Computer Security Update

Christos Arvanitis
CERN Computer Security Team

HEPiX, Autumn 2021

Overview

Spyware

Data leaks

Ransomware

Supply Chain Attacks

Spyware

- 0-day vulnerabilities become off-the-shelf products that can be bought by anyone willing to pay huge amounts
- Legitimate companies are offering access to vulnerabilities, arguing that they only provide services to government institutes for anti-terrorism and safety reasons
- No regulation exists for cyberweapon redistribution

Spyware - Pegasus

- Infecting Android/iOS devices
- Introduced in 2016, developed by NSO Group as a commercial product for governments to combat terrorism and serious crime.
- Initially using spear-phishing to infect devices, then evolved to exploit 0-day vulnerabilities.
- It can copy data, activate microphone and camera recording as well as track device location.

Spyware - Pegasus

- A leaked list of 50k targets depicts governments around the word using Pegasus to spy on people and silence journalists. (The Pegasus Project)
- Staggering array of potential targets including political dissidents, human rights activists, 180 journalists in nearly two dozen countries and even heads of state like Emmanuel Macron.
- Apple claims to have patched the known security vulnerability that Pegasus was exploiting. Update your devices!

https://home.cern/news/news/cern/computer-security-kill-horse
https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

Data leaks

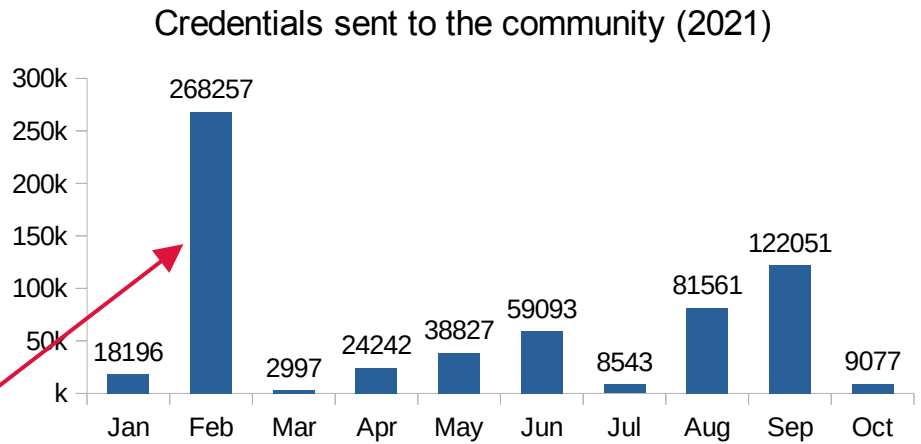
- We have established a system to notify concerned organizations when email addresses under their domain are included in data dumps provided by trusted contacts.

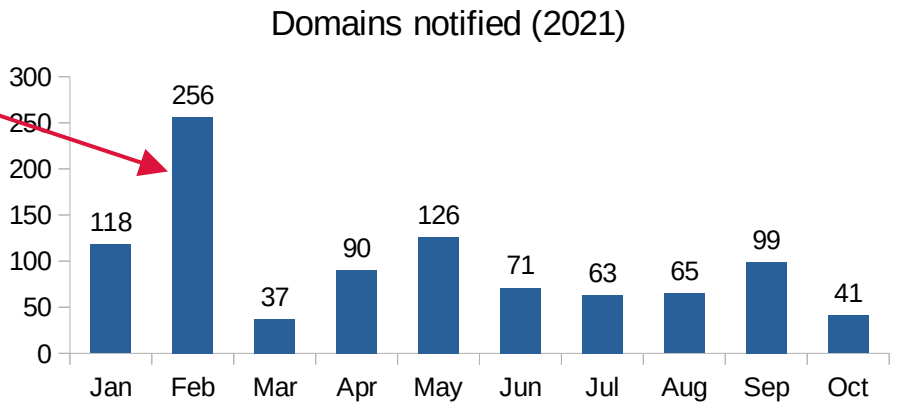
- Specifically:
  - Data leak material is ingested daily
  - Data dumps are filtered to avoid false positives by removing entries that are not passwords
  - Duplicate entries are also removed to avoid re-notifying
  - Concerned organizations monitoring domains are notified

Data leaks

- In 2021, we notified organizations for more than 270 domains and over 630k passwords included in received data dumps

COMB, 3.8B credentials leaked – cybernews.com





Data leaks

Advice:

- Avoid password reuse
- Use a password manager
- Use multi-factor authentication

Contact CERN Computer Security Team
if you want to be included in future alerts

Hello,

You are receiving this information as the registered security contact with the CERN Computer Security Team.

