



Monthly MDR Threat Briefing

Covering your MDR Security Posture Review, Trend Analysis, Threat Intel Briefing & MDR Service Updates

[#CUSTOMER NAME]

[#Your Name]

Customer Advisor

[#DATE]

Agenda

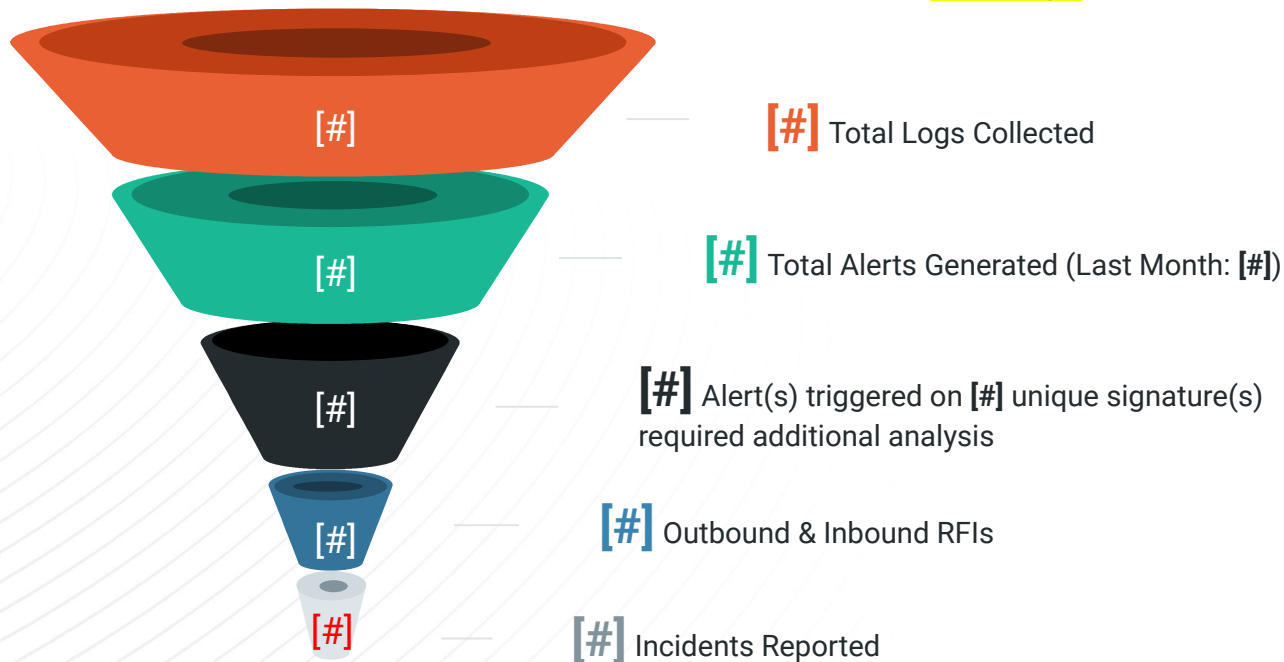
- Service Status Update
- New IDR Features, Improvements, & Fixes
- MDR Updates & Recommendations
- Workshops & Webinars
- Trending Malware & Ongoing Campaigns
- Trending Vulnerabilities
- Q&A

Service Status Update

Alerts, RFIs, & Incident Reports

Month: January

Update/Edit
this page



	Closed Alerts by Priority	Incident Reports
High	[#]	[#]
Medium	[#]	[#]
Low	[#]	[#]

User Accounts and Event Sources

Update/Edit
this page

- Administrators
 - [#]
 - [#] Previous month
- Users with Non-Expiring Passwords
 - [#]
 - [#] Previous month
- Service Accounts with Non-Expiring Password
 - [#]
 - [#] Previous month

Reconcile the IDR identified administrator accounts reported in the monthly report with your approved organizational administrators list.

Recommended event sources	
Active Directory	√/X
LDAP	√/X
DHCP	√/X
DNS	√/X
Firewall	√/X
Web Proxy	√/X
VPN	√/X
Cloud Services	
Office365	√/X
AWS	√/X
G Suite Apps	√/X
Google Cloud	√/X
Azure	√/X

MDR Threat Hunt - January

Update/Edit
this page

Potentially Unwanted Programs (PuP)

- [#] Entries
- [#] Entries Previous Month
- Imposter Domains [Delete if not needed]
- Threat Hunts Performed
 - Malicious Cloudflare daemon usage
 - During an Incident Response investigation, Rapid7 identified a novel attacker technique making use of CloudFlare's legitimate tunnel client "cloudflared" (Cloudflare Daemon) to tunnel C2 traffic through CloudFlare's infrastructure.
 - This hunt searched all customer environments for instances of "cloudflared.exe" running that were inconsistent with legitimate usage.
 - Malicious OneNote File Execution
 - Conducted investigations that uncovered the emergence of attackers using malicious OneNote documents to gain initial access to client environments

Key Takeaways

[#REMOVE IF THE CLIENT HAS ZERO PuPs] Review the reported Potentially Unwanted Programs to determine whether they serve a business need. Otherwise, it is advised that they be removed.

