Monthly news - November 2023

techcommunity.microsoft.com/t5/microsoft-365-defender-blog/monthly-news-november-2023/ba-p/3970796

Microsoft 365 Defender
Monthly news
November 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 October 2023.

Legend:

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

Microsoft 365 Defender

**<u>Operationalizing Microsoft Security Copilot to Reinvent SOC
Productivity</u>**. (Preview) Microsoft Security Copilot in Microsoft 365 Defender is now in
preview. Microsoft 365 Defender users can take advantage of Security Copilot
capabilities to summarize incidents, analyze scripts and codes, use guided responses
to resolve incidents, generate KQL queries, and create incident reports within the
portal. Security Copilot is on an invitation-only preview. Learn more about Security
Copilot in the Microsoft Security Copilot Early Access Program <u>Frequently Asked
Questions</u>.

Using advanced hunting to secure OAuth apps. In <u>this blog</u>, we'll demonstrate how
SOC teams can benefit from App governance and its integration with Advanced
Hunting to better secure SaaS apps.

(Preview) You can now **get email notifications for manual or automated actions**
done in Microsoft 365 Defender. Learn how to configure email notifications for manual
or automated response actions performed in the portal.

(Preview) **Exchange Online permission management** for Microsoft Defender for
Office 365 is **now supported in Microsoft 365 Defender Unified role-based access
control (RBAC)**. In addition to the existing support for scenarios that are controlled by
Exchange Online Protection (EOP) roles, configured in the Microsoft 365 Defender
portal (under Permissions > Email & collaboration roles), Microsoft 365 Defender
Unified RBAC now also supports the management of Exchange Online (EXO) roles
and permissions, which could previously only be managed in the Exchange Admin
Center. Learn more <u>in our documentation</u>.

The Virtual Ninja Show Season 6 is coming to help wrap up your 2023! We go
live November 6th – December 20th with tons of security features and tips to share
with you! Visit <u>the show site</u> (site will get updated Nov 2nd, please check back!) to see
all upcoming details and add events to your calendar.

Microsoft Security Experts

New FAQ for Defender Experts for XDR managed response.

Microsoft Defender for Endpoint

Automatic disruption of human-operated attacks through containment of compromised user accounts. One of the main powerful components of the automatic attack disruption capability is "User contain", which limits attacker activity using compromised accounts, regardless of their domain status. The control is triggered and applied automatically based on XDR signals indicating a human operated attack, and is deployed to endpoints in real-time.

Announcing a streamlined device connectivity experience for Microsoft Defender for Endpoint. This new experience makes it **easier for security teams to configure and manage Microsoft Defender for Endpoint services** by reducing the number of URLs required to connect to cloud services during onboarding, expanding network configuration options to support IPs, and simplifying post-deployment network management.

Updates:

10/9/2023 - The eBPF-based sensor for Defender for Endpoint on Linux is now generally available.

10/31/2023 - Device isolation and AV scan response actions for Defender for Endpoint on Linux and macOS are now generally available.

Microsoft Defender for Identity

Simplified deployment with Defender for Identity. In this blog we will show you the simple steps for deploying Microsoft Defender for Identity within your environment.

Microsoft Defender for Cloud Apps

Automatic redirection from Defender for Cloud Apps to Microsoft 365 Defender is generally available. **All users accessing Microsoft Defender for Cloud Apps will be automatically rerouted to the Microsoft 365 Defender portal**. Admins will still have the option to not automatically redirect their users. Learn more here.

Microsoft Defender for Office 365

Authenticate Outbound Email to Improve Deliverability. This blog explains how to set up email authentication for your domain, so you can ensure that your messages are less likely to be rejected or marked as spam by email providers like Gmail, Yahoo, AOL, Outlook.com.

Blogs on Microsoft Security

Defending new vectors: Threat actors attempt SQL Server to cloud lateral movement. The Microsoft Defender for Cloud research and development team recently identified a unique attack where attackers attempted to gain access to cloud environments through an SQL server. The attackers exploited an SQL injection vulnerability to access a Microsoft SQL server, which was deployed in an Azure Virtual Machine (VM), and attempted to perform lateral movement to additional cloud resources.

