Aug 18 2023

NETMANAGEIT

Intelligence Report

DotRunpeX - demystifying new virtualized .NET injector used in the wild

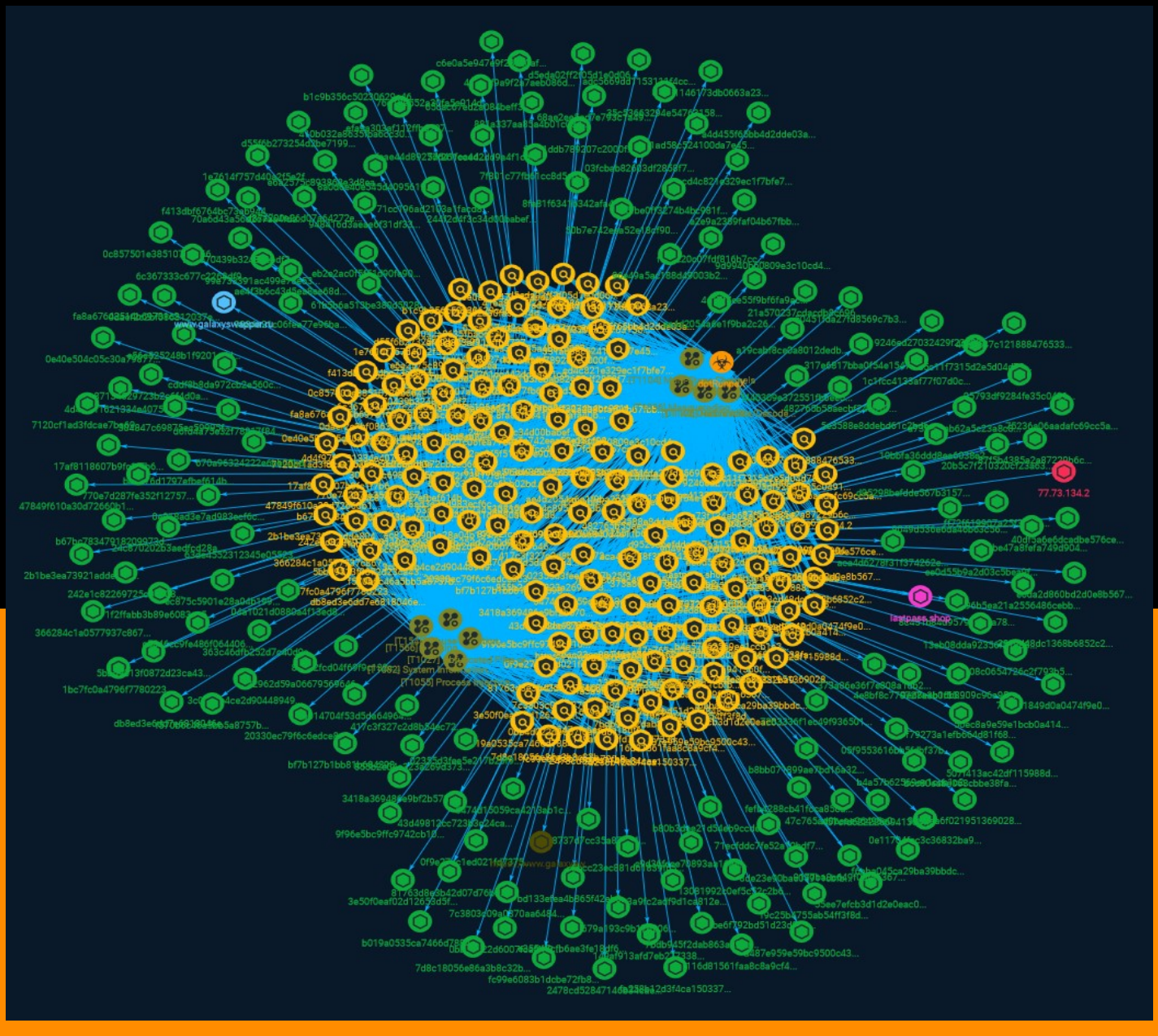

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Check Point Research has identified a new type of malware that is being used in the wild to deliver a variety of known malware families, mainly related to stealers, RATs and downloaders.

Confidence

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

15 / 100

Indicator

Name
ae4d2054a6e1f9ba2c269eace61aac7259adb0645d18da82779717d83174837d
Description
Win64:PWSX-gen\ [Trj]
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ae4d2054a6e1f9ba2c269eace61aac7259adb0645d18da82779717d83174837d']
Name
cb014704f53d5da64964c2b0bfc7e13bbdf389555294c6f6c98c2527f6406d6d
Description
Win64:PWSX-gen\ [Trj]
Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cb014704f53d5da64964c2b0bfc7e13bbdf389555294c6f6c98c2527f6406d6d']

Name

ddae8737d7cc35a87274a26b886e6b48ae947aa849c3d7ecb84de6f6d553aa96

Description

Generic Stealer, RecordBreaker

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ddae8737d7cc35a87274a26b886e6b48ae947aa849c3d7ecb84de6f6d553aa96']

Name

61b5b6a513be380d50282c1c8391a5362d746bd70506343d04bda3751c3b25de

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '61b5b6a513be380d50282c1c8391a5362d746bd70506343d04bda3751c3b25de']

Name

948416d3aeae6f31df3341118a25a4231a7eed23b3db73a022e9da70734163c9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '948416d3aeae6f31df3341118a25a4231a7eed23b3db73a022e9da70734163c9']

Name

670a96324222e6bb02bd36c7e5b100fb5d52d2d59891bd9599b1a47438ac9578

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '670a96324222e6bb02bd36c7e5b100fb5d52d2d59891bd9599b1a47438ac9578']

Name

855b2e04c323a269d3731c093f0bc80ab3497a69ab8d2967847451a87f04fb0a

Description

Generic Stealer, RecordBreaker

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '855b2e04c323a269d3731c093f0bc80ab3497a69ab8d2967847451a87f04fb0a']

Name

fcc4c20c07fdf816b7cc6dfba34d42af827ecf01e9972f266ac395e54db028af

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fcc4c20c07fdf816b7cc6dfba34d42af827ecf01e9972f266ac395e54db028af']

Name

8c451b84d9579b625a7821ad7ddcb87bdd665a9e6619eaecf6ab93cd190cf504

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8c451b84d9579b625a7821ad7ddcb87bdd665a9e6619eaecf6ab93cd190cf504']

Name

244f2d4f3c34d00babef5f1765e91c0abda9dbd1d131fc93ecb48c91ecc801a8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '244f2d4f3c34d00babef5f1765e91c0abda9dbd1d131fc93ecb48c91ecc801a8']

Name

ae4f3b6c43d5ea8ee68d862362d4e8d7b317889eb9abead948a9b791ad9d7071

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ae4f3b6c43d5ea8ee68d862362d4e8d7b317889eb9abead948a9b791ad9d7071']

Name

0f9e27ec1ed021fd7375ca46f233c06b354d12d57aed44132208cd9308bfee11

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0f9e27ec1ed021fd7375ca46f233c06b354d12d57aed44132208cd9308bfee11']

Name

71cc196ad2103a1facd81f2b8bd985273f682019b2a88841d2f34ecc373d1d69

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '71cc196ad2103a1facd81f2b8bd985273f682019b2a88841d2f34ecc373d1d69']

Name

8fa81f6341b342afa40b7dc76dd6e0a1874583d12ea04acf839251cb5ca61591

Description

Win64:RATX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8fa81f6341b342afa40b7dc76dd6e0a1874583d12ea04acf839251cb5ca61591']

Name

363c46dfb252d7c40d9c3bb63bdc40c2eff0ce16c0c1b77f507d73058104c6e1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '363c46dfb252d7c40d9c3bb63bdc40c2eff0ce16c0c1b77f507d73058104c6e1']

Name

8a0d6e40e545d40956194230f03608859f2a47420a9b11b199142641bc6419ee

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8a0d6e40e545d40956194230f03608859f2a47420a9b11b199142641bc6419ee']

Name

482765b55aecbf24eb102f531afb6c8905ab7a058a447d217be70984f15b4573

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '482765b55aecbf24eb102f531afb6c8905ab7a058a447d217be70984f15b4573']

Name

417c3f327c2d8b54ec72a5a89280fecb589a3e0b89c281bbc077d7de445cc76b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '417c3f327c2d8b54ec72a5a89280fecb589a3e0b89c281bbc077d7de445cc76b']

Name

1c1fcc4133af77f07d0c0299d0320aa9f447748ebead74b429f73c44d950e38b

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1c1fcc4133af77f07d0c0299d0320aa9f447748ebead74b429f73c44d950e38b']

Name

bd133efea4b865f42eb05e0c92e3ab3b58ac087c0682ea9112b96596a7111ff6

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bd133efea4b865f42eb05e0c92e3ab3b58ac087c0682ea9112b96596a7111ff6']

