Mar 01 2024

NETMANAGEIT

Intelligence Report

Dissecting DarkGate: Modular Malware Delivery and Persistence as a Service

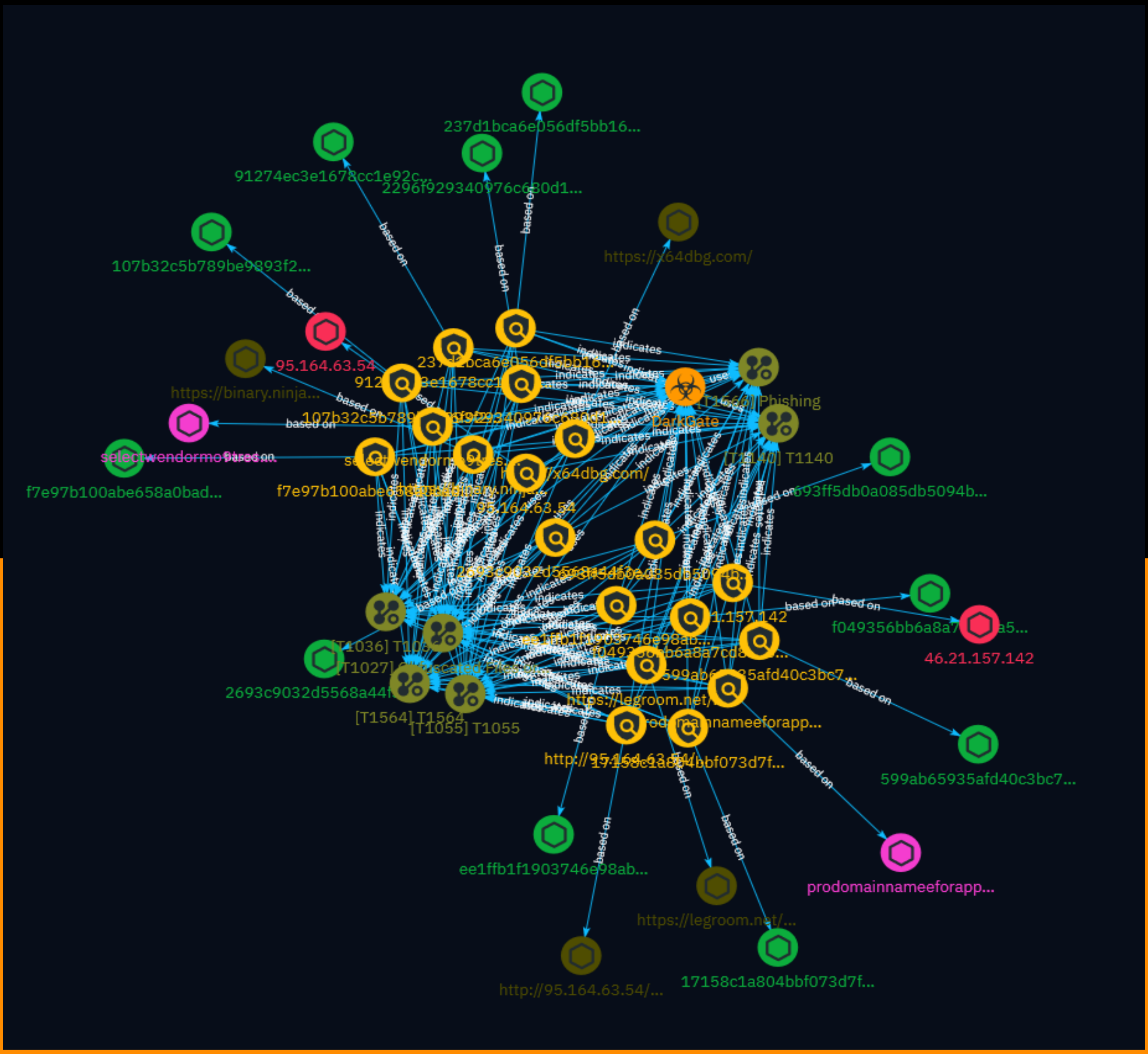

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This report analyzes a phishing PDF that led to the delivery of a signed MSI file containing layered stages designed to avoid detection and deliver the DarkGate malware for persistence and remote access. The analysis covers extracting and decrypting the stages to uncover the final payload.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

https://x64dbg.com/

Pattern Type

stix

Pattern

[url:value = 'https://x64dbg.com/']

Name

https://legroom.net/software/uniextract

Pattern Type

stix

Pattern

[url:value = 'https://legroom.net/software/uniextract']

