Jul 27 2023

NETMANAGEIT

Intelligence Report

Beyond File Search: A Novel Method for Exploiting the "search-ms" URI Protocol Handler

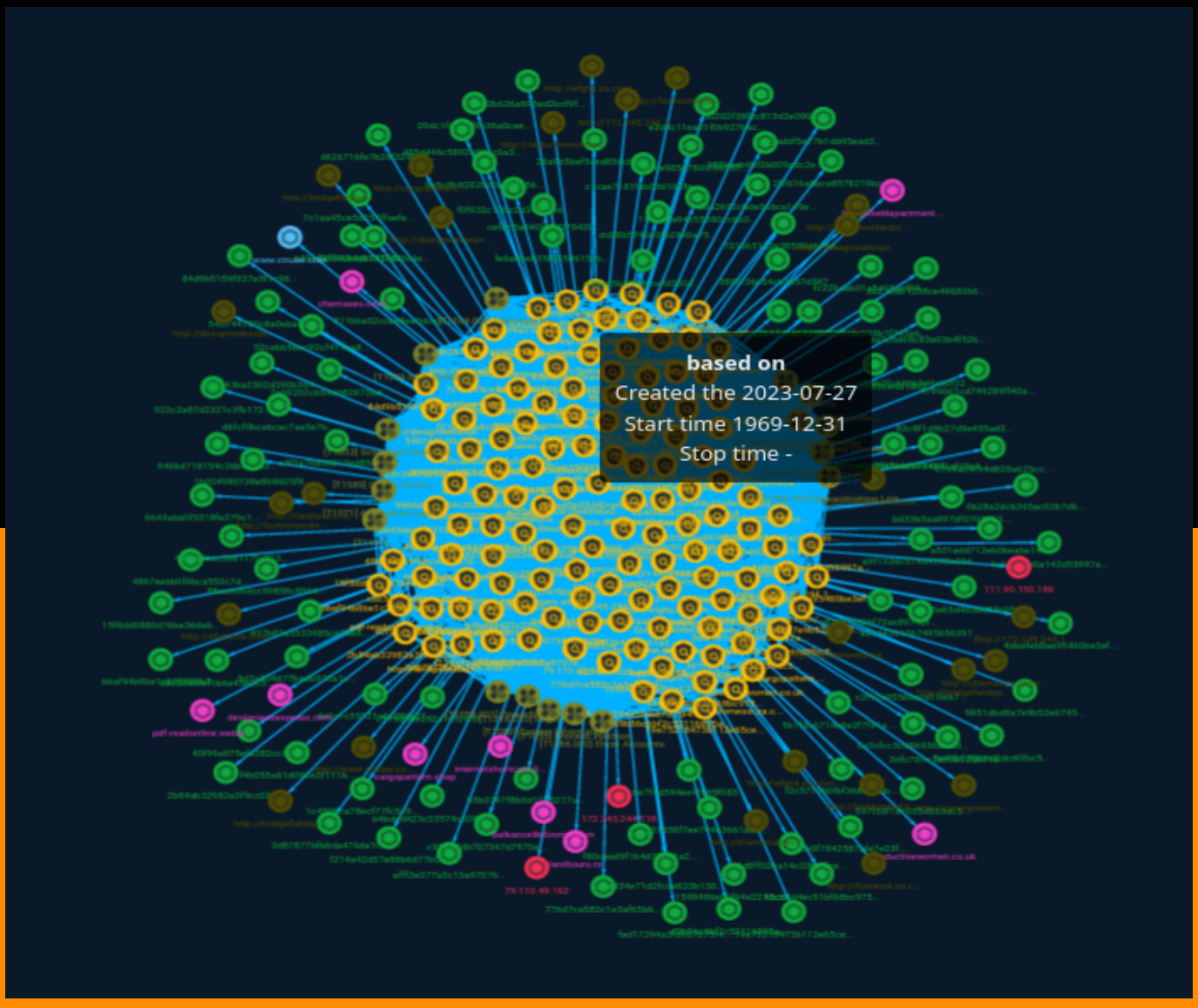

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Researchers have uncovered a novel attack technique leveraging the “search-ms” URI protocol handler

Confidence

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

15 / 100

Indicator

Name

47097f706f72ac8979bfd846d779f3c520f47241b83563dbbcf0e4df94805a21

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '47097f706f72ac8979bfd846d779f3c520f47241b83563dbbcf0e4df94805a21']

Name

http://designwebexpress.com/Invoice_4221.html

Pattern Type

stix

Pattern

[url:value = 'http://designwebexpress.com/Invoice_4221.html']

Name

811bba52ccee8ee0dce9f96f402a7c33427622276028bfb5e9d661130fa0e3fc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '811bba52ccee8ee0dce9f96f402a7c33427622276028bfb5e9d661130fa0e3fc']

Name

a214430106749565639 1aaa937e47b27706d7db8ea7fd12412e7796196f91fe8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a214430106749565639 1aaa937e47b27706d7db8ea7fd12412e7796196f91fe8']

Name

cef2c8a040fe4d27843f601b76c13169fcc0f1d5c7f20e71e830967dffa89baa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cef2c8a040fe4d27843f601b76c13169fcc0f1d5c7f20e71e830967dffa89baa']

Name

c519d06e252a1cf04f8fb38f20c76a39363e51bf31864bac638f662a698b244e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c519d06e252a1cf04f8fb38f20c76a39363e51bf31864bac638f662a698b244e']

Name

6e7f4d594ee4f5d5f08321ede7c32e51d72acbd0700f37c621f9145d8c86309d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6e7f4d594ee4f5d5f08321ede7c32e51d72acbd0700f37c621f9145d8c86309d']

Name

fe6a8beb35f9550615cb3190b1b207bbe11c23a16248644c09ba0d007822c132

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fe6a8beb35f9550615cb3190b1b207bbe11c23a16248644c09ba0d007822c132']

Name

b26144c6e42601f1f1be09ece7c7fcb127637db3b953065648d1b1f371da7e8a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b26144c6e42601f1f1be09ece7c7fcb127637db3b953065648d1b1f371da7e8a']

Name

http://landtours.rs/BB/index.html

Pattern Type

stix

Pattern

[url:value = 'http://landtours.rs/BB/index.html']

Name

5be46ac9b6fd4d07db8710315b6fa8597464756005235472cf1562a0398921bf

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '5be46ac9b6fd4d07db8710315b6fa8597464756005235472cf1562a0398921bf']
Name
5b7fdc6714e6e2f7f91a1b895204d630561f1f1431636875f6a270f3db06a55b
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '5b7fdc6714e6e2f7f91a1b895204d630561f1f1431636875f6a270f3db06a55b']
Name
437b82a5533485ce26a8b983cffa787e629120422e49b28a2608337158c883fc
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '437b82a5533485ce26a8b983cffa787e629120422e49b28a2608337158c883fc']

