Aug 01 2023

NETMANAGEIT

Intelligence Report

NodeStealer 2.0 – The Python Version: Stealing Facebook Business Accounts

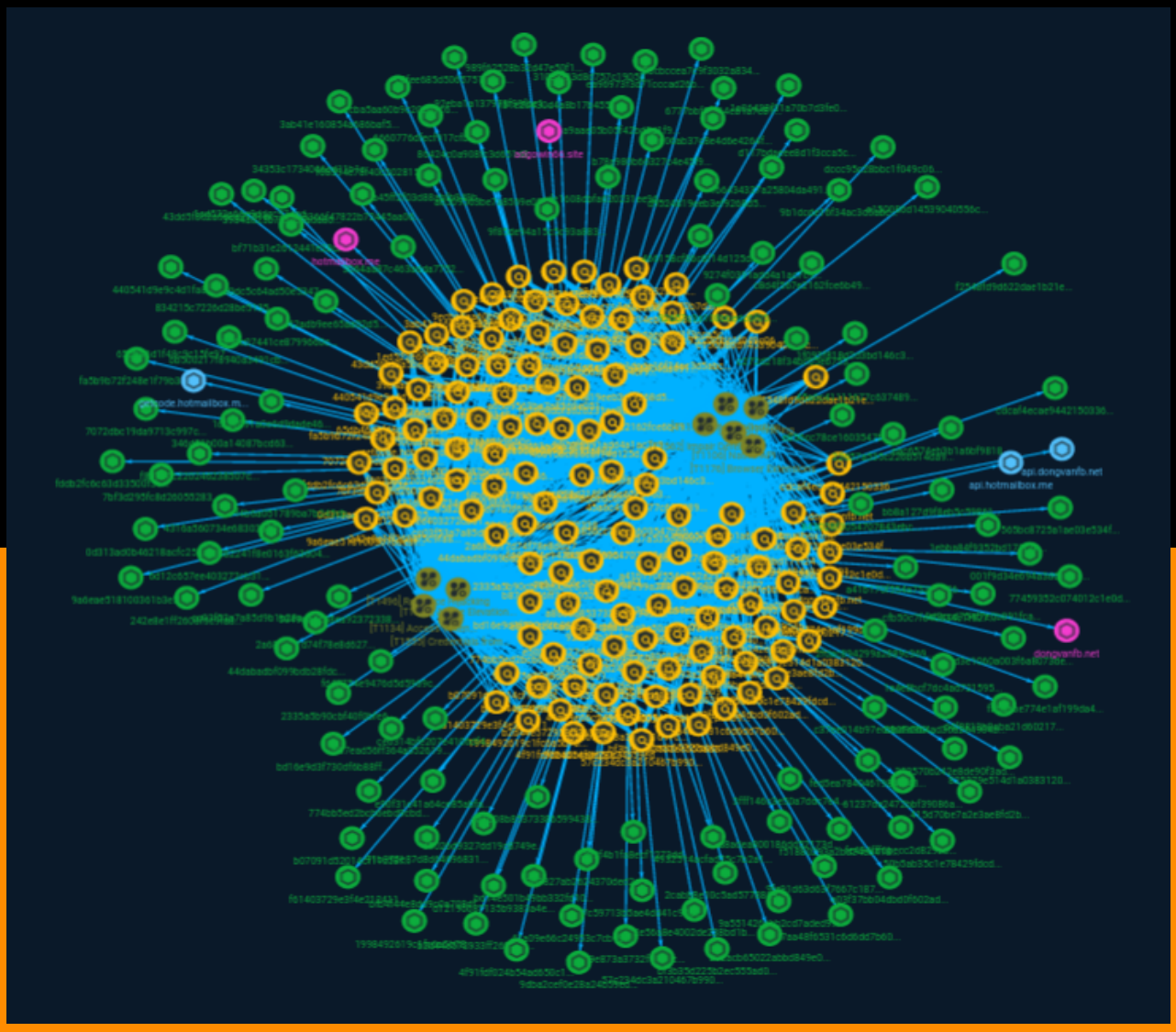

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Unit 42 researchers have recently discovered a previously unreported phishing campaign that distributed an infostealer equipped to fully take over Facebook business accounts. Facebook business accounts were targeted with a phishing lure offering tools such as spreadsheet templates for business. This is part of a growing trend of threat actors targeting Facebook business accounts – for advertising fraud and other purposes – which emerged around July 2022 with the discovery of the Ducktail infostealer.

Confidence

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

15 / 100

Indicator

Name
a6509563be7a8569e05198858658b8934d7bc5ad3d41e9806e261995c99a6acf
Description
md5_constants
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'a6509563be7a8569e05198858658b8934d7bc5ad3d41e9806e261995c99a6acf']
Name
e5026d9327dd19c8749ef1d93ebfbd7c1d3c3e1055bb2c1efc7ed261d7dd16de
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = 'e5026d9327dd19c8749ef1d93ebfbd7c1d3c3e1055bb2c1efc7ed261d7dd16de']

Name

22d57a535c226b514da92d0dcc902f0029414c5f2b1141bc14ac9a057c791414

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '22d57a535c226b514da92d0dcc902f0029414c5f2b1141bc14ac9a057c791414']

Name

5049de4c58ea923723389e4d732f1c134dc38582971f4872593e1153db945078

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5049de4c58ea923723389e4d732f1c134dc38582971f4872593e1153db945078']

Name

fd47754e9476d5d5969cd1c2db1a4d3203ab50e4b92e31bc7cc02945b8d2857e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fd47754e9476d5d5969cd1c2db1a4d3203ab50e4b92e31bc7cc02945b8d2857e']

Name

843028f3054707843ebc650a01b1ded0414d6933525cb056cf5a66a49afe3022

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '843028f3054707843ebc650a01b1ded0414d6933525cb056cf5a66a49afe3022']

Name

fed5ea7840461984fa40784d84ed1a0961cbf48b03d8b79c522286bf6e220922

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fed5ea7840461984fa40784d84ed1a0961cbf48b03d8b79c522286bf6e220922']

Name

a45ff2f03d88abfb949b8c8f40fa08fa7e72d22e756716f8dc18e2f34376b722

Description

Win64:Malware-gen

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a45ff2f03d88abfb949b8c8f40fa08fa7e72d22e756716f8dc18e2f34376b722']

Name

c8d4f567e2162fce6b49c15ca0908f9e3171e6bb6acbfd2c7b129872053b025d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c8d4f567e2162fce6b49c15ca0908f9e3171e6bb6acbfd2c7b129872053b025d']

