burhani | THE MICROSOFT CLOUD EXPERTS

Detect and disrupt in-progress cyberattacks automatically

Microsoft

Cybersecurity attacks are getting more common and targeted. They're also accelerating; attacks that used to take months now take days. And even the most advanced security operations teams need to take breaks to keep their organizations protected. Our cyber security experts can help you stay ahead of evolving threats.

The threats are real

Ransomware attacks
Commodity and human-operated

<20 minutes from deployment to mitigate the attack.

Business Email Compromise (BEC) attacks
Attackers pose as a trusted figure and asks recipients for payment or to share sensitive info

81% between the first and second half of 2022[1]

Adversary-in-the Middle (AitM)
An unauthorized party intercepts communication between two systems or people

$100 or less the cost of an AitM kit, which lowers the tooling and skills required to launch an attack.[2]

Protect your business with automatic attack disruption

"What if you could detect and disrupt an in-progress attack automatically and dramatically reduce the overall impact? As a trusted technology partner with experience in security, we can help you get this capability with extended detection and response (XDR) from Microsoft.

- Security signals from many different sources
- Identify affected assets
- Disrupt the attack in real time

Why we recommend Microsoft Defender XDR

Microsoft analyzes 65 trillion signals analyzed daily and correlates them in real time across attack surfaces.[3] This threat intelligence powers automatic attack disruption in Microsoft Defender XDR.

The anatomy of a real-life BEC attack

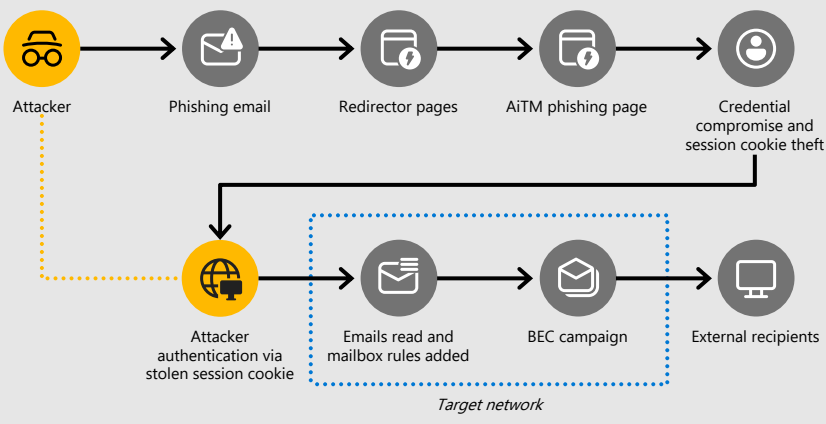
Microsoft 365 Defender used a combination of signals from identity and email security solutions—such as unfamiliar sign-in, inbox rule creation, and sending and deletion of emails—to identify the BEC attack and detect the fraud attempt. Having established a high level of confidence through the combination of signals and alerts, Microsoft's XDR-automated actions then disabled the user account and disrupted the attack within three hours. It prevented follow-up conversations and preventing the wire instructions from being acted upon.

BEC ATTACK CHAIN

- **2:00 PM** — Sign-in with stolen cookie with MFA claim
- **2:00 PM - 4:00 PM** — Mailbox search for interesting email threads
- **4:00 PM** — Registration of homoglyph domains: one looks like target org's domain name, another impersonates domain of partner org
- **4:05 PM** — Creation of inbox rule that moves emails from partner org to "Conversation History" folder
- **4:06 PM** — Conversation hijack: mail sent to business partner org with wire transfer instruction change
- **4:07 PM** — Deletion of sent email
- **4:27 PM** — User account disabled
- **5:05 PM** — Email reply asking for clarifications regarding wire transfer instruction change; mail not accessible to the attacker

Automatic attack disruption is a powerful, out-of-the-box capability that can automatically stop the progression of some of the most targeted attacks.

Automatic disruption: AitM attacks



The goal of automatic disruption is to contain the attack as early as possible.

1. Identify with high confidence an AiTM attack based on multiple correlated Microsoft 365 Defender signals.
2. Automatically disable the compromised user account.
3. Automatically revoke the stolen session cookie to prevent additional malicious activity.
4. Leave the SOC in full control of remediation.

Contact us for more details

By 2025, 60% of organizations will be actively using remote threat disruption and containment capabilities delivered.[4] We want to help you be one of them. As a Microsoft partner and trusted technology advisor to many businesses like yours, we have the knowledge and expertise to get you started—as well as a variety of services and offerings that can help you stay ahead of cybercrime. Whether you need an assessment, help with licensing, or managed services, we can implement the security solution your company needs.

Reach out today

Burhani Managed Services | sales@burhani.co | www.burhani.co

1. Abnormal, "H1 2023: "Read " Alert, 2023.
2. Microsoft, "DEV-1101 enables high volume AiTM campaigns with open-source phishing kit," March 13, 2023
3. Microsoft, "Microsoft Security reaches another milestone," January 25, 2023.
4. Gartner®, Market Guide for Managed Detection and Response Services, 14 February 2023