Multiple North Korean threat actors exploiting the TeamCity CVE-2023-42793 vulnerability. Since early October 2023, Microsoft has observed North Korean nation-state threat actors Diamond Sleet and Onyx Sleet exploiting the Jet Brains TeamCity CVE-2023-42793 remote-code execution vulnerability.

Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction. Microsoft Incident Response (Microsoft IR) has observed a recent uptake of novel tactics, techniques, and procedures (TTPs) used by threat actors to take advantage of misconfigurations in IaaS and PaaS workloads in Azure.

Threat Analytics Reports / Actor, activity & technique profiles (Portal access needed)

Threat overview: Cloud identity abuse. With more organizations moving to hybrid or cloud-only models, it is becoming increasingly important to secure both cloud resources as well as cloud identities. Cloud identity compromise was initially thought to be a technique reserved for only a handful of advanced actors in the past such as Midnight Blizzard with the Solar Winds supply chain compromise. However, other tracked actors including Peach Sandstorm, Storm-0219, and Octo Tempest have recently shown sophisticated competency in the cloud across a large variety of industry verticals.

Activity profile: Threat actors attempt SQL to cloud lateral movement. Microsoft security researchers recently identified an attack where attackers attempted to move laterally to a cloud environment through a SQL Server instance. This attack technique demonstrates an approach we've seen in other cloud services such as VMs and Kubernetes cluster, but not in SQL Server.

Vulnerability profile: WS_FTP Server critical vulnerabilities. Multiple vulnerabilities are impacting WS_FTP Server, a secure file transfer solution, according to a Progress Software advisory. Two of the identified vulnerabilities affecting versions prior to 8.7.4 and 8.8.2 are rated critical: CVE-2023-40044 and CVE-2023-42657. These vulnerabilities could allow an unauthenticated attacker to launch remote commands and perform file operations outside of their authorized folder path.

Vulnerability profile: Pre-authentication RCE chain on SharePoint Server 2019. On September 25, 2023 STAR Labs researcher Nguyễn Tiến Giang published a technical analysis describing a pre-authentication remote code execution exploit chain impacting vulnerable versions of SharePoint Server 2019.

Activity profile: Diamond Sleet compromises TeamCity servers. Diamond Sleet, a North Korean based threat actor, has compromised multiple servers running JetBrains TeamCity. The servers were likely compromised from the recently disclosed vulnerability CVE-2023-42793. Once Diamond Sleet successfully compromised the server, two payloads were downloaded from other infrastructure compromised earlier by Diamond Sleet. Microsoft also observed Diamond Sleet deploying files to the compromised servers that were used in dynamic link library (DLL) search-order hijacking attacks.

Actor profile: Storm-1575. The actor group Microsoft tracks as Storm-1575 is behind the development, support, and sale of a phishing-as-a-service (PhaaS) platform with adversary-in-the-middle (AiTM) capabilities. This platform, known as Dadsec, has been active since approximately May 5, 2023.

Actor profile: Pinstripe Lightning. The threat actor that Microsoft tracks as Pinstripe Lightning is a Gaza-based actor active as far back as 2015. Pinstripe Lightning is known to target Palestinian government agencies, universities, and pro-Fateh organizations in the West Bank.

Vulnerability profile: CVE-2023-41763 Skype for Business Elevation of Privilege vulnerability. Microsoft has released a patch for CVE-2023-41763, an elevation of privilege vulnerability in Skype for Business, which was reported by a third-party researcher in May 2022. Proof of concept exploit code shows that this vulnerability enables server-side request forgery (SSRF) attacks which could cause a server to make requests to unintended locations.

Actor profile: Diamond Sleet. The actor that Microsoft tracks as Diamond Sleet (formerly ZINC) is a North Korea-based activity group. Diamond Sleet is known to target media, defense, and information technology (IT) industries globally. Diamond Sleet focuses on espionage, theft of personal and corporate data, financial gain, and corporate network destruction.

