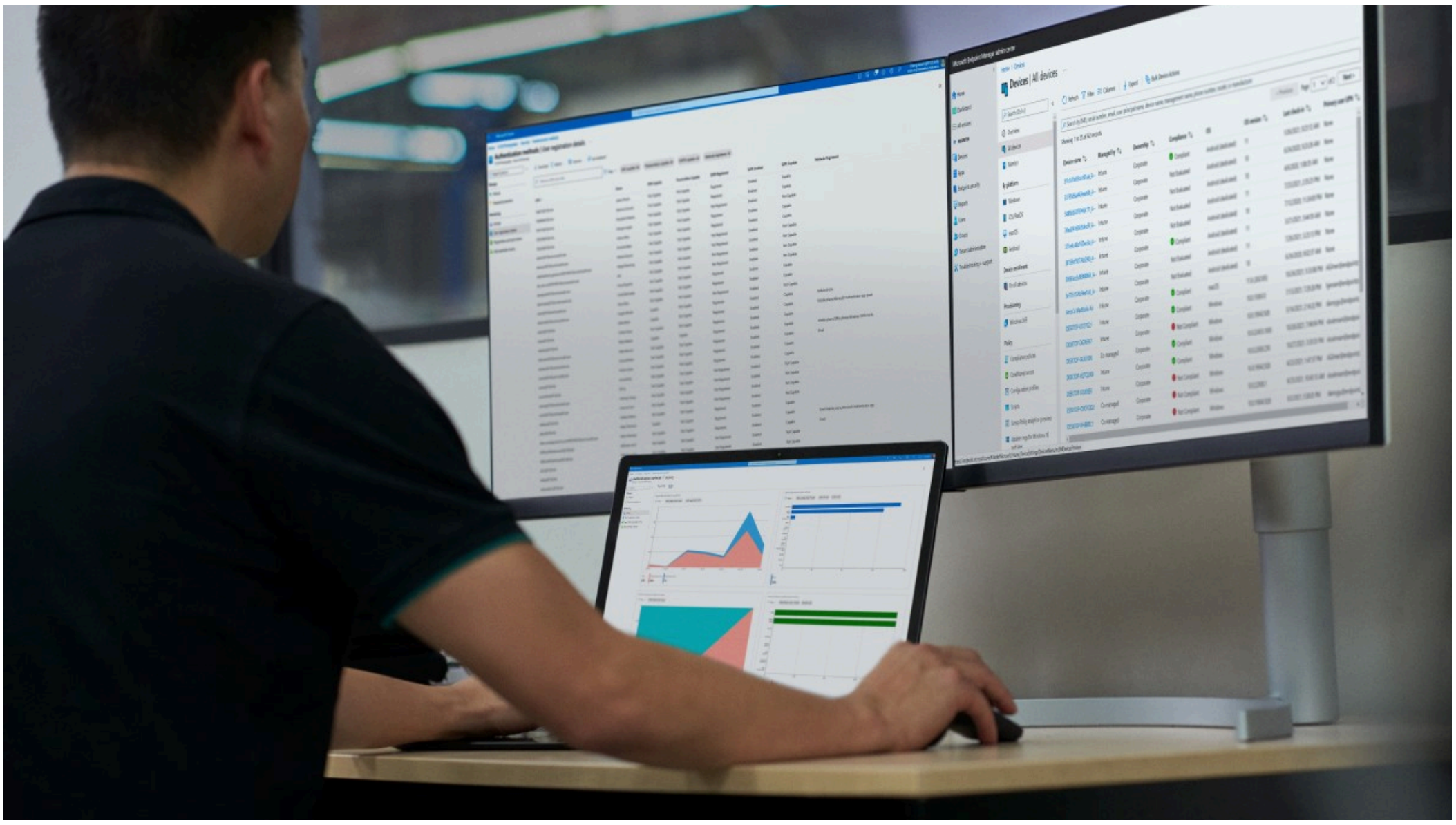


Best practices Data protection Microsoft Purview

6 min read

Microsoft Purview data security mitigations for BazaCall and other human-operated data exfiltration attacks

By Steve Vandenberg, Principal Global Black Belt, Security, Compliance and Privacy

August 8, 2023

Compliance Data security Zero Trust more

I recently worked with an enterprise customer who experienced a data exfiltration attack using the characteristics of the BazaCall campaign. BazaCall can be both a ransomware and data exfiltration attack that are used together to increase pressure on and damage to the victim. Microsoft Purview has data security capabilities that form part of a holistic mitigation strategy.

Microsoft 365 Defender is our security solution for phishing and related cyberthreats. Some great analysis has been done by the Microsoft Threat Intelligence team on BazaCall's Tactics, Techniques, and Procedures (TTPs). They've also shared how to use Microsoft 365 Defender to locate exploitation activity.

