Microsoft Digital Defence Report

With Jeff Beckitt

Powered by Microsoft

Microsoft Digital Defense Report

https://aka.ms/mddr

Microsoft Digital Defense Report Overview - 2023

Executive Summary - MDDR 2023

Full Report - MDDR 2023

Microsoft Security

Microsoft Security Community
The 2023 Microsoft Digital Defense Report

We will start at **1-2 minutes after** the scheduled time to accommodate those still connecting.

Questions? Feel free to type them in the instant message window (**Live event Q&A**) at any time.

Note that any questions you post will be public. You have the option to post questions anonymously.

This webinar is being **recorded**. Recordings will be posted after the session ends at https://aka.ms/SecurityCommunity, located under the **Videos & Webinar Recordings** section.

Closed captions are available during the session, including the recordings. During the live broadcasting you can enable the closed captions by pressing the "**Cc**" button and selecting from the available languages.

Please submit your **feedback** on this webinar session at https://aka.ms/SecurityWebinarFeedback.

Join our Community: https://aka.ms/SecurityCommunity.

MDDR – Report Chapters

Introduction

The State of Cybercrime

Nation State Threats

Critical Cybersecurity Challenges

Innovating for Security and Resilience

Collective Defense

Opportunities for nations to further improve its cyber defenses

1. Defend with the power and scale of the cloud
2. Apply Zero Trust principles
3. Use extended detection and response and antimalware
4. Make cybersecurity a core priority for central government bodies and agencies
5. Leverage external partners to enhance societal resilience to combat current and emerging influence actors and threats

65 trillion
signals synthesized

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
attacks blocked per second

4,000 identity authentication threats blocked per second.

15,000+
partners

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

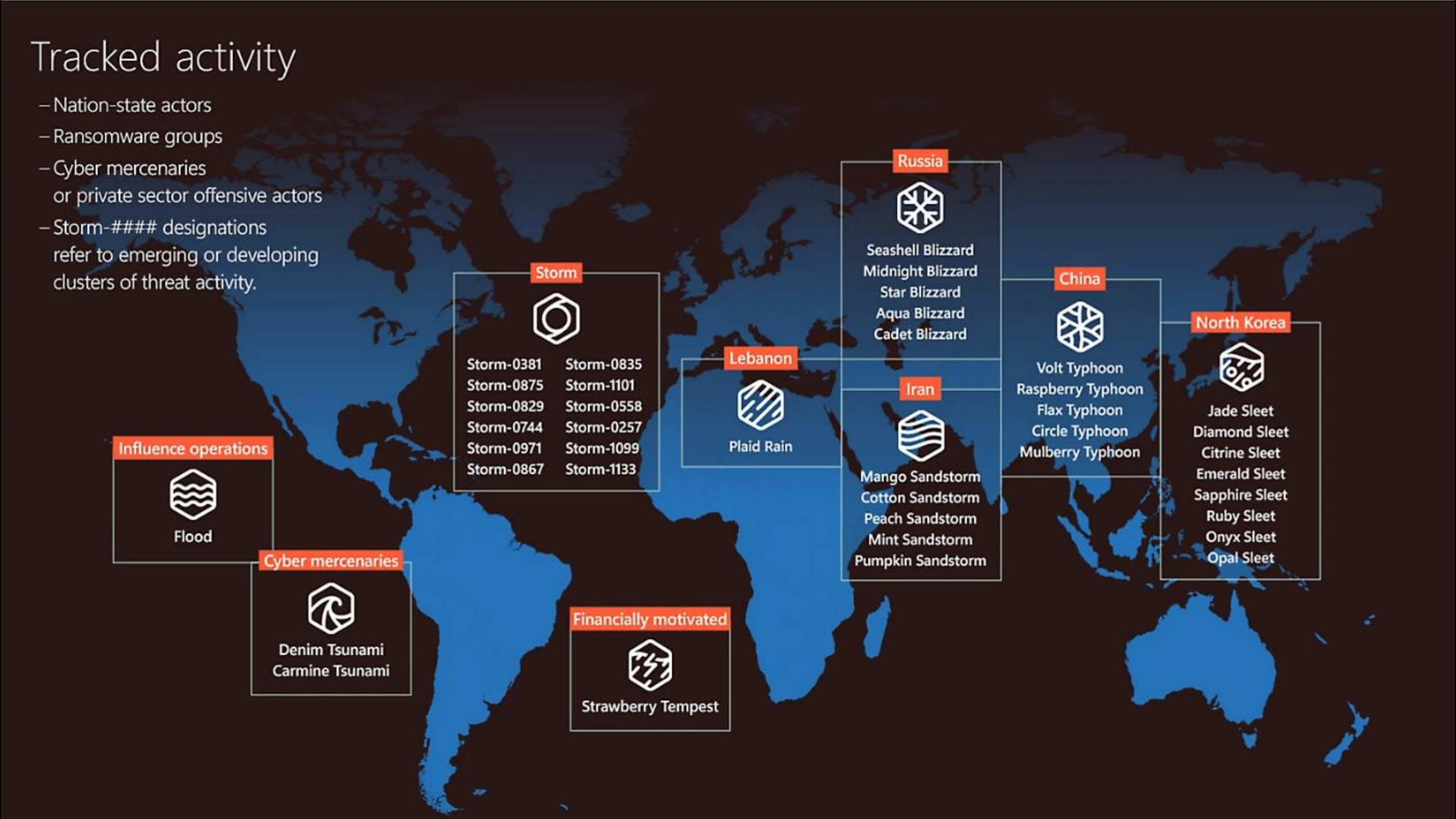
100,000+ domains utilized by cybercriminals, including over 600 employed by nation-state threat actors, have been removed (all time).

