Oct 29 2023

NETMANAGEIT

Intelligence Report

DarkGate malware campaign

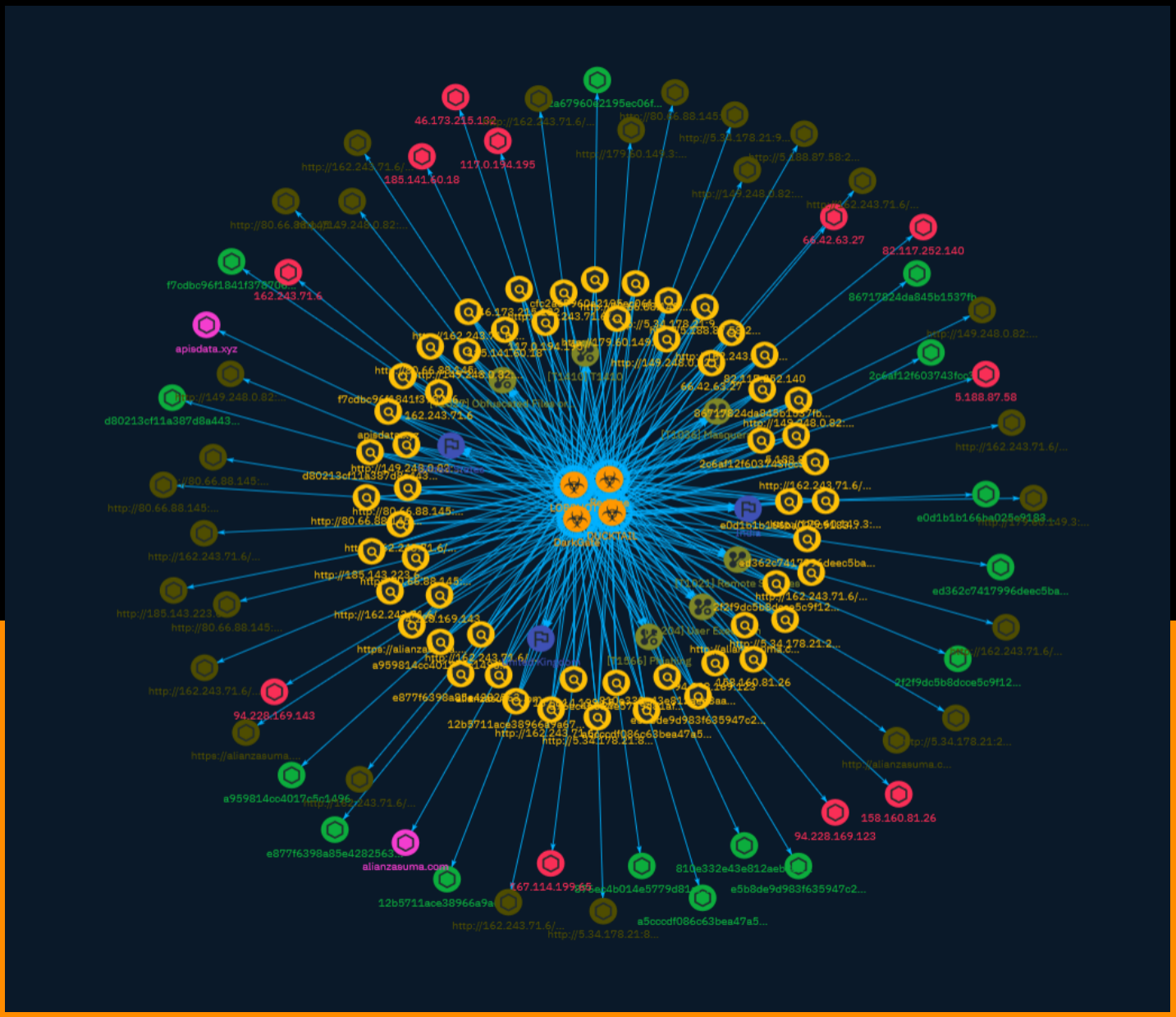

Table of contents

Overview

Entities

Observables

External References

Overview

Description

WithSecure Detection and Response Team (DRT) detected and identified multiple DarkGate malware infection attempts against WithSecure Managed Detection and Response (MDR) customers in the UK, US, and India.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Masquerading
ID
T1036
Description
Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)
Name
Phishing
ID
T1566
Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

