Jul 13 2023

NETMANAGEIT

Intelligence Report

Malicious campaigns target government, military and civilian entities in Ukraine, Poland

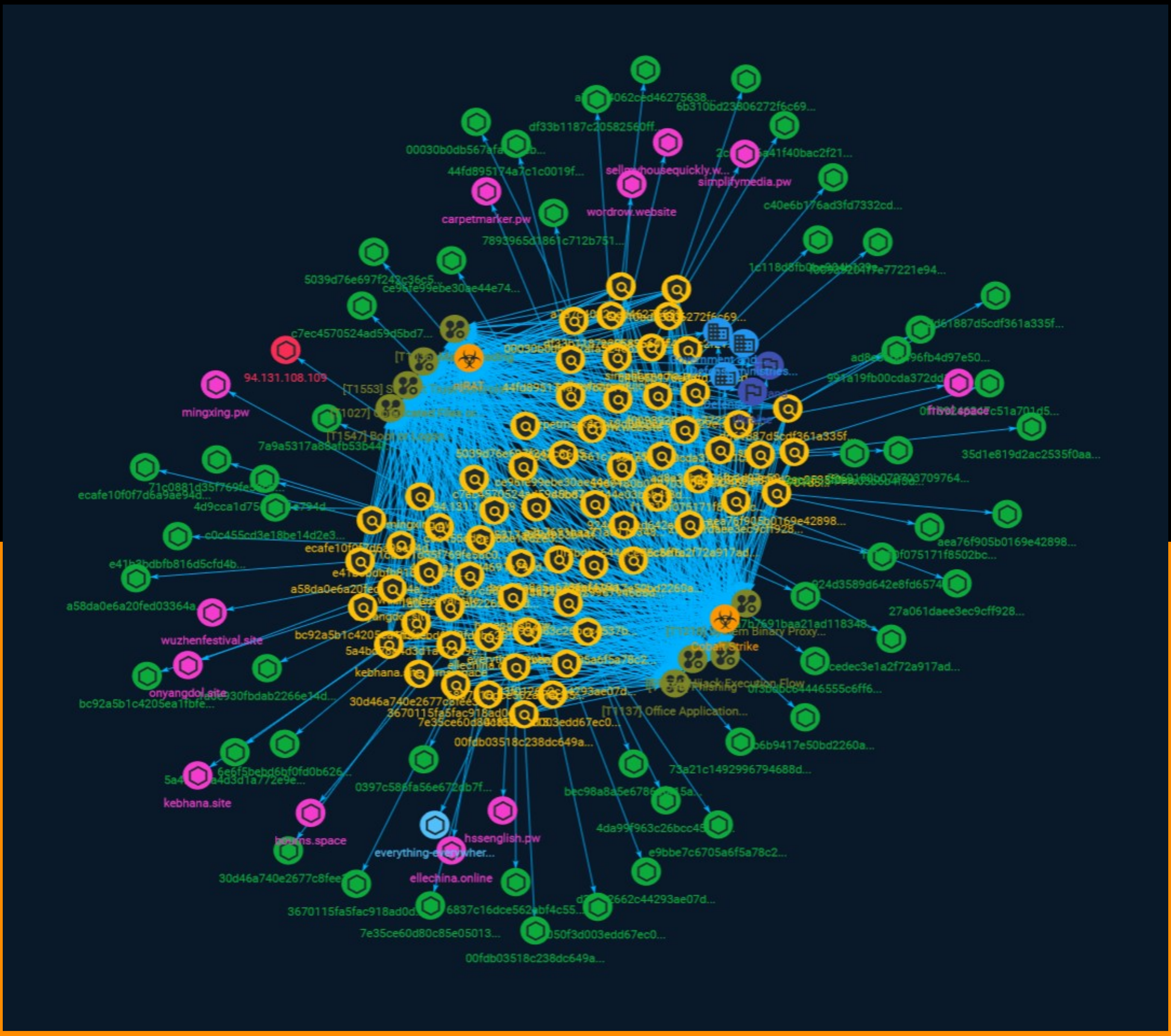

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A threat actor is targeting government and military targets in Ukraine and Poland, Cisco Talos has discovered, as part of a series of operations linked to the Belarusian government, which it believes may be carrying out a sophisticated cyber-attack.

