

OH.. THAT'S RANSOMWARE AND..  
LOOK BEHIND YOU...  
A THREE-HEADED MONKEY!...

A FLAMBOYANT TALE OF SWASHBUCKLERS AND LEAKWARE...



# AGENDA



# STEFANO MACCAGLIA

I am a Senior Principal Consultant and a leading figure of the RSA IR Team operating worldwide.

I started my career cracking software in 1985 with a Commodore C64...

I decided to get out of the cracking scene in early 2000s and for about three years I remained focused on Networking... until Nimda and Blaster came out and testing networks and systems security became an interesting career...

I worked on the offensive side until 2009 when I jumped onto the IR bandwagon.

Since then, I got busy with engagement around the world covering investigation in banks, military, governments and telco companies.



# MARCO FAGGIAN

I am a Senior Consultant for Incident Response operating in the EMEA area.

I joined RSA in 2012 as Delivery Specialist performing implementation, design and analytics support to customers globally.

From 2016 I am part of the RSA Incident Response team and I participate to engagements covering Private and Public companies and the Telco sector.

Graduated in Computer Engineering in Padua, I started my career by dealing with issues related to computer security, collaborating with different consultancy companies located in Italy and in UK.

My actual role led me to follow some of the most important customers in the EMEA region.



**RSA**



# EVOLUTION OF THE RANSOM-WORLD

- If we look at the common definition of Ransomware, we stumble on something like this...

*Ransomware is malware that employs encryption to hold a victim's information at ransom.*


*A user or organization's critical data is encrypted so that they cannot access files, databases, or applications.*

*A ransom is then demanded to provide access.*

*Ransomware is often designed to spread across a network and target database and file servers and can thus quickly paralyze an entire organization.*

*It is a growing threat, generating billions of dollars in payments to cybercriminals and inflicting significant damage and expenses for businesses and governmental organizations.*

- Are we sure this description is exhaustive nowadays???



**Kremez**  
floppy-диск  
Пользователь

Регистрация: 09.01.2020  
Сообщения: 3  
Реакции: 7  
Баллы: 1

Вчера в 04:11

Greetings forum members.

Yet another company refused to work with us and thought that they can get away with this.  
Because MDL ( <http://www.mdllab.com/> ) doesn't want to continue the dialog we will now present to the forum members their private research data.  
Check out immunology research, very interesting stuff.

Reminder:  
This data provided "as-is" so please, use some kind of sandbox (VMWare, Virtualbox ) without internet connection to explore this files.  
[PrivatLab](#)  
[PrivatLab](#)  
[PrivatLab](#)

We hope that everyone will find something useful, clients data etc.

Attention!

| What happened?

We hacked your network and now all your files, documents, photos, databases, and other important data are safely encrypted with reliable algorithms.

You cannot access the files right now. But do not worry. You have a chance to get it back! It is easy to recover in a few steps.

We have also downloaded a lot of data from your network, so in case of not paying this data will be released.  
If you don't believe we have any data you can contact us and ask a proof, also you can google "Allied Universal Maze Ransomware".

When you pay us the data will be removed from our disks and decryptor will be given to you, so you can restore all your files.

| How to contact us and get my files back?

The only method to restore your files and be safe from data leakage is to purchase a unique for you private key which is securely stored on our servers.

To contact us and purchase the key you have to visit our website in a hidden TOR network.

There are general 2 ways to reach us:

1) [Recommended] Using hidden TOR network.

- a) Download a special TOR browser: <https://www.torproject.org/>
- b) Install the TOR Browser.
- c) Open the TOR Browser.
- d) Open our website in the TOR browser: <http://aoacugmutagkwctu.onion/12ef0a96d63c4e21>
- e) Follow the instructions on this page.

2) If you have any problems connecting or using TOR network

- a) Open our website: <https://mazedecrypt.top/12ef0a96d63c4e21>
- b) Follow the instructions on this page.

Warning: the second (2) method can be blocked in some countries. That is why the first (1) method is recommended to use.

On this page, you will see instructions on how to make a free decryption test and how to pay.  
Also it has a live chat with our operators and support team.

| What about guarantees?

We understand your stress and worry.  
So you have a FREE opportunity to test a service by instantly decrypting for free three files from every system in your network.  
If you have any problems our friendly support team is always here to assist you in a live chat!



# EVOLUTION OF THE RANSOM-WORLD

- Let's just play with this...
- Do you see anything strange in this ransomware message?...
- C'mon... don't focus on the fact they hacked the network... there is more in this message...

Attention!

| What happened?

We hacked your network and now all your files, documents, photos, databases, and other important data are safely encrypted with reliable algorithms.  
You cannot access the files right now. But do not worry. You have a chance to get it back! It is easy to recover in a few steps.

We have also downloaded a lot of data from your network, so in case of not paying this data will be released.  
If you don't believe we have any data you can contact us and ask a proof, also you can google "Allied Universal Maze Ransomware".

When you pay us the data will be removed from our disks and decryptor will be given to you, so you can restore all your files.

| How to contact us and get my files back?

The only method to restore your files and be safe from data leakage is to purchase a unique for you private key which is securely stored on our servers.  
To contact us and purchase the key you have to visit our website in a hidden TOR network.

There are general 2 ways to reach us:

1) [Recommended] Using hidden TOR network.

- a) Download a special TOR browser: <https://www.torproject.org/>
- b) Install the TOR Browser.
- c) Open the TOR Browser.
- d) Open our website in the TOR browser: <http://aoacugmutagkwctu.onion/12ef0a96d63c4e21>
- e) Follow the instructions on this page.

2) If you have any problems connecting or using TOR network

- a) Open our website: <https://mazedecrypt.top/12ef0a96d63c4e21>
- b) Follow the instructions on this page.

Warning: the second (2) method can be blocked in some countries. That is why the first (1) method is recommended to use.

On this page, you will see instructions on how to make a free decryption test and how to pay.  
Also it has a live chat with our operators and support team.

| What about guarantees?

We understand your stress and worry.  
So you have a FREE opportunity to test a service by instantly decrypting for free three files from every system in your network.  
If you have any problems our friendly support team is always here to assist you in a live chat!



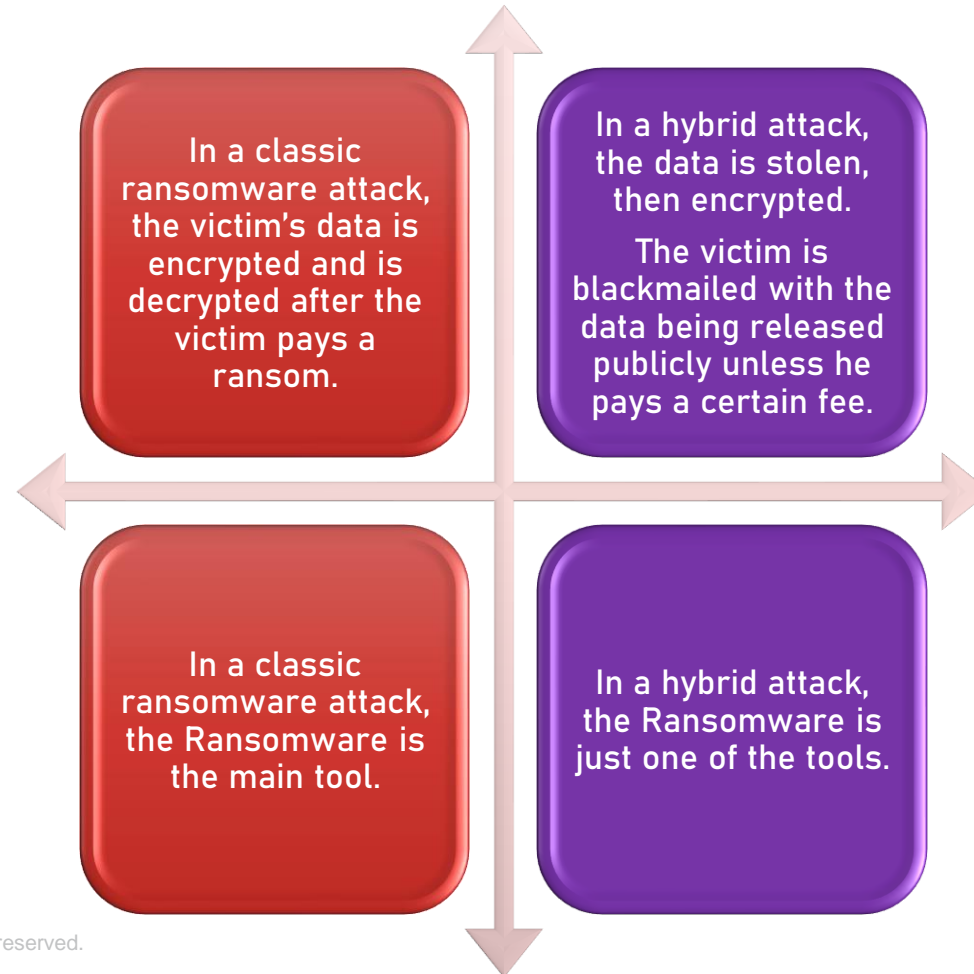
# EVOLUTION OF THE RANSOM-WORLD

- Look!... A the three headed monkey!...