Name

7263336f1ec49f936501c508a9edf072a81002e64e52a1ed0cafb1378bb07a2a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7263336f1ec49f936501c508a9edf072a81002e64e52a1ed0cafb1378bb07a2a']

Name

eb2e2ac0f5f51d90fe90b63c3c385af155b2fee30bc3dc6309776b90c21320f5

Description

Win64:RATX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'eb2e2ac0f5f51d90fe90b63c3c385af155b2fee30bc3dc6309776b90c21320f5']

Name

c5646cc9fe486f0644067fc294f83eb6a39ce6f28eea3708c9bf49e244acc0f9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c5646cc9fe486f0644067fc294f83eb6a39ce6f28eea3708c9bf49e244acc0f9']

Name

9984a21c06fea77e96ba410cffb99de530201ef0c74f3e8b38b3afd4fdf0b333

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9984a21c06fea77e96ba410cffb99de530201ef0c74f3e8b38b3afd4fdf0b333']

Name

https://www.galaxyswapper.ru/

Pattern Type

stix

Pattern

[url:value = 'https://www.galaxyswapper.ru/']

Name

304847c69875ec59995fbb453f8d1106f80c5eb380ae6b8676e76f5372290194

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '304847c69875ec59995fbb453f8d1106f80c5eb380ae6b8676e76f5372290194']

Name

05f9553616bb5fdbf37bd4036c210929e08d7181de898c1bea1bdae7afb0766f

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '05f9553616bb5fdbf37bd4036c210929e08d7181de898c1bea1bdae7afb0766f']

Name

bf7b127b1bb81b68439851386cd3d1600bb8b9ec56135e668a88062d913410dd

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bf7b127b1bb81b68439851386cd3d1600bb8b9ec56135e668a88062d913410dd']

Name

03fcbab82603df2858f7d6fefdb6ae3cc8e17393af6d44f24634d28fccf3f181

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '03fcbab82603df2858f7d6fefdb6ae3cc8e17393af6d44f24634d28fccf3f181']

Name

a19cabf8ce0a8012dedbf65855981db1efa3b9773365554401a74bfb7a45490f

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a19cabf8ce0a8012dedbf65855981db1efa3b9773365554401a74bfb7a45490f']

Name

5474d15059ca4213ab1c13fba25ab8ba38559cac7ec2ab336d2411b90eab1217

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5474d15059ca4213ab1c13fba25ab8ba38559cac7ec2ab336d2411b90eab1217']

Name

35c11f7315d2e5d04d783de4314d8cde2def382f1e3fc49ccc555337c54d63cc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '35c11f7315d2e5d04d783de4314d8cde2def382f1e3fc49ccc555337c54d63cc']

Name

f440309e372551fb6ee00ecca71a70a1b8b7e077fe61b0687411147b582ab415

Description

Generic Stealer, RecordBreaker

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f440309e372551fb6ee00ecca71a70a1b8b7e077fe61b0687411147b582ab415']

Name

e6a2575c893868e3d8ea5982699c9c2b75a07b8ec092b0cb26d7b5c3c2640f33

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e6a2575c893868e3d8ea5982699c9c2b75a07b8ec092b0cb26d7b5c3c2640f33']

Name

77.73.134.2

Description

ISP: GLOBAL INTERNET SOLUTIONS LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **8000:**

``` HTTP/1.0 407 Proxy Authentication Required Proxy-Authenticate: Basic realm="proxy" Connection: close Content-type: text/html; charset=utf-8 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '77.73.134.2']

Name

43d49812cc723b3c24ca7048faa859800c7e303e074243e4348f65d34127367b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '43d49812cc723b3c24ca7048faa859800c7e303e074243e4348f65d34127367b']

Name

1321037324c895784e3bc9bc8ef7b9e4d2ece075

Description

Detects new and old version of dotRunpeX - configurable .NET injector

Pattern Type

yara
```

Pattern

```
rule injector_ZZ_dotRunpeX_oldnew { meta: description = "Detects new and old version of dotRunpeX - configurable .NET injector" author = "Jiri Vinopal (jiriv)" date = "2022-10-30" hash1_New = "373a86e36f7e808a1db263b4b49d2428df4a13686da7d77edba7a6dd63790232" // injects Formbook hash2_New = "41ea8f9a9f2a7aeb086dedf8e5855b0409f31e7793cbba615ca0498e47a72636" // injects Formbook hash3_New = "5e3588e8ddebd61c2bd6dab4b87f601bd6a4857b33eb281cb5059c29cfe62b80" // injects AsyncRat hash4_New = "8c451b84d9579b625a7821ad7ddcb87bdd665a9e6619eaecf6ab93cd190cf504" // injects Remcos hash5_New = "8fa81f6341b342afa40b7dc76dd6e0a1874583d12ea04acf839251cb5ca61591" // injects Formbook hash6_New = "cd4c821e329ec1f7bfe7ecd39a6020867348b722e8c84a05c7eb32f8d5a2f4db" // injects AgentTesla hash7_New = "fa8a67642514b69731c2ce6d9e980e2a9c9e409b3947f2c9909d81f6eac81452" // injects AsyncRat hash8_New = "eb2e2ac0f5f51d90fe90b63c3c385af155b2fee30bc3dc6309776b90c21320f5" // injects SnakeKeylogger hash1_Old = "1e7614f757d40a2f5e2f4bd5597d04878768a9c01aa5f9f23d6c87660f7f0fbc" // injects Lokibot hash2_Old = "317e6817bba0f54e1547dd9acf24ee17a4cda1b97328cc69dc1ec16e11c258fc" // injects Redline hash3_Old = "65cac67ed2a084beff373d6aba6f914b8cba0caceda254a857def1df12f5154b" // injects SnakeKeylogger hash4_Old = "68ae2ee5ed7e793c1a49cbf1b0dd7f5a3de9cb783b51b0953880994a79037326" // injects Lokibot hash5_Old = "81763d8e3b42d07d76b0a74eda4e759981971635d62072c8da91251fc849b91e" // injects SnakeKeylogger strings: // Used ImplMap imports (PInvoke) $implmap1 = "VirtualAllocEx" $implmap2 = "CreateProcess" $implmap3 = "CreateRemoteThread" $implmap4 = "Wow64SetThreadContext" $implmap5 = "Wow64GetThreadContext" $implmap6 = "RtlInitUnicodeString" $implmap7 = "NtLoadDriver" $implmap8 = "LoadLibrary" $implmap9 = "VirtualProtect" $implmap10 = "AdjustTokenPrivileges" $implmap11 = "GetProcAddress" $modulerefKernel1 = "Kernel32" $modulerefKernel2 = "kernel32" $modulerefNtdll1 = "Ntdll" $modulerefNtdll2 = "ntdll" $regPath = "\\Registry\\Machine\\System\\CurrentControlSet\\Services\\TaskKill" wide // Registry path for installing Sysinternals Procexp driver $rsrcName = "BIDEN_HARRIS_PERFECT_ASSHOLE" wide $koiVM1 = "KoiVM" $koiVM2 = "#Koi" condition: uint16(0) == 0x5a4d and uint16(uint32(0x3c)) == 0x4550 and ($regPath or $rsrcName or 1 of ($koiVM*)) and 9 of ($implmap*) and 1 of ($modulerefKernel*) and 1 of ($modulerefNtdll*) }
```

Name
373a86e36f7e808a1db263b4b49d2428df4a13686da7d77edba7a6dd63790232
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '373a86e36f7e808a1db263b4b49d2428df4a13686da7d77edba7a6dd63790232']
Name
50b7e742eea52e18cf908cd676b87c0f145ecc3ff9692b01c90c47750fe989a7
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '50b7e742eea52e18cf908cd676b87c0f145ecc3ff9692b01c90c47750fe989a7']
Name
lastpass.shop
Pattern Type
stix
Pattern

[domain-name:value = 'lastpass.shop']

Name

fa3a9fc2adf9d1ca812e0951e21bf72ba3ec9ceb1c0cf0bfc0171b6d4adadf83

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fa3a9fc2adf9d1ca812e0951e21bf72ba3ec9ceb1c0cf0bfc0171b6d4adadf83']

Name

d6fd4a75e32f78817f84de3dcb9e3fd767f602b7da1edecd06391ff62a481571

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd6fd4a75e32f78817f84de3dcb9e3fd767f602b7da1edecd06391ff62a481571']

Name

71ecfddc7fe52a10bdf79c39cf9a1d911257ed0deee1bfef21386053bfe88110

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '71ecfddc7fe52a10bdf79c39cf9a1d911257ed0deee1bfef21386053bfe88110']

Name

b4c876d1797efbef614b44e52482c835c32e8ee020975a30fa2d25ed9cf8aa2b

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b4c876d1797efbef614b44e52482c835c32e8ee020975a30fa2d25ed9cf8aa2b']

