



THE BEST OF 2022-2023:

inside the biggest hacks and facts of the past year





- Love BruCON and just about everything geeky
- Since 2009 in security
- Threat Intelligence analyst
- Global lead Attack Surface Management



THREAT EXPOSURE

We manage your attack surface



threatexposure.eu



dieter.vandenbosch@threatexposure.eu



[@Threat_Exposure](https://twitter.com/Threat_Exposure) (**Twitter/X**)



[@Threat_Exposure@infosec.exchange](https://infosec.exchange/@Threat_Exposure) (**Mastadon**)

BruCON 2022

START

ProxyNotShell

Zero-day in Microsoft
Exchange server,
again

SEP
29

ProxyLogon

Remote Code Execution (RCE)
in Microsoft Exchange



Mar
2021

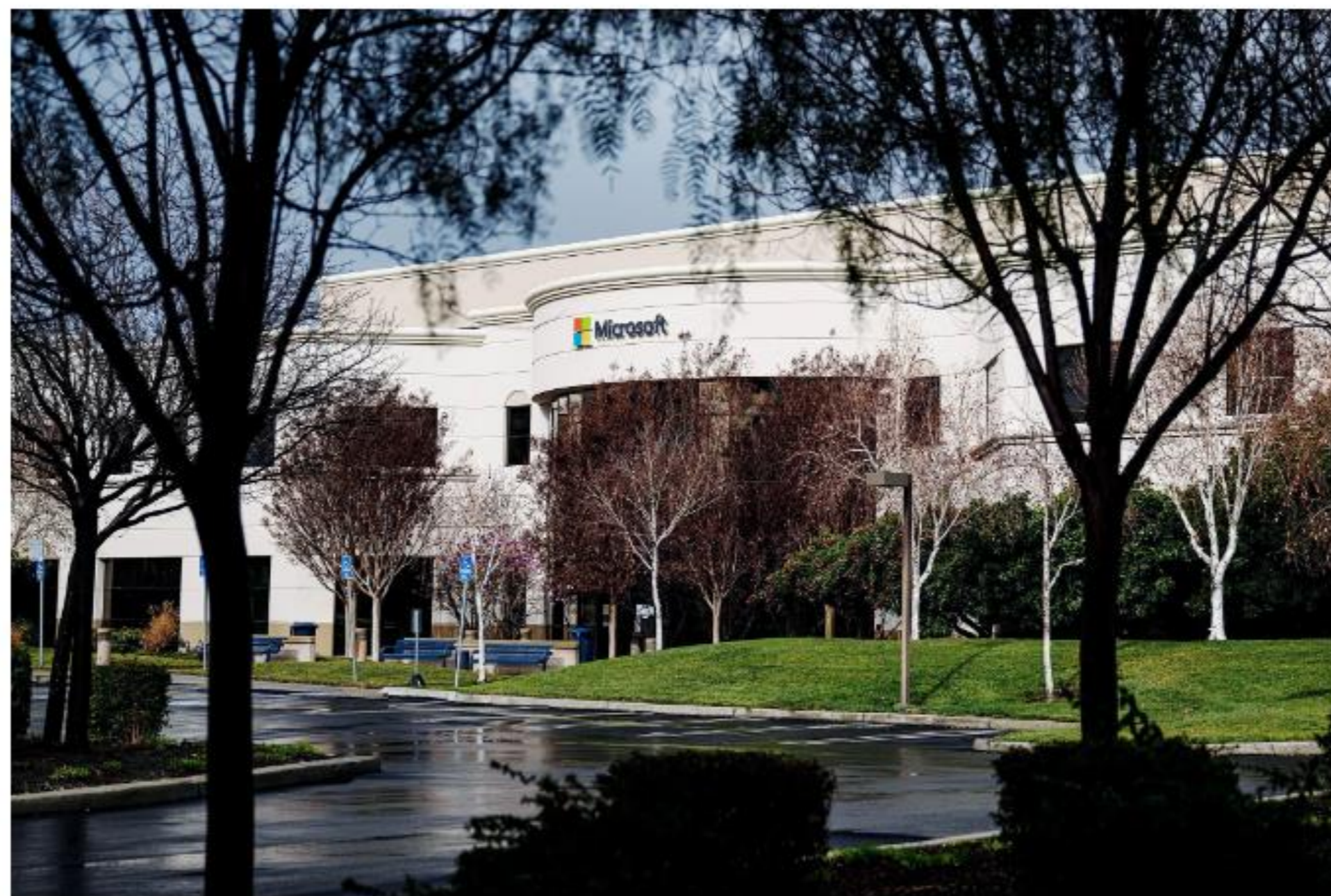
Aug
2021

ProxyShell

Again, RCE in Microsoft
Exchange server,
mass exploited

Chinese Hacking Spree Hit an 'Astronomical' Number of Victims

A single group appears to have infiltrated tens of thousands of Microsoft Exchange servers in an ongoing onslaught.



PHOTOGRAPH: DAVID PAUL MORRIS/BLOOMBERG/GETTY IMAGES

ProxyLogon

Remote Code Execution (RCE)
in Microsoft Exchange



Mar
2021

Aug
2021

ProxyShell

Again, RCE in Microsoft
Exchange server,
mass exploited

ProxyNotShell

Zero-day in Microsoft
Exchange server,
again

SEP
29

Kevin Beaumont @GossiTheDog writes a blog



30/09:

Update: Microsoft have been through triage now, and issued CVE-2022-41040 and CVE-2022-41082. These are two new zero day vulnerabilities in Exchange. It appears the ProxyShell patches from early 2021 did not fix the issue. There are currently no patches.

I am calling this ProxyNotShell, as it is the same path and SSRF/RCE pair from back then... but with authentication.

7. Add String `.*autodiscover\.json.*\@.*Powershell.*` (excluding quotes) and click OK.

03/10:

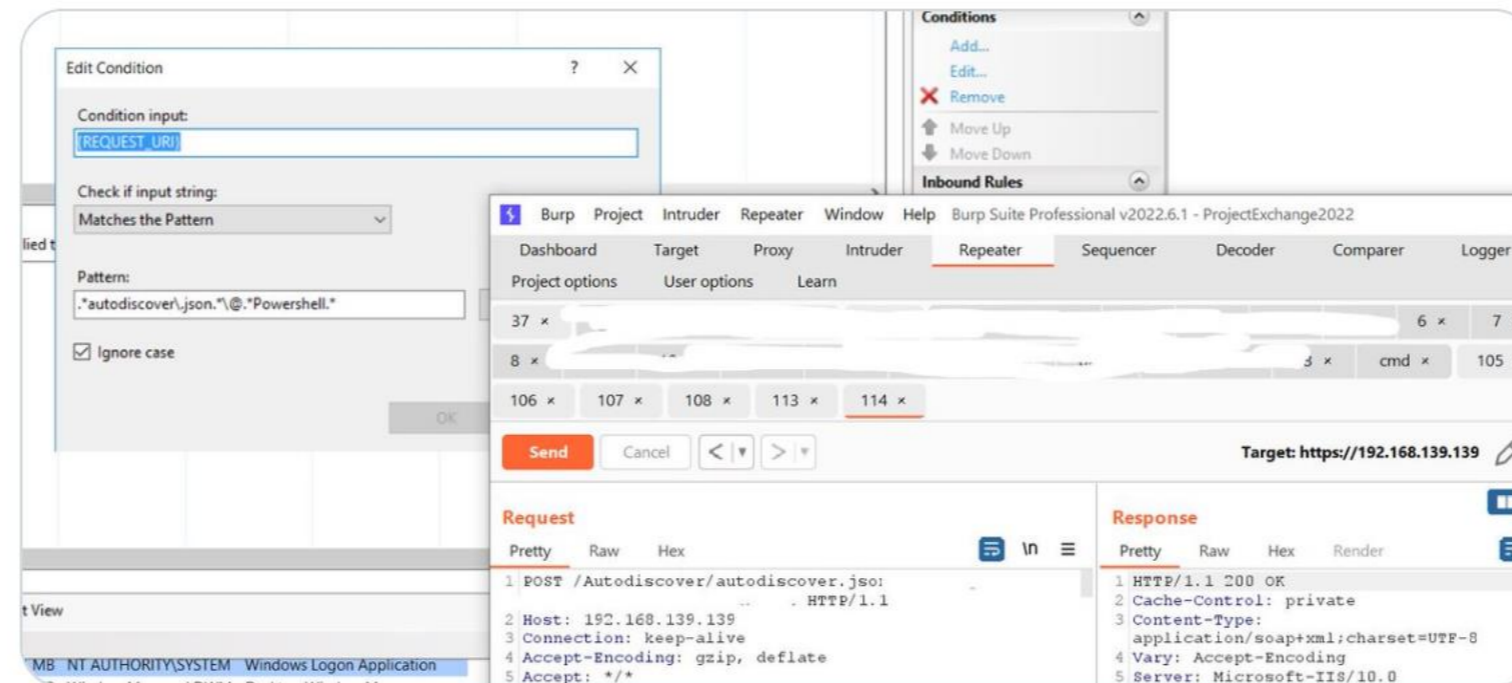
 **Janggggg**
@testanull

Lol

The URL pattern to detect/prevent the Exchange Oday provided in MSRC's blog post can easily be bypassed

