shamoon-the-wiper-further-details-part-ii/57784/>); In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back – Nicole Perlroth, The New York Times (<https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html>); Hack on Saudi Aramco hit 30,000 Workstations, Oil Firm Admits – John Leyden, The Register ([https://www.theregister.co.uk/2012/08/29/saudi\\_aramco\\_malware\\_attack\\_analysis/](https://www.theregister.co.uk/2012/08/29/saudi_aramco_malware_attack_analysis/))

47 Now You See It, Now You Don't: Wipers in the Wild – Saher Naumann, Virus Bulletin (<https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Naumaan.pdf>)

48 Shamoon 2: Return of the Disttrack Wiper – Robert Falcone, PaloAlto Unit42 (<https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/>); Shamoon: Destructive Threat Re-Emerges with New Sting in Its Tail – Symantec (<https://www.symantec.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail>); Everything We Know about Ukraine's Power Plant Hack – Kim Zetter, Wired (<https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/>); ICS Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure – Cyber-Infrastructure Security Agency, US Department of Homeland Security (<https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01>)

49 A Flawed Ransomware Encryptor – Victor Alyushin & Fedor Sinitsyn, Kaspersky (<https://securelist.com/a-flawed-ransomware-encryptor/69481/>); Faulty Ransomware Renders Files Unrecoverable, Even by the Attacker – Lucian Constantin, PCWorld (<https://www.pcworld.com/article/3022162/faulty-ransomware-renders-files-unrecoverable-even-by-the-attacker.html>)

50 Petya – Taking Ransomware to the Low Level – MalwareBytes (<https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/>)

51 Hack Petya – Leo Stone (<https://github.com/leo-stone/hack-petya>); Decrypting NotPetya/Petya: Tools for Recovering your MFT after an Attack – Sebastian Eschweiler, CrowdStrike (<https://www.crowdstrike.com/blog/decrypting-notpetya-tools-for-recovering-your-mft-after-an-attack/>)

52 Petya Ransomware Outbreak: Here's What You Need to Know – Symantec (<https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper>)

53 NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft – Karan Sood & Shaun Hurley, CrowdStrike (<https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/>)



- 54 Cyberattack Hits Ukraine Then Spreads Internationally – Nicole Perlroth, Mark Scott, and Sheera Frenkel, The New York Times (<https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html>)
- 55 UK and US Blame Russia for ‘Malicious’ NotPetya Cyber-Attack – BBC (<https://www.bbc.com/news/uk-politics-43062113>)
- 56 ExPetr/Petya/NotPetya is a wiper, Not Ransomware – Anton Ivanov & Orkhan Mamedov, Kaspersky (<https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/>); Petya.2017 is a Wiper not A Ransomware – Matt Suiche, Comae (<https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b>)
- 57 Petya.2017 is a Wiper not A Ransomware – Matt Suiche, Comae (<https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b>)
- 58 The MeDoc Connection – David Maynor, Aleksandar Nikolic, Matt Olney & Yves Younan, Cisco Talos (<https://blog.talosintelligence.com/2017/07/the-medoc-connection.html>); TeleBots are Back: Supply-Chain Attacks against Ukraine – Anton Cherepanov, ESET (<https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/>)
- 59 Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference (École militaire, Paris) – NATO ([https://www.nato.int/cps/en/natohq/opinions\\_154462.htm](https://www.nato.int/cps/en/natohq/opinions_154462.htm))
- 60 Big Game Hunting: How Ryuk Ransomware Takes Down Imposing Targets – Max Heinemeyer, DarkTrace (<https://www.darktrace.com/en/blog/big-game-hunting-how-ryuk-ransomware-takes-down-its-imposing-targets/>)
- 61 Russia’s Work with Cyber Criminals Surging – Former National Security Official – Rebecca Falconer, Axios (<https://www.axios.com/russia-spies-working-with-cyber-criminals-5c2f12f7-8f25-419a-a850-3bc89de346a3.html>); Disorganized Crime and State-Backed Hackers: How the Cybercrime and Cyberwar Landscape is Constantly Changing – Karen Roby, ZDNet (<https://www.zdnet.com/article/disorganized-crime-and-state-backed-hackers-the-cybercrime-landscape-is-changing/>); Chinese Cyberhackers ‘Blurring the Line between State Power and Crime’ – Josh Taylor, The Guardian (<https://www.theguardian.com/technology/2019/aug/08/chinese-cyberhackers-blurring-line-between-state-power-and>)
- 62 Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks – US Department of the Treasury (<https://home.treasury.gov/news/press-releases/sm0312>); Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups – US Department of the Treasury (<https://home.treasury.gov/news/press-releases/sm774>); U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations – US Department of Justice (<https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and>)
- 63 How Ukraine Became a Test Bed for Cyberweaponry – Laurens Cerulus, Politico (<https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/>); How an Entire Nation Became Russia’s Test Lab for Cyberwar – Andy Greenberg, Wired (<https://www.wired.com/story/russian-hackers-attack-ukraine/>)
- 64 Was It an Act of War? That’s Merck Cyber Attack’s \$1.3 Billion Insurance Question – Riley Griffin, Katherine Chiglinksky & David Voreacos, Insurance Journal/Bloomberg (<https://www.insurancejournal.com/news/national/2019/12/03/550039.htm>); Big Companies Thought Insurance Covered a Cyberattack. They May be Wrong – Adam Satariano & Nicole Perlroth, The New York Times (<https://www.nytimes.com/2019/04/15/technology/cyber-insurance-notpetya-attack.html>)
- 65 For example, the lawsuits resulting from the 2013 Target breach: Target to Pay \$18.5 Million to 47 States in Security Breach Settlement – Rachel Abrams, The New York Times (<https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html>); Target in \$39.4 Million Settlement with Banks over Data Breach – Jonathan Stempel & Nandita Bose, Reuters (<https://www.reuters.com/article/us-target-breach-settlement-idUSKBN0TL20Y20151203>)