Name

7f801c77fb61cc8d5c03e9fa3068163b595f5bf8c176628398bbbea5aa0a1b74

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7f801c77fb61cc8d5c03e9fa3068163b595f5bf8c176628398bbbea5aa0a1b74']

Name

4e8bf8c770727a3b0f551adcff2716c941234708e679c868ce42532714a29d27

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4e8bf8c770727a3b0f551adcff2716c941234708e679c868ce42532714a29d27']

Name

www.galaxyswapper.ru

Pattern Type

stix

Pattern

[hostname:value = 'www.galaxyswapper.ru']

Name

21a570237cdacdb8c69679e59c4dba6aa05f123f9db7470ec34e2f4024c3646b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '21a570237cdacdb8c69679e59c4dba6aa05f123f9db7470ec34e2f4024c3646b']

Name

7c3803c09a0370aa6484d8ad2f5690b96212d98e45fc8f9cb6022f87dff637fc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7c3803c09a0370aa6484d8ad2f5690b96212d98e45fc8f9cb6022f87dff637fc']

Name

881a337aa85a4b01c08706ab941573c5dc9b76ea0e4e1c2693a9b4aa4453ec8c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '881a337aa85a4b01c08706ab941573c5dc9b76ea0e4e1c2693a9b4aa4453ec8c']

Name

ee0d55b9a2d03c5bea9f69f98b042ab7b3064366f335a8a53096387876bf48d7

Description

Win32/BeamWinHTTP

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ee0d55b9a2d03c5bea9f69f98b042ab7b3064366f335a8a53096387876bf48d7']

Name

87b92fcd04f69f9c132c9f350dbb3686888a5e388b1f787f6a658f09582c0da6

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '87b92fcd04f69f9c132c9f350dbb3686888a5e388b1f787f6a658f09582c0da6']

Name

96e49a5ac188d49003b2fe77ad8a4c8866a94cc828dc6172d9a13a8c26e49b9b

Description

Win64:Evo-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '96e49a5ac188d49003b2fe77ad8a4c8866a94cc828dc6172d9a13a8c26e49b9b']

Name

e35547cfb6ae3fe18df6d887334952e7a38cc51a230f02c7f62a5fef083de7cf

Description

RedLine

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e35547cfb6ae3fe18df6d887334952e7a38cc51a230f02c7f62a5fef083de7cf']

Name

feae44d8927dd41feaed997b3dbf7b41933496d6285b79554b83e72ae8a045c4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'feae44d8927dd41feaed997b3dbf7b41933496d6285b79554b83e72ae8a045c4']

Name

d95298befdde567b31571d16f327840fa0f0dd9c54bf876531820910418a52b6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd95298befdde567b31571d16f327840fa0f0dd9c54bf876531820910418a52b6']

Name

b67bc78347918209973d633287c4e1f514a0917b8678c2cf2066ba80b2004f78

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b67bc78347918209973d633287c4e1f514a0917b8678c2cf2066ba80b2004f78']

Name

4c17f7ee55f9bf6fa9acaeeb9574feab39ba4a3cccd4426dfa85aaf58b90ae73

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4c17f7ee55f9bf6fa9acaeeb9574feab39ba4a3cccd4426dfa85aaf58b90ae73']

Name

b8bb071899ae7bd16a328c0998b3cd40261d61e564ac77f9bf3e495fab0ad267

Description

Win64:RATX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b8bb071899ae7bd16a328c0998b3cd40261d61e564ac77f9bf3e495fab0ad267']

Name

63de4552312345e055236c82ecdc55c2bc8b3c37f363cb081f8f788b5203d759

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '63de4552312345e055236c82ecdc55c2bc8b3c37f363cb081f8f788b5203d759']

Name

10bbfa36ddd8ea6038e2071320ee84f7a9208a5be3a4dda448e83393cdf39a4d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '10bbfa36ddd8ea6038e2071320ee84f7a9208a5be3a4dda448e83393cdf39a4d']

Name

fc99e6083b1dcbe72fb818dbd53903f30c312731f2cfc8607f9d2bf2586be1ee

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fc99e6083b1dcbe72fb818dbd53903f30c312731f2cfc8607f9d2bf2586be1ee']

Name

57f261cc442dd9a4f1cd4ffd281c9855f4f9a736abffaf539d9df2a6ea0dd409

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '57f261cc442dd9a4f1cd4ffd281c9855f4f9a736abffaf539d9df2a6ea0dd409']

Name

ff72f619907a25f3d99f0c3aa84710c6ff6cb4c3fd8ebad14f85f96c6da49222

Description

Win32/BeamWinHTTP

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ff72f619907a25f3d99f0c3aa84710c6ff6cb4c3fd8ebad14f85f96c6da49222']

Name

1bc7fc0a4796f7780223b4f0bf8d6816b3721f0b52eedc0df9a32dc4ea4829e8

Description

Win32/RisePro

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '1bc7fc0a4796f7780223b4f0bf8d6816b3721f0b52eedc0df9a32dc4ea4829e8']
Name
5e3588e8ddebd61c2bd6dab4b87f601bd6a4857b33eb281cb5059c29cfe62b80
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '5e3588e8ddebd61c2bd6dab4b87f601bd6a4857b33eb281cb5059c29cfe62b80']
Name
457cfd6222266941360fdbe36742486ee12419c95f1d7d350243e795de28200e
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '457cfd6222266941360fdbe36742486ee12419c95f1d7d350243e795de28200e']

Name

202570439b32480e6df232977d5435be9be94822c75f89b09f571e5b03f8c9ab

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '202570439b32480e6df232977d5435be9be94822c75f89b09f571e5b03f8c9ab']

Name

301be47a8fefa749d904425b43ae459249e2b44ff62051f3a5529d6222259f42

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '301be47a8fefa749d904425b43ae459249e2b44ff62051f3a5529d6222259f42']

Name

22962d59a066795696464868700fa7d3f735bfdb494a7a879fb54668a0ca3d46

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '22962d59a066795696464868700fa7d3f735bfdb494a7a879fb54668a0ca3d46']

Name

25fbe0ff3274b4bc981fa6ec0459e9b95cec6397194e10ea6287bf4b899a9b07

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '25fbe0ff3274b4bc981fa6ec0459e9b95cec6397194e10ea6287bf4b899a9b07']

Name

fefb4288cb41fcca85cd50653093d7b27c9c51769b03f72adf951c5a1f111ddf

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fefb4288cb41fcca85cd50653093d7b27c9c51769b03f72adf951c5a1f111ddf']

Name

24c870202b3aedfcd28a8afb93b5212b791c265abd872ef94e44401d1ca309ad

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '24c870202b3aedfcd28a8afb93b5212b791c265abd872ef94e44401d1ca309ad']

Name

8c093e92da0aa840d4e14fd9d105a7ee9b386591

Description

Detects new version of dotRunpeX - configurable .NET injector

Pattern Type

yara

Pattern

rule injector_ZZ_dotRunpeX { meta: description = "Detects new version of dotRunpeX - configurable .NET injector" author = "Jiri Vinopal (jiriv)" date = "2022-10-30" hash1 = "373a86e36f7e808a1db263b4b49d2428df4a13686da7d77edba7a6dd63790232" // injects Formbook hash2 = "41ea8f9a9f2a7aeb086dedf8e5855b0409f31e7793cbba615ca0498e47a72636" // injects Formbook hash3 = "5e3588e8ddebd61c2bd6dab4b87f601bd6a4857b33eb281cb5059c29cfe62b80" // injects