- Review the remote access software presence on each system reported in the hunt report to determine whether it has a business need and if the system owner is authorized to use the application.
 - Bomgar, Remote Desktop, VNC, TeamViewer(36), Chrome Remote Desktop, NoMachine(1), PSEXec(12), LogMeIn/GoToMyPC/Hamachi(13), AnyDesk(3)
- Ensure that users follow corporate cloud storage usage policies by uninstalling unwanted software or blocking cloud storage network traffic.
 - Dropbox(36), CrashPlan, Microsoft OneDrive, Carbonite, iCloud(6), Amazon Drive
- Rapid7 identified multiple registered domains potentially designed to be imposters of the registered domain. If the identified domains are not owned by your organization, Rapid7 recommends reviewing and blocking the identified domains.

Insight Agent Update

Why track? Old versions lack the latest features and improved performance.

Latest version: **3.2.3**

Update/Edit
this page

New

- We updated the Insight Agent data collection on Windows to support Patch Tuesday vulnerability checks for January 2023 (IVM Only).

Improved

- Directory exclusion support for PowerShell: We now support directory exclusions for running PowerShell on Windows machines. The primary use case for this capability is for InsightVM customers who want to exclude directories for the Log4j/Log4Shell vulnerability checks. Just as with existing macOS and Linux directory exclusion requests, create a case with Rapid7 Support to get started.

Agent Version	Endpoint Count
1.4.X	[#] ([#]offline, [#] stale) previous [#]
3.1.12 & <	[#] ([#]offline, [#] stale) previous [#]
3.2.0	

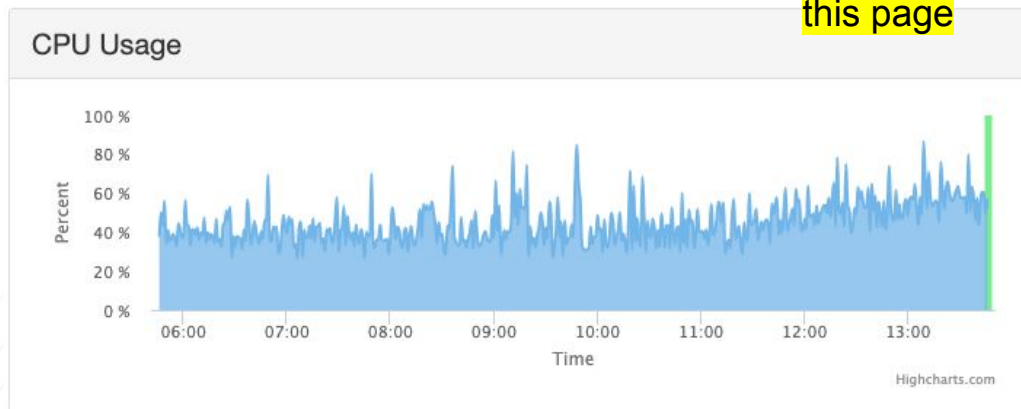
- [#] Licensed Endpoints
- [#] Endpoints checked in the last 30 days
- [#] Stale Endpoints

Key Takeaways

- [#] Agents with Errors
 - [#] Windows hosts with agent job fails
 - [#] Linux hosts are giving errors for audit Compatibility not enabled
- [#] offline and stale agents include servers
 - agent.description CONTAINS "server" OR agent.description CONTAINS "linux"
- Upgrade the remaining old agents to the latest version