[@GossiTheDog](#)

[Post vertalen](#)



The screenshot displays the Burp Suite Professional v2022.6.1 interface. An 'Edit Condition' dialog box is open, showing a condition input of 'REQUEST_URI' and a pattern of '*.autodiscover/json,*/@*Powershell.*'. The 'Matches the Pattern' dropdown is set to 'Matches the Pattern', and the 'Ignore case' checkbox is checked. The main interface shows the 'Repeater' tab with a target URL of 'https://192.168.139.139'. The 'Request' and 'Response' sections are visible, showing a POST request to '/Autodiscover/autodiscover.json' and an HTTP/1.1 200 OK response.

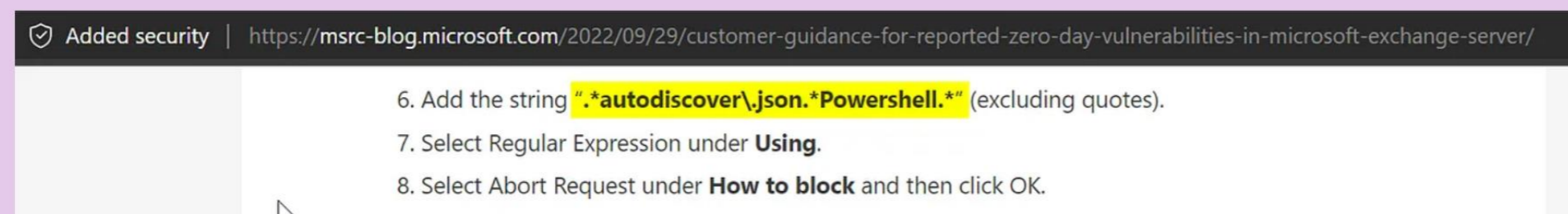
5:19 a.m. · 3 okt. 2022



More than a day later:

4th October 2022–9pm BST

Microsoft have corrected the mitigation guidance for the bypass:



They have not mentioned the mitigation was easily bypassable.

If you manually applied this mitigation you need to manually ***change*** the mitigation string above. If you ran **EOMTv2**, you need to **redownload** the script and **run it again**. The EOMTv2 website *doesn't say the script has changed* —



One day later:

5th October 2022–4pm BST

There is now **a bypass of the mitigation for the bypass of the mitigation.**

Microsoft forgot to enable URL decoding in IIS URL Rewrite, so you can just encode the P in Powershell as %50 as an example:



Two days later:

7th October 2022-10am BST

People have found there is another bypass to the mitigation to bypass to the mitigation to the bypass to the mitigation.

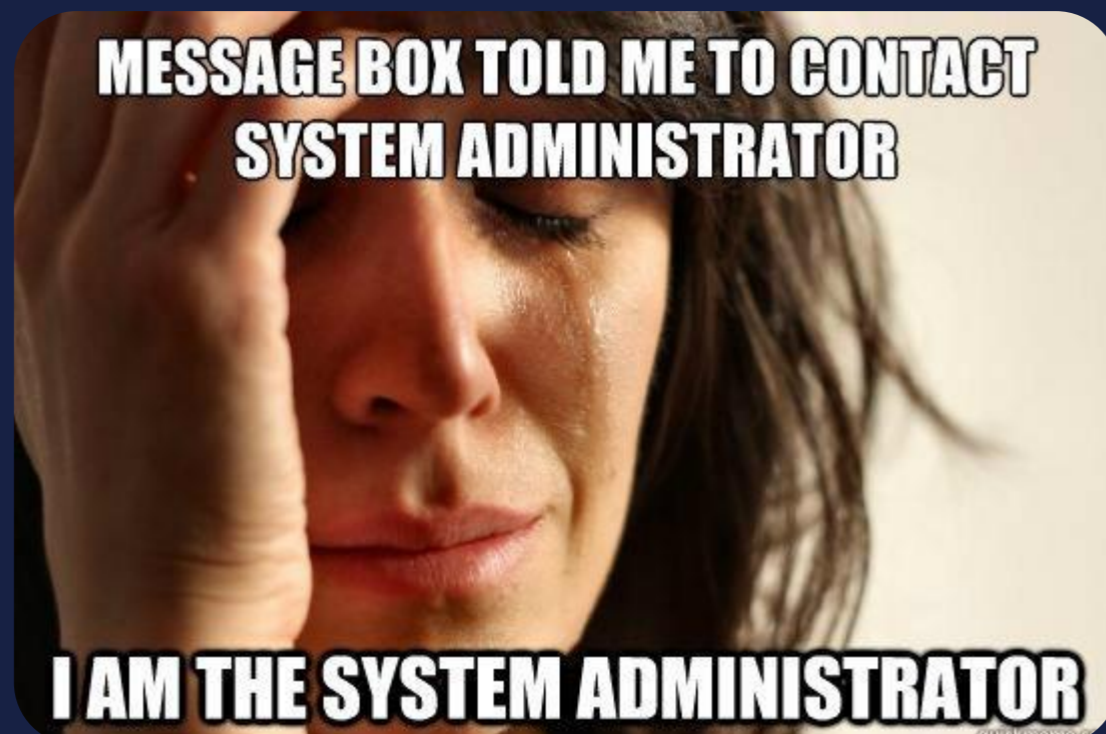
**MESSAGE BOX TOLD ME TO CONTACT
SYSTEM ADMINISTRATOR**



Two days later:

7th October 2022-10am BST

People have found there is another bypass to the mitigation to bypass to the mitigation to the bypass to the mitigation.





Two days later:

October 9th 2022-10am BST

The mitigation has been updated again by MS.

Regex changed from:

| `(?=.*autodiscover.json)(?=.*powershell)`

to:

| `(?=.*autodiscover)(?=.*powershell)`



One month and 6 f*ups later...

8th November 2022–7pm GMT

Microsoft have finally released a patch for this. Head over to Security Updates on this to grab the patches (you need to be on a supported Cumulative Update to have a patch).





Rackspace Cloud Office suffers destructive security breach



Kevin Beaumont · [Follow](#)

Published in DoublePulsar · 9 min read · Dec 3, 2022

- The Microsoft supplied mitigations for ProxyNotShell are bypassable. IIS Rewrite, which Microsoft used for mitigations, doesn't decode all URLs correct and as such can be bypassed for exploitation. If you relied on the PowerShell mitigation or EEMS application, your Exchange Server is still vulnerable — Microsoft just haven't told you this clearly. The fix is to patch.



Hosted Exchange Issues

[< Back to Dashboard](#)

Hosted Exchange Disruption

⚠ 05:41 PM EST
01/05/23

The forensic investigation determined that the threat actor, known as PLAY, used a previously unknown security exploit to gain initial access to the Rackspace Hosted Exchange email environment. This zero-day exploit is associated with CVE-2022-41080. Microsoft disclosed CVE-2022-41080 as a privilege escalation vulnerability and did not include notes for being part of a Remote Code Execution chain that was exploitable.