I wanted to take another perspective with this post and share the role that Microsoft Purview data security solutions play, together with Microsoft 365 Defender and Microsoft Sentinel, to provide defense-in-depth mitigation. With

defense-in-depth, we create barriers to the bad actor, increasing their resources required and uncertainty, interfering with their business case.

Microsoft Purview provides important value with unified data governance and compliance solutions but it's Microsoft Purview's data security capabilities within Microsoft 365 we'll be discussing in this blog.

What makes BazaCall different from most phishing attacks is using a malicious email to have the victim initiate a call to a phony call center run by the bad actor that then coaches the victim to install malware. Replacing malicious links and attachments in email with a phone number to the call center is used to evade email protection.

An overview of the BazaCall attack flow is provided at the end of this post.

The mitigations suggested here will be of value for attacks where the bad actor has control of a Microsoft 365 account and is attempting to exfiltrate sensitive data.

The data security benefits of Microsoft Purview for attack mitigation are sometimes overlooked. These solutions may be managed by other groups in the organization, such as the compliance team rather than the security team, and so may not be the go-to tools in the toolbox when preparing for or responding to an attack. These solutions should be part of a defense-in-depth strategy and Zero Trust architecture.

Microsoft Purview Mitigations

Microsoft Purview Information Protection sensitivity labels can be applied to protect sensitive files from unauthorized access. These sensitivity labels can have scoped encryption, among other protections, which travels with the file inside and outside of the organization's environment. This would make the file unreadable except by the party for which the encryption is scoped—for example, only employees, a partner, or a customer organization—or it can be defined by the user to be consumable only by specific individuals.

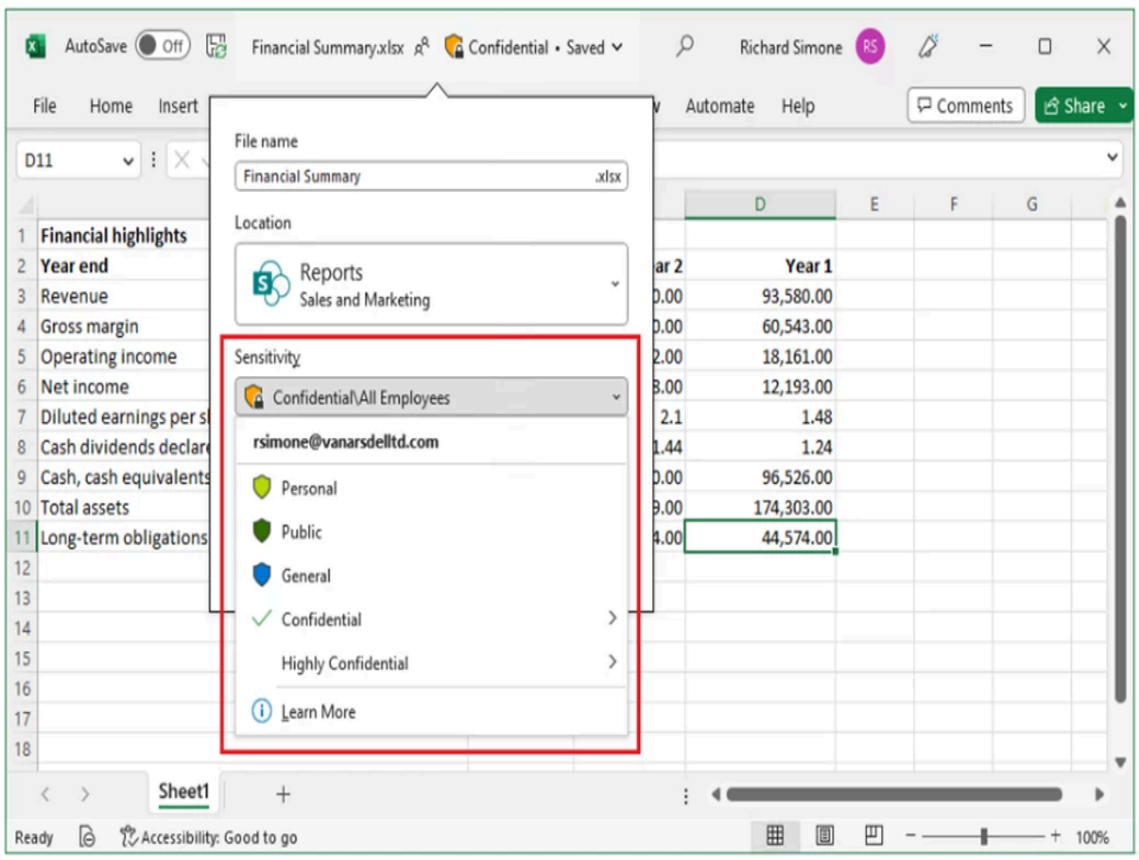


Figure 1. Sensitivity Label with scoped encryption—accessible only to employees.

Automation, configured by the administrators, can be used to support the user in applying these labels including making the application of a label mandatory if the file contains sensitive information.