Activity profile: Storm-0062 attempts to exploit CVE-2023-22515 in Atlassian Confluence. Microsoft has observed nation-state actor Storm-0062 attempting to exploit CVE-2023-22515 in the wild since September 14, 2023. CVE-2023-22515 was disclosed on October 4, 2023. CVE-2023-22515 is a critical privilege escalation vulnerability in Atlassian Confluence Data Center and Server. Any device with a network connection to a vulnerable application can exploit CVE-2023-22515 to create a Confluence administrator account within the application. The Storm-0062 campaign targets government and defense industrial base organizations in North America and Europe.

Actor profile: Storm-0539. The actor that Microsoft tracks as Storm-0539 is a financially motivated group active since late 2021. Storm-0539 is known to primarily target retail organizations for gift card fraud and theft. Storm-0539 carries out extensive reconnaissance of targeted organizations in order to craft convincing phishing lures and steal user credentials and tokens for initial access. The actor is well-versed in cloud providers and leverages resources from the target organization's cloud services for post-compromise activities.

Vulnerability profile: CVE-2023-4863 and CVE-2023-5217 vulnerabilities in WebP and libvpx. In September 2023, Google published CVE-2023-4863 and CVE-2023-5217 to address vulnerabilities in WebP (a compression format for images on the web) and libvpx (a software video codec library) that may result in remote code execution. The subsequent impact to Microsoft products has been documented in the Security Update Guide and the MSRC blog. Google is aware that exploits exist for both vulnerabilities.

Actor profile: Storm-0249. The actor Microsoft tracks as Storm-0249 (DEV-0249) is an access broker active since 2021 and known for distributing BazaLoader, Gozi, Emotet, IcedID, and Bumblebee malware. Storm-0249 typically uses phishing emails to distribute their malware payloads in opportunistic attacks. Microsoft observed Storm-0249 activity leading to hands-on-keyboard activity by ransomware operators like Storm-0501 (DEV-0501).

Actor profile: Storm-0589. The actor that Microsoft tracks as Storm-0589 (DEV-0589) is an activity group based out of Iran. Storm-0589 is known to target organizations in government, travel, hospitality, human resources, information technology, and telecommunications sectors in countries in Africa, Asia, Europe, and the Middle East. Storm-0589 has used a combination of commodity and custom tools, notably a custom scanner, in its operations. Given the profile of targeted organizations and the nature of known post-exploitation activity, Microsoft assesses that this group is seeking data that can be used to identify and track individuals of interest.

Vulnerability profile: CVE-2023-20198 and CVE-2023-20273 Cisco IOS XE web UI feature vulnerabilities. CVE-2023-20198 and CVE-2023-20273 are critical vulnerabilities in Cisco IOS XE Software web UI that could let an attacker remotely access and elevate privileges on impacted systems to achieve full compromise. Attackers reportedly exploited these then-zero-day vulnerabilities prior to their public disclosure. Microsoft has observed activity indicating threat actors are actively targeting these security flaws, and many impacted devices remain exposed to the web.

Vulnerability profile: CVE-2023-38831 in WinRAR. CVE-2023-38831 is a vulnerability in the WinRAR compression tool, which an attacker can exploit to run arbitrary code using a weaponized archive file. The vulnerability was reportedly exploited as early as April 2023 prior to its public disclosure. Since the disclosure in July 2023, exploitation activity increased in both widespread phishing operations as well as targeted spear phishing operations by threat actors such as Forrest Blizzard, Twill Typhoon, and Opal Sleet. Proof-of-concept code is widely available, further contributing to adoption among threat actors.

Vulnerability profile: CVE-2023-4966 and CVE-2023-4967 in NetScaler ADC and NetScaler Gateway. CVE-2023-4966 and CVE-2023-4967 are vulnerabilities in Citrix NetScaler ADC and NetScaler Gateway that, if exploited, can result in information disclosure and denial-of-service, respectively. Citrix disclosed these issues in an October 10, 2023, advisory and has since provided builds addressing the flaws.