Confidence

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

15 / 100

Indicator

Name

0397c586fa56e672db7f14afa8c19992b6e08ab0c1d282c960df1af26371bd72

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'0397c586fa56e672db7f14afa8c19992b6e08ab0c1d282c960df1af26371bd72']

Name

71c0881d35f769fe58c084883d2aaee9ec284fcdc04500e5e5272973dfc78944

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'71c0881d35f769fe58c084883d2aaee9ec284fcdc04500e5e5272973dfc78944']

Name

7a9a5317a88afb53b44f6cfed59c48907f63aaa7ef63b1587f990951c423c211

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7a9a5317a88afb53b44f6cfed59c48907f63aaa7ef63b1587f990951c423c211']

Name

4d9cca1d75d4691e794dfe9efb9eef6e9e64b4e978ad17831b459d4bb6722829

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4d9cca1d75d4691e794dfe9efb9eef6e9e64b4e978ad17831b459d4bb6722829']

Name

wordrow.website

Pattern Type

stix

Pattern

[domain-name:value = 'wordrow.website']

Name

924d3589d642e8fd65746dc156ff9f104d43114a04ea9509f51ee6a439d1915b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '924d3589d642e8fd65746dc156ff9f104d43114a04ea9509f51ee6a439d1915b']

Name

1a0e930fbdab2266e14dc501abdbb5623b5762d687df3670d86bb05f252509ac

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1a0e930fbdab2266e14dc501abdbb5623b5762d687df3670d86bb05f252509ac']

Name

40b87c5444e03b6b4f3d38315c1525cedfafc20355fff84502cc594799dc41df

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '40b87c5444e03b6b4f3d38315c1525cedfafc20355fff84502cc594799dc41df']

Name

bec98a8a5e6786ef415a7a7bf7e60cbd384d43ede4e882aa560fdcb24865ac55

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bec98a8a5e6786ef415a7a7bf7e60cbd384d43ede4e882aa560fdcb24865ac55']

Name

e41b3bdbfb816d5cfd4b235d2b985894153c41da6726ebfa83e45f3b5b4a1945

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e41b3bdbfb816d5cfd4b235d2b985894153c41da6726ebfa83e45f3b5b4a1945']

Name

f00939201f7e77221e94e917a8e34c3d2143324e02fdf35058526d870a0023a0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f00939201f7e77221e94e917a8e34c3d2143324e02fdf35058526d870a0023a0']

Name

everything-everywhere.at.ply.gg

Pattern Type

stix

Pattern

[hostname:value = 'everything-everywhere.at.ply.gg']

Name

7893965d1861c712b751bc2d5fb53a34ec0d276bcf389b7fc574728940575152

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7893965d1861c712b751bc2d5fb53a34ec0d276bcf389b7fc574728940575152']

Name

ce96fe99ebe30ae44e74c22c0b2a055005d0da131e0082a1c290ddeb79dd1114

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ce96fe99ebe30ae44e74c22c0b2a055005d0da131e0082a1c290ddeb79dd1114']

Name

hssenglish.pw

Pattern Type

stix

Pattern

[domain-name:value = 'hssenglish.pw']

Name

sellmyhousequickly.website

Pattern Type

stix

Pattern

[domain-name:value = 'sellmyhousequickly.website']

Name

0f3bdbc64446555c6ff611b02f2e64250fcaf39b78237ae4cca7c74d94731b32

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0f3bdbc64446555c6ff611b02f2e64250fcaf39b78237ae4cca7c74d94731b32']

Name

c7ec4570524ad59d5bd7a3e8f0d23c8cf05cc0e8a98dcdbec00c9dc075084558

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c7ec4570524ad59d5bd7a3e8f0d23c8cf05cc0e8a98dcdbec00c9dc075084558']

Name

f11310f075171f8502bcd32dcb2fe5894808b17a37f6fd960fb26653871e7b7d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'f11310f075171f8502bcd32dcb2fe5894808b17a37f6fd960fb26653871e7b7d']

Name

a7b7691baa21ad118348661a035b69605a6efd1cd1fa0fd52e5645c64f5f61e6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'a7b7691baa21ad118348661a035b69605a6efd1cd1fa0fd52e5645c64f5f61e6']

Name

carpetmarker.pw

Pattern Type

stix

Pattern

[domain-name:value = 'carpetmarker.pw']