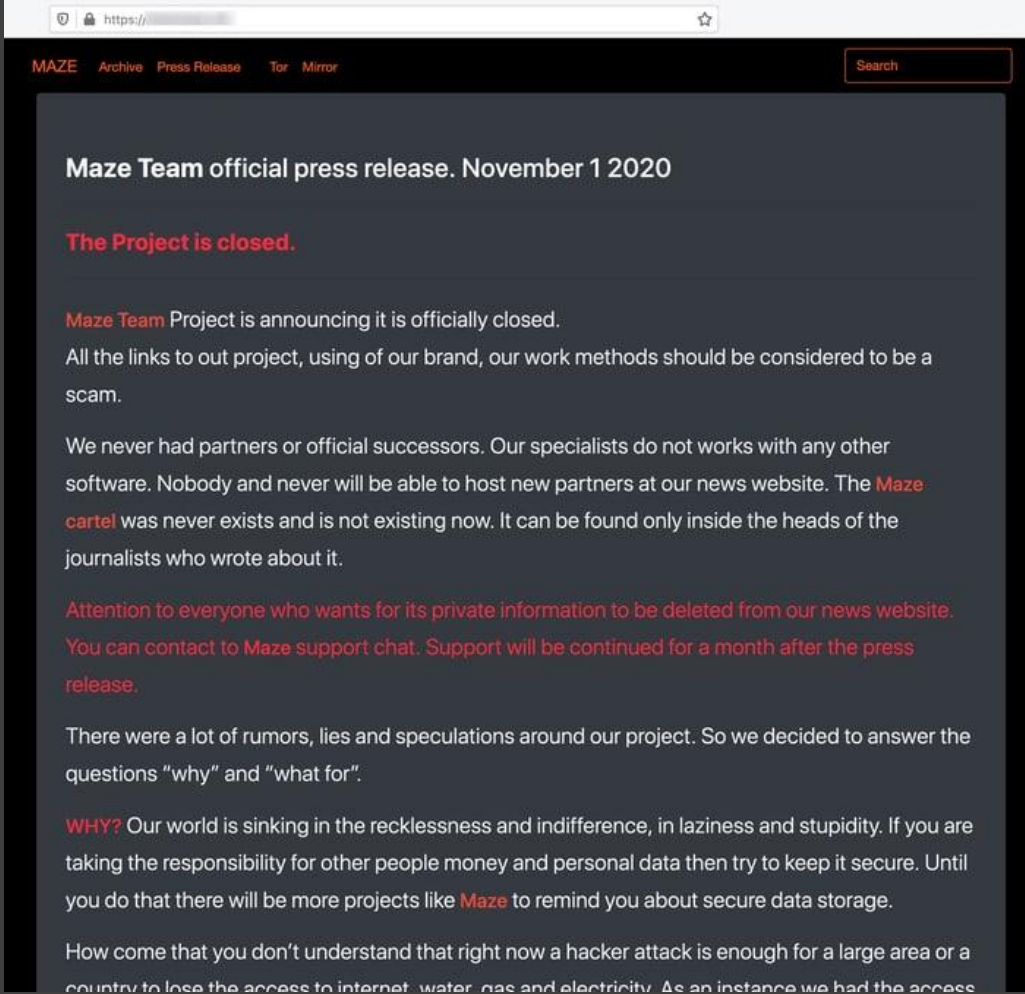


# EVOLUTION OF THE RANSOM-WORLD

- Since December 2019, ransomware operators have been using leakware/ransomware hybrid attacks more and more often.
- These attacks combine the classic ransomware attack with a leakware attack.





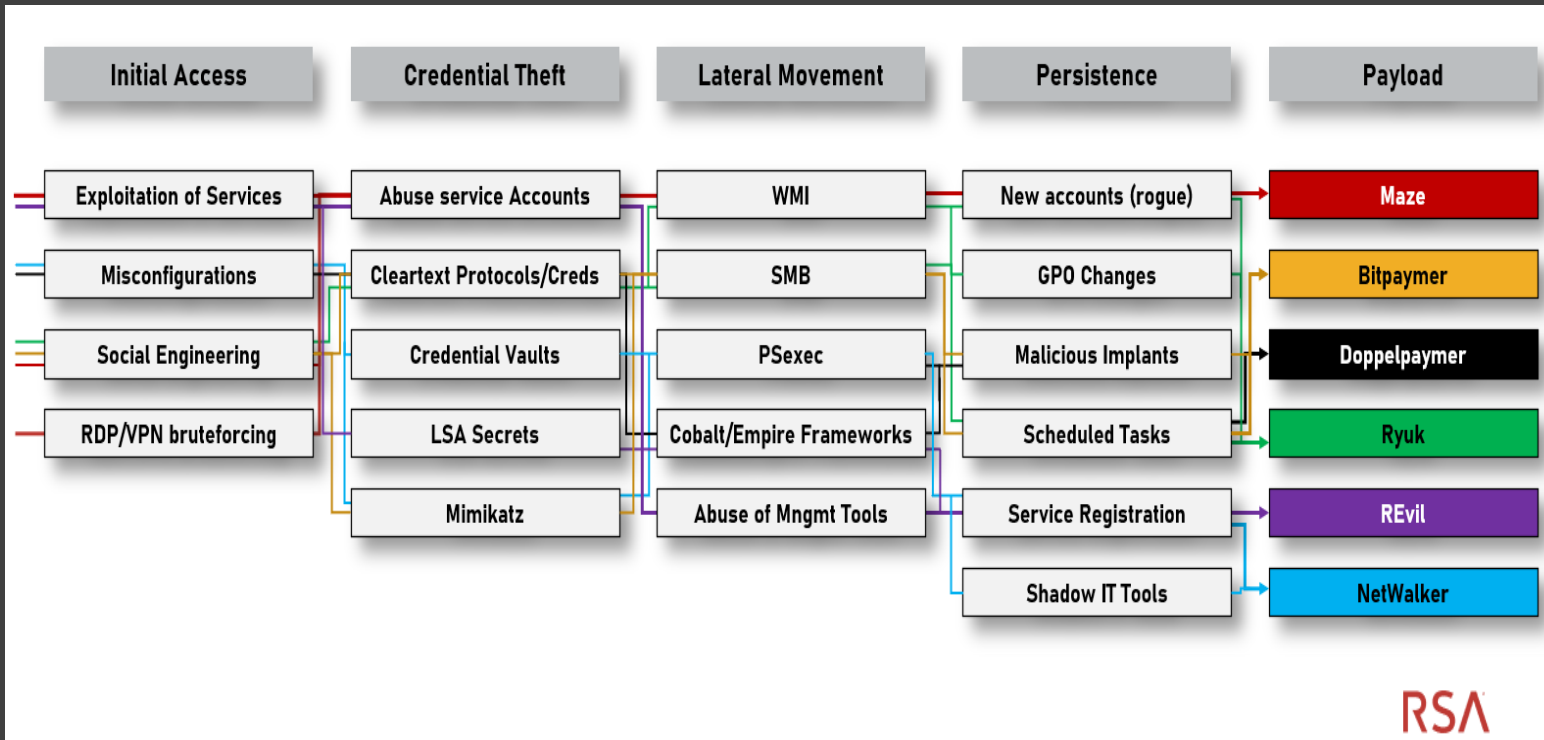


*They just forgot to tell us:*



LONG STORY SHORT...

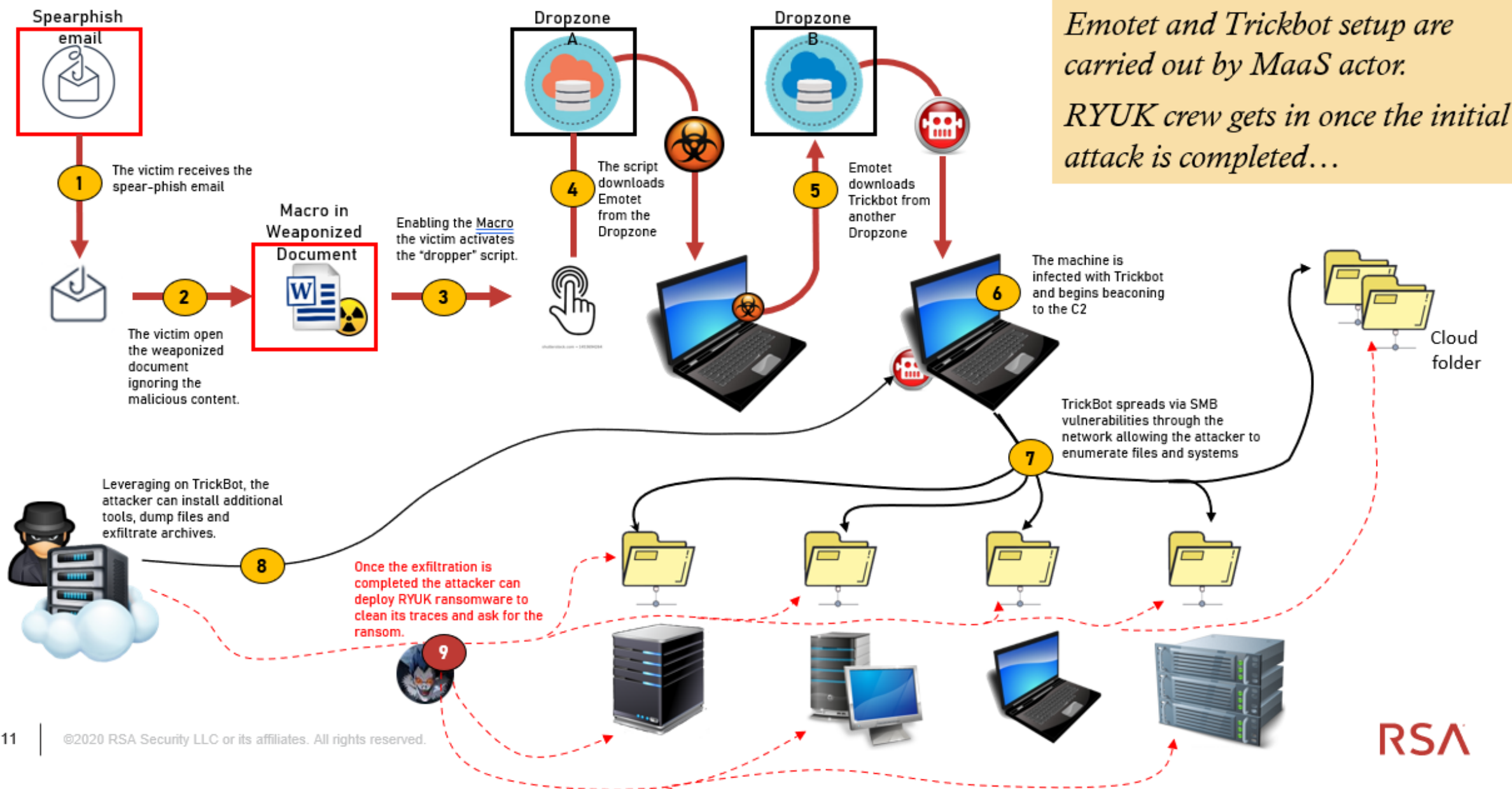
# HYBRID ATTACKS



- In a hybrid attack, the data is first stolen, then encrypted.
- Then the victim is asked to pay the ransom for decryption.
- If the victim declines to pay the ransom, the attackers threaten him to release the stolen data publicly.
- In some cases, business partners and/or customers of the victim are also informed of the impending data release to put even more pressure on the victim.

