BattleRoyal, DarkGate Cluster Spreads via Email and Fake Browser Updates

proofpoint.com/us/blog/threat-insight/battleroyal-darkgate-cluster-spreads-email-and-fake-browser-updates

December 20, 2023

Blog

Threat Insight

BattleRoyal, DarkGate Cluster Spreads via Email and Fake Browser Updates

Share with your network!

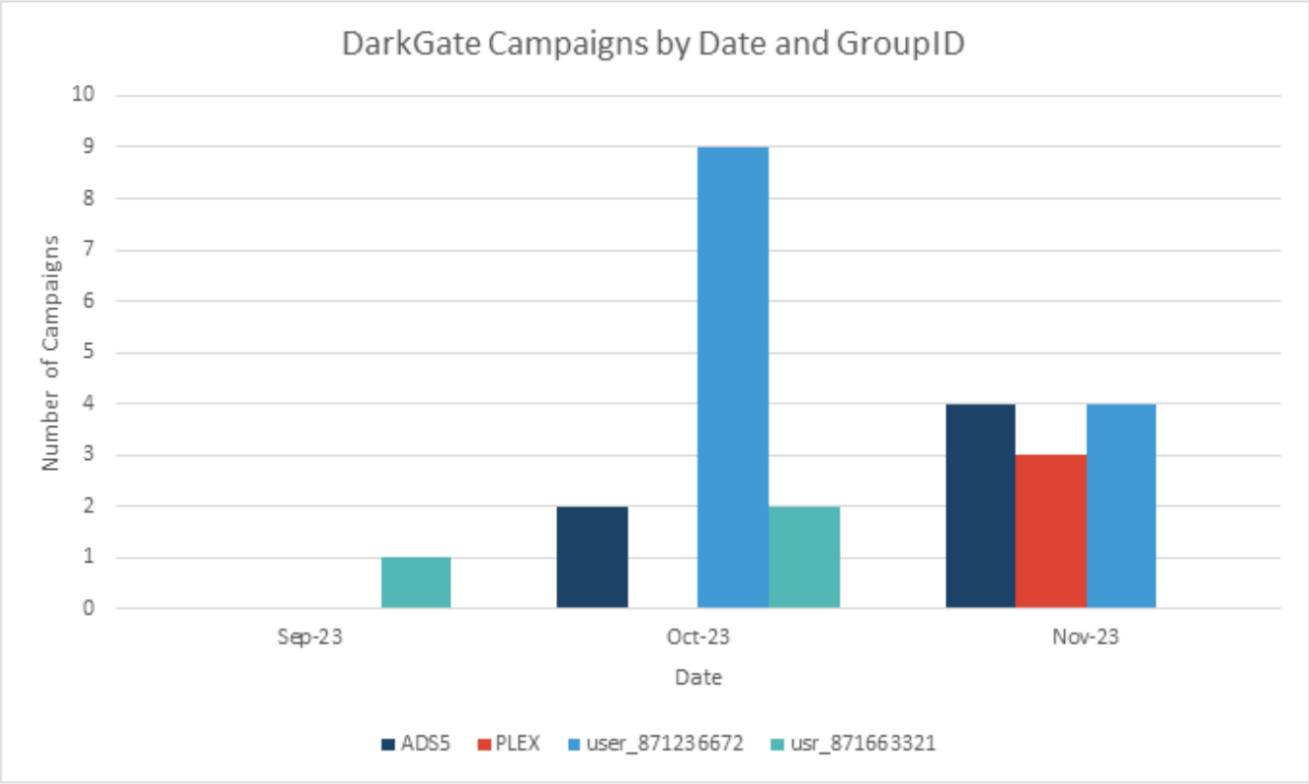
December 21, 2023 Axel F, Dusty Miller, Tommy Madjar and Selena Larson

Overview

Throughout the summer and fall of 2023, DarkGate entered the ring competing for the top spot in the remote access trojan (RAT) and loader category. It was observed in use by multiple cybercrime actors and was spread via many methods such as email, Microsoft Teams, Skype, malvertising and fake updates.

