Cyber Risk

lun., oct. 9, 2023

Microsoft Teams Used as Initial Access for DARKGATE Malware

George Glass

Ryan Hicks

Key Takeaways

- Kroll has observed DARKGATE malware being delivered to users through files shared in Microsoft Teams messages.
- These campaigns have targeted the transportation and hospitality sectors.
- Files hosted to public SharePoint sites were downloaded and executed by victims, which led to batch scripts copying the AutoIT interpreter and scripts from adversary-controlled infrastructure.
- The DARKGATE payload was injected into a running process and further AutoIt scripts were created and used for persistence in the user's Start Menu.
- This appears to be part of a wider DARKGATE campaign, also reported across open-source.
- This continues a surge of Microsoft Teams-related social engineering observed since Q2 2023, following the identification of a vulnerability in Teams that relies on organizational

Summary

Kroll has observed an uptick in cases of DARKGATE malware being delivered through Microsoft Teams messages. These campaigns have mainly targeted organizations in the transportation and hospitality sectors. This activity has also been reported throughout open-source reporting, sharing a number of key indicators with Kroll observations, such as common filenames, adversary infrastructure and similar domain name conventions to host the initial download.

Kroll observed that the file was hosted on a public SharePoint site and was initially delivered to several victims via Microsoft Teams messages. The file that was hosted on this site and downloaded by the victim was "**C_onfidential Sign_ificant Company Changes[.]zip**", which appears to be part of a generic list of lure filenames for this campaign. Other examples of filenames observed both by Kroll and open-source reporting include "**Vacation schedule[.]zip**", "**Reduction of employees[.]zip**" and "**Repair[.]zip**". Both the filenames themselves—and the fact that they have been observed across multiple cases—leads us to assess that the lures are almost certainly part of a generic preset list of lures, rather than targeted social engineering specifically towards the victim organization.

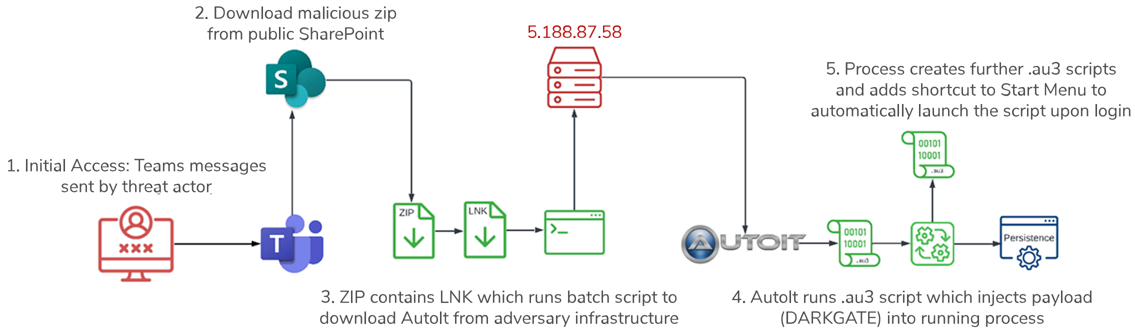

2. Download malicious zip from public SharePoint
5.188.87.58
5. Process creates further .au3 scripts and adds shortcut to Start Menu to automatically launch the script upon login
1. Initial Access: Teams messages sent by threat actor
ZIP
LNK
AUTOIT
00101 10001 .au3
Persistence
3. ZIP contains LNK which runs batch script to download AutoIt from adversary infrastructure
4. AutoIt runs .au3 script which injects payload (DARKGATE) into running process

