Threat actors strive to cause Tax Day headaches

By Microsoft Threat Intelligence

Published: 2023-04-13 · Archived: 2026-04-10 02:25:39 UTC

Threat actors often take advantage of current events and major news headlines to align attacks and leverage social engineering when people could be more likely to be distracted or misled. Tax season is particularly appealing to threat actors because not only are people busy and under stress, but it is intrinsically tied to financial information. With U.S. Tax Day approaching, Microsoft has observed phishing attacks targeting accounting and tax return preparation firms to deliver the Remcos remote access trojan (RAT) and compromise target networks beginning in February of this year.

Remcos, which stands for “Remote Control and Surveillance”, is a closed-source tool that allows threat actors to gain administrator privileges on Windows systems remotely. It was released in 2016 by BreakingSecurity, a European company that markets Remcos and other offensive security tools as legitimate software. In 2021, CISA listed Remcos among its top malware strains, citing its use in mass phishing attacks using COVID-19 pandemic themes targeting businesses and individuals.

While social engineering lures like this one are common around Tax Day and other big topic current events, these campaigns are specific and targeted in a way that is uncommon. The targets for this threat are exclusively organizations that deal with tax preparation, financial services, CPA and accounting firms, and professional service firms dealing in bookkeeping and tax. This campaign can be detected in Microsoft Defender Antivirus, built into Windows and on by default, as well as Microsoft 365 Defender.

The campaign uses lures masquerading as tax documentation sent by a client, while the link in the email uses a legitimate click-tracking service to evade detection. The target is then redirected to a legitimate file hosting site, where the actor has uploaded Windows shortcut (.LNK) files.

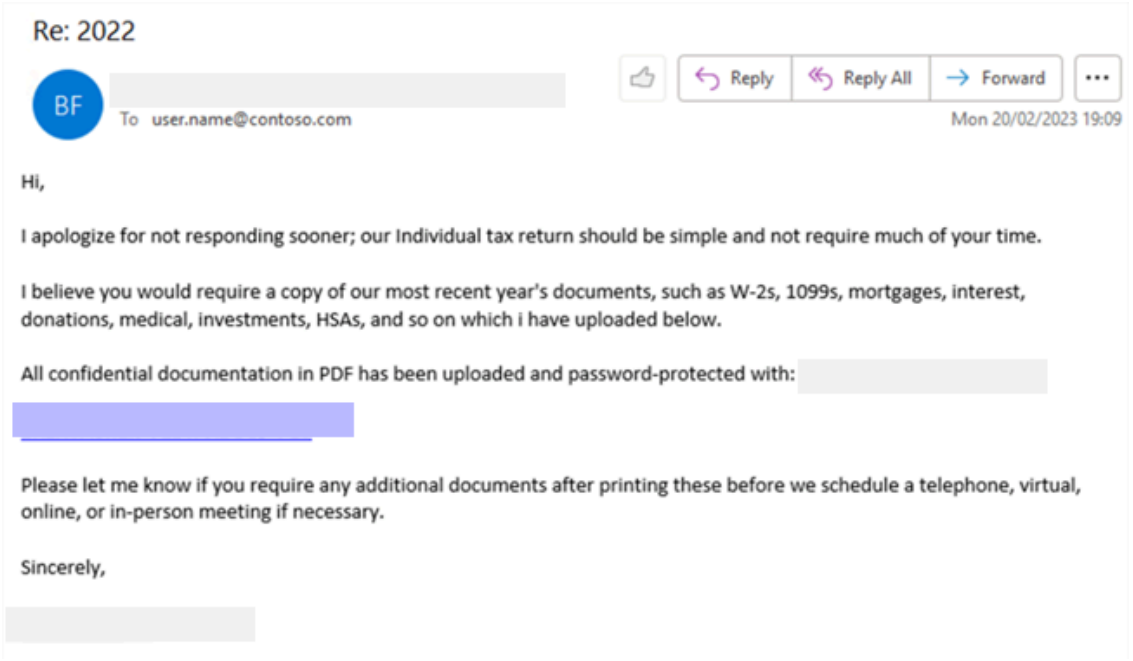

Figure 1. Remcos malware phishing lure

These LNK files generate web requests to actor-controlled domains and/or IP addresses to download malicious files. These malicious files then perform actions on the target device and download the Remcos payload, providing the actor potential access to the target device and network.

Microsoft is sharing this information along with detections and recommendations with the community to help users and defenders stay vigilant against this campaign with Tax Day approaching in the U.S. on April 18. Microsoft 365 Defender and Microsoft Defender Antivirus detect and block Remcos and other malicious activity related to this campaign.

Phishing campaign analysis

What we have observed is that the link in the phishing email points to Amazon Web Services click tracking service at *awstrack[.]me*. The initial link then redirects the target to a ZIP file hosted on legitimate file-sharing service *spaces[.]hightail[.]com*. The ZIP file contains LNK files that act as Windows shortcuts to other files. The LNK files make web requests to actor-controlled domains and

IP addresses to download additional malicious files such as MSI files containing DLLs or executables, VBScript files containing PowerShell commands, or deceptive PDFs.

