EclecticIQ Intelligence at the core

Intelligence
Hunting
Response

Ransomware as Smokescreen for Nation State Sponsored Cyber Operations

Ippolito Forni
Threat Intelligence Consultant & Senior CTI Analyst EclecticIQ
iforni@eclecticiq.com

Briefing Agenda

- Quick ransomware tactics historical overview
- Unusual ransomware campaigns
- Ransomware as smokescreen for espionage
- NCSCs, LEOs challenges
- What this means for your organization

EclecticIQ Intelligence at the core

RAS: Not Your Average Ransomware Presentation

What is a **Smokescreen**?

- A cloud of smoke created to conceal military operations.
- A ruse designed to disguise someone's real intentions or activities.

What is **Ransomware as Smokescreen**?

- RAS is a Standard Operating Procedure describing Cyber-Criminal Gangs cooperating with Nation States to target victims in order to steal data of value for the Nation State sponsoring the operation, hiding the Nation State attribution and the espionage/sabotage motive behind the Cyber-Criminal Gang's attribution and financial motive.

EclecticIQ Intelligence at the core

Looking Back...

2013

Cryptolocker
Half a million computers targeted;
Total of $2.78 million in ransoms.

2017

WannaCry
200,000 networks targeted in
150 countries.

2018

Ransomware as a Service (RaaS)
GandCrab affected +1.5 million victims
Alleged a total of $2 billion in ransoms.
($140 million according to the FBI).

2019

Big Game Hunting
Local governments and big corporations targeted: ransom amount per victim in the multi-million dollars range.

2020 Ransomware Trend = Double Extortion

Previously

🔒 Encryption

Now

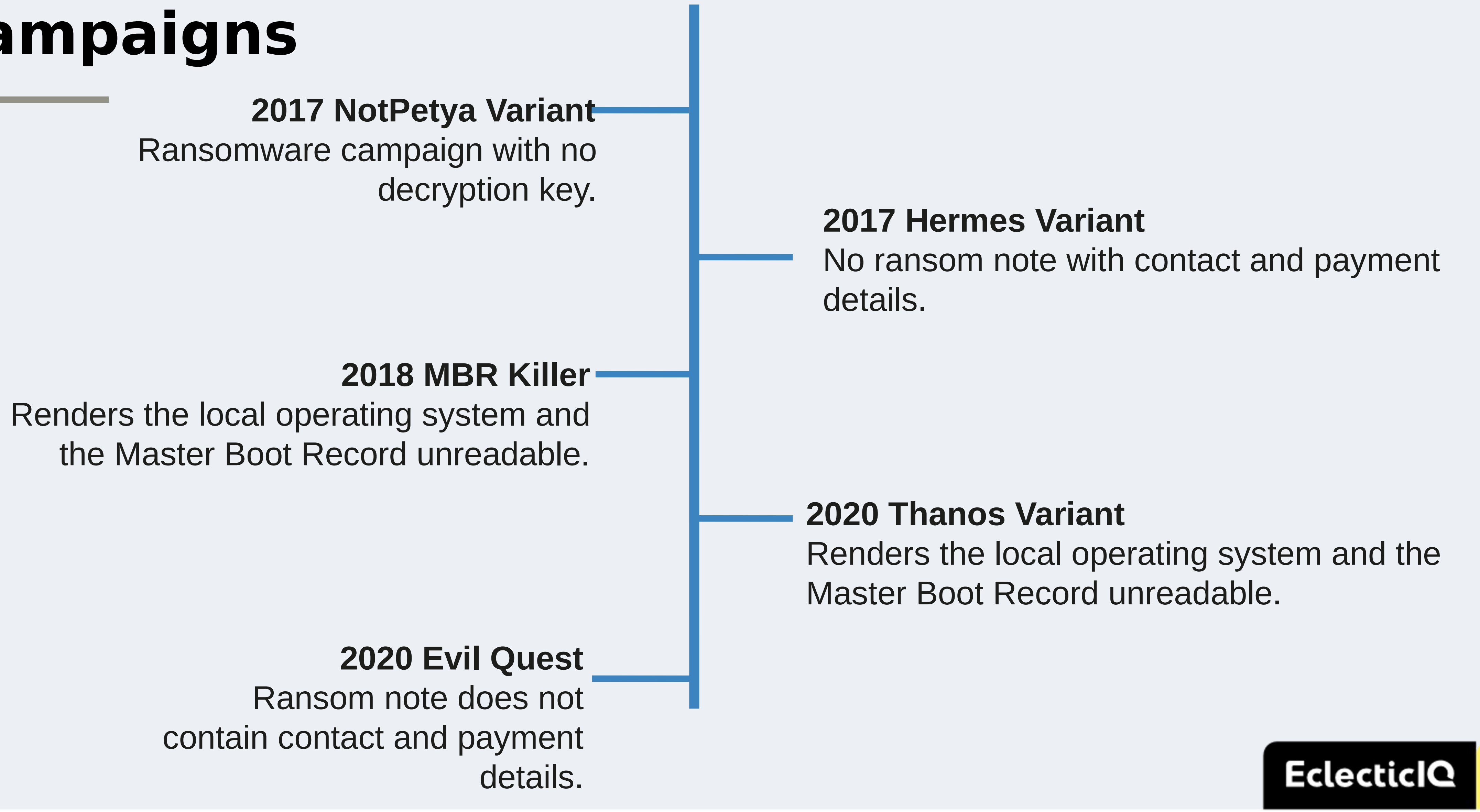
🔒 Encryption + 🧲 Data Exfiltration → 💰 Data sale

Double, Triple and Quadruple Extortion

Ransomware Operators

- Threatening to dump the exfiltrated data on publicly available sites to cause brand damage to the targeted victim. Parsing the data they exfiltrate to see if they can further monetize it by selling it on underground markets.
- Threatening to execute Denial of Service attacks that will make the victim's website unavailable.
- Threatening to report the data breach to government authorities to have the victim incur in data breach fines. Threatening to report the data breach to stock exchanges and media. Harassment of targeted victims' customers, employees, business partners.