Name
5c31f5cfa003b1f745eb5019d76aa43f06a7d46c6403eeb2deabd44ee1a1a97a
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '5c31f5cfa003b1f745eb5019d76aa43f06a7d46c6403eeb2deabd44ee1a1a97a']
Name
internetshortcuts.link
Pattern Type
stix
Pattern
[domain-name:value = 'internetshortcuts.link']
Name
a3f5a76a50819ed856e22e690989f4e0b1bf6c88bab3d989868700cafa26c4b7
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = 'a3f5a76a50819ed856e22e690989f4e0b1bf6c88bab3d989868700cafa26c4b7']

Name

http://efghij.za.com/Invoice_898277.html

Pattern Type

stix

Pattern

[url:value = 'http://efghij.za.com/Invoice_898277.html']

Name

http://fashionstylist.za.com/Invoice_0020317.html

Pattern Type

stix

Pattern

[url:value = 'http://fashionstylist.za.com/Invoice_0020317.html']

Name

388f736c54cb1e57d5877d35da5ecdcf46b88ad2e44ca5d2ecffa0dcf0e1b8d9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '388f736c54cb1e57d5877d35da5ecdcf46b88ad2e44ca5d2ecffa0dcf0e1b8d9']

Name

31038f7ee74463661addd7378b26076898e20d19e69f672f829af07b8ff816a9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '31038f7ee74463661addd7378b26076898e20d19e69f672f829af07b8ff816a9']

Name

chemaxes.com

Pattern Type

stix

Pattern

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

Name

http://designwebexpress.com/Invoice_6211.html

Pattern Type

stix

Pattern

[url:value = 'http://designwebexpress.com/Invoice_6211.html']

Name

5d7e304d77bedb970a1c9a5b3aa6f5c4252825c9c0a94fe60ec56a0f1b2664b5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5d7e304d77bedb970a1c9a5b3aa6f5c4252825c9c0a94fe60ec56a0f1b2664b5']

Name

dd28b5740c0fb2890a7579d75c65cf09a36ba5d9fc5df5c9581771e40420f35b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dd28b5740c0fb2890a7579d75c65cf09a36ba5d9fc5df5c9581771e40420f35b']

Name

d99ed5b55440cefd33047490937b9b729f6b7a93bcb7d3877d07391fbec2a13a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd99ed5b55440cefd33047490937b9b729f6b7a93bcb7d3877d07391fbec2a13a']

Name

d6fcf0bcebcac7aa5e7b21b189dbd89f314f79871b770911a7d7b780207fb83d

Description

ConventionEngine_Term_Desktop

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd6fcf0bcebcac7aa5e7b21b189dbd89f314f79871b770911a7d7b780207fb83d']

Name

964f9489714241afd3c422eb164fe96dfe72c12ab1d3f58613694f73bc7e839e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '964f9489714241afd3c422eb164fe96dfe72c12ab1d3f58613694f73bc7e839e']

Name

de0a1c35121a6e08bf07267aca78fb8fe9c46ead95ed1acebfb3a77b72e869b8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'de0a1c35121a6e08bf07267aca78fb8fe9c46ead95ed1acebfb3a77b72e869b8']

Name

http://designwebexpress.com/Invoice.html

Pattern Type

stix

Pattern

[url:value = 'http://designwebexpress.com/Invoice.html']

Name

c2f10c9556eecd1ffe67e763190c630262dfdb593245357283b02df2b4d696de

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c2f10c9556eecd1ffe67e763190c630262dfdb593245357283b02df2b4d696de']

Name

http://efghij.za.com/Invoice_662243.html

Pattern Type

stix

Pattern

[url:value = 'http://efghij.za.com/Invoice_662243.html']

Name

7316651d2e38599d6e46a1ac52dff4eee7ae16f22e87cd244efb9a6ed748f358

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7316651d2e38599d6e46a1ac52dff4eee7ae16f22e87cd244efb9a6ed748f358']

Name

balkancelikdovme.com

Pattern Type

stix

Pattern

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

Name

7a69202cb54dd828736d63dae6b948fcef815658859f1d10220727d242eb6fd4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7a69202cb54dd828736d63dae6b948fcef815658859f1d10220727d242eb6fd4']

Name

72a79351d602ce6a1d0267bcd6d57c17cd8adc44c78197138cc3be5f4100b5b6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '72a79351d602ce6a1d0267bcd6d57c17cd8adc44c78197138cc3be5f4100b5b6']

Name

b5b3747f8b0d11b5217a7a39c2420fb5a0c1044c82cbe9cba596dacf521a1a01

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b5b3747f8b0d11b5217a7a39c2420fb5a0c1044c82cbe9cba596dacf521a1a01']

Name

19cd76a94c55380cc6b053b05eb8896fa1329f03d65a7937225196c356bb0c6a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '19cd76a94c55380cc6b053b05eb8896fa1329f03d65a7937225196c356bb0c6a']

Name

http://fashionstylist.za.com/Invoice_82637.html

Pattern Type

stix

Pattern

[url:value = 'http://fashionstylist.za.com/Invoice_82637.html']

Name

1b004980738e868605f88d6b764f72d0d6c50fddea3a7bdf4508ff3057501562

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1b004980738e868605f88d6b764f72d0d6c50fddea3a7bdf4508ff3057501562']

Name

ea2c8d68c83a93b4f526d2bdb25aa20920b43b7985b9bb8a8109912b74adf1df

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ea2c8d68c83a93b4f526d2bdb25aa20920b43b7985b9bb8a8109912b74adf1df']

Name

ed34e71d2fcae823b130a7e54a4404c15e34060e45c73654d16f34c799f91509

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ed34e71d2fcae823b130a7e54a4404c15e34060e45c73654d16f34c799f91509']

Name

9b5c8b82828c0aa94956671b3b9f2a6ec4f34a642d621938e86bffe9ce8b1acb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9b5c8b82828c0aa94956671b3b9f2a6ec4f34a642d621938e86bffe9ce8b1acb']

Name

f493a5a65d460bd53b05fde1ee5562db08e52c34989321a9bd09ecc5dc3f4d6d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f493a5a65d460bd53b05fde1ee5562db08e52c34989321a9bd09ecc5dc3f4d6d']

Name

f4b055a61d096e2f111bdaf7b171719188c02d74fa946dabdae0bbc72671d2db

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f4b055a61d096e2f111bdaf7b171719188c02d74fa946dabdae0bbc72671d2db']

Name

http://designwebexpress.com/Invoice_3221.html

Pattern Type

stix

Pattern

[url:value = 'http://designwebexpress.com/Invoice_3221.html']

Name

http://internetshortcuts.link/VdXiIRQo/payload.iso

Pattern Type

stix

Pattern

[url:value = 'http://internetshortcuts.link/VdXiIRQo/payload.iso']