T1410

ID

T1410

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

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the

plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Remote Services

ID

T1021

Description

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user. In an enterprise environment, servers and workstations can be organized into domains. Domains provide centralized identity management, allowing users to login using one set of credentials across the entire network. If an adversary is able to obtain a set of valid domain credentials, they could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP).(Citation: SSH Secure Shell)(Citation: TechNet Remote Desktop Services) They could also login to accessible SaaS or IaaS services, such as those that federate their identities to the domain. Legitimate applications (such as [Software Deployment Tools](https://attack.mitre.org/techniques/T1072) and other administrative programs) may utilize [Remote Services](https://attack.mitre.org/techniques/T1021) to access remote hosts. For example, Apple Remote Desktop (ARD) on macOS is native software used for remote management. ARD leverages a blend of protocols, including [VNC](https://attack.mitre.org/techniques/T1021/005) to send the screen and control buffers and [SSH](https://attack.mitre.org/techniques/T1021/004) for secure file transfer. (Citation: Remote Management MDM macOS)(Citation: Kickstart Apple Remote Desktop commands)(Citation: Apple Remote Desktop Admin Guide 3.3) Adversaries can abuse applications such as ARD to gain remote code execution and perform lateral movement. In versions of macOS prior to 10.14, an adversary can escalate an SSH session to an ARD

session which enables an adversary to accept TCC (Transparency, Consent, and Control) prompts without user interaction and gain access to data.(Citation: FireEye 2019 Apple Remote Desktop)(Citation: Lockboxx ARD 2019)(Citation: Kickstart Apple Remote Desktop commands)

Indicator

Name
94.228.169.123
Description
CC=AT ASN=AS210644 Aeza International Ltd
Pattern Type
stix
Pattern
[ipv4-addr:value = '94.228.169.123']
Name
http://80.66.88.145:2840/
Pattern Type
stix
Pattern
[url:value = 'http://80.66.88.145:2840/']

Name

http://5.34.178.21:9999/

Pattern Type

stix

Pattern

[url:value = 'http://5.34.178.21:9999/']

Name

http://162.243.71.6/no_halt_opts_enabled.msi

Description

Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 3.3.14.5, Subject: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft, Keywords: Installer, Template: Intel;1033, Revision Number: {896BC09F-FB22-46F5-A093-94508EDEDD72}, Create Time/Date: Sat Jul 23 12:0
54f52ef506f6649c09838b9935aed223f0f320798e13fdb9541ffd1db3e08816

Pattern Type

stix

Pattern

[url:value = 'http://162.243.71.6/no_halt_opts_enabled.msi']

Name

http://162.243.71.6/persist.msi

Description

Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 3.3.14.5, Subject: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft, Keywords: Installer, Template: Intel;1033, Revision Number: {4674AB38-D425-49C3-80A7-C42B4A62C997}, Create Time/Date: Sat Jul 23 12:0
394ee7c88a0925698ce1a2e0268ca49404591eb5cdd961d657d785993212cd86

Pattern Type

stix

Pattern

[url:value = 'http://162.243.71.6/persist.msi']

Name

http://alianzasuma.com/wzxfh

Pattern Type

stix

Pattern

[url:value = 'http://alianzasuma.com/wzxfh']

Name

http://149.248.0.82:2351/msiyfucokvo

Pattern Type
stix
Pattern
[url:value = 'http://149.248.0.82:2351/msiyfucokvo']
Name
162.243.71.6
Description
CC=US ASN=AS14061 DIGITALOCEAN-ASN
Pattern Type
stix
Pattern
[ipv4-addr:value = '162.243.71.6']
Name
5.188.87.58
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.188.87.58']