Unusual Ransomware Campaigns



2017 NotPetya Variant
Ransomware campaign with no decryption key.

2017 Hermes Variant
No ransom note with contact and payment details.

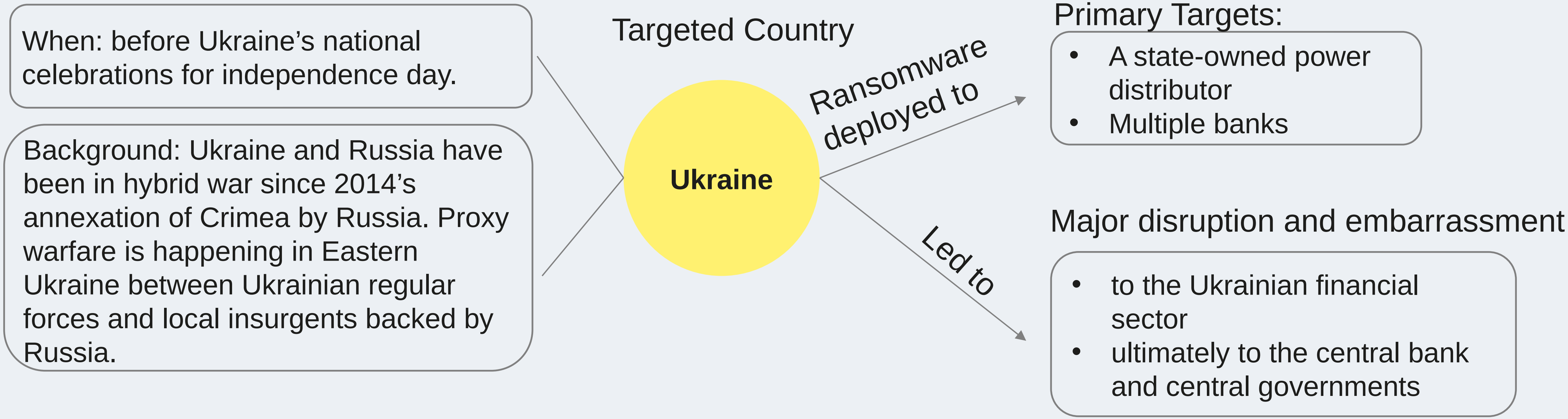
2018 MBR Killer
Renders the local operating system and the Master Boot Record unreadable.

2020 Thanos Variant
Renders the local operating system and the Master Boot Record unreadable.

2020 Evil Quest
Ransom note does not contain contact and payment details.

Why the Unusual Ransomware Behavior?

2017 NotPetya Variant - Ransomware campaign with no decryption key (Russia – Ukraine)



When: before Ukraine’s national celebrations for independence day.

Background: Ukraine and Russia have been in hybrid war since 2014’s annexation of Crimea by Russia. Proxy warfare is happening in Eastern Ukraine between Ukrainian regular forces and local insurgents backed by Russia.

Targeted Country

Ukraine

Primary Targets:

- A state-owned power distributor
- Multiple banks

Major disruption and embarrassment

- to the Ukrainian financial sector
- ultimately to the central bank and central governments

- **The Security Service of Ukraine ultimately attributed the campaign to Russia.**
- **It appears the goal of the ransomware was disruption and embarrassment rather than monetization.**

2017 Hermes Variant - No ransom note, no payment details!

1. Ransomware: Data encryption on multiple (not all) machines

2. Hackers: SWIFT payment system exploitation with $60 million unauthorized transaction

Same exploitation tools used by hackers in the attack of Central Bank of Bangladesh.

More about the attack:

- Unauthorized transaction of $81 million.
- The money was laundered via the same money mule accounts in Sri Lanka and Cambodia.
- Threat actor: Lazarus, a DPRK nation state sponsored APT group.

MBR Killer (DPRK – Chile)

Banco de Chile

- The local operating system and the Master Boot Record unreadable.
- Ransomware data encryption on multiple (not all) machines.
- SWIFT payment system exploitation by hackers with unauthorized transactions of $10 million.

No definitive attribution, Lazarus is the prime suspect.

2020 Thanos Variant (Iran – Israel)

Targets: State run orgs in the Middle East, primarily in Israel

- The local operating system and the Master Boot Record unreadable.
- Data destruction

- **Security community concurred this was a wiper masquerading as ransomware, consistent with previous Iranian campaigns delivering a wiper.**
- **This variant of Thanos used the PowGoop loader, previously attributed to MuddyWater, an Iranian nation state sponsored APT group.**