AsyncRat hash4 = "8c451b84d9579b625a7821ad7ddcb87bdd665a9e6619eaecf6ab93cd190cf504" // injects Remcos hash5 = "8fa81f6341b342afa40b7dc76dd6e0a1874583d12ea04acf839251cb5ca61591" // injects Formbook hash6 = "cd4c821e329ec1f7bfe7ecd39a6020867348b722e8c84a05c7eb32f8d5a2f4db" // injects AgentTesla hash7 = "fa8a67642514b69731c2ce6d9e980e2a9c9e409b3947f2c9909d81f6eac81452" // injects AsyncRat hash8 = "eb2e2ac0f5f51d90fe90b63c3c385af155b2fee30bc3dc6309776b90c21320f5" // injects SnakeKeylogger strings: // Used ImplMap imports (PInvoke) $implmap1 = "VirtualAllocEx" $implmap2 = "CreateProcess" $implmap3 = "CreateRemoteThread" $implmap4 = "Wow64SetThreadContext" $implmap5 = "Wow64GetThreadContext" $implmap6 = "NtResumeThread" $implmap7 = "ZwUnmapViewOfSection" $implmap8 = "NtWriteVirtualMemory" $implmap9 = "MessageBox" // ImplMap not presented in all samples - maybe different versions? $implmap10 = "Wow64DisableWow64FsRedirection" $implmap11 = "Wow64RevertWow64FsRedirection" $implmap12 = "CreateFile" $implmap13 = "RtlInitUnicodeString" $implmap14 = "NtLoadDriver" $implmap15 = "NtUnloadDriver" $implmap16 = "OpenProcessToken" $implmap17 = "LookupPrivilegeValue" $implmap18 = "AdjustTokenPrivileges" $implmap19 = "CloseHandle" $implmap20 = "NtQuerySystemInformation" $implmap21 = "DeviceIoControl" $implmap22 = "GetProcessHeap" $implmap23 = "HeapFree" $implmap24 = "HeapAlloc" $implmap25 = "GetProcAddress" $implmap26 = "CopyMemory" // ImplMap added by KoiVM Protector used by this injector $modulerefKernel1 = "Kernel32" $modulerefKernel2 = "kernel32" $modulerefNtdll1 = "Ntdll" $modulerefNtdll2 = "ntdll" $modulerefAdvapi1 = "Advapi32" $modulerefAdvapi2 = "advapi32" $regPath = "\\Registry\\Machine\\System\\CurrentControlSet\\Services\\TaskKill" wide // Registry path for installing Sysinternals Procexp driver $rsrcName = "BIDEN_HARRIS_PERFECT_ASSHOLE" wide $koiVM1 = "KoiVM" $koiVM2 = "#Koi" condition: uint16(0) == 0x5a4d and uint16(uint32(0x3c)) == 0x4550 and ($regPath or $rsrcName or 1 of ($koiVM*)) and 24 of ($implmap*) and 1 of ($modulerefKernel*) and 1 of ($modulerefNtdll*) and 1 of ($modulerefAdvapi*) }

Name

b80b3dae21d54eb9ccde40b9ba728ba3d45a73e0fc91adae3d7c375208631527

Description

RedLine

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b80b3dae21d54eb9ccde40b9ba728ba3d45a73e0fc91adae3d7c375208631527']

Name

fa8a67642514b69731c2ce6d9e980e2a9c9e409b3947f2c9909d81f6eac81452

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fa8a67642514b69731c2ce6d9e980e2a9c9e409b3947f2c9909d81f6eac81452']

Name

87f5b4385a2a87229b6c448a3b4b19a7e75fe6bc607dffc0e1f860e9e4499eca

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '87f5b4385a2a87229b6c448a3b4b19a7e75fe6bc607dffc0e1f860e9e4499eca']

Name

04a1021d0880a4f13ed8693dfe65889a5f827fe5ee9369abbc00b58efc40e69b

Description

RedLine

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '04a1021d0880a4f13ed8693dfe65889a5f827fe5ee9369abbc00b58efc40e69b']

Name

68ae2ee5ed7e793c1a49cbf1b0dd7f5a3de9cb783b51b0953880994a79037326

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '68ae2ee5ed7e793c1a49cbf1b0dd7f5a3de9cb783b51b0953880994a79037326']

Name

f79273a1efb664d81f68e808b9ec963bfeb79d63bd277108863d6ae3c4801a9e

Description

RedLine

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f79273a1efb664d81f68e808b9ec963bfeb79d63bd277108863d6ae3c4801a9e']

Name

87134629723b2c6f4d0a74c35fdce89653471d9880b23f4faea6664ae151db0e

Description

Generic Stealer, RecordBreaker

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '87134629723b2c6f4d0a74c35fdce89653471d9880b23f4faea6664ae151db0e']

Name

13eb08dda92356f21888d95a6611a46728dfcefcdf769e7edad1a70e958e5367

Description

RedLine

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '13eb08dda92356f21888d95a6611a46728dfcefcdf769e7edad1a70e958e5367']

Name

ada1679a193c9b17b206b3d9ff2a19d64c6c8c5f882a321381c9d5347a8b4b3e

Description

Generic Stealer, RecordBreaker

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ada1679a193c9b17b206b3d9ff2a19d64c6c8c5f882a321381c9d5347a8b4b3e']

Name

efa9a303af112ffb6737846755e3a995510fd65b6ced9032dc68cd7bbe4c307d

Description

Generic Stealer, RecordBreaker

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'efa9a303af112ffb6737846755e3a995510fd65b6ced9032dc68cd7bbe4c307d']

Name

47c765ad0baae96498e05e3f0984002cbce6b3f1bacd1cf238681a677c2f8036

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '47c765ad0baae96498e05e3f0984002cbce6b3f1bacd1cf238681a677c2f8036']

Name

0daef2c2bf086312037ebc91beec0302a7e4d1750f260d02bf815bd13c611559

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0daef2c2bf086312037ebc91beec0302a7e4d1750f260d02bf815bd13c611559']

Name

331ad58c524100da7e459e5c3943e970414617f60b3ed0f1a74f3bf189aafea7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '331ad58c524100da7e459e5c3943e970414617f60b3ed0f1a74f3bf189aafea7']

Name

c1be6f792bd51d23d848e54cd217bdf9edcbb2b89df741190929f6fa327a10cb

Description

Generic Stealer, RecordBreaker

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c1be6f792bd51d23d848e54cd217bdf9edcbb2b89df741190929f6fa327a10cb']

Name

e56c525248b1f9201cddcf1802377a7157029e8935696d1a9d9169e1d0501fa4

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e56c525248b1f9201cddcf1802377a7157029e8935696d1a9d9169e1d0501fa4']

Name

283cd48dc1368b6852c2f3168bf7a78ad593df010d9a67ed1c938508da5de783

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '283cd48dc1368b6852c2f3168bf7a78ad593df010d9a67ed1c938508da5de783']

Name

1f2ffabb3b89e6083ca5de70f5d718295c7a633c2d957da7c4469de059efde2c

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1f2ffabb3b89e6083ca5de70f5d718295c7a633c2d957da7c4469de059efde2c']

Name

35c53663294e5476315853228b4ae642f552c6c6b1253412a7f981c7ddf3d0b7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '35c53663294e5476315853228b4ae642f552c6c6b1253412a7f981c7ddf3d0b7']

Name

c9d36fcce70893aa16a846b48009bbd8b46fc11c6821b750083a9c89669038cc

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c9d36fcce70893aa16a846b48009bbd8b46fc11c6821b750083a9c89669038cc']

Name

770e7d287fe352f12757ebfbb4502b10f61001630d70ddf414157b12e1f5e9a3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '770e7d287fe352f12757ebfbb4502b10f61001630d70ddf414157b12e1f5e9a3']

Name

9246ed27032429f234888b2713529001344850c608cab9f5ab7274195d330bec

Description

Generic Stealer, RecordBreaker

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9246ed27032429f234888b2713529001344850c608cab9f5ab7274195d330bec']

Name

7d8c18056e86a3b8c32b524f9de009ced61caf463abe1bca285fa305d4b5616a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7d8c18056e86a3b8c32b524f9de009ced61caf463abe1bca285fa305d4b5616a']

Name

cddf8b8da972cb2e560c70d01366f582445441864fcff884b8194eb6c21a768c

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cddf8b8da972cb2e560c70d01366f582445441864fcff884b8194eb6c21a768c']

Name

9ed8eeb1db8909c96a958d91213093d2488dc172a8d22ba62657b9bfeb044fec

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9ed8eeb1db8909c96a958d91213093d2488dc172a8d22ba62657b9bfeb044fec']

Name

3c0c55b4ce2d90448949980fbca1fa447832f67fb864472551513b6e4eff5304

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3c0c55b4ce2d90448949980fbca1fa447832f67fb864472551513b6e4eff5304']

Name

f0ee1ddb789207c2000f728f6adabbe344ded7cba0804926a7cfc53bdbbc54eb

Description

Generic Stealer, RecordBreaker

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f0ee1ddb789207c2000f728f6adabbe344ded7cba0804926a7cfc53bdbbc54eb']

Name

b4a57b62569ee1ccb1c2dae148488dc9e37d738f0fed4f0a6e144caeb910f546

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b4a57b62569ee1ccb1c2dae148488dc9e37d738f0fed4f0a6e144caeb910f546']

Name

70a6d43a56d267aa4fdac5a96722a2ff05e2ac1cc9ba996d173f0b3252e09898

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '70a6d43a56d267aa4fdac5a96722a2ff05e2ac1cc9ba996d173f0b3252e09898']

Name

20b5c7f210320cf23a63ac7f76086a6e257dd0c248d77deff444cb3dcf624799

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '20b5c7f210320cf23a63ac7f76086a6e257dd0c248d77deff444cb3dcf624799']

Name

3e50f0eaf02d12653d5f757372240adcb5c16a5ab647a667637ba4c50d37aaad

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3e50f0eaf02d12653d5f757372240adcb5c16a5ab647a667637ba4c50d37aaad']