Name

https://binary.ninja/

Pattern Type

stix

Pattern

[url:value = 'https://binary.ninja/']

Name

46.21.157.142

Description

ISP: HIVELOCITY, Inc. **OS:** - -------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.11 Key type: ssh-rsa Key:
AAAAB3NzaC1yc2EAAAADAQABAAABgQDLPnjzxsF0CnXiI1YbkaxNzCYQLIlDSGmshCC0HFUUTA6O
dALDGw3et8/9+F/s9QA7fZahRqFDq/1XMQkfC7lTUZ73lk9AJ70UMEW9oNsHDZqPG8WwwCo0L/
bq 6UGweCYw3z9PRgQLzRfjr5cKS0C9B5r2haAYBgiT1qJq4onE80YBgAOGCDnzkq/9YCeLO6/
E4u4T
jSf96bujUgczqXuhqLJSQrdETBCQSn4jwxgAYpQTJXUnd0+Ywdh0Qv7qE29NFZ8Ox0KKJSaxYWx+
Xo6zxTjfw+A09/RaKZQq8fLF1M5kZJMtdJRhFmIkHYfZg+FvtHGXm8npbcrDoNsXqmWjpIMC4yOu
+33hJUQasdedibLPg6XYSXv6kOfGB8GYTSBrHLfVEjBHyWmRaytbJsn1QUgqmcI+kJ2Jrc/XHhg0
r6Q88NZMarmxrrIhfmLQMeAliugN+gOqK8iWkcgU9xE3m/qHPLWplJ/gVjO2qYoNBtfpIItP6D/U
lzAhaiYYdoM= Fingerprint: 88:32:58:a3:13:b1:a3:37:0b:7c:53:ff:84:4c:7a:7d 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 ```

Pattern Type

stix

Pattern

[ipv4-addr:value = '46.21.157.142']

Name

f7e97b100abe658a0bad506218ff52b5b19adb75a421d7ad91d500c327685d29

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f7e97b100abe658a0bad506218ff52b5b19adb75a421d7ad91d500c327685d29']

Name

ee1ffb1f1903746e98aba2b392979a63a346fa0feab0d0a75477eacc72fc26a6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ee1ffb1f1903746e98aba2b392979a63a346fa0feab0d0a75477eacc72fc26a6']

Name

f049356bb6a8a7cd82a58cdc9e48c492992d91088dda383bd597ff156d8d2929

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'f049356bb6a8a7cd82a58cdc9e48c492992d91088dda383bd597ff156d8d2929']

Name

91274ec3e1678cc1e92c02bc54a24372b19d644c855c96409b2a67a648034ccf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'91274ec3e1678cc1e92c02bc54a24372b19d644c855c96409b2a67a648034ccf']

Name

599ab65935afd40c3bc7f1734cbb8f3c8c7b4b16333b994472f34585ebebe882

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'599ab65935afd40c3bc7f1734cbb8f3c8c7b4b16333b994472f34585ebebe882']

Name
2693c9032d5568a44f3e0d834b154d82310490532212 1328ae0a1600607a2175
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '2693c9032d5568a44f3e0d834b154d823104905322121328ae0a1600607a2175']
Name
2296f929340976c680d199ce8e47bd7136d9f4c1f7abc9df79843e094f894236
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '2296f929340976c680d199ce8e47bd7136d9f4c1f7abc9df79843e094f894236']
Name
17158c1a804bbf073d7f0f64a9c974312b3967a43bdc029219ab62545b94e724
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' =
'17158c1a804bbf073d7f0f64a9c974312b3967a43bdc029219ab62545b94e724']

Name

107b32c5b789be9893f24d5bfe22633d25b7a3cae80082ef37b30e056869cc5c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'107b32c5b789be9893f24d5bfe22633d25b7a3cae80082ef37b30e056869cc5c']

Name

693ff5db0a085db5094bb96cd4c0ce1d1d3fdc2fbf6b92c32836f3e61a089e7a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'693ff5db0a085db5094bb96cd4c0ce1d1d3fdc2fbf6b92c32836f3e61a089e7a']