Proofpoint researchers are tracking a particularly interesting operator of the DarkGate malware. At the time of publication, researchers are not attributing this cluster of activity to a known threat actor and are temporarily calling it BattleRoyal. Between September and November 2023, at least 20 email campaigns used DarkGate malware with GroupIDs “PLEX”, “ADS5”, “user_871236672” and “usr_871663321”. The GroupID is a configuration setting that is also referred to as username, botnet, campaign, or flag 23. The campaigns are notable for:

- **Delivery:** via email and RogueRaticate fake browser updates
- **Volumes and geography:** email campaigns include tens of thousands of emails targeting dozens of industries primarily in USA and Canada
- **Attack chain:** includes a variety of notable tools such as 404 TDS, Keitaro TDS, and .URL files exploiting CVE-2023-36025



Volume of DarkGate campaigns based on four GroupIDs discussed in this report.

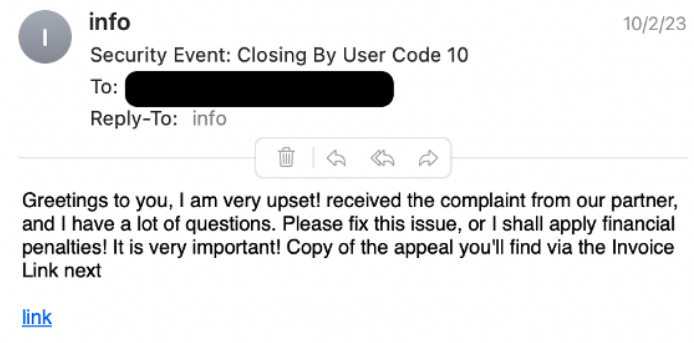
TDS all the things! (an email campaign example)

On October 2, 2023, Proofpoint identified one of the first campaigns in this cluster. It was notable due to the use of more than one traffic delivery system (TDS), specifically 404 TDS and Keitaro TDS. Additionally, the .URL files involved exploited CVE-2023-36025, a vulnerability in Windows SmartScreen. While other parts of the attack chain from this actor changed or varied, .URL files were involved in every campaign.

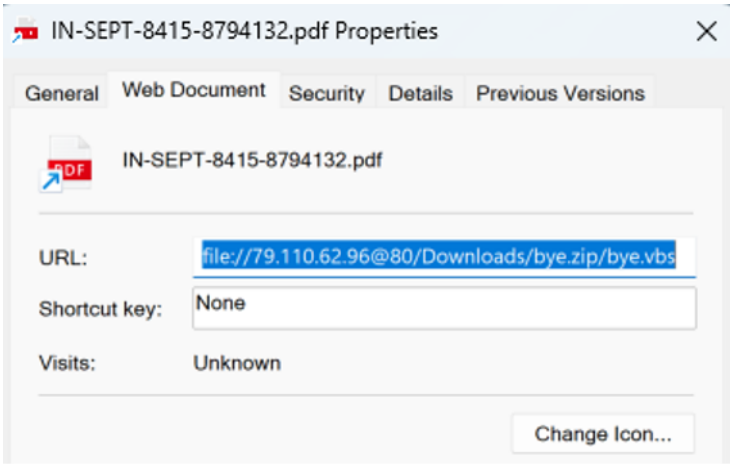
The emails in this campaign contained:

- 404 TDS URLs that, if clicked by the user, redirected to Keitaro TDS
- Keitaro TDS was observed serving an internet shortcut (.URL) file
- The internet shortcut, if double clicked, downloaded a zipped VBS script
- The VBS in turn downloaded and executed several shell commands (cmd.exe)
- The shell commands (a) created a directory on C: drive, (b) copied curl.exe from system folder to this new directory, (c) used the curl to download Autoit3.exe, (d) used curl to download and save an AutoIT script, and (e) ran the downloaded AutoIT script with the downloaded AutoIT interpreter
- The AutoIT script ran an embedded DarkGate

Attack chain summary that follows the flow of: Email > 404 TDS > Keitaro TDS > .URL > .VBS > Shell commands > AutoIT / AutoIT script > DarkGate.



Screenshot of an example email from October 2 campaign.