*This strategy is a “game-changer” as it introduces new techniques and new actors...  
let’s see an example...*

# EMOTET \* RYUK





# THE MALWARE-AS-A-SERVICE

- The underground black market offers an array of services and is not limited to malware or bits of code, like it was until few years ago.
- Today, it is possible to purchase all the necessary pieces to make it as easy as possible for the investors to profit from a tool or from a botnet or... from the access to an already breached environment.
- In fact... due to the significant increment of Hybrid Attacks, a new “type of service” has polarized the interest of talented Blackhats:

the “**Malware-as-a-Service**” arranged around auctions.

- Basically these actors exploit corporate networks or “interesting individuals” aiming to implant backdoor and allow malicious actors to access through their tools and infrastructures.

Once they successfully ensure the access, they raise auctions to monetize such accesses negotiating with malicious actors such as the Ransomware crews.





# MAAS AUCTION EXAMPLE

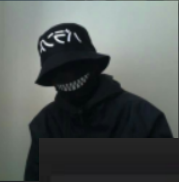
SELLING

SELLING ACCESS TO A FAMOUS COMPANY OF FINANCIAL AND INSURANCE PRODUCTS

by 7h0rf1nn - November 22, 2020 at 09:14 PM

New Reply

7h0rf1nn




November 22, 2020 at 09:14 PM

#1

Corporation name: **REDACTED**

Type: **FINANCIAL AND INSURANCE PRODUCTS**


Selling oob roe access to a **famous financial and insurance products company**, it is well located, with a good pivoting to get **critical** information.

4 hours ago · This post was last modified: 3 hours ago by  Edited 2 times in total.


**PRICE: \$7000 (only bitcoin)**

I'm back. This time, I am offering a vulnerability that allows Blind RCE in a large Austrian bank.

You might be wondering why I didn't put the bank's name in the ad.

This is to prevent this guy (  ) from sharing information about this sale with the vulnerable bank and damaging my client's access.

Seeing this access only to those who have a high reputation, if you are interested contact me first via PM and I share the information necessary for us to negotiate. (including proof of vulnerability)




**GOD**

Posts8

Threads4

JoinedAug 2020

Reputation50



→

Reply

13

©2020 RSA Security LLC or its affiliates. All rights reserved.

**RSA**

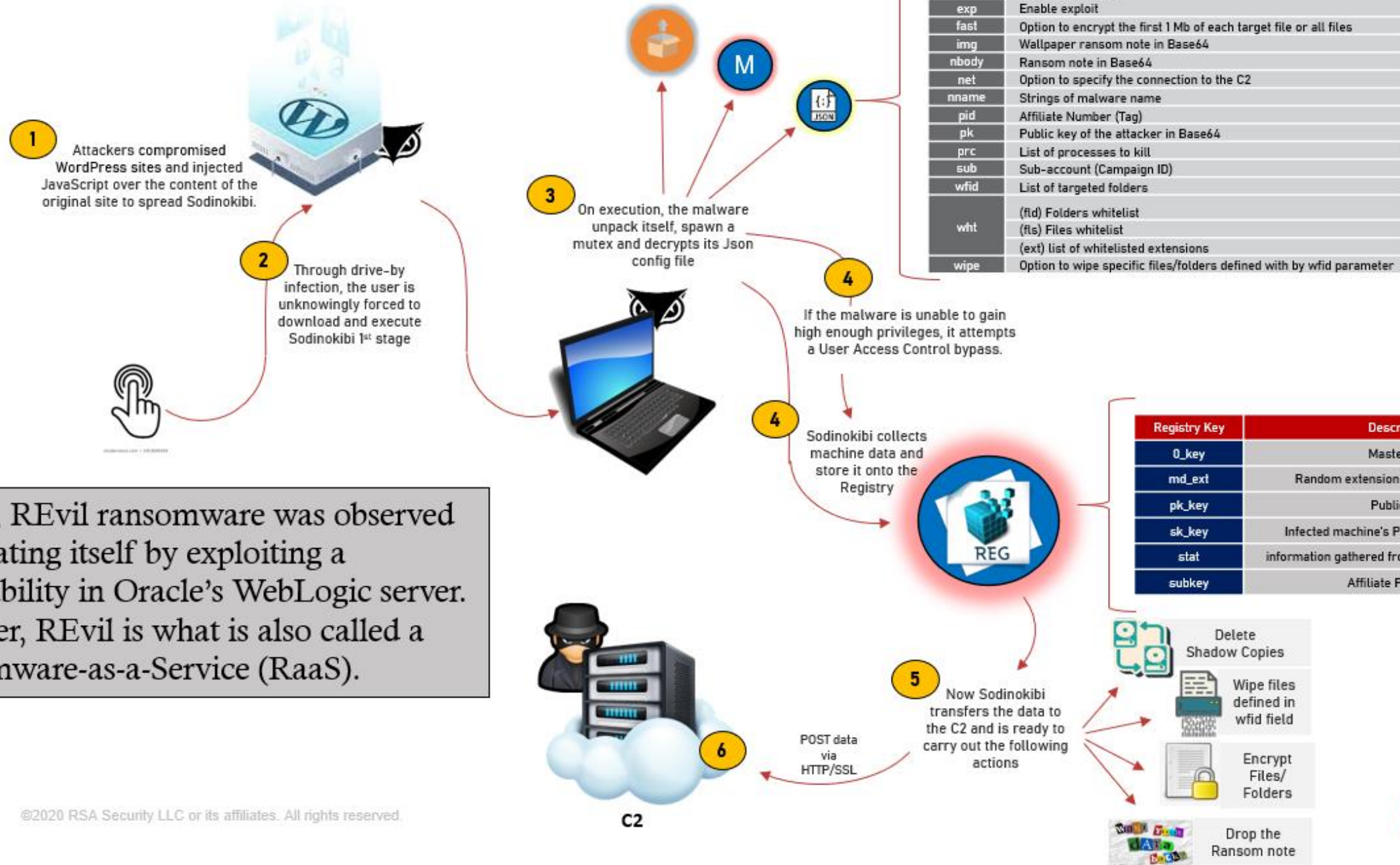


## NOT TO MENTION "RANSOMWARE- AS-A-SERVICE"...

- While the MaaS Providers are a relatively new type of Actors to join the Cybercriminal world, we are already noticing another evolutionary step: the **"Ransomware-as-a-Service"**...
- Under this malicious franchise-like deployment model, cybercriminals write ransomware code and sell/rent it under an affiliate program to other cybercriminals who have the intent to launch an attack. **They provide technical know-how and step-by-step information on how to launch a ransomware attack using the service**, a platform which may even display the status of the attack using a real-time dashboard. Once the attack is successful, the ransom money is divided between the service provider, coder and attacker.
- This vicious model is so enticing to some cybercriminals that you can even see the RaaS provider's advertisements on the dark web. There are numerous reasons why cybercriminals are attracted to this franchise-like deployment. First and foremost, it enables the ransomware authors to earn some quick money. As for the affiliates, it decreases the need for them to write malicious code. They can simply rent out easy-to-use packages at low prices from the dark web.



# REvil/SODINOKIBI



At first, REvil ransomware was observed propagating itself by exploiting a vulnerability in Oracle's WebLogic server. However, REvil is what is also called a Ransomware-as-a-Service (RaaS).

My name's Guybrush Threepwood, and I want to be a pirate!



## RANSOMWARE-AS-A-SERVICE

- The RaaS model allows affiliates to distribute REvil ransomware in any way they want, such as mass-spread attacks using exploit-kits and phishing-campaigns, where other affiliates adopt a more targeted approach by uploading tools and scripts to gain more rights and execute the ransomware in the internal network of a victim or brute-forcing RDP access.
- Malware by itself is not profitable. Access to secure systems by itself is not valuable. When a middleman is inserted and takes the malware to infect secure systems, that is where the potential for monetizing access and malware becomes a reality.
- Sodinokibi infections have netted ransoms ranging between \$150,000 and \$240,000 according to public reports.