Name

d5eda02ff2f05d1e0d06a69018de463ab36497048a1ef2b69af93aa76ccfc07d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd5eda02ff2f05d1e0d06a69018de463ab36497048a1ef2b69af93aa76ccfc07d']

Name

bcc80eabe068cbbe38fa37b58e67fee54af75fa9e8a1fc30d93b7d30886d05da

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bcc80eabe068cbbe38fa37b58e67fee54af75fa9e8a1fc30d93b7d30886d05da']

Name

0e918ad3e7ad983ecf6c3238991c13a230acc897193e0ad360d2eeaab42bf078

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0e918ad3e7ad983ecf6c3238991c13a230acc897193e0ad360d2eeaab42bf078']

Name

317e6817bba0f54e1547dd9acf24ee17a4cda1b97328cc69dc1ec16e11c258fc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '317e6817bba0f54e1547dd9acf24ee17a4cda1b97328cc69dc1ec16e11c258fc']

Name

7bdb945f2dab863a299e26ab4c6dfb1e4f7321c38fe101224252d993495bc157

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7bdb945f2dab863a299e26ab4c6dfb1e4f7321c38fe101224252d993495bc157']

Name

410b032a8635fba6cc30f0c2049a53f93b98128388a4a7ce2c3a0bfb33591f9f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '410b032a8635fba6cc30f0c2049a53f93b98128388a4a7ce2c3a0bfb33591f9f']

Name

507f413ac42df115988df498a90fc1ae610cafb66cb30a3a7de53e71ec90e7cd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '507f413ac42df115988df498a90fc1ae610cafb66cb30a3a7de53e71ec90e7cd']

Name

81763d8e3b42d07d76b0a74eda4e759981971635d62072c8da91251fc849b91e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '81763d8e3b42d07d76b0a74eda4e759981971635d62072c8da91251fc849b91e']

Name

a2e9a2389faf04b67fbbd6fc71134860a145db7643d88ba312390493d5619302

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a2e9a2389faf04b67fbbd6fc71134860a145db7643d88ba312390493d5619302']

Name

55ee7efcb3d1d2e0eac0ecadd651d6a299de82d94347ef9862bc981ae619532b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '55ee7efcb3d1d2e0eac0ecadd651d6a299de82d94347ef9862bc981ae619532b']

Name

6c367333c677c2268df9deaff6ad4e711e73e53504aa1aa845bebfbfe635f1d2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6c367333c677c2268df9deaff6ad4e711e73e53504aa1aa845bebfbfe635f1d2']

Name

9049d536e6da46b63c562197ab92f511d5f5e2883eb8bf29f72217282ae25772

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9049d536e6da46b63c562197ab92f511d5f5e2883eb8bf29f72217282ae25772']

Name

b019a0535ca7466d7884825542ac6910fe037913118e1136dcac7e9ef3dc0dc9

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b019a0535ca7466d7884825542ac6910fe037913118e1136dcac7e9ef3dc0dc9']

Name

99e733391ac499e78e535a98551c4d27408abfad4e56fe4c46956636655df29c

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '99e733391ac499e78e535a98551c4d27408abfad4e56fe4c46956636655df29c']

Name

9177ba0c649f08fa6367d04091a7672fedb82215b26e08346645544f0631ebfd

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9177ba0c649f08fa6367d04091a7672fedb82215b26e08346645544f0631ebfd']

Name

4d4f97f1621334e4075e0229265ac6c5da14754eff1378a7d77ea6d3821e8a33

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4d4f97f1621334e4075e0229265ac6c5da14754eff1378a7d77ea6d3821e8a33']

Name

a73f134ab62a5c23a8c8bafabbfbd5e0408c826ba5418488639724708ec5ef28

Description

Win64:Malware-gen

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a73f134ab62a5c23a8c8bafabbfbd5e0408c826ba5418488639724708ec5ef28']

Name

f9c25b4755ab54ff3f8d827b6422d43ed14dbd03fd4faa266348eee177f7957f

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f9c25b4755ab54ff3f8d827b6422d43ed14dbd03fd4faa266348eee177f7957f']

Name

0e40e504c05c30a7987785996e2542c332100ae7ecf9f67ebe3c24ad2468527c

Description

ALF:Trojan:MSIL/AgentTesla.KM

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0e40e504c05c30a7987785996e2542c332100ae7ecf9f67ebe3c24ad2468527c']

Name

6c08c0654726c2f793b5191d5e7c74fdf3a2461118a45aa8527a0a30e3f256fd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6c08c0654726c2f793b5191d5e7c74fdf3a2461118a45aa8527a0a30e3f256fd']

Name

3418a369486e9bf2b57023dc0b02cb00f12a5214fca8bae20ff93586cc8c678a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3418a369486e9bf2b57023dc0b02cb00f12a5214fca8bae20ff93586cc8c678a']

Name

c6e0a5e947e9f23cd0af6fa8bd44411a12212ab1de5007036926089800ac8692

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c6e0a5e947e9f23cd0af6fa8bd44411a12212ab1de5007036926089800ac8692']

Name

13081992c0ef5c52c2b6224f3ff1ab38160bca9424e7c0470e0c175c920bdc9d

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '13081992c0ef5c52c2b6224f3ff1ab38160bca9424e7c0470e0c175c920bdc9d']

Name

17af8118607b9fc1f7b6aa82fd72f4fc115320d293e103dfe356706bb7c581b7

Description

Generic Stealer, RecordBreaker

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '17af8118607b9fc1f7b6aa82fd72f4fc115320d293e103dfe356706bb7c581b7']

Name

9d9940b60809e3c10cd4540f8e589626a293244a999bea16c259f9712969a742

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9d9940b60809e3c10cd4540f8e589626a293244a999bea16c259f9712969a742']

Name

149af913afd7eb2773386d14e88a46449cbc9096e0748cfbaa2e061b59525bf0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '149af913afd7eb2773386d14e88a46449cbc9096e0748cfbaa2e061b59525bf0']

Name

d55f6b273254d2be71991cdbdb288cc94a7bc715c4be7ad97c0e1625bc0f2696

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd55f6b273254d2be71991cdbdb288cc94a7bc715c4be7ad97c0e1625bc0f2696']

Name

76eed1849d0a0474f9e0a58afcda2cc1ea7af316535b4b4b27ff810a162d4f8f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '76eed1849d0a0474f9e0a58afcda2cc1ea7af316535b4b4b27ff810a162d4f8f']

Name

db8ed3e6dd7e6818046e7ee1e9c6c91f98aa5ce3113b14fb1c85a50a45569b18

Description

Generic Stealer, RecordBreaker

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'db8ed3e6dd7e6818046e7ee1e9c6c91f98aa5ce3113b14fb1c85a50a45569b18']

Name

02355d3fee5e217b25f9210ad0f6bacc3807b6ef1a59aa4d428c01017dcbcf28

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '02355d3fee5e217b25f9210ad0f6bacc3807b6ef1a59aa4d428c01017dcbcf28']

Name

aca4d6278f31f374262e0388d16ee6fdcdbbad8257374f1feaabf75b0ec23157

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aca4d6278f31f374262e0388d16ee6fdcdbbad8257374f1feaabf75b0ec23157']

Name

7120cf1ad3fdcae7ba6956749a8988e8181837a05948b432cec6ae11229b1d12

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7120cf1ad3fdcae7ba6956749a8988e8181837a05948b432cec6ae11229b1d12']

Name

40df5a6e6dcadbe576ce4a8b01cfb82bf3f56a87bae674200e60814eab666c6d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '40df5a6e6dcadbe576ce4a8b01cfb82bf3f56a87bae674200e60814eab666c6d']

Name

9f96e5bc9ffc9742cb10384566dc7fb232e0f0d633e643bd487b747b6e88f369

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9f96e5bc9ffc9742cb10384566dc7fb232e0f0d633e643bd487b747b6e88f369']

Name

76e129552a30fa5c914d9f946f40b2ec2bbbbeb4e5e2f324e70455725030e157

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '76e129552a30fa5c914d9f946f40b2ec2bbbbeb4e5e2f324e70455725030e157']

Name

f6aba045ca29ba39bbdcb2f8bde63efc971d138f88bf03aea2d13ddec88a0483

Description

RedLine

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f6aba045ca29ba39bbdcb2f8bde63efc971d138f88bf03aea2d13ddec88a0483']

Name

47849f610a30d72660b1725a0b18d78c5204257b3740641727bdcbfd1ebd466a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '47849f610a30d72660b1725a0b18d78c5204257b3740641727bdcbfd1ebd466a']

Name

cd4c821e329ec1f7bfe7ecd39a6020867348b722e8c84a05c7eb32f8d5a2f4db

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cd4c821e329ec1f7bfe7ecd39a6020867348b722e8c84a05c7eb32f8d5a2f4db']