Name

9466d718154c26b8d003b99faff2a8868e2a26788e2946b68245e6dfe54da610

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9466d718154c26b8d003b99faff2a8868e2a26788e2946b68245e6dfe54da610']

Name

a9f132dc514d4598a29d004a38e71d3a389e43b46149a36314d2f55e20e1ebb6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a9f132dc514d4598a29d004a38e71d3a389e43b46149a36314d2f55e20e1ebb6']

Name

landtours.rs

Pattern Type

stix

Pattern

[domain-name:value = 'landtours.rs']

Name

f0f932c136c2d34b0f9da7a83e1a2f87063ea2bce48d3a9af004189bf49d98d9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f0f932c136c2d34b0f9da7a83e1a2f87063ea2bce48d3a9af004189bf49d98d9']

Name

ce3cfcc3cd86936aff5d43de6f0298cc8f0c5cfd7675d951dd23de53c3b8b154

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ce3cfcc3cd86936aff5d43de6f0298cc8f0c5cfd7675d951dd23de53c3b8b154']

Name

c8c5386fef1b6e45e02323f3a45b1e73b5d5be60a8a5f5ebe3b95bce77b03167

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c8c5386fef1b6e45e02323f3a45b1e73b5d5be60a8a5f5ebe3b95bce77b03167']

Name

fc226deb01a8d15acf98fd6e9daa3d95b73687f46e9029523fd7e8fe8ad5fb83

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fc226deb01a8d15acf98fd6e9daa3d95b73687f46e9029523fd7e8fe8ad5fb83']

Name

172.245.244.118

Description

ISP: ColoCrossing **OS:** None ---------- Hostnames: - 172-245-244-118-host.colocrossing.com ---------- Domains: - colocrossing.com ---------- Services: **79:** ``` ``` ---------- **139:** ``` \x83\x00\x00\x01\x8f ``` ---------- **445:** ``` SMB Status: Authentication: enabled SMB Version: 2 Capabilities: raw-mode ``` ---------- **3306:** ``` MariaDB: Error Message: Host '224.219.109.218' is not allowed to connect to this MariaDB server Error Code: 1130 ``` ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x03\x00\x08\x00\x02\x00\x00\x00 ; Administrator SES ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Tue, 18 Jul 2023 01:58:56 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2019 (version 1809) OS Build: 10.0.17763 Target Name: HBHJJDOL-43067 NetBIOS Domain Name: HBHJJDOL-43067 NetBIOS Computer Name: HBHJJDOL-43067 DNS Domain Name: hbhjjdol-43067 FQDN: hbhjjdol-43067 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.245.244.118']

Name

b8998dff4684d815538b1c57c3bba0f9914f8436fde99ddedc1e9b1e658dabcb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b8998dff4684d815538b1c57c3bba0f9914f8436fde99ddedc1e9b1e658dabcb']

Name

http://chemaxes.com/Invoice-Payment.html

Pattern Type

stix

Pattern

[url:value = 'http://chemaxes.com/Invoice-Payment.html']

Name

http://bridgefieldapartmentsapp.ie/EX/index.html

Pattern Type

stix

Pattern

[url:value = 'http://bridgefieldapartmentsapp.ie/EX/index.html']

Name

2da9b5bef5ced856c6367e990dc2bf0424ad2c551016c3f1d2068b9284310e53

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2da9b5bef5ced856c6367e990dc2bf0424ad2c551016c3f1d2068b9284310e53']

Name

f2c577360fbf36859eeb194970f734810f2954493e5428d71add4edb6c11c4f1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f2c577360fbf36859eeb194970f734810f2954493e5428d71add4edb6c11c4f1']

Name
540744100c8a0eba6c4d24fcee5df40a274ecd51f33c41e11dbe482bd32d271d
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '540744100c8a0eba6c4d24fcee5df40a274ecd51f33c41e11dbe482bd32d271d']
Name
http://designwebexpress.com/Invoice_5221.html
Pattern Type
stix
Pattern
[url:value = 'http://designwebexpress.com/Invoice_5221.html']
Name
f214a42d57e88b6d77b036934cf93fb9c9126335925bdafc9bb8a326abe2d652
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = 'f214a42d57e88b6d77b036934cf93fb9c9126335925bdafc9bb8a326abe2d652']

Name

485d446c5892b931c0a3a238dca84bebb787052c877deb73f02ae5ee5632de9d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '485d446c5892b931c0a3a238dca84bebb787052c877deb73f02ae5ee5632de9d']

Name

901dd6b7fb5aae90840191eb5e0b8e2578503feaef93fd58b99a3314a2008b4b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '901dd6b7fb5aae90840191eb5e0b8e2578503feaef93fd58b99a3314a2008b4b']

Name

88aeb09dcc59858c9969b7ae1e0e2b58f0aa90b2d27a5edfe9cd82e602ed5952

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '88aeb09dcc59858c9969b7ae1e0e2b58f0aa90b2d27a5edfe9cd82e602ed5952']

Name

98ab2fc44063d4e00f221e502419d9cca598fafb9e1e00352149327267604bc1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '98ab2fc44063d4e00f221e502419d9cca598fafb9e1e00352149327267604bc1']

Name

f80caed9f1b4d71e61a2869c240206f55c44fb9075d4da283df0bcedf7a11d3a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f80caed9f1b4d71e61a2869c240206f55c44fb9075d4da283df0bcedf7a11d3a']

Name

52cebb58ec92cf411ea8482502d8aea3580ded02edc1482609283e0dff541dec

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '52cebb58ec92cf411ea8482502d8aea3580ded02edc1482609283e0dff541dec']

Name

a531edd712eb0beabe14cb4e9ff91dc7635b743e71b6fdc20ec4c0247eccff62

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a531edd712eb0beabe14cb4e9ff91dc7635b743e71b6fdc20ec4c0247eccff62']

Name

cargopattern.shop

Pattern Type

stix

Pattern

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

Name

e3d4c11ea01f0b927bac052aa01e246cd2890445d848a7abe4b03882cccaaaf7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e3d4c11ea01f0b927bac052aa01e246cd2890445d848a7abe4b03882cccaaaf7']

Name

seductivewomen.co.uk

Pattern Type

stix

Pattern

[domain-name:value = 'seductivewomen.co.uk']

Name

904343ba2502d390b36403181e77192a62f31e98c87eb91906fbae27019b4c0d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '904343ba2502d390b36403181e77192a62f31e98c87eb91906fbae27019b4c0d']

Name

56a2692cbde566ca149ef196f9bf4f843839f36ebfdb8acd47acaf2cd01703e9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '56a2692cbde566ca149ef196f9bf4f843839f36ebfdb8acd47acaf2cd01703e9']

Name

1598486e69f94e221dcbd02b10bb33352baf5886db9c06475470159ab16eadbd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1598486e69f94e221dcbd02b10bb33352baf5886db9c06475470159ab16eadbd']