Microsoft Exchange Server Elevation of Privilege Vulnerability

CVE-2022-41080
Security Vulnerability

Released: 8 nov. 2022 Last updated: 15 dec. 2022

Assigning CNA: [📄](#) Microsoft

[CVE-2022-41080](#) [🔗](#)

Impact: Elevation of Privilege Max Severity: Critical

CVSS:3.1 8.8 / 7.7 [📄](#)

Exploitability

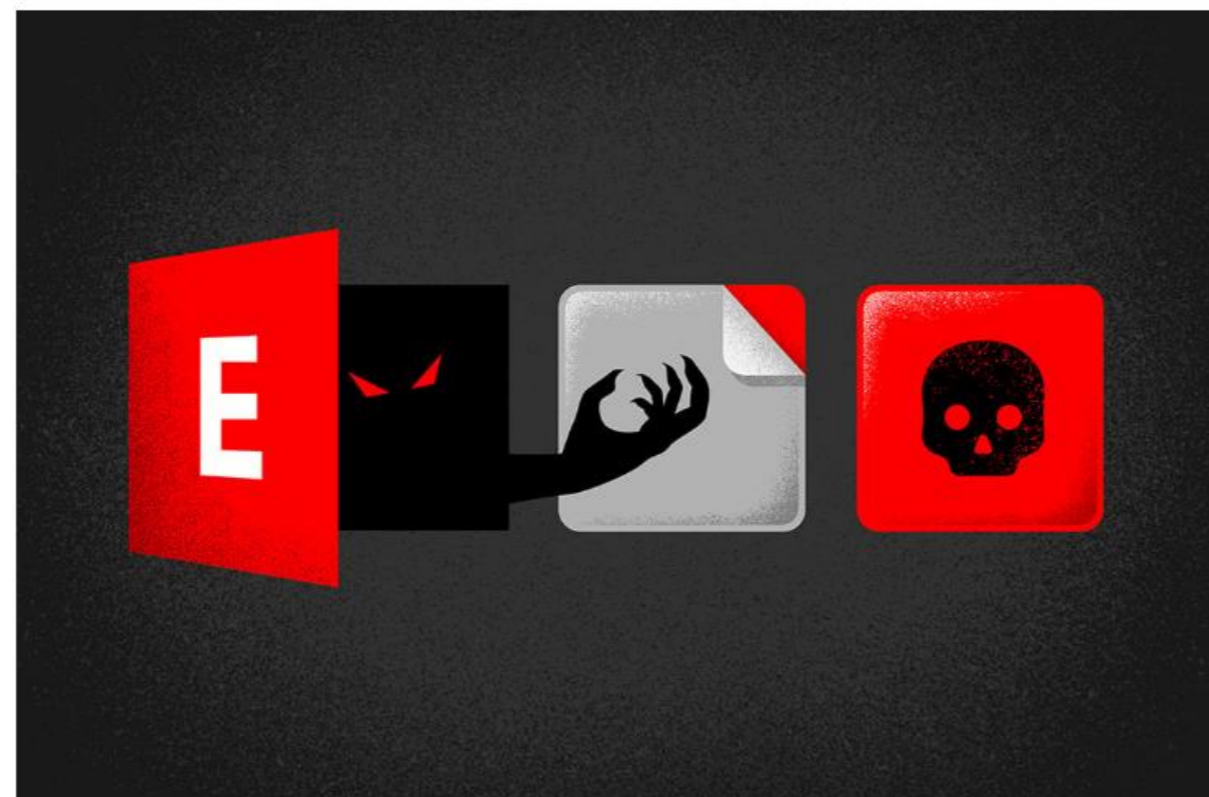
The following table provides an [exploitability assessment](#) for this vulnerability at the time of original publication.

Publicly disclosed	Exploited	Exploitability assessment
No	No	Exploitation More Likely

Microsoft still says so!

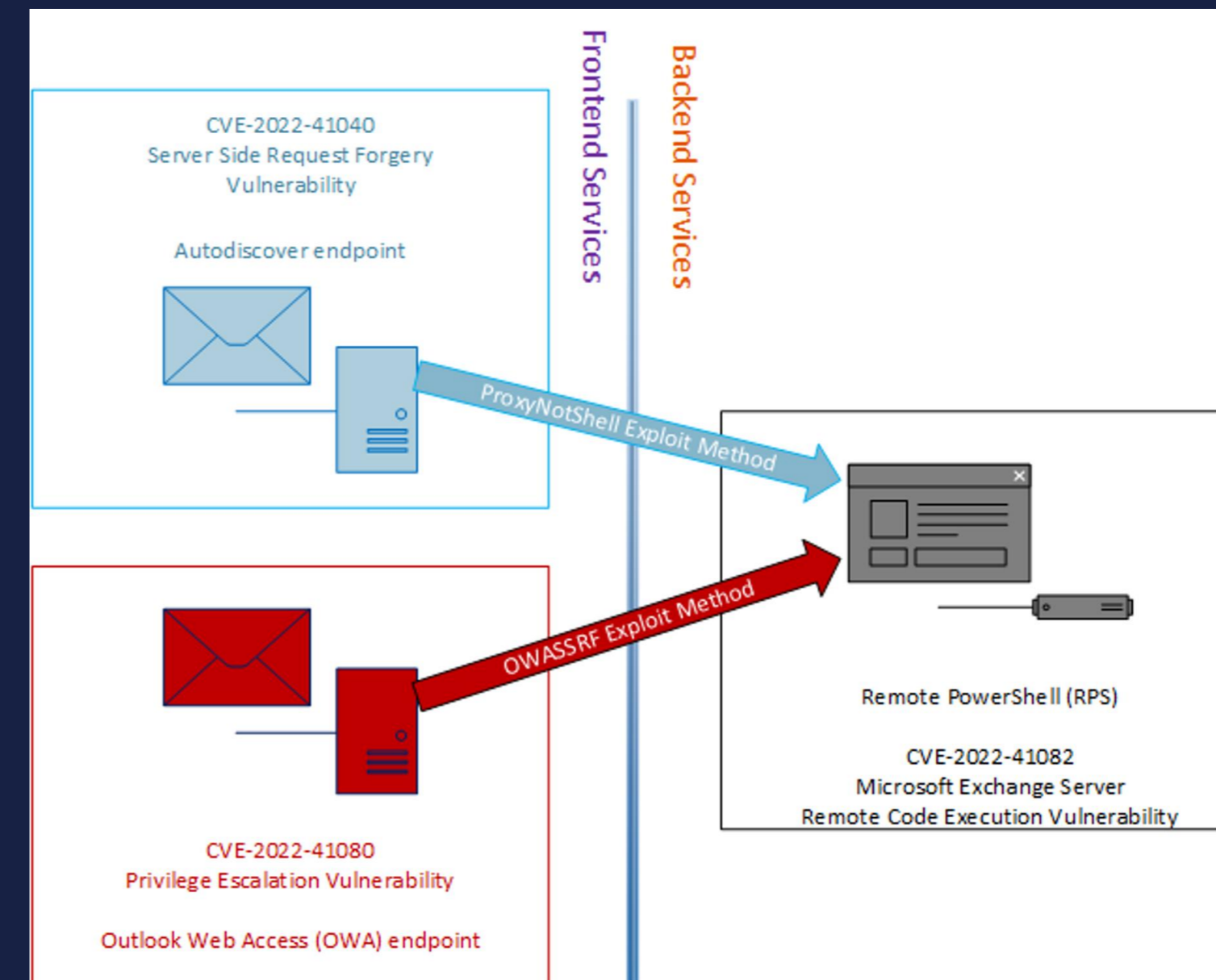
OWASSRF: CrowdStrike Identifies New Exploit Method for Exchange Bypassing ProxyNotShell Mitigations

December 20, 2022 Brian Pritchard - Erik Iker - Nicolas Zilio From The Front Lines



- o CrowdStrike recently discovered a new exploit method (called OWASSRF) consisting of CVE-2022-41080 and CVE-2022-41082 to achieve remote code execution (RCE) through Outlook Web Access (OWA). The new exploit method bypasses URL rewrite mitigations for the Autodiscover endpoint provided by Microsoft in response to ProxyNotShell.
- o The discovery was part of recent CrowdStrike Services investigations into several Play ransomware intrusions where the common entry vector was confirmed to be Microsoft Exchange.