Microsoft Purview Data Loss Prevention (Purview DLP) can be used to prevent the sensitive information from being exfiltrated through several egress channels, including user's endpoint devices, Microsoft cloud services such as SharePoint Online, OneDrive for Business, Exchange Online, Teams, and Microsoft PowerBI, browsers such as Microsoft Edge, Chrome, and Firefox, as well as non-Microsoft applications such as Salesforce, Dropbox, Box, and more, including the free file-sharing services used as part of the BazaCall TTPs.

Customers can create policies that block and do not allow override for their top priority sensitive information such that even if the bad actor manages to get access to the user's account, they are blocked from exfiltrating any sensitive content. Purview DLP policies can be configured leveraging a variety of out-of-the-box or custom criteria including machine learning-based trainable classifiers as well as the sensitivity labels created in Information Protection.

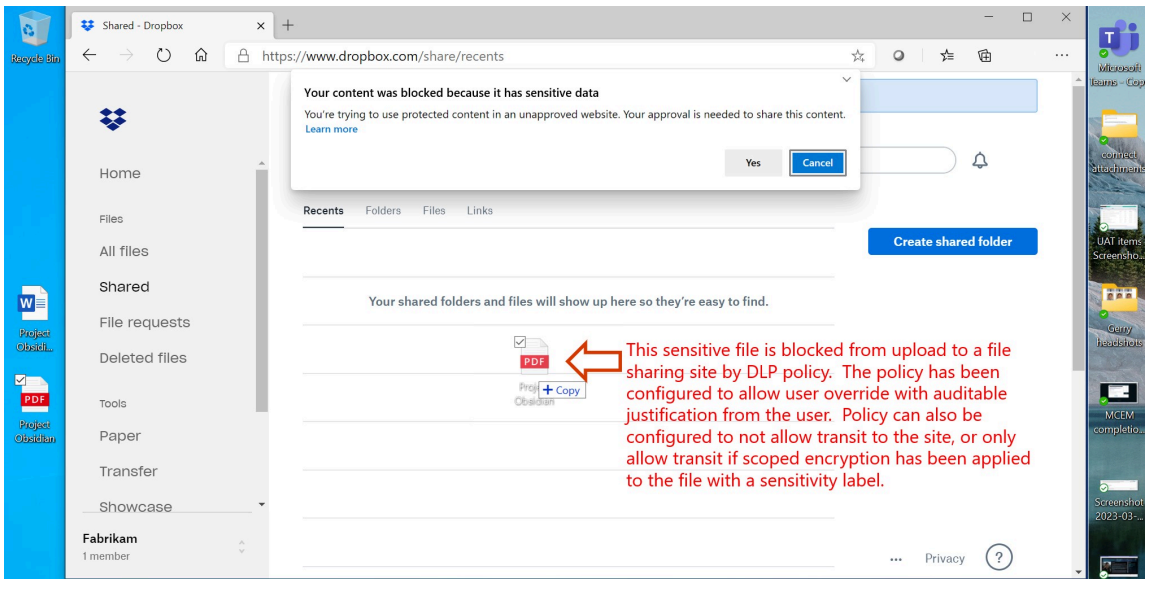


Figure 2. Purview DLP preventing the upload of sensitive files into Dropbox.

Microsoft Purview Insider Risk Management can alert the security team to the bad actor's activities, including the exfiltration of sensitive information to the file-sharing service. Insider Risk Management can reason over and parse through user activity signals, by leveraging more than 100 ready-to-use indicators and machine learning models, including sequence detection and cumulative exfiltration detection. With Adaptive Protection powered by Insider Risk Management, the security team can detect high-risk actors, such as a bad actor-controlled account, and automatically enforce the strictest DLP policy to prevent them from exfiltrating data.

