


# How Lockergoga took down Hydro — ransomware used in targeted attacks aimed at big business

---

 [doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880](https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880)

Kevin Beaumont

April 18, 2019



[Kevin Beaumont](#)

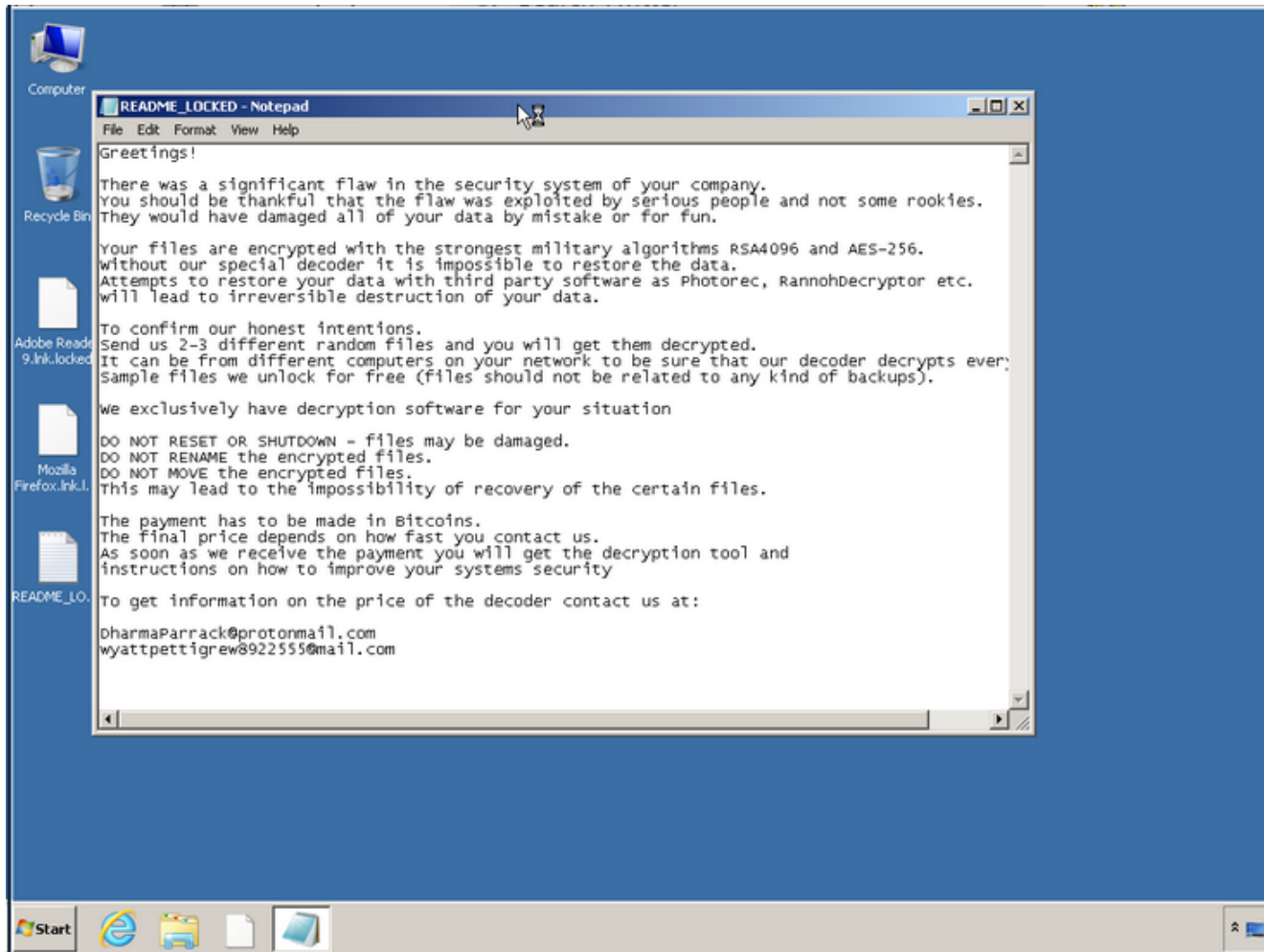
[Follow](#)

Mar 21, 2019

.

13 min read

This week Norsk Hydro, a large multinational manufacturer with 35,000 staff and over 100 years of history, had the nightmare scenario of a worldwide apparent ransom attempt — their systems began to malfunction, and attackers had placed the following ransom note on their business and some production systems across the world:



The ransom note.