Name

66.42.63.27

Description

CC=SG ASN=AS20473 AS-CHOOPA

Pattern Type

stix

Pattern

[ipv4-addr:value = '66.42.63.27']

Name

http://80.66.88.145:2841/

Pattern Type

stix

Pattern

[url:value = 'http://80.66.88.145:2841/']

Name

http://162.243.71.6/no_halt_7891.msi

Description

Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 3.3.14.5, Subject: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft, Keywords: Installer, Template: Intel;1033, Revision Number: {D2579E46-A1AB-40A2-85EE-AA6C12A7AF50}, Create Time/Date: Sat Jul 23 12:0
5b608a6729343cf8b6752d5bb201f906920fcb472f5949e04173b907f65ceff1

Pattern Type

stix

Pattern

[url:value = 'http://162.243.71.6/no_halt_7891.msi']

Name

http://162.243.71.6/all_enabled_vm_enabled7891.msi

Description

Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 3.3.14.5, Subject: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft, Keywords: Installer, Template: Intel;1033, Revision Number: {F442633C-69A2-446C-BDA4-40DCACB51DF3}, Create Time/Date: Sat Jul 23 12:0
4b63f7683808aaba727f11516eb35961e6aa15646f2062e9bfcdbcfe1e8d0951

Pattern Type

stix

Pattern

[url:value = 'http://162.243.71.6/all_enabled_vm_enabled7891.msi']

Name
http://179.60.149.3:2351/
Pattern Type
stix
Pattern
[url:value = 'http://179.60.149.3:2351/']
Name
http://80.66.88.145:7891/
Pattern Type
stix
Pattern
[url:value = 'http://80.66.88.145:7891/']
Name
185.141.60.18
Description
CC=BG ASN=AS44901 Belcloud LTD
Pattern Type
stix

Pattern

[ipv4-addr:value = '185.141.60.18']

Name

e5b8de9d983f635947c25183efc9b490cf185388634cf937426e3cd1235b250e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e5b8de9d983f635947c25183efc9b490cf185388634cf937426e3cd1235b250e']

Name

http://80.66.88.145:9999/

Pattern Type

stix

Pattern

[url:value = 'http://80.66.88.145:9999/']

Name

86717824da845b1537fb24583dd9825be1ea8e032d3f5758357d1da615e82567

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '86717824da845b1537fb24583dd9825be1ea8e032d3f5758357d1da615e82567']

Name

http://5.34.178.21:81/files/twitter.msi

Pattern Type

stix

Pattern

[url:value = 'http://5.34.178.21:81/files/twitter.msi']

Name

http://179.60.149.3:9999/

Pattern Type

stix

Pattern

[url:value = 'http://179.60.149.3:9999/']

Name

2f2f9dc5b8dcce5c9f1261b8d693218017cf348240284820359cd8e86794b282

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2f2f9dc5b8dcce5c9f1261b8d693218017cf348240284820359cd8e86794b282']

Name

alianzasuma.com

Pattern Type

stix

Pattern

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

Name

http://162.243.71.6/error_no_decoy_2840.msi

Description

Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 3.3.14.5, Subject: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft, Keywords: Installer, Template: Intel;1033, Revision Number: {8C2AAD6B-0C5D-4BA0-9A09-2635C51AAC57}, Create Time/Date: Sat Jul 23 12:0 52d4ccbd95e4285e8169baa601b89675a0e29ca1d4320b7f309192287476ebf9

Pattern Type

stix

Pattern

[url:value = 'http://162.243.71.6/error_no_decoy_2840.msi']

Name

https://alianzasuma.com/wzxfh

Pattern Type

stix

Pattern

[url:value = 'https://alianzasuma.com/wzxfh']

Name

117.0.194.195

Description

CC=VN ASN=AS7552 Viettel Group

Pattern Type

stix

Pattern

[ipv4-addr:value = '117.0.194.195']

Name

e0d1b1b166ba025c918335b3733d908bb89ecbce776ee273941bfa38acbba765

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e0d1b1b166ba025c918335b3733d908bb89ecbce776ee273941bfa38acbba765']

