Microsoft

Identity
Is the New Battleground

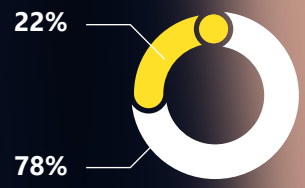
Cyber Signals

Identity is the new battleground, but most are unprotected against attacks

83

Million attacks

11/26 to 12/31 commercial/ enterprise customers



- **22%** of Azure Active Directory with strong authentication
- **78%** of Azure Active Directory without strong authentication

Introduction

Dangerous mismatch in scale of identity-focused attacks vs. preparedness

Digital identity takes many forms. For most of us, it's the email address and different passwords we use to access apps and services online. This is the currency threat actors use to penetrate networks, steal credentials, and impersonate employees and consumers in the digital world.

We are All Cybersecurity Defenders

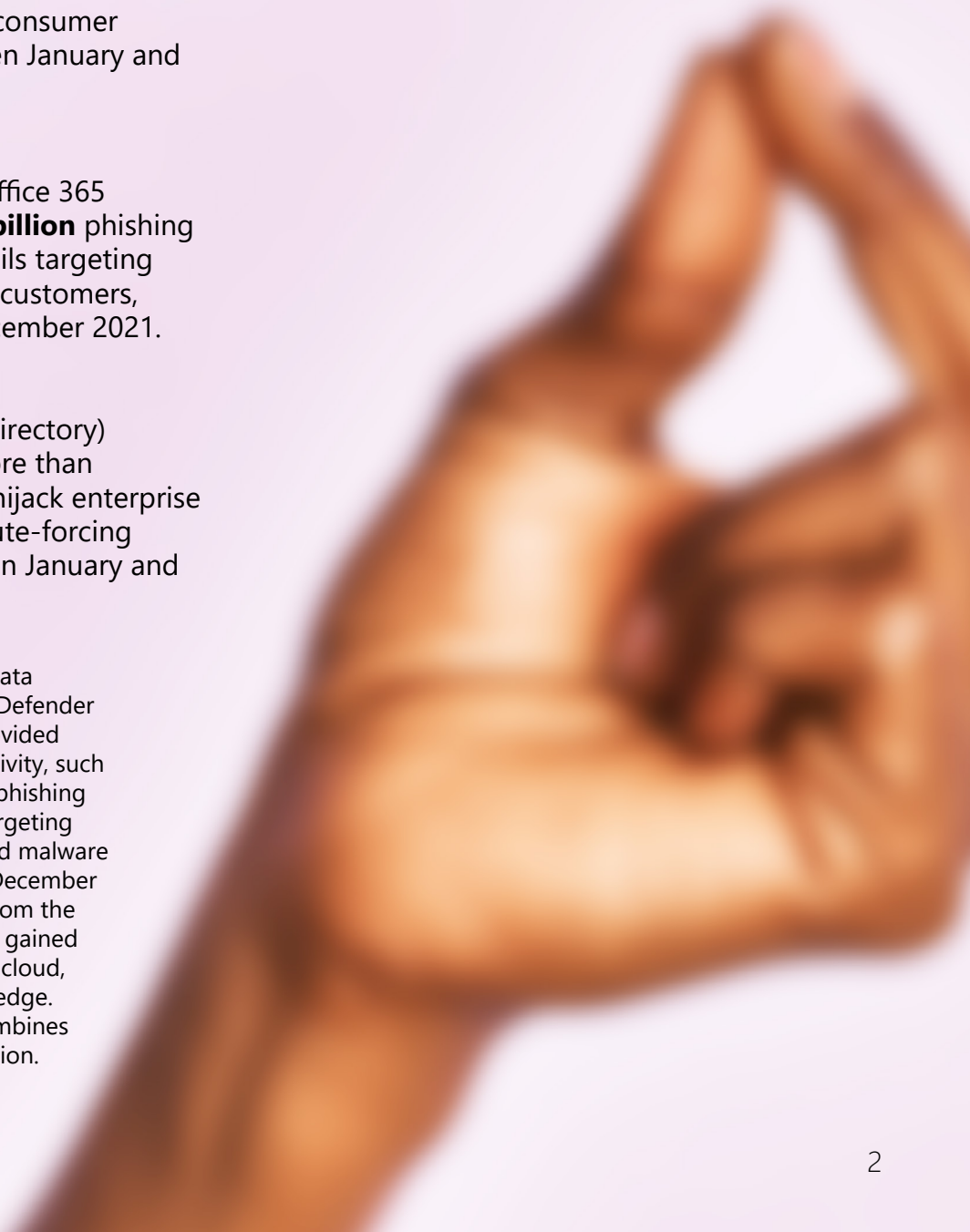
Security snapshot

Endpoint threats:
Microsoft Defender for Endpoint blocked more than **9.6 billion** malware threats targeting enterprise and consumer customer devices, between January and December 2021.