Does that name ring a bell? ←



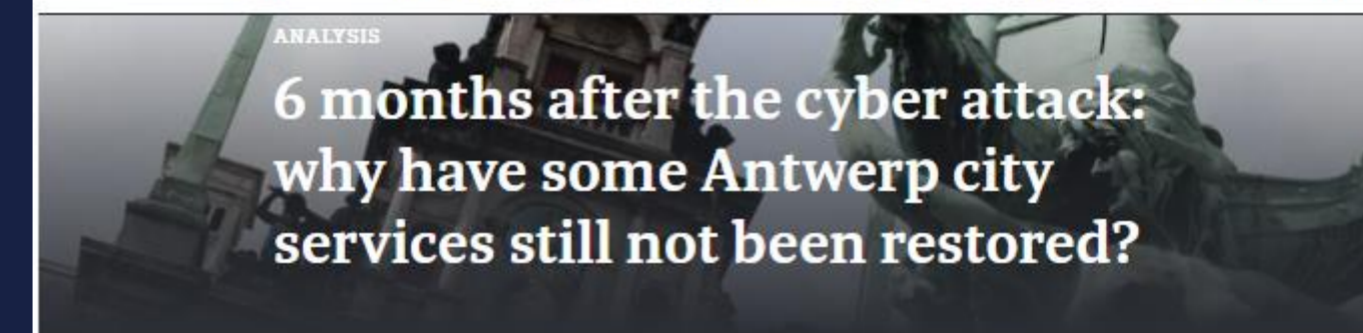
OWASSRF: Critical Vulnerability in Exchange Servers

The hackers behind the Play ransomware, which also shut down the services of the [City of Antwerp](#), found a way to penetrate Exchange servers with OWASSRF.

Researchers from cybersecurity firm CrowdStrike were the first to discover the vulnerability. It concerns a vulnerability in Microsoft Exchange called OWASSRF. This allows the people behind Play Exchange servers to penetrate and remotely load and activate their malware.

Microsoft cataloged the vulnerability as CVE-2022-41082 and immediately assigned it a “critical” status. The vulnerability allows hackers to bypass security mechanisms such as ProxyNotShell and remotely run code on a system. To do that, Remote PowerShell is abused.

Source: techpulse.be



The city hall in Antwerp.



Pieterjan Van Leemputten

25-05-2023, 10:51 • Updated on: 25-05-2023, 12:08 • Source: Data News •

At the beginning of December, Antwerp was hit by a cyber attack. Almost six months later, not all services are operational again. Complexity, but also extra measures, mean that the recovery will take some time.

Residents of the city of Antwerp will remember the [ransomware attack](#) for a long time. Although the [stolen data](#), 557 gigabytes, has not been misused anywhere as far as is known, the attack compromised a large part of the digital service. The city estimates that the cost of the attack could be [as high as 70 million euros](#).

Source: datanews.be

ProxyNotShell

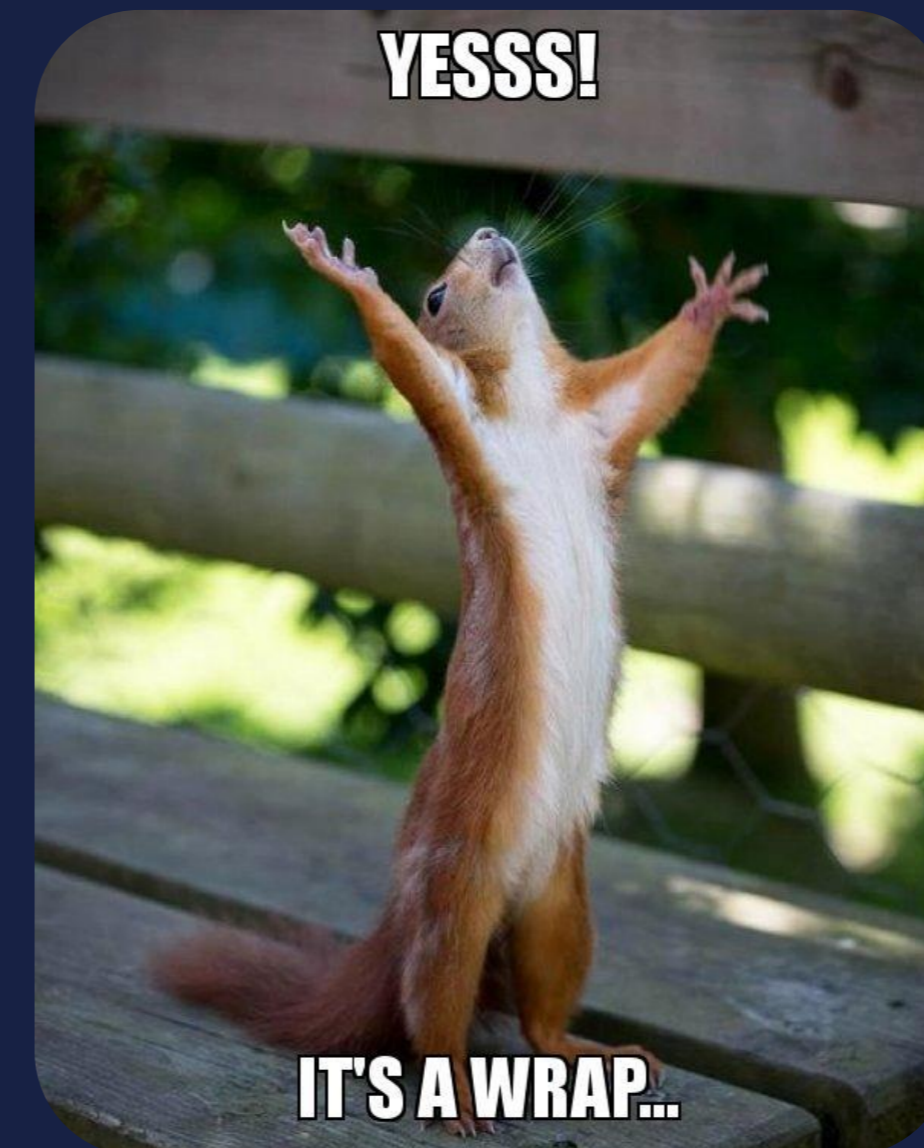
3rd zero-day RCE in Microsoft Exchange server since 2021

SEP
30

OWASSRF

4th zero-day RCE in Microsoft Exchange server

NOV/
DEC



'Critical' bug in OpenSSL v3

It was a 'Heartbleed-level' bug!

But... almost impossible to exploit.
Winner of the Most Overhyped Bug of the Year.

Honorable mention for Text4Shell (19 October)


OCT
25

NOV
16

Police Zwijndrecht



Home Page of Ragnar_Locker Leaks site



WALL OF SHAME

Here will be permanent list of companies who would like to keep in secret the info leakage, exposing themselves and their customers, partners to even greater risk than a bug-hunting reward!

[\[redacted\] - Leaked](#)
Published: 11/24/2022 21:20:25

[\[redacted\]](#)
Published: 11/20/2022 14:06:19

[Belgium company Zwijndrecht - Leaked](#) ←
Published: 11/16/2022 14:33:09

Source: Bleepingcomputer



Example of speed camera picture. Source: hln.be

LOKALE POLITIE ZWIJNDRECHT
Zoncode 6346

NAVOLGEND PROCES-VERBAAL

Proces-verbaalnummer: [redacted]
di [redacted]

Referentie:
• Aanvankelijk nummer: [redacted] (ZZ ZWIJNDRECHT)

Bestemming:
• Procureur des Konings sectie jeugd & gezin te Antwerpen (origineel + afschrift)

Aandachtspunten:

Feiten:

- Inbreuk op artikel SWB 383: poging tot Doodslag zonder verdere specificaties
- Inbreuk op artikel SWB 386, 399, 400, 401, 495bis, 495ter: opzettelijke slagen en/of verwondingen aan een minderjarige, door de ouders
- Inbreuk op artikel: rookbal probleem - verontuurde opvoedingssituatie

Plaats: 2070 Zwijndrecht
Tijdstip: op [redacted]

Verdachte:
[redacted]
Ger. Trilijn: Foto: NEE - Vingerafdrukken: NEE - Ind. beschrijving: NEE

Slachtoffer:
[redacted]
Geboren te: [redacted] 2003
Wonende te: 2070 Zwijndrecht

Aantal bijlagen: 1 (44n)

Verzonden op: [redacted] Vak bestemd voor het parket: [redacted]

LOKALE POLITIE ZWIJNDRECHT
Zoncode 6346

Vervolg 1 proces-verbaal [redacted]

Op [redacted]
Wij [redacted] Inspecteur van politie bij de lokale politie Zwijndrecht, dragers van onze dienstkaat en in uniform gekleed, berichten:

Aand. plaats, tijdstip, kennisname van de feiten:

- Inbreuk op artikel SWB 383: poging tot Doodslag zonder verdere specificaties
- Inbreuk op artikel SWB 386, 399, 400, 401, 495bis, 495ter: opzettelijke slagen en/of verwondingen aan een minderjarige, door de ouders
- Inbreuk op artikel: rookbal probleem - verontuurde opvoedingssituatie

Plaats: 2070 Zwijndrecht
Tijdstip: op [redacted]
Kennisname van de feiten: [redacted]

Betrokken partijen:

[redacted] (verdachte)
[redacted] (slachtoffer)

Vaststellingen door de opstellers:
Zoals beschreven in het aanvankelijk proces-verbaal met nummer [redacted] voegen wij aan huidige akte de foto van de verwondingen van het slachtoffer toe als bijlage 01

Op deze foto is te zien dat er ter hoogte van de nek van het slachtoffer meerdere schrammen zijn. Dit komt volgens het slachtoffer omdat de verdachte hem trachtte te wurgen.