Name

a959814cc4017c5c14969addb80c6967c8ad20650896005e4dd22d5dc54da614

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a959814cc4017c5c14969addb80c6967c8ad20650896005e4dd22d5dc54da614']

Name

http://162.243.71.6/startup_persist_no_halt2840.msi

Description

Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 3.3.14.5, Subject: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft, Keywords: Installer, Template: Intel;1033, Revision Number:

{23E63E7F-635E-4AF6-98CE-CDF77CDF1DAD}, Create Time/Date: Sat Jul 23 12:0
de2064d4363a3ccbda5518c619f1c803393b0876e349530583a72b1d1643c16a

Pattern Type

stix

Pattern

[url:value = 'http://162.243.71.6/startup_persist_no_halt2840.msi']

Name

158.160.81.26

Description

ISP: Yandex.Cloud LLC **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.3 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDKTg3/TVZmF0ytvawJUUGynuGLVXuM8EBsgjQ6v+O+m/v5 sP5UnUuhpIsi6Z98unTaZy/Wrb+gWZ9lUDyWp8ekAIQMIbLR8RYpmsteEKlgDoiJyKIUpLQVKtFk xcdNryKJDKbnbHmcBVaZzBaiRsIt6Rh9KothSUw1tX6oA/CfGaam+MnialLC/8TIqRsfMJkRZbKi FGqWJj0cYvYo+hquIaMw/yeBsMWeSMJrwsjw+LRiBiOiDIIA3MoiJiF5JdaH3ENpD0Fs6rNLokkz AULuxpG35wCcJdmf1qAZdW1r9ka0Qnb7hxuykueG3dw+EAJC+lRoNUMygz0CgIqoYPyIDqhnRt9E mEsMLhaoxw4TU2aTVgtEeb+9dQJzRekJBKPtj1Ao4Vv8hUHtIRziY8Xhf9Yhbuf7SQ/j+k3ozAcN / Zd0m/x60RY3T+641+8pxWcfMybfP8cXStCXE1tGWHN3zMjoRnbWnO0G3PIIUzVv/TC7nJS/vn61 xwJuIJC4yPE= Fingerprint: 83:3f:9a:1d:55:53:c1:37:c8:31:db:fc:55:75:b7:02 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 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 ``` ---------- **1194:** ``` @\xf5d\xc68\xf2\xcc\x08\xe3\x01\x00\x00\x00\x00\xd9\xce:

\xbe\xf6\x98\xa5m\x00\x00\x00\x00 ``` ---------- **9091:** ``` HTTP/1.1 404 Not found, not supported, go away Content-Type: text/html Content-Length: 33 Connection: Keep-Alive Not found, not supported, go away ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '158.160.81.26']

Name

http://149.248.0.82:2351/

Pattern Type

stix

Pattern

[url:value = 'http://149.248.0.82:2351/']

Name

http://149.248.0.82:9999/

Pattern Type

stix

Pattern

[url:value = 'http://149.248.0.82:9999/']

Name

2c6af12f603743fcc3effdc24783c969c906816960fbfbf012974fc04722a679

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2c6af12f603743fcc3effdc24783c969c906816960fbfbf012974fc04722a679']

Name

94.228.169.143

Description

CC=AT ASN=AS210644 Aeza International Ltd

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.228.169.143']

Name

http://162.243.71.6/ais_binded_moderate_halt_vm_enabled_2840.msi

Description

Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 3.3.14.5, Subject: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft, Keywords: Installer, Template: Intel;1033, Revision Number: {C2990676-8624-4A8E-B979-5326889BC8B1}, Create Time/Date: Sat Jul 23 12:0
8c4fa2e64e0bd3b3e162e6f74fab12efdb30df68db69c12506038c54ed601580

Pattern Type

stix

Pattern

[url:value = 'http://162.243.71.6/ais_binded_moderate_halt_vm_enabled_2840.msi']