E-mail threats:
Microsoft Defender for Office 365 blocked more than **35.7 billion** phishing and other malicious e-mails targeting enterprise and consumer customers, between January and December 2021.

Identity threats:
Microsoft (Azure Active Directory) detected and blocked more than **25.6 billion** attempts to hijack enterprise customer accounts by brute-forcing stolen passwords, between January and December 2021.

Methodology: For snapshot data Microsoft platforms including Defender and Azure Active Directory provided anonymized data on threat activity, such as brute force login attempts, phishing and other malicious e-mails targeting enterprises and consumers, and malware attacks between January and December 2021. Additional insights are from the 24 trillion daily security signals gained across Microsoft including the cloud, endpoints, and the intelligent edge. Strong authentication data combines MFA and passwordless protection.



Nation-state actors redouble efforts to simply grab identity building blocks

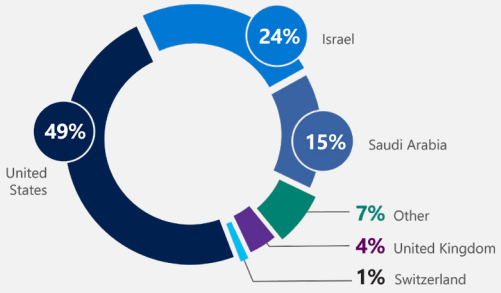
Cyberattacks by nation-state actors are on the rise. Despite their vast resources, these adversaries often rely on simple tactics to steal easily guessed passwords. By so doing, they can gain fast and easy access to customer accounts. In the case of enterprise attacks, penetrating an organization's network allows nation-state actors to gain a foothold they can use to move either vertically, across similar users and resources, or horizontally, gaining access to more valuable credentials and resources.

Spear-phishing, social engineering attacks, and large-scale password sprays are basic nation-state actor tactics used to steal or guess passwords. Microsoft gains insight into attackers' tradecraft and successes by observing what tactics and techniques they invest in and find success with. If user credentials are poorly managed or left vulnerable without crucial safeguards like multi-factor authentication (MFA) and passwordless features, nation-states will keep using the same simple tactics.

The need to enforce MFA adoption or go passwordless cannot be overstated, because the simplicity and low cost of identity-focused attacks make them convenient and effective for actors. While MFA is not the only identity and access management tool organizations should use, it can provide a powerful deterrent to attacks.

Abusing credentials is a fixture of NOBELIUM, a nation-state adversary linked to Russia. However, other adversaries, such as Iran-linked DEV 0343 rely on password sprays too. Activity from DEV-0343 has been observed across defense companies producing military-grade radars, drone technology, satellite systems, and emergency response communication systems. Further activity has targeted regional ports of entry in the Persian Gulf, and several maritime and cargo transportation companies with a business focus in the Middle East.

Iran: Most targeted countries
(July 2020-June 2021)



To see diagram at full size

Click here

Recommendations

Organizations should:

Enable multi-factor authentication: By so doing, they mitigate the risk of passwords falling into the wrong hands. Even better, eliminate passwords altogether by using passwordless MFA.

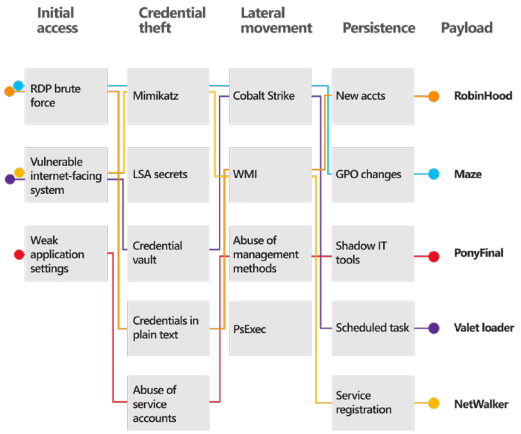
Audit account privileges: Privileged-access accounts, if hijacked, become a powerful weapon attackers can use to gain greater access to networks and resources. Security teams should audit access privileges frequently, using the principle of least-privilege granted to enable employees to get jobs done.