2020 Evil Quest - Ransom note does not contain contact and payment details

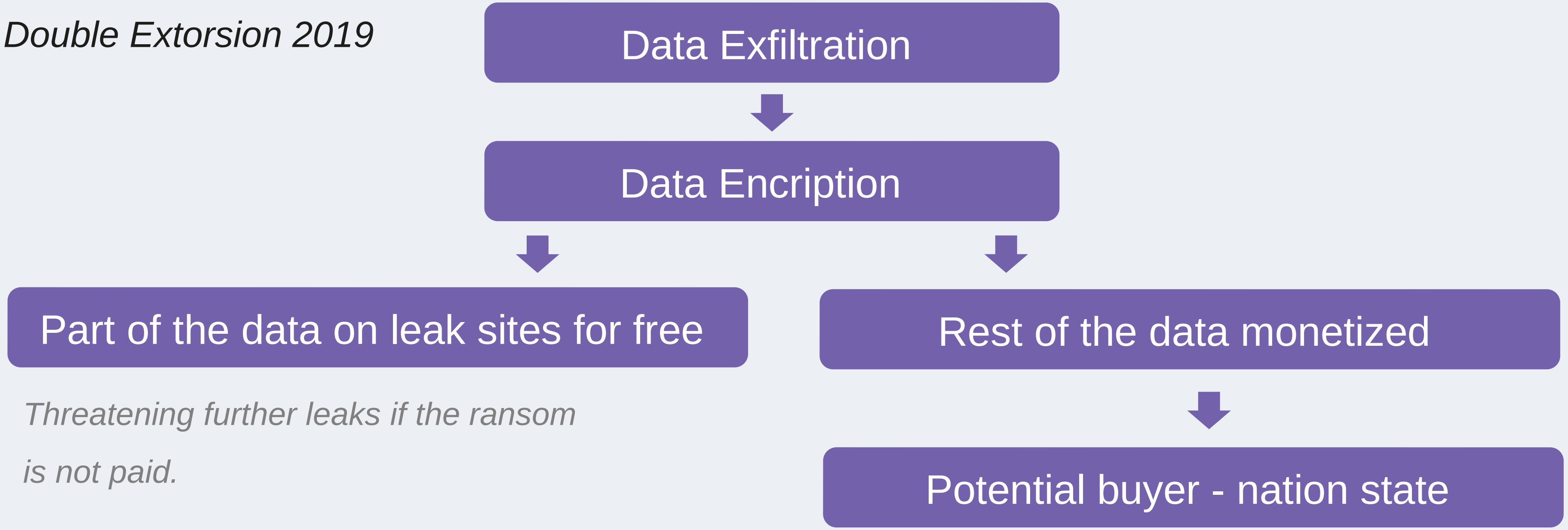
- Unusually small ransom amount requested: $50.
- Downloads a keylogger and opens a reverse shell.
- Malware is too buggy and encrypts random files.

No attribution but consensus in the security community is the goal with this malware is espionage.

Nation State sponsored Ransomware APTs

Ransomware as smokescreen for espionage?

Double Extorsion 2019



Data Exfiltration

Data Encription

Part of the data on leak sites for free

Rest of the data monetized

Potential buyer - nation state

Threatening further leaks if the ransom is not paid.

A more efficient model : coordinating potential targets beforehand with a third party who might be interested in some of the stolen data.

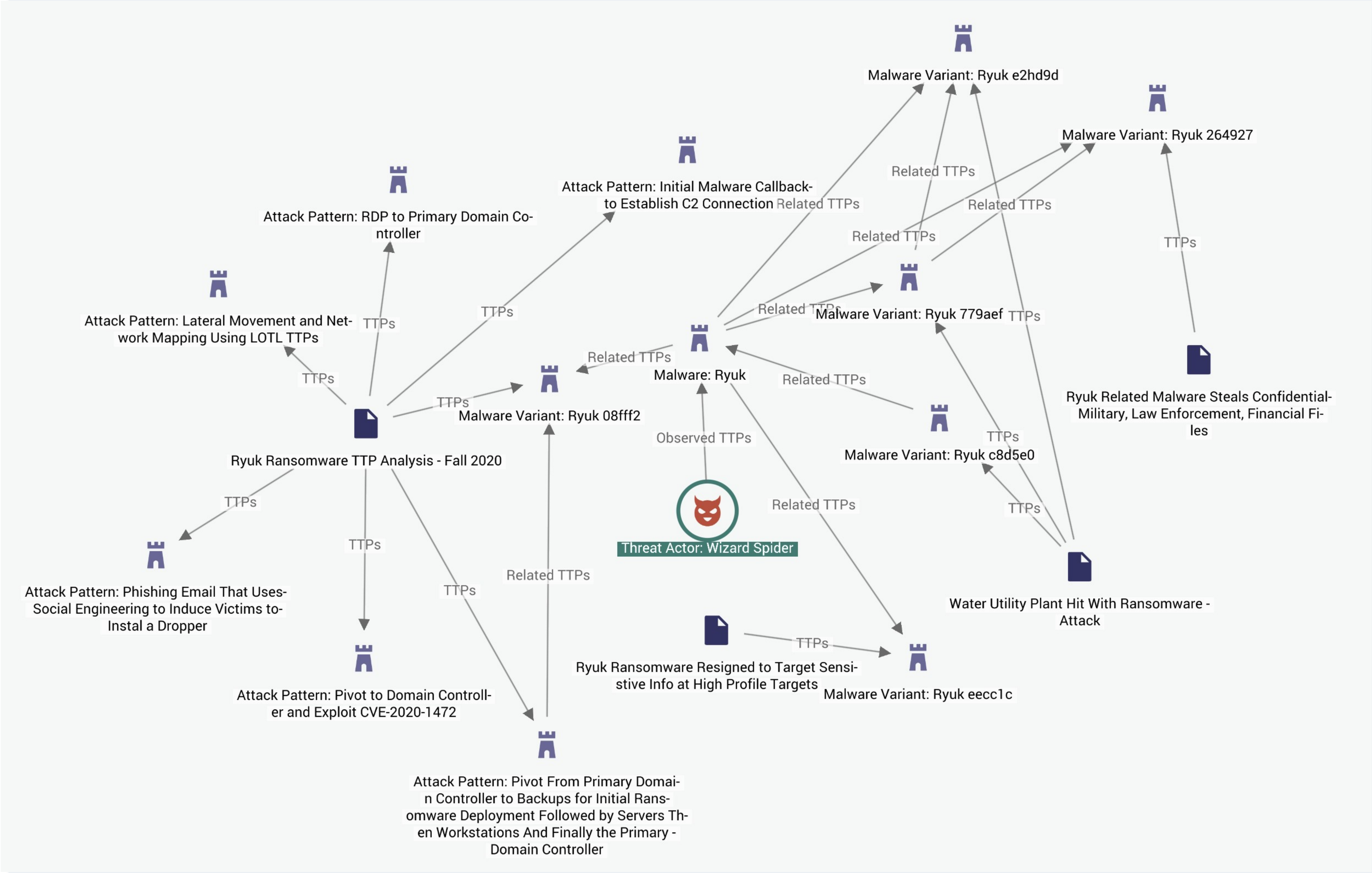
- *The espionage effort is hidden behind the smokescreen of financially motivated criminal threat actors.*
- *In some nations, the boundaries between Nation State and Cyber Criminal groups are blurred.*