# A RECENT CASE

# NEFILIM CREW...

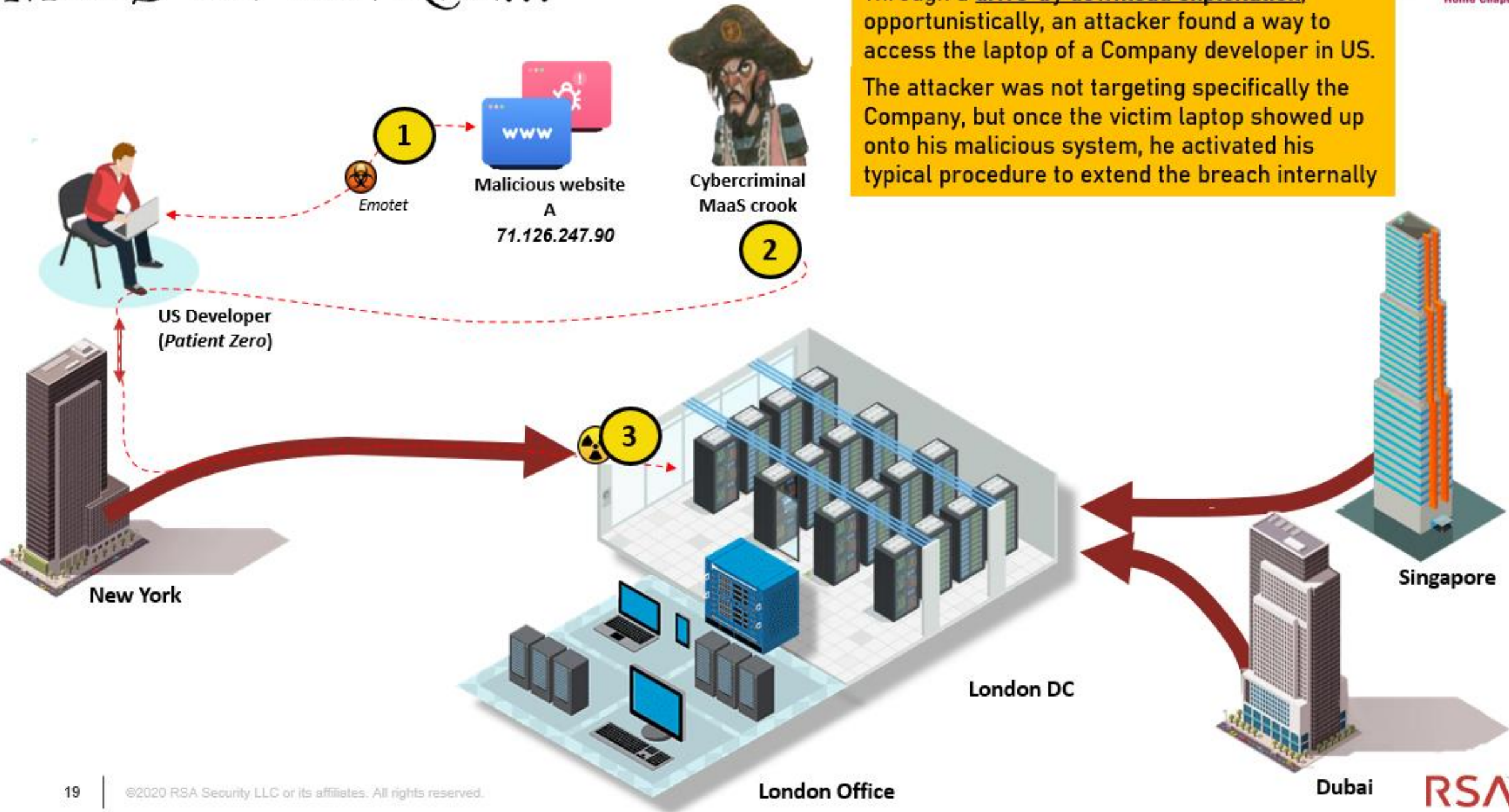
- Nefilim is a ransomware crew that recently compromised a significant number of high profile targets.
- They usually leverage on MaaS providers to gain a foothold onto a network.
- When Nefilim gets in, the typical strategy is to harvest credentials, exploit SMB and RDP and quickly gain access to confidential data in order to steal it.
- Once the exfil occurred, the crew deploys the Ransomware in order to show up, but also to clean the traces.
- The Nefilim Ransomware, usually, has devastating effect destabilizing the company's operations and surely it gains the victim's attention.
- In addition, the crew is used to negotiate with the victims and leverage on traditional crime syndicates to collect the money from the ransom via an escrow payment scheme.



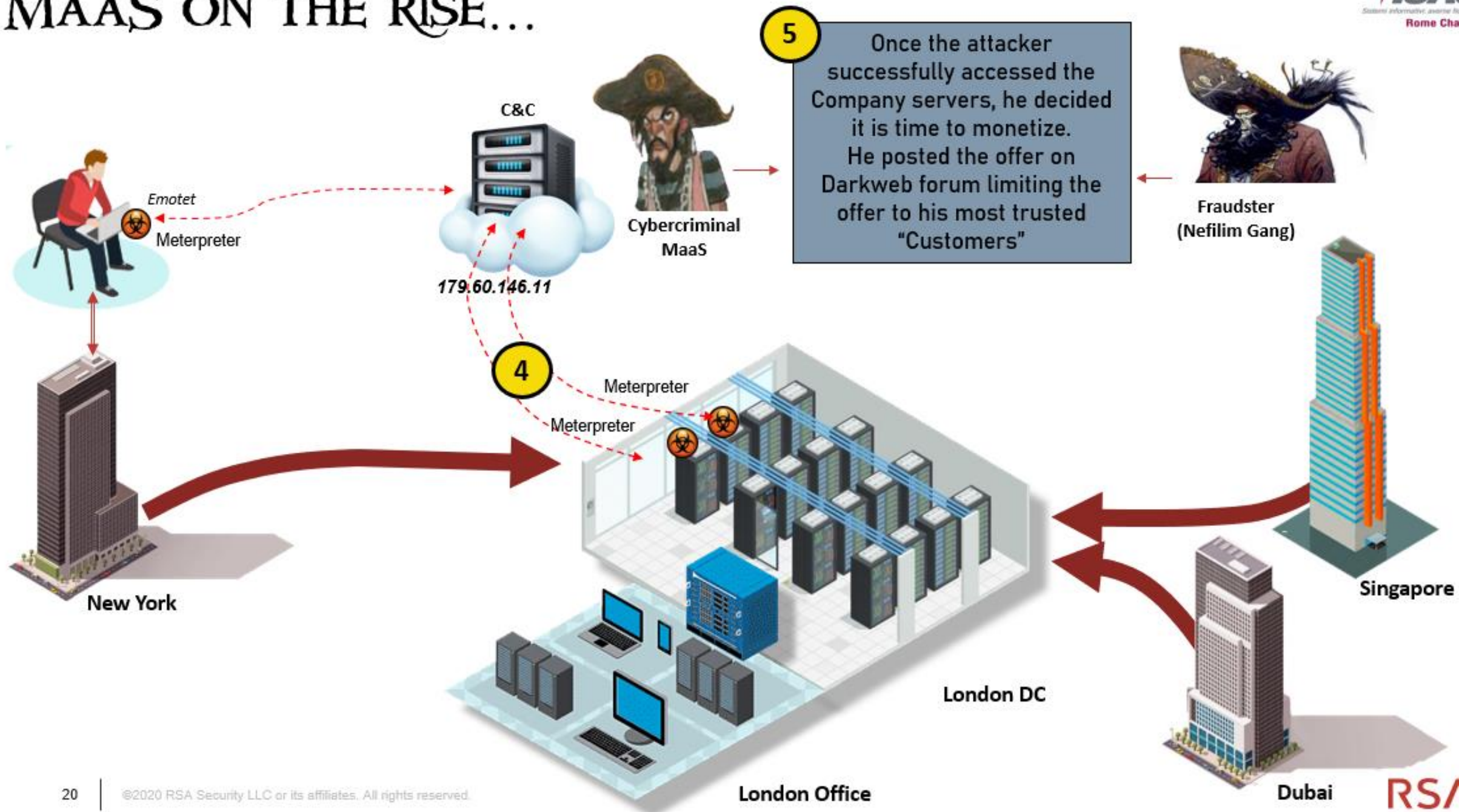


# MAAS ON THE RISE...

Through a **drive-by download exploitation**, opportunistically, an attacker found a way to access the laptop of a Company developer in US. The attacker was not targeting specifically the Company, but once the victim laptop showed up onto his malicious system, he activated his typical procedure to extend the breach internally