Each impacted system had four key elements:

- They all ran Microsoft Windows.
- Files, including some system files, had been encrypted.
- The network interface on every system had been disabled.
- The local user accounts on every system had their password changed.

From what I can gather, they have an existing security team and controls, and one of the things you haven't seen this time is people online highlighting a ton of obvious security flaws with their systems (see also, Equifax etc) — *so what happened?*

“Essentially, there are cascading failures in the technology and security industry to protect customers.”

## The event

---

The timeline is known as so:

- .

- Around midnight (UTC) on Tuesday 19th March, security events were detected in Americas locations of Hydro.
- In the early hours of the morning, the attack began.
- By 5am (UTC) Hydro had opted to disconnect their worldwide network (WAN).
- Over a month later, the company is still attempting to recover from the attack, and most of its 160 manufacturing locations are still operating in manual (non-IT driven) operations.

## Why Norsk Hydro ASA as a target?

---

I do not know, nor care to speculate. I can say for sure they were specifically targeted, as each LockerGoga payload contains a unique four digital reference number and information unique to the target.

As business began on Tuesday 19th March 2019, Hydro had no website, no network and no self managed IT. This is an incredibly difficult situation for a manufacturing company.

The CEO had started the job the day before.

Hydro posted notices at their 40 offices and manufacturing facilities across the world asking staff to disconnect their devices from local networks, and the recovery effort began.

They informed stock markets they were moving to ‘manual production’, which means they would operate factories without modern IT.

Each local factory manager was tasked with maintaining customer orders — for example, some operated from pre-printed list of orders.

For communication, Norsk Hydro ASA uses Office365, which was completely unimpacted — so staff could still communicate with each other, the press and customers using mobile phones and tables. Had Hydro not already moved communications to a managed cloud service, the situation would have been more grave.

For communication with the outside world they used their Facebook account, and redirected hydro.com to an Azure temporary website:

← → ↻ 🏠 ⚠ Not secure | hydrotemp.azurewebsites.net

Norsk Hydro: Hydro subject to cyber-attack

Hydro became victim of an extensive cyber-attack in the early hours of Tuesday (CET), impacting operations in several of the company's business areas.

IT-systems in most business areas are impacted and Hydro is switching to manual operations as far as possible. Hydro is working to contain and neutralize the attack, but does not yet know the full extent of the situation.

**Investor contact**  
 Stian Hasle  
 +47 97736022  
[Stian.Hasle@hydro.com](mailto:Stian.Hasle@hydro.com)

**Press contact**  
 Halvor Molland  
 +47 92979797  
[Halvor.Molland@hydro.com](mailto:Halvor.Molland@hydro.com)

Follow us on Facebook:  
[facebook.com/norskhydroasa](https://facebook.com/norskhydroasa)

This website has since been moved to behind Cloudflare, a managed DDoS protection provider.

## Incident representation

---



Hydro started the best incident representation response plan I've ever seen — they had a temporary website up, they told the press, they told their staff, they apparently didn't hide any details — they even had daily webcasts with the most senior staff talking through what was happening, and answering questions. On the 2nd day they even took questions from webcast watchers.



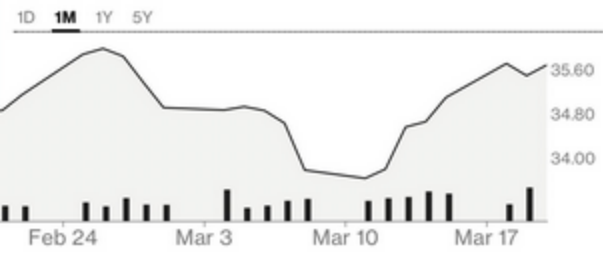
NHY:NO Oslo  
Norsk Hydro ASA [COMPANY INFO](#)

**35.87** NOK +0.29 +0.82% ▲

+ ADD TO WATCHLIST

● MARKET OPEN  
AS OF 05:43 AM EDT 03/20/2019 EDT

OPEN	PREV CLOSE
35.20	35.58
VOLUME	MARKET CAP
1,513,185	73.615B
DAY RANGE	52 WEEK RANGE
35.17-35.94	33.02-56.40



In contrast to some other incidents, their stock price actually went up — despite a difficult trading period for past 2 years involving some major business setbacks, they have actually gained in value.