Name

9282f4b1fa8ecf1273ddf3291abcc8fc073b2e99a00f70985077197112a46c4c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9282f4b1fa8ecf1273ddf3291abcc8fc073b2e99a00f70985077197112a46c4c']

Name

8582241f8e0163f6360486e9b59e54c91dd3219538e03619e9e999f90aa92f81

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8582241f8e0163f6360486e9b59e54c91dd3219538e03619e9e999f90aa92f81']

Name

009827ab2624370ded2cb8240ca2fe82af36e3a94cff1f8a2eac574b4b928c4e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '009827ab2624370ded2cb8240ca2fe82af36e3a94cff1f8a2eac574b4b928c4e']

Name

3064aa87c463adda7752b84cd18e2e859723a9953e090f7757edf7ce4b96e536

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '3064aa87c463adda7752b84cd18e2e859723a9953e090f7757edf7ce4b96e536']
Name
cfb50c7fe40334c1f52759a08289e36be0ada9056e3dcb22898efd8187b6464d
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'cfb50c7fe40334c1f52759a08289e36be0ada9056e3dcb22898efd8187b6464d']
Name
d12196087135b9383a4e9820d27625c059511c4776593a4d2eb83409a96af3a5
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'd12196087135b9383a4e9820d27625c059511c4776593a4d2eb83409a96af3a5']

Name

fe1608dbfa620231ee9649a4687ac03c2acfbcec9b7ab49da06e182209c31eb5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fe1608dbfa620231ee9649a4687ac03c2acfbcec9b7ab49da06e182209c31eb5']

Name

9f85de94a15c5c93a88375d9aacb9f9e111cedec611ee4f2b58a53727db92a88

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9f85de94a15c5c93a88375d9aacb9f9e111cedec611ee4f2b58a53727db92a88']

Name

92657c3a108bbedc6f05b4af0a174e99a58e51e69c15c707d9c9cc63cdf1b4ea

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '92657c3a108bbedc6f05b4af0a174e99a58e51e69c15c707d9c9cc63cdf1b4ea']

Name

cd06ab37c8e4d6e4264f2ac0949ab7694eb5cc11925853a50c33b13b012eca6f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cd06ab37c8e4d6e4264f2ac0949ab7694eb5cc11925853a50c33b13b012eca6f']

Name

a8adea800186dd52173dc6e55c46aa0b3619bef3eee25b17b7edba9353d5d08e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a8adea800186dd52173dc6e55c46aa0b3619bef3eee25b17b7edba9353d5d08e']

Name

b78a980b66327c4e45f95f2e0fc2dbaffebcac00107cd16ac2d2c2a42618e645

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b78a980b66327c4e45f95f2e0fc2dbaffebcac00107cd16ac2d2c2a42618e645']

Name

c272d218f34bc65e6753e7ece1fe6e56799782678a66a5084e71bbb8690fe724

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c272d218f34bc65e6753e7ece1fe6e56799782678a66a5084e71bbb8690fe724']

Name

1cf31091a0e6d9dade4675497593d04815d7ba22b0b018d06358211f3429ab49

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1cf31091a0e6d9dade4675497593d04815d7ba22b0b018d06358211f3429ab49']

Name

2fdac894299a2889c36959e34bacd3898029974af1b2f60552534454c54bd976

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2fdac894299a2889c36959e34bacd3898029974af1b2f60552534454c54bd976']

Name

1a4e8bcf7dc4ad7215957210c8e047f552b45a70daf3d623436940979c38f94c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1a4e8bcf7dc4ad7215957210c8e047f552b45a70daf3d623436940979c38f94c']

Name

e90f31c41a64ce85abfa284126e63b693088934fd83ef8fea13724810f394efa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e90f31c41a64ce85abfa284126e63b693088934fd83ef8fea13724810f394efa']

Name

a8608b8537338659943802bd4c3f37465b6b7146c60088e890f1201452690510

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a8608b8537338659943802bd4c3f37465b6b7146c60088e890f1201452690510']

Name

3fff146c3e50a7ddc7e446ae51742c59c3d3277931f3c511d9651497e4ab14a7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3fff146c3e50a7ddc7e446ae51742c59c3d3277931f3c511d9651497e4ab14a7']

Name

a9aae05b05f42bd3d1f9d7894a68db976977573741ddcdf6f388b7d685765564

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a9aae05b05f42bd3d1f9d7894a68db976977573741ddcdf6f388b7d685765564']

Name

b87ead56ff364a052619c373b8c06d2150561196f87e584590f67a341ba78abc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b87ead56ff364a052619c373b8c06d2150561196f87e584590f67a341ba78abc']

Name

346d51b00a14087bcd63f063e4a3f572f49b1c41a5c60fa03095aac42837a7ce

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '346d51b00a14087bcd63f063e4a3f572f49b1c41a5c60fa03095aac42837a7ce']

Name

31038f33d8d757c19050d41e62036a85026bbe99d37fd806fdde7f261fd2651b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '31038f33d8d757c19050d41e62036a85026bbe99d37fd806fdde7f261fd2651b']

Name

9fe91d63d63f7667c1879f7ea3e31b9d6dacc2d3216df2b47392bb1dff741f89

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9fe91d63d63f7667c1879f7ea3e31b9d6dacc2d3216df2b47392bb1dff741f89']

Name

14000dc5c64ad50e534739afa86ce37c30b04a8aba48feb0f645b0a74b545744

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '14000dc5c64ad50e534739afa86ce37c30b04a8aba48feb0f645b0a74b545744']

Name

9d3ccd754f7e0b891fcad461df92746f52abcf727082750e3aefade7531f162e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9d3ccd754f7e0b891fcad461df92746f52abcf727082750e3aefade7531f162e']

Name

bfb4f44e8dd9c0a708df89f0f114b523c446baaee19205d62ad99bb53a8b5935

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bfb4f44e8dd9c0a708df89f0f114b523c446baaee19205d62ad99bb53a8b5935']

Name

3366f47822b72445aa06d2e2c455dd4816e5df2f83e7bd03f21e77b1cb2b8948

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3366f47822b72445aa06d2e2c455dd4816e5df2f83e7bd03f21e77b1cb2b8948']

Name

415d70be7a2e3ae8fd2babc929c3110fce7ce66d23ec32c473c6aab73c5c00f8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '415d70be7a2e3ae8fd2babc929c3110fce7ce66d23ec32c473c6aab73c5c00f8']