Name

95.164.63.54

Description

ISP: STARK INDUSTRIES SOLUTIONS LTD **OS:** Windows 11 (version 21H2) (build 10.0.22000) -------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDjMXySIkdOXJJBg2bvtp5fDSUJUyXlBAMEOrVh2YRyVtKKp231Gompxym0yNbiDmDxNx03npyZZxiavhuFgo8ySYpMQYXFLXFFLVLzuClbACf293B5dw8c2l18oF769Y8MUpju/qqes/kIny3qPGWio09ArptMZaAoS3MTdOBbKeZCWHjkzEQtsYb2HxSW0Im5a8WuCX0dHGLqC11+pieTYbJm98V890Pm8SCNQDbdQfLQPLskF+MQmcxDO47ZdcUxuS15RrC/MnqqMkmr qCl4QxMvtW0JY8gu/c2T2xAKeOPOFBAf13baoZl5oKqKLxryzzen11uIw4Hph8qpgA41 Fingerprint: e2:d5:79:da:31:af:f2:7c:07:c6:55:86:7e:1c:ce:66 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-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 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 aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc 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 ``` ------------------ **137:** ``` NetBIOS Response: Server Name: CENTOS MAC Address: 00:00:00:00:00:00 Names: CENTOS <0x0> CENTOS <0x3> CENTOS <0x20> \x01\x02__MSBROWSE__\x02 <0x1> WORKGROUP <0x0> WORKGROUP <0x1d> WORKGROUP <0x1e> ``` ------------------ **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x0f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 11 (version 21H2) OS Build: 10.0.22000 Target Name: DESKTOP-2NFCDE2 NetBIOS Domain Name: DESKTOP-2NFCDE2 NetBIOS Computer Name: DESKTOP-2NFCDE2 DNS Domain Name: DESKTOP-2NFCDE2 FQDN: DESKTOP-2NFCDE2 ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '95.164.63.54']

Name

selectwendormo9tres.com

Pattern Type

stix

Pattern

[domain-name:value = 'selectwendormo9tres.com']

Name

prodomainnameeforappru.com

Pattern Type

stix

Pattern

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

Name

http://95.164.63.54/documents/build-x64.zip/build-x64.msi

Description

Threat: malware_download - Reporter: RandomMalware - Status: offline

Pattern Type

stix

Pattern

[url:value = 'http://95.164.63.54/documents/build-x64.zip/build-x64.msi']
Name
237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d']

Malware

Name
DarkGate

Attack-Pattern

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

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

T1055

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

T1036

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) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

T1140

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [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)

Name
T1564

ID
T1564

Description
Adversaries may attempt to hide artifacts associated with their behaviors to evade detection. Operating systems may have features to hide various artifacts, such as important system files and administrative task execution, to avoid disrupting user work environments and prevent users from changing files or features on the system. Adversaries may abuse these features to hide artifacts such as files, directories, user accounts, or other system activity to evade detection.(Citation: Sofacy Komplex Trojan)(Citation: Cybereason OSX Pirrit)(Citation: MalwareBytes ADS July 2015) Adversaries may also attempt to hide artifacts associated with malicious behavior by creating computing regions that are isolated from common security instrumentation, such as through the use of virtualization technology.(Citation: Sophos Ragnar May 2020)

Url

Value
https://x64dbg.com/
https://legroom.net/software/uniextract
https://binary.ninja/
http://95.164.63.54/documents/build-x64.zip/build-x64.msi

IPv4-Addr

Value
46.21.157.142
95.164.63.54

StixFile

Value
f7e97b100abe658a0bad506218ff52b5b19adb75a421d7ad91d500c327685d29
f049356bb6a8a7cd82a58cdc9e48c492992d91088dda383bd597ff156d8d2929
ee1ffb1f1903746e98aba2b392979a63a346fa0feab0d0a75477eacc72fc26a6
91274ec3e1678cc1e92c02bc54a24372b19d644c855c96409b2a67a648034ccf
599ab65935afd40c3bc7f1734cbb8f3c8c7b4b16333b994472f34585ebebe882
2693c9032d5568a44f3e0d834b154d823104905322121328ae0a1600607a2175
2296f929340976c680d199ce8e47bd7136d9f4c1f7abc9df79843e094f894236
17158c1a804bbf073d7f0f64a9c974312b3967a43bdc029219ab62545b94e724
107b32c5b789be9893f24d5bfe22633d25b7a3cae80082ef37b30e056869cc5c
693ff5db0a085db5094bb96cd4c0ce1d1d3fdc2fbf6b92c32836f3e61a089e7a
237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d

Domain-Name

Value
selectwendormo9tres.com
prodomainnameeforappru.com

External References

- https://isc.sans.edu/diary/Guest+Diary+Dissecting+DarkGate+Modular+Malware+Delivery+and+Persistence+as+a+Service/30700
- https://otx.alienvault.com/pulse/65e0cf54bfb52f1ba760d092