Name

1c118d8fb0be904b129e4552f86cd0b3e239ecd25f4d599c54cc96c1096747af

Pattern Type

stix

Pattern
[file:hashes.'SHA-256' = '1c118d8fb0be904b129e4552f86cd0b3e239ecd25f4d599c54cc96c1096747af']
Name
ellechina.online
Pattern Type
stix
Pattern
[domain-name:value = 'ellechina.online']
Name
991a19fb00cda372dd1ce4a42580dc40872da5c5bfbb34301615f3870ea3fb58
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '991a19fb00cda372dd1ce4a42580dc40872da5c5bfbb34301615f3870ea3fb58']
Name
41f050f3d003edd67ec02710c60a7b4022685465cb61ae37fc0b3193c1dab5cb
Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '41f050f3d003edd67ec02710c60a7b4022685465cb61ae37fc0b3193c1dab5cb']

Name

94.131.108.109

Description

CC=TR ASN=AS44477 Stark Industries Solutions Ltd

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.131.108.109']

Name

frivol.space

Pattern Type

stix

Pattern

[domain-name:value = 'frivol.space']

Name
7e35ce60d80c85e050133de142a3b261160259846c9c967c7b2bb84923328f8c
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '7e35ce60d80c85e050133de142a3b261160259846c9c967c7b2bb84923328f8c']
Name
00030b0db567afa524eb68faf6f194f25bc5361c380599668a82dbae12af088e
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '00030b0db567afa524eb68faf6f194f25bc5361c380599668a82dbae12af088e']
Name
ad8e3ebd496fb4d97e5075adb4f2f1b91195cca059800d0acd182a07698c13b6
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' =
'ad8e3ebd496fb4d97e5075adb4f2f1b91195cca059800d0acd182a07698c13b6']

Name

6e6f5bebd6bf0fd0b626d6521cdb4faa06275f558bacd419c76702e2728f734c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'6e6f5bebd6bf0fd0b626d6521cdb4faa06275f558bacd419c76702e2728f734c']

Name

simplifymedia.pw

Pattern Type

stix

Pattern

[domain-name:value = 'simplifymedia.pw']

Name

e9bbe7c6705a6f5a78c2a9b8060a7e32374b81058f7c2f24851c4d1ea38d7411

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'e9bbe7c6705a6f5a78c2a9b8060a7e32374b81058f7c2f24851c4d1ea38d7411']

Name

5039d76e697f242c36c5a0ebf7dec127757bc34ddaf33c58251c2798da3ce03e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'5039d76e697f242c36c5a0ebf7dec127757bc34ddaf33c58251c2798da3ce03e']

Name

0f189246247c51a701d5a88a06e1fc4932f333d24d7ff40dc8152ad6224f6ca4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'0f189246247c51a701d5a88a06e1fc4932f333d24d7ff40dc8152ad6224f6ca4']

Name

bourns.space

Pattern Type
stix
Pattern
[domain-name:value = 'bourns.space']
Name
df33b1187c20582560ffaa1c3e86b92003c4a7c8a61acbbe886ab195531c5c89
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'df33b1187c20582560ffaa1c3e86b92003c4a7c8a61acbbe886ab195531c5c89']
Name
73a21c1492996794688d9751edd1e5c287da645fa7a960e945bb4ea69855424a
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '73a21c1492996794688d9751edd1e5c287da645fa7a960e945bb4ea69855424a']
Name

wuzhenfestival.site

Pattern Type

stix

Pattern

[domain-name:value = 'wuzhenfestival.site']

Name

dd61887d5cdf361a335fec917cd6d1bb186aad56b1f9f5d09b66355ff7f41751

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dd61887d5cdf361a335fec917cd6d1bb186aad56b1f9f5d09b66355ff7f41751']

Name

3670115fa5fac918ad0dafe399568788690f0f205dd0bebe4f55180fd70d36e9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3670115fa5fac918ad0dafe399568788690f0f205dd0bebe4f55180fd70d36e9']

Name

mingxing.pw

Pattern Type

stix

Pattern

[domain-name:value = 'mingxing.pw']

Name

aea76f905b0169e4289895a8d85980896f802fd18fe246a27d601310bfa5905e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aea76f905b0169e4289895a8d85980896f802fd18fe246a27d601310bfa5905e']

Name

30d46a740e2677c8fee383c2a4762561a10c66c5b99215262e42bfabf6bfb1aa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'30d46a740e2677c8fee383c2a4762561a10c66c5b99215262e42bfabf6bfb1aa']