Name

2478cd52847146b34cae6b768c794210838a3002a622ce61c2f90d075f6e0e65

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2478cd52847146b34cae6b768c794210838a3002a622ce61c2f90d075f6e0e65']

Name

d87a200a26d07a64272e93fb3ae8f8d9e4d34bdfedb0cf7c685a6c97912e967f

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd87a200a26d07a64272e93fb3ae8f8d9e4d34bdfedb0cf7c685a6c97912e967f']

Name

95793df9284fe35c0491e5cfa36bc8f49fd426ccdf35f5fe2f098e07d160a4dc

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '95793df9284fe35c0491e5cfa36bc8f49fd426ccdf35f5fe2f098e07d160a4dc']

Name

f570b6c46a5bb5a8757b1125c7d4b5d4aca2c7e9354ed1d34b78fd4f08280e30

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f570b6c46a5bb5a8757b1125c7d4b5d4aca2c7e9354ed1d34b78fd4f08280e30']

Name

a4d455f65bb4d2dde03a0686433b6d515c71b5655fa78b86a4f9bdae503c1295

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a4d455f65bb4d2dde03a0686433b6d515c71b5655fa78b86a4f9bdae503c1295']

Name

0e11704fcc3c36832ba98b80ea44a3013660d1ed3fb48158b982fed9f9050391

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0e11704fcc3c36832ba98b80ea44a3013660d1ed3fb48158b982fed9f9050391']

Name

2b1be3ea73921adde804b85e93817869556fa9919bf7a528639a796e27351755

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2b1be3ea73921adde804b85e93817869556fa9919bf7a528639a796e27351755']

Name

4068637c121888476533a3bbb16bec6bc3b4f81f7b9de635ef3576d56dc54c75

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4068637c121888476533a3bbb16bec6bc3b4f81f7b9de635ef3576d56dc54c75']

Name

8bcc23ec881d61839fc57e8ec7425ac5ed625425fbf265fcb53ad73a73825b18

Description

Generic Stealer, RecordBreaker

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8bcc23ec881d61839fc57e8ec7425ac5ed625425fbf265fcb53ad73a73825b18']

Name

b1c9b356c50230629c4697b0527fd7a0fa8d6f0e8342a1eb5b5a4f90d8f0eb86

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b1c9b356c50230629c4697b0527fd7a0fa8d6f0e8342a1eb5b5a4f90d8f0eb86']

Name

50ec8a9e59e1bcb0a41477e20f5bb809a80329d56e20cf99e93d756b9e0ceefc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '50ec8a9e59e1bcb0a41477e20f5bb809a80329d56e20cf99e93d756b9e0ceefc']

Name

366284c1a0577937c86744349ac47e6e578da500ada3deb857ff233d9851ee6b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '366284c1a0577937c86744349ac47e6e578da500ada3deb857ff233d9851ee6b']

Name

44a11146173db0663a23787bffbb120f3955bc33e60e73ecc798953e9b34b2f2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '44a11146173db0663a23787bffbb120f3955bc33e60e73ecc798953e9b34b2f2']

Name

a487e959e59bc9500c43ac270eaf345eaf28173b07ed7dd82b2495aa19cdab88

Description

Generic Stealer, RecordBreaker

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a487e959e59bc9500c43ac270eaf345eaf28173b07ed7dd82b2495aa19cdab88']

Name

f413dbf6764bc73ab94428831e0ce3fc0369856aa50c4f9c0f5948eac85d2d08

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f413dbf6764bc73ab94428831e0ce3fc0369856aa50c4f9c0f5948eac85d2d08']

Name

96b5ea21a2556486cebbed76711a8bbae42de1e97e3311213833c6567a4fbbdc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '96b5ea21a2556486cebbed76711a8bbae42de1e97e3311213833c6567a4fbbdc']

Name

20330ec79f6c6edce8c3d87e3340aebc60f528d3751339e57437b178b9cb914d

Description

RedLine

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '20330ec79f6c6edce8c3d87e3340aebc60f528d3751339e57437b178b9cb914d']

Name

41ea8f9a9f2a7aeb086dedf8e5855b0409f31e7793cbba615ca0498e47a72636

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '41ea8f9a9f2a7aeb086dedf8e5855b0409f31e7793cbba615ca0498e47a72636']

Name

8de23e90bac05911cbfb6b036c6808ce7c244e4e875cb7edcdb90f75e89e5476

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8de23e90bac05911cbfb6b036c6808ce7c244e4e875cb7edcdb90f75e89e5476']

Name

ec875c5901e28a04b199f577b16a8ba6ac8c9ab7e90bc51a5809f668882ba54f

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ec875c5901e28a04b199f577b16a8ba6ac8c9ab7e90bc51a5809f668882ba54f']

Name

50451fda27fd8569c7b32bfe82197b82a8637cac928164e1b091a389060e957e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '50451fda27fd8569c7b32bfe82197b82a8637cac928164e1b091a389060e957e']

Name

fa258b12d3f4ca1503379a4f6a800bdb1d589ef15ab8bfc20d452f70c8a0745c

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fa258b12d3f4ca1503379a4f6a800bdb1d589ef15ab8bfc20d452f70c8a0745c']

Name

1e7614f757d40a2f5e2f4bd5597d04878768a9c01aa5f9f23d6c87660f7f0fbc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1e7614f757d40a2f5e2f4bd5597d04878768a9c01aa5f9f23d6c87660f7f0fbc']

Name

e6da2d860bd2d0e8b56737b4c8c47cdeea78a404cd0d6fa5a26cbb5ac7682d1d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e6da2d860bd2d0e8b56737b4c8c47cdeea78a404cd0d6fa5a26cbb5ac7682d1d']

Name

5bbd9513f0872d23ca43dd553a63a12882be274fef983fab427721257d60eaec

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5bbd9513f0872d23ca43dd553a63a12882be274fef983fab427721257d60eaec']

Name

adc5669dd1153111f4cc07714599145a775d8c260c1acae9c142280147d1793a

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'adc5669dd1153111f4cc07714599145a775d8c260c1acae9c142280147d1793a']

Name

116d81561faa8c8a9cf4fbc947e9eee11185f3960daead8179a968dea143bfd0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '116d81561faa8c8a9cf4fbc947e9eee11185f3960daead8179a968dea143bfd0']

Name

0c857501e3851072db666386136929c06bcf4c8d3160b41b7d82a3ce9afca1be

Description

Win64:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0c857501e3851072db666386136929c06bcf4c8d3160b41b7d82a3ce9afca1be']

Name

75236a06aadafc69cc5aa8032468869fb868a9a100b687f19c66be03410c2487

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '75236a06aadafc69cc5aa8032468869fb868a9a100b687f19c66be03410c2487']

Name

0bb4d022d6007fcaf1d0707b646063b4b66cf5177da6a1fc6c5d0fc217501d6f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0bb4d022d6007fcaf1d0707b646063b4b66cf5177da6a1fc6c5d0fc217501d6f']

Name

65cac67ed2a084beff373d6aba6f914b8cba0caceda254a857def1df12f5154b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '65cac67ed2a084beff373d6aba6f914b8cba0caceda254a857def1df12f5154b']

Name

93e2ea6f021951369028b73637d9558c8baf3c99d9de1a2a60c1461cb9d571bf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '93e2ea6f021951369028b73637d9558c8baf3c99d9de1a2a60c1461cb9d571bf']

Name

242e1c82269725c01108e52376be8ddad39ab29da49356d10e527af6d78058f5

Pattern Type
stix

Pattern
[file:hashes.'SHA-256' = '242e1c82269725c01108e52376be8ddad39ab29da49356d10e527af6d78058f5']

Malware

Name
dotRunpeX

Attack-Pattern

Name
Abuse Elevation Control Mechanism
ID
T1548
Description
Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.
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

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

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

Native API

ID

T1106

Description

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes. (Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations. Native API functions (such as `NtCreateProcess`) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For

example, functions such as the Windows API `CreateProcess()` or GNU `fork()` will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations. (Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC) Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation) Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system. While invoking API functions, adversaries may also attempt to bypass defensive tools (ex: unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001)).