One interesting case: Ryuk

- First hypothesis over Ryuk employing RAS in January 2021, no conclusive evidence.
- First appeared in August 2018 and has been extremely successful ever since.
- Long list of targeted victims from all the industry verticals.
- Made more than $150 million in ransomware attacks.

BUT never leaks the data, even though the bots that deliver it are capable of data exfiltration. Why not monetizing the data?

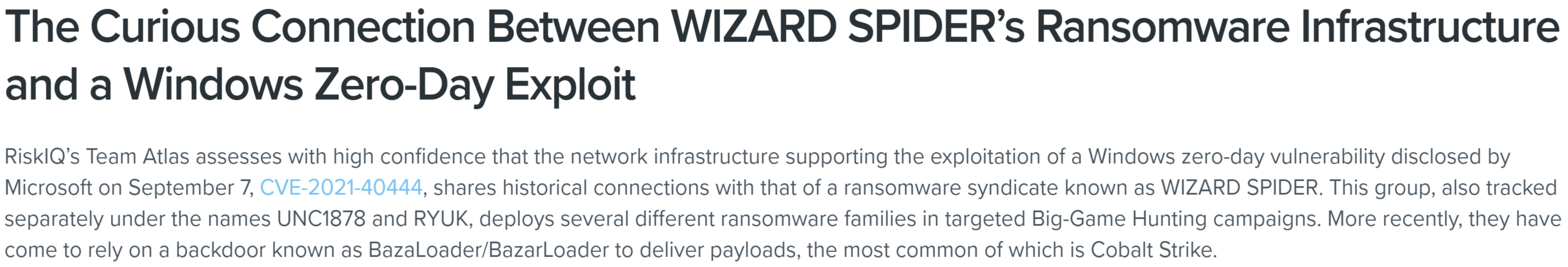
The data could be exfiltrated and delivered to third parties who want to maintain a strong degree of plausible deniability in exchange for money or other benefits.


Malware Variant: Ryuk e2hd9d
Malware Variant: Ryuk 264927
Attack Pattern: Initial Malware Callback-to Establish C2 Connection
Attack Pattern: RDP to Primary Domain Controller
Attack Pattern: Lateral Movement and Network Mapping Using LOTL TTPs
Malware Variant: Ryuk 779aef
Malware: Ryuk
Malware Variant: Ryuk 08fff2
Ryuk Ransomware TTP Analysis - Fall 2020
Ryuk Related Malware Steals Confidential-Military, Law Enforcement, Financial Files
Malware Variant: Ryuk c8d5e0
Threat Actor: Wizard Spider
Attack Pattern: Phishing Email That Uses-Social Engineering to Induce Victims to-Instal a Dropper
Water Utility Plant Hit With Ransomware - Attack
Ryuk Ransomware Resigned to Target Sensistive Info at High Profile Targets
Malware Variant: Ryuk eecc1c
Attack Pattern: Pivot to Domain Controller and Exploit CVE-2020-1472
Attack Pattern: Pivot From Primary Domain Controller to Backups for Initial Ransomware Deployment Followed by Servers Then Workstations And Finally the Primary - Domain Controller
TTPs
Related TTPs
Observed TTPs

One interesting suspect: Ryuk

September 2021, the hypothesis is validated

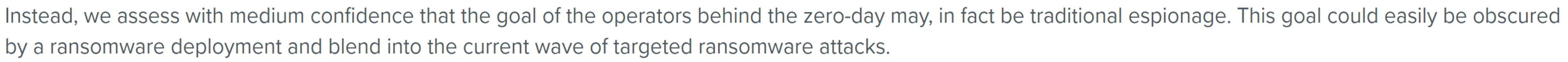
RiskIQ Report from 15 September 2021
https://community.riskiq.com/article/c88cf7e6/description



The Curious Connection Between WIZARD SPIDER's Ransomware Infrastructure and a Windows Zero-Day Exploit

RiskIQ's Team Atlas assesses with high confidence that the network infrastructure supporting the exploitation of a Windows zero-day vulnerability disclosed by Microsoft on September 7, CVE-2021-40444, shares historical connections with that of a ransomware syndicate known as WIZARD SPIDER. This group, also tracked separately under the names UNC1878 and RYUK, deploys several different ransomware families in targeted Big-Game Hunting campaigns. More recently, they have come to rely on a backdoor known as BazaLoader/BazarLoader to deliver payloads, the most common of which is Cobalt Strike.