Name

4316a560734e68303860899d0f2b07a9ef4618647da2e8ad38bab70a4e532f88

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4316a560734e68303860899d0f2b07a9ef4618647da2e8ad38bab70a4e532f88']

Name

bb8a127d9f8eb5c598617682a4ab29ee023ae8f40428c6076b0b493116eca8bb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bb8a127d9f8eb5c598617682a4ab29ee023ae8f40428c6076b0b493116eca8bb']

Name

91b975e87d8d6469683168a48ca0bc11a333e3f5692f224d33f2008573173cc6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '91b975e87d8d6469683168a48ca0bc11a333e3f5692f224d33f2008573173cc6']

Name

hotmailbox.me

Pattern Type

stix

Pattern

[domain-name:value = 'hotmailbox.me']

Name

466158cf86c8f14d125d661f75fe0c4c2410e2896eaabd90b1d28137b7df81b3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '466158cf86c8f14d125d661f75fe0c4c2410e2896eaabd90b1d28137b7df81b3']

Name

bd14e501b49bb332fd102f65558be47e762ff8885d9c7dfe6c152597603664f1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bd14e501b49bb332fd102f65558be47e762ff8885d9c7dfe6c152597603664f1']

Name

c150086d14539040556c3c91c93c31395d23ee7bc348bd3dc1d0afa0ff9365bb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c150086d14539040556c3c91c93c31395d23ee7bc348bd3dc1d0afa0ff9365bb']

Name

2cabb8e10c5ad57788d99f5218a1248e0ada9a5bdbd5f976d9523b2e4a47aacf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2cabb8e10c5ad57788d99f5218a1248e0ada9a5bdbd5f976d9523b2e4a47aacf']

Name

8896c07441ce8799660c1d94d64231a41735bac10a2e984838bc21a2682c9c99

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8896c07441ce8799660c1d94d64231a41735bac10a2e984838bc21a2682c9c99']

Name

45a6c41111677c6374899475aa253f713a08158ce9b5dbd7566e15eda1e61a0a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '45a6c41111677c6374899475aa253f713a08158ce9b5dbd7566e15eda1e61a0a']

Name

4f91fdf024b54ad650c13f7ffe1a7f3eb6cad66eb457e8a7fe494cf9bdb6f42a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4f91fdf024b54ad650c13f7ffe1a7f3eb6cad66eb457e8a7fe494cf9bdb6f42a']

Name

6660776dfecf917cfbd51a0fa853052005f3d4a136c1edce0a3d6b7002c3f48e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6660776dfecf917cfbd51a0fa853052005f3d4a136c1edce0a3d6b7002c3f48e']

Name

0901d9b4ad36a264904bb41b555b32c87790e7861969fa7495da7892aef8f67c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0901d9b4ad36a264904bb41b555b32c87790e7861969fa7495da7892aef8f67c']

Name

f4b6a051789ba7b245db69a3b56dee1404b3f9eff9c7e7c80c54328bedcc44e9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f4b6a051789ba7b245db69a3b56dee1404b3f9eff9c7e7c80c54328bedcc44e9']

Name

9274f0391add4a1ac7c90942628a9fd80a9fca3d11aabb74b4e385eee4f66354

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9274f0391add4a1ac7c90942628a9fd80a9fca3d11aabb74b4e385eee4f66354']

Name

f51880293a2bd24da4182965ad5c9b4936eab23a20ed0b4264b75d6c3a3eeac5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f51880293a2bd24da4182965ad5c9b4936eab23a20ed0b4264b75d6c3a3eeac5']

Name

65db46d1f48c9c15fe97147ee918fae626225c5603293b72da8e484a9c91123f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '65db46d1f48c9c15fe97147ee918fae626225c5603293b72da8e484a9c91123f']

Name

c37ee014b97eddbd9060e6bc3a27ec5de2c37a03c45f3a50fd9420a847145a20

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c37ee014b97eddbd9060e6bc3a27ec5de2c37a03c45f3a50fd9420a847145a20']

Name

cc03f53a7a85d9b1b28a6422556b295cb9b00e93b5afc96559140f32f96305e9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cc03f53a7a85d9b1b28a6422556b295cb9b00e93b5afc96559140f32f96305e9']

Name

adgowin66.site

Pattern Type

stix

Pattern

[domain-name:value = 'adgowin66.site']

Name

fe434fff6becc2d829bbfed6ba9bf88154028d0327e7c6aa870ad050235fc334

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fe434fff6becc2d829bbfed6ba9bf88154028d0327e7c6aa870ad050235fc334']

Name

1ada42adb9ee65aa02d5eb9d24d3455df61c85f69e84f310b9630d62ca83a518

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1ada42adb9ee65aa02d5eb9d24d3455df61c85f69e84f310b9630d62ca83a518']

Name

1f093f818d2d3bd146c34d10bdb9de0a33931d3586f0bb942f881052a20114f9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1f093f818d2d3bd146c34d10bdb9de0a33931d3586f0bb942f881052a20114f9']

Name
4932514acfad25c7b2a1631706aef8d91a415315e5207e1bc9a24791298e6319
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '4932514acfad25c7b2a1631706aef8d91a415315e5207e1bc9a24791298e6319']
Name
34353c1734066cd11b1c002f770834d392aa225434e1bc8b4ec65ef753241e23
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '34353c1734066cd11b1c002f770834d392aa225434e1bc8b4ec65ef753241e23']
Name
e856cc78ce1603547bb6fdb3eb9da137f671e9547c072abea63b0248ec82ecb1
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = 'e856cc78ce1603547bb6fdb3eb9da137f671e9547c072abea63b0248ec82ecb1']

Name

7072dbc19da9713c997cdbcacbc68ca709e900d44bb3572bc34fb3c91ecbea9f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7072dbc19da9713c997cdbcacbc68ca709e900d44bb3572bc34fb3c91ecbea9f']

Name

1a06498f31a70b7d3fe043269cc87dcd70528a9303af3fa66933ceaa372006b3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1a06498f31a70b7d3fe043269cc87dcd70528a9303af3fa66933ceaa372006b3']

Name

9a551426cbb2cd7aded923f277eec195a282913d51c41f1791683e03a85379e0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9a551426cbb2cd7aded923f277eec195a282913d51c41f1791683e03a85379e0']

Name

3984a025b7fb7c5ada86da0b4fa32bef88eb2a01fb337a7f73619cb716c859ab

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3984a025b7fb7c5ada86da0b4fa32bef88eb2a01fb337a7f73619cb716c859ab']