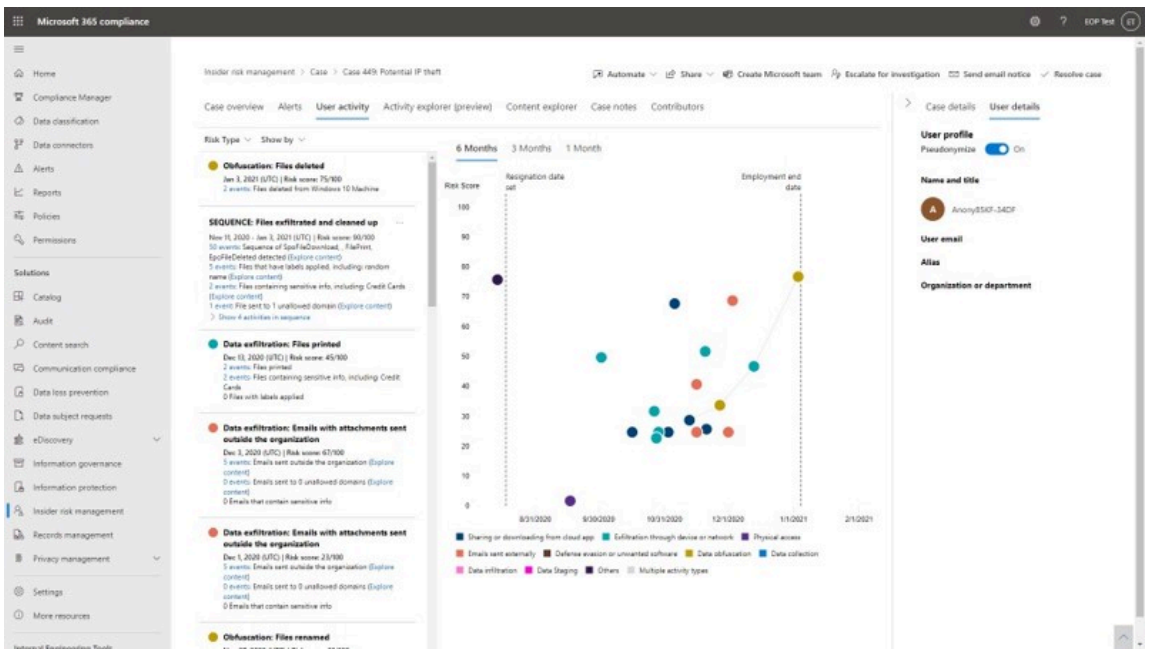


Figure 3. Insider Risk Management uses specialized algorithms and machine learning to identify data exfiltration and other risks.

Microsoft Defender for Cloud Apps can make a file-sharing site used for sensitive file exfiltration unreachable from the user's browser or it can prevent sensitive files from being moved to the site. Alternatively, the policy can be configured to only allow files to be moved to the file-sharing site if they have a sensitivity label applied that contains scoped encryption. If this protected file is exfiltrated it would not be readable by the bad actor.

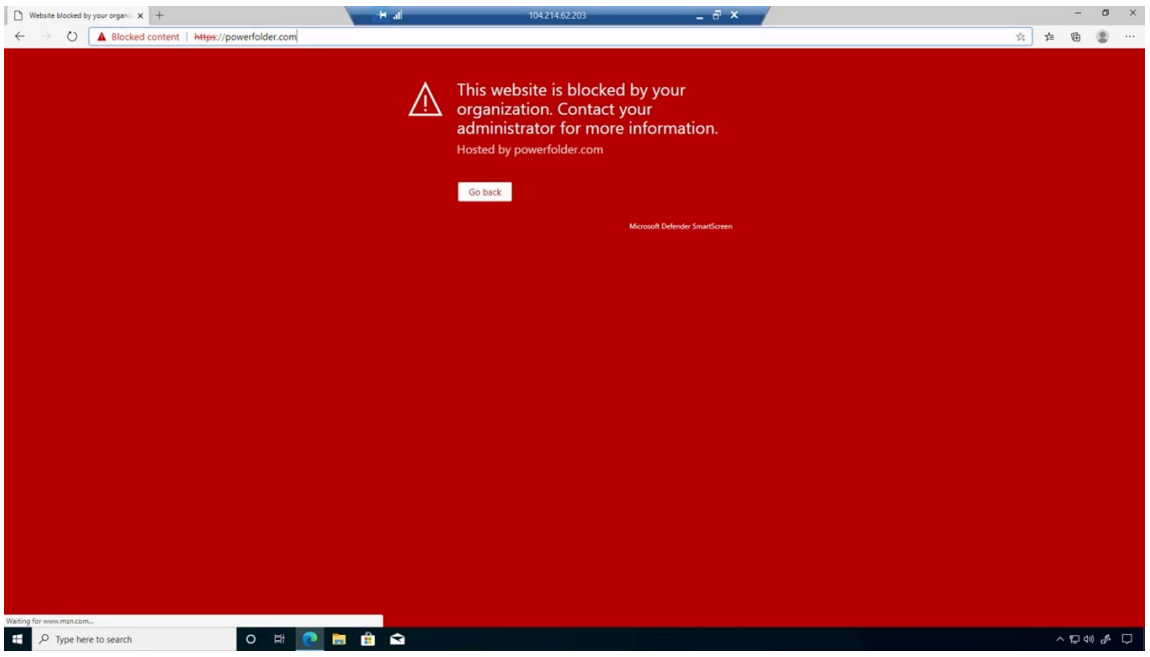


Figure 4. Microsoft Defender for Cloud Apps blocking access to file sharing and backup site.

Microsoft Purview Audit provides forensic information to scope a possible breach. This is especially valuable when bad actors are "living off the land." Among the audit items made available are the terms that a user searched in email and SharePoint. If the bad actor was searching for sensitive information to exfiltrate, this item will assist the investigation.