Name

2c5ba56a41f40bac2f21065fb9883545ef8d359883cb7bc351c481cb9542e104

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'2c5ba56a41f40bac2f21065fb9883545ef8d359883cb7bc351c481cb9542e104']

Name

d3f012662c44293ae07d8c763914db18fc9795673da7c1cdc4d862b1a7c887b9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'd3f012662c44293ae07d8c763914db18fc9795673da7c1cdc4d862b1a7c887b9']

Name

ecafe10f0f7d6a9ae94d9735b45f88492b6ea11ff58f37e62fbf7070778af20a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ecafe10f0f7d6a9ae94d9735b45f88492b6ea11ff58f37e62fbf7070778af20a']

Name

35d1e819d2ac2535f0aa9e2294570135f37519386872c415e326146e931b8fb9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '35d1e819d2ac2535f0aa9e2294570135f37519386872c415e326146e931b8fb9']

Name

kebhana.site

Pattern Type

stix

Pattern

[domain-name:value = 'kebhana.site']

Name

a7a7c4062ced46275638719c100ea2397c673148e8473e56a3ec4313ca7dc5f9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a7a7c4062ced46275638719c100ea2397c673148e8473e56a3ec4313ca7dc5f9']

Name

a5fb6b9417e50bd2260afdcdb5a9eed33e48a283a51408344a4caa2b1025b9a7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a5fb6b9417e50bd2260afdcdb5a9eed33e48a283a51408344a4caa2b1025b9a7']

Name

a58da0e6a20fed03364a0cbae18008eb4f8d6bee7c9f5e8ffcdac34fb823d363

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a58da0e6a20fed03364a0cbae18008eb4f8d6bee7c9f5e8ffcdac34fb823d363']

Name
6b310bd23806272f6c69b84a0381915f16d705e79ce423f19de940247543c76a
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '6b310bd23806272f6c69b84a0381915f16d705e79ce423f19de940247543c76a']
Name
6837c16dce562abf4c55949cfc8d00b019f7fcc6db6a2e9a71d268312fba813e
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '6837c16dce562abf4c55949cfc8d00b019f7fcc6db6a2e9a71d268312fba813e']
Name
44fd895174a7c1c0019fc95bb04201106dc165704c70e902e3de58db98f03c7e
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' =
'44fd895174a7c1c0019fc95bb04201106dc165704c70e902e3de58db98f03c7e']

Name

27a061daee3ec9cff928b8152159a472797821834a3aa7639749489b90f703c3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'27a061daee3ec9cff928b8152159a472797821834a3aa7639749489b90f703c3']

Name

5a4bd78a4d3d1a772e9e9b14983646a4c1c6a25cc983b804e4522774ebfa1c14

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'5a4bd78a4d3d1a772e9e9b14983646a4c1c6a25cc983b804e4522774ebfa1c14']

Name

5969180b072703709764d1ca40be3eeb40f2eb0090859b3743cc21b884fa2106

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'5969180b072703709764d1ca40be3eeb40f2eb0090859b3743cc21b884fa2106']

Name

4da99f963c26bcc4537ba0437c9cc1445be8bea64067d34308dda6c2e49c8c65

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'4da99f963c26bcc4537ba0437c9cc1445be8bea64067d34308dda6c2e49c8c65']

Name

onyangdol.site

Pattern Type

stix

Pattern

[domain-name:value = 'onyangdol.site']

Name

c40e6b176ad3fd7332cd217191e557352ef4b82bf91f29939121267598737990

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'c40e6b176ad3fd7332cd217191e557352ef4b82bf91f29939121267598737990']

Name

00fdb03518c238dc649a39e94f0bcc95dacf3b832979d14d0ed5194b9b482b87

Description

#Lowfi:Lua:Mampa:99!ml

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'00fdb03518c238dc649a39e94f0bcc95dacf3b832979d14d0ed5194b9b482b87']

Name

c0c455cd3e18be14d2e34cf4e3fb98e7ab0a75ef04b6049ff9f7b306d62704b8

Description

DotNET_Reactor

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'c0c455cd3e18be14d2e34cf4e3fb98e7ab0a75ef04b6049ff9f7b306d62704b8']

Name

4cedec3e1a2f72a917ad9a59ebe116ed50c3268567946d1e493c8163486b888b

Description

#Lowfi:Lua:Mampa:99!ml

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'4cedec3e1a2f72a917ad9a59ebe116ed50c3268567946d1e493c8163486b888b']