Name

http://cargopattern.shop/page.html

Pattern Type

stix

Pattern

[url:value = 'http://cargopattern.shop/page.html']

Name

http://172.245.244.118/home.html

Pattern Type

stix

Pattern

[url:value = 'http://172.245.244.118/home.html']

Name

pdf-readonline.website

Pattern Type

stix

Pattern

[domain-name:value = 'pdf-readonline.website']

Name

c7bdce98567809f96907d5a005ae7ff8295c63b9d93aa2a9846f903d688fd657

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c7bdce98567809f96907d5a005ae7ff8295c63b9d93aa2a9846f903d688fd657']

Name

597f58f1ec035d553dc5f5e9e0d0d0ed656a2488f5f93c30bf528278b3d615a1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '597f58f1ec035d553dc5f5e9e0d0d0ed656a2488f5f93c30bf528278b3d615a1']

Name

http://designwebexpress.com/Invoice_3211.html

Pattern Type

stix

Pattern

[url:value = 'http://designwebexpress.com/Invoice_3211.html']

Name

bd33b3aa897df0702913dbecd5ad2f7e63df11f4c2a7e461dad7f89abe218a45

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bd33b3aa897df0702913dbecd5ad2f7e63df11f4c2a7e461dad7f89abe218a45']

Name

b4bded423c23574c5080f449d7c92c95b7aa480fedb756568d7280db3ec80cf0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b4bded423c23574c5080f449d7c92c95b7aa480fedb756568d7280db3ec80cf0']

Name

http://172.245.244.118/Quote.html

Pattern Type

stix

Pattern

[url:value = 'http://172.245.244.118/Quote.html']

Name

http://bridgefieldapartmentsapp.ie/EX

Pattern Type

stix

Pattern

[url:value = 'http://bridgefieldapartmentsapp.ie/EX']

Name

designwebexpress.com

Pattern Type

stix

Pattern

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

Name

c1cae7181fab03d16c8e10dbe0993319dca6597e2a2f28ba07014d64f996a1fa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c1cae7181fab03d16c8e10dbe0993319dca6597e2a2f28ba07014d64f996a1fa']

Name

fad17294a3fd687d75f49040c837af39ca2bb9ea84e022aa750e81ddc4cd1583

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fad17294a3fd687d75f49040c837af39ca2bb9ea84e022aa750e81ddc4cd1583']

Name

http://bridgefieldapartmentsapp.ie/home.html

Pattern Type

stix

Pattern

[url:value = 'http://bridgefieldapartmentsapp.ie/home.html']

Name

111.90.150.186

Description

Malicious SSL connections

Pattern Type

stix

Pattern

[ipv4-addr:value = '111.90.150.186']

Name

1c450bca78ecf77fc5c9b03ced93f5410f03804fcbf17c9c5e584770eec03403

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1c450bca78ecf77fc5c9b03ced93f5410f03804fcbf17c9c5e584770eec03403']

Name

http://fashionstylist.za.com/Invoice_898277.html

Pattern Type

stix

Pattern

[url:value = 'http://fashionstylist.za.com/Invoice_898277.html']

Name

http://lfomessi.za.com/home.html

Pattern Type

stix

Pattern

[url:value = 'http://lfomessi.za.com/home.html']

Name

923c2a87d2321c3fb172d8998574f4d2695e6c8f5f5d5d568c26aefb5fe2d198

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '923c2a87d2321c3fb172d8998574f4d2695e6c8f5f5d5d568c26aefb5fe2d198']

Name

41960d1cd749289ff40a1c92970706ead76f73fb3b61276a2f34a7ac38f989c6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '41960d1cd749289ff40a1c92970706ead76f73fb3b61276a2f34a7ac38f989c6']

Name

79.110.49.162

Description

CC=US ASN=AS46308 AS46308

Pattern Type

stix

Pattern

[ipv4-addr:value = '79.110.49.162']

Name

7c1aa45ce5d254ffaefea8396128a55318bf937fbb3400b327f5dc528134730d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7c1aa45ce5d254ffaefea8396128a55318bf937fbb3400b327f5dc528134730d']

Name

5a47b18066d8dcd0fbc524f529002cf0a270d8394de928e8426fa06959a82704

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5a47b18066d8dcd0fbc524f529002cf0a270d8394de928e8426fa06959a82704']

Name

40f99a875efa382cc0cae003c7b3b0519a7fcaa10a95989103b1e3e2bb20832a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '40f99a875efa382cc0cae003c7b3b0519a7fcaa10a95989103b1e3e2bb20832a']

Name

188baeb6bf2b009adc2efb648b068be71d5b55d1d11e000c473b429f3dda4a86

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '188baeb6bf2b009adc2efb648b068be71d5b55d1d11e000c473b429f3dda4a86']

Name

d9b56c6bf2c52116855a79e0008b6cfd7baef20e5af06ba142f774c8bf3b7401

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'd9b56c6bf2c52116855a79e0008b6cfd7baef20e5af06ba142f774c8bf3b7401']
Name
f21010eb8c0f2fd23c4ee941a394853597bfb90527f43f3c61bf6ce004b7f367
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f21010eb8c0f2fd23c4ee941a394853597bfb90527f43f3c61bf6ce004b7f367']
Name
0b28a2dcb365ac02b7d6c3928d5a1cfdd5ed669206eb176ab65ebb6084b58545
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '0b28a2dcb365ac02b7d6c3928d5a1cfdd5ed669206eb176ab65ebb6084b58545']

Name
http://www.cttuae.com/ems/page.html
Pattern Type
stix
Pattern
[url:value = 'http://www.cttuae.com/ems/page.html']
Name
http://efghij.za.com/Invoice_72638.html
Pattern Type
stix
Pattern
[url:value = 'http://efghij.za.com/Invoice_72638.html']
Name
3dfc781c1b656925b91a22b48b85b6ce2bf8f9cb9c1288be6ec3b760f6f7402d
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '3dfc781c1b656925b91a22b48b85b6ce2bf8f9cb9c1288be6ec3b760f6f7402d']

Name

4f8ba8eec38e117fa323bc24074993a7f1cc31c5ce112f9c6696c724628f53dc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4f8ba8eec38e117fa323bc24074993a7f1cc31c5ce112f9c6696c724628f53dc']

Name

bridgefieldapartmentsapp.ie

Pattern Type

stix

Pattern

[domain-name:value = 'bridgefieldapartmentsapp.ie']

Name

c91527db707347d7970e8197c8a11446c40d945adfb47eb68f666b02f56d8c22

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c91527db707347d7970e8197c8a11446c40d945adfb47eb68f666b02f56d8c22']

Name

d626716fe7b26f3299438cca864216c3dacadaba145ce2decc2eededb3d4bf38

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd626716fe7b26f3299438cca864216c3dacadaba145ce2decc2eededb3d4bf38']