Review, harden, and monitor all tenant administrator accounts: Security teams should thoroughly review all tenant administrator users or accounts tied to delegated administrative privileges to verify the authenticity of users and activities. They should then disable or remove any unused delegated administrative privileges.

Establish and enforce a security baseline to reduce risk: Nation-states play the long game and have the funding, will, and scale to develop new attack strategies and techniques. Every network-hardening initiative delayed due to bandwidth or bureaucracy works in their favor. Security teams should prioritize implementing zero-trust practices like MFA and passwordless upgrades. They can begin with privileged accounts to gain protection quickly, then expand in incremental and continuous phases.

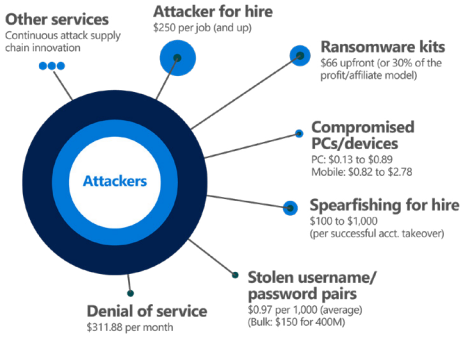
Ransomware dominates mindshare, but only a few strains dominate

The dominant narrative seems to be that there are massive numbers of novel ransomware threats outstripping defenders' capabilities. However, Microsoft analysis shows this is incorrect. There's also a perception that certain ransomware groups are a single monolithic entity, which is also incorrect. What exists is a cyber-criminal economy where different players in commoditized attack chains make deliberate choices. They are driven by an economic model to maximize profit based on how they each exploit the information they have access to. The graphic below shows how different groups profit from various cyberattack strategies and information from data breaches.



To see diagram at full size **Click here**

Average prices of cybercrime services for sale



To see diagram at full size **Click here**

That said, no matter how much ransomware is out there, or what strains are involved, it really comes down to three primary entrance vectors: remote desktop protocol (RDP) brute force, vulnerable internet-facing systems, and phishing. All of these vectors can be mitigated with proper password protection, identity management, and software updates in addition to a comprehensive security and compliance toolset. A type of ransomware can only become prolific when it gains access to credentials and the ability to spread. From there, even if it is a known strain, it can do a lot of damage.

Recommendations

Security teams should:

Understand that ransomware thrives on default or compromised credentials: As a result, security teams should accelerate safeguards like implementing passwordless or MFA on all user accounts and prioritizing executive, administrator and other privileged roles.

Identify how to spot telltale anomalies in time to act: Early logins, file movement, and other behaviors that introduce ransomware can seem nondescript. Nonetheless, teams need to monitor for anomalies and act on them swiftly.

Have a ransomware response plan and conduct recovery exercises: We live in the era of cloud sync-and-share, but data copies are different from entire IT systems and databases. Teams should visualize and practice what full restorations look like.

Manage alerts and move fast on mitigation: While everyone fears ransomware attacks, security teams' primary focus should be on strengthening weak security configurations that allow the attack to succeed. They should manage security configurations so alerts and detections are being responded to properly.

The cybersecurity bell curve: Basic security hygeine still protects against 98% attacks

To see diagram at full size **Click here**

Expert Profile

Christopher Glyer:

Principal Threat Intelligence Lead at MSTIC

As Principal Threat Intelligence Lead with a focus on ransomware at the Microsoft Threat Intelligence Center (MSTIC), Christopher Glyer is part of the team that investigates how the most advanced threat actors access and exploit systems. For the inaugural edition of Cyber Signals, he shares his thoughts on identity and security.

The shift to the cloud makes identity one of the core components organizations must prioritize when implementing proactive security protections. Identity is also an early focus area in any security investigation related to possible intrusions.

"When an attacker gains access to someone's identity and then reuses that identity to access applications and data, organizations need to understand exactly how that identity was accessed, what applications were touched, and what was done within those applications," Glyer explains. "From a protection perspective, the number one thing you must do is prevent an identity from being stolen, abused, or misused. Preventing this from happening in the first place is critical."