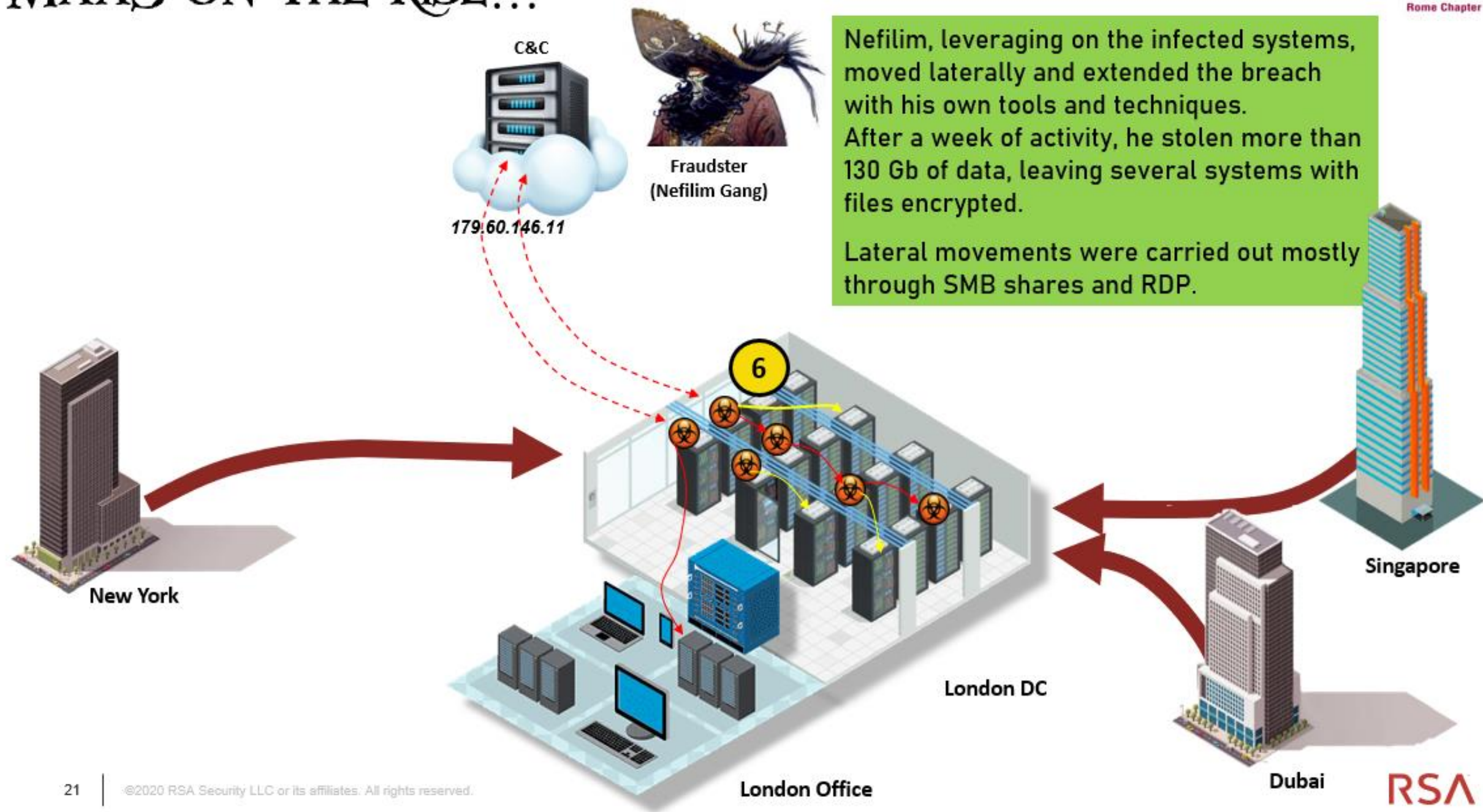


# MAAS ON THE RISE...

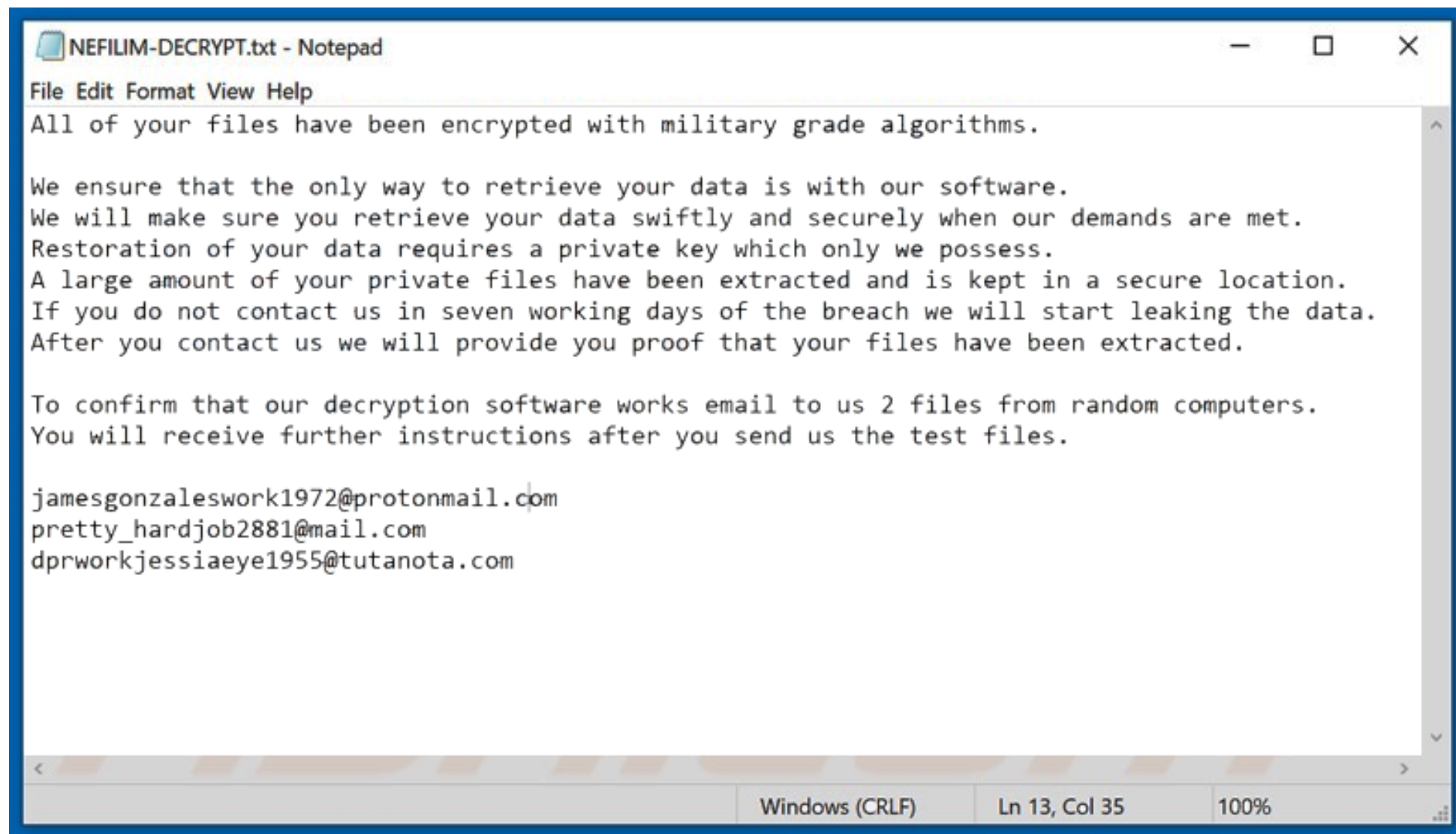


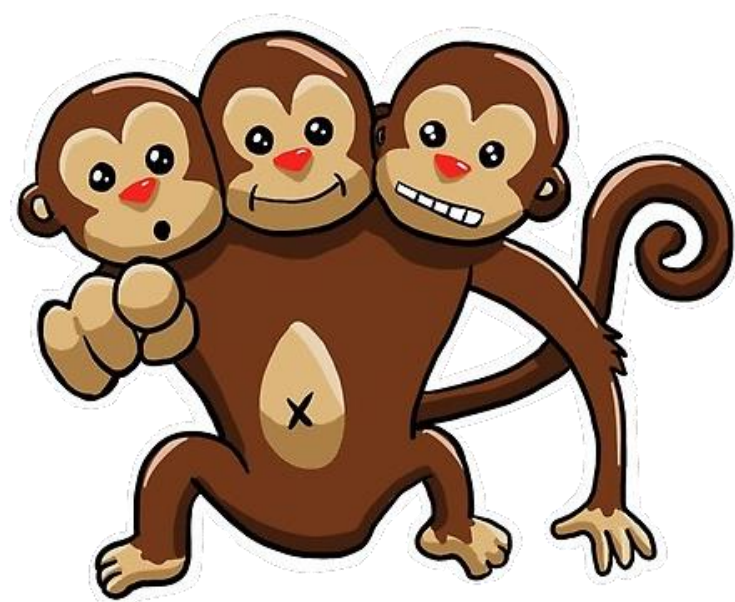


# MAAS ON THE RISE...



# NEFILIM RANSOMWARE BANNER







It would hardly be ethical, sporting, or even interesting to fight someone as unskilled as yourself.



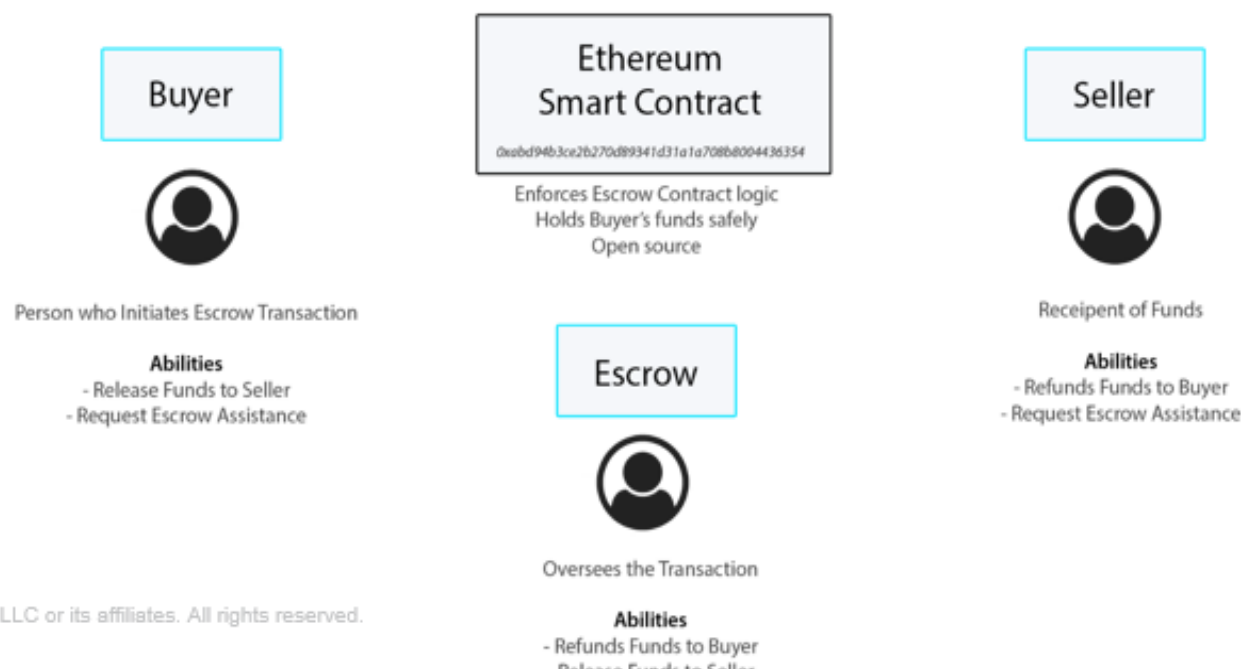
## THE OUTCOME...

- The Company called our Team to investigate...
- The Ransomware was spread throughout the Servers with devastating effects on the Company business.
- We suggested to open a channel with the attacker, which in turn showed a very professional approach to the negotiation.
- Our goal was to buy time and to allow us to connect the dots between the evidences we were slowly gathering and the actions the attacker was describing... Including the type of data he stolen.



# THE OUTCOME...

- The negotiation turned to be a very important step to find some missing pieces and thanks to the extended time granted to the victim, we were able to build a “remediation plan”.
- We tried also to convince the Customer to avoid to pay the price without the total assurance of the recovery of the leaked data, but in the end the Customer decided to find an agreement with the gang.
- In a case like that you need to choose the lesser evil.
- Nevertheless, based on our findings, the Company was able to lower the initial request to about 40%.
- Another significant aspect we found of Nefilim is that the crew was leveraging on money mules... probably linked to traditional criminal syndicates...