Name

77459352c074012c1e0d010e2b8792d08f36ca6f7bf4882b2db2af4aa1944e5f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '77459352c074012c1e0d010e2b8792d08f36ca6f7bf4882b2db2af4aa1944e5f']

Name

b07091d52014cf11c58f07f676eb150db006d9f9274ce6888d5aa8d7a6e4f793

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b07091d52014cf11c58f07f676eb150db006d9f9274ce6888d5aa8d7a6e4f793']

Name

d9524819eeb3ef9268d526703af8a7921a5d98429341834eb84f04b9edb34b64

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd9524819eeb3ef9268d526703af8a7921a5d98429341834eb84f04b9edb34b64']

Name

283570b242e8de90f3ad4b9f332c03eefc3c8464981d1ad072cc061f9e29ce97

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '283570b242e8de90f3ad4b9f332c03eefc3c8464981d1ad072cc061f9e29ce97']

Name

bb500217f8940a3491cb69a26d10b5753e3ef1fab59909d88a12dba44344df1e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bb500217f8940a3491cb69a26d10b5753e3ef1fab59909d88a12dba44344df1e']

Name

a41b170f554a752a23769b28f3fa93703fa160b74897a8f35078d1e8923b91b0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a41b170f554a752a23769b28f3fa93703fa160b74897a8f35078d1e8923b91b0']

Name

61237de2472bbf39086a18d462fd5fd9649292d17fe630f1dd550159e26d711e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '61237de2472bbf39086a18d462fd5fd9649292d17fe630f1dd550159e26d711e']

Name

getcode.hotmailbox.me

Pattern Type

stix

Pattern

[hostname:value = 'getcode.hotmailbox.me']

Name

api.dongvanfb.net

Pattern Type

stix

Pattern

[hostname:value = 'api.dongvanfb.net']

Name

bd16e9d3f730df6b88fff91485d3d27e544f3bb819347b0886806b1c14cbd575

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'bd16e9d3f730df6b88fff91485d3d27e544f3bb819347b0886806b1c14cbd575']
Name
f66434337a25804da491d45a7108eab49ad0de1b2b26f41650ae9567ec45a02a
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f66434337a25804da491d45a7108eab49ad0de1b2b26f41650ae9567ec45a02a']
Name
a03f37bb04dbd0f602ad8f5e52e87650ecf8fc57763c043de436996ce222e81d
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'a03f37bb04dbd0f602ad8f5e52e87650ecf8fc57763c043de436996ce222e81d']

Name

fddb2fc6c63d33500f3ef0d8c3fe212abe21044820a2524379904131e7f11765

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fddb2fc6c63d33500f3ef0d8c3fe212abe21044820a2524379904131e7f11765']

Name

001f9d34e694a3d6e301a4e660f2d96bc5d6aa6898f34d441886c6f9160d9e48

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '001f9d34e694a3d6e301a4e660f2d96bc5d6aa6898f34d441886c6f9160d9e48']

Name

774bb5ed2bcb6ebd9cbd6b53e4dc1a352df58dfda17ef11da9c8ffa4d4851681

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '774bb5ed2bcb6ebd9cbd6b53e4dc1a352df58dfda17ef11da9c8ffa4d4851681']

Name

f31e2c430d4a8b17b45591bf68e5c4c7f7c28e4ccbd4cabcd10c33ba14b388c3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f31e2c430d4a8b17b45591bf68e5c4c7f7c28e4ccbd4cabcd10c33ba14b388c3']

Name

d3e1060a003f6a8073dea4f6c976f552372cd4ab9251953c0932be22c6f6605f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd3e1060a003f6a8073dea4f6c976f552372cd4ab9251953c0932be22c6f6605f']

Name

7bf3d295fc8d2605528331c0da32d83f2b98489884bd92a24b71425fa13290db

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7bf3d295fc8d2605528331c0da32d83f2b98489884bd92a24b71425fa13290db']

Name

9b1dcde16f34ac3d5abc15510060cd169259105498841616 7dae3c4643e5796c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9b1dcde16f34ac3d5abc15510060cd169259105498841616 7dae3c4643e5796c']

Name

2e56a8e4002de238bd1b792d495f59edd598cda49d649d42112f951ecb003432

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2e56a8e4002de238bd1b792d495f59edd598cda49d649d42112f951ecb003432']

Name

f08394c78f40c3028156c78672d1a8030c64a9f292b1fbb4bd42437381c96a54

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f08394c78f40c3028156c78672d1a8030c64a9f292b1fbb4bd42437381c96a54']

Name

api.hotmailbox.me

Pattern Type

stix

Pattern

[hostname:value = 'api.hotmailbox.me']

Name

2a685317d74f78e8d627791ccf6ffec9e2a8690e4bffacbbffab934b12669ae9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2a685317d74f78e8d627791ccf6ffec9e2a8690e4bffacbbffab934b12669ae9']

Name

92eba1a137918f99fbe15651568b8b76ad5f59788b1bce9076bfb33bbc3484de

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '92eba1a137918f99fbe15651568b8b76ad5f59788b1bce9076bfb33bbc3484de']

Name

7aa48f6531c6d6dd7b60a4c6d10cacc69bdee98034b25379a04a8e308dece36f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7aa48f6531c6d6dd7b60a4c6d10cacc69bdee98034b25379a04a8e308dece36f']

Name

0d313ad0b46218acfc25fae744b53eb539169e56f9976eec47f37d99ebce510c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0d313ad0b46218acfc25fae744b53eb539169e56f9976eec47f37d99ebce510c']

Name

d117bdaeee8d1f3cca5c685930f19754b82ffbd6de8f2a6dc1895fee1a00e220

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd117bdaeee8d1f3cca5c685930f19754b82ffbd6de8f2a6dc1895fee1a00e220']

Name

7c59713b5ae4dd41c94cda9c2cb15a2e6173b886157a2ba5a68842cc7bdde698

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7c59713b5ae4dd41c94cda9c2cb15a2e6173b886157a2ba5a68842cc7bdde698']

Name

bf71b31e2612441e28df35f7e4ae56616ded9c6802758b010007b49e05876011

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bf71b31e2612441e28df35f7e4ae56616ded9c6802758b010007b49e05876011']

Name

ce6314bfe207e4106df4249452b654ffa892a1bd45bc7ff9d6871b1dbe8e3e3b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ce6314bfe207e4106df4249452b654ffa892a1bd45bc7ff9d6871b1dbe8e3e3b']

Name

6d12c657ee403272cb3115fd0a6cf1ffe69cd4476c5a03bbc13c624ddd153518

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6d12c657ee403272cb3115fd0a6cf1ffe69cd4476c5a03bbc13c624ddd153518']