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

Multi-Stage Channels

ID

T1104

Description

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult. Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

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

System Information Discovery

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with

information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

Domain-Name

Value
lastpass.shop

StixFile

Value
f9c25b4755ab54ff3f8d827b6422d43ed14dbd03fd4faa266348eee177f7957f
99e733391ac499e78e535a98551c4d27408abfad4e56fe4c46956636655df29c
70a6d43a56d267aa4fdac5a96722a2ff05e2ac1cc9ba996d173f0b3252e09898
20b5c7f210320cf23a63ac7f76086a6e257dd0c248d77deff444cb3dcf624799
1bc7fc0a4796f7780223b4f0bf8d6816b3721f0b52eedc0df9a32dc4ea4829e8
0e11704fcc3c36832ba98b80ea44a3013660d1ed3fb48158b982fed9f9050391
41ea8f9a9f2a7aeb086dedf8e5855b0409f31e7793cbba615ca0498e47a72636
cd4c821e329ec1f7bfe7ecd39a6020867348b722e8c84a05c7eb32f8d5a2f4db
2478cd52847146b34cae6b768c794210838a3002a622ce61c2f90d075f6e0e65
283cd48dc1368b6852c2f3168bf7a78ad593df010d9a67ed1c938508da5de783
ae4d2054a6e1f9ba2c269eace61aac7259adb0645d18da82779717d83174837d
8c451b84d9579b625a7821ad7ddcb87bdd665a9e6619eaecf6ab93cd190cf504
0e40e504c05c30a7987785996e2542c332100ae7ecf9f67ebe3c24ad2468527c