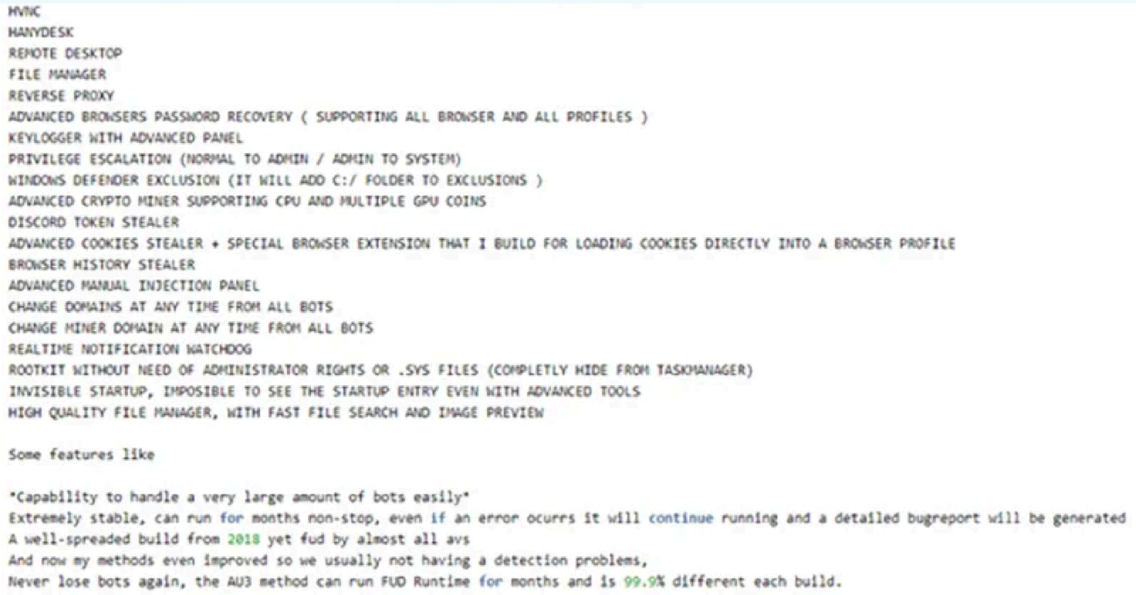
Figure 1 – DARKGATE Attack Chain

DARKGATE Attack Chain

curl executable to download the legitimate AutoIt script interpreter and a malicious AutoIt script from the IP: 5[.]188[.]87[.]58. This script injected a payload into legitimate processes already in memory, which was identified as DARKGATE. After the code was injected, the target process would create an AutoIT script that was unique to each host. It also created a shortcut in the user's Start Menu to automatically launch the script on each login. This allows for persistence across user sessions.

What is DARKGATE?

DARKGATE is a Windows-based malware that has capabilities ranging from cryptocurrency mining, file encryption, credential stealing and remote access to victim endpoints. It was first publicly reported in 2018; however, the author made a post in May 2023 stating they have decided to rent out the malware for a daily ($333), monthly ($10,000) or lifetime ($100,000) subscription fee. In the post, they list the extensive suggested features of the malware, which identifies its full suite of capabilities, from keylogging and privilege escalation to bot and file management. A full list of these can be found in Figure 2.



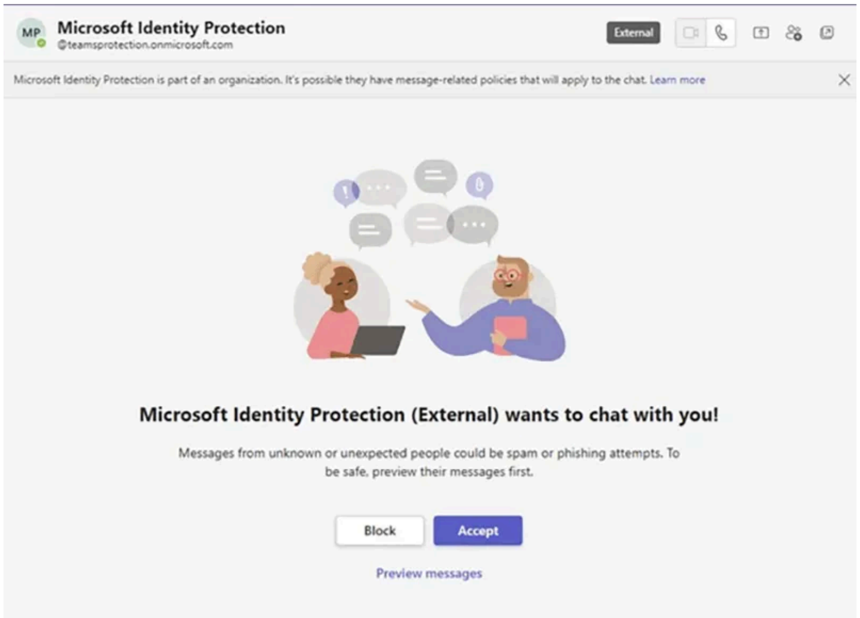
```
HVNC
HANYDESK
REMOTE DESKTOP
FILE MANAGER
REVERSE PROXY
ADVANCED BROWSERS PASSWORD RECOVERY ( SUPPORTING ALL BROWSER AND ALL PROFILES )
KEYLOGGER WITH ADVANCED PANEL
PRIVILEGE ESCALATION (NORMAL TO ADMIN / ADMIN TO SYSTEM)
WINDOWS DEFENDER EXCLUSION (IT WILL ADD C:/ FOLDER TO EXCLUSIONS )
ADVANCED CRYPTO MINER SUPPORTING CPU AND MULTIPLE GPU COINS
DISCORD TOKEN STEALER
ADVANCED COOKIES STEALER + SPECIAL BROWSER EXTENSION THAT I BUILD FOR LOADING COOKIES DIRECTLY INTO A BROWSER PROFILE
BROWSER HISTORY STEALER
ADVANCED MANUAL INJECTION PANEL
CHANGE DOMAINS AT ANY TIME FROM ALL BOTS
CHANGE MINER DOMAIN AT ANY TIME FROM ALL BOTS
REALTIME NOTIFICATION WATCHDOG
ROOTKIT WITHOUT NEED OF ADMINISTRATOR RIGHTS OR .SYS FILES (COMPLETLY HIDE FROM TASKMANAGER)
INVISIBLE STARTUP, IMPOSIBLE TO SEE THE STARTUP ENTRY EVEN WITH ADVANCED TOOLS
HIGH QUALITY FILE MANAGER, WITH FAST FILE SEARCH AND IMAGE PREVIEW

Some features like

*Capability to handle a very large amount of bots easily*
Extremely stable, can run for months non-stop, even if an error ocurrs it will continue running and a detailed bugreport will be generated
A well-spreaded build from 2018 yet fud by almost all avs
And now my methods even improved so we usually not having a detection problems,
Never lose bots again, the AU3 method can run FUD Runtime for months and is 99.9% different each build.
```

