Jun 11 2023

NETMANAGEIT

Intelligence Report

Uncovering RedStinger - Undetected APT cyber operations in Eastern Europe since 2020

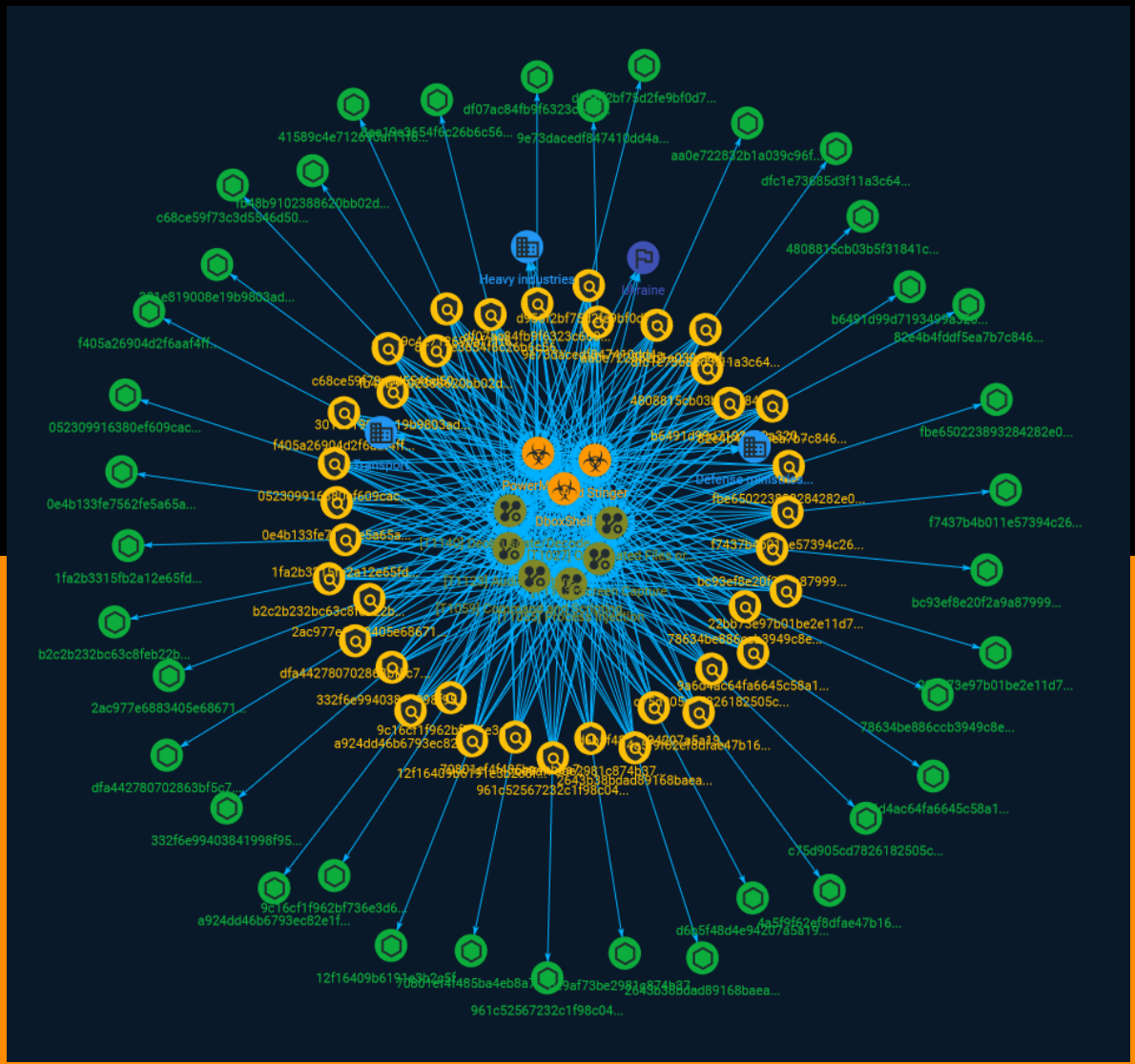

Table of contents

Overview

Entities

Observables

External References

Overview

Description

While looking for activities from the usual suspects, researchers discovered a new interesting lure that targeted the Eastern Ukraine region and reported that finding to the public. Moreover, we started tracking the actor behind it, which we internally codenamed Red Stinger.