*The payment went through Ethereum Escrow... subsequent investigations from legal authorities, tracked partially the path taken by the money and significant evidences linked the recipients of the initial payment with East European crime syndicate operating from Canada.*

# A SECOND CASE

# DEAD MEN TELL NO TALES

- On a lazy morning in a far land... a customer IPS sent an alert to the SOC:



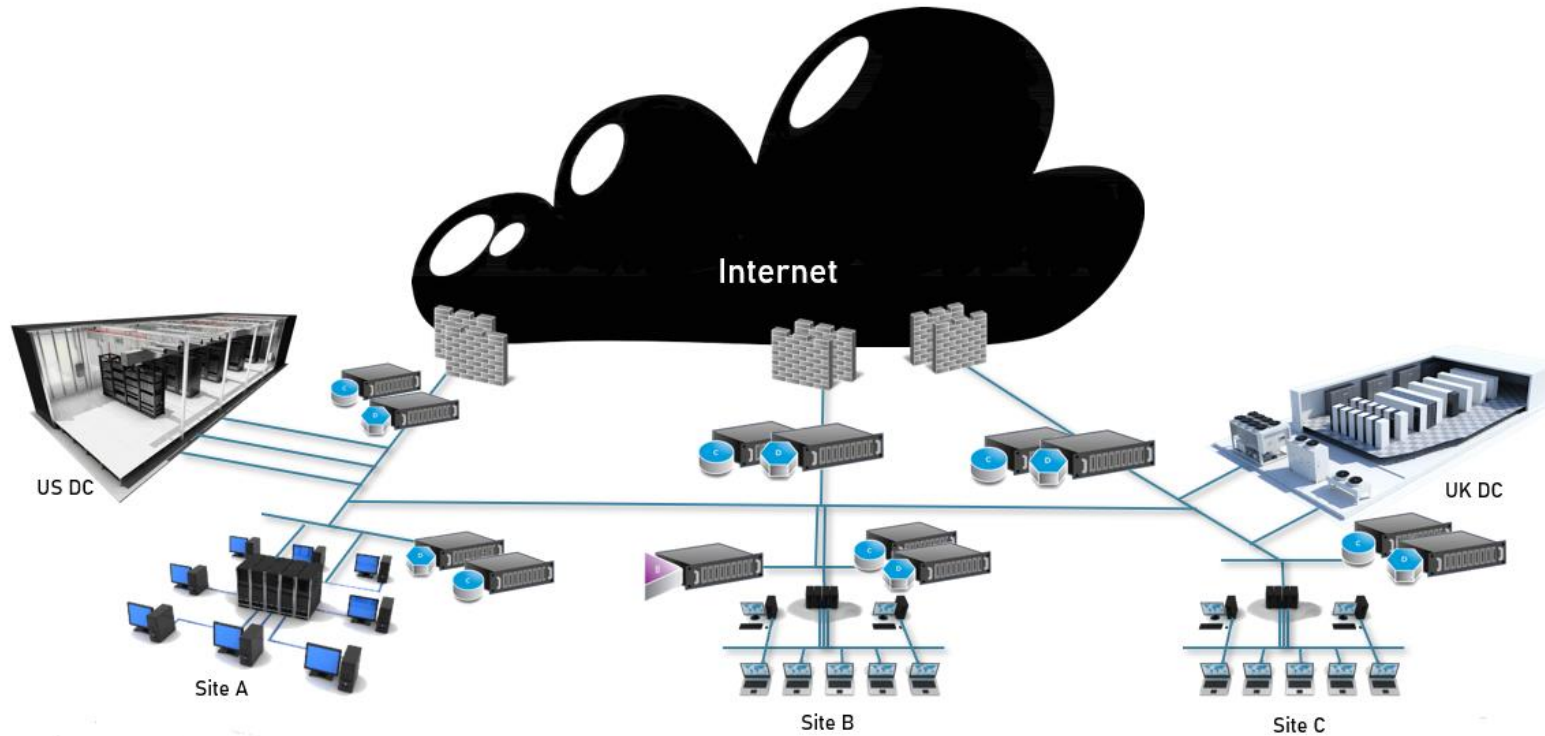
**"Possible Metasploit Reverse HTTPS traffic"**

- Due the fact that the customer has a retainer contract in place with RSA, SOC team decide to open a call to verify if the IPS alert is anything to worry about... more a scruple from the SOC team, than a real point of attention.



# DEAD MEN TELL NO TALES

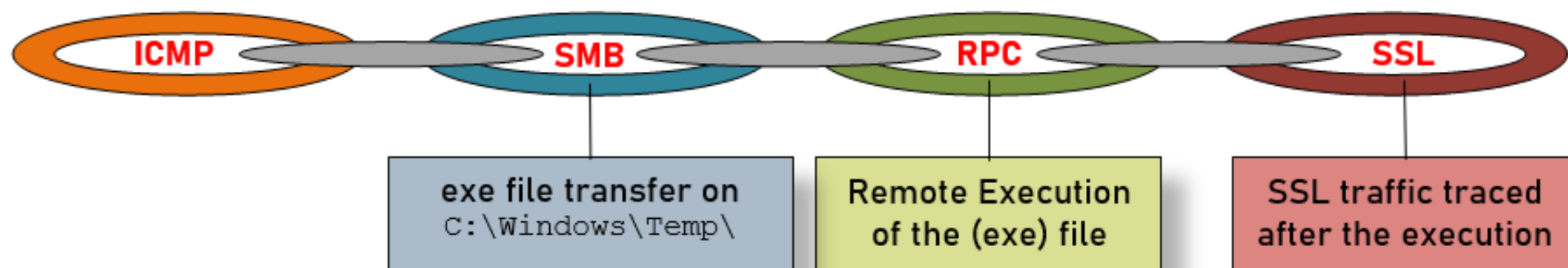
- RSA NetWitness packet was already in place on the main datacenter to monitor the network traffic.



- When the incident occurred, the Customer was not having an EDR solution in place, so RSA IR Team proceeded to deploy RSA NetWitness Endpoint and started to distribute the agent on all the involved hosts.

# RSA INITIAL FINDINGS

- RSA identified a pattern on the unusual communication that happened from two server that never communicated each other.
- Within the network traffic it was evident the SMB transfer of an executable file followed by the execution of some of remote commands.

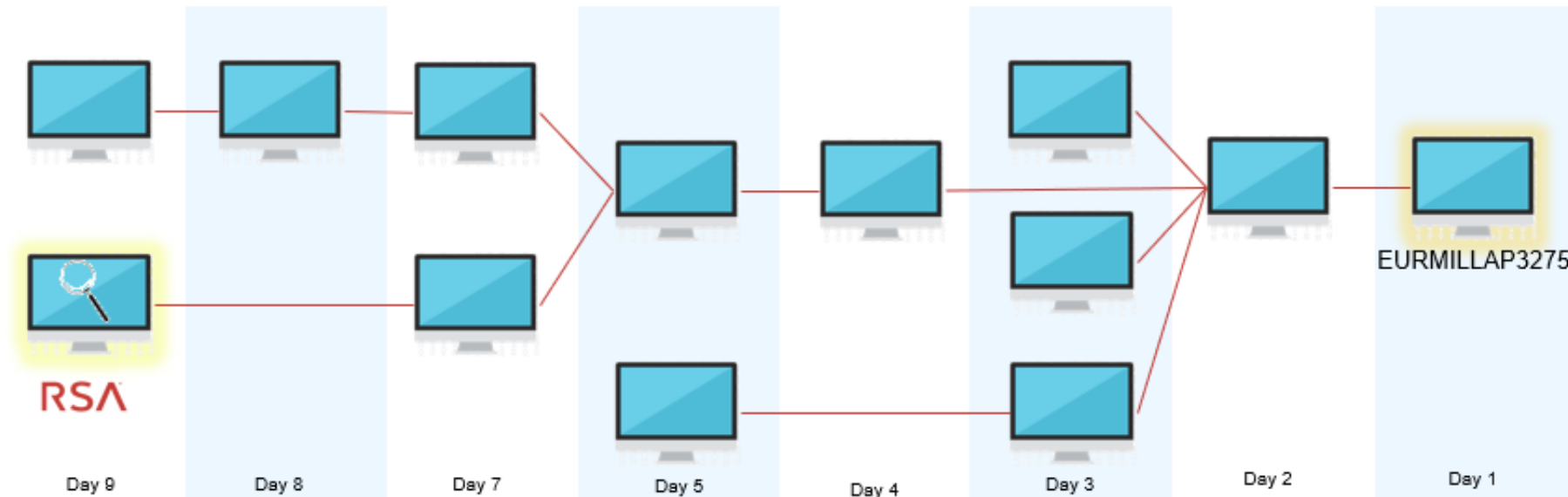


By expanding the scope of network traffic to all SMB sessions that contained executable file transfers to the Window's temp directory, RSA identified a bounce of systems infected with a similar chain of events (i.e. ICMP > SMB > RPC > SSL).



# RSA INITIAL FINDINGS

- Following the backlinks RSA could identify the first infected system



- RSA identified on the host EURMILLAP3275 the Patient Zero.
- The first file transferred to `C:\Windows\Temp` via an **SMB session** happened a week before the call.



# PATIENT ZERO

Multiple Gmail accounts were used to send the emails

Event Reconstruction

service	id	type	source	destination	service
Broker	82116733901	Network Session	172.24.71.74 : 58049	172.24.70.125 : 25	25

Request & Response Top To Bottom Best Reconstruction Actions Open Event in New Tab Event Analysis

From: 'Miller, John (JobSecure)' <tharris235@gmail.com> Sent on 2020-04-24 17:34:58.000  
To: [REDACTED]  
Subject: Manager position (Remote) more

Hi Darren,  
based on the recent discussion that we have i send you the link containing the job proposal. Please have a look to it and let me know if you are intereested to continue the conversation.

<https://jobscure.com/?offer=%dbfhtyukrb38573dhd74n2bshe74i5medhd738932ghb>

John  
Talent manager

The email contains an URL that downloads malicious software

- Looking at the network traffic RSA identified a phishing email contained a link.
- Similar email was sent to multiple person inside the company.