Name

12b5711ace38966a9a6767fc331f835a3ee5b68d0f901aabf2c5d069d46f7b44

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '12b5711ace38966a9a6767fc331f835a3ee5b68d0f901aabf2c5d069d46f7b44']

Name

cfc2a67960e2195ec06fc923122bf4a4ce6f4c734801914b1ff250abb564b398

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cfc2a67960e2195ec06fc923122bf4a4ce6f4c734801914b1ff250abb564b398']

Name

a5cccdf086c63bea47a509c683e7b4214d1a2be0522fc835788887117e92d41a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a5cccdf086c63bea47a509c683e7b4214d1a2be0522fc835788887117e92d41a']

Name

d80213cf11a387d8a443c022a8e46e1c881f319c966113a2d3cc565af665ca2c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd80213cf11a387d8a443c022a8e46e1c881f319c966113a2d3cc565af665ca2c']

Name

82.117.252.140

Description

CC=US ASN=AS204957 Green Floid LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '82.117.252.140']

Name

167.114.199.65

Description

CC=CA ASN=AS16276 OVH SAS

Pattern Type

stix

Pattern

[ipv4-addr:value = '167.114.199.65']

Name

apisdata.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'apisdata.xyz']

Name

ed362c7417996deec5ba3b2f41e0b0f907d701aea8b403cf3fa4050cbe3a21b6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ed362c7417996deec5ba3b2f41e0b0f907d701aea8b403cf3fa4050cbe3a21b6']

Name

e877f6398a85e428256352d6a82f4219eed939404a00aaeec9a98eb35a3e518f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e877f6398a85e428256352d6a82f4219eed939404a00aaeec9a98eb35a3e518f']

Name

http://5.188.87.58:2351/msibtbgvbyy

Pattern Type

stix

Pattern

[url:value = 'http://5.188.87.58:2351/msibtbgvbyy']

Name

810e332e43e812aeb8aabca6bd0d00b693d20cbb61f486be28ce1287a337a4fa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '810e332e43e812aeb8aabca6bd0d00b693d20cbb61f486be28ce1287a337a4fa']

Name

f7cdbc96f1841f378706d0d609b29999d202801403807c23ac89c63224314d09

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f7cdbc96f1841f378706d0d609b29999d202801403807c23ac89c63224314d09']

Name

http://162.243.71.6/no_sec_no_startup51.msi

Description

Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 3.3.14.5, Subject: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft, Keywords: Installer, Template: Intel;1033, Revision Number: {DBBA8977-ACC2-4500-B8F4-BEEE19DF5E12}, Create Time/Date: Sat Jul 23 12:0
aa92f9692dfa98ba9ee991156612f2015c10a5ecf02b605b0b6d528827430601

Pattern Type

stix

Pattern

[url:value = 'http://162.243.71.6/no_sec_no_startup51.msi']

Name

http://162.243.71.6/ais_to_sign.msi

Description

Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 3.3.14.5, Subject: Application Verifier x64 External Package - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Microsoft, Keywords: Installer, Template: Intel;1033, Revision Number: {A5EA087F-6B4B-4FAD-A214-66AE6482BA2A}, Create Time/Date: Sat Jul 23 12:0
cde0f0b6a29a11aa8a5a4ee543fd632cb460bc11927c7153c1f5f8664e474d23

Pattern Type

stix

Pattern

[url:value = 'http://162.243.71.6/ais_to_sign.msi']

Name

46.173.215.132

Description

CC=RU ASN=AS47196 Garant-Park-Internet LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '46.173.215.132']

Name

http://5.34.178.21:2351/

Pattern Type

stix

Pattern

[url:value = 'http://5.34.178.21:2351/']

Name

http://185.143.223.64:2351/

Pattern Type

stix

Pattern

[url:value = 'http://185.143.223.64:2351/']

Name

http://149.248.0.82:2351/yfucokvo

Pattern Type

stix

Pattern

[url:value = 'http://149.248.0.82:2351/yfucokvo']