Name

bc92a5b1c4205ea1fbfec9144b8aab485e095142c7105c9d616b089ec668f198

Description

SLFPER:MSIL/AsmblyLoadInvoke

Pattern Type

stix

Pattern
[file:hashes.'SHA-256' = 'bc92a5b1c4205ea1fbfec9144b8aab485e095142c7105c9d616b089ec668f198']

Country

Name
Poland

Name
Ukraine

Malware

Name

njRAT

Description

[njRAT](https://attack.mitre.org/software/S0385) is a remote access tool (RAT) that was first observed in 2012. It has been used by threat actors in the Middle East.(Citation: Fidelis njRAT June 2013)

Name

Cobalt Strike

Description

[Cobalt Strike](https://attack.mitre.org/software/S0154) is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors". Cobalt Strike's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.(Citation: cobaltstrike manual) In addition to its own capabilities, [Cobalt Strike](https://attack.mitre.org/software/S0154) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: cobaltstrike manual)

Attack-Pattern

Name
Office Application Startup
ID
T1137
Description
Adversaries may leverage Microsoft Office-based applications for persistence between startups. Microsoft Office is a fairly common application suite on Windows-based operating systems within an enterprise network. There are multiple mechanisms that can be used with Office for persistence when an Office-based application is started; this can include the use of Office Template Macros and add-ins. A variety of features have been discovered in Outlook that can be abused to obtain persistence, such as Outlook rules, forms, and Home Page.(Citation: SensePost Ruler GitHub) These persistence mechanisms can work within Outlook or be used through Office 365.(Citation: TechNet O365 Outlook Rules)
Name
Subvert Trust Controls
ID
T1553

Description

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site. Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [Modify Registry](https://attack.mitre.org/techniques/T1112) in support of subverting these controls. (Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)

Name

Hijack Execution Flow

ID

T1574

Description

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution. There are many ways an adversary may hijack the flow of execution, including by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be intercepted. Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads.

Name

Boot or Logon Autostart Execution

ID

T1547

Description

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

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
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

System Binary Proxy Execution

ID

T1218

Description

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.(Citation: LOLBAS Project) Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands. Similarly, on Linux systems adversaries may abuse trusted binaries such as `split` to proxy execution of malicious commands.(Citation: split man page)(Citation: GTFO split)

Sector

Name

Defense

Description

Public and private entities involved in the conception and production of weapons and the planning and conducting of military operations.

Name

Defense ministries (including the military)

Description

Includes the military and all defense related-space activities.

Name

Government and administrations

Description

Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Domain-Name

Value
hssenglish.pw
sellmyhousequickly.website
ellechina.online
bourns.space
wordrow.website
wuzhenfestival.site
simplifymedia.pw
frivol.space
kebhana.site
carpetmarker.pw
mingxing.pw
onyangdol.site

StixFile

Value
a7b7691baa21ad118348661a035b69605a6efd1cd1fa0fd52e5645c64f5f61e6
0f3bdbc64446555c6ff611b02f2e64250fcaf39b78237ae4cca7c74d94731b32
e41b3bdbfb816d5cfd4b235d2b985894153c41da6726ebfa83e45f3b5b4a1945
d3f012662c44293ae07d8c763914db18fc9795673da7c1cdc4d862b1a7c887b9
4da99f963c26bcc4537ba0437c9cc1445be8bea64067d34308dda6c2e49c8c65
2c5ba56a41f40bac2f21065fb9883545ef8d359883cb7bc351c481cb9542e104
30d46a740e2677c8fee383c2a4762561a10c66c5b99215262e42bfabf6bfb1aa
1a0e930fbdab2266e14dc501abdbb5623b5762d687df3670d86bb05f252509ac
5039d76e697f242c36c5a0ebf7dec127757bc34ddaf33c58251c2798da3ce03e
5969180b072703709764d1ca40be3eeb40f2eb0090859b3743cc21b884fa2106
4d9cca1d75d4691e794dfe9efb9eef6e9e64b4e978ad17831b459d4bb6722829
40b87c5444e03b6b4f3d38315c1525cedfafc20355fff84502cc594799dc41df
a58da0e6a20fed03364a0cbae18008eb4f8d6bee7c9f5e8ffcdac34fb823d363