Name

ea96973f3d71cccad26bce7f106f5800fcb007cf33d82fa00f5d564994397153

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ea96973f3d71cccad26bce7f106f5800fcb007cf33d82fa00f5d564994397153']

Name

9dba2cef0e28a24b59eda107633528cd83257f033a5d4330cf3302943b3e07c2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9dba2cef0e28a24b59eda107633528cd83257f033a5d4330cf3302943b3e07c2']

Name

440541d9e9c4d1fa8a1f33ce8c434ace11786e278278df7a600978290b33e93f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '440541d9e9c4d1fa8a1f33ce8c434ace11786e278278df7a600978290b33e93f']

Name

eac6574eb3b1a6bf9818136875378ee2362901092b61d221541977925076edf3

Description

md5_constants

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'eac6574eb3b1a6bf9818136875378ee2362901092b61d221541977925076edf3']

Name

b2d44e572933ff26977e25a254c0ce705939fac9f422871fd22a875323487bcf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b2d44e572933ff26977e25a254c0ce705939fac9f422871fd22a875323487bcf']

Name

9ecba5aa60b9c202b1c69aade1edabb1c04072471a3618a5d714aa8833d570f4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9ecba5aa60b9c202b1c69aade1edabb1c04072471a3618a5d714aa8833d570f4']

Name

825379e514d1a0383120735c4c19530a3d4130d5e77ff51b7bb2eb3b6ca1d704

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '825379e514d1a0383120735c4c19530a3d4130d5e77ff51b7bb2eb3b6ca1d704']

Name

fa5b9b72f248e1f79b3a424b61a1bcce8bf6a99452545cfe15d7211f3eb3e93b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fa5b9b72f248e1f79b3a424b61a1bcce8bf6a99452545cfe15d7211f3eb3e93b']

Name

6777bbf5fd14eb1a7e81de33c477ac5ba4f446699df447995e8d362a8438a0a3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6777bbf5fd14eb1a7e81de33c477ac5ba4f446699df447995e8d362a8438a0a3']

Name

65669e873a3732f1617c9c80667a1c3efda5f72538b5abd475e80a25efc0e5e2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '65669e873a3732f1617c9c80667a1c3efda5f72538b5abd475e80a25efc0e5e2']

Name

1ed522e66e9ddcc97ded3e008c014500e3c3e22a1db995199baa52a7dc93845b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1ed522e66e9ddcc97ded3e008c014500e3c3e22a1db995199baa52a7dc93845b']

Name

d4f8813b0aba21d6021719d022fcc6feab5cdd6e2a999dfe178347a394abfb84

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd4f8813b0aba21d6021719d022fcc6feab5cdd6e2a999dfe178347a394abfb84']

Name

f80700c220246238507cf5eedcb2e1397c32b3646bb90ad990e7fb69199752b5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f80700c220246238507cf5eedcb2e1397c32b3646bb90ad990e7fb69199752b5']

Name

86424c0a908fc3d651d86bc7c3d87ce38ef626516f48a160e2cfcf2630a1e9b8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '86424c0a908fc3d651d86bc7c3d87ce38ef626516f48a160e2cfcf2630a1e9b8']

Name

a62acb65022abbd849e0a741a17485156333fbfe26f32c50654b3818335c1d0d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a62acb65022abbd849e0a741a17485156333fbfe26f32c50654b3818335c1d0d']

Name

2335a5b90cbf40f0bfe6434c7e9b461ab1ed8f470a9c3d5703d430af30cf5371

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2335a5b90cbf40f0bfe6434c7e9b461ab1ed8f470a9c3d5703d430af30cf5371']

Name

1ebba84f9352bd171f241bc5d0e06af3145a050fd3e063c503d78085aeba2c34

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1ebba84f9352bd171f241bc5d0e06af3145a050fd3e063c503d78085aeba2c34']

Name

f61403729e3f4e212411db486a537eabca2d0b84be21b789cddca4fc3aa85923

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f61403729e3f4e212411db486a537eabca2d0b84be21b789cddca4fc3aa85923']

Name

c8fee685d506575138c8b02f118323ca586f62a6e80edf1d726fd555a1c386ba

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c8fee685d506575138c8b02f118323ca586f62a6e80edf1d726fd555a1c386ba']

Name

50b5ab35c1e78429fdcdd45e2a0ceacc140fbf4022f7c34bac4b5f296a17379a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '50b5ab35c1e78429fdcdd45e2a0ceacc140fbf4022f7c34bac4b5f296a17379a']

Name

242e8e1ff2608f5c9fa80b89b31f605bb9432b15dace2eba961605b245d577d5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '242e8e1ff2608f5c9fa80b89b31f605bb9432b15dace2eba961605b245d577d5']

Name

dccc95c28bbc1f049c06e7b3a9866a920c4c4081e3176b26fc6aea2cb59daed7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dccc95c28bbc1f049c06e7b3a9866a920c4c4081e3176b26fc6aea2cb59daed7']

Name

bf3b35d225b2ec555ad06eb1dd0af464bb48596bebb0b2543eaf9e060f0fb1b9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bf3b35d225b2ec555ad06eb1dd0af464bb48596bebb0b2543eaf9e060f0fb1b9']

Name

834215c7226d28be513562991cacd7f56f4914b8ae1e27ff3ae85ca82e208605

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '834215c7226d28be513562991cacd7f56f4914b8ae1e27ff3ae85ca82e208605']

Name

cdcaf4ecae94421503364d28ef72eb65a83f300980cd1a8ba02bea1c29e193ec

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cdcaf4ecae94421503364d28ef72eb65a83f300980cd1a8ba02bea1c29e193ec']

Name

1998492619c1fc6a5b78d5c4c6beb05c582a1be6ad2b9ac734179c731bbcf5cc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1998492619c1fc6a5b78d5c4c6beb05c582a1be6ad2b9ac734179c731bbcf5cc']

Name

989f62528b32d47e50f1bd61cc7dc2e9cb25f54514374902d8a9ce41fcfcd779

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '989f62528b32d47e50f1bd61cc7dc2e9cb25f54514374902d8a9ce41fcfcd779']

Name

fab5abe774e1af199da4b85df87077e2e8f66c6f00f083b9074fd2186e455bfb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fab5abe774e1af199da4b85df87077e2e8f66c6f00f083b9074fd2186e455bfb']