Purview Audit, recently expanded for accessibility and flexibility, will also provide insight to mail items accessed and mail sent, which would be impactful when investigating scope and possible exfiltration channels. Although a bad actor's known TTPs may not include these channels, we need a fulsome investigation. Their TTPs are likely not static.

Purview Audit Premium provides more logging event retention capabilities, with one-year retention (up from 180 days with Standard) and an option to increase retention to 10 years among other upgraded features.

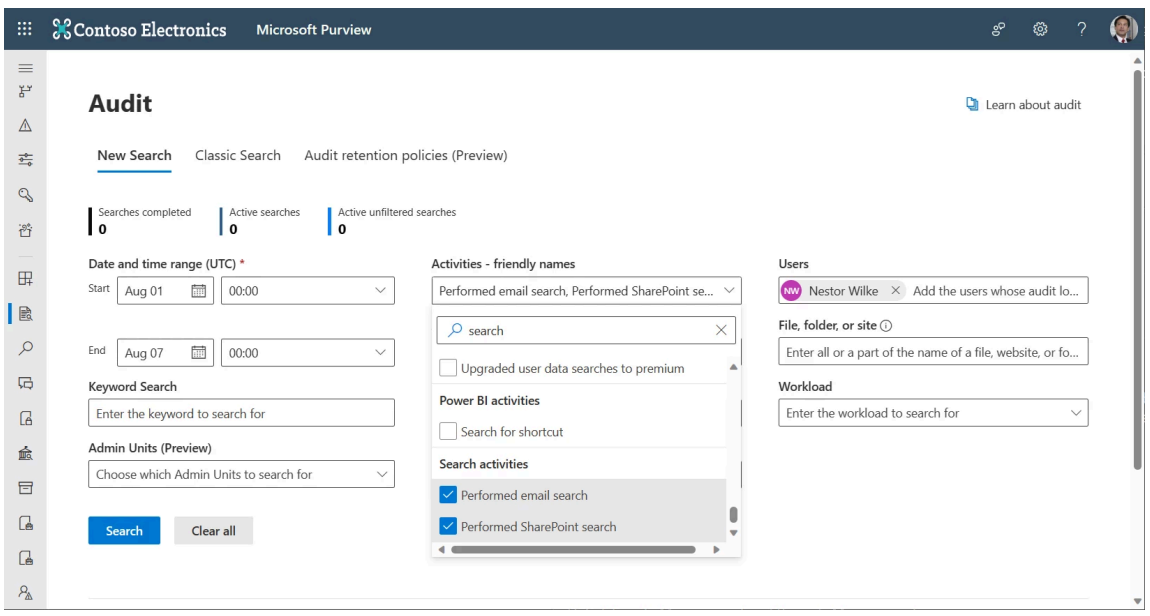


Figure 5. Premium Audit solution searching forensic events.

Microsoft Purview Data Lifecycle Management policies and labeling could be used to purge unneeded information from the organization's environment. An auditable review can be required prior to deletion or deletion can be automated without user or administrator action.

If information is not in the environment, it cannot be exfiltrated by the bad actor or put the organization at risk.

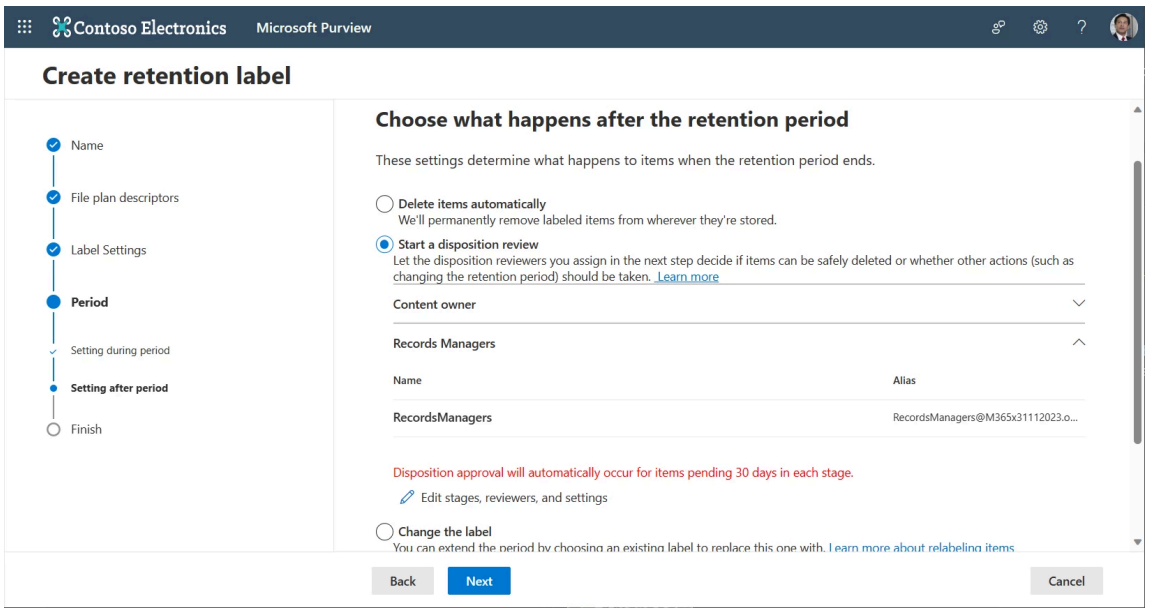


Figure 6. Disposal of unneeded documents reduces exfiltration risk to the organization.