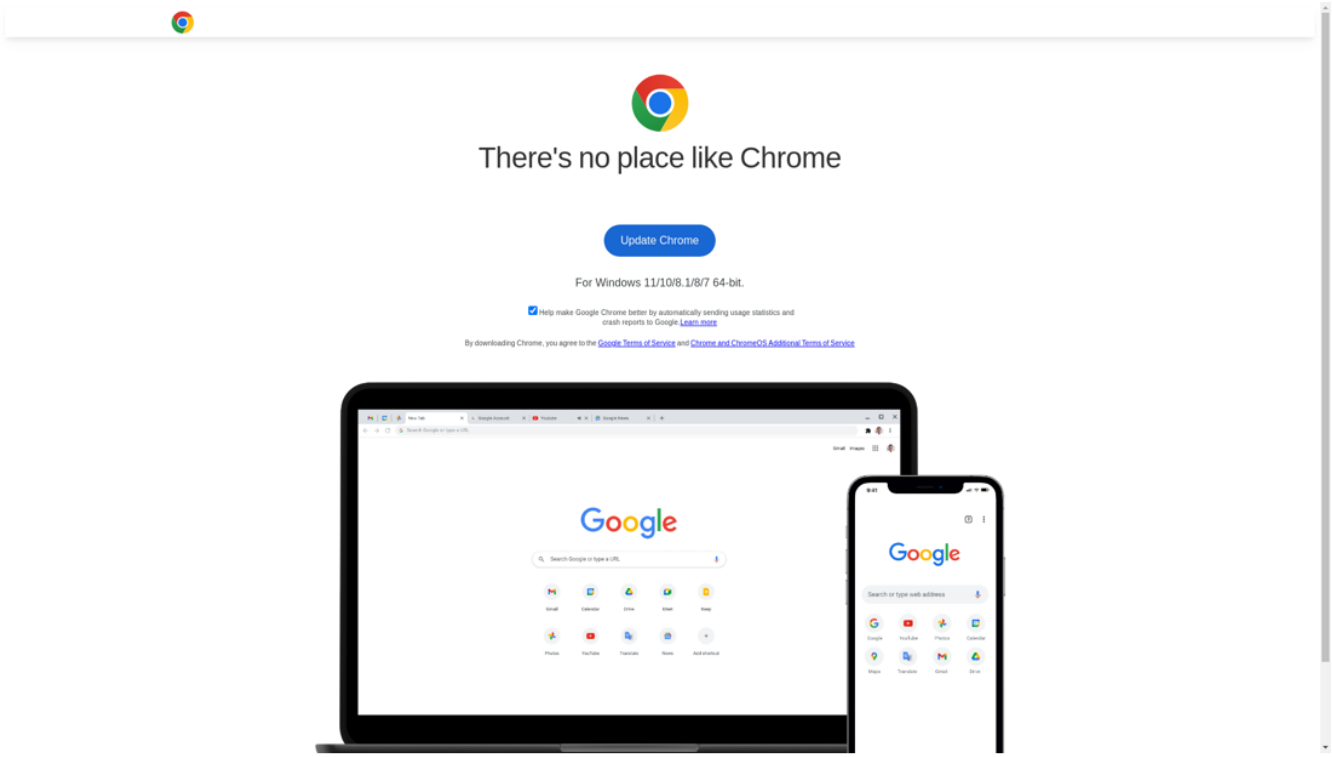


Screenshot of the .URL file involved in the October 2 campaign.

Proofpoint has identified multiple cybercriminal campaigns exploiting CVE-2023-36025; however, the BattleRoyal cluster exploited this vulnerability more than any other actor observed in Proofpoint threat data. Notably, this activity cluster exploited CVE-2023-36025 before it was published by Microsoft. SmartScreen is a security feature that is designed to prevent people from visiting malicious websites. The vulnerability could allow an actor to bypass the SmartScreen defenses if a user clicked on a specially crafted .URL file or a hyperlink pointing to a .URL file. More specifically, a SmartScreen alert would not be triggered when a .URL points to a SMB or WebDav share as file:// and the malicious payload is inside a ZIP file which is specified in the URL target.

RogueRaticate (fake browser update campaign example)

On October 19, 2023, an external researcher identified and publicly shared details of the RogueRaticate fake update activity cluster using an interesting obfuscation technique first identified in 2020. Proofpoint subsequently identified the activity in Proofpoint data. This campaign delivered fake browser update requests to end users on their web browsers that dropped a DarkGate payload with the “ADS5” GroupID. The threat actor injected a request to a domain they controlled that used .css steganography to conceal the malicious code. The stenography would then make a request to an actor controlled Keitaro domain that would filter out unwanted traffic. Users who passed the traffic inspection would be redirected to a fake browser update. If an end user clicked on the fake browser update button, it would download a similar .URL file as the email campaign described above and follow the attack chain from that point to deliver DarkGate.