A data leak has surfaced recently, with no specific context regarding its source or origin.
Such leaked data is typically used by cyber-criminals to conduct further attacks, steal personal or corporate information etc.

We found 93% of the data to be new. We decided to notify you with the new entries relevant to your organisation / domain, so that you can handle this information as you see fit:

https://cernbox.cern.ch/[redacted]

This email is sent from an unmonitored address, please do not reply to it.
If you have specific questions not already addressed in this notification, please feel free to contact us at <Computer.Security@cern.ch> or me directly at [redacted].

Regards,

Ransomware

- Continuously evolving attacking scheme. Every 11 seconds, a company is hit by a ransomware attack
- In 2021, ransomware has cost at least $20 billion so far
- Almost 1 out of 5 companies hit with ransomware are reporting business closure

https://www.cybereason.com/press/new-cybereason-ransomware-study-reveals-true-cost-to-business
https://www.cloudwards.net/ransomware-statistics/

Ransomware – Types of extortion

Attackers are creating new revenue opportunities, introducing different levels of extortion to make the victim succumb in paying the ransom

- **Ransom**
  Attackers are encrypting data and extort the victim to pay in order to provide the decryption key

- **Double extortion**
  Attackers are threatening to leak sensitive and confidential information

- **Triple extortion**
  Attackers are launching DoS attacks to victim's services, disrupting operations

- **Quadruple extortion**
  Attackers are threatening to notify customers, business partners, employees and shareholders regarding the attack

https://www.cybereason.com/press/new-cybereason-ransomware-study-reveals-true-cost-to-business
https://www.cloudwards.net/ransomware-statistics/

Ransomware – It doesn’t pay to pay

- Almost **50%** of businesses that paid ransoms did not regain access to all of their critical data after receiving their decryption keys
- **80%** of businesses that pay the ransom subsequently suffer another attack, and **46%** of companies believe this to be the same attacker
- Organizations with cyber insurance coverage are likely to pay, so attackers target insurance providers directly, extorting them while acquiring lists of future targets
  - Cyber insurance firm Chubb was targeted by the “Maze” ransomware group (March 2020)
- CNA Financial Corp. paid **40M$** to regain network access after a Phoenix CryptoLocker based ransomware attack (March 2021)

https://www.cybereason.com/press/new-cybereason-ransomware-study-reveals-true-cost-to-business
https://www.cloudwards.net/ransomware-statistics/

Ransomware – RaaS

- Business model used by ransomware developers (Operators). They rent out the tool, getting a commission on victim payments
- Ransomware becomes a software tool that can be sold to people having access to vulnerable systems (Affiliates)
- Beneficial for both parties, Operators do not have to bother with compromising the target system while Affiliates do not spend time developing the malware
- RaaS operators in many cases run them like a legitimate small business, offering support hotlines and websites for publishing victim details

Who is actually responsible for an attack – the affiliate, or the operator?

Ransomware – Lockbit 2.0

- Automatic encryption of devices across Windows domains by abusing Active Directory(AD) group policies
- Software product ready to be used by affiliates
- Support for virtually any modern Windows OS version.
- Lockbit self spreads across the network even periodically prints ransom requirements on network connected printers
- Affiliates are required to have access to the core server
- Lockbit is actively recruiting insiders to cut the affiliate middleman and get direct access

Ransomware – Lockbit 2.0

- Like any legitimate business, Lockbit group invests a lot in advertising their products, even providing a comparative table with ransomware alternatives
- Lockbit 2.0 makes it to the top of the encryption speed comparative table by utilizing partial file encryption along with multithreaded encryption
- Lockbit group also offers StealBIT to implement double extortion
- Victim company data is automatically exfiltrated while encryption takes place
- A new entry in the Lockbit Name and Shame blog is created for the victim company with a countdown meter, threatening to publish exfiltrated data should the victim not pay the ransom

Ransomware

- Do not get it
- Assume you will get it, and be prepared:
  - Incident response plan
  - Recovery plan
  - Procedures, communications, roles & responsibilities
  - Try role-play, tabletop exercise
  - Train your management
- Keep secure backups while keeping in mind that this is not the panacea
- Proactively mitigate or eliminate critical attack paths and lateral network movement
  - In this direction, @ CERN we have established automatic Active Directory analysis
- Do not pay, do not trust criminals