About BazaCall

BazaCall uses a phishing campaign that tricks unsuspecting users into phoning the attacker, who coaches them into downloading BazaLoader malware, which retrieves and installs a remote monitoring and management (RMM) tool onto the user's device. The email typically claims that the user has reached the end of a free trial of some type, that billing will begin shortly and provides an option to cancel by phoning a call center. The threat of unjustified billing is the lever that the attacker uses to get the victim to comply.

Typically, the file download has been a malicious Excel document that purports to be a "cancellation form" for the unwanted service and charges referred to in the phishing campaign. The bad actor coaches the victim into accepting macros and disabling security solutions to complete the phony "cancellation."

RMM software provides multiple useful purposes for attackers: The software allows an attacker to maintain persistence and deploy malicious tools within a compromised network. It can also be used for an interactive command-and-control system. With command and control established, the bad actor organization can spread laterally through the environment to steal sensitive data and deploy ransomware. Once command and control of the user's machine is established, bad actor hands-on keyboard is used to exfiltrate data including through free cloud-based file-sharing sites. TTPs have evolved in the last two years, including the use of file-sharing sites for exfiltration in addition to open-source tools like RClone.

The user is also subject to human-operated ransomware.

The mitigations discussed in this post are focused on the data exfiltration aspects in the "hands-on-keyboard" phase of the attack.

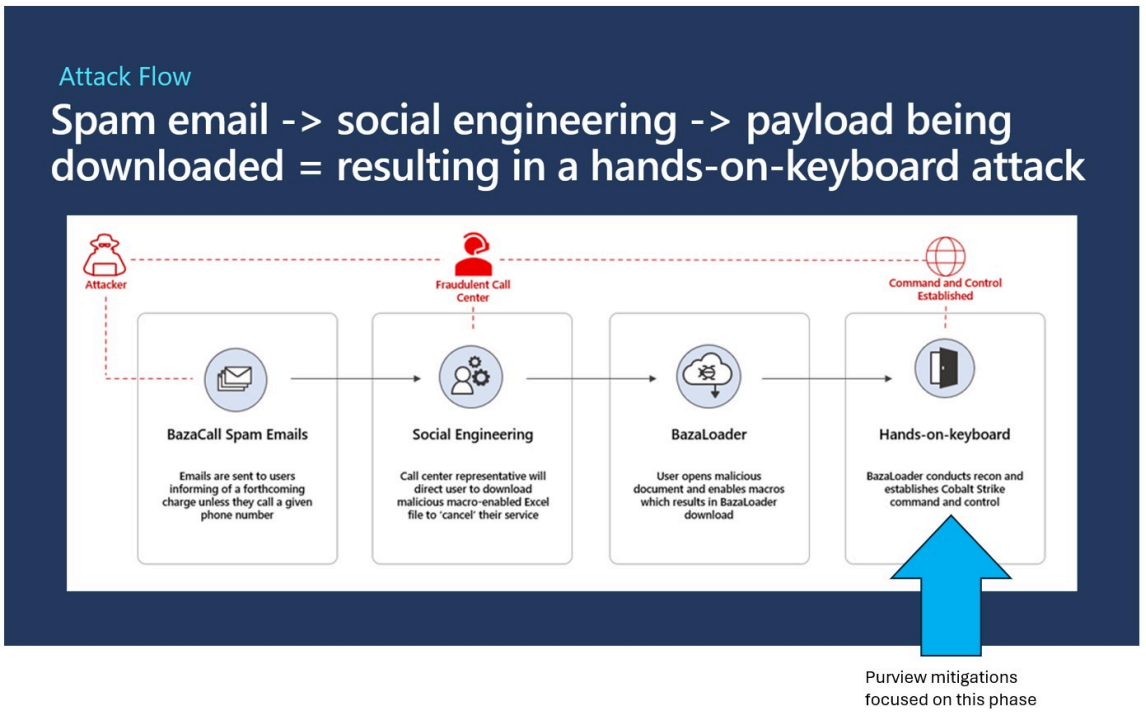


Figure 7. BazaCall attack flow.