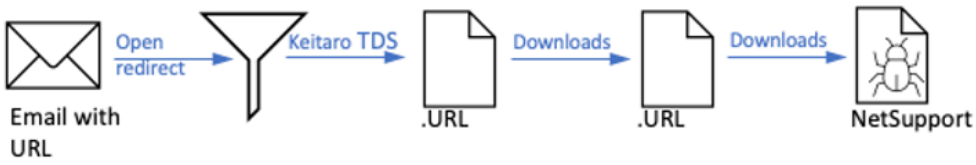
Fake browser update request screenshot.

Switch to NetSupport (an email campaign example)

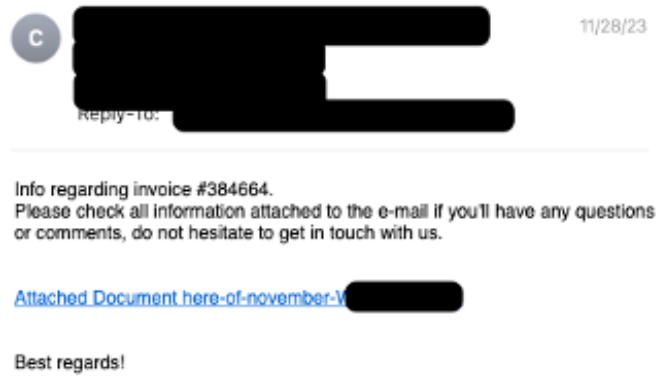
In late November to early December, Proofpoint analysts observed the activity cluster replace DarkGate with NetSupport, a legitimate remote access tool, in observed campaigns. Compared to DarkGate, NetSupport is a more established tool in the toolbelt of various crime actors. It has steadily been observed in the landscape in the past four years. Meanwhile, the use of DarkGate before summer 2023 has been very rare. It remains to be seen if the reason for payload switch is due to the spike in DarkGate's popularity and the subsequent attention paid to the malware by threat researchers and security community (which can lead to reduction of efficacy), or simply a temporary change to a different payload. Besides the payload switch, another notable change in this campaign that represents a gradual evolution of the cluster includes the use of two .URL files instead of one.

In an example campaign on November 28, 2023, the emails contained:

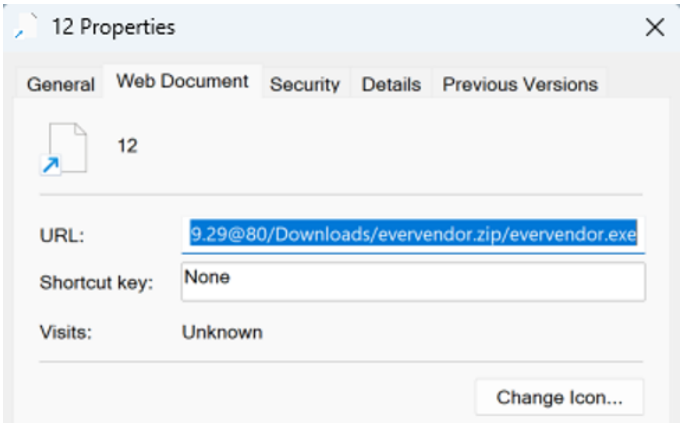
- Doubleclick.net URLs that, if clicked by the user, redirected to Keitaro TDS
- Keitaro TDS was observed serving an Internet shortcut (.URL) file
- The Internet shortcut, if double clicked, downloaded another Internet shortcut (.URL) file
- The second Internet shortcut linked to a NetSupport executable



Attack chain summary that follows the flow of: Email > URL (doubleclick.net) > Keitaro TDS (Cookie: 6e41c) > .URL > .URL > NetSupport.



Screenshot of an example email from November 28 campaign.



Screenshot of the .URL file involved in the November 28 campaign.

Conclusion

The newly identified cluster of activity Proofpoint calls BattleRoyal is notable for its use of multiple attack chains to deliver malware. DarkGate can be used to steal information and download additional malware payloads, and NetSupport can enable threat actors to gain control of an infected host, install additional malware, and enable lateral movement throughout a compromised environment. The actor's use of both email and compromised websites with fake update lures to deliver DarkGate and NetSupport is unique but aligns with the overall trend Proofpoint has observed of cybercriminal threat actors adopting new, varied, and increasingly creative attack chains – including the use of various TDS tools – to enable malware delivery. Additionally, the use of both email and fake update lures shows the actor using multiple types of social engineering techniques in an attempt to get users to install the final payload.

