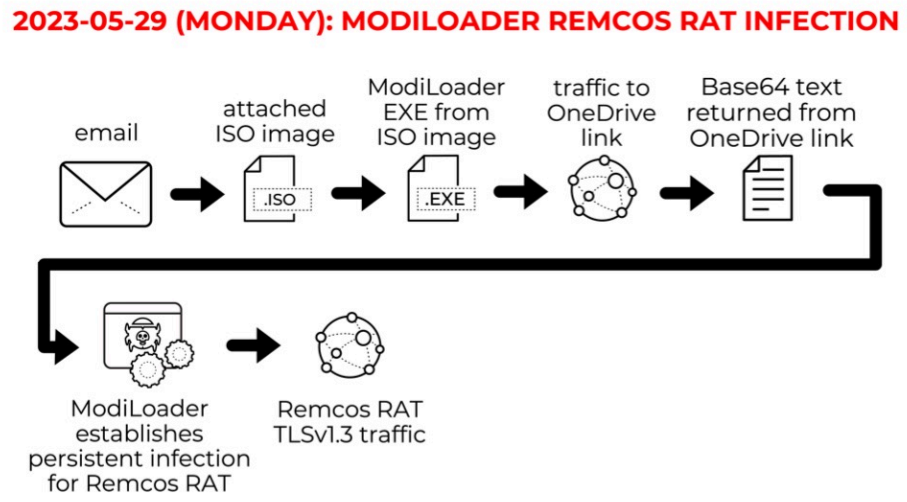
Malspam pushes ModiLoader (DBatLoader) infection for Remcos RAT

By SANS Internet Storm Center

Archived: 2026-04-05 18:48:21 UTC

Introduction

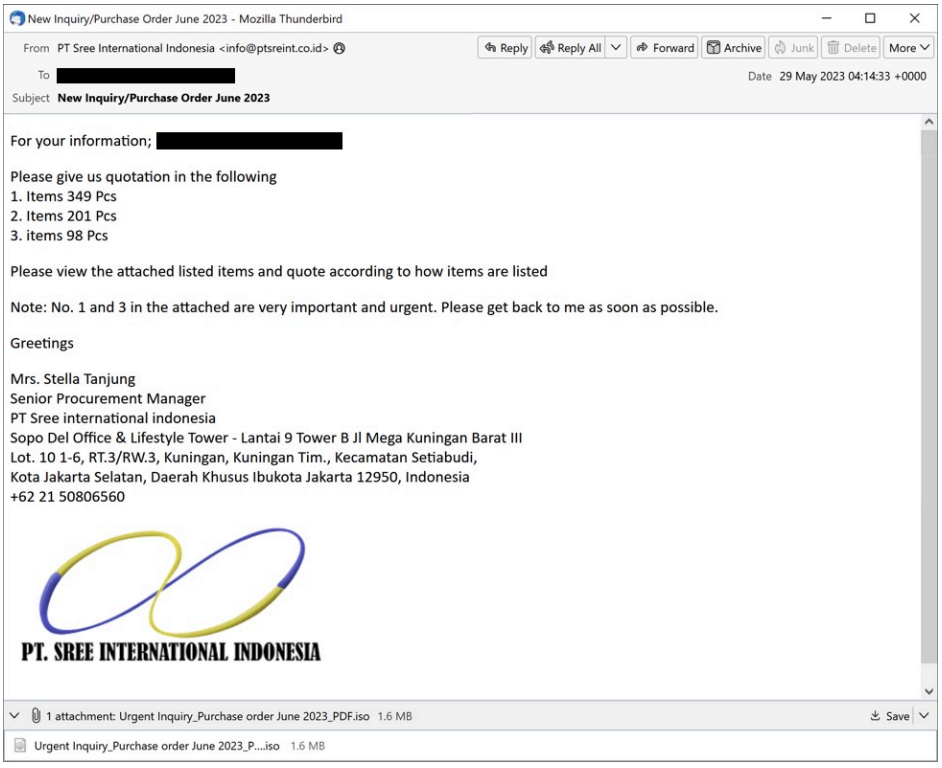
Also known as DBatLoader, ModiLoader is malware that retreives and runs payloads like Formbook, Warzone RAT, Remcos RAT, or other types of malware. Today's diary reviews a ModiLoader infection for Remcos RAT on Monday 2023-05-29.