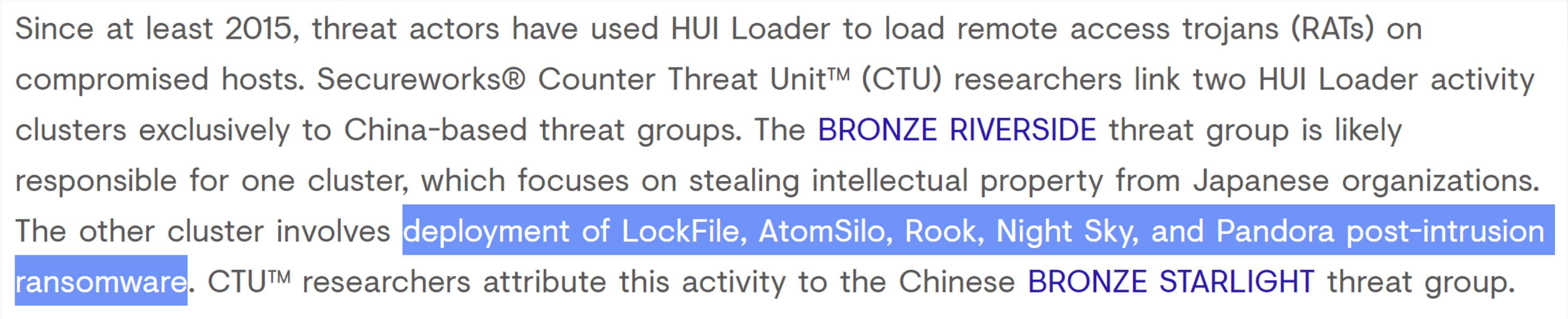
The conclusion of the report is Ransomware as Smokescreen for Nation State sponsored espionage operations:



Instead, we assess with medium confidence that the goal of the operators behind the zero-day may, in fact be traditional espionage. This goal could easily be obscured by a ransomware deployment and blend into the current wave of targeted ransomware attacks.

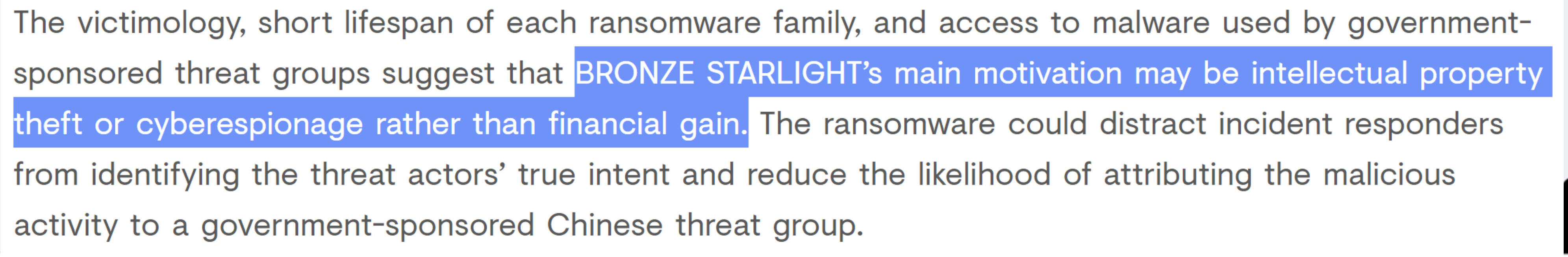
Another interesting case: Bronze Starlight

Secureworks Report from 23 June 2021
https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader



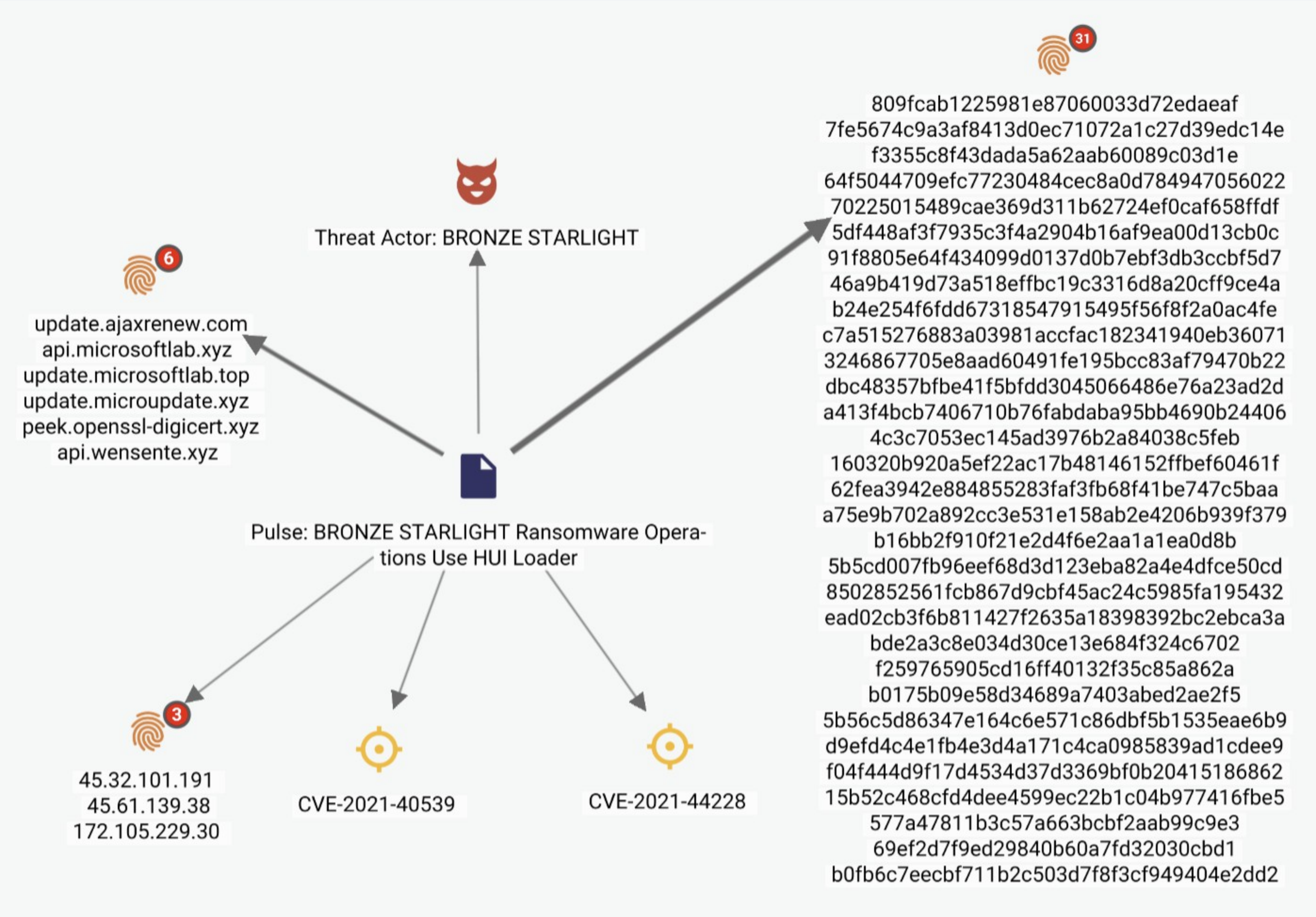
Since at least 2015, threat actors have used HUI Loader to load remote access trojans (RATs) on compromised hosts. Secureworks® Counter Threat Unit™ (CTU) researchers link two HUI Loader activity clusters exclusively to China-based threat groups. The BRONZE RIVERSIDE threat group is likely responsible for one cluster, which focuses on stealing intellectual property from Japanese organizations. The other cluster involves deployment of LockFile, AtomSilo, Rook, Night Sky, and Pandora post-intrusion ransomware. CTU™ researchers attribute this activity to the Chinese BRONZE STARLIGHT threat group.

The conclusion of the report is Ransomware as Smokescreen for Nation State sponsored espionage operations:



The victimology, short lifespan of each ransomware family, and access to malware used by government-sponsored threat groups suggest that BRONZE STARLIGHT's main motivation may be intellectual property theft or cyberespionage rather than financial gain. The ransomware could distract incident responders from identifying the threat actors' true intent and reduce the likelihood of attributing the malicious activity to a government-sponsored Chinese threat group.

Another interesting case: Bronze Starlight



Threat Actor: BRONZE STARLIGHT

Pulse: BRONZE STARLIGHT Ransomware Operations Use HUI Loader

6

update.ajaxrenew.com
api.microsoftlab.xyz
update.microsoftlab.top
update.microupdate.xyz
peek.openssl-digicert.xyz
api.wensente.xyz

3

45.32.101.191
45.61.139.38
172.105.229.30

CVE-2021-40539

CVE-2021-44228

31

809fcab1225981e87060033d72edaeaf
7fe5674c9a3af8413d0ec71072a1c27d39edc14e
f3355c8f43dada5a62aab60089c03d1e
64f5044709efc77230484cec8a0d784947056022
70225015489cae369d311b62724ef0caf658ffdf
5df448af3f7935c3f4a2904b16af9ea00d13cb0c
91f8805e64f434099d0137d0b7ebf3db3ccbf5d7
46a9b419d73a518effbc19c3316d8a20cff9ce4a
b24e254f6fdd67318547915495f56f8f2a0ac4fe
c7a515276883a03981accfac182341940eb36071
3246867705e8aad60491fe195bcc83af79470b22
dbc48357bfbe41f5bfdd3045066486e76a23ad2d
a413f4bcb7406710b76fabdaba95bb4690b24406
4c3c7053ec145ad3976b2a84038c5feb
160320b920a5ef22ac17b48146152ffbef60461f
62fea3942e884855283faf3fb68f41be747c5baa
a75e9b702a892cc3e531e158ab2e4206b939f379
b16bb2f910f21e2d4f6e2aa1a1ea0d8b
5b5cd007fb96eef68d3d123eba82a4e4dfce50cd
8502852561fcb867d9cbf45ac24c5985fa195432
ead02cb3f6b811427f2635a18398392bc2ebca3a
bde2a3c8e034d30ce13e684f324c6702
f259765905cd16ff40132f35c85a862a
b0175b09e58d34689a7403abed2ae2f5
5b56c5d86347e164c6e571c86dbf5b1535eae6b9
d9efd4c4e1fb4e3d4a171c4ca0985839ad1cdee9
f04f444d9f17d4534d37d3369bf0b20415186862
15b52c468cfd4dee4599ec22b1c04b977416fbe5
577a47811b3c57a663bcbf2aab99c9e3
69ef2d7f9ed29840b60a7fd32030cbd1
b0fb6c7eecbf711b2c503d7f8f3cf949404e2dd2

One more? Cuba Ransomware

- Cuba is the name of the Ransomware, no affiliation with the country of Cuba.