Emerging Threats signatures

2049321 - ET MALWARE WebDAV Retrieving .exe from .url M2 (CVE-2023-36025)

2049320 - ET MALWARE WebDAV Retrieving .zip from .url M2 (CVE-2023-36025)

2049317 - ET MALWARE WebDAV Retrieving .zip from .url M1 (CVE-2023-36025)

2049316 - ET MALWARE WebDAV Retrieving .exe from .url M1 (CVE-2023-36025)

2048098 - ET MALWARE DarkGate AutoIt Downloader

2048089 - ET MALWARE Darkgate Stealer CnC Checkin

2035895 - ET INFO NetSupport Remote Admin Response

2034559 - ET POLICY NetSupport GeoLocation Lookup Request

2035892 - ET INFO NetSupport Remote Admin Checkin

2827745 - ETPRO MALWARE NetSupport RAT CnC Activity

Indicators of compromise

Indicator	Description	First Observed
hxxps[:]//heilee[.]com/qxz3l	Example 404 TDS URL (DarkGate campaign)	2 October 2023
Hxxps[:]//nathumvida[.]org/	Keitaro TDS (DarkGate campaign)	2 October 2023
96ca146b6bb95de35f61289c2725f979a2957ce54761aff5f37726a85f2f9e77	SHA256 of “IN-SEPT-8415-8794132.pdf.url” served by Keirato (DarkGate campaign)	2 October 2023
file[:]//79.110.62[.]96@80/Downloads/bye.zip/bye.vbs	Target of the .URL file “IN-SEPT-8415-8794132.pdf.url” (DarkGate campaign)	2 October 2023
e2a8a53e117f1dda2c09e5b83a13c99b848873a75b14d20823318840e84de243	SHA256 of file “bye.vbs” downloaded by .URL (DarkGate campaign)	2 October 2023
hxxp[:]//searcherbigdealk[.]com:2351/zjbicvmd	“bye.vbs” downloads shell commands from this URL (DarkGate campaign)	2 October 2023

hxxp[:]//searcherbigdealk[.]com:2351	Shell command downloads “Autoit3.exe” from this URL (DarkGate campaign)	2 October 2023
hxxp[:]//searcherbigdealk[.]com:2351/msizjbicvmd	Shell command downloads “iabyhu.au3” from this URL (DarkGate campaign)	2 October 2023
237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d	SHA256 of “Autoit3.exe” (DarkGate campaign)	2 October 2023
2f5af97b13b077a00218c60305b4eee5d88d14a9bd042beed286434c3fc6e084	SHA256 of “ggvjzi.au3” (DarkGate campaign)	2 October 2023
161.35.113[.]58:443	DarkGate C2 (DarkGate campaign)	2 October 2023
zxcdota2huysasi[.]com	RogueRaticate Payload Host	19 October 2023
hxxps[:]//adclick.g.doubleclick[.]net/pcs/click?fjWWEJMP5797-NovemberQFRSQG65799kd&&adurl=hxxps[:]//kairoscounselingmi[.]com/	Example doubleclick[.]net URL (NetSupport campaign)	28 November 2023
hxxps[:]//kairoscounselingmi[.]com/	Keitaro TDS (NetSupport campaign)	28 November 2023
hxxps[:]//kairoscounselingmi[.]com/wp-content/uploads/astra/help/pr-nv28-2023.url	Keitaro TDS downloading .URL file (NetSupport campaign)	28 November 2023
fce452bcf10414ece8eee6451cf52b39211eb65ecaa02a15bc5809c8236369a4	SHA256 of file “pr-nv28-2023.url” (NetSupport campaign)	28 November 2023

file[:]//5.181.159[.]29@80/Downloads/12.url	Target of the .URL file “pr-nv28-2023.url” (NetSupport campaign)	28 November 2023
ea8f893c080159a423c9122b239ec389939e4c3c1f218bdee16dde744e08188f	SHA256 of file “12.url” (NetSupport campaign)	28 November 2023
file[:]//5.181.159[.]29@80/Downloads/evervendor.zip/evervendor.exe	Targetof the .URL file “12.url” (NetSupport campaign)	28 November 2023
7562c213f88efdb119a9bbe95603946ba3beb093c326c3b91e7015ae49561f0f	SHA256 of file “evervendor.exe” (NetSupport campaign)	28 November 2023