Figure 2 - DARKGATE Author Post Extract

Microsoft Teams Used for Initial Access

Although it is not fully understood how the threat actor in this campaign delivered the initial Teams messages to victims, there has been reporting on how initial access could be achieved using Teams since Q2 2023. This led to the tool “TeamsPhisher” being released on Github, which operationalizes sending attachments to victims on Teams on a larger scale. The tool combines ideas from JUMPSEC's researchers, techniques from Andrea Santese and authentication functions from Bastian Kanbach's “TeamsEnum” tool. The tool verifies target users' ability to receive external messages, then creates a new thread and sends the victim a message with a SharePoint attachment link. TeamsPhisher requires a Microsoft Business account with valid Teams and SharePoint licenses, and it offers features like preview mode, secure file links, delay specification and logging. It is therefore likely that the threat actor behind the ongoing DARKGATE campaign is utilizing a similar tool to TeamsPhisher to facilitate initial access.

attachments to victims, which ultimately led to JSSLOADER and additional post-compromise tooling. Furthermore, in August 2023, Microsoft reported that "Midnight Blizzard," also known as APT29, expanded their social engineering techniques by sending victims a Teams message request masquerading as technical support or the organization's security team (Figure 3). If accepted, this could lead to attempts to steal multi-factor authentication (MFA) tokens from the victim, and grant access to the account (assuming previous credentials were accessed by the actor).



Microsoft Identity Protection
@teamsprotection.onmicrosoft.com

Microsoft Identity Protection is part of an organization. It's possible they have message-related policies that will apply to the chat. Learn more

Microsoft Identity Protection (External) wants to chat with you!

Messages from unknown or unexpected people could be spam or phishing attempts. To be safe, preview their messages first.

Figure 3 - Midnight Blizzard (APT29) Teams Social Engineering

Teams-related phishing has seen a surge in recent months, with the DARKGATE campaign being the latest in successful social engineering that Kroll has observed. But, this is not just limited to DARKGATE; rather, the emergence of publicly available tooling has made this vector widely accessible to any threat actor that currently uses, or plans to use, social engineering as an initial access vector against an organization.

Key Recommendations

- If external access is required, it is recommended to review the Teams security settings to only allow communication from domains on an allow-list.
- Provide security awareness training to employees on the potential risks of opening files or interacting with unknown senders through Microsoft Teams.

Cyber and Data Resilience

Incident response, digital forensics, breach notification, security strategy, managed security services, discovery solutions, security transformation.

Cyber Threat Intelligence

Threat intelligence are fueled by frontline incident response intel and elite analysts to effectively hunt and respond to threats.

Malware Analysis and Reverse Engineering

24x7 Incident Response

Kroll is the largest global IR provider with experienced responders who can handle the entire security incident lifecycle.

Business Email Compromise (BEC) Response and Investigation

In a business email compromise (BEC) attack, fast and decisive response can make a tremendous difference in limiting financial, reputational and litigation risk. With decades of experience investigating BEC scams across a variety of platforms and proprietary forensic tools, Kroll is your ultimate BEC response partner.

Ransomware Preparedness Assessment

Kroll's ransomware preparedness assessment helps your organization avoid ransomware attacks by examining 14 crucial security areas and attack vectors.

Stop cyberattacks. Kroll Responder managed detection and response is fueled by seasoned IR experts and frontline threat intelligence to deliver unrivaled response.

Managed Security Services

World-renowned cyber investigators and leading technology fuel Kroll's managed security services, augmenting security operations centres and incident response capabilities.

News >

Press Release

Kroll Appoints Katherine Keefe to Lead Global Cyber Insurance Industry Capabilities

octobre 18, 2024

Press Release

Kroll Becomes Relativity Gold Provider Partner

septembre 19, 2024

Kroll Recognized in 2024 Gartner Market Guide for Digital Forensics and Incident Response Retainer Services for the Fifth Consecutive Year

septembre 12, 2024

Press Release

Kroll Expands AI Risk Consulting Services

août 27, 2024

Kroll is headquartered in New York with offices around the world.

One World Trade Center
285 Fulton Street, 31st Floor
New York NY 10007

+1 212 593 1000

Accessibility
Cookies
Disclosure
Modern Slavery Statement
Licensing

Code of Conduct
Data Privacy Framework
Kroll Ethics Hotline
Privacy Policy