Dec 22 2023

NETMANAGEIT

Intelligence Report

BattleRoyal, DarkGate Cluster Spreads via Email and Fake Browser Updates

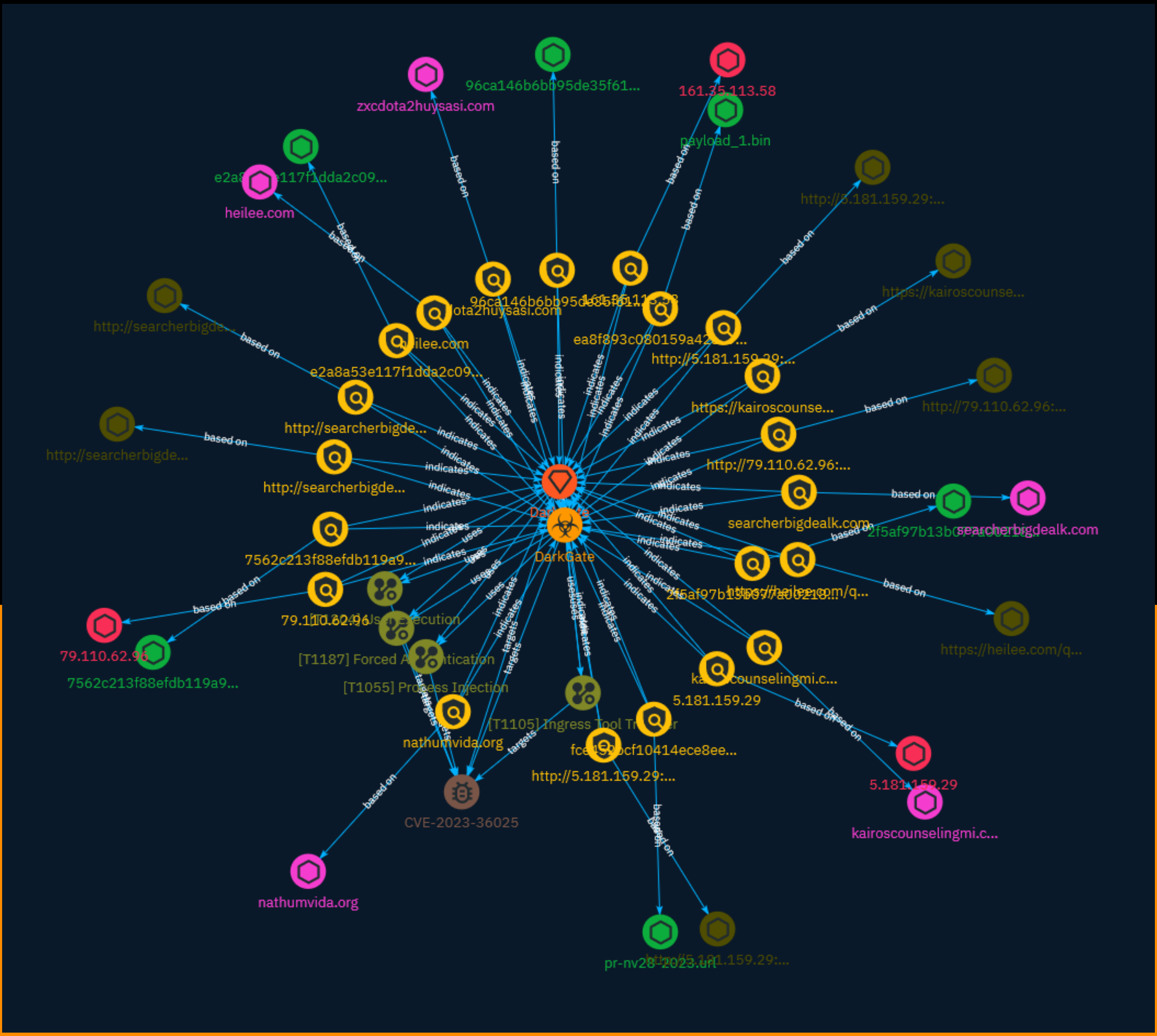

Table of contents

Overview

Entities

Observables

External References

Overview

Description

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.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Attack-Pattern