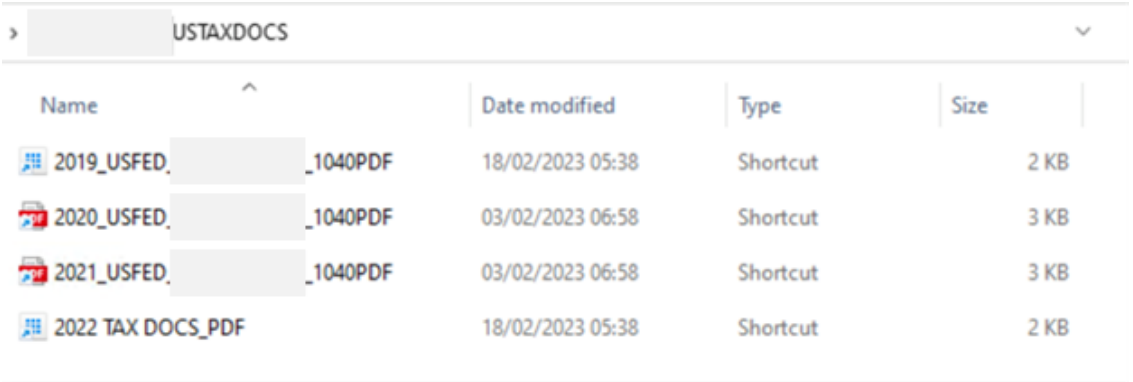

Figure 2. Unpacked file names referencing tax documents in the malware

In some cases, GuLoader was used to execute shellcode and subsequently download Remcos on the target system. GuLoader is a malicious downloader that has been used by many different actors to deliver a wide variety of malware, including several RATs such as Remcos, through phishing campaigns since it was first observed in the wild in December 2019. The downloader uses several techniques to evade analysis and detection such as using legitimate file-sharing sites and cloud hosting services for payload storage and delivery as well as encryption and obfuscation of the GuLoader shellcode and payloads.

Successful delivery of a Remcos payload could provide an attacker the opportunity to take control of the target device to steal information and/or move laterally through the target network.

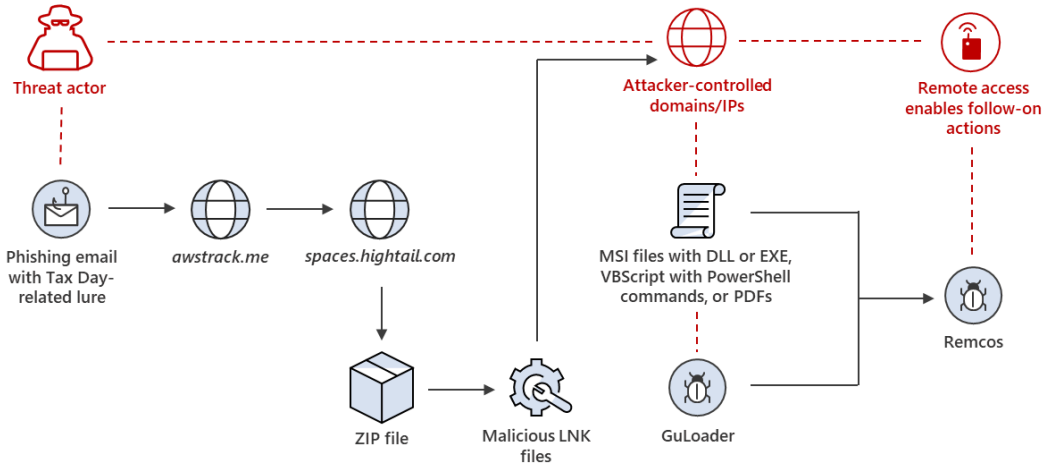

Figure 3. Tax Day-themed Remcos attack chain

We continue to learn from these campaigns to improve how we protect customers.

Recommendations and detections

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

- Block JavaScript or VBScript from launching downloaded executable content
- Block executable files from running unless they meet a prevalence, age, or trusted list criterion
- Enable Microsoft Defender Antivirus scanning of downloaded files and attachments
- Enable Microsoft Defender Antivirus real-time behavior monitoring

- Enable cloud-delivered protection

Detection details

Microsoft Defender for Office 365

Microsoft Defender for Office 365 detects phishing emails associated with the campaign discussed in this blog.

Microsoft Defender Antivirus

Microsoft Defender Antivirus, on by default on Windows machines, detects threat components as the following malware:

- Backdoor:Win32/Remcos.GA!MTB

Microsoft Defender for Endpoint

Alerts with the following titles in the security center can indicate threat activity on your network:

- 'Remcos' backdoor
- Suspicious 'Remcos' behavior
- 'Remcos' malware
- 'Guloader' malware

Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytic (a series of analytics all prefixed with "TI map") to automatically match the 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. More details on the Content Hub can be found here: https://learn.microsoft.com/azure/sentinel/sentinel-solutions-deploy

Indicators of compromise (IOCs)

Domain:
uymm[.]org

URL:
https[:]//uymm[.]org/roman.msi

SHA-256 hashes:
23597910ec60cf8b97144447c5cddd2e657d09e2f2008d53a3834b6058f36a41
95a2d34db66ce4507d05ac33bea3bdc054860d9d97e91bdc2ce7ce689ae06e9f
ac55905e6f5a2ab166f9a2ea7d1f4f68f5660f39b5c28b7746df1e9db6dd4430

References:

- 2021 Top Malware Strains | Cybersecurity and Infrastructure Security Agency (CISA)
- GuLoader: A Popular New VB6 Downloader that Abuses Cloud Services | Proofpoint US
- GuLoader: Peering Into a Shellcode-based Downloader | CrowdStrike

---