## Incident response

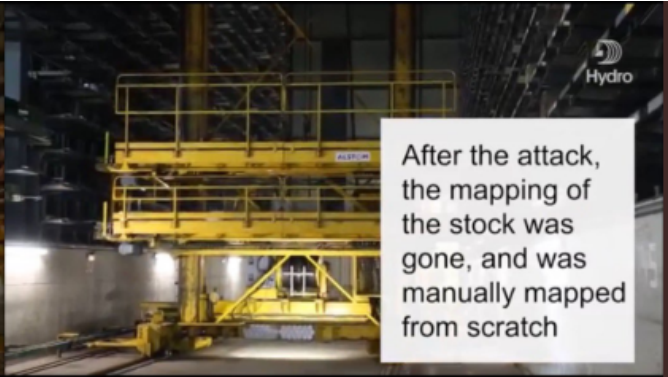
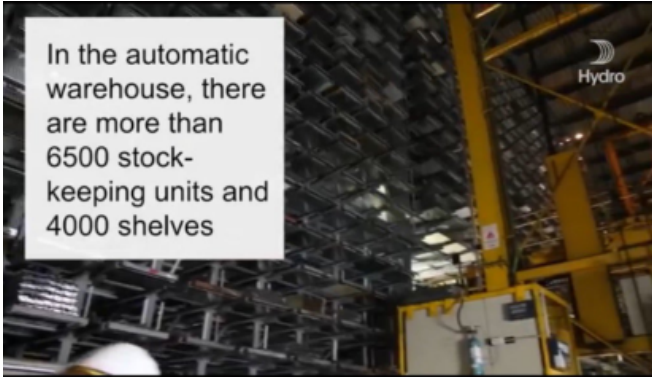
Hydro's website says they have flown in staff from Microsoft and unnamed companies to help them recover. They have also engaged with national cybercrime bodies, industry groups and police authorities. The incident is now a police investigation.

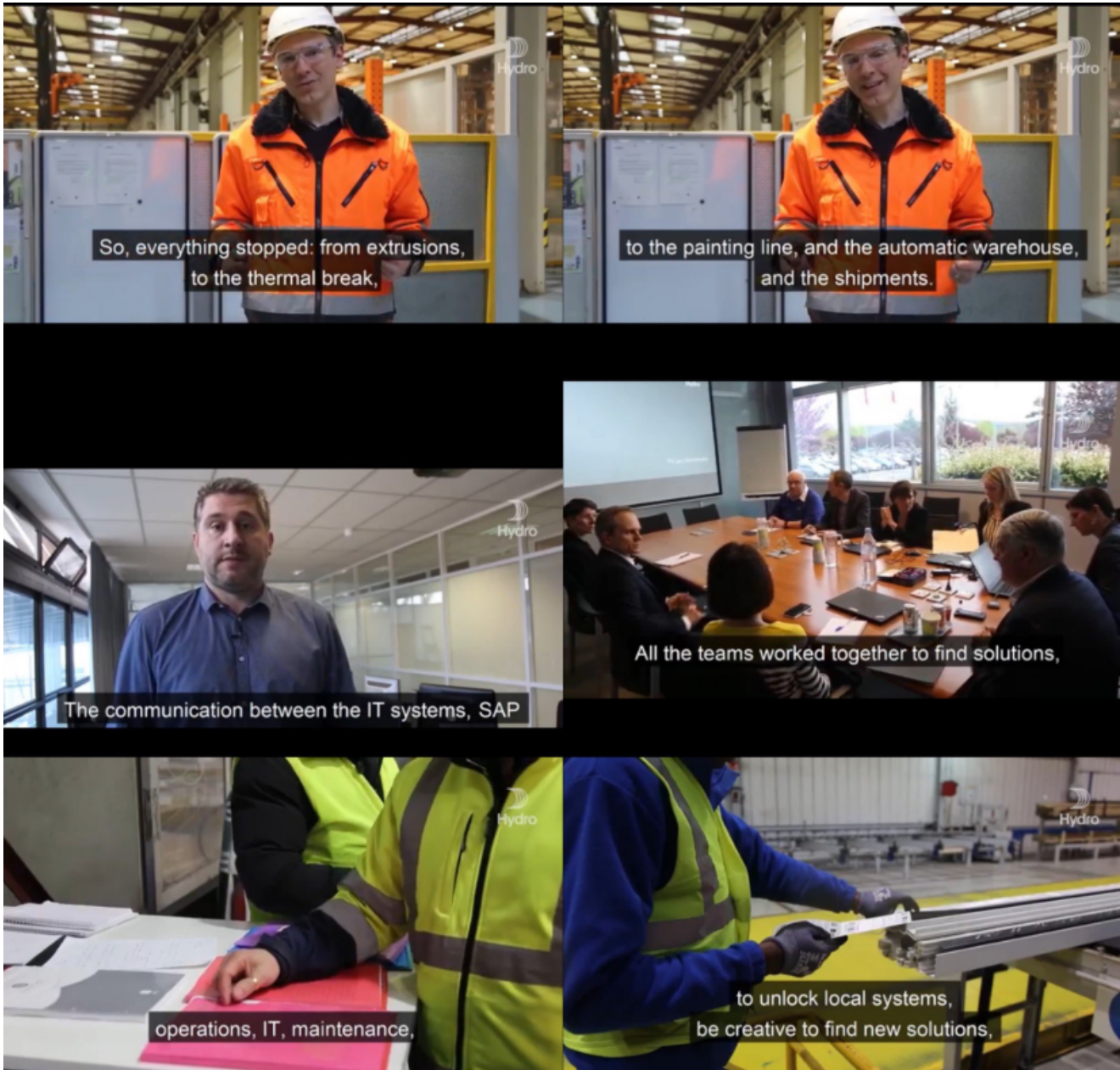
Their CFO says they have backups of data which they are attempting to restore, and they have not paid a ransom.