Name

4daafeb8ae95460be3ef93577983db33cca28ecb67fff9b958a7f71ae17504bf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4daafeb8ae95460be3ef93577983db33cca28ecb67fff9b958a7f71ae17504bf']

Name

2b84ab32982a3f9cc03dd4f020751dcaaf8ad5ef32d0e7975a0b1d17045ee07e

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '2b84ab32982a3f9cc03dd4f020751dcaaf8ad5ef32d0e7975a0b1d17045ee07e']
Name
90202f38f8c813d2e09063432542573e3e7792b9111f2c56d12a451c9dd25b48
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '90202f38f8c813d2e09063432542573e3e7792b9111f2c56d12a451c9dd25b48']
Name
d0b0f7842587afe7e23fc0218fd0a391996e72b1a804a6bfc33e97d9aecb6b2e
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'd0b0f7842587afe7e23fc0218fd0a391996e72b1a804a6bfc33e97d9aecb6b2e']

Name

6643aba0f5318fe279c1cae871ec32540b65265a68fb98aedae5a6fc0707b3c7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6643aba0f5318fe279c1cae871ec32540b65265a68fb98aedae5a6fc0707b3c7']

Name

0764a24f94d829a625cca37f92863a84553db77469b68eadf875e73fcf0d3036

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0764a24f94d829a625cca37f92863a84553db77469b68eadf875e73fcf0d3036']

Name

afff3e377a5c13a9707680ed926c15718eeb2d3b4d9dcf0993019b3766fc16aa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'afff3e377a5c13a9707680ed926c15718eeb2d3b4d9dcf0993019b3766fc16aa']

Name

8a22b626a893ed2bcf9f63ffe5dcb2198f7d5dc991b5cec434e8b0f050ebbfeb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8a22b626a893ed2bcf9f63ffe5dcb2198f7d5dc991b5cec434e8b0f050ebbfeb']

Name

9851dbd8a7e9b52e6745b7fb2ff854ce573d4a56be0cd0b700a30eca15e331e5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9851dbd8a7e9b52e6745b7fb2ff854ce573d4a56be0cd0b700a30eca15e331e5']

Name

15f8dd0880d76be36de65dd8412d7171d2cc00c35d3461452dfdae2f657aaf31

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '15f8dd0880d76be36de65dd8412d7171d2cc00c35d3461452dfdae2f657aaf31']

Name

25f616a8bce8578219bc884a64d1a3bc60ec87f07cdff8da3c386ae5b49445a9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '25f616a8bce8578219bc884a64d1a3bc60ec87f07cdff8da3c386ae5b49445a9']

Name

19e75218473b112e65cec4c2c5afd0c3cc6b4fb8f847127018e0815bd64b6480

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '19e75218473b112e65cec4c2c5afd0c3cc6b4fb8f847127018e0815bd64b6480']

Name

www.cttuae.com

Pattern Type

stix

Pattern

[hostname:value = 'www.cttuae.com']

Name

83c8f1d9b27d9e455ad2602b1005f6837ac6040cf61acc3124f7179fd5894d27

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '83c8f1d9b27d9e455ad2602b1005f6837ac6040cf61acc3124f7179fd5894d27']

Name

3d87877bfb6da476da1f51410416bef22cc216d941c79268f6de17d8dde1c0b8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3d87877bfb6da476da1f51410416bef22cc216d941c79268f6de17d8dde1c0b8']

Name

http://seductivewomen.co.uk/invoice44201.html

Pattern Type

stix

Pattern

[url:value = 'http://seductivewomen.co.uk/invoice44201.html']

Name

45cd3d4ec91bf68bc975d99d90612e459aeb4a0f31321a440d7d41fcdea798f3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '45cd3d4ec91bf68bc975d99d90612e459aeb4a0f31321a440d7d41fcdea798f3']

Name

4867eebb0f6bca553c7d50e878e3cb19f7471c1c89cbd85f49b6d50f7a44e779

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4867eebb0f6bca553c7d50e878e3cb19f7471c1c89cbd85f49b6d50f7a44e779']

Name

db27ba01238ce49683b68bc9c2b925caac6008ae178d14c0dce4cce161bde746

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'db27ba01238ce49683b68bc9c2b925caac6008ae178d14c0dce4cce161bde746']

Name

776d7ce582c1e3af65b60073986c78da394cbbab1bf6b83a6c0d736c58d33758

Description

invalid_trailer_structure

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '776d7ce582c1e3af65b60073986c78da394cbbab1bf6b83a6c0d736c58d33758']

Name

09dc1f4a21f9b36a0ceeef791d2bf3463299d172712943139ace33d476d7d7c2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '09dc1f4a21f9b36a0ceeef791d2bf3463299d172712943139ace33d476d7d7c2']

Name

http://cargopattern.shop/home/home.html

Pattern Type

stix

Pattern

[url:value = 'http://cargopattern.shop/home/home.html']

Name

bbaf94b8be1c355328e5db962577b26ae73f9c3fbf81e6892019bffbf0513698

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bbaf94b8be1c355328e5db962577b26ae73f9c3fbf81e6892019bffbf0513698']

Name

58addf5e77b1dd45ead377c2a8d52b12a0db4edbc607f17b650c27428e24bbfd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '58addf5e77b1dd45ead377c2a8d52b12a0db4edbc607f17b650c27428e24bbfd']

Name

4d8ff026a14c03fc7fce40fe5bb9c287320f66102693e74e40a48247999f4a0a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4d8ff026a14c03fc7fce40fe5bb9c287320f66102693e74e40a48247999f4a0a']

Name

84d9b5159f937e5f1c98e221d23546fb38775097e983fb660144b4d4a8955582

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '84d9b5159f937e5f1c98e221d23546fb38775097e983fb660144b4d4a8955582']

Name

4c1cb32e0a142d55997a55bfc239e4b5b31a6e021014d023d5ff9787948490df

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4c1cb32e0a142d55997a55bfc239e4b5b31a6e021014d023d5ff9787948490df']

Attack-Pattern

Name
Email Accounts
ID
T1586.002
Description
Adversaries may compromise email accounts that can be used during targeting. Adversaries can use compromised email accounts to further their operations, such as leveraging them to conduct [Phishing for Information](https://attack.mitre.org/techniques/T1598), [Phishing](https://attack.mitre.org/techniques/T1566), or large-scale spam email campaigns. Utilizing an existing persona with a compromised email account may engender a level of trust in a potential victim if they have a relationship with, or knowledge of, the compromised persona. Compromised email accounts can also be used in the acquisition of infrastructure (ex: [Domains](https://attack.mitre.org/techniques/T1583/001)). A variety of methods exist for compromising email accounts, such as gathering credentials via [Phishing for Information](https://attack.mitre.org/techniques/T1598), purchasing credentials from third-party sites, brute forcing credentials (ex: password reuse from breach credential dumps), or paying employees, suppliers or business partners for access to credentials.(Citation: AnonHBGary)(Citation: Microsoft DEV-0537) Prior to compromising email accounts, adversaries may conduct Reconnaissance to inform decisions about which accounts to compromise to further their operation. Adversaries may target compromising well-known email accounts or domains from which malicious spam or [Phishing](https://attack.mitre.org/techniques/T1566) emails may evade reputation-based email filtering rules. Adversaries can use a compromised email account to hijack existing email threads with targets of interest.