135 million
managed devices

135 million managed devices providing security and threat landscape insights.

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.



The State of **Cybercrime**

Key developments

80-90%

of all successful ransomware compromises originate through unmanaged devices.

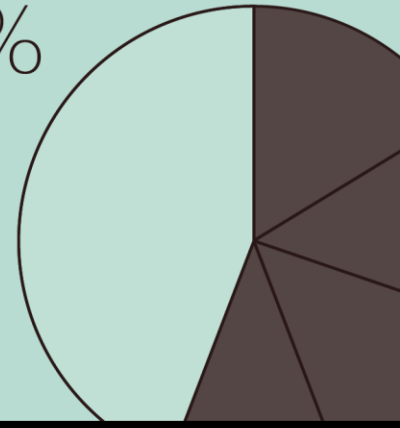
A return on mitigation (ROM) framework is helpful for prioritization and may highlight actions requiring low effort or resources but that have a high impact.

70%

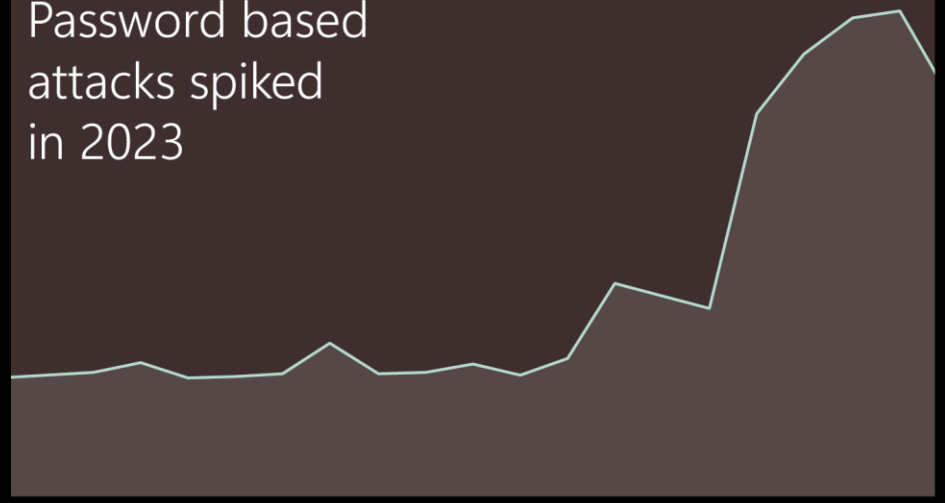
of organizations encountering human-operated ransomware had fewer than 500 employees.

Human-operated ransomware attacks are up more than

200%



Password based attacks spiked in 2023



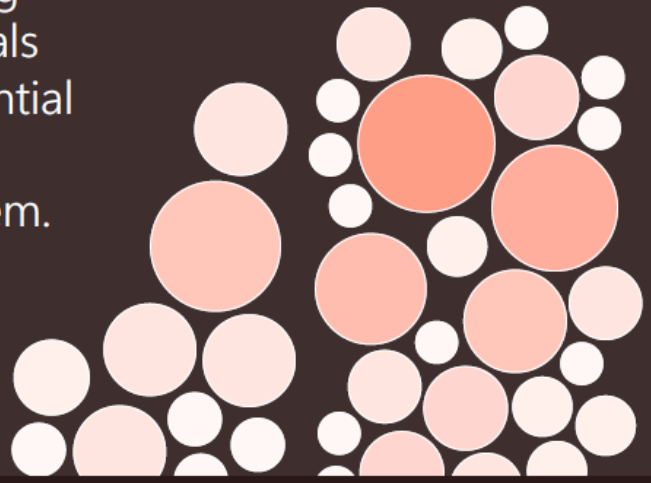
Last year marked a significant shift in cybercriminal tactics

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.

Innovating for Security and Resilience

Key developments

With modern AI advancements analyzing trillions of security signals daily, we have the potential to build a safer, more resilient online ecosystem.



Find out more on page 106

Our approach for the next year will focus on bringing to bear AI in combating threats while also embracing the three SDL principles of Secure by Design, Secure by Default, and Secure in Deployment (SD3).

Find out more on page 99

LLMs have the potential to transform cyber defense for next-gen cybersecurity.

Microsoft's researchers and applied scientists are exploring many scenarios for LLM application in cyber defense.

Find out more on page 101

Many modern apps will become LLM-based in time.

This will increase the threat surface, making them vulnerable to both inadvertent and deliberate misalignments. As LLM-based apps bring new and unique threats, we adapt our security measures and protocols to address them.

Find out more on page 104

Three key lessons

Innovation

We need to use the latest innovations, such as AI, to supercharge our cyber defense.

Partnerships

We need to work together with all stakeholders – be they public or private.

Skills

According to LinkedIn data, EU cyber skills demand is up by 22%. A clear skills gap is here.

How can we protect against 99% of attacks?

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.

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 XDR and MFA are constantly updated with trillions of daily signals, providing dynamic protection that adjusts to the current threat landscape.

Thank You

the lowdown

1st Nov 2023 Session #172

Powered by Microsoft