Confidence

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

15 / 100

Attack-Pattern

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
Audio Capture
ID
T1123

Description

An adversary can leverage a computer's peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information. Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture audio. Audio files may be written to disk and exfiltrated later.

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

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Deobfuscate/Decode Files or Information

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

Screen Capture

ID

T1113

Description

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as `CopyFromScreen`, `xwd`, or `screencapture`.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

Sector

Name
Heavy industries
Description
Private entities working to transform raw materials into manufactured products (Chemicals, metal etc.).
Name
Defense ministries (including the military)
Description
Includes the military and all defense related-space activities.
Name
Transport
Description
All entities involved in the movement of people or goods from one place to another.

Indicator

Name

301e819008e19b9803ad8b75ecede9ecfa5b11a3ecd8df0316914588b95371c8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '301e819008e19b9803ad8b75ecede9ecfa5b11a3ecd8df0316914588b95371c8']

Name

fbe650223893284282e0be8f7719b554ff7a1d9fbbc72d3e17a47a9a1ceb6231

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fbe650223893284282e0be8f7719b554ff7a1d9fbbc72d3e17a47a9a1ceb6231']

Name

9c16cf1f962bf736e3d6fb9ec3a37bb6f92c5f6cb1886d4332694ccc94735de8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9c16cf1f962bf736e3d6fb9ec3a37bb6f92c5f6cb1886d4332694ccc94735de8']

Name

8aa19e3654f6c26b6c564a8103781174abc540384b20f645e87531c754814cf1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8aa19e3654f6c26b6c564a8103781174abc540384b20f645e87531c754814cf1']

Name

9a6d4ac64fa6645c58a19b8c8795a8cb586b82f6a77aaf8f06eb83ba1f1390e8

Description

SUSP_XORed_URL_in_EXE

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9a6d4ac64fa6645c58a19b8c8795a8cb586b82f6a77aaf8f06eb83ba1f1390e8']

Name

b2c2b232bc63c8feb22b689e44ce2fb5bf85f228fef665f2f1517e542e9906c6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b2c2b232bc63c8feb22b689e44ce2fb5bf85f228fef665f2f1517e542e9906c6']

Name

4808815cb03b5f31841c74755897b65ed03e56dbddbe0d1fed06af3710f32d51

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4808815cb03b5f31841c74755897b65ed03e56dbddbe0d1fed06af3710f32d51']

Name

ce9af73be2981c874b37b767873fa4d47219810e2672bf7e0b5af8c865448069

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ce9af73be2981c874b37b767873fa4d47219810e2672bf7e0b5af8c865448069']

Name

fb48b9102388620bb02d1a47297ba101f755632f9a421d09e9ab419cbeb65db8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fb48b9102388620bb02d1a47297ba101f755632f9a421d09e9ab419cbeb65db8']

Name

bc93ef8e20f2a9a8799934d629fe494d5d82ea49e06ed8fb00ea6cc2e96f407e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bc93ef8e20f2a9a8799934d629fe494d5d82ea49e06ed8fb00ea6cc2e96f407e']

Name

332f6e99403841998f950ce2543b4a54c78aace2a2e1901b08917f63c7faa2f4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '332f6e99403841998f950ce2543b4a54c78aace2a2e1901b08917f63c7faa2f4']

Name

9e73dacedf847410dd4a0caa6aac83d31f848768336514335d4872d0fde28202

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9e73dacedf847410dd4a0caa6aac83d31f848768336514335d4872d0fde28202']

Name

d6b5f48d4e94207a5a192c1784f9f121b59311bfd6a5e94be7c55b0108c4ed93

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd6b5f48d4e94207a5a192c1784f9f121b59311bfd6a5e94be7c55b0108c4ed93']

Name

0e4b133fe7562fe5a65a8b7463f0c4f69d951f18d351cafe44e5cae393392057

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0e4b133fe7562fe5a65a8b7463f0c4f69d951f18d351cafe44e5cae393392057']

Name

b6491d99d7193499a320bf6ad638146193af2ced6128afe8af3666a828f1b900

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b6491d99d7193499a320bf6ad638146193af2ced6128afe8af3666a828f1b900']

Name

961c52567232c1f98c04b1e605c34b0309ff280afe01e1a31384589e30eccf05

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '961c52567232c1f98c04b1e605c34b0309ff280afe01e1a31384589e30eccf05']

Name

41589c4e712690af11f6d12efc6cca2d584a53142782e5f2c677b4e980fae5bd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '41589c4e712690af11f6d12efc6cca2d584a53142782e5f2c677b4e980fae5bd']