Name

Gather Victim Identity Information

ID

T1589

Description

Adversaries may gather information about the victim's identity that can be used during targeting. Information about identities may include a variety of details, including personal data (ex: employee names, email addresses, etc.) as well as sensitive details such as credentials. Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about users could also be enumerated via other active means (i.e. [Active Scanning](https://attack.mitre.org/techniques/T1595)) such as probing and analyzing responses from authentication services that may reveal valid usernames in a system. (Citation: GrimBlog UsernameEnum) Information about victims may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: OPM Leak)(Citation: Register Deloitte)(Citation: Register Uber)(Citation: Detectify Slack Tokens)(Citation: Forbes GitHub Creds)(Citation: GitHub truffleHog)(Citation: GitHub Gitrob)(Citation: CNET Leaks) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566) or [Valid Accounts](https://attack.mitre.org/techniques/T1078)).

Name

Hidden Window

ID

T1564.003

Description

Adversaries may use hidden windows to conceal malicious activity from the plain sight of users. In some cases, windows that would typically be displayed when an application carries out an operation can be hidden. This may be utilized by system administrators to avoid disrupting user work environments when carrying out administrative tasks. On Windows, there are a variety of features in scripting languages in Windows, such as [PowerShell](https://attack.mitre.org/techniques/T1059/001), Jscript, and [Visual Basic](https://attack.mitre.org/techniques/T1059/005) to make windows hidden. One example of this is `powershell.exe -WindowStyle Hidden`. (Citation: PowerShell About 2019) Similarly, on macOS the configurations for how applications run are listed in property list (plist) files. One of the tags in these files can be `apple.awt.UIElement`, which allows for Java applications to prevent the application's icon from appearing in the Dock. A common use for this is when applications run in the system tray, but don't also want to show up in the Dock. Adversaries may abuse these functionalities to hide otherwise visible windows from users so as not to alert the user to adversary activity on the system.(Citation: Antiquated Mac Malware)

Name

Regsvr32

ID

T1218.010

Description

Adversaries may abuse Regsvr32.exe to proxy execution of malicious code. Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls, including dynamic link libraries (DLLs), on Windows systems. The Regsvr32.exe binary may also be signed by Microsoft. (Citation: Microsoft Regsvr32) Malicious usage of Regsvr32.exe may avoid triggering security tools that may not monitor execution of, and modules loaded by, the regsvr32.exe process because of allowlists or false positives from Windows using regsvr32.exe for normal operations. Regsvr32.exe can also be used to specifically bypass application control using functionality to load COM scriptlets to execute DLLs under user permissions. Since Regsvr32.exe is network and proxy aware, the scripts can be loaded by passing a uniform resource locator (URL) to file on an external Web server as an argument during invocation. This method makes no changes to the Registry as the COM object is not actually registered, only executed. (Citation: LOLBAS Regsvr32)

This variation of the technique is often referred to as a "Squiblydoo" and has been used in campaigns targeting governments. (Citation: Carbon Black Squiblydoo Apr 2016) (Citation: FireEye Regsvr32 Targeting Mongolian Gov) Regsvr32.exe can also be leveraged to register a COM Object used to establish persistence via [Component Object Model Hijacking](https://attack.mitre.org/techniques/T1546/015). (Citation: Carbon Black Squiblydoo Apr 2016)

Name

JavaScript

ID

T1059.007

Description

Adversaries may abuse various implementations of JavaScript for execution. JavaScript (JS) is a platform-independent scripting language (compiled just-in-time at runtime) commonly associated with scripts in webpages, though JS can be executed in runtime environments outside the browser.(Citation: NodeJS) JScript is the Microsoft implementation of the same scripting standard. JScript is interpreted via the Windows Script engine and thus integrated with many components of Windows such as the [Component Object Model](https://attack.mitre.org/techniques/T1559/001) and Internet Explorer HTML Application (HTA) pages.(Citation: JScrip May 2018)(Citation: Microsoft JScript 2007)(Citation: Microsoft Windows Scripts) JavaScript for Automation (JXA) is a macOS scripting language based on JavaScript, included as part of Apple's Open Scripting Architecture (OSA), that was introduced in OSX 10.10. Apple's OSA provides scripting capabilities to control applications, interface with the operating system, and bridge access into the rest of Apple's internal APIs. As of OSX 10.10, OSA only supports two languages, JXA and [AppleScript](https://attack.mitre.org/techniques/T1059/002). Scripts can be executed via the command line utility `osascript`, they can be compiled into applications or script files via `osacompile`, and they can be compiled and executed in memory of other programs by leveraging the OSAKit Framework.(Citation: Apple About Mac Scripting 2016) (Citation: SpecterOps JXA 2020)(Citation: SentinelOne macOS Red Team)(Citation: Red Canary Silver Sparrow Feb2021)(Citation: MDSec macOS JXA and VSCode) Adversaries may abuse various implementations of JavaScript to execute various behaviors. Common uses include hosting malicious scripts on websites as part of a [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) or downloading and executing these script files as secondary payloads. Since these payloads are text-based, it is also very common for

adversaries to obfuscate their content as part of [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027).

Name

Non-Standard Port

ID

T1571

Description

Adversaries may communicate using a protocol and port pairing that are typically not associated. For example, HTTPS over port 8088(Citation: Symantec Elfin Mar 2019) or port 587(Citation: Fortinet Agent Tesla April 2018) as opposed to the traditional port 443. Adversaries may make changes to the standard port used by a protocol to bypass filtering or muddle analysis/parsing of network data. Adversaries may also make changes to victim systems to abuse non-standard ports. For example, Registry keys and other configuration settings can be used to modify protocol and port pairings.(Citation: change_rdp_port_conti)

Name

Virtualization/Sandbox Evasion

ID

T1497

Description

Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned

from [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) during automated discovery to shape follow-on behaviors.(Citation: Deloitte Environment Awareness) Adversaries may use several methods to accomplish [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) such as checking for security monitoring tools (e.g., Sysinternals, Wireshark, etc.) or other system artifacts associated with analysis or virtualization. Adversaries may also check for legitimate user activity to help determine if it is in an analysis environment. Additional methods include use of sleep timers or loops within malware code to avoid operating within a temporary sandbox. (Citation: Unit 42 Pirpi July 2015)

Name

Query Registry

ID

T1012

Description

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. The Registry contains a significant amount of information about the operating system, configuration, software, and security.(Citation: Wikipedia Windows Registry) Information can easily be queried using the [Reg](https://attack.mitre.org/software/S0075) utility, though other means to access the Registry exist. Some of the information may help adversaries to further their operation within a network. Adversaries may use the information from [Query Registry](https://attack.mitre.org/techniques/T1012) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

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

Scheduled Task/Job

ID

T1053

Description

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.(Citation: TechNet Task Scheduler Security) Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process. (Citation: ProofPoint Serpent)

Name

Encrypted Channel

ID

T1573

Description

Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.