Microsoft Purview can help protect from BazaCall attacks

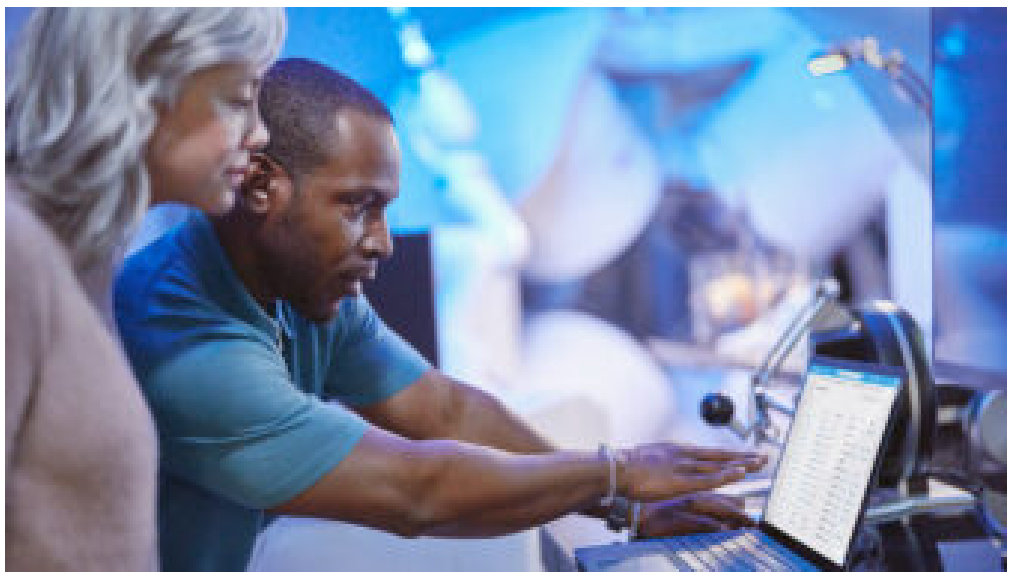
Microsoft Purview data security for Microsoft 365 is not a cure-all for phishing attacks. It is part of a defense-in-depth strategy that includes user training, antimalware, vulnerability management, email security, access control, monitoring, and response. The data security solutions within Microsoft Purview should be considered based on risk-based criteria for inclusion in the strategy.

These tools may be managed by different teams in the organization. Collaboration among these teams is critical for coordinated defense and incident response.

Learn more

To learn more about Microsoft Security solutions, visit our website. 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.

Related Posts

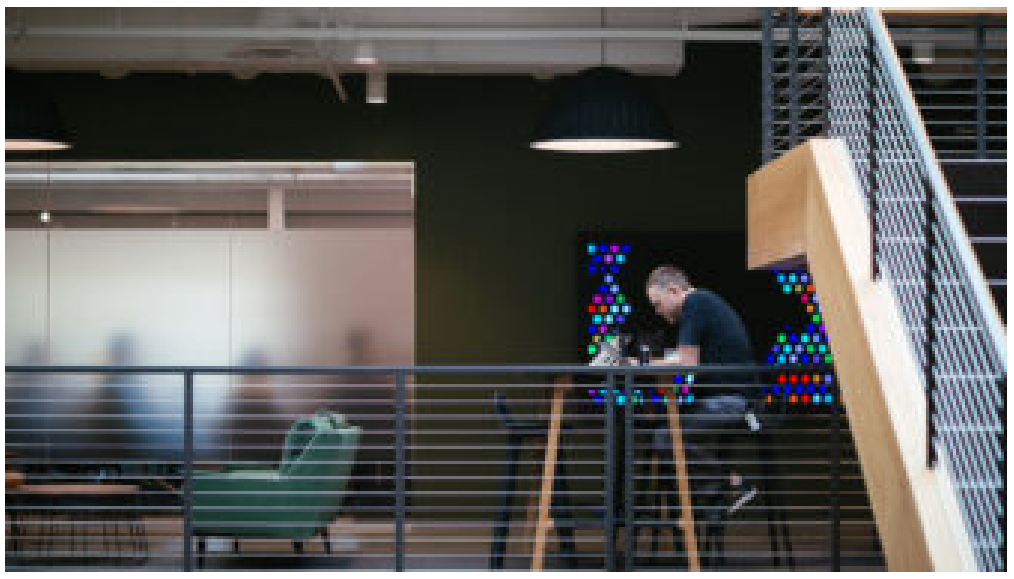


Research Endpoint security Microsoft Defender for Endpoint Ransomware

Oct 11, 2023 10 min read

Automatic disruption of human-operated attacks through containment of compromised user accounts

User containment is a unique and innovative defense mechanism that stops human-operated attacks in their tracks. We've added user containment to the automatic attack disruption capability in Microsoft Defender for Endpoint. User containment is automatically triggered by high-fidelity signals and limits attackers' ability to move laterally within a network regardless of the compromised account's Active Directory state or privilege level.