Name

78634be886ccb3949c8e5b8f0893cff32c474a466e4d4ceba35ba05c3d373bff

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '78634be886ccb3949c8e5b8f0893cff32c474a466e4d4ceba35ba05c3d373bff']

Name

2ac977e6883405e68671d523eab41fe4162b0a20fac259b201ac460a691d3f79

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2ac977e6883405e68671d523eab41fe4162b0a20fac259b201ac460a691d3f79']

Name

aa0e722832b1a039c96fd9ff169df8f48419f48e1dacf88633a5c561e6db0ba5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aa0e722832b1a039c96fd9ff169df8f48419f48e1dacf88633a5c561e6db0ba5']

Name

2643b38bdad89168baea4226dd6496b91ed283330b2c5d8ca134befa796e0f34

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2643b38bdad89168baea4226dd6496b91ed283330b2c5d8ca134befa796e0f34']

Name

f405a26904d2f6aaf4ff5f24dc345a24751d13b691a0bf17ba8c94f08ebb8b5b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f405a26904d2f6aaf4ff5f24dc345a24751d13b691a0bf17ba8c94f08ebb8b5b']

Name

f7437b4b011e57394c264ed42bb46ad6f2c6899f9ca62f507bebbff29f2a3d3f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f7437b4b011e57394c264ed42bb46ad6f2c6899f9ca62f507bebbff29f2a3d3f']

Name

a924dd46b6793ec82e1f32e3fb4215295e21c61eaafc7995cb08c20c5fbadc47

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a924dd46b6793ec82e1f32e3fb4215295e21c61eaafc7995cb08c20c5fbadc47']

Name

df07ac84fb9f6323c66036e86ad9a5f0d118734453342257f7a2d063bf69e39d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'df07ac84fb9f6323c66036e86ad9a5f0d118734453342257f7a2d063bf69e39d']

Name

c75d905cd7826182505c15d39ebe952dca5b4c80fb62b8f7283fa09d7f51c815

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c75d905cd7826182505c15d39ebe952dca5b4c80fb62b8f7283fa09d7f51c815']

Name

1fa2b3315fb2a12e65fd5258d1395597101f225e7bc204f672bcf253c82aea55

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1fa2b3315fb2a12e65fd5258d1395597101f225e7bc204f672bcf253c82aea55']

Name

dfc1e73685d3f11a3c64a50bb023532963807193169d185584f287aa8ce22a8b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dfc1e73685d3f11a3c64a50bb023532963807193169d185584f287aa8ce22a8b']

Name

70801ef4f485ba4eb8a76da0d50fc53563d82fdf37951b421b3ae864a04ccd1c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '70801ef4f485ba4eb8a76da0d50fc53563d82fdf37951b421b3ae864a04ccd1c']

Name

c68ce59f73c3d5546d500a296922d955ccc57c82b16ce4bd245ca93de3e32366

Description

Cabinet_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c68ce59f73c3d5546d500a296922d955ccc57c82b16ce4bd245ca93de3e32366']

Name

22bb73e97b01be2e11d741f3f4852380b3dae91d9ac511f33de8877a9e7c0534

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '22bb73e97b01be2e11d741f3f4852380b3dae91d9ac511f33de8877a9e7c0534']

Name

dfa442780702863bf5c71af0c475743eef754743c3d0336ff8c5032a30f30dc0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dfa442780702863bf5c71af0c475743eef754743c3d0336ff8c5032a30f30dc0']

Name

d956f2bf75d2fe9bf0d7c319b22a834976f1786b09ff1bba0d2e26c771b19ca2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd956f2bf75d2fe9bf0d7c319b22a834976f1786b09ff1bba0d2e26c771b19ca2']

Name

4a5f9f62ef8dfae47b164a4d46d242a19a11061284325e560df22b4da44bb97d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4a5f9f62ef8dfae47b164a4d46d242a19a11061284325e560df22b4da44bb97d']

Name

052309916380ef609cacb7bafbd71dc54b57f72910dca9e5f0419204dba3841d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '052309916380ef609cacb7bafbd71dc54b57f72910dca9e5f0419204dba3841d']

Name

82e4b4fddf5ea7b7c846d44bcc24d75edcec5726dfa5b81b9f43387a1fc1922a

Description

RC6_Constants

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '82e4b4fddf5ea7b7c846d44bcc24d75edcec5726dfa5b81b9f43387a1fc1922a']