Event Source & Collector Health

Update/Edit
this page



Key Takeaways

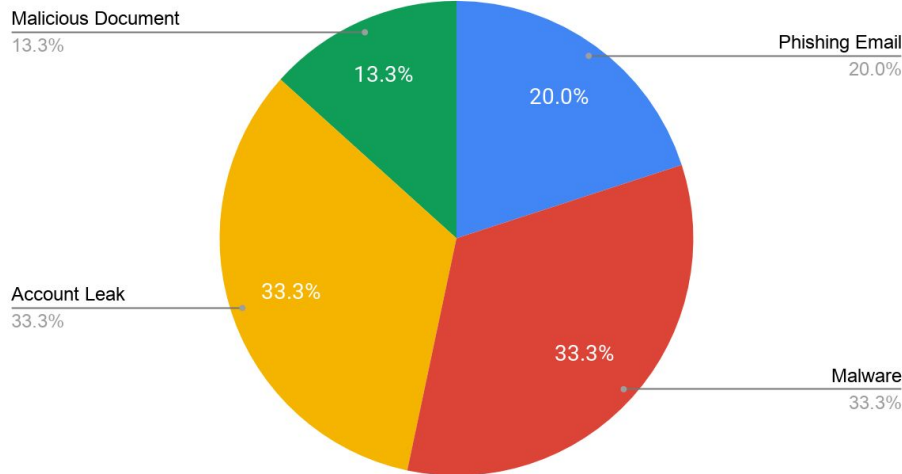
- Event Sources with errors:
 - Event Source Meraki - BR Corporate (All) hasn't seen logs since Jul 1, 2020 7:14:28 PM
- Collectors with Issue:

Service & Trends Update

[#CUSTOMER_NAME] Investigation Report Breakdown by Type([#DATE_RANGE])

Investigation Report Type	Count
Unauthorized Access	97
Phishing Email	75
Malware	46
Account Leak	34
Malicious Document	8
Pentest	1
Lateral Movement	1

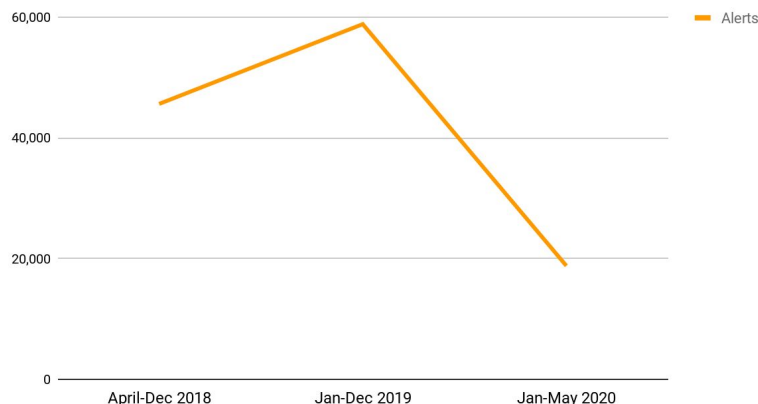
Findings Report Type



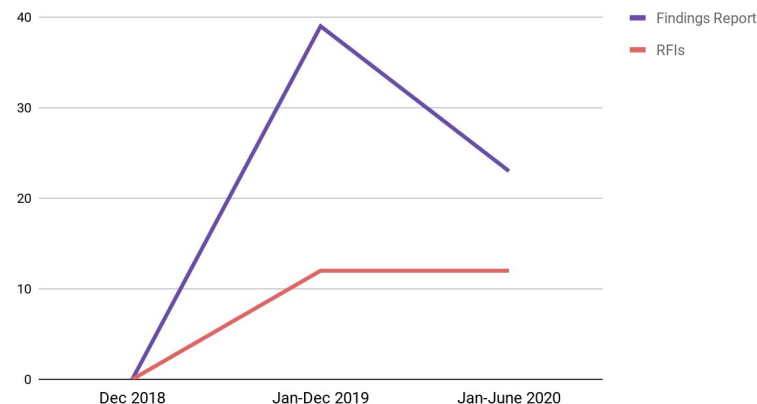
Over [#]% of the Investigation Reports were for [FILL_IN]

[CUSTOMER_NAME] Alerts, Investigation Reports, & RFIs Year Over Year ([Date-Range])