Shown above: Flow chart for the ModiLoader Remcos RAT infection on Monday 2023-05-29.

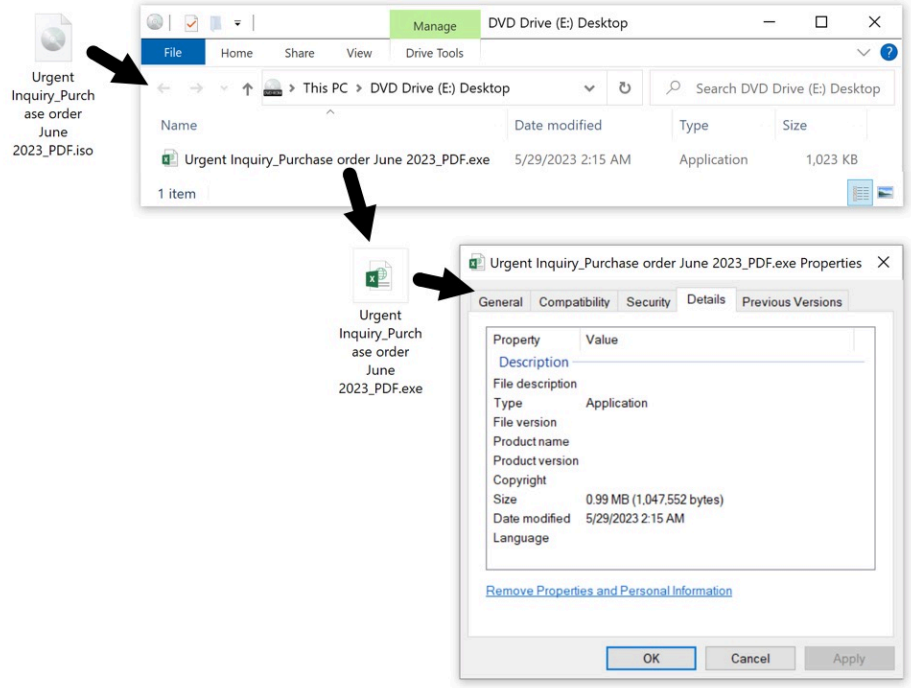
Email

I caught the email in one of my honeypot accounts on Monday 2023-05-29 at 4:14 UTC. These messages often spoof companies sending invoices or purchase orders. This campaign didn't appear to be specifically targeted at my honeypot account.



Shown above: Screenshot of the email distributing ModiLoader for Remcos RAT on Monday 2023-05-29.

The email contains an ISO image presented as a purchase order. The ISO image contains a Windows executable (EXE) file for ModiLoader. The EXE file icon impersonates an Excel spreadsheet.

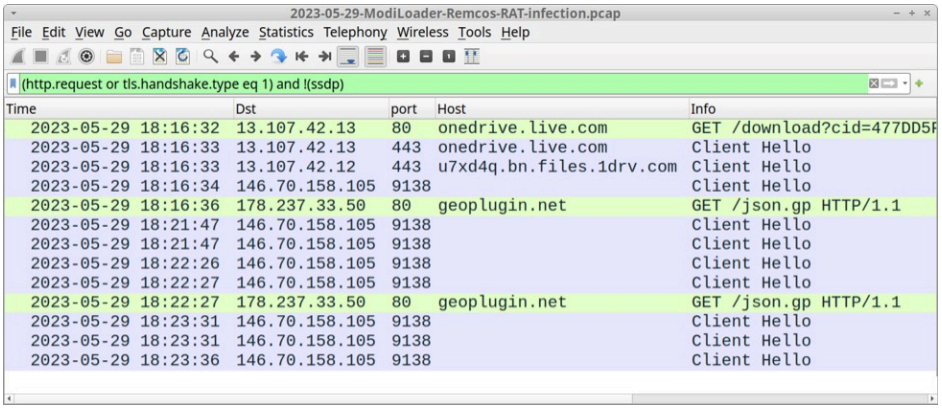


Shown above: The attached ISO image contains a malicious Windows EXE file for ModiLoader.