Name

PowerShell

ID

T1059.001

Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack) PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying

`System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

Name

Malicious File

ID

T1204.002

Description

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001). Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl. Adversaries may employ various forms of [Masquerading](https://attack.mitre.org/techniques/T1036) and [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to increase the likelihood that a user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying instructions to a user on how to open it.(Citation: Password Protected Word Docs) While [Malicious File](https://attack.mitre.org/techniques/T1204/002) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534).

Name

Spearphishing Link

ID

T1566.002

Description

Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments. Spearphishing may also involve social engineering techniques, such as posing as a trusted source. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging [User Execution](https://attack.mitre.org/techniques/T1204). The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place. Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly. Additionally, adversaries may use seemingly benign links that abuse special characters to mimic legitimate websites (known as an "IDN homograph attack").(Citation: CISA IDN ST05-016) Adversaries may also utilize links to perform consent phishing, typically with OAuth 2.0 request URLs that when accepted by the user provide permissions/access for malicious applications, allowing adversaries to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s.(Citation: Trend Micro Pawn Storm OAuth 2017) These stolen access tokens allow the adversary to perform various actions on behalf of the user via API calls. (Citation: Microsoft OAuth 2.0 Consent Phishing 2021)

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including

those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

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
chemaxes.com
seductivewomen.co.uk
landtours.rs
bridgefieldapartmentsapp.ie
internetshortcuts.link
pdf-readonline.website
cargopattern.shop
designwebexpress.com
balkancelikdovme.com

StixFile

Value
a3f5a76a50819ed856e22e690989f4e0b1bf6c88bab3d989868700cafa26c4b7
597f58f1ec035d553dc5f5e9e0d0d0ed656a2488f5f93c30bf528278b3d615a1
58addf5e77b1dd45ead377c2a8d52b12a0db4edbc607f17b650c27428e24bbfd
5a47b18066d8dcd0fbc524f529002cf0a270d8394de928e8426fa06959a82704
cef2c8a040fe4d27843f601b76c13169fcc0f1d5c7f20e71e830967dffa89baa
7c1aa45ce5d254ffaefea8396128a55318bf937fbb3400b327f5dc528134730d
90202f38f8c813d2e09063432542573e3e7792b9111f2c56d12a451c9dd25b48
09dc1f4a21f9b36a0ceeef791d2bf3463299d172712943139ace33d476d7d7c2
d6fcf0bcebcac7aa5e7b21b189dbd89f314f79871b770911a7d7b780207fb83d
540744100c8a0eba6c4d24fcee5df40a274ecd51f33c41e11dbe482bd32d271d
ce3cfcc3cd86936aff5d43de6f0298cc8f0c5cfd7675d951dd23de53c3b8b154
b8998dff4684d815538b1c57c3bba0f9914f8436fde99ddedc1e9b1e658dabcb
1c450bca78ecf77fc5c9b03ced93f5410f03804fcbf17c9c5e584770eec03403