Alerts



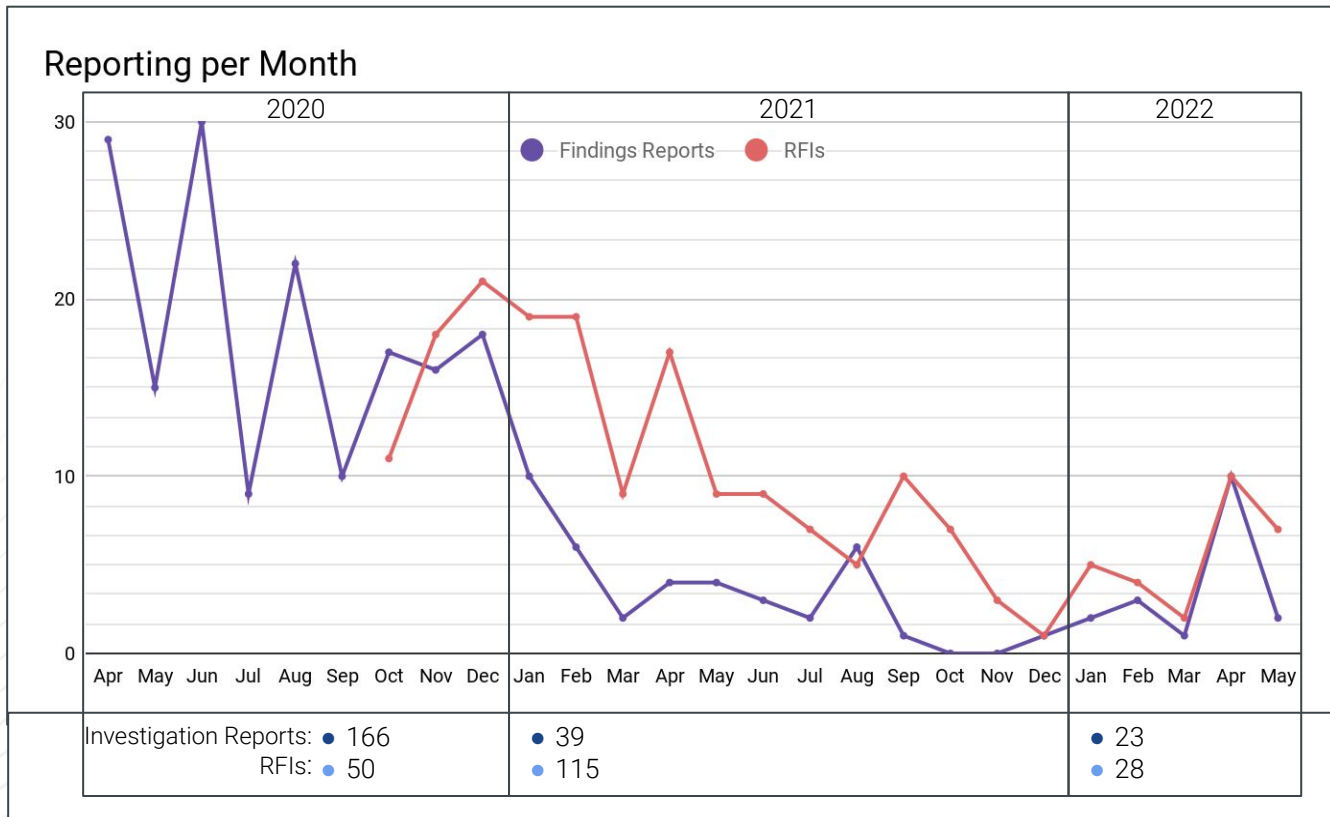
Findings Report & RFI



- Prior to start of Rapid7 MDR service, the [CUSTOMER_NAME] environment [FILL_IN].
- [CUSTOMER_NAME]'s remediation efforts, guided by recommendations provided in Investigation Reports, resulted in a decline in alerts and RFIs.