Name

9a6eae518100361b3e3fd4f34877623af5544e2b95cdf29a7e9e2d91e4baa271

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9a6eae518100361b3e3fd4f34877623af5544e2b95cdf29a7e9e2d91e4baa271']

Name

f2548fd9d622dae1b21e18323a2d8dca2f7670789dfbb5f6d32320f4fd289039

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f2548fd9d622dae1b21e18323a2d8dca2f7670789dfbb5f6d32320f4fd289039']

Name

41a09e66c24953c7cb19f4a09b0779c8e9bcb39f0e544d0bdc9760c9b3d56e03

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '41a09e66c24953c7cb19f4a09b0779c8e9bcb39f0e544d0bdc9760c9b3d56e03']

Name

3ab41e160854a686baf56e5032b933778663c37e03d148d3bf669a6c3228f6da

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3ab41e160854a686baf56e5032b933778663c37e03d148d3bf669a6c3228f6da']

Name

dongvanfb.net

Pattern Type

stix

Pattern

[domain-name:value = 'dongvanfb.net']

Name

44dabadbf099bdb28fdc4d86cebe53c00085c9c2ad52df4d4774320409e7358b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '44dabadbf099bdb28fdc4d86cebe53c00085c9c2ad52df4d4774320409e7358b']

Name

38cbccea7c9f3032a8348e54bb94871b26279a7cca64f5b79c3fa54c240960d2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '38cbccea7c9f3032a8348e54bb94871b26279a7cca64f5b79c3fa54c240960d2']

Name

57c234dc3a210467b990c16092fbd3af2dc0aaf8aabbdfa1b566138b2abc5e82

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '57c234dc3a210467b990c16092fbd3af2dc0aaf8aabbdfa1b566138b2abc5e82']

Name

43dd5f8d2a5bea2751bf8d02920038e93df6ba3b8f5c0b1193fa70cac1e9b9a2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '43dd5f8d2a5bea2751bf8d02920038e93df6ba3b8f5c0b1193fa70cac1e9b9a2']

Name

565bc8725a1ae03e534f66ad8995854d24ba3893fe37c8e3e13c58874129849b

Pattern Type
stix

Pattern
[file:hashes.'SHA-256' = '565bc8725a1ae03e534f66ad8995854d24ba3893fe37c8e3e13c58874129849b']

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
Email Collection
ID
T1114
Description

Adversaries may target user email to collect sensitive information. Emails may contain sensitive data, including trade secrets or personal information, that can prove valuable to adversaries. Adversaries can collect or forward email from mail servers or clients.

Name

Browser Extensions

ID

T1176

Description

Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition) Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions. Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `.mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install configuration profiles, however `.mobileconfig` files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS) Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence. (Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension) There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions.(Citation: Stantinko Botnet) There have also been similar examples of extensions being used for command & control.(Citation: Chrome Extension C2 Malware)

Name

Resource Hijacking

ID

T1496

Description

Adversaries may leverage the resources of co-opted systems in order to solve resource intensive problems, which may impact system and/or hosted service availability. One common purpose for Resource Hijacking is to validate transactions of cryptocurrency networks and earn virtual currency. Adversaries may consume enough system resources to negatively impact and/or cause affected machines to become unresponsive.(Citation: Kaspersky Lazarus Under The Hood Blog 2017) Servers and cloud-based systems are common targets because of the high potential for available resources, but user endpoint systems may also be compromised and used for Resource Hijacking and cryptocurrency mining.(Citation: CloudSploit - Unused AWS Regions) Containerized environments may also be targeted due to the ease of deployment via exposed APIs and the potential for scaling mining activities by deploying or compromising multiple containers within an environment or cluster.(Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro Exposed Docker APIs) Additionally, some cryptocurrency mining malware identify then kill off processes for competing malware to ensure it’s not competing for resources.(Citation: Trend Micro War of Crypto Miners) Adversaries may also use malware that leverages a system's network bandwidth as part of a botnet in order to facilitate [Network Denial of Service](https://attack.mitre.org/techniques/T1498) campaigns and/or to seed malicious torrents.(Citation: GoBotKR)

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

Credentials from Password Stores

ID

T1555

Description

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications that store passwords to make it easier for users manage and maintain. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

Name

Impair Defenses

ID

T1562

Description

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators. Adversaries may also impair routine operations that contribute to defensive hygiene, such as blocking users from logging out of a computer or stopping it from being shut down. These restrictions can further enable malicious operations as well as the continued propagation of incidents.(Citation: Emotet shutdown) Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components.

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

Access Token Manipulation

ID

T1134

Description

Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token. An adversary can use built-in Windows API functions to copy access tokens from existing processes; this is known as token stealing. These token can then be applied to an existing process (i.e. [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001)) or used to spawn a new process (i.e. [Create Process with Token](https://attack.mitre.org/techniques/T1134/002)). An adversary must already be in a privileged user context (i.e. administrator) to steal a token. However, adversaries commonly use token stealing to elevate their security context from the administrator level to the SYSTEM level. An adversary can then use a token to authenticate to a remote system as the account for that token if the

account has appropriate permissions on the remote system.(Citation: Pentestlab Token Manipulation) Any standard user can use the `runas` command, and the Windows API functions, to create impersonation tokens; it does not require access to an administrator account. There are also other mechanisms, such as Active Directory fields, that can be used to modify access tokens.

Domain-Name

Value
hotmailbox.me
dongvanfb.net
adgowin66.site

StixFile

Value
fddb2fc6c63d33500f3ef0d8c3fe212abe21044820a2524379904131e7f11765
fa5b9b72f248e1f79b3a424b61a1bcce8bf6a99452545cfe15d7211f3eb3e93b
d9524819eeb3ef9268d526703af8a7921a5d98429341834eb84f04b9edb34b64
d117bdaeee8d1f3cca5c685930f19754b82ffbd6de8f2a6dc1895fee1a00e220
cdcaf4ecae94421503364d28ef72eb65a83f300980cd1a8ba02bea1c29e193ec
440541d9e9c4d1fa8a1f33ce8c434ace11786e278278df7a600978290b33e93f
283570b242e8de90f3ad4b9f332c03eefc3c8464981d1ad072cc061f9e29ce97
65669e873a3732f1617c9c80667a1c3efda5f72538b5abd475e80a25efc0e5e2
001f9d34e694a3d6e301a4e660f2d96bc5d6aa6898f34d441886c6f9160d9e48
14000dc5c64ad50e534739afa86ce37c30b04a8aba48feb0f645b0a74b545744
565bc8725a1ae03e534f66ad8995854d24ba3893fe37c8e3e13c58874129849b
6660776dfecf917cfbd51a0fa853052005f3d4a136c1edce0a3d6b7002c3f48e
9d3ccd754f7e0b891fcad461df92746f52abcf727082750e3aefade7531f162e