Supply Chain Attacks

- Infiltrating a system through weaker links of an organization's supply-chain enables the attacker to:
  - Access confidential client information (bank details, legal/corporate documents)
  - Impersonate the supplier in communications, abusing the trust of the customer
  - Deploy malware to clients

- How many suppliers do you have?
  - CERN has **11000+** suppliers
  - No way of tracking the complete set of compromised suppliers

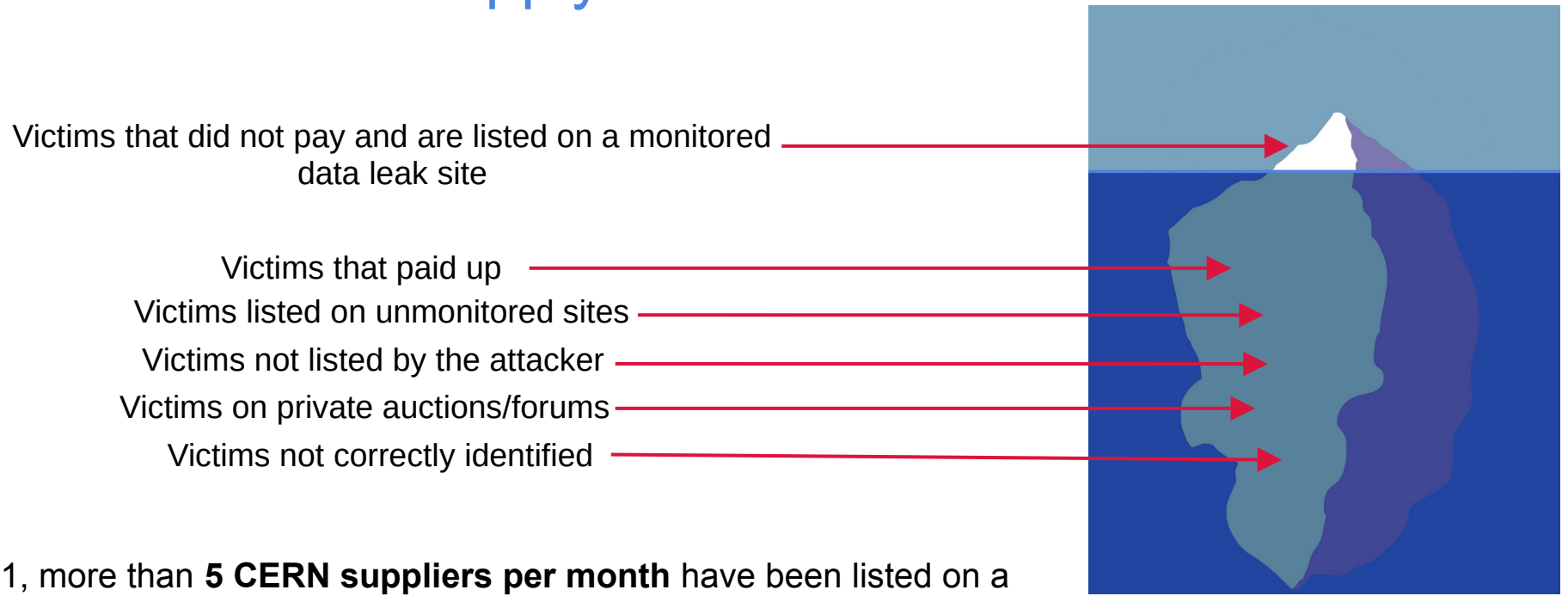
- We can check an estimate using a subset provided by data leak websites

https://home.cern/news/news/computing/computer-security-fancy-dinner-or-burned-pie

Supply Chain Attacks - 2CRSi

- French tech group, providing IT & HPC solutions with clientele extending to 50 countries
- Grief group published on their Name & Shame website that 2CRSi was ransomwared
- Rare happy ending: the group confused 2CRSi with cloud service Linkoffice and eventually updated the URL to the ransomwared company.

Supply Chain Attacks



- In 2021, more than **5 CERN suppliers per month** have been listed on a data leak site:
  - Only victims that did not pay and got listed to a monitored data leak site
  - Probably more have been ransomwared/extorted
  - Not all groups publish victims

https://home.cern/news/news/computing/computer-security-fancy-dinner-or-burned-pie

Supply Chain Attacks

- Not an exotic case and apparently close to CERN
- **Choose your partners wisely**
  - Define risk criteria for different types of suppliers and services
  - Define security requirements for the products and services acquired
  - Add requirement for self-reporting of data breaches in supplier contracts

https://home.cern/news/news/computing/computer-security-fancy-dinner-or-burned-pie
https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Thank you