- A hypothesis over Cuba Ransomware employing RAS in September 2022, not enough evidence available at the time of writing.

- Cuba Ransomware first appeared in December 2019, 60 organizations targeted, most of them in the Critical Infrastructure Vertical. Cuba Ransomware collected a total of $43.9 million in ransoms.

- Targeted more than 10 Government Agencies in Montenegro in late August 2022.

- Montenegro's National Security Agency (ANB) linked the attack to Russia.

- Early September 2022 the FBI sends CAT (Cyber Action Teams) to Montenegro to help investigate recent cyber-attacks on government digital infrastructure.

- As per the April 2021 investigation of Profero and SecurityJoes, Cuba Ransomware group comprises Russian speaking individuals.

RaaS as the Ultimate False Flag Enabler

Ransomware as a Service provides concealment and deception.

- Nation States can contract Cyber Criminal gangs to do their bidding.
- Known Nation State affiliated Cyber Criminal gangs can operate under a different name and unattributed infrastructure.
- Countless sock puppet APT groups pretending to be independent Cyber Criminal gangs can be created.
- The exponentially increasing number of Ransomware as a Service Groups provides the ideal theater to camouflage and hide nation state affiliated groups activity in plain sight.

NCSC / GovCERT Challenges

The “big picture” is more important than ever: you need visibility into the threat landscape.

- Nation States could use ransomware for a variety of cyber operations under the guise of an independent financially motivated APT group.
- Only by putting the pieces of the puzzle together you will be able to uncover Nation State driven, “maskirovka” type of activity.
- Collaboration and intelligence sharing from the private sector is of utmost importance. Supply chain and organizations supporting the national interests of US and European countries are likely targets of interest.
- Victims of ransomware, particularly private organizations, do not always share information with the authorities for a variety of reason. The Omertà needs to stop.

Diplomatic and LEO Challenges

Plausible deniability is the name of the game.

- Lack of international legal agreements and clear definitions in foreign policy.
- Nation States can deny any affiliation with the entity behind the cyber attack.
- Prosecution efforts lead to no real impact when the APT groups are operating in countries that do not cooperate with Western LEOs.
- Members or the affiliates of the APT group can be apprehended when traveling through Western aligned countries, but nowadays most of them know better.
- Without a “smoking gun”, any retaliation against the alleged Nation State of origin could cause a diplomatic international backlash.

Nation States Using Mafia TTPs

”It’s a nice shop you have here, it would be a shame if something happened to it… there are bad people out there, we can protect you from them.”

- Nation States employing Ransomware as Smokescreen utilize the same strategic communication used by Mafia groups.
- Nation States actively deny any involvement, pointing responsibilities and attribution to “unaffiliated” cyber criminal gangs.
- A ransomware gang can claim it disabled Critical Infrastructure “by mistake,” but looking at the operation with the Ransomware as Smokescreen glasses, you know that was probably not the case.
- Nation States can leverage threats like the mafioso warning the shop owner. The ransomware gang executes the attack like the mafiosi executing the attack on the shop. They are all tentacles of the same octopus.

It's a shame your clearing data platform is encrypted...

Lack of liquidity scares people in Wall Street and you don't want that to happen, now, do you? Capeesh?

What does this mean for public and private organizations?

- Some Threat Actors avoid targeting victims such as hospitals, schools, NGOs, etc. Most private and public verticals have never been in an exception list.
- Any industry vertical could be the target of a cyber operation hidden behind a ransomware attack.
- Depending on the mission objectives, any type of information could potentially be of great value for espionage/destructive operations.
- The importance of an organization in supporting national interests is likely to make you an attractive target for espionage/sabotage operations.
- Once the mission objectives of the Nation States are achieved, e.g. espionage/sabotage, you will still be at the mercy of the Cyber Criminal gang.

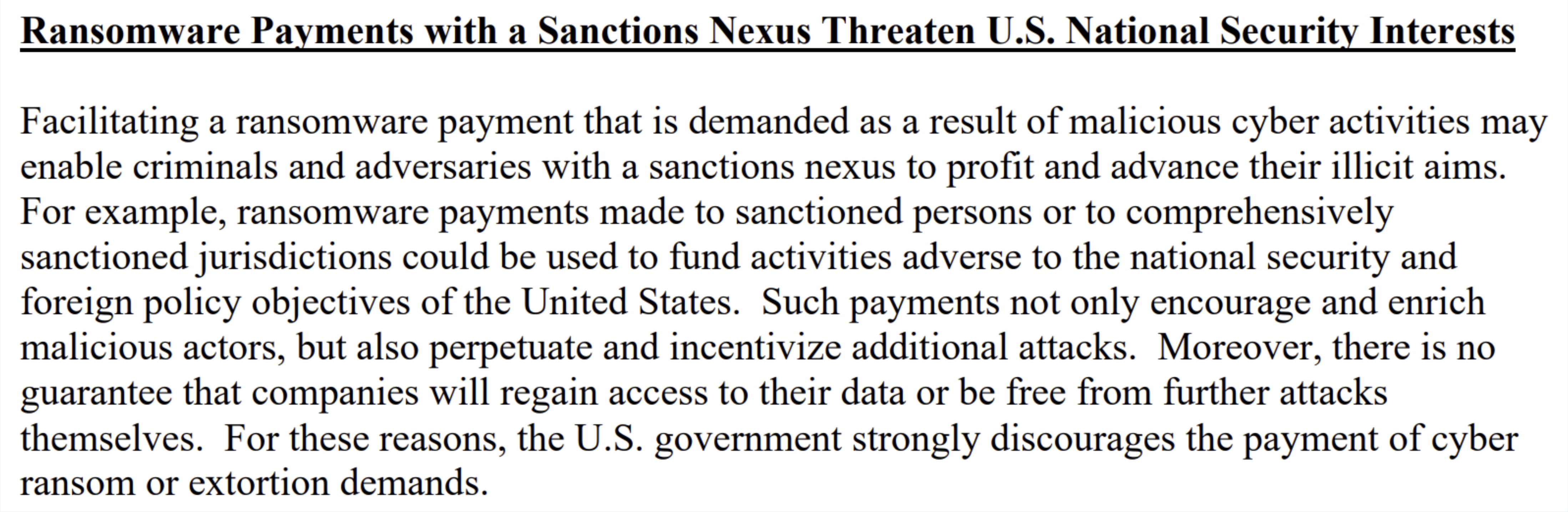
So, are you gonna pay or what?!?