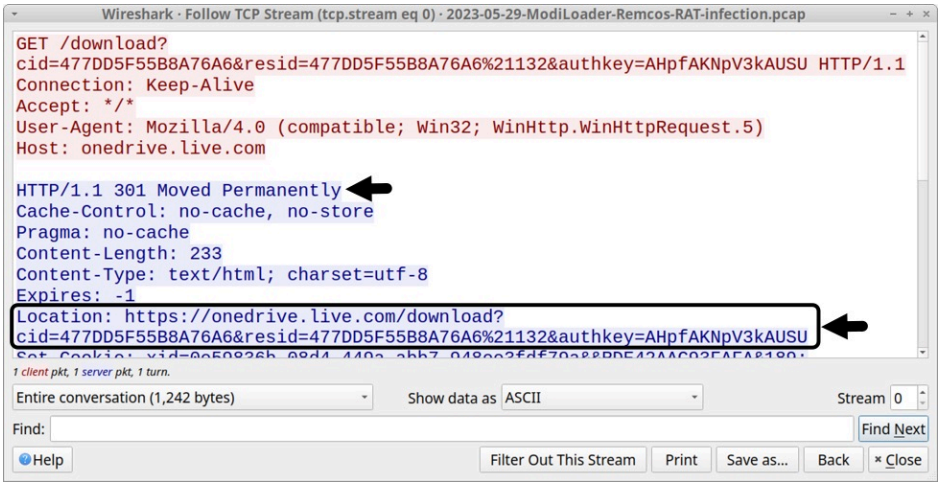
This ModiLoader EXE will infect a vulnerable Windows host with Remcos RAT. Let's look at the infection traffic.

Infection Traffic

The ModiLoader EXE first generated a OneDrive URL using HTTP over TCP port 80. This redirected to an HTTPS version of the same URL over TCP port 443.

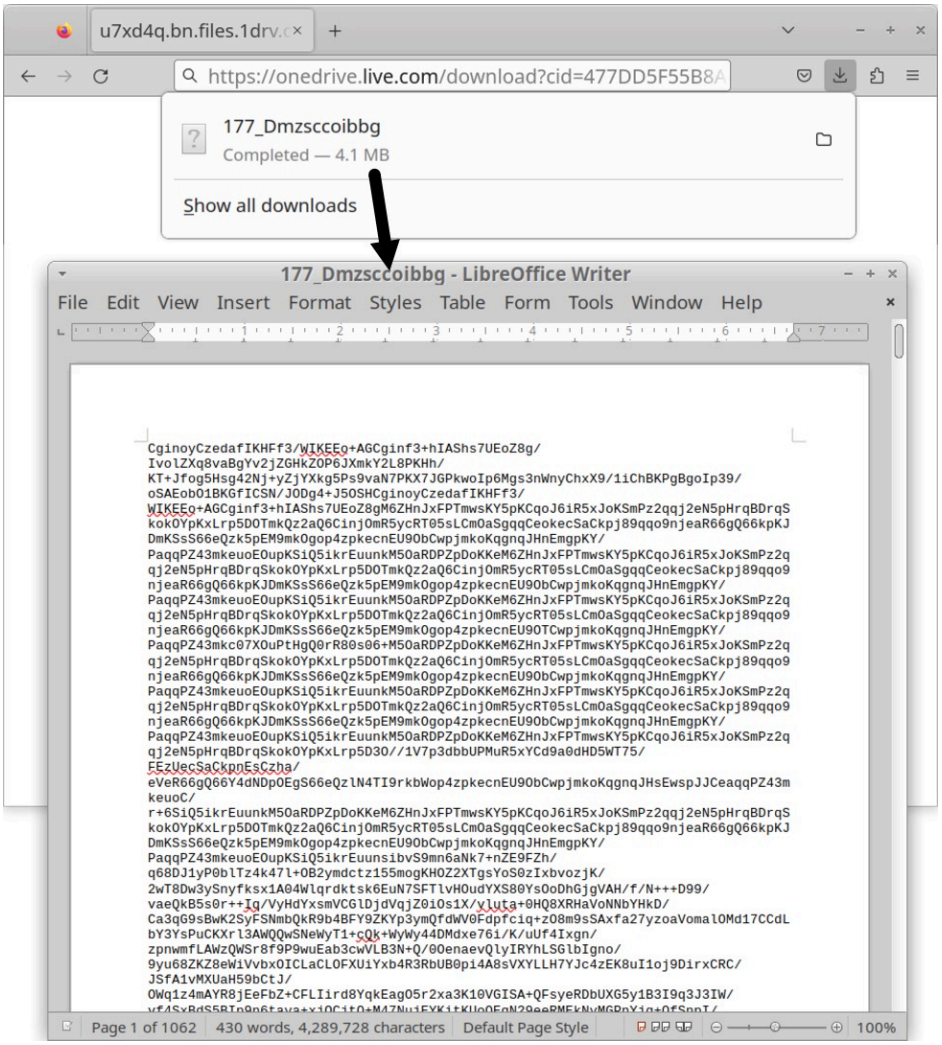


Shown above: Traffic from an infection filtered in Wireshark.



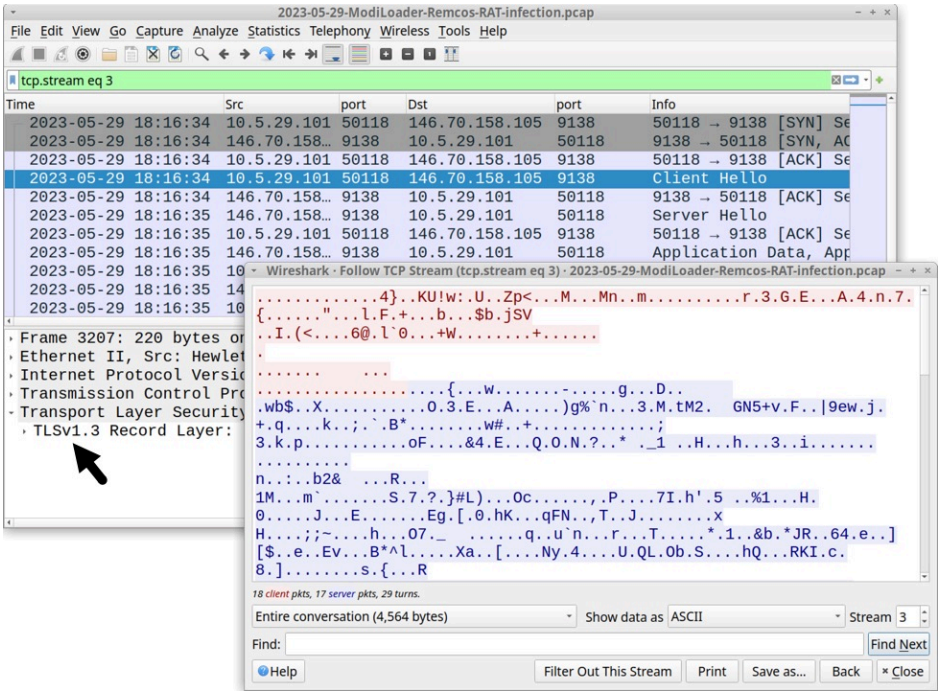
Shown above: Initial traffic generated by ModiLoader redirected to an HTTPS version of the same URL.

The OneDrive URL returned a base64 text file, approximately 4.3 MB in size. I retrieved a copy of it by entering the URL in a web brower.



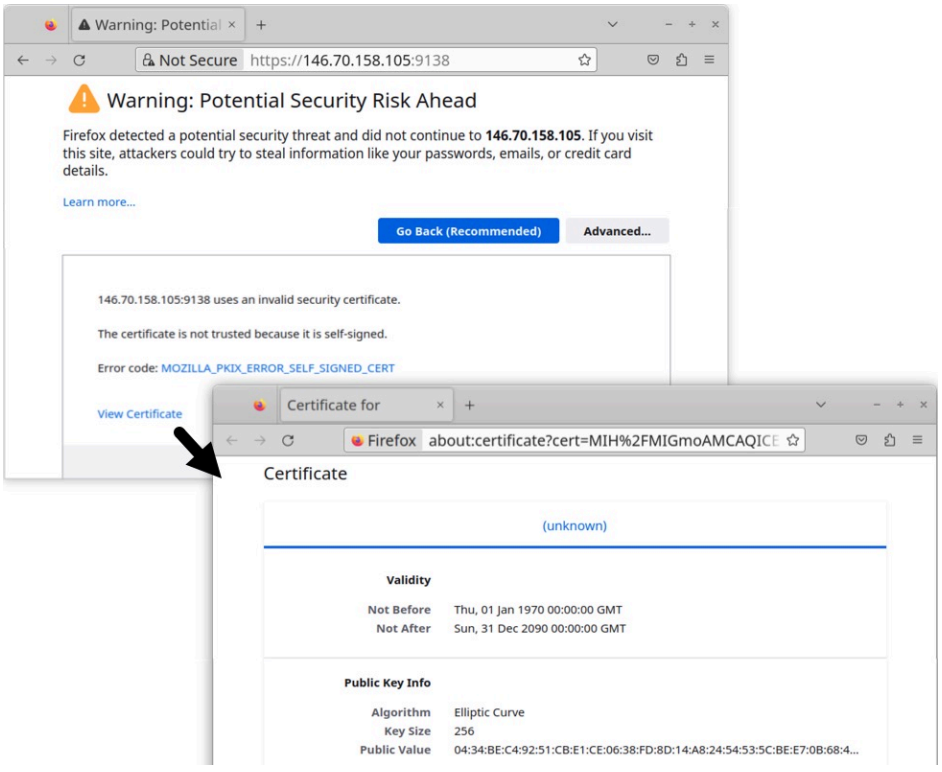
Shown above: Using a web browser to retrieve base64 text file returned from OneDrive URL generated by the ModiLoader EXE.

Shortly after ModiLoader retrieved the base64 text file, my infected host started generating TLSv1.3 infection traffic to a server at ***146.70.158[.]105*** over TCP port ***9138***. Online sandbox analysis indicates this is Remcos RAT traffic, so I'm calling ***146.70.158[.]105*** a Remcos RAT C2 server.



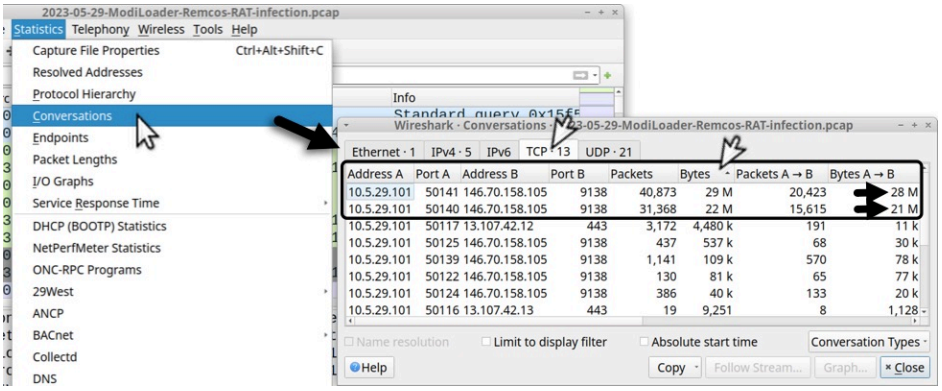
Shown above: Wireshark showing TLSv1.3 traffic from the infected Windows host.

No domain is associated with this Remcos RAT C2 server. Checking it in a web browser revealed the server used a self-signed certificate. No identification fields were used for this self-signed certificate.



Shown above: Info about self-signed certificate used for TLSv1.3 traffic to the Remcos RAT C2 server.

At least 49 MB of data was sent from the infected Windows host to the Remcos RAT C2 server, as shown below when viewing TCP conversation statistics of the traffic in Wireshark.

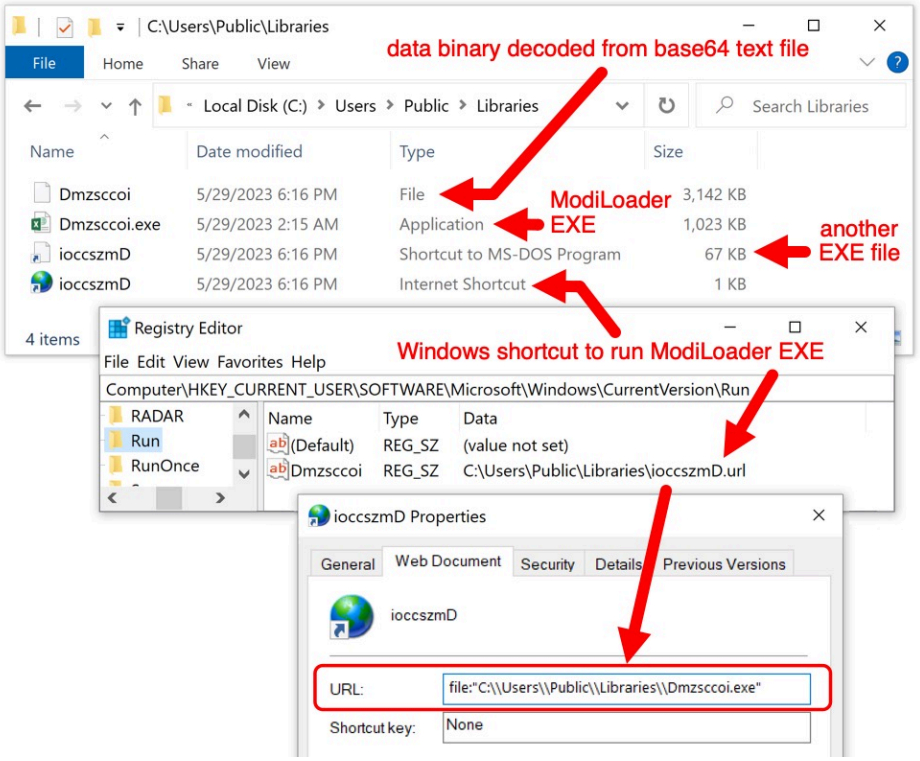


Shown above: TCP conversation statistics in Wireshark reveal the infected host sent at least 49 MB of data to the Remcos RAT C2 server.

The infected Windows host also checked its location using ***geoplugin.net,*** which is a legitimate service.

Forensics on the Infected Windows Host

This infection was made persistent through the Windows registry key at ***HKCU\sofware\Microsoft\Windows\CurrentVersion\Run***. Persistent files were stored in the host's ***C:\Users\Public\Libraries*** directory.



Shown above: ModiLoader/Remcos RAT files persistent on the infected Windows host.

Indicators of Compromise (IOCs)

Some headers from the email:

```
Return-Path: <william.cheng@foodicon[.]com[.]sg>
Received: from cp2-de1.host-global[.]net (cp2-de1.host-global[.]net [88.99.82[.]246])
    for <[recipient's email address]>; Mon, 29 May 2023 04:14:43 +0000 (UTC)
Received: from ec2-3-135-201-214.us-east-2.compute.amazonaws[.]com ([3.135.201[.]214]:55643)
    by cp2-de1.host-global[.]net with esmtpa (Exim 4.96)
    Mon, 29 May 2023 06:14:35 +0200
From: PT Sree International Indonesia <info@ptsreint[.]co[.]id>
Subject: New Inquiry/Purchase Order June 2023
Date: 29 May 2023 04:14:33 +0000
Message-ID: <20230529041433.6E03B75D7043B6B7@ptsreint[.]co[.]id>
```

Traffic from an infected Windows host:

- hxxp://onedrive.live[.]com/download?cid=477DD5F55B8A76A6&resid=477DD5F55B8A76A6%21132&authkey=AHpfAKNpV3kAUSU
- hxxps://onedrive.live[.]com/download?cid=477DD5F55B8A76A6&resid=477DD5F55B8A76A6%21132&authkey=AHpfAKNpV3kAUSU
- hxxps://u7xd4q.bn.files.1drv[.]com/y4mnljoeykY0rqANGppY0yGovJuGPFqCUKN1PI2BK5j71L0nAtxaBfppI5gHLhyPiXM3swFe-quRw1e41cGALOL4QoSWpyud0yDeU-ImxNuXWR9bIksaWiXsgL2UyTD2D2DtHZaxPuuqz7hy09zjLvcrr_HTTMA8fF4iRUQ1H6Bjm6lTFEK9eLm6t5M9xXenlHLDiE4qye22jg5SWedownload&psid=1
- ***146.70.158[.]105*** port ***9138*** - TLSv1.3 traffic for Remcos RAT
- hxxp://geoplugin.net/json.jp <-- IP address/location check of the infected host

Malware from the infected Windows host:

SHA256 hash: f69e25c8c6d512b60024504124d46cfbf08741bc7f53104466d1483f034a73e4

- File size: 1,638,400 bytes
- File name: Urgent Inquiry_Purchase order June 2023_PDF.iso
- File description: Email attachment, an ISO disk image containing DBatLoader/ModiLoader EXE

SHA256 hash: de33fd9d4c89f8d5ffad69cb7743922d8d22f54890f9ca69161edce001cba9ad

- File size: 1,047,552 bytes
- File name: Urgent Inquiry_Purchase order June 2023_PDF.exe
- Persistent file location: C:\Users\Public\Libraries\Dmzsccoi.exe
- File description: ModiLoader EXE
- Analysis: https://tria.ge/230529-vtyr7sdc5x/behavioral2
- Analysis: https://app.any.run/tasks/8f428a98-e2b5-49ae-a073-b4feb6c9f4ca
- Analysis: https://capesandbox.com/submit/status/393224/
- Reference: https://malpedia.caad.fkie.fraunhofer.de/details/win.dbatloader

SHA256 hash: 1d863f9486cef770383b16ed95763abe222b702dafad4e529793288c83fff52f

- File size: 4,289,728 bytes
- File description: Base64 text file retrieved from OneDrive URL generated by ModiLoader malware
- File location: hxxps://onedrive.live[.]com/download?cid=477DD5F55B8A76A6&resid=477DD5F55B8A76A6%21132&authkey=AHpfAKNpV3kAUSU

SHA256 hash: a2796cc5deaca203fd9c1ed203517c74b8fd516619cd0ded67551f727498dcb3

- File size: 3,217,294 bytes
- File location: C:\Users\Public\Libraries\Dmzsccoi
- File description: Data binary decoded from above base64 text file

SHA256 hash: 13ad5aa8c9424fd866ea5b5ed6f603983c626f60cdb5b680c98cd046174b4667

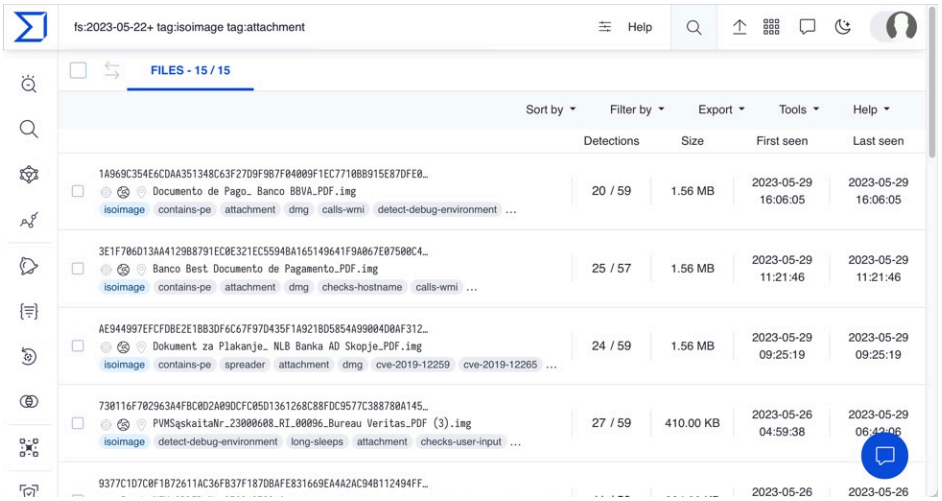
- File size: 100 bytes
- File location: C:\Users\Public\Libraries\ioccszmD.url
- File description: URL file persistent through Windows registry
- URL file target: C:\\Users\\Public\\Libraries\\Dmzsccoi.exe

SHA256 hash: 7bcdc2e607abc65ef93afd009c3048970d9e8d1c2a18fc571562396b13ebb301

- File size: 68,096 bytes
- File location: C:\Users\Public\Libraries\ioccszmD.pif
- File description: Another Windows EXE used for this infection

Final Words

This example of ModiLoader/Remcos RAT was not targeted, nor was it particularly sophisticated. Emails using ISO attachments to deliver malware are routinely submitted to VirusTotal. I did a quick search for the last week of ISO attachments in VirusTotal, and I found 15 examples.



Shown above: Results of a search for ISO attachments from emails submitted to VirusTotal from 2023-05-22 until the date of this diary.

A sanitized copy of the email, along with malware/artifacts from the infection, and a packet capture (pcap) of the infection traffic are available here.

Brad Duncan
brad [at] malware-traffic-analysis.net