Name

12f16409b6191e3b2c5fd874cca5010711347d28900c108506dbc7f4d403c365

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '12f16409b6191e3b2c5fd874cca5010711347d28900c108506dbc7f4d403c365']

Country

Name
Ukraine

Malware

Name
PowerMagic

Name
DboxShell

Name
Red Stinger

StixFile

Value
c68ce59f73c3d5546d500a296922d955ccc57c82b16ce4bd245ca93de3e32366
2643b38bdad89168baea4226dd6496b91ed283330b2c5d8ca134befa796e0f34
9e73dacedf847410dd4a0caa6aac83d31f848768336514335d4872d0fde28202
82e4b4fddf5ea7b7c846d44bcc24d75edcec5726dfa5b81b9f43387a1fc1922a
301e819008e19b9803ad8b75ecede9ecfa5b11a3ecd8df0316914588b95371c8
22bb73e97b01be2e11d741f3f4852380b3dae91d9ac511f33de8877a9e7c0534
fbe650223893284282e0be8f7719b554ff7a1d9fbbc72d3e17a47a9a1ceb6231
b6491d99d7193499a320bf6ad638146193af2ced6128afe8af3666a828f1b900
f405a26904d2f6aaf4ff5f24dc345a24751d13b691a0bf17ba8c94f08ebb8b5b
78634be886ccb3949c8e5b8f0893cff32c474a466e4d4ceba35ba05c3d373bff
a924dd46b6793ec82e1f32e3fb4215295e21c61eaafc7995cb08c20c5fbadc47
70801ef4f485ba4eb8a76da0d50fc53563d82fdf37951b421b3ae864a04ccd1c
fb48b9102388620bb02d1a47297ba101f755632f9a421d09e9ab419cbeb65db8

332f6e99403841998f950ce2543b4a54c78aace2a2e1901b08917f63c7faa2f4

9c16cf1f962bf736e3d6fb9ec3a37bb6f92c5f6cb1886d4332694ccc94735de8

df07ac84fb9f6323c66036e86ad9a5f0d118734453342257f7a2d063bf69e39d

aa0e722832b1a039c96fd9ff169df8f48419f48e1dacf88633a5c561e6db0ba5

dfa442780702863bf5c71af0c475743eef754743c3d0336ff8c5032a30f30dc0

9a6d4ac64fa6645c58a19b8c8795a8cb586b82f6a77aaf8f06eb83ba1f1390e8

12f16409b6191e3b2c5fd874cca5010711347d28900c108506dbc7f4d403c365

4a5f9f62ef8dfae47b164a4d46d242a19a11061284325e560df22b4da44bb97d

41589c4e712690af11f6d12efc6cca2d584a53142782e5f2c677b4e980fae5bd

0e4b133fe7562fe5a65a8b7463f0c4f69d951f18d351cafe44e5cae393392057

2ac977e6883405e68671d523eab41fe4162b0a20fac259b201ac460a691d3f79

dfc1e73685d3f11a3c64a50bb0235329638071931 69d185584f287aa8ce22a8b

f7437b4b011e57394c264ed42bb46ad6f2c6899f9ca62f507bebbff29f2a3d3f

b2c2b232bc63c8feb22b689e44ce2fb5bf85f228fef665f2f1517e542e9906c6

c75d905cd7826182505c15d39ebe952dca5b4c80fb62b8f7283fa09d7f51c815

961c52567232c1f98c04b1e605c34b0309ff280afe01e1a31384589e30eccf05

d6b5f48d4e94207a5a192c1784f9f121b59311bfd6a5e94be7c55b0108c4ed93

ce9af73be2981c874b37b767873fa4d47219810e2672bf7e0b5af8c865448069

d956f2bf75d2fe9bf0d7c319b22a834976f1786b09ff1bba0d2e26c771b19ca2

8aa19e3654f6c26b6c564a8103781174abc540384b20f645e87531c754814cf1

052309916380ef609cacb7bafbd71dc54b57f72910dca9e5f0419204dba3841d

1fa2b3315fb2a12e65fd5258d1395597101f225e7bc204f672bcf253c82aea55

4808815cb03b5f31841c74755897b65ed03e56dbddbe0d1fed06af3710f32d51

bc93ef8e20f2a9a8799934d629fe494d5d82ea49e06ed8fb00ea6cc2e96f407e

External References

- https://otx.alienvault.com/pulse/645d0d54b53b61ad269d68e3
- https://www.malwarebytes.com/blog/threat-intelligence/2023/05/redstinger