Bijlagen:

- bijlage 01: foto van de verwondingen van het slachtoffer

Proces-verbaal afgesloten op [redacted]
Waarvan akte: [redacted]

Source: hln.be

'Critical' bug in OpenSSL v3

It was a 'Heartbleed-level' bug!
But... almost impossible to exploit.
Winner of the Most Overhyped Bug of the Year.
And an honorable mention for Text4Shell (October 19)

OCT
25

Police Zwijndrecht

NOV
16



ChatGPT released

I'm not going to say anything about
GhatGPT & A.I. But I do have a
message from someone who will...

NOV
30





A message from Snoop Dogg
(& Midjourney & Speechify)

Belgian City of Diest

City of Diest: "The impact of the ransomware attack was gigantic"

DEC
12

DEC
13

Zero-day Citrix Netscaler
citrix™

citrix™

Dec 13

CVE-2022-27518 Zero-day RCE in Citrix Netscaler Gateway & ADC.

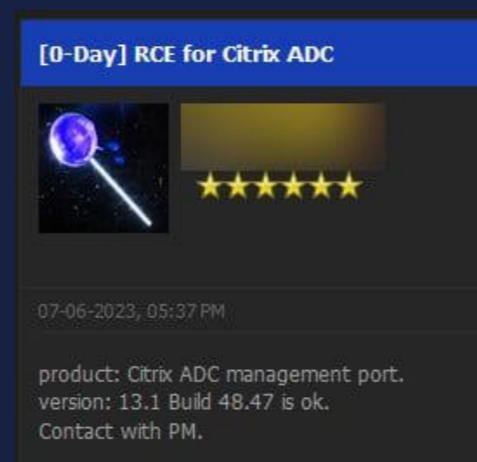
For appliances are configured as SAML SP or IdP



Exploited by Chinese state-sponsored hacking group APT5

July 07

Zero-day being sold on underground forum



Distribution of backdoored Citrix NetScaler servers (Fox-IT)

July 18

CVE-2023-3519 Citrix Netscaler ADC & Gateway

Webshells on around 2000 Citrix systems

Almost no web shells in Russia, Canada, U.S.

16 August

CVE-2023-24489 in StorageZones Controller in Citrix ShareFile

PoC exploit published

An unauthenticated attacker can remotely compromise customer-managed ShareFile storage zones controllers



DEC
22

The LastPass hack

LastPass: "Our customers' passwords remain safely encrypted due to LastPass's Zero Knowledge architecture"

\$35 million in crypto stolen from more than 150 confirmed victims

JAN
19

T-Mobile breached

...for the eight time since 2018.
37 million personal records stolen.

In March they were breached for the 9th time.

Belgian law ethical hacking

As first country in the world, it's allowed to search for vulnerabilities of Belgian companies without their approval.

Be aware: there are a lot of rules that force you to be really ethical.

FEB
15

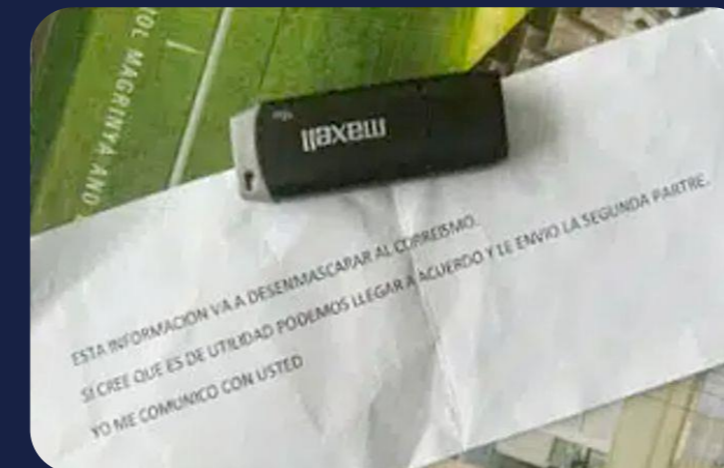


MAR
12

Journalist opens USB bomb in newsroom

Five Ecuadorian journalists received a USB-stick. One journalist inserted it in the newsroom at which point it exploded in his face.

The USB-stick contained explosives that detonate when it is connected to 5-volt.



“

That moment when
your life is saved by a faulty
Chinese USB cable

”

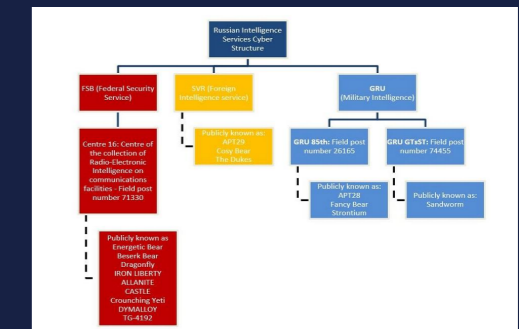
MAR
15

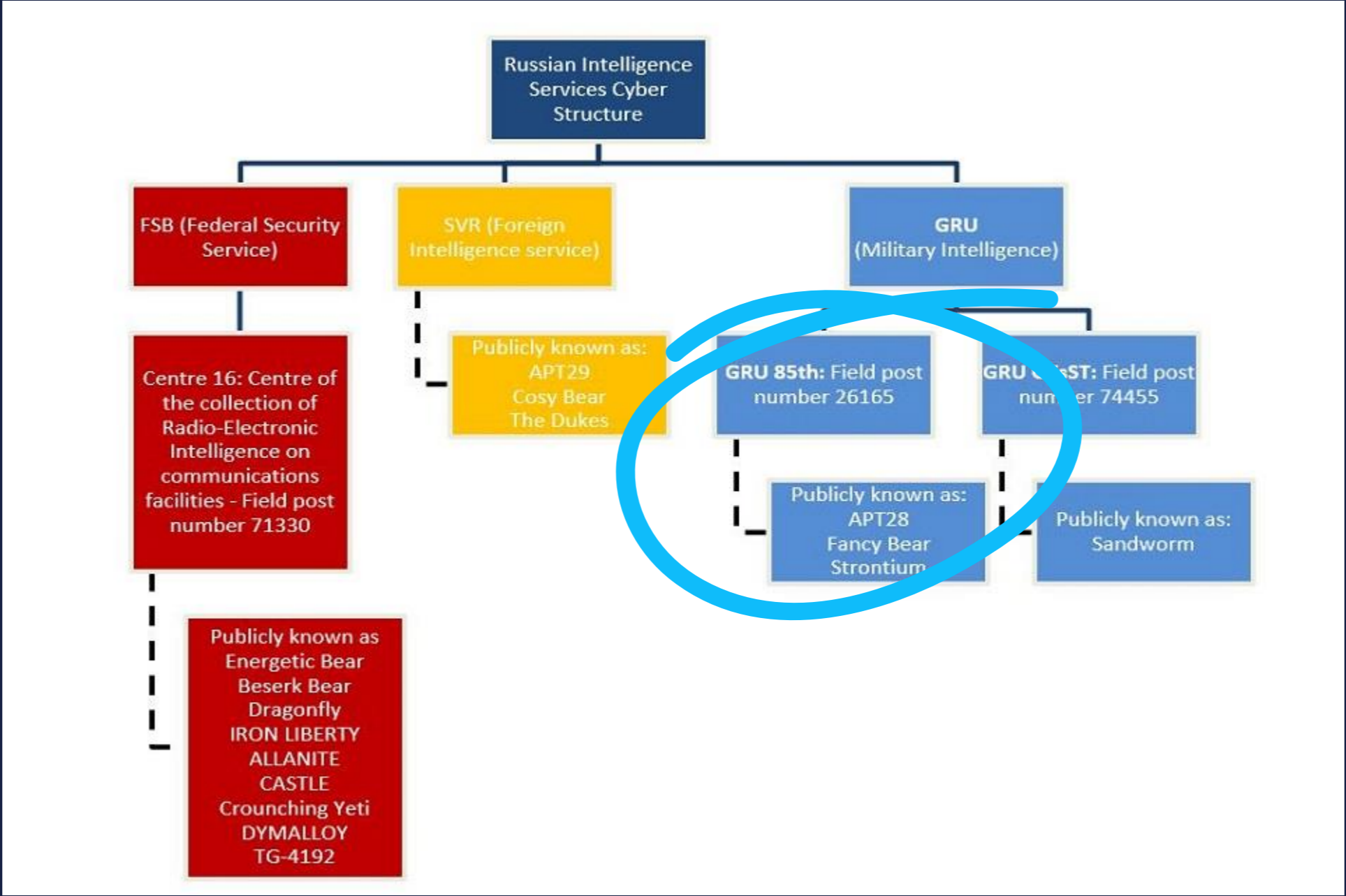
Zero-day in Outlook

Allows hackers to remotely steal hashed passwords by simply receiving an email (in NTLM-relay attacks)

By APT28/Fancy Bear/Strontium = Unit 26165 from the GRU

May 11: The patch was...