15f8dd0880d76be36de65dd8412d7171d2cc00c35d3461452dfdae2f657aaf31

f2c577360fbf36859eeb194970f734810f2954493e5428d71add4edb6c11c4f1

afff3e377a5c13a9707680ed926c15718eeb2d3b4d9dcf0993019b3766fc16aa

c1cae7181fab03d16c8e10dbe0993319dca6597e2a2f28ba07014d64f996a1fa

923c2a87d2321c3fb172d8998574f4d2695e6c8f5f5d5d568c26aefb5fe2d198

52cebb58ec92cf411ea8482502d8aea3580ded02edc1482609283e0dff541dec

6643aba0f5318fe279c1cae871ec32540b65265a68fb98aedae5a6fc0707b3c7

5b7fdc6714e6e2f7f91a1b895204d630561f1f1431636875f6a270f3db06a55b

84d9b5159f937e5f1c98e221d23546fb38775097e983fb660144b4d4a8955582

c91527db707347d7970e8197c8a11446c40d945adfb47eb68f666b02f56d8c22

964f9489714241afd3c422eb164fe96dfe72c12ab1d3f58613694f73bc7e839e

437b82a5533485ce26a8b983cffa787e629120422e49b28a2608337158c883fc

e3d4c11ea01f0b927bac052aa01e246cd2890445d848a7abe4b03882cccaaaf7

a9f132dc514d4598a29d004a38e71d3a389e43b46149a36314d2f55e20e1ebb6

c7bdce98567809f96907d5a005ae7ff8295c63b9d93aa2a9846f903d688fd657

8a22b626a893ed2bcf9f63ffe5dcb2198f7d5dc991b5cec434e8b0f050ebbfeb

188baeb6bf2b009adc2efb648b068be71d5b55d1d11e000c473b429f3dda4a86

904343ba2502d390b36403181e77192a62f31e98c87eb91906fbae27019b4c0d

7a69202cb54dd828736d63dae6b948fcef815658859f1d10220727d242eb6fd4

4d8ff026a14c03fc7fce40fe5bb9c287320f66102693e74e40a48247999f4a0a

bbaf94b8be1c355328e5db962577b26ae73f9c3fbf81e6892019bffbf0513698

88aeb09dcc59858c9969b7ae1e0e2b58f0aa90b2d27a5edfe9cd82e602ed5952

d626716fe7b26f3299438cca864216c3dacadaba145ce2decc2eededb3d4bf38

19e75218473b112e65cec4c2c5afd0c3cc6b4fb8f847127018e0815bd64b6480

f214a42d57e88b6d77b036934cf93fb9c9126335925bdafc9bb8a326abe2d652

9851dbd8a7e9b52e6745b7fb2ff854ce573d4a56be0cd0b700a30eca15e331e5

fad17294a3fd687d75f49040c837af39ca2bb9ea84e022aa750e81ddc4cd1583

388f736c54cb1e57d5877d35da5ecdcf46b88ad2e44ca5d2ecffa0dcf0e1b8d9

f493a5a65d460bd53b05fde1ee5562db08e52c34989321a9bd09ecc5dc3f4d6d

bd33b3aa897df0702913dbecd5ad2f7e63df11f4c2a7e461dad7f89abe218a45

fe6a8beb35f9550615cb3190b1b207bbe11c23a16248644c09ba0d007822c132

47097f706f72ac8979bfd846d779f3c520f47241b83563dbbcf0e4df94805a21

2da9b5bef5ced856c6367e990dc2bf0424ad2c551016c3f1d2068b9284310e53

2b84ab32982a3f9cc03dd4f020751dcaaf8ad5ef32d0e7975a0b1d17045ee07e

db27ba01238ce49683b68bc9c2b925caac6008ae178d14c0dce4cce161bde746

d99ed5b55440cefd33047490937b9b729f6b7a93bcb7d3877d07391fbec2a13a

9466d718154c26b8d003b99faff2a8868e2a26788e2946b68245e6dfe54da610

5d7e304d77bedb970a1c9a5b3aa6f5c4252825c9c0a94fe60ec56a0f1b2664b5

56a2692cbde566ca149ef196f9bf4f843839f36ebfdb8acd47acaf2cd01703e9

4867eebb0f6bca553c7d50e878e3cb19f7471c1c89cbd85f49b6d50f7a44e779

811bba52ccee8ee0dce9f96f402a7c33427622276028bfb5e9d661130fa0e3fc

31038f7ee74463661addd7378b26076898e20d19e69f672f829af07b8ff816a9

0764a24f94d829a625cca37f92863a84553db77469b68eadf875e73fcf0d3036

72a79351d602ce6a1d0267bcd6d57c17cd8adc44c78197138cc3be5f4100b5b6

6e7f4d594ee4f5d5f08321ede7c32e51d72acbd0700f37c621f9145d8c86309d

de0a1c35121a6e08bf07267aca78fb8fe9c46ead95ed1acebfb3a77b72e869b8

25f616a8bce8578219bc884a64d1a3bc60ec87f07cdff8da3c386ae5b49445a9

98ab2fc44063d4e00f221e502419d9cca598fafb9e1e00352149327267604bc1

1b004980738e868605f88d6b764f72d0d6c50fddea3a7bdf4508ff3057501562

f21010eb8c0f2fd23c4ee941a394853597bfb90527f43f3c61bf6ce004b7f367

c8c5386fef1b6e45e02323f3a45b1e73b5d5be60a8a5f5ebe3b95bce77b03167

fc226deb01a8d15acf98fd6e9daa3d95b73687f46e9029523fd7e8fe8ad5fb83

c2f10c9556eecd1ffe67e763190c630262dfdb593245357283b02df2b4d696de

d9b56c6bf2c52116855a79e0008b6cfd7baef20e5af06ba142f774c8bf3b7401

776d7ce582c1e3af65b60073986c78da394cbbab1bf6b83a6c0d736c58d33758

40f99a875efa382cc0cae003c7b3b0519a7fcaa10a95989103b1e3e2bb20832a

485d446c5892b931c0a3a238dca84bebb787052c877deb73f02ae5ee5632de9d

b5b3747f8b0d11b5217a7a39c2420fb5a0c1044c82cbe9cba596dacf521a1a01

a531edd712eb0beabe14cb4e9ff91dc7635b743e71b6fdc20ec4c0247eccff62

d0b0f7842587afe7e23fc0218fd0a391996e72b1a804a6bfc33e97d9aecb6b2e

4daafeb8ae95460be3ef93577983db33cca28ecb67fff9b958a7f71ae17504bf

83c8f1d9b27d9e455ad2602b1005f6837ac6040cf61acc3124f7179fd5894d27

3d87877bfb6da476da1f51410416bef22cc216d941c79268f6de17d8dde1c0b8

4c1cb32e0a142d55997a55bfc239e4b5b31a6e021014d023d5ff9787948490df

4f8ba8eec38e117fa323bc24074993a7f1cc31c5ce112f9c6696c724628f53dc

1598486e69f94e221dcbd02b10bb33352baf5886db9c06475470159ab16eadbd

f80caed9f1b4d71e61a2869c240206f55c44fb9075d4da283df0bcedf7a11d3a

19cd76a94c55380cc6b053b05eb8896fa1329f03d65a7937225196c356bb0c6a

45cd3d4ec91bf68bc975d99d90612e459aeb4a0f31321a440d7d41fcdea798f3

b26144c6e42601f1f1be09ece7c7fcb127637db3b953065648d1b1f371da7e8a

a2144301067495656391aaa937e47b27706d7db8ea7fd12412e7796196f91fe8

f4b055a61d096e2f111bdaf7b171719188c02d74fa946dabdae0bbc72671d2db

5c31f5cfa003b1f745eb5019d76aa43f06a7d46c6403eeb2deabd44ee1a1a97a

0b28a2dcb365ac02b7d6c3928d5a1cfdd5ed669206eb176ab65ebb6084b58545

901dd6b7fb5aae90840191eb5e0b8e2578503feaef93fd58b99a3314a2008b4b

5be46ac9b6fd4d07db8710315b6fa8597464756005235472cf1562a0398921bf

41960d1cd749289ff40a1c92970706ead76f73fb3b61276a2f34a7ac38f989c6

7316651d2e38599d6e46a1ac52dff4eee7ae16f22e87cd244efb9a6ed748f358

ea2c8d68c83a93b4f526d2bdb25aa20920b43b7985b9bb8a8109912b74adf1df

3dfc781c1b656925b91a22b48b85b6ce2bf8f9cb9c1288be6ec3b760f6f7402d

dd28b5740c0fb2890a7579d75c65cf09a36ba5d9fc5df5c9581771e40420f35b

ed34e71d2fcae823b130a7e54a4404c15e34060e45c73654d16f34c799f91509

f0f932c136c2d34b0f9da7a83e1a2f87063ea2bce48d3a9af004189bf49d98d9

b4bded423c23574c5080f449d7c92c95b7aa480fedb756568d7280db3ec80cf0

c519d06e252a1cf04f8fb38f20c76a39363e51bf31864bac638f662a698b244e

9b5c8b82828c0aa94956671b3b9f2a6ec4f34a642d621938e86bffe9ce8b1acb

Hostname

Value
www.cttuae.com

IPv4-Addr

Value
111.90.150.186
172.245.244.118
79.110.49.162

Url

Value
http://bridgefieldapartmentsapp.ie/EX/index.html
http://designwebexpress.com/Invoice_6211.html
http://designwebexpress.com/Invoice_3211.html
http://internetshortcuts.link/VdXiIRQo/payload.iso
http://efghij.za.com/Invoice_898277.html
http://bridgefieldapartmentsapp.ie/EX
http://172.245.244.118/home.html
http://cargopattern.shop/home/home.html
http://fashionstylist.za.com/Invoice_898277.html
http://designwebexpress.com/Invoice_3221.html
http://seductivewomen.co.uk/invoice44201.html
http://cargopattern.shop/page.html
http://chemaxes.com/Invoice-Payment.html

http://landtours.rs/BB/index.html

http