Name
Forced Authentication
ID
T1187
Description
Adversaries may gather credential material by invoking or forcing a user to automatically provide authentication information through a mechanism in which they can intercept. The Server Message Block (SMB) protocol is commonly used in Windows networks for authentication and communication between systems for access to resources and file sharing. When a Windows system attempts to connect to an SMB resource it will automatically attempt to authenticate and send credential information for the current user to the remote system. (Citation: Wikipedia Server Message Block) This behavior is typical in enterprise environments so that users do not need to enter credentials to access network resources. Web Distributed Authoring and Versioning (WebDAV) is also typically used by Windows systems as a backup protocol when SMB is blocked or fails. WebDAV is an extension of HTTP and will typically operate over TCP ports 80 and 443. (Citation: Didier Stevens WebDAV Traffic) (Citation: Microsoft Managing WebDAV Security) Adversaries may take advantage of this behavior to gain access to user account hashes through forced SMB/WebDAV authentication. An adversary can send an attachment to a user through spearphishing that contains a resource link to an external server controlled by the adversary (i.e. [Template Injection](https://attack.mitre.org/techniques/T1221)), or place a specially crafted file on navigation path for privileged accounts (e.g. .SCF file placed on desktop) or on a publicly accessible share to be accessed by victim(s). When the user's system accesses the untrusted resource it will attempt authentication and send information, including the user's hashed credentials, over SMB to the adversary controlled server. (Citation: GitHub Hashjacking) With access to the credential hash, an adversary can

perform off-line [Brute Force](https://attack.mitre.org/techniques/T1110) cracking to gain access to plaintext credentials. (Citation: Cylance Redirect to SMB) There are several different ways this can occur. (Citation: Osanda Stealing NetNTLM Hashes) Some specifics from in-the-wild use include: * A spearphishing attachment containing a document with a resource that is automatically loaded when the document is opened (i.e. [Template Injection](https://attack.mitre.org/techniques/T1221)). The document can include, for example, a request similar to `file[:]//[remote address]/Normal.dotm` to trigger the SMB request. (Citation: US-CERT APT Energy Oct 2017) * A modified .LNK or .SCF file with the icon filename pointing to an external reference such as `\\[remote address]\pic.png` that will force the system to load the resource when the icon is rendered to repeatedly gather credentials. (Citation: US-CERT APT Energy Oct 2017)

Name

Process Injection

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

Ingress Tool Transfer

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`.(Citation: t1105_lolbas) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Indicator

Name
http://79.110.62.96:80/Downloads/bye.zip/bye.vbs
Description
Created by VirusTotal connector as the positive count was >= 10
Pattern Type
stix
Pattern
[url:value = 'http://79.110.62.96:80/Downloads/bye.zip/bye.vbs']
Name
searcherbigdealk.com
Description
Created by VirusTotal connector as the positive count was >= 10
Pattern Type
stix

Pattern

[domain-name:value = 'searcherbigdealk.com']

Name

http://searcherbigdealk.com:2351/msizjbicvmd

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://searcherbigdealk.com:2351/msizjbicvmd']

Name

kairoscounselingmi.com

Pattern Type

stix

Pattern

[domain-name:value = 'kairoscounselingmi.com']

Name

79.110.62.96

Description

DarkGate botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '79.110.62.96']

Name

96ca146b6bb95de35f61289c2725f979a2957ce54761aff5f37726a85f2f9e77

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '96ca146b6bb95de35f61289c2725f979a2957ce54761aff5f37726a85f2f9e77']

Name

2f5af97b13b077a00218c60305b4eee5d88d14a9bd042beed286434c3fc6e084

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2f5af97b13b077a00218c60305b4eee5d88d14a9bd042beed286434c3fc6e084']

Name

7562c213f88efdb119a9bbe95603946ba3beb093c326c3b91e7015ae49561f0f

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7562c213f88efdb119a9bbe95603946ba3beb093c326c3b91e7015ae49561f0f']

Name

ea8f893c080159a423c9122b239ec389939e4c3c1f218bdee16dde744e08188f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ea8f893c080159a423c9122b239ec389939e4c3c1f218bdee16dde744e08188f']

Name

http://5.181.159.29:80/Downloads/evervendor.zip/evervendor.exe

Pattern Type

stix

Pattern

[url:value = 'http://5.181.159.29:80/Downloads/evervendor.zip/evervendor.exe']

Name

http://searcherbigdealk.com:2351/zjbicvmd

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://searcherbigdealk.com:2351/zjbicvmd']

Name

https://kairoscounselingmi.com/wp-content/uploads/astra/help/pr-nv28-2023.url

Pattern Type

stix

Pattern

[url:value = 'https://kairoscounselingmi.com/wp-content/uploads/astra/help/pr-nv28-2023.url']

Name

zxcdota2huysasi.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'zxcdota2huysasi.com']

Name

161.35.113.58

Description

DarkGate botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '161.35.113.58']

Name

fce452bcf10414ece8eee6451cf52b39211eb65ecaa02a15bc5809c8236369a4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fce452bcf10414ece8eee6451cf52b39211eb65ecaa02a15bc5809c8236369a4']