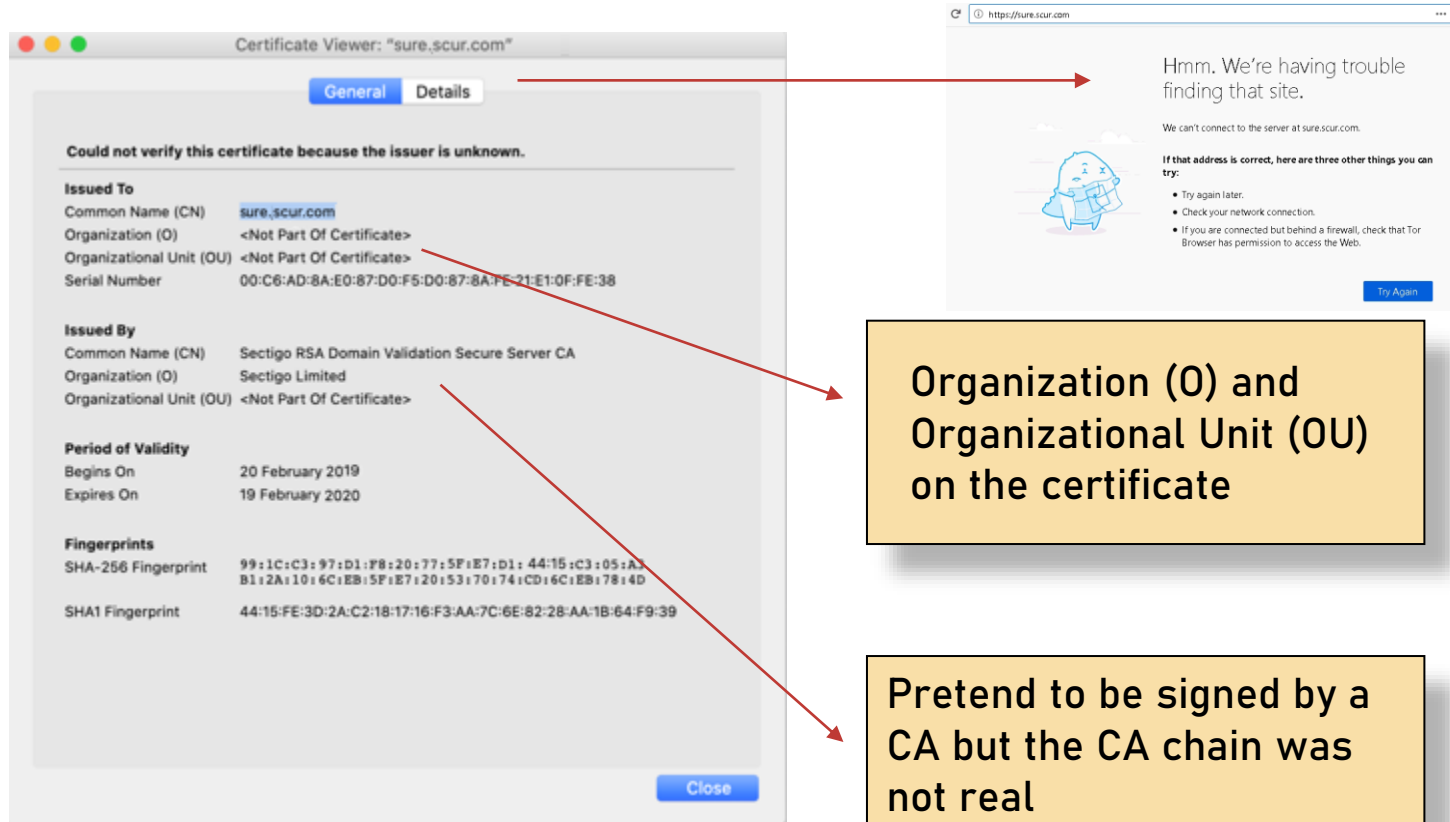
RSA

Using RSA NetWitness Packets, we were able to reconstruct the original email and retrieve the link used to download the malicious code.

At the time of the analysis the link was no longer active.

# PATIENT ZERO ANALYSIS

- EURMILLAP3275 contacts the link included on the email and few minutes after starts to communicate on SSL with 2 more hosts.



No website associate to the hostname and no information on Google about it!

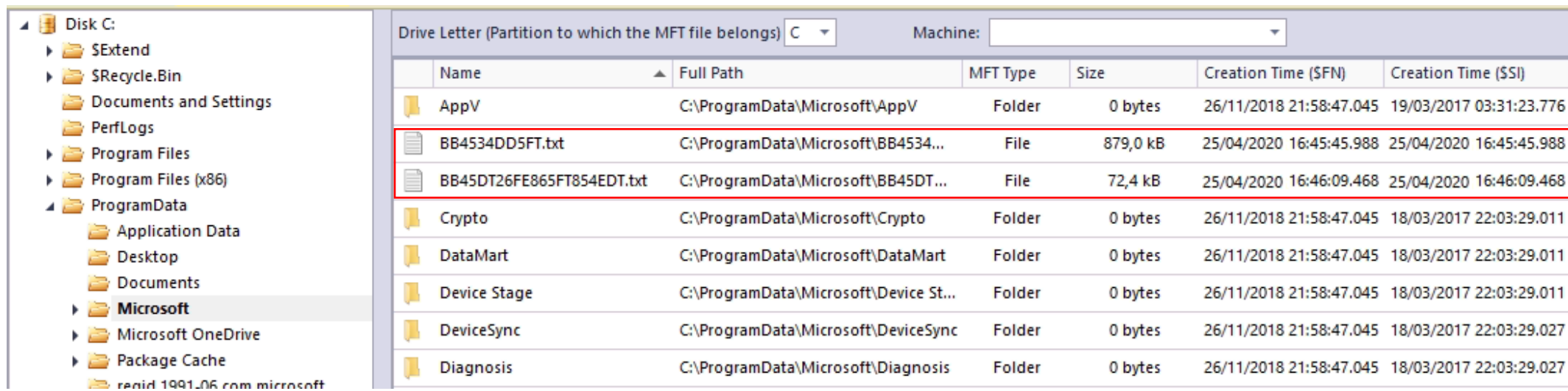
Organization (O) and Organizational Unit (OU) on the certificate

Pretend to be signed by a CA but the CA chain was not real

Looking for all the SSL traffic with similar characteristics allow RSA analysts to uncover all the C2 stations used by the attacker.

# PATIENT ZERO ANALYSIS

Through the endpoint analysis performed using NetWitness Endpoint, RSA analyst was able to retrieve part of the malware artifacts used for the initial infection.



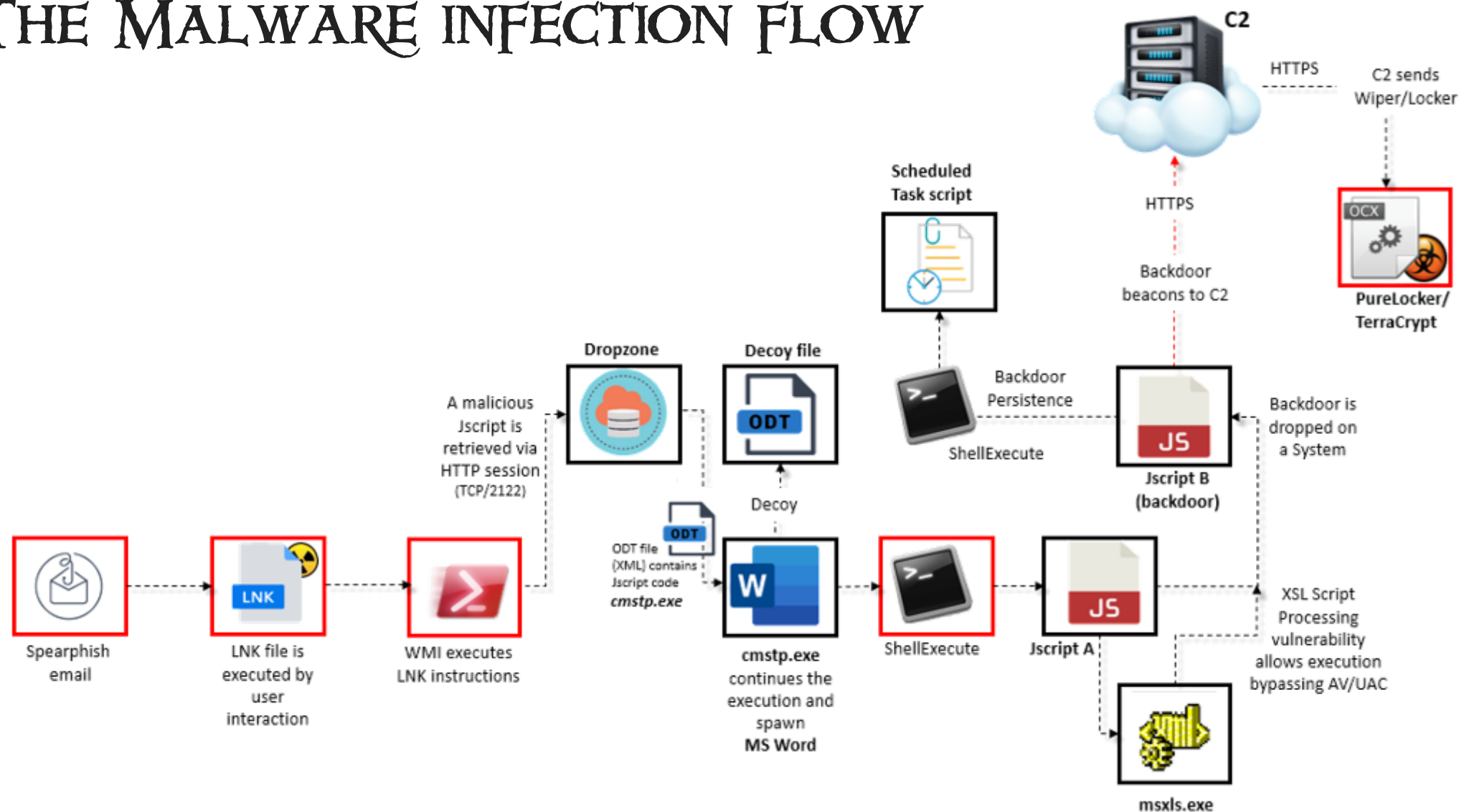
Name	Full Path	MFT Type	Size	Creation Time (\$FN)	Creation Time (\$SI)
AppV	C:\ProgramData\Microsoft\AppV	Folder	0 bytes	26/11/2018 21:58:47.045	19/03/2017 03:31:23.776
BB4534DD5FT.txt	C:\ProgramData\Microsoft\BB4534...	File	879,0 kB	25/04/2020 16:45:45.988	25/04/2020 16:45:45.988
BB45DT26FE865FT854EDT.txt	C:\ProgramData\Microsoft\BB45DT...	File	72,4 kB	25/04/2020 16:46:09.468	25/04/2020 16:46:09.468
Crypto	C:\ProgramData\Microsoft\Crypto	Folder	0 bytes	26/11/2018 21:58:47.045	18/03/2017 22:03:29.011
DataMart	C:\ProgramData\Microsoft\DataMart	Folder	0 bytes	26/11/2018 21:58:47.045	18/03/2017 22:03:29.011
Device Stage	C:\ProgramData\Microsoft\Device St...	Folder	0 bytes	26/11/2018 21:58:47.045	18/03/2017 22:03:29.011
DeviceSync	C:\ProgramData\Microsoft\DeviceSync	Folder	0 bytes	26/11/2018 21:58:47.045	18/03/2017 22:03:29.027
Diagnosis	C:\ProgramData\Microsoft\Diagnosis	Folder	0 bytes	26/11/2018 21:58:47.045	18/03/2017 22:03:29.027