They say it is unknown how long recovery will take, although in an interview with a Norwegian news organisation the CIO says full recovery will take months.

Hydro have provided videos about their recovery efforts:







## What went wrong?

---

### Security controls and industry

---

Several weeks ago, I highlighted on Twitter that despite a high profile attack on Altran in January (34,000 staff members) using LockerGoga, a vast majority of endpoint security anti-malware products were failing to detect it. I highlighted this because @malwrhunterteam on Twitter sent me a message saying 'look at this and the poor detection':

SHA256: eda26a1cd80aac1c42cdbba9af813d9c4bc81f6052080bc33435d1e076e75aa0

File name: yxugwjud6698.exe

Detection ratio: 0 / 67

Analysis date: 2019-03-08 12:43:50 UTC ( 1 week, 6 days ago ) [View latest](#)

Analysis | File detail | Relationships | Additional information | Comments 5 | Votes

Antivirus	Result	Update
Acronis	✓	20190222
Ad-Aware	✓	20190308
AegisLab	✓	20190308
AhnLab-V3	✓	20190308
Alibaba	✓	20190306
ALYac	✓	20190308

As you can see above the detection rate was 0 out of 67 anti-virus engines. Now, before vendors get annoyed, I am well aware that VirusTotal results don't tell the full story — however having zero detection from any engine is **an extremely bad sign**. I actually detonated the ransomware myself on several real world endpoints (in isolated fashion — as you'll learn later it doesn't self replicate too) and I couldn't find an endpoint security tool which actually triggered a detection (although Cisco's ThreatGrid sandbox technology did classify it as Generic Ransomware).

I used that Twitter thread to pressure several anti-malware producers into action, DMing staff I knew at said companies to get them to take a look.

I found a few more samples in VirusTotal, clearly still in development — those, too, had little to no detection. I sent them on informally.





After the Altran attack, which downed systems at a 34,000 employee company, only a handful of dialogue happened in the industry — I can only find one news article which actually mentions LockerGoga, for example, and little to no technical detail.

As far as I'm aware there is not any centralised way to contact everybody in antivirus industry on international interest, so I completely forgot about it a few people in, and went to watch Captain Marvel instead.

Essentially, Norsk Hydro's anti-malware solution did not have detection for the threat because not all the industry players were paying attention to a cartoon porg on Twitter (me) and a random person who I think doesn't work in the industry (MalwareHunterTeam).

I'm not saying that's how the industry should work, by the way, and I know it sounds self aggrandising — but I'm trying to make the point that maybe, as an industry, we're really good at hyping threats in the media which are not practical in the real world and not great at looking at all the real world, actual attack data.

While we may be sharing Indicators of Compromise — IoCs — a long list of meaningless hashes aren't enough to protect people. The cyber security industry and partners missed a trick here, as we knew a major company had been attacked in a meaningful way, but it wasn't followed up.