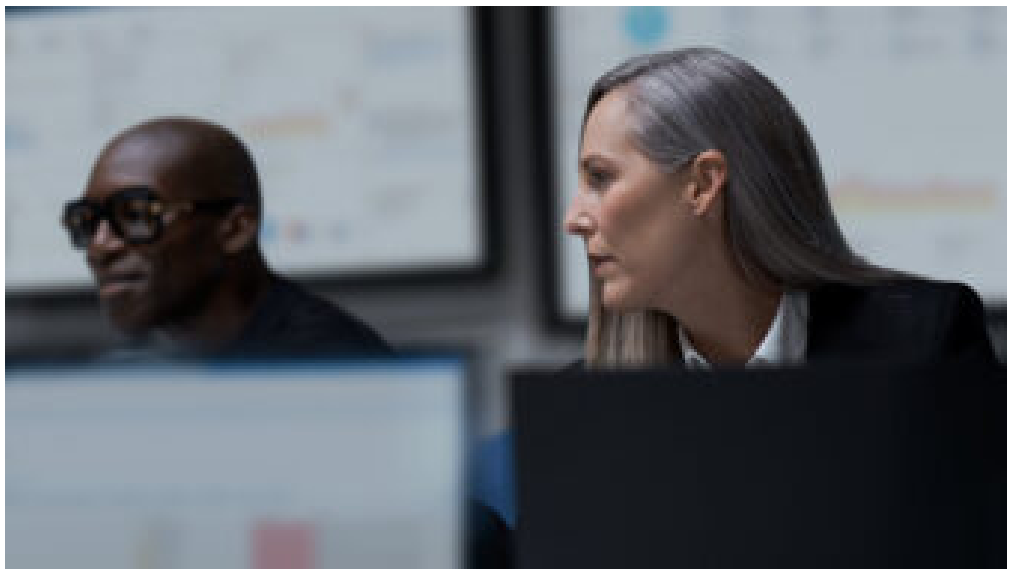


Research Endpoint security Microsoft Defender XDR Threat actors

Sep 12, 2023 8 min read

Malware distributor Storm-0324 facilitates ransomware access

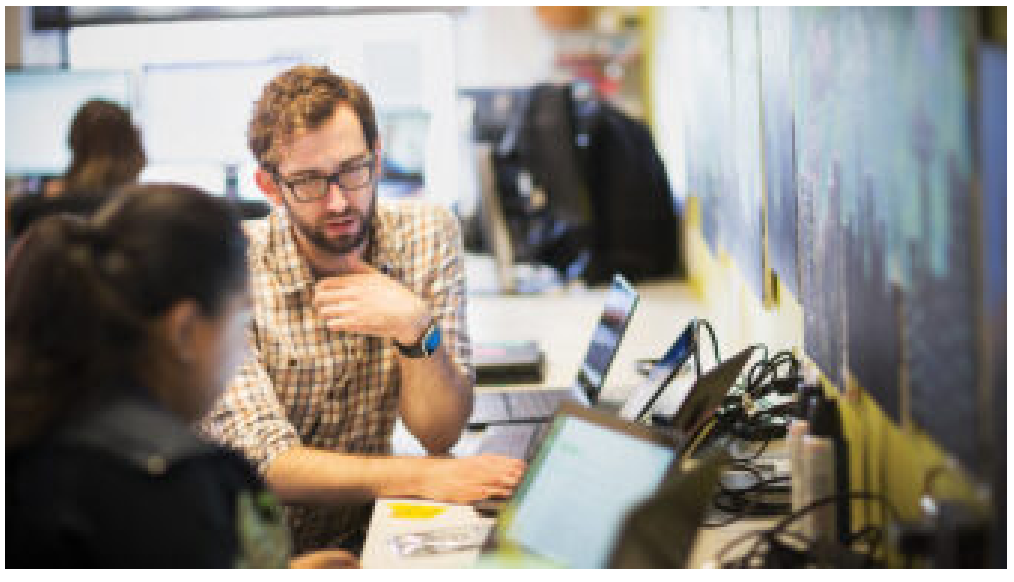
The threat actor that Microsoft tracks as Storm-0324 is a financially motivated group known to gain initial access using email-based initial infection vectors and then hand off access to compromised networks to other threat actors. These handoffs frequently lead to ransomware deployment. Beginning in July 2023, Storm-0324 was observed distributing payloads using an open-source tool […]



Research Threat intelligence Microsoft Defender XDR Threat actors
Aug 24, 2023 13 min read

Flax Typhoon using legitimate software to quietly access Taiwanese organizations ›

China-based actor Flax Typhoon is exploiting known vulnerabilities for public-facing servers, legitimate VPN software, and open-source malware to gain access to Taiwanese organizations, but not taking further action.



Research Threat intelligence Microsoft Defender
Attacker techniques, tools, and infrastructure
Jul 25, 2023 13 min read

Cryptojacking: Understanding and defending against cloud compute resource abuse ›

Cloud cryptojacking, a type of cyberattack that uses computing power to mine cryptocurrency, could result in financial loss to targeted organizations due to the compute fees that can be incurred from the abuse.

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