Source: gov.uk

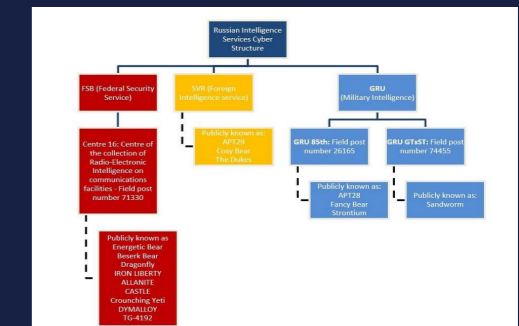
MAR
15

Zero-day in Outlook

Zero-day that allows hackers to remotely steal hashed passwords by simply receiving an email (in NTLM-relay attacks).

By APT28/Fancy Bear/Strontium = Unit 26165 from the GRU

**May 11: The patch was...
bypassed, and Microsoft patched it again.**



UK ran fake DDoS-for-hire sites

UK's National Crime Agency publishes that they set up a number of fake DDoS-for-hire sites to infiltrate the online criminal underground

MAR
17

Owner BreachForums arrested

An 'underground' forum used to buy and sell stolen data (or release them for free)

Owner was a 20-year-old
Law enforcement got their hands on a chat between the owner and someone who leaked data: why is this e-mail address not in this leak because on HaveIBeenPwned it is. It's myfirstname.lastname2002@gmail.com

He plead guilty and the maximum penalty is 40 years of imprisonment

MAR
24

Make love not war

Ukrainian hackers send surprise
delivery of 25 000 EUR

APR
3



Ukrainian hackers hacked into the account of a Z-volunteer who was raising money for the Russian army and ordered sex toys

The money was supposed to be used to buy drones

[Цей матеріал також доступний українською](#)

3 APRIL 2023, 18:05

5041 VIEW



“

This legend deserves a monument.
A giant butt plug must be erected
in his honour.

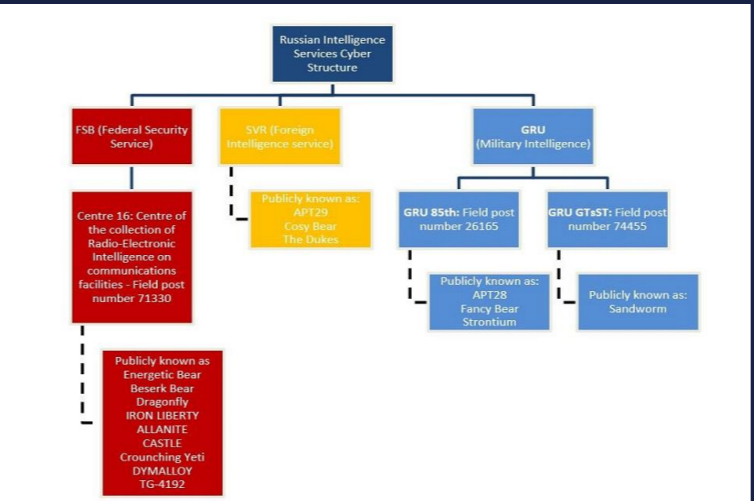
”

**- GooseTheSluice,
Some random guy on Reddit -**

MAY
09

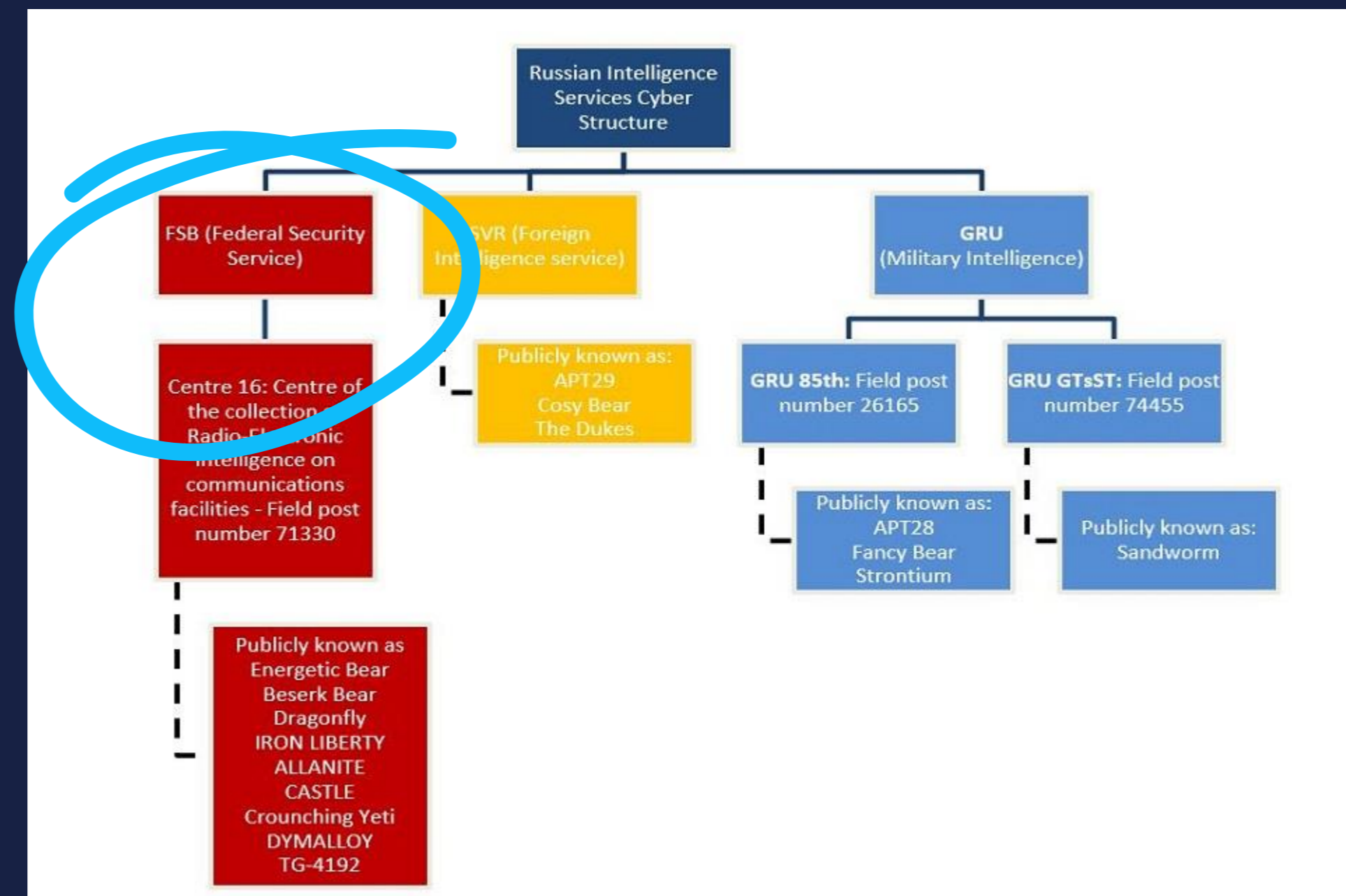
Snake takedown

Snake was “the most sophisticated cyber espionage tool”
Operated by Center 16 of the FSB