Name

876ec4b014e5779d81af67d04fbb50ccfd965dcb8ea3283cdcb3817e8543c593

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '876ec4b014e5779d81af67d04fbb50ccfd965dcb8ea3283cdcb3817e8543c593']

Name

http://80.66.88.145:2351/

Pattern Type
stix
Pattern
[url:value = 'http://80.66.88.145:2351/']

Country

Name
India
Name
United Kingdom
Name
United States

Malware

Name
DUCKTAIL

Name
LOBSHOT

Name
RedLine

Name
DarkGate

Domain-Name

Value
alianzasuma.com
apisdata.xyz

StixFile

Value
12b5711ace38966a9a6767fc331f835a3ee5b68d0f901aabf2c5d069d46f7b44
a5cccdf086c63bea47a509c683e7b4214d1a2be0522fc835788887117e92d41a
ed362c7417996deec5ba3b2f41e0b0f907d701aea8b403cf3fa4050cbe3a21b6
86717824da845b1537fb24583dd9825be1ea8e032d3f5758357d1da615e82567
2c6af12f603743fcc3effdc24783c969c906816960fbfbf012974fc04722a679
f7cdbc96f1841f378706d0d609b29999d202801403807c23ac89c63224314d09
2f2f9dc5b8dcce5c9f1261b8d693218017cf348240284820359cd8e86794b282
e5b8de9d983f635947c25183efc9b490cf185388634cf937426e3cd1235b250e
a959814cc4017c5c14969addb80c6967c8ad20650896005e4dd22d5dc54da614
e0d1b1b166ba025c918335b3733d908bb89ecbce776ee273941bfa38acbba765
e877f6398a85e428256352d6a82f4219eed939404a00aaeec9a98eb35a3e518f
810e332e43e812aeb8aabca6bd0d00b693d20cbb61f486be28ce1287a337a4fa
876ec4b014e5779d81af67d04fbb50ccfd965dcb8ea3283cdcb3817e8543c593

cfc2a67960e2195ec06fc923122bf4a4ce6f4c734801914b1ff250abb564b398

d80213cf11a387d8a443c022a8e46e1c881f319c966113a2d3cc565af665ca2c

IPv4-Addr

Value
185.141.60.18
158.160.81.26
82.117.252.140
66.42.63.27
94.228.169.123
5.188.87.58
117.0.194.195
46.173.215.132
167.114.199.65
94.228.169.143
162.243.71.6

Url

Value
http://162.243.71.6/ais_to_sign.msi
http://162.243.71.6/all_enabled_vm_enabled7891.msi
http://149.248.0.82:2351/yfucokvo
http://80.66.88.145:2351/
http://179.60.149.3:2351/
http://80.66.88.145:9999/
http://5.34.178.21:9999/
http://162.243.71.6/no_halt_7891.msi
http://80.66.88.145:7891/
http://162.243.71.6/persist.msi
http://162.243.71.6/startup_persist_no_halt2840.msi
http://149.248.0.82:2351/
http://alianzasuma.com/wzxfh

http://80.66.88.145:2841/

http://179.60.149.3:9999/

http://80.66.88.145:2840/

http://149.248.0.82:2351/msiyfucokvo

http://149.248.0.82:9999/

http://162.243.71.6/no_halt_opts_enabled.msi

http://5.34.178.21:2351/

http://185.143.223.64:2351/

http://5.188.87.58:2351/msibtbgvbyy

http://162.243.71.6/ais_binded_moderate_halt_vm_enabled_2840.msi

http://162.243.71.6/error_no_decoy_2840.msi

http://162.243.71.6/no_sec_no_startup51.msi

http://5.34.178.21:81/files/twitter.msi

https://alianzasuma.com/wzxfh

External References

- https://otx.alienvault.com/pulse/6537e8def0365b581ec16e96
- https://labs.withsecure.com/publications/darkgate-malware-campaign
- https://www.malwarebytes.com/blog/business/2023/10/on-the-frontlines-battling-an-in-the-wild-darkgate-infection-with-malwarebytes-mdr