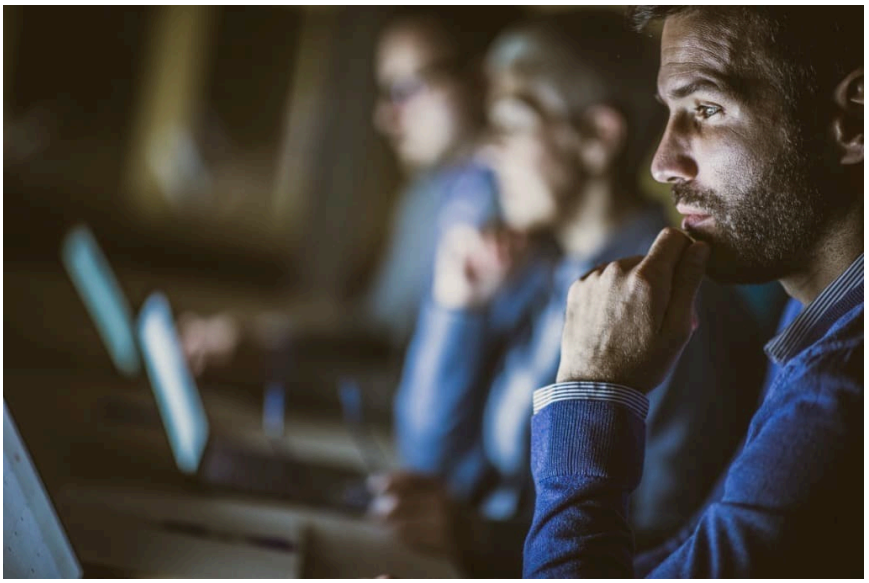
Title: DarkGate Loader delivered via Teams - Truesec

By siteadmin

Published: 2023-09-06 · Archived: 2026-04-05 14:53:17 UTC

DarkGate Loader Malware Delivered via Microsoft Teams

Malspam campaigns involving DarkGate Loader have been on the rise since its author started advertising it as a Malware-as-a-Service offering on popular cybercrime forums in June 2023. Until now DarkGate Loader was seen delivered via traditional email malspam campaigns similar to those of Emotet. In August an operator started using Microsoft Teams to deliver the malware via HR-themed social engineering chat messages.



Investigating the Senders

Using Microsoft Purview's eDiscovery tool we searched for the senders (participants) in Microsoft Teams.

The senders of the external Microsoft Teams chat messages were identified as "Akkaravit Tattamanas" (63090101@my.buu.ac.th) and "ABNER DAVID RIVERA ROJAS" (adriverar@unadvirtual.edu.co). Truesec Threat Intelligence confirmed the accounts were compromised via an unknown malware and put up for sale on the Dark Web in August 2023.

Using AADInternal's OSINT tool, we could gather more information on the O365 tenant to which the accounts belong and use the listed domains to search for additional messages.

Figure 1: Screenshot from AADInternal's OSINT tool with the sender's O356 tenant details.

HR-Themed Social Engineering Lure

Both senders had an identical-sounding message with a link to an externally hosted file, "Changes to the vacation schedule.zip" (hosted on the senders SharePoint sites).

Figure 2: Screenshot of one of the MS Teams chat messages.

The SharePoint URLs hosting the remote attachment can be seen in the figure below.

Figure 3: URLs to the SharePoint sites hosting the remote ZIP file.

Downloading the Malware

Clicking the URL would take the victim to the SharePoint sites where the file “Changes to the vacation schedule.zip” could be downloaded.

Figure 4: Screenshot of a SharePoint site hosting the file “Changes to the vacation schedule.zip.”

The file was later identified by Microsoft Defender as malware “BAT/Tisifi.A#”.

Figure 5: Screenshot of MS Defender detecting the file as malicious.

Analyzing the Malicious Files

Using a combination of static and dynamic malware analysis our goal was to identify the final payload delivered in the campaign.

The ZIP file contains a malicious LNK file (shortcut) posing as a PDF document: “Changes to the vacation schedule.pdf.lnk.”

Figure 6: Screenshot of the extracted LNK file as shown in File Explorer.

Using Eric Zimmerman’s “LECmd.exe” to analyze the malicious LNK file, we can extract the command line it would execute upon opening.

Figure 7: Screenshot of the command executed after opening the LNK file.