Leading with identity-focused solutions including enforcing multifactor authentication (MFA), adopting passwordless solutions, and creating conditional access policies for all users dramatically improves protection for devices and data, particularly as hybrid work continues to create scenarios where remote access, user roles, and physical locations vary. These solutions help organizations better control access to business-critical information and identify potentially anomalous activity.

The point is to place a higher security premium on identity, which in turn lets you tighten access privileges linked to those stronger authentications, minimizing the risk of an unauthorized login having unchecked consequences, Glyer explains.

"Attackers are always raising the bar," Glyer adds. "Fortunately, there are a lot of tools organizations can leverage as they conduct tabletop or red team exercises that may reveal gaps or limitations in their identity and other security controls."

Glyer says a focus on finding weaknesses in identity is a common attack tactic shared by many threat actors, cybercriminals, and nation-state actors, alike.

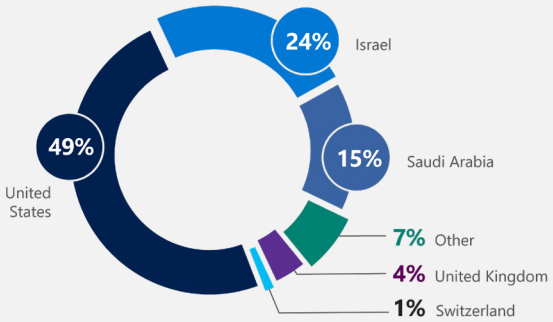
"If you look at a more macro trend over time, nation-states are going to leverage cyberattacks for espionage more frequently," he explains.

"I think you're going to see the number of players involved leveraging these capabilities continue to rise, because the intelligence gains are potentially quite large, versus the cost of executing these attacks. Having secure identity protections, whether it's MFA, passwordless, and other defenses like conditional access policies, minimize that opportunity and make it much harder to raise the attack bar. Securing those identities is key."

> **"From a protection perspective, the number one thing you must do is aim to prevent an identity from being stolen, abused, or misused. Preventing this from happening in the first place is critical."**
>
> Principal Threat Intelligence Lead at MSTIC
> **Christopher Glyer**

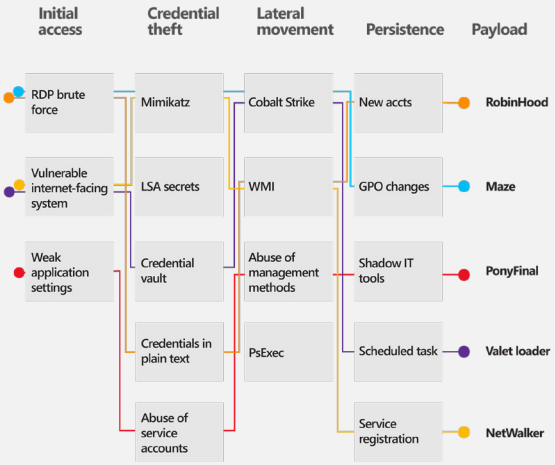
Appendix

Iran: Most targeted countries
(July 2020-June 2021)



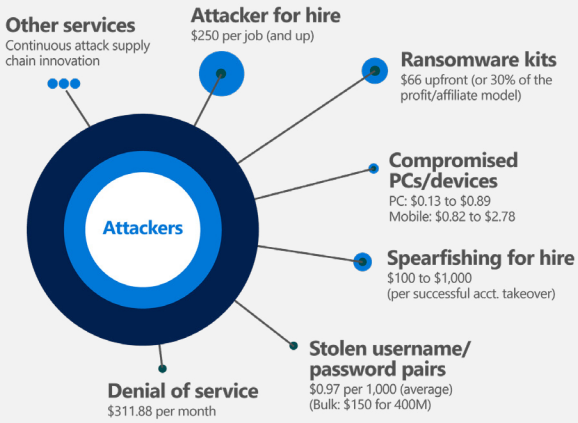
Click here to return to Threat Briefing page

Human-operated ransomware payloads



Click here to return to Defending Attacks page

Average prices of cybercrime services for sale



Click here to return to Defending Attacks page

The cybersecurity bell curve:
Basic security hygiene still protects against 98% of attacks

Click here to return to Defending Attacks page

Microsoft