Monthly RFIs and Investigation Reports

#Date Range



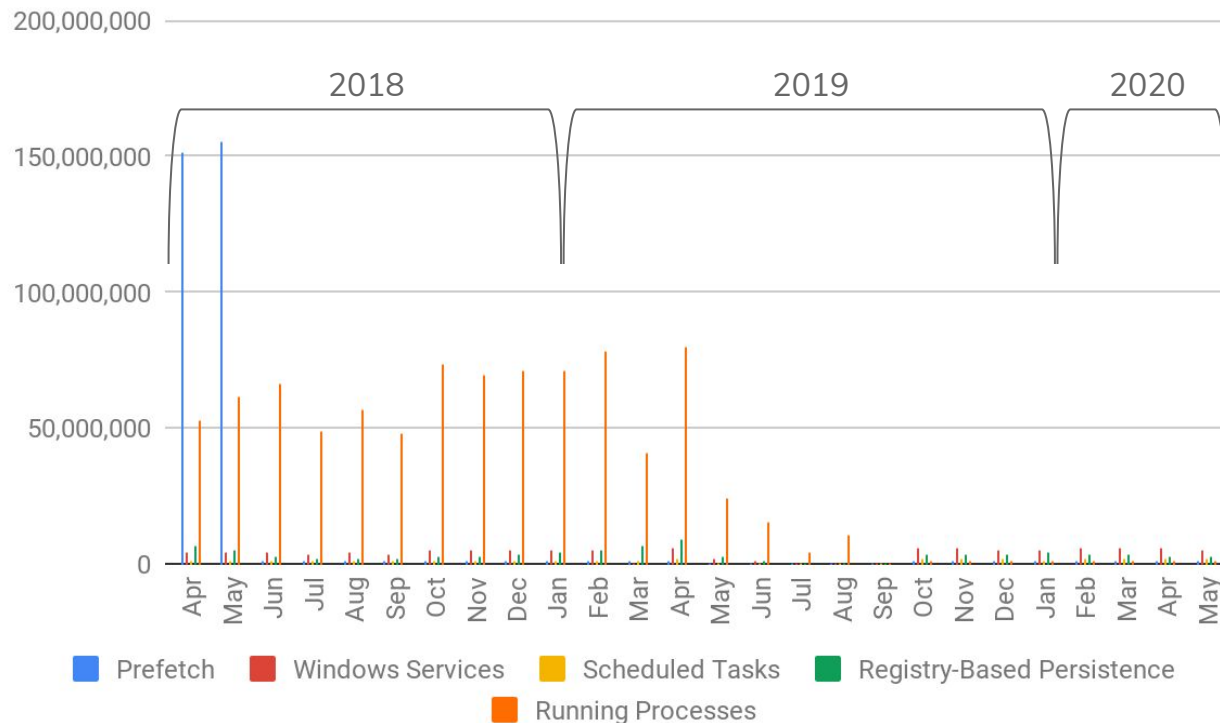
[CUSTOMER_NAME]

Monthly RFIs and Investigation Reports Analysis

Beginning in [DATE] through today, the [decline or up tick] in the number of Investigation Report and RFIs for [CUSTOMER_NAME] can be directly correlated to:

- [Examples shown below]
- The [decline or up tick] in the number of new hosts and user accounts compromised over time
- As [CUSTOMER_NAME] actioned the MDR remediation recommendations and implemented the mitigation recommendations, the trend shows a continued decline in the number of RFIs and Investigation Report over time
- The remediation and mitigation recommendations consisted of: blacklisting countries like Nigeria where [CUSTOMER_NAME] does not have users, rebuilding affected systems from a known-good baseline image, and blocking identified malicious IPs and domains

R7 Proactive Threat & Risk Hunting for [CUSTOMER_NAME] (Date Range)



Beginning in [TIME_FRAME], MDR baselined [CUSTOMER_NAME]'s environment, whitelisting benign applications and processes.

The **result is a month-over-month [decline/uptick]** in the number of anomaly artifacts reviewed and identified.

New Detections, Features, Improvements & Fixes

New MDR Detections Added

In January, Rapid7's MDR's Threat Intelligence and Detection Engineering (TIDE) team created 77 new detection rules. The TIDE team also implemented X suppressions, tuning the rules listed under "Rules with new Suppressions."

*Only a subset of the new rules are shown

Newly Created Rules and Suppressions	
In January, Rapid7's MDR's Threat Intelligence and Detection Engineering (TIDE) team created 77 new detection rules. The TIDE team also implemented 2 suppressions, tuning the rules listed under "Rules with new Suppressions." Each month, TIDE actively researches new detections to increase coverage, and implements suppressions to raise the fidelity of existing detections which helps cover the BTIG LLC environment.	
Newly Created Rules	
Name	Description
Attacker Technique - Cloudflared Agent Service Installed	This detection identifies services being installed with 'Cloudflared agent' in the service name. This legitimate software is used by malicious actors in order to perform tunneling of network traffic and hide the IP address of the attackers infrastructure from the victim.
Attacker Technique - Cloudflared Agent Tunnel Initiated From Unusual Location	This detection identifies the execution of the common flags passed to the legitimate 'cloudflared' binary to tunnel traffic, but when executed from a non standard location. Malicious actors use this technique with this legitimate utility in this manner to tunnel network traffic.
Attacker Technique - Powershell Collects Active Directory Computer Information	This detection identifies PowerShell being used to push to collect computer information from all systems found in Active Directory. Malicious actors use this technique during network discovery phase so see which hosts can be targeted.
Attacker Technique - Service Installed To Perflogs	This detection identifies services being installed with 'perflogs' in the command line. This technique is used by malicious actors in order to perform execution of commands through a system service.
Cryptocurrency Miner - Process Has Monero Wallet Environment Variables	This detection identifies processes that have environment variable names consistent with the Monero coinminer. Coinminers such as this are often installed post-compromise by malicious actors in order to monetize intrusions.
ET EXPLOIT ManageEngine Unauthenticated RCE Attempt M1 (CVE-2022-47966)	This detection identifies malware related activity using Rapid7's Network Traffic Analysis sensor. Malicious actors often use malware in order to gain access to victim organizations.
ET EXPLOIT ManageEngine Unauthenticated RCE Attempt M2 (CVE-2022-47966)	This detection identifies malware related activity using Rapid7's Network Traffic Analysis sensor. Malicious actors often use malware in order to gain access to victim organizations.
ET MALWARE AHK Bot Domain Profiler CnC Activity	This detection identifies malware related activity using Rapid7's Network Traffic Analysis sensor. Malicious actors often use malware in order to gain access to victim organizations.
ET MALWARE Cobalt Strike Domain (fepopeguc.com) in TLS SNI	This detection identifies malware related activity using Rapid7's Network Traffic Analysis sensor. Malicious actors often use malware in order to gain access to victim organizations.
ET MALWARE Gamaredon APT Related Activity (GET)	This detection identifies malware related activity using Rapid7's Network Traffic Analysis sensor. Malicious actors often use malware in order to gain access to victim organizations.