a03f37bb04dbd0f602ad8f5e52e87650ecf8fc57763c043de436996ce222e81d

825379e514d1a0383120735c4c19530a3d4130d5e77ff51b7bb2eb3b6ca1d704

34353c1734066cd11b1c002f770834d392aa225434e1bc8b4ec65ef753241e23

1ebba84f9352bd171f241bc5d0e06af3145a050fd3e063c503d78085aeba2c34

7bf3d295fc8d2605528331c0da32d83f2b98489884bd92a24b71425fa13290db

9b1dcde16f34ac3d5abc15510060cd16925910549884161 67dae3c4643e5796c

466158cf86c8f14d125d661f75fe0c4c2410e2896eaabd90b1d28137b7df81b3

f66434337a25804da491d45a7108eab49ad0de1b2b26f41650ae9567ec45a02a

9ecba5aa60b9c202b1c69aade1edabb1c04072471a3618a5d714aa8833d570f4

a6509563be7a8569e05198858658b8934d7bc5ad3d41e9806e261995c99a6acf

9a6eae518100361b3e3fd4f34877623af5544e2b95cdf29a7e9e2d91e4baa271

7072dbc19da9713c997cdbcacbc68ca709e900d44bb3572bc34fb3c91ecbea9f

c8d4f567e2162fce6b49c15ca0908f9e3171e6bb6acbfd2c7b129872053b025d

6d12c657ee403272cb3115fd0a6cf1ffe69cd4476c5a03bbc13c624ddd153518

ea96973f3d71cccad26bce7f106f5800fcb007cf33d82fa00f5d564994397153

45a6c41111677c6374899475aa253f713a08158ce9b5dbd7566e15eda1e61a0a

bf71b31e2612441e28df35f7e4ae56616ded9c6802758b010007b49e05876011

9f85de94a15c5c93a88375d9aacb9f9e111cedec611ee4f2b58a53727db92a88

b78a980b66327c4e45f95f2e0fc2dbaffebcac00107cd16ac2d2c2a42618e645

fe434fff6becc2d829bbfed6ba9bf88154028d0327e7c6aa870ad050235fc334

41a09e66c24953c7cb19f4a09b0779c8e9bcb39f0e544d0bdc9760c9b3d56e03

7aa48f6531c6d6dd7b60a4c6d10cacc69bdee98034b25379a04a8e308dece36f

f80700c220246238507cf5eedcb2e1397c32b3646bb90ad990e7fb69199752b5

2335a5b90cbf40f0bfe6434c7e9b461ab1ed8f470a9c3d5703d430af30cf5371

c37ee014b97eddbd9060e6bc3a27ec5de2c37a03c45f3a50fd9420a847145a20

61237de2472bbf39086a18d462fd5fd9649292d17fe630f1dd550159e26d711e

50b5ab35c1e78429fdcdd45e2a0ceacc140fbf4022f7c34bac4b5f296a17379a

3ab41e160854a686baf56e5032b933778663c37e03d148d3bf669a6c3228f6da

bb500217f8940a3491cb69a26d10b5753e3ef1fab59909d88a12dba44344df1e

91b975e87d8d6469683168a48ca0bc11a333e3f5692f224d33f2008573173cc6

989f62528b32d47e50f1bd61cc7dc2e9cb25f54514374902d8a9ce41fcfcd779

f08394c78f40c3028156c78672d1a8030c64a9f292b1fbb4bd42437381c96a54

6777bbf5fd14eb1a7e81de33c477ac5ba4f446699df447995e8d362a8438a0a3

fe1608dbfa620231ee9649a4687ac03c2acfbcec9b7ab49da06e182209c31eb5

9fe91d63d63f7667c1879f7ea3e31b9d6dacc2d3216df2b47392bb1dff741f89

1a4e8bcf7dc4ad7215957210c8e047f552b45a70daf3d623436940979c38f94c

2e56a8e4002de238bd1b792d495f59edd598cda49d649d42112f951ecb003432

e5026d9327dd19c8749ef1d93ebfbd7c1d3c3e1055bb2c1efc7ed261d7dd16de

4932514acfad25c7b2a1631706aef8d91a415315e5207e1bc9a24791298e6319

0d313ad0b46218acfc25fae744b53eb539169e56f9976eec47f37d99ebce510c

774bb5ed2bcb6ebd9cbd6b53e4dc1a352df58dfda17ef11da9c8ffa4d4851681

1ada42adb9ee65aa02d5eb9d24d3455df61c85f69e84f310b9630d62ca83a518

8582241f8e0163f6360486e9b59e54c91dd3219538e03619e9e999f90aa92f81

43dd5f8d2a5bea2751bf8d02920038e93df6ba3b8f5c0b1193fa70cac1e9b9a2

9a551426cbb2cd7aded923f277eec195a282913d51c41f1791683e03a85379e0

86424c0a908fc3d651d86bc7c3d87ce38ef626516f48a160e2cfcf2630a1e9b8

3064aa87c463adda7752b84cd18e2e859723a9953e090f7757edf7ce4b96e536

fd47754e9476d5d5969cd1c2db1a4d3203ab50e4b92e31bc7cc02945b8d2857e

57c234dc3a210467b990c16092fbd3af2dc0aaf8aabbdfa1b566138b2abc5e82

1998492619c1fc6a5b78d5c4c6beb05c582a1be6ad2b9ac734179c731bbcf5cc

eac6574eb3b1a6bf9818136875378ee2362901092b61d221541977925076edf3

2a685317d74f78e8d627791ccf6ffec9e2a8690e4bffacbbffab934b12669ae9

834215c7226d28be513562991cacd7f56f4914b8ae1e27ff3ae85ca82e208605

ce6314bfe207e4106df4249452b654ffa892a1bd45bc7ff9d6871b1dbe8e3e3b

c150086d14539040556c3c91c93c31395d23ee7bc348bd3dc1d0afa0ff9365bb

2fdac894299a2889c36959e34bacd3898029974af1b2f60552534454c54bd976

c8fee685d506575138c8b02f118323ca586f62a6e80edf1d726fd555a1c386ba

f31e2c430d4a8b17b45591bf68e5c4c7f7c28e4ccbd4cabcd10c33ba14b388c3

b07091d52014cf11c58f07f676eb150db006d9f9274ce6888d5aa8d7a6e4f793

f4b6a051789ba7b245db69a3b56dee1404b3f9eff9c7e7c80c54328bedcc44e9

843028f3054707843ebc650a01b1ded0414d6933525cb056cf5a66a49afe3022