Barracuda zero-day

May
23

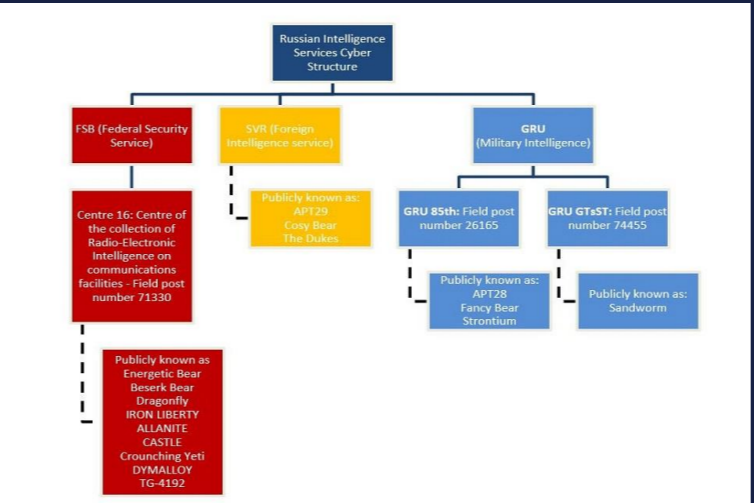


Source: gov.uk

MAY
09

Snake takedown

Snake was “the most sophisticated cyber espionage tool”
Operated by Center 16 of the FSB



Barracuda zero-day

May
23



Ten days later

The company revealed that the zero-day exploit had been used in attacks for at least seven months



Source: Bleepingcomputer



May 23

Barracuda announces that a zero-day vulnerability in the Barracuda Email Security Gateway (ESG) has been exploited in the wild.

One week later

Barracuda says all hacked appliances must be replaced immediately, even those already patched.

What happened? After Barracuda released the patches, the Chinese APT started using totally new malware to be more persistent. The hacker anticipated being caught!



UNC4841

Hackers gonna hack

Also, a prediction

Barracuda urges to replace the ESGs.

Throw it out and get a new one. Many companies will say: Throw it out. And don't get a new one.



June 15

Mandiant discovered that Chinese state-sponsored APT UNC4841 was behind it.

UNCategorized because Mandiant doesn't know yet which Chinese APT is really behind it

Future prediction

This will not stop.

Mandiant: "It is likely that we will continue to observe Chinese cyber espionage operations targeting edge infrastructure with zero-day vulnerabilities".



STATE-SPONSORED APTs

Just try and stop me

ClOp

...and the
Massive MOVEit Massacre

June
1



Cl0p

Ransomware gang

= Russian based TA505. Active since 2014. One of the most prolific cybercrime organizations in the world.

CISA estimates they have compromised more than 8,000 organizations worldwide.



Dec 2020

Cl0p breached up to 100 companies using a RCE zero-day in Accellion's File Transfer Appliance



July 2021

Cl0p exploited SolarWinds Serv-U file transfer servers with a zero-day



Jan 2023

Zero-day attack on GoAnywhere Managed File Transfer servers. The group claimed to have exfiltrated data from approximately 130 victims over the course of 10 days.



Never change a winning formula

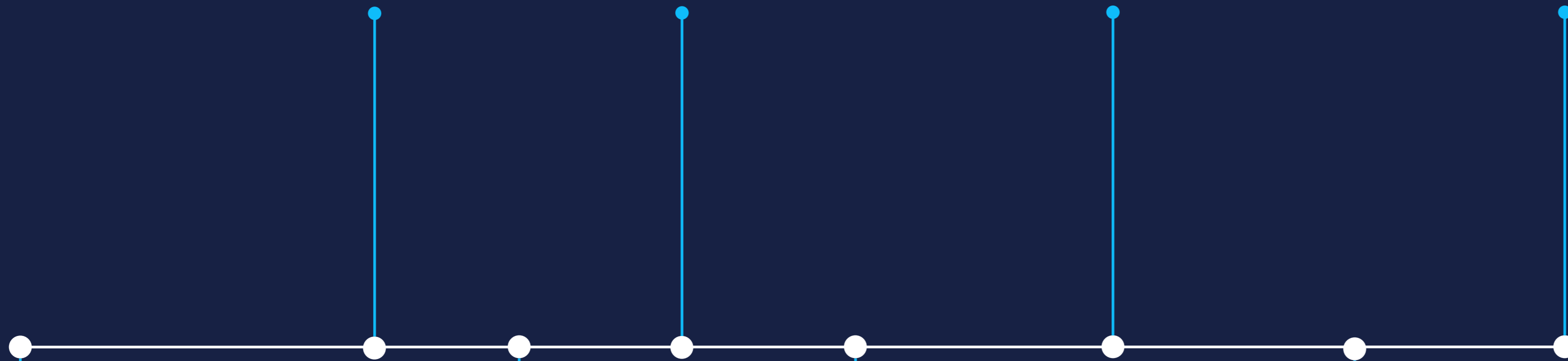
Trend to buy zero-days to mass exploit internet-facing servers, also for ransomware

“

Turns out letting ransomware groups make hundreds of millions to reinvest in exploits is a bad idea.

”

- **Kevin Beaumont @GossiTheDog** -



**June 01,
2023**

Zero-day attack on MOVEit Transfer.

Used by thousands of governments, financial institutions and so on.

Scanning started in March.



July

Coveware estimates CIOp earns between 75 and 100 million dollars with this Massive MOVEit Massacre

July

EMSISOFT: more than 2000 organizations have been impacted

Organization	Individuals
Maximus	11 million
Louisiana Office of Motor Vehicles	6 million
Alogent	4.5 million
Colorado Department of Health Care Policy and Financing	4 million
Oregon Department of Transportation	3.5 million
Teachers Insurance and Annuity Association of America	2.6 million
Genworth	2.5 million
PH Tech	1.7 million
Milliman Solutions	1.2 million
Wilton Reassurance Company	1.2 million



“

CI0p stole personal data of
56 million individuals

”

- *Emsisoft* -

santat7kpllt6iyvqbr7q4amd6dzrh6paatvyrz17ry3zm72zigf4ad.onion



DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.

STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM

STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE

UNTIL JUNE 12



FILES PART1

https://	/1.zip
https://	1.z01
https://	1.z02
https://	1.z03
https://	1.z04
https://	1.z05
https://	1.z06
https://	1.z07
https://	1.z08
https://	1.z09
https://	1.z10
https://	1.z11
https://	1.z12
https://	1.z13
https://	1.z14
https://	1.z15
https://	1.z16
https://	1.z17
https://	1.z18

Source: BleepingComputer

Company	Logo	Magnet
gripa.org		FULL FILES magnet:2x
jti.com		FULL FILES magnet:2x
voss.net		FULL FILES magnet:2x
ufcu.org		FULL FILES magnet:2x
yakult.com.ph		FULL FILES magnet:2x
rochester.edu		FULL FILES magnet:2x
discovery.com		FULL FILES magnet:2x
motherjones.com		FULL FILES magnet:2x
slb.com		FULL FILES magnet:2x
amc.theatres.com		FULL FILES magnet:2x



June
13

Fortinet

5 zero-days in total since last Brucon

10 Okt

CVE-2022-40684: Fortinet firewalls & FortiProxy authentication bypass in admin interface. 3 days later actively exploited in the wild. Again 3 days later PoC exploit public.

By Chinese APTs & Iranian state-sponsored APTs

Feb 16

CVE-2022-39952: RCE in FortiNAC in Feb 2023

June 13

CVE-2023-27997 RCE in SSL-VPN



Exploited by Chinese state-sponsored APT 'Volt Typhoon'

March 7

CVE-2022-41328: authenticated RCE in CLI Fortinet firewalls and FortiProxy in March 2023

Exploited by Chinese state-sponsored APT UNC3886, again

Dec 12

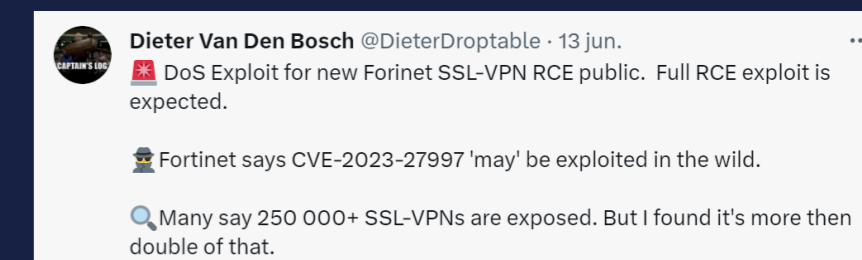
CVE-2022-42475: RCE in Fortinet SSL-VPN servers

Other exploited vulnerabilities:

CVE-2018-13379: 500 000 SSL-VPN credentials stolen and leaked for free

CVE-2018-13382: Change the SSL-VPN password

CVE-2020-12812: Bypass 2FA





RCE IN INTERNET-FACING SERVICE

Why is it, when something happens, it is always you three?