MDR Updates

Consistent Incident Terminology and Reporting

To simplify the classification and clearly delineate RFIs from Incidents, we have updated incident classification to three *severities*: Low, Medium, and High. The SOC will only assign a severity level to incident notifications. RFIs will have a severity level of 'RFI' in the Incident Severity field on the Customer Portal case (if applicable).

Update

- We have deployed these changes as of, **February 1, 2023**.
- The updated [MDR Scope of Service](#) is live on the Managed Resource Site.
- You will now receive updated MDR notifications distinguished between Requests for Information (RFIs) and incident notifications.
- Please view details on these notifications and how to action them here: [MDR Notifications](#). If you use mail forwarding rules or other automation to manage alerts, please update accordingly.
- See how we reflect these changes in the Customer Portal (if applicable) here: [Customer Portal](#).

If you have any questions or would like to provide us with feedback, please reach out to your Rapid7 Customer Advisor.

New IDR Features

- **Investigations audit log:** InsightIDR now provides visibility into actions that were taken on an investigation. The investigation audit log records updates made in the investigation, when those updates were made, and the user who made them. Additional features include:
 - Audit log visibility in Log Search: The audit logs from Investigations are also available in Log Search as part of the Audit Logs log set.
 - Audit log for Managed Detection and Response (MDR) customers: If you're an MDR customer, the audit log shows the updates that your organization made to an investigation. The ability to view updates made by the Rapid7 SOC is planned for a future release.
- To learn more about the audit log, [read the documentation](#).
- **API collection method for Palo Alto Cortex Data Lake:** You can now set up the Palo Alto Cortex Data Lake event source using an API collection method, which makes setup easier and more secure. To learn more about the API collection method, [read the documentation](#).
- **Onboarding Progress Tracker for MDR customers:** If you're an MDR customer you now have access to the Onboarding Progress Tracker, which was previously available to InsightIDR Essential, Advanced, and Ultimate customers only. The Onboarding Progress Tracker is available from the Home page as a self-serve, centralized checklist of onboarding tasks with step-by-step guidance, completion statuses, and context on the "what" and "why" of a task. This feature is available for new user onboarding, beyond the 90 day onboarding period.
- **Search faster with a redesigned Log Search user interface:** Now in open preview, you can load selected log sets more quickly using the fully updated Log Search experience. Equipped with new features and better interactivity for a more seamless user experience, Log Search Open Preview is available in the left navigation alongside the original Log Search until development is complete.

IDR Improvements

- LEQL having clause includes all calculation functions: When grouping log results using `groupby`, you can now leverage the `having` clause with calculation functions, such as `sum`, `max`, and `unique`, which help you isolate interesting events and reduce noise.
- Updated Home page metrics: We removed the Latest Processes and Cloud Services widgets from the Home page to better utilize screen space and make other metrics more visible. You can still view your Latest Processes and Cloud Services in Users and Accounts.

IDR Bug Fixes

- We fixed an issue in Users and Accounts, which caused data in the Ingress Locations chart to be difficult to read.
- We fixed an issue where the Barracuda Firewall event source was not parsing LocalBlock events. You might notice an increase in Barracuda Firewall events as a result.
- We fixed an issue in Investigations that caused attachments to be difficult to read in dark theme.
- We fixed an issue in Assets and Endpoints where the Create endpoint ID address range panel did not include a close icon.