NOT SO FAST!

If you do pay, Washington D.C.’s OFAC and Brussel’s CFSP will want to have a word with you.

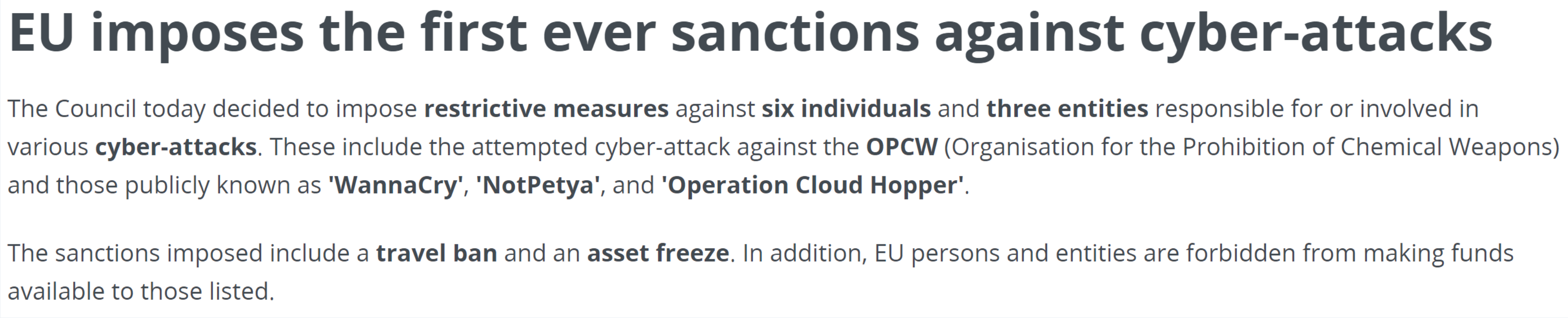
Sanctioned Entities and Ransom Payments

Transferring funds to a sanctioned entity can result in multi-million dollar fines!



Ransomware Payments with a Sanctions Nexus Threaten U.S. National Security Interests

Facilitating a ransomware payment that is demanded as a result of malicious cyber activities may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims. For example, ransomware payments made to sanctioned persons or to comprehensively sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States. Such payments not only encourage and enrich malicious actors, but also perpetuate and incentivize additional attacks. Moreover, there is no guarantee that companies will regain access to their data or be free from further attacks themselves. For these reasons, the U.S. government strongly discourages the payment of cyber ransom or extortion demands.



EU imposes the first ever sanctions against cyber-attacks

The Council today decided to impose **restrictive measures** against **six individuals** and **three entities** responsible for or involved in various **cyber-attacks**. These include the attempted cyber-attack against the **OPCW** (Organisation for the Prohibition of Chemical Weapons) and those publicly known as **'WannaCry'**, **'NotPetya'**, and **'Operation Cloud Hopper'**.

The sanctions imposed include a **travel ban** and an **asset freeze**. In addition, EU persons and entities are forbidden from making funds available to those listed.

EclecticIQ Intelligence at the core

Anti-Ransomware Best Practices

- ✓ Test your disaster recovery process. Execute drills on a regular basis.
- ✓ Make sure your back-up data is physically disconnected from your corporate network.
- ✓ Make sure you have a strict vulnerability management process in place.
- ✓ Provide your user community with security awareness training.
- ✓ Implement security controls on all the systems and devices that might contain company data.
- ✓ If you have to choose between an insurance policy and increasing your security posture, go for the second option.
- ✓ Onedrive or Sharepoint synchronization for all files.
- ✓ Secondary Backup to your Primary Backups with less frequent execution.
- ✓ The entire Security Stack should be Intelligence Driven.
- ✓ Leverage Cyber Threat Intelligence as the center of your operations and as separate auditing entity of your security framework and operations.

Lessons Learned - Takeaways

- ✓ Intelligence Driven Security approach: tailor your security operations.
- ✓ If your organization suffered a ransomware attack, don't rush the post-mortem analysis and conclusions: attribution and motive are very hard to identify, do not make assumptions.
- ✓ Fully cooperate with Law Enforcement and responsible Agencies the very moment you become aware a ransomware attack is taking place.
- ✓ Be aware that your organization, even if small, could be attacked in a pivot to target wider National Security Interests. Supply chain disruptions can be leveraged to create or amplify outages.
- ✓ If you decide to pay the ransom, make sure Law Enforcement and responsible agencies are informed.

Intelligence at the core™

Questions - iforni@eclecticiq.com

EclecticIQ