Best practices Incident response Microsoft Incident Response
3 min read

Protecting credentials against social engineering: Cyberattack Series

By Microsoft Incident Response

December 4, 2023

Microsoft Security Experts

Our story begins with a customer whose help desk unwittingly assisted a threat actor posing as a credentialed employee. In this fourth report in our ongoing Cyberattack Series, we look at the steps taken to discover, understand, and respond to a credential phishing and smishing (text-based phishing) cyberattack that targeted a legitimate, highly-privileged user with social engineering—allowing the cyberattacker to impersonate the victim and weaponize a help desk to remove their multifactor authenticated device and register their own.

Highly privileged users at risk

Credential-based cyberattacks often begin with cyberthreat actors targeting individuals who they believe are connected to the people who have the credentials they need. Then they conduct social and dark web reconnaissance to find and wind their way to highly privileged users and gain enough information to impersonate them. In the past, cyberthreat actors have even been known to impersonate and masquerade as staff, including chief information security officers (CISOs) and other incident response firms. Cybercriminals use trust, context, and emotion to trick people with smishing links. At that point, they don't need to hack, they just log in. Many smishing and social engineering attacks employ a rush of push notifications that can overwhelm or confuse a target, causing multifactor authentication fatigue. Researchers believe the onslaught of notifications is causing us to get tired faster and lose focus, leaving us especially prone to distraction as the day wears on.[1] All the pings, clicks, swipes, buzzes, texts, and taps can weigh on a target, causing them to believe an access attempt is legitimate. And cyberthreat actors don't let up. By the end of June 2023, we observed approximately 6,000 multifactor authentication fatigue attempts—per day—every day.[2]

Untangling the tentacles of a cyberattack

In the case of threat actor Octo Tempest, once they gained access, they began wrapping their tentacles around valuable assets and collecting additional credentials by using third-party credential-harvesting tools against cloud and on-premises assets. They searched through the customer's SharePoint and email system for sensitive information about IT processes and VPN architecture. Then they modified the normal authentication flow, which allowed them to authenticate as any user in the organization, without requiring their credentials.

In this report, we examine the factors contributing to the cyberthreat actor's initial incursion and explore what could have happened without prompt tactical mitigation efforts. We walk through mitigation efforts step by step. Then we examine Octo Tempest's tactics, techniques, and procedures (TTPs) to understand the extent of the compromise and how we were able to help the customer evict the cyberthreat actor completely. We'll also explore how organizations can educate employees to reduce the chance of social engineering attacks, and share five proactive elements of a Zero Trust approach that can protect against highly motivated, tenacious cyberthreat actors like Octo Tempest.

Preventing cyberattacks

Many cyberattacks can be prevented—or at least made more difficult to execute—through the implementation and maintenance of basic security controls. Organizations can strengthen their cybersecurity defenses and better protect against cyberattacks by understanding in-depth the tentacles of a far-reaching credential breach like this one. Microsoft Incident Response can provide expert guidance to customers when an attack becomes too complex and challenging to mitigate alone—and before an attack happens—to develop a comprehensive incident response plan and ensure security personnel are trained to recognize and respond to social engineering attacks. With Microsoft's intelligence-driven incident response, customers can access the help they need on a global scale with global incident response, all day, every day—both on-site and remotely. The proactive and reactive incident response services let customers take advantage of the depth and breadth of Microsoft Threat Intelligence and gain unique access to product engineering. It also means customers can benefit from the longstanding Microsoft partnerships with government agencies and global security organizations for the latest, most comprehensive intelligence available. **Read the report** to learn more about the cyberattack, including the response activity, and lessons that other organizations can learn to avoid being caught in the tentacles of a social engineering compromise.

What is the Cyberattack Series?

With this Cyberattack Series, customers will discover how Microsoft incident responders investigate unique and notable exploits. For each cyberattack story, we will share:

- How the cyberattack happened.
- How the breach was discovered.
- Microsoft's investigation and eviction of the cyberthreat actor.
- Strategies to avoid similar cyberattacks.

Read the first blog in the Cyberattack Series, Solving one of NOBELIUM's most novel attacks.

Microsoft Incident Response

Strengthen your security with an end-to-end portfolio of proactive and reactive incident response services.

Explore services ›

Learn more

To learn more about Microsoft Incident Response, visit our website or reach out to your Microsoft account manager or Premier Support contact. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and Twitter (@MSFTSecurity) for the latest news and updates on cybersecurity.

[1] Phone Notifications Are Messing With Your Brain, Discover Magazine. April 29, 2022.

[2] Microsoft Digital Defense Report 2023

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social

What's new

Surface Laptop Studio 2

Surface Laptop Go 3

Surface Pro 9

Surface Laptop 5

Microsoft Copilot

Copilot in Windows

Explore Microsoft products

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy

Sitemap Contact Microsoft Privacy Terms of use Trademarks Safety & eco Recycling About our ads © Microsoft 2024