Additionally, the digital certificate being used to sign the ransomware was used to sign other malicious code — in fact it had only been used to sign malicious code — and had been issued to a company with £1 of assets which wasn't even a trading company. Upon being informed of this, the Certificate Authority failed to revoke the certificate in a timely manner — a continuing issue with the same Certificate Authority, which is trusted by all Windows

certificate stores. To compound the issue even when revoked a vast majority of security tools fail to do anything, as they do not retrieve the CRL and check the serial number for revocation. All security and technology should immediately block or flag code signed with specifically distrusted certificates. Essentially, there are cascading failures in the technology and security industry to protect customers.

Another element — some LockerGoga deployments stop endpoint security products (and backup products) before further deployment:

## Lateral movement

---

LockerGoga does not have any code to self spread, meaning it can not self replicate around a network — unlike other destructive code such as WannaCry and NotPetya.

This may actually be intentional — because it doesn't use C2 ('Command and Control') servers and DNS traffic it means it is less likely to be picked up by network detection and endpoint classification tools, too.

So how did they plant LockerGoga? I speculated above it was probably using Active Directory — something like scheduled tasks or services. The initial assessment from NorCERT appears to back this up, although the investigation is still ongoing:

### Løsepenge-virus

*«NorCERT varsler om at Hydro er utsatt for et ransomwareangrep (LockerGoga). Angrepet ble kombinert med et angrep mot Active Directory (AD).*

*NorCERT ber om informasjon om andre er rammet av tilsvarende hendelser. NorCERT bistår Hydro og hendelsen regnes som pågående», står det i varselet.*

In order to pull that off you need remote access — it is not known how the attackers got access to Norsk Hydro's network at this stage. I would actually call upon Hydro to do something very unusual (so far) in incident response and open source release some of the information in this area later, as I strongly believe it can help protect every company — including their customers.

Once inside their network, they must have had Domain Administrator rights to execute the attack. Usually in companies it is extremely easy to get this access, despite the industry hard selling a range of privileged access management tools, by simply:

- fishing logins out of memory using Mimikatz

- taking passwords from Active Directory Group Policy Preferences — they're often right there in the XML files. It's the go to, bread and butter of 'Red Teams'.
- Pass The Hash attacks and surf around the entire network using the same local administrator passwords because almost nobody deploys Microsoft .

However it happened, they got to domain administrator. Like I say, normally this isn't problematic as almost all companies make the same simple Active Directory configuration errors and fail to prioritise remediation.

## Got root?

---

Once you're an Active Directory administrator, if you are an attacker you can place the executable somewhere where every system in an organisation can reach — normally, organisations universally firewall accept Active Directory traffic internally.

Bingo, you have the keys to the kingdom — the only thing stopping you now is security controls around endpoint malware, and as we already established those won't detect LockerGoga at the time of the attack.



So you can place it on a Domain Controller in the NETLOGON share under Sysvol, which is replicated to every site with a Domain Controller. Then you can use Group Policy such as scheduled task creation or service creation to automatically start the LockerGoga executable.

Immediately, every single laptop, desktop and server connected to Active Directory will trigger the malicious software.

Another way to do it is, of course, psexec \* – psexec handily supports wildcards.

Many people will talk about ‘air gapping’ Industrial Control Systems (ICS), however many organisations — almost every organisation I’ve met, in fact — ends up connecting some elements to Active Directory for benefits such as easy licensing, centralised account control etc. This leads to a situation where production systems — I’m not talking the technologist use of production, I mean the manufacturing industry term of systems which do something critical on the coalface — are linked to a central system which can be misused.

I should be clear here that I’m not saying ICS systems shouldn’t be joined to Active Directory because risk assessment wise unless you’re an extremely high profile target the benefits may outweigh the risks. I am saying they should probably be joined to an entirely separate Active Directory forest, and administrator access should be incredibly tightly controlled.

## The impact

---

### Left adrift

---

LockerGoga does a few things, some unique:

- It ends up using every CPU core and thread during encryption and is very, very fast. This is because it spawns hundreds of executables for encryption. On an average system within a few minutes, it is toast.
- Additionally, some technical blogs on LockerGoga mention a list of file types that are encrypted which only includes things like Office files — I can say first hand that it also encrypts system files such as DLL files across the C: drive. Since it is deployed as administrator level using Active Directory, it has full control of all files.
- It depends on the version being run (on VirusTotal you can see different LockerGoga executables with different features) but newer versions use netsh.exe to disable all network cards after encryption is done.
- It then changes every local administrator account password.
- It then logs you off, using logoff.exe.

