

Monthly news - July 2023

 techcommunity.microsoft.com/t5/microsoft-365-defender-blog/monthly-news-july-2023/ba-p/3860740









Microsoft 365 Defender

Monthly news
July 2023 Edition



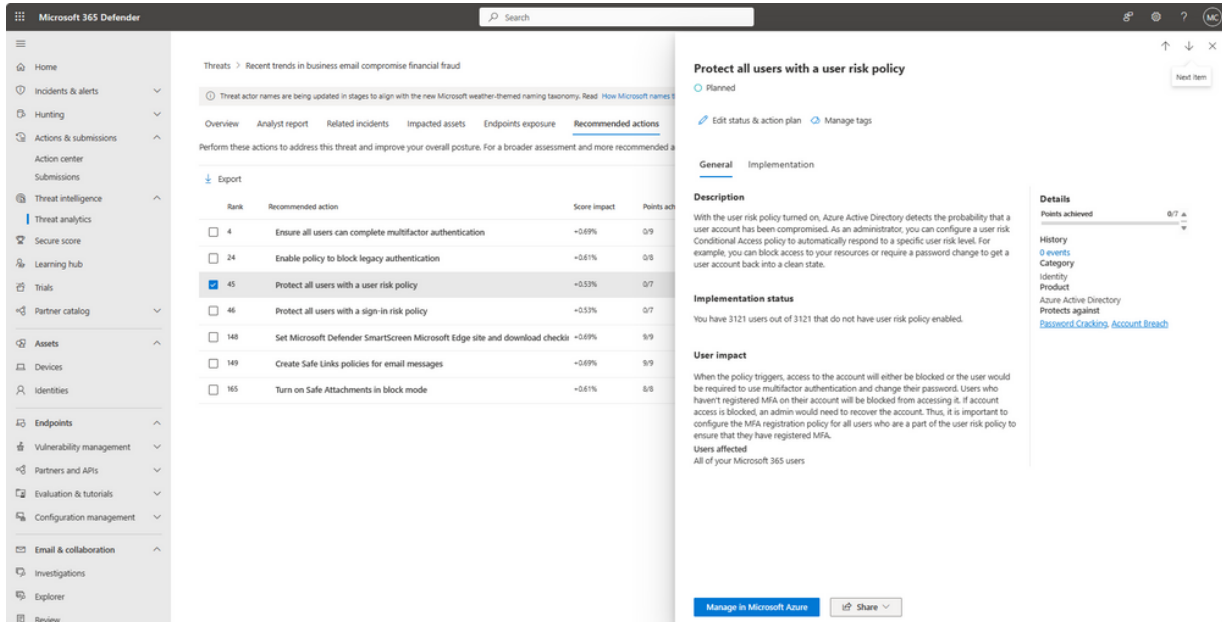
This is our monthly "What's new" blog post, summarizing product updates and various new assets we released over the past month across our Defender products. In this edition, we are looking at all the goodness from June 2023.

Legend:

 Product videos	 Webcast (recordings)	 Docs on Microsoft	 Blogs on Microsoft
 GitHub	 External	 Product improvements	 Previews / Announcements

Microsoft 365 Defender

Prevent repeat attacks with threat-informed security posture recommendations. Microsoft 365 Defender now makes it easy for security operations (SOC) teams to identify and prioritize the right controls with the general availability of threat-informed security posture recommendations.



Share your feedback on Microsoft 365 Defender via the new feedback portal. We're excited to announce that Microsoft 365 Defender is now part of the new community feedback experience, and our customers now have a dedicated platform to submit their suggestions and feature requests for our security products.

Ninja Show Season 4 recap! In this season we had a special mini-series on incident response, with lots of demos on how to investigate incidents following playbooks. Check out [this summary](#) and let us know your favorite topic from this season or what you're looking forward to next!

A graphic for the 'Virtual Ninja Training' series. On the left, a grey cat character with a red headband and a blue patch on its chest sits on a yellow director's chair, giving a thumbs-up. The background features a large, faint Microsoft logo. To the right of the cat, the Microsoft logo is displayed above the text 'Microsoft 365 Defender', 'Virtual Ninja Training', and 'with Heike Ritter'. Below this, the text 'Season 4 Summary' is written in bold. At the bottom right, a grey button with a white double arrow icon contains the text 'Watch all episodes on-demand'.

Microsoft Defender for Endpoint

[Forcibly releasing devices from isolation](#) is now available for public preview. This new capability allows you to forcibly release devices from isolation, when isolated devices become unresponsive. For more information, see [Take response actions on a device in Microsoft Defender for Endpoint](#).

[New Monthly security summary](#). Gain insights into an organization's security posture and performance, as well as visualizing the team's effort in managing the environment.

Microsoft Defender for Cloud Apps

App governance is now included as part of the Defender for Cloud Apps licenses and no longer requires an add-on license. In the Microsoft 365 Defender portal, go to Settings > Cloud apps > App governance > Service status to either enable app governance if available, or sign up for the waitlist.

Webinar: [App Governance Inclusion in Defender for Cloud Apps Overview](#).

Safeguarding your OAuth apps with App Governance. Learn why App Governance is the essential layer of defence to protect your OAuth apps. [Learn how to enable it and start using in a couple of steps](#).

[Defender for Cloud Apps Operational Guide is ready to download](#) for your SOC and security teams to help with planning and performing security activities.

Update Defender for Cloud Apps IP addresses for reverse proxy infrastructure. We recently completed infrastructure enhancements which resulted in new IPs that need to be added for Defender for Cloud Apps proxy infrastructure. We recommend that customers review the network list for proxy and ensure these have been updated in their environments.

Enhanced hunting experience for OAuth app activities.

App governance now makes it easy for you to take hunting with app data to the next level by providing deeper OAuth app insights, helping your SOC identify an app's activities and the resources it has accessed.

OAuth app insights include:

- Out-of-the-box queries that help to streamline the investigation
- Visibility into the data using the results view
- The ability to include OAuth app data such as resource, app, user, and app activity details in custom detections.

For more information, see [Hunt for threats in app activities](#).

App hygiene update with Microsoft Entra. Starting June 1, 2023, management of unused apps, unused credentials, and expiring credentials will only be available to app governance customers with Microsoft Entra Workload Identities Premium. See [Secure apps with app hygiene features](#) and [What are workload identities?](#).

Microsoft Defender for Identity

Advanced hunting with an enhanced IdentityInfo table. For tenants with Defender for Identity deployed, the Microsoft 365 IdentityInfo advanced hunting table now includes more attributes per identity, as well as identities detected by the Defender for Identity sensor from your on-premises environment. For more information, see the [Microsoft 365 Defender advanced hunting documentation](#).

Webinar recording: [Become an Advisor to Our Product Engineering Team](#).

The Defender for Identity product engineering team is excited to share a program for customers to become trusted advisors and impact our feature planning. Engage directly with the engineering team, learn what's coming, test out private previews, and share your experiences and recommendations. Microsoft uses the program to put the customer at the center of product development and, ultimately, help us better secure your organization and your customers.

Microsoft Defender for IoT

On June 1, 2023, [Microsoft Defender for IoT moved to site-based licensing](#) for organizations looking to protect their operation technology (OT) environments. The previous Azure consumption model for this solution will no longer be available for purchase by new customers. Existing customers can choose to transition to site-based licensing or remain on the consumption model.

[IoT devices and Linux-based systems targeted by OpenSSH trojan campaign](#). Microsoft has uncovered an attack leveraging custom and open-source tools to target internet-facing IoT devices and Linux-based systems. The attack involves deploying a patched version of OpenSSH on affected devices to allow root login and the hijack of SSH credentials.

Microsoft Defender for Business

Streaming API for Defender for Business customers is now in public preview! We are delighted to announce that Microsoft Defender for Business now supports streaming events through Advanced Hunting! This means that Defender for Business customers can stream the data to Event Hubs, Azure, or local storage.

Blogs on Microsoft Security

Detecting and mitigating a multi-stage AiTM phishing and BEC campaign. Microsoft Defender Experts observed a multi-stage adversary-in-the-middle (AiTM) and business email compromise (BEC) attack targeting banking and financial services organizations over two days. This attack originated from a compromised trusted vendor, involved AiTM and BEC attacks across multiple supplier/partner organizations for financial fraud, and did not use a reverse proxy like typical AiTM attacks.

Cadet Blizzard emerges as a novel and distinct Russian threat actor. Microsoft attributes several campaigns to a distinct Russian state-sponsored threat actor tracked as Cadet Blizzard (DEV-0586), including the WhisperGate destructive attack, Ukrainian website defacements, and the hack-and-leak front “Free Civilian”.

Microsoft 365 Defender Threat Analytics reports (Portal access needed)

Detecting and mitigating a multi-stage AiTM phishing and BEC campaign. In April 2023 Microsoft Defender Experts uncovered a multi-stage adversary-in-the-middle (AiTM) phishing and business email compromise (BEC) attack against banking and financial services organizations. The attack originated from a compromised trusted vendor and showcases the complexity of AiTM and BEC threats which abuse trusted relationships between vendors, suppliers, and other partner organizations with the intent of financial fraud.

Technique profile: Antivirus tampering. One of the first steps many attackers take after the initial compromise of an organization is to identify and tamper with security solutions. By disabling or otherwise tampering with defenses, attackers gain time to install malicious tools, exfiltrate data for espionage or extortion, and potentially launch destructive attacks like ransomware.

Vulnerability profile: MOVEit Transfer zero-day exploitation (CVE-2023-34362). On May 31, 2023, Progress Software Corporation disclosed a critical SQL injection vulnerability (CVE-2023-34362) in their MOVEit Transfer application that could lead to unauthenticated access to the underlying database. Microsoft has observed active exploitation of the MOVEit Transfer vulnerabilities as early as May 27, 2023.

MediaArena potentially unwanted application detection surge. Microsoft observed an increasing number of detections for a new family of unwanted applications named MediaArena, a highly prevalent family of browser modifier applications that bypass a browser's supported extensibility model to change Microsoft Edge's default search provider.

Actor profile: Lace Tempest ransomware and extortion group. Lace Tempest (DEV-0950) is a cybercriminal group known to conduct ransomware operations. They target organizations across a diverse array of industries and have traditionally used phishing campaigns and exploited public-facing Serv-U FTP server vulnerabilities to obtain initial access. Recently, Microsoft observed activity originating from Raspberry Robin worm infections attributed to Lace Tempest.

Activity Profile: Peach Sandstorm uses sophisticated TTPs in a new campaign. Microsoft observed a resurgence of activity attributed to Peach Sandstorm, an Iran-based nation state actor. While the majority of activity Microsoft saw in this campaign can be characterized as reconnaissance, in March 2023, Microsoft identified a successful intrusion where Peach Sandstorm used a GoldenSAML attack to ultimately exfiltrate data from a compromised organization.

Actor profile: Cadet Blizzard. Cadet Blizzard (DEV-0586) is a Russian GRU-sponsored threat group that Microsoft began tracking following disruptive and destructive events occurring at multiple government agencies in Ukraine in mid-January 2022. Primary targeted sectors include government organizations and information technology providers in Ukraine, although organizations in Europe and Latin America have also been targeted.

Actor profile: Storm-0288 leverages handoffs from multiple actors to deploy ransomware. Storm-0288 (DEV-0288) is a financially-motivated cybercrime group known to use the malware families PUNCHBUGGY, BadHatch, and White Rabbit, among others. Identified operations have focused on point-of-sale compromise, data exfiltration, extortion, and ransomware deployment.

Actor profile: Storm-0396 operates LockBit ransomware as a service. Storm-0396 (DEV-0396) is a cybercriminal group known as the likely operators of LockBit ransomware as a service (RaaS). They manage the LockBit RaaS offerings, including LockBit 2.0, LockBit Black (aka LockBit 3.0), the recently discovered variant LockBit Green, and an ESXI variant to encrypt Linux servers. LockBit RaaS is one of the most prominent RaaS models and has historically impacted numerous organizations worldwide.

Activity profile: Storm-1359 launches distributed denial of service attacks. Microsoft has attributed distributed denial of service (DDoS) attacks in early June 2023 to the threat actor tracked as Storm-1359. These attacks against multiple Microsoft cloud services, including Microsoft 365 and Azure, likely rely on access to multiple virtual private servers (VPS) in conjunction with rented cloud infrastructure, open proxies, and DDoS tools.

Actor profile: Storm-0201. Storm-0201 (DEV-0201) is a criminal group that focuses on the development and distribution of the Emotet malware. They are known to primarily target organizations in opportunistic email attacks worldwide, and prior Storm-0201 infections have led to ransomware. Storm-0201 is tracked by other security companies as Mummy Spider and TA542.

Activity profile: Midnight Blizzard credential attacks. Since at least March 2023, Microsoft Threat Intelligence detected an increase in credential attacks and initial access operations utilizing residential proxy services conducted by the threat actor that Microsoft tracks as Midnight Blizzard. The credential attacks use a variety of password spray, brute force, and token theft techniques to gain access to target environments.

IoT devices and Linux-based systems targeted by OpenSSH trojan campaign. Microsoft researchers have recently discovered an attack leveraging custom and open-source tools to target internet-facing Linux-based systems and IoT devices. The attack uses a patched version of OpenSSH to take control of impacted devices and install cryptomining malware.

Tool profile: Greatness adversary-in-the-middle phishing-as-a-service platform. Greatness is a phishing-as-a-service (PhaaS) platform with adversary-in-the-middle (AiTM) capabilities that has been active since mid-2022 and is attributed to the threat that Microsoft tracks as Storm-1295 (DEV-1295).