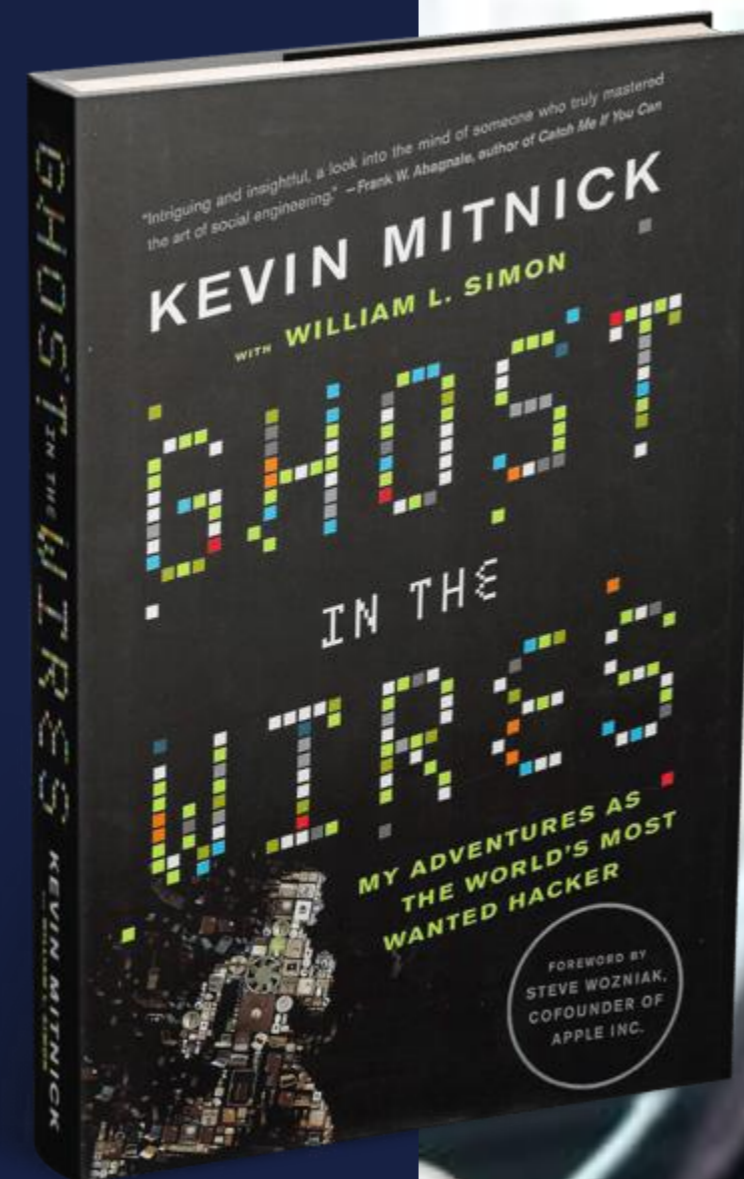
FORTINET CITRIX

MS EXCHANGE

imgflip.com

KEVIN MITNICK

† 6 augustus 1963 - 16 July 2023



Compromised Microsoft Keys

Chinese cyber-espionage group Storm-0558 found the signing keys in a crash dump

JUL
12

Ivanti Mobile Iron zero-day

Who needs authentication for your admin-API anyway?

JUL
25

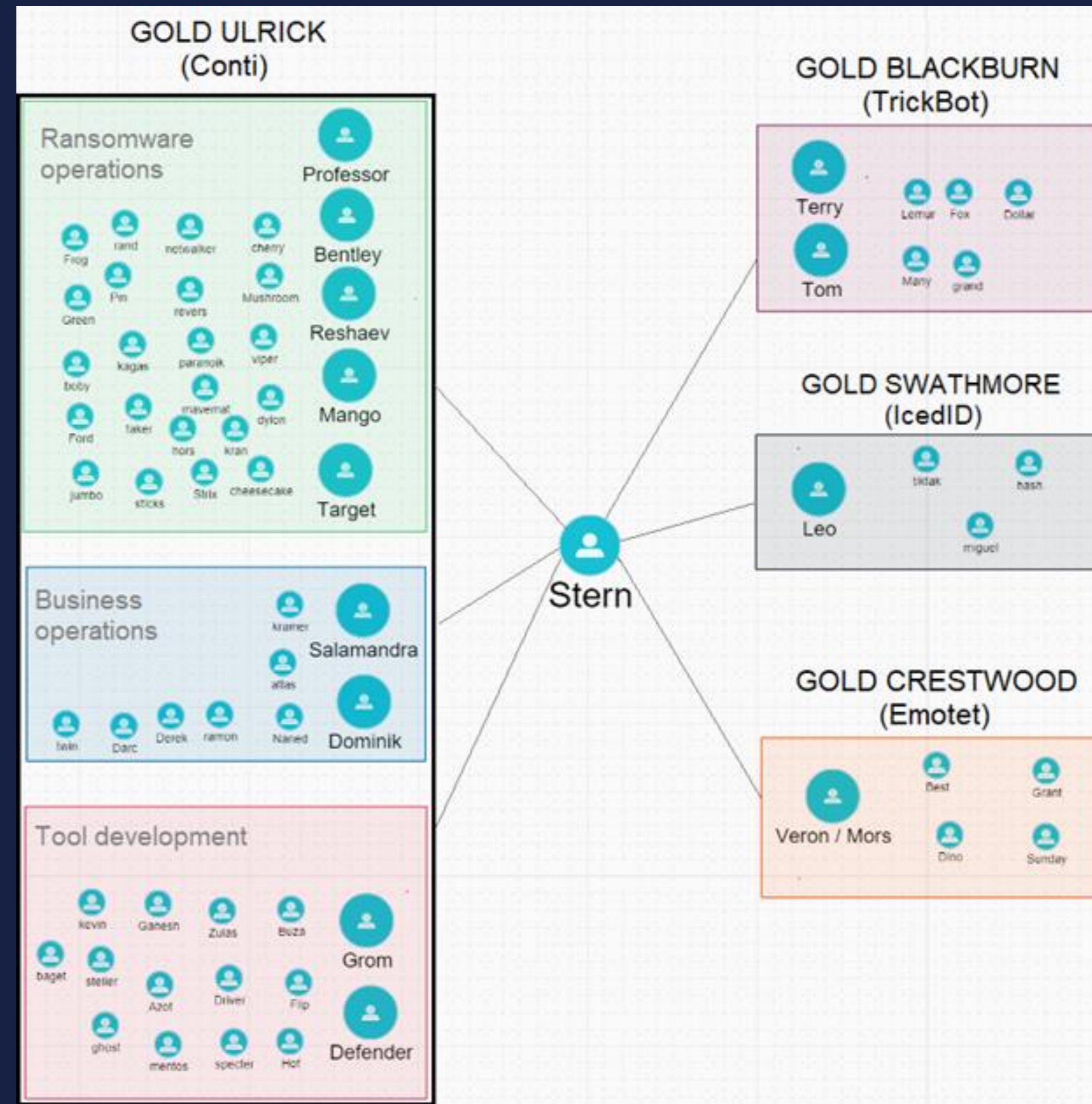
TrickBot/Conti/Wizard Spider

US and the UK sactioned this year 18 individuals of the Russia-based Trickbot/Conti group

The Trickbot crew one of the biggest cybercrime gangs companies in the world

SEP
7





Source: Secureworks

**WHEN YOU SEE HOW SOPHISTICATED
CYBERTHREATS HAVE BECOME**



imgflip.com

A large graphic consisting of a circle formed by many concentric, slightly irregular blue lines, with a vertical blue line passing through the center from the top edge of the frame.

BruCON 2023

The End

Thanks!
Questions?



THREAT EXPOSURE

We manage your attack surface

 threatexposure.eu/brucon.pdf

 dieter.vandenbosch@threatexposure.eu

 [@Threat_Exposure](https://twitter.com/Threat_Exposure) (**Twitter/X**)

 [@Threat_Exposure@infosec.exchange](https://infosec.exchange/@Threat_Exposure) (**Mastadon**)