## Recovery

---

On laptops and desktops, what you’re left with is the ability to log back in using domain user accounts (it can’t impact Active Directory accounts) on a cached basis, but your users are off the network, as an administrator you cannot reach the PC remotely to fix it, and all the user can do is read the ransom note. They cannot use email, they cannot read a broadcast from the company on their PC, they cannot work likely as their files are encrypted.

You cannot log in at the physical console to recover the system as you do not know the local administrator details any more.

On servers you have service issues, as changing the local administrator passwords can impact system services using local accounts (such as Microsoft SQL, Sophos etc).

## Learning opportunities

---

Here's the top ten things I think we can take away from this:

### Governments and industry

---

There is a serious lack of open information sharing after ransomware incidents which involve unusual code. Right now we're super protected against, say, WannaCry — but after Altran, a lack of transparency and openness lead to the same issue elsewhere.

This will happen again with other threats. In my opinion it is in national and international interests for governments to be informed of technical details of all major business incidents around malicious code causing outages (e.g. wipers, ransomware) and that information should be shared with security vendors and other governments. I know many organisations won't want to provide this information so governments or regulators might need levers to pull to compel disclosure.

### Companies

---

Organisations should look at how Hydro disclosed and dealt with the issue so far in the public arena. It looks like it may be a textbook example of how incident response *should* be done, with transparency and openness. Not only the public and media perception went well, but the business end went well too — people didn't sell off shares because they felt genuinely informed and that Hydro had a dire situation under control.

### Security industry

---

I feel the industry could do a better job at advising what benefits and weak spots of their products have in terms of detection, so customers can make informed choices about where they may need to introduce additional controls and investment.

I know, I'm naive.

The cyber security industry is currently going through a hype cycle where some vendors are simply overselling their products — including internally — so you can end up with customers like Hydro which likely had a reasonable security stack, but got wiped out anyway. Hydro aren't alone here in their journey.

I've seen vendors talking about Artificial Intelligence made malware — where AI creates the malware itself — which isn't even a real thing. The reality here is we had an in the wild, classic ransomware attack around for months and there wasn't anywhere approaching good



detection. Stop talking about blockchain and start detecting.

## Detection inside organisations

---

- Your Security Incident Event Management (SIEM) tool should have alerts to detect excessive addition of new scheduled tasks and/or services. This is not a default alert I've seen in any vendor, and I don't think it's a CIS control either. I might write this up one day.
- If you don't have a SIEM tool, deploy Azure Sentinel. It's currently free, no infrastructure, Microsoft managed, and comes with a bucket load of free use cases (it ships with over a thousand detections) out the box. You can onboard your entire organisation faster than you can set up a Splunk Heavy Forwarder.
- Detect things like Mimikatz and Pass The Hash attacks. Azure Sentinel does this out the box, no config. If you get your alerts configured right and without false positives (it's possible) then jump on them as soon as they go off. Priority -3493289. Make it monitored 24/7 and on call.
- Detect excessive usage of netsh.exe and logoff.exe.
- Detect local administrator password changes, particularly on servers.
- Detect your endpoint security solutions being stopped and/or disabled.
- Enable 'tamper protection' in your security products — e.g. in Sophos Endpoint with Sophos Enterprise Console you need to manually enable , otherwise attackers can easily just stop Sophos.
- Make sure endpoint security products are universally deployed (e.g. via enforced Group Policy deployment), do not allow IT staff to disable them, and do not allow policies to be weakened outside change management (e.g. too broad whitelists).
- Backup everything.
- Have read only backups, too, if you use disk-to-disk.
- Have a very heavily defended backup infrastructure. Only the people who access to a backup server should have access. Take Domain Admins out the Local Administrator group; make it truly secure.
- Keep an eye on infections of Trickbot and Emotet via Office macros.
- Keep an eye on infections of Empire Powershell and Cobalt Strike on endpoints and servers.
- Use a service like to monitor your external IP ranges for open RDP servers and other misconfigurations.
- Do not pay the ransom.
- Do not pay the ransom.
- Do not pay the ransom.

~g