MDR Updates & Recommendations

MDR Recommendations

Follow Microsoft's Best Practices for Updating your Exchange servers:

- Be sure to always read our blog post announcements, noting known issues and recommended or required manual actions. For CUs, always follow our [guidance and best practices](#), and for SUs, use the [Security Update Guide](#) to find relevant information.
- Be sure to review our update FAQ in the article [Why Exchange Server Updates Matter](#).
- Use the [Exchange Server Health Checker](#) to inventory your servers and see which Exchange servers need updates (CUs or SUs), and if any manual action needs to be taken.
- Once you know what updates are needed, use the [Exchange updates step-by-step guide](#) (aka the Exchange Update Wizard) to choose your currently running CU and your target CU and get directions for updating your environment.
- If you encounter errors during update installation, the [SetupAssist](#) script can help troubleshoot them. And if something does not work properly after updates, have a look at the [Update Troubleshooting Guide](#), which covers the most common issues and how to resolve them.
- Be sure to install any necessary updates for Windows Server and other software that might be running on your Exchange server(s).
- Be sure to install any necessary updates on dependency servers, including Active Directory, DNS, and other servers used by Exchange.

New Educational Resources

Resources

- [Machine Learning from our CTO](#): Read this article to hear what Rapid7's CTO has to say about the benefits of machine learning and why small companies are not immune from cyber attacks.
- [Air Traffic Outage](#): Check out this Blog Post to learn what the recent air traffic outage taught us about security.
- [Forbes Cybersecurity + KPIs](#): An explanation about why it's time to align security with organizational key performance indicators (KPIs).
- **Medical Device Security:**
 - Part 1: [How to Scan Devices Without Letting Safety Flatline](#)
 - Part 2: [How to Give Medical Devices a Security Checkup](#)
 - Part 3: [Putting Safe Scanning into Practice](#)

Workshops & Webinars

- **New CSE Workshops:** Check out the new (free) recordings we've recently added to our CSE Workshop catalog, including...
 - [TC: Configuration Best Practices](#)
 - [ICS: Getting Started with InsightCloudSec](#)
 - [IVM Console Reporting Overview](#)
 - [IDR Log Search Fundamentals: Using Queries and LEQL](#)
 - [Metasploit: Configuration Best Practices](#)
- **Agent-Based Policy Scanning Webinar:** Available on-demand for those who missed it, check out our recent webinar focused on the new Agent-Based Policy Scanning capability recently added to IVM.
- **EMEA Hackers 're Gonna Hack:** Check out this 3-part series to revisit the fundamentals needed to keep pace with the changing threat landscape...
 - [Part 1 on demand](#)
 - [Part 2 on demand](#)
 - [Part 3 on demand](#)

Threat Landscape Update

Trending Malware & Ongoing Campaigns

Malware Delivered by USB Drives

- Still a commonly used method of delivering malware
- Malware that targets USB drives can detect when the USB device is plugged in before downloading malicious code onto the drive

Prevention:

- Disable USB storage devices via Group Policy or Registry:
<https://www.windowcentral.com/how-disable-access-removable-storage-devices-windows-10>
- Disable AutoRun via Registry or Group Policy:
<https://learn.microsoft.com/en-us/windows/win32/shell/autoplay-reg#using-the-registry-to-disable-autorun>

Raspberry Robin

What is it?

- Malware dropper that sells initial access to compromised networks to ransomware groups and malicious actors.
- Has been seen deploying malware such as IcedID, Bumblebee, and Truebot

How does it work?

- Spreads to Windows systems through infected USB drives that contain a Windows shortcut (LNK) file disguised as a folder.
- Most recently, the file name has been brands of USB drives, but in earlier infections it used a generic name like *recovery.lnk*.
- Raspberry Robin uses both autorun to launch and social engineering to encourage users to click the LNK file

Prevention:

- Ensure autorun of removable media is disabled
- User awareness training

Detections:

- Attacker Technique - MSIEExec loading object via HTTP

Microsoft OneNote

Attachments to drop Payloads

Overview:

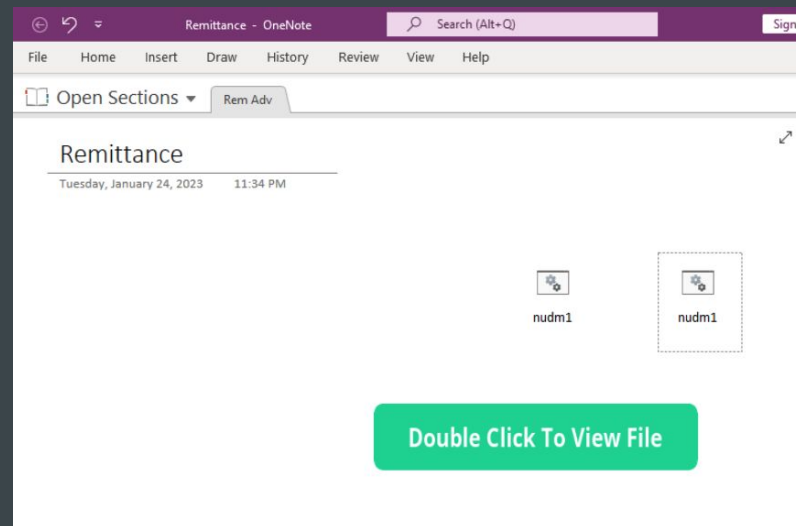
- Over the past month, attackers have been seen using Microsoft OneNote attachments to spread malware and password stealers. Most commonly through phishing emails.
- Malicious attachment is downloaded together with the '.one' file
- User is tricked into downloading and opening .one attachment > user is deceived by a "click to view content" button that loads the attachment > user gets warning sign about the risks of opening attachments (typically ignored) > if user selects "OK", the attached payload executes and acts as a downloader for the payload
- Rapid7 SOC is currently seeing this lead to ASYNCRAT and REDLINEINFOSTEALER

Prevention:

- Block .one at the perimeter or email gateway
- User awareness training

Resources:

- <https://www.rapid7.com/blog/post/2023/01/31/rapid7-observes-use-of-microsoft-onenote-to-spread-redline-infostealer-malware/>



Example of the OneNote file- once victim double clicks, it executes malicious payload "nudm1". This launches a malicious PowerShell command, to download an additional payload.

MFA

Let's review last year's R7 IR stats:

Rapid7 MDR Major Incident - Root Cause Stats YTD:

38% - No MFA on VPN/VDI/SaaS

We have seen, and are currently still seeing IRs involving VDI

- Citrix ADC, NetScaler, and VMware Horizon

Recommendations from our IR team:

Harden MFA to prevent push fraud: As attackers advance in the perpetual cat-and-mouse game, it's important our controls keep pace. Rapid7 MDR has observed an uptick in push fraud caused by notification fatigue.

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match>

Out-of-the-box Conditional Access Policy recommendations:

These are templates within AzureAD that can be applied without having to be built from scratch.

- [Secure security info registration](#)
- [Block legacy authentication](#)
- [Require MFA for administrators](#)
- [Require MFA for all users](#)
- [Require MFA for Azure management](#)
- [Require MFA for risky sign-in](#)
- [Require password change for risky users](#)
- [Require compliant or hybrid joined devices](#)
- [Block access by location](#) (Proceed with caution, especially with globally distributed organizations)

Further Recommendations for Implementing Phishing-Resistant MFA in Azure: <https://learn.microsoft.com/en-us/azure/active-directory/standards/memo-22-09-multi-factor-authentication>

Trending Vulnerabilities

VMware vRealize Log Insight




- VMware vRealize Log Insight Directory Traversal Vulnerability (CVE-2022-31706)
- VMware vRealize Log Insight broken access control Vulnerability (CVE-2022-31704)
 - CVSSv3 base score of 9.8.
 - An unauthenticated, malicious actor can inject files into the operating system of an impacted appliance which can result in remote code execution.
- VMware vRealize Log Insight contains a Deserialization Vulnerability (CVE-2022-31710)
 - CVSSv3 base score of 7.5.
 - An unauthenticated malicious actor can remotely trigger the deserialization of untrusted data which could result in a denial of service.
- **Affected Products**
 - VMware vRealize Log Insight
 - VMware Cloud Foundation (VMware vRealize Log Insight)
- [Fixed version 8.10.2](#)
- [Workaround Scripts KB90635](#)

Links: [VMWare Advisory](#)

CVE-2022-47966

Unauthenticated RCE vulnerability in multiple products

- ManageEngine  • [CVE-2022-47966](#) - This advisory addresses an unauthenticated remote code execution vulnerability reported and patched in the following ManageEngine products due to the usage of an outdated third party dependency, Apache Santuario.
- **Applicability:** This advisory is applicable only when SAML SSO is/was enabled in the ManageEngine setup.

Links: [ManageEngine](#) / [AttackerKB](#)