202570439b32480e6df232977d5435be9be94822c75f89b09f571e5b03f8c9ab

a73f134ab62a5c23a8c8bafabbfbd5e0408c826ba5418488639724708ec5ef28

68ae2ee5ed7e793c1a49cbf1b0dd7f5a3de9cb783b51b0953880994a79037326

149af913afd7eb2773386d14e88a46449cbc9096e0748cfbaa2e061b59525bf0

417c3f327c2d8b54ec72a5a89280fecb589a3e0b89c281bbc077d7de445cc76b

b4c876d1797efbef614b44e52482c835c32e8ee020975a30fa2d25ed9cf8aa2b

a4d455f65bb4d2dde03a0686433b6d515c71b5655fa78b86a4f9bdae503c1295

363c46dfb252d7c40d9c3bb63bdc40c2eff0ce16c0c1b77f507d73058104c6e1

e6a2575c893868e3d8ea5982699c9c2b75a07b8ec092b0cb26d7b5c3c2640f33

3c0c55b4ce2d90448949980fbca1fa447832f67fb864472551513b6e4eff5304

87f5b4385a2a87229b6c448a3b4b19a7e75fe6bc607dffc0e1f860e9e4499eca

bcc80eabe068cbbe38fa37b58e67fee54af75fa9e8a1fc30d93b7d30886d05da

75236a06aadafc69cc5aa8032468869fb868a9a100b687f19c66be03410c2487

373a86e36f7e808a1db263b4b49d2428df4a13686da7d77edba7a6dd63790232

0bb4d022d6007fcaf1d0707b646063b4b66cf5177da6a1fc6c5d0fc217501d6f

13081992c0ef5c52c2b6224f3ff1ab38160bca9424e7c0470e0c175c920bdc9d

4d4f97f1621334e4075e0229265ac6c5da14754eff1378a7d77ea6d3821e8a33

02355d3fee5e217b25f9210ad0f6bacc3807b6ef1a59aa4d428c01017dcbcf28

a19cabf8ce0a8012dedbf65855981db1efa3b9773365554401a74bfb7a45490f

fa258b12d3f4ca1503379a4f6a800bdb1d589ef15ab8bfc20d452f70c8a0745c

17af8118607b9fc1f7b6aa82fd72f4fc115320d293e103dfe356706bb7c581b7

b1c9b356c50230629c4697b0527fd7a0fa8d6f0e8342a1eb5b5a4f90d8f0eb86

76eed1849d0a0474f9e0a58afcda2cc1ea7af316535b4b4b27ff810a162d4f8f

20330ec79f6c6edce8c3d87e3340aebc60f528d3751339e57437b178b9cb914d

fcc4c20c07fdf816b7cc6dfba34d42af827ecf01e9972f266ac395e54db028af

f0ee1ddb789207c2000f728f6adabbe344ded7cba0804926a7cfc53bdbbc54eb

4e8bf8c770727a3b0f551adcff2716c941234708e679c868ce42532714a29d27

05f9553616bb5fdbf37bd4036c210929e08d7181de898c1bea1bdae7afb0766f

670a96324222e6bb02bd36c7e5b100fb5d52d2d59891bd9599b1a47438ac9578

b80b3dae21d54eb9ccde40b9ba728ba3d45a73e0fc91adae3d7c375208631527

7d8c18056e86a3b8c32b524f9de009ced61caf463abe1bca285fa305d4b5616a

410b032a8635fba6cc30f0c2049a53f93b98128388a4a7ce2c3a0bfb33591f9f

35c11f7315d2e5d04d783de4314d8cde2def382f1e3fc49ccc555337c54d63cc

304847c69875ec59995fbb453f8d1106f80c5eb380ae6b8676e76f5372290194

4068637c121888476533a3bbb16bec6bc3b4f81f7b9de635ef3576d56dc54c75

e56c525248b1f9201cddcf1802377a7157029e8935696d1a9d9169e1d0501fa4

b67bc78347918209973d633287c4e1f514a0917b8678c2cf2066ba80b2004f78

87134629723b2c6f4d0a74c35fdce89653471d9880b23f4faea6664ae151db0e

43d49812cc723b3c24ca7048faa859800c7e303e074243e4348f65d34127367b

f440309e372551fb6ee00ecca71a70a1b8b7e077fe61b0687411147b582ab415

fa3a9fc2adf9d1ca812e0951e21bf72ba3ec9ceb1c0cf0bfc0171b6d4adadf83

3418a369486e9bf2b57023dc0b02cb00f12a5214fca8bae20ff93586cc8c678a

f413dbf6764bc73ab94428831e0ce3fc0369856aa50c4f9c0f5948eac85d2d08

9984a21c06fea77e96ba410cffb99de530201ef0c74f3e8b38b3afd4fdf0b333

eb2e2ac0f5f51d90fe90b63c3c385af155b2fee30bc3dc6309776b90c21320f5

feae44d8927dd41feaed997b3dbf7b41933496d6285b79554b83e72ae8a045c4

6c08c0654726c2f793b5191d5e7c74fdf3a2461118a45aa8527a0a30e3f256fd

44a11146173db0663a23787bffbb120f3955bc33e60e73ecc798953e9b34b2f2

ec875c5901e28a04b199f577b16a8ba6ac8c9ab7e90bc51a5809f668882ba54f

8de23e90bac05911cbfb6b036c6808ce7c244e4e875cb7edcdb90f75e89e5476

c1be6f792bd51d23d848e54cd217bdf9edcbb2b89df741190929f6fa327a10cb

cb014704f53d5da64964c2b0bfc7e13bbdf389555294c6f6c98c2527f6406d6d

8fa81f6341b342afa40b7dc76dd6e0a1874583d12ea04acf839251cb5ca61591

770e7d287fe352f12757ebfbb4502b10f61001630d70ddf414157b12e1f5e9a3

96e49a5ac188d49003b2fe77ad8a4c8866a94cc828dc6172d9a13a8c26e49b9b

457cfd6222266941360fdbe36742486ee12419c95f1d7d350243e795de28200e

d6fd4a75e32f78817f84de3dcb9e3fd767f602b7da1edecd06391ff62a481571

f570b6c46a5bb5a8757b1125c7d4b5d4aca2c7e9354ed1d34b78fd4f08280e30

50451fda27fd8569c7b32bfe82197b82a8637cac928164e1b091a389060e957e

cddf8b8da972cb2e560c70d01366f582445441864fcff884b8194eb6c21a768c

948416d3aeae6f31df3341118a25a4231a7eed23b3db73a022e9da70734163c9

71ecfddc7fe52a10bdf79c39cf9a1d911257ed0deee1bfef21386053bfe88110

2b1be3ea73921adde804b85e93817869556fa9919bf7a528639a796e27351755

35c53663294e5476315853228b4ae642f552c6c6b1253412a7f981c7ddf3d0b7

ddae8737d7cc35a87274a26b886e6b48ae947aa849c3d7ecb84de6f6d553aa96

5bbd9513f0872d23ca43dd553a63a12882be274fef983fab427721257d60eaec

87b92fcd04f69f9c132c9f350dbb3686888a5e388b1f787f6a658f09582c0da6

e6da2d860bd2d0e8b56737b4c8c47cdeea78a404cd0d6fa5a26cbb5ac7682d1d

04a1021d0880a4f13ed8693dfe65889a5f827fe5ee9369abbc00b58efc40e69b

d5eda02ff2f05d1e0d06a69018de463ab36497048a1ef2b69af93aa76ccfc07d

d55f6b273254d2be71991cdbdb288cc94a7bc715c4be7ad97c0e1625bc0f2696

ada1679a193c9b17b206b3d9ff2a19d64c6c8c5f882a321381c9d5347a8b4b3e

10bbfa36ddd8ea6038e2071320ee84f7a9208a5be3a4dda448e83393cdf39a4d

b8bb071899ae7bd16a328c0998b3cd40261d61e564ac77f9bf3e495fab0ad267

fefb4288cb41fcca85cd50653093d7b27c9c51769b03f72adf951c5a1f111ddf

bf7b127b1bb81b68439851386cd3d1600bb8b9ec56135e668a88062d913410dd

65cac67ed2a084beff373d6aba6f914b8cba0caceda254a857def1df12f5154b

c6e0a5e947e9f23cd0af6fa8bd44411a12212ab1de5007036926089800ac8692

47c765ad0baae96498e05e3f0984002cbce6b3f1bacd1cf238681a677c2f8036

55ee7efcb3d1d2e0eac0ecadd651d6a299de82d94347ef9862bc981ae619532b

d87a200a26d07a64272e93fb3ae8f8d9e4d34bdfedb0cf7c685a6c97912e967f

0daef2c2bf086312037ebc91beec0302a7e4d1750f260d02bf815bd13c611559

efa9a303af112ffb6737846755e3a995510fd65b6ced9032dc68cd7bbe4c307d

1f2ffabb3b89e6083ca5de70f5d718295c7a633c2d957da7c4469de059efde2c

1c1fcc4133af77f07d0c0299d0320aa9f447748ebead74b429f73c44d950e38b

7c3803c09a0370aa6484d8ad2f5690b96212d98e45fc8f9cb6022f87dff637fc

881a337aa85a4b01c08706ab941573c5dc9b76ea0e4e1c2693a9b4aa4453ec8c

7263336f1ec49f936501c508a9edf072a81002e64e52a1ed0cafb1378bb07a2a

7120cf1ad3fdcae7ba6956749a8988e8181837a05948b432cec6ae11229b1d12

71cc196ad2103a1facd81f2b8bd985273f682019b2a88841d2f34ecc373d1d69

5e3588e8ddebd61c2bd6dab4b87f601bd6a4857b33eb281cb5059c29cfe62b80

116d81561faa8c8a9cf4fbc947e9eee11185f3960daead8179a968dea143bfd0

a487e959e59bc9500c43ac270eaf345eaf28173b07ed7dd82b2495aa19cdab88

0e918ad3e7ad983ecf6c3238991c13a230acc897193e0ad360d2eeaab42bf078

d95298befdde567b31571d16f327840fa0f0dd9c54bf876531820910418a52b6

507f413ac42df115988df498a90fc1ae610cafb66cb30a3a7de53e71ec90e7cd

331ad58c524100da7e459e5c3943e970414617f60b3ed0f1a74f3bf189aafea7

b4a57b62569ee1ccb1c2dae148488dc9e37d738f0fed4f0a6e144caeb910f546

b019a0535ca7466d7884825542ac6910fe037913118e1136dcac7e9ef3dc0dc9

adc5669dd1153111f4cc07714599145a775d8c260c1acae9c142280147d1793a

242e1c82269725c01108e52376be8ddad39ab29da49356d10e527af6d78058f5

7f801c77fb61cc8d5c03e9fa3068163b595f5bf8c176628398bbbea5aa0a1b74

ff72f619907a25f3d99f0c3aa84710c6ff6cb4c3fd8ebad14f85f96c6da49222

40df5a6e6dcadbe576ce4a8b01cfb82bf3f56a87bae674200e60814eab666c6d

50ec8a9e59e1bcb0a41477e20f5bb809a80329d56e20cf99e93d756b9e0ceefc

22962d59a066795696464868700fa7d3f735bfdb494a7a879fb54668a0ca3d46

0f9e27ec1ed021fd7375ca46f233c06b354d12d57aed44132208cd9308bfee11

21a570237cdacdb8c69679e59c4dba6aa05f123f9db7470ec34e2f4024c3646b

301be47a8fefa749d904425b43ae459249e2b44ff62051f3a5529d6222259f42

fa8a67642514b69731c2ce6d9e980e2a9c9e409b3947f2c9909d81f6eac81452

317e6817bba0f54e1547dd9acf24ee17a4cda1b97328cc69dc1ec16e11c258fc

fc99e6083b1dcbe72fb818dbd53903f30c312731f2cfc8607f9d2bf2586be1ee

9177ba0c649f08fa6367d04091a7672fedb82215b26e08346645544f0631ebfd

03fcbab82603df2858f7d6fefdb6ae3cc8e17393af6d44f24634d28fccf3f181

c5646cc9fe486f0644067fc294f83eb6a39ce6f28eea3708c9bf49e244acc0f9

aca4d6278f31f374262e0388d16ee6fdcdbbad8257374f1feaabf75b0ec23157

f6aba045ca29ba39bbdcb2f8bde63efc971d138f88bf03aea2d13ddec88a0483

855b2e04c323a269d3731c093f0bc80ab3497a69ab8d2967847451a87f04fb0a

95793df9284fe35c0491e5cfa36bc8f49fd426ccdf35f5fe2f098e07d160a4dc

bd133efea4b865f42eb05e0c92e3ab3b58ac087c0682ea9112b96596a7111ff6

9d9940b60809e3c10cd4540f8e589626a293244a999bea16c259f9712969a742

4c17f7ee55f9bf6fa9acaeeb9574feab39ba4a3cccd4426dfa85aaf58b90ae73

db8ed3e6dd7e6818046e7ee1e9c6c91f98aa5ce3113b14fb1c85a50a45569b18

482765b55aecbf24eb102f531afb6c8905ab7a058a447d217be70984f15b4573

63de4552312345e055236c82ecdc55c2bc8b3c37f363cb081f8f788b5203d759

c9d36fcce70893aa16a846b48009bbd8b46fc11c6821b750083a9c89669038cc

50b7e742eea52e18cf908cd676b87c0f145ecc3ff9692b01c90c47750fe989a7

96b5ea21a2556486cebbed76711a8bbae42de1e97e3311213833c6567a4fbbdc

0c857501e3851072db666386136929c06bcf4c8d3160b41b7d82a3ce9afca1be

81763d8e3b42d07d76b0a74eda4e759981971635d62072c8da91251fc849b91e

47849f610a30d72660b1725a0b18d78c5204257b3740641727bdcbfd1ebd466a

1e7614f757d40a2f5e2f4bd5597d04878768a9c01aa5f9f23d6c87660f7f0fbc

93e2ea6f021951369028b73637d9558c8baf3c99d9de1a2a60c1461cb9d571bf

61b5b6a513be380d50282c1c8391a5362d746bd70506343d04bda3751c3b25de

5474d15059ca4213ab1c13fba25ab8ba38559cac7ec2ab336d2411b90eab1217

9049d536e6da46b63c562197ab92f511d5f5e2883eb8bf29f72217282ae25772

f79273a1efb664d81f68e808b9ec963bfeb79d63bd277108863d6ae3c4801a9e

24c870202b3aedfcd28a8afb93b5212b791c265abd872ef94e44401d1ca309ad

8a0d6e40e545d40956194230f03608859f2a47420a9b11b199142641bc6419ee

8bcc23ec881d61839fc57e8ec7425ac5ed625425fbf265fcb53ad73a73825b18

a2e9a2389faf04b67fbbd6fc71134860a145db7643d88ba312390493d5619302

366284c1a0577937c86744349ac47e6e578da500ada3deb857ff233d9851ee6b

25fbe0ff3274b4bc981fa6ec0459e9b95cec6397194e10ea6287bf4b899a9b07

76e129552a30fa5c914d9f946f40b2ec2bbbbeb4e5e2f324e70455725030e157

ee0d55b9a2d03c5bea9f69f98b042ab7b3064366f335a8a53096387876bf48d7

13eb08dda92356f21888d95a6611a46728dfcefcdf769e7edad1a70e958e5367

9f96e5bc9ffc9742cb10384566dc7fb232e0f0d633e643bd487b747b6e88f369

7bdb945f2dab863a299e26ab4c6dfb1e4f7321c38fe101224252d993495bc157

9ed8eeb1db8909c96a958d91213093d2488dc172a8d22ba62657b9bfeb044fec

9246ed27032429f234888b2713529001344850c608cab9f5ab7274195d330bec

57f261cc442dd9a4f1cd4ffd281c9855f4f9a736abffaf539d9df2a6ea0dd409

ae4f3b6c43d5ea8ee68d862362d4e8d7b317889eb9abead948a9b791ad9d7071

244f2d4f3c34d00babef5f1765e91c0abda9dbd1d131fc93ecb48c91ecc801a8

e35547cfb6ae3fe18df6d887334952e7a38cc51a230f02c7f62a5fef083de7cf

6c367333c677c2268df9deaff6ad4e711e73e53504aa1aa845bebfbfe635f1d2

3e50f0eaf02d12653d5f757372240adcb5c16a5ab647a667637ba4c50d37aaad

Hostname

Value
www.galaxyswapper.ru

IPv4-Addr

Value
77.73.134.2

Url

Value
https://www.galaxyswapper.ru/

External References

- https://otx.alienvault.com/pulse/64df6cf26aef695423496e21
- https://research.checkpoint.com/2023/dotrunpex-demystifying-new-virtualized-net-injector-used-in-the-wild/