The two TXT files, with a name formed by strings of random characters, saved in c:\ProgramData\Microsoft are actually the two javascript that allow communication with the C2



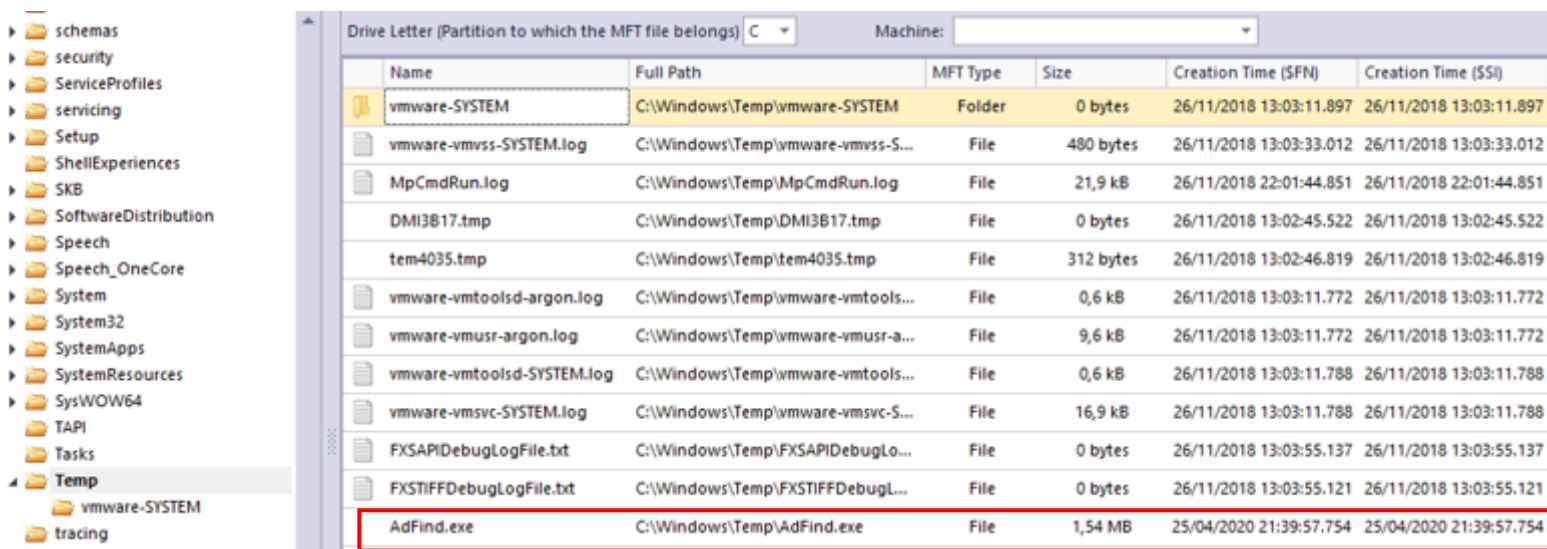
# THE MALWARE INFECTION FLOW



# PATIENT ZERO ANALYSIS

On the same client RSA was able to identify a command line Active Directory query tool called:

**AdFind.exe**



The screenshot shows a Windows File Explorer window with the 'Temp' folder selected in the left sidebar. The main pane displays a list of files and folders. The 'AdFind.exe' file is highlighted with a red box. The table below represents the data shown in the screenshot.

Name	Full Path	MFT Type	Size	Creation Time (SFN)	Creation Time (SSI)
vmware-SYSTEM	C:\Windows\Temp\vmware-SYSTEM	Folder	0 bytes	26/11/2018 13:03:11.897	26/11/2018 13:03:11.897
vmware-vmvss-SYSTEM.log	C:\Windows\Temp\vmware-vmvss-S...	File	480 bytes	26/11/2018 13:03:33.012	26/11/2018 13:03:33.012
MpCmdRun.log	C:\Windows\Temp\MpCmdRun.log	File	21,9 kB	26/11/2018 22:01:44.851	26/11/2018 22:01:44.851
DMI3B17.tmp	C:\Windows\Temp\DMI3B17.tmp	File	0 bytes	26/11/2018 13:02:45.522	26/11/2018 13:02:45.522
tem4035.tmp	C:\Windows\Temp\tem4035.tmp	File	312 bytes	26/11/2018 13:02:46.819	26/11/2018 13:02:46.819
vmware-vmtoolsd-argon.log	C:\Windows\Temp\vmware-vmtools...	File	0,6 kB	26/11/2018 13:03:11.772	26/11/2018 13:03:11.772
vmware-vmusr-argon.log	C:\Windows\Temp\vmware-vmusr-a...	File	9,6 kB	26/11/2018 13:03:11.772	26/11/2018 13:03:11.772
vmware-vmtoolsd-SYSTEM.log	C:\Windows\Temp\vmware-vmtools...	File	0,6 kB	26/11/2018 13:03:11.788	26/11/2018 13:03:11.788
vmware-vmtoolsd-SYSTEM.log	C:\Windows\Temp\vmware-vmtools...	File	16,9 kB	26/11/2018 13:03:11.788	26/11/2018 13:03:11.788
FXSAPIDebugLogFile.txt	C:\Windows\Temp\FXSAPIDebugLo...	File	0 bytes	26/11/2018 13:03:55.137	26/11/2018 13:03:55.137
FXSTIFFDebugLogFile.txt	C:\Windows\Temp\FXSTIFFDebugL...	File	0 bytes	26/11/2018 13:03:55.121	26/11/2018 13:03:55.121
AdFind.exe	C:\Windows\Temp\AdFind.exe	File	1,54 MB	25/04/2020 21:39:57.754	25/04/2020 21:39:57.754

File has been stored under `c:\Windows\Temp` and executed on the day of the initial infection, presumably to enumerate the the Active Directory servers.

RSA was not able to recover the data exfiltrated due the missing of an EDR in place during the attack.



# LIVING-OFF-THE-LAND ATTACKS

- Attacker behavior that uses tools or features that already exist in the target environment.
- Using pre-existing software avoids the process being flagged as suspicious and reduce the possibility to be intercepted.
- Distinguish malicious use of built-in tools versus the authorized use of tools by the system administrator can be tough for the analyst.
- Additionally, the attacker is secure to find the correct version of the software on each machine, don't need to be worried about compatibility of it is artifacts.
- Attacker tend to use fileless attack where the resources used are not written to disk. Thinks that stay in memory are much harder to both detect and to find later.



# TO PROTECT AND SERVE...

# ADVICES FOR THE NEGOTIATION

---

- When the Ransomware is detonated it will display information about on how to contact (the crime gang) to pay the fee that they are looking for and receive the key to unencrypt the data.
- While we recommend not to pay, unless critical to keep the business on, we advise to open the channel for a conversation with the cybercriminals.
- Once authorized by counsel/client, contact is made with the gang on the dark web to advise them that systems are impacted and we would like to discuss getting our data back, or data not being released to public sites, etc.
- We provide them with a known encrypted file to make sure they are able to unencrypt and provide us back the known file to ensure that actually have the decryptor.
- In addition, to gain credibility, we have a discussion about how to lower price, funds available, etc...
- There is always room in negotiating a fee lower, and the cybercriminals expect that.



# NEGOTIATION PITFALLS

- In the last twelve months we participated to the negotiation in several cases and we learned some important aspects:
- Do not underestimate the negotiation from the Cybercriminal gang, they are often skilled individual with wide experience on such topics... in fact, in one case, we clearly faced a conversation with a former FSB negotiator (he told us about that).
- The conversation should be strictly limited in number of participants. In one case, when an uninvited participant joined the negotiation at a later stage, the attacker get off the channel and the data went immediately released...
- The attackers are willing to explain how good they are... this is the only weak spot we found during the negotiations... you can leverage on this to collect some critical items useful for the IR investigation.
- The attacker is usually not keen to overreact, he knows he has some good files in his hand... He reviewed his stuff before detonating the ransomware, so every attempt to downsize the value of the stolen material, during the negotiation, will fail... sometime will fail miserably...



# LESSON LEARNED

DON'T LET THE PRESSURE GUIDE YOU... ALWAYS THINK ABOUT POSSIBILITIES...

THE BLACKHATS TELL YOU THEY ARE PERFECT... BUT THEY ARE NOT...

THE KEY IS TO USE THE NEGOTIATION AS A FUNCTIONAL STEP

DON'T TAKE SHORTCUTS... TRY TO SUPPORT THE INVESTIGATION

THINK POSITIVE...



## POST-INCIDENT RECOMMENDATIONS

- Even with the decryptor, unencrypting the data is a painful and costly experience for a company...
- Our continuous message to clients is to **secure and segment** their **infrastructure so these attacks are not as successful**. *That is cheaper than the response efforts that occur with a breach.*
- The anonymity of the Internet and the lack of international cooperation between the countries have really hampered the ability of law enforcement/prosecutors to take any real meaningful action to identify and prosecute these OC (organized crime) and nation-state actors.
- Thus, since this avenue is a long shot to dissuade threat actors, it is up to companies to do a better job of protecting themselves



# Q'N'A

rights reserved.

CONFIDENTIAL

RSA



# THANKS!