Name

e2a8a53e117f1dda2c09e5b83a13c99b848873a75b14d20823318840e84de243

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e2a8a53e117f1dda2c09e5b83a13c99b848873a75b14d20823318840e84de243']

Name

http://5.181.159.29:80/Downloads/12.url

Pattern Type

stix

Pattern

[url:value = 'http://5.181.159.29:80/Downloads/12.url']

Name

https://heilee.com/qxz3l

Pattern Type

stix

Pattern

[url:value = 'https://heilee.com/qxz3l']

Name

heilee.com

Pattern Type

stix

Pattern

[domain-name:value = 'heilee.com']

Name

5.181.159.29

Description

ISP: MivoCloud SRL **OS:** None ------------------------- Hostnames: - no-
rdns.mivocloud.com ------------------------- Domains: - mivocloud.com
------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.10
Key type: ssh-rsa Key:
AAAAB3NzaC1yc2EAAAADAQABAAABgQDjvOKuLYUfCYIS3NI9ijRWp0K1F5tJt1sz3qxNfidIlQwu
T9w0Uiz2Q145NZwHvh9UHFKrZ/7tZaUgAHQ4v1EkpkiH4zn4DluRRcrFN0WulPkY+zXZR/CiJqh6
9AwWRIMkmN23juw9ZT12jaoGIPMH5yhbFnCXf/dgSKK9DbG03UDDoGRHi5VR8U9/
DuNI+GIpLZa/ jn0rZjpuuk94IvpaemFnJ6I/
F+5YNRSJdmTl+4XUQrj5eg4GoLiJLFKGU4E2nMtatFOH03b6JQSK
GPeJrbwAi+96tnHh1iJNuhh9HmgZLG12dRj/NWplt6avtau71vVNApYLe/0SEEBV9MGH6ArYTKAC
18m1eFvckzVSFV+JY2I015L3w43PzeVz4ciBeuLMG4MBN08HXKvydNxyQ5cH4a9g/hFD0rmbOPpN
HJuAEk3Wi7pR8qPMBMLFOmZwlGt6zZVsITWNQ00dN+9LJla5rVcs4B9WBC/
ECLwuO542MKqEgJEq bqQB9AjVxxs= Fingerprint: 0f:29:7b:f2:4e:8d:2b:0e:bf:f1:13:02:58:90:1e:47
Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256
ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-
hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256
kex-strict-s-v00@openssh.com Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-
rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-
poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com
aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-
etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com
hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-
sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ```
------------------ **80:** ``` HTTP/1.1 207 Multi-Status Content-Type: text/xml; charset=utf-8
Date: Fri, 22 Dec 2023 04:41:40 GMT Transfer-Encoding: chunked ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.181.159.29']

Name

nathumvida.org

Pattern Type
stix

Pattern
[domain-name:value = 'nathumvida.org']

Intrusion-Set

Name
DarkGate

Malware

Name
DarkGate

Vulnerability

Name
CVE-2023-36025
Description
Microsoft Windows SmartScreen contains a security feature bypass vulnerability that could allow an attacker to bypass Windows Defender SmartScreen checks and their associated prompts.

Domain-Name

Value
zxcdota2huysasi.com
kairoscounselingmi.com
heilee.com
searcherbigdealk.com
nathumvida.org

StixFile

Value
2f5af97b13b077a00218c60305b4eee5d88d14a9bd042beed286434c3fc6e084
96ca146b6bb95de35f61289c2725f979a2957ce54761aff5f37726a85f2f9e77
fce452bcf10414ece8eee6451cf52b39211eb65ecaa02a15bc5809c8236369a4
e2a8a53e117f1dda2c09e5b83a13c99b848873a75b14d20823318840e84de243
7562c213f88efdb119a9bbe95603946ba3beb093c326c3b91e7015ae49561f0f
ea8f893c080159a423c9122b239ec389939e4c3c1f218bdee16dde744e08188f

IPv4-Addr

Value
5.181.159.29
79.110.62.96
161.35.113.58

Url

Value
http://searcherbigdealk.com:2351/zjbicvmd
http://79.110.62.96:80/Downloads/bye.zip/bye.vbs
http://searcherbigdealk.com:2351/msizjbicvmd
https://kairoscounselingmi.com/wp-content/uploads/astra/help/pr-nv28-2023.url
http://5.181.159.29:80/Downloads/evervendor.zip/evervendor.exe
http://5.181.159.29:80/Downloads/12.url
https://heilee.com/qxz3l

External References

- https://otx.alienvault.com/pulse/65855c8bd0709c708a894ca2
- https://www.proofpoint.com/us/blog/threat-insight/battleroyal-darkgate-cluster-spreads-email-and-fake-browser-updates