71c0881d35f769fe58c084883d2aaee9ec284fcdc04500e5e5272973dfc78944

a5fb6b9417e50bd2260afdcdb5a9eed33e48a283a51408344a4caa2b1025b9a7

7a9a5317a88afb53b44f6cfed59c48907f63aaa7ef63b1587f990951c423c211

aea76f905b0169e4289895a8d85980896f802fd18fe246a27d601310bfa5905e

27a061daee3ec9cff928b8152159a472797821834a3aa7639749489b90f703c3

00030b0db567afa524eb68faf6f194f25bc5361c380599668a82dbae12af088e

991a19fb00cda372dd1ce4a42580dc40872da5c5bfbb34301615f3870ea3fb58

0397c586fa56e672db7f14afa8c19992b6e08ab0c1d282c960df1af26371bd72

a7a7c4062ced46275638719c100ea2397c673148e8473e56a3ec4313ca7dc5f9

41f050f3d003edd67ec02710c60a7b4022685465cb61ae37fc0b3193c1dab5cb

6b310bd23806272f6c69b84a0381915f16d705e79ce423f19de940247543c76a

924d3589d642e8fd65746dc156ff9f104d43114a04ea9509f51ee6a439d1915b

73a21c1492996794688d9751edd1e5c287da645fa7a960e945bb4ea69855424a

1c118d8fb0be904b129e4552f86cd0b3e239ecd25f4d599c54cc96c1096747af

7e35ce60d80c85e050133de142a3b261160259846c9c967c7b2bb84923328f8c

5a4bd78a4d3d1a772e9e9b14983646a4c1c6a25cc983b804e4522774ebfa1c14

3670115fa5fac918ad0dafe399568788690f0f205dd0bebe4f55180fd70d36e9

ecafe10f0f7d6a9ae94d9735b45f88492b6ea11ff58f37e62fbf7070778af20a

0f189246247c51a701d5a88a06e1fc4932f333d24d7ff40dc8152ad6224f6ca4
f00939201f7e77221e94e917a8e34c3d2143324e02fdf35058526d870a0023a0
bec98a8a5e6786ef415a7a7bf7e60cbd384d43ede4e882aa560fdcb24865ac55
c7ec4570524ad59d5bd7a3e8f0d23c8cf05cc0e8a98dcdbec00c9dc075084558
35d1e819d2ac2535f0aa9e2294570135f37519386872c415e326146e931b8fb9
df33b1187c20582560ffaa1c3e86b92003c4a7c8a61acbbe886ab195531c5c89
44fd895174a7c1c0019fc95bb04201106dc165704c70e902e3de58db98f03c7e
f11310f075171f8502bcd32dcb2fe5894808b17a37f6fd960fb26653871e7b7d
ad8e3ebd496fb4d97e5075adb4f2f1b91195cca059800d0acd182a07698c13b6
6e6f5bebd6bf0fd0b626d6521cdb4faa06275f558bacd419c76702e2728f734c
ce96fe99ebe30ae44e74c22c0b2a055005d0da131e0082a1c290ddeb79dd1114
7893965d1861c712b751bc2d5fb53a34ec0d276bcf389b7fc574728940575152
e9bbe7c6705a6f5a78c2a9b8060a7e32374b81058f7c2f24851c4d1ea38d7411
6837c16dce562abf4c55949cfc8d00b019f7fcc6db6a2e9a71d268312fba813e
dd61887d5cdf361a335fec917cd6d1bb186aad56b1f9f5d09b66355ff7f41751
4cedec3e1a2f72a917ad9a59ebe116ed50c3268567946d1e493c8163486b888b
c40e6b176ad3fd7332cd217191e557352ef4b82bf91f29939121267598737990
c0c455cd3e18be14d2e34cf4e3fb98e7ab0a75ef04b6049ff9f7b306d62704b8

bc92a5b1c4205ea1fbfec9144b8aab485e095142c7105c9d616b089ec668f198

00fdb03518c238dc649a39e94f0bcc95dacf3b832979d14d0ed5194b9b482b87

Hostname

Value
everything-everywhere.at.ply.gg

IPv4-Addr

Value
94.131.108.109

External References

- https://otx.alienvault.com/pulse/64b04758abb03a6d38607273
- https://blog.talosintelligence.com/malicious-campaigns-target-entities-in-ukraine-poland/
- https://raw.githubusercontent.com/Cisco-Talos/IOCs/main/2023/07/malicious-campaigns-target-entities-in-ukraine-poland.txt