The execution of the VBScript file in C:tgphasrxmp.vbs triggers the download and execution of the file hXXp://5[.]188[.]87[.]58:2351/wbzadczl

Figure 8: Wireshark trace of the VBScript file download.

The commands make use of a Windows version of cURL (renamed to wbza) to download and execute Autoit3.exe and the bundled script eszexz.au3. The pre-compiled AutoIT script hides the code in the middle of the file by looking for the magic bytes 0x4155332145413036 (AU3!EA06).

Figure 9: Screenshot of the bundled AutoIT script file.

Upon executing the script, AutoIT drops a new file that contains shellcode, and before execution, it makes a check to see if Sophos antivirus is installed.

Figure 10: The deobfuscated AutoIT script showing a check for Sophos antivirus.

If Sophos is not installed, additional code in the AutoIT script is deobfuscated to launch the shellcode.

Figure 11: Screenshot of AutoIT shellcode execution.

When the shellcode is run, the first thing it does is load “byte by byte.” This technique is called stacked strings, to create a new file. It can be seen in the figure below that the first bytes of the created file are 0x4d and 0x5a, which indicates a Windows executable.

Figure 12: Screenshot from Ghidra showing the shellcode’s use of stack strings to load a new Windows executable.

The payload could then be extracted from memory and analyzed with PE Studio from www.winitor.com:

Figure 13: Screenshot from PE Studio showing technical details about the payload.

The payload was identified as “DarkGateLoader” on VirusTotal. After the identification of the malware, we found an excellent writeup from Deutsche Telekom CERT and used their config extractor on the AutoIT script file “eszexz.au3” to extract the DarkGate malware’s configuration:

Figure 14: Configuration extracted from the DarkGate malware.

Further reading on the DarkGate Loader and DarkGate malware capabilities:

https://github.security.telekom.com/2023/08/darkgate-loader.html

https://0xtoxin.github.io/threat%20breakdown/DarkGate-Camapign-Analysis/

Recommendations

This attack was detected due to the security awareness training of the recipients. Unfortunately, current Microsoft Teams security features such as Safe Attachments or Safe Links was not able to detect or block this attack. Right now, the only way to prevent this attack vector within Microsoft Teams is to only allow Microsoft Teams chat requests from specific external domains, albeit it might have business implications since all trusted external domains need to be whitelisted by an IT administrator.
More on how these settings can be activated and used can be found here:
https://learn.microsoft.com/en-us/microsoftteams/trusted-organizations-external-meetings-chat?tabs=organization-settings

Indicators of Compromise

Filename	**SHA256 Hash**
Changes to the vacation schedule.zip	0c59f568da43731e3212b6461978e960644be386212cc448a715dbf3f489d758
Changes to the vacation schedule.pdf.lnk	bcd449470626f4f34a15be00812f850c5e032723e35776fb4b9be6c7be6c8913
c:tgphasrxpm.vbs	4c21711de81bb5584d35e744394eed2f36fef0d93474dfc5685665a9e159eef1
c:wbzaeszexz.au3	1bcde4d4613f046b63e970aa10ea2662d8aa7d326857128b59cb88484cce9a2d

A similar file with the same filename, “Changes to the vacation schedule.zip,” and behavior (but with a different hash) is available on VirusTotal:
https://www.virustotal.com/gui/file/09904d65e59f3fbbbf38932ae7bff9681ac73b0e30b8651ec567f7032a94234f.

URLs
hXXps://burapha-my[.]sharepoint[.]com/:u:/g/personal/63090101_my_buu_ac_th/EWkB0l3nR4dCjDmwAe7jb7kBWPPkDObt8wVbmB1O6UztmA
hXXps://unadvirtualedu-my[.]sharepoint[.]com/personal/adriverar_unadvirtual_edu_co/Documents/Microsoft%20Teams%20Chat%20Files/Changes%20to%20the%20vacati
hXXp://5[.]188[.]87[.]58:2351/wbzadczl
hXXp:// 5[.]188[.]87[.]58:2351/msiwbzadczl

Command & Control Server
hXXp://5[.]188[.]87[.]58:2351

Compromised Email Addresses
63090101@my.buu.ac.th
adriverar@unadvirtual.edu.co

Stay ahead with cyber insights

Newsletter

Stay ahead in cybersecurity! Sign up for Truesec's newsletter to receive the latest insights, expert tips, and industry news directly to your inbox. Join our community of professionals and stay informed about emerging threats, best practices, and exclusive updates from Truesec.