7c59713b5ae4dd41c94cda9c2cb15a2e6173b886157a2ba5a68842cc7bdde698

a8adea800186dd52173dc6e55c46aa0b3619bef3eee25b17b7edba9353d5d08e

d4f8813b0aba21d6021719d022fcc6feab5cdd6e2a999dfe178347a394abfb84

346d51b00a14087bcd63f063e4a3f572f49b1c41a5c60fa03095aac42837a7ce

b2d44e572933ff26977e25a254c0ce705939fac9f422871fd22a875323487bcf

a62acb65022abbd849e0a741a17485156333fbfe26f32c50654b3818335c1d0d

1a06498f31a70b7d3fe043269cc87dcd70528a9303af3fa66933ceaa372006b3

bd16e9d3f730df6b88fff91485d3d27e544f3bb819347b0886806b1c14cbd575

f2548fd9d622dae1b21e18323a2d8dca2f7670789dfbb5f6d32320f4fd289039

bd14e501b49bb332fd102f65558be47e762ff8885d9c7dfe6c152597603664f1

a8608b8537338659943802bd4c3f37465b6b7146c60088e890f1201452690510

1f093f818d2d3bd146c34d10bdb9de0a33931d3586f0bb942f881052a20114f9

a41b170f554a752a23769b28f3fa93703fa160b74897a8f35078d1e8923b91b0

e856cc78ce1603547bb6fdb3eb9da137f671e9547c072abea63b0248ec82ecb1

8896c07441ce8799660c1d94d64231a41735bac10a2e984838bc21a2682c9c99

4316a560734e68303860899d0f2b07a9ef4618647da2e8ad38bab70a4e532f88

cd06ab37c8e4d6e4264f2ac0949ab7694eb5cc11925853a50c33b13b012eca6f

e90f31c41a64ce85abfa284126e63b693088934fd83ef8fea13724810f394efa

cc03f53a7a85d9b1b28a6422556b295cb9b00e93b5afc96559140f32f96305e9

1cf31091a0e6d9dade4675497593d04815d7ba22b0b018d06358211f3429ab49

dccc95c28bbc1f049c06e7b3a9866a920c4c4081e3176b26fc6aea2cb59daed7

31038f33d8d757c19050d41e62036a85026bbe99d37fd806fdde7f261fd2651b

3fff146c3e50a7ddc7e446ae51742c59c3d3277931f3c511d9651497e4ab14a7

9dba2cef0e28a24b59eda107633528cd83257f033a5d4330cf3302943b3e07c2

9274f0391add4a1ac7c90942628a9fd80a9fca3d11aabb74b4e385eee4f66354

bfb4f44e8dd9c0a708df89f0f114b523c446baaee19205d62ad99bb53a8b5935

1ed522e66e9ddcc97ded3e008c014500e3c3e22a1db995199baa52a7dc93845b

f51880293a2bd24da4182965ad5c9b4936eab23a20ed0b4264b75d6c3a3eeac5

009827ab2624370ded2cb8240ca2fe82af36e3a94cff1f8a2eac574b4b928c4e

3984a025b7fb7c5ada86da0b4fa32bef88eb2a01fb337a7f73619cb716c859ab

cfb50c7fe40334c1f52759a08289e36be0ada9056e3dcb22898efd8187b6464d

242e8e1ff2608f5c9fa80b89b31f605bb9432b15dace2eba961605b245d577d5

c272d218f34bc65e6753e7ece1fe6e56799782678a66a5084e71bbb8690fe724

38cbccea7c9f3032a8348e54bb94871b26279a7cca64f5b79c3fa54c240960d2

92eba1a137918f99fbe15651568b8b76ad5f59788b1bce9076bfb33bbc3484de

92657c3a108bbedc6f05b4af0a174e99a58e51e69c15c707d9c9cc63cdf1b4ea

44dabadbf099bdb28fdc4d86cebe53c00085c9c2ad52df4d4774320409e7358b

bf3b35d225b2ec555ad06eb1dd0af464bb48596bebb0b2543eaf9e060f0fb1b9

415d70be7a2e3ae8fd2babc929c3110fce7ce66d23ec32c473c6aab73c5c00f8

a45ff2f03d88abfb949b8c8f40fa08fa7e72d22e756716f8dc18e2f34376b722

0901d9b4ad36a264904bb41b555b32c87790e7861969fa7495da7892aef8f67c

2cabb8e10c5ad57788d99f5218a1248e0ada9a5bdbd5f976d9523b2e4a47aacf

f61403729e3f4e212411db486a537eabca2d0b84be21b789cddca4fc3aa85923

22d57a535c226b514da92d0dcc902f0029414c5f2b1141bc14ac9a057c791414

3366f47822b72445aa06d2e2c455dd4816e5df2f83e7bd03f21e77b1cb2b8948

a9aae05b05f42bd3d1f9d7894a68db976977573741ddcdf6f388b7d685765564

4f91fdf024b54ad650c13f7ffe1a7f3eb6cad66eb457e8a7fe494cf9bdb6f42a

5049de4c58ea923723389e4d732f1c134dc38582971f4872593e1153db945078

bb8a127d9f8eb5c598617682a4ab29ee023ae8f40428c6076b0b493116eca8bb

d12196087135b9383a4e9820d27625c059511c4776593a4d2eb83409a96af3a5

fab5abe774e1af199da4b85df87077e2e8f66c6f00f083b9074fd2186e455bfb

77459352c074012c1e0d010e2b8792d08f36ca6f7bf4882b2db2af4aa1944e5f

65db46d1f48c9c15fe97147ee918fae626225c5603293b72da8e484a9c91123f

d3e1060a003f6a8073dea4f6c976f552372cd4ab9251953c0932be22c6f6605f

9282f4b1fa8ecf1273ddf3291abcc8fc073b2e99a00f70985077197112a46c4c

b87ead56ff364a052619c373b8c06d2150561196f87e584590f67a341ba78abc

fed5ea7840461984fa40784d84ed1a0961cbf48b03d8b79c522286bf6e220922

Hostname

Value
api.hotmailbox.me
getcode.hotmailbox.me
api.dongvanfb.net

External References

- https://otx.alienvault.com/pulse/64c9624677d427f6f94ef691
- https://unit42.paloaltonetworks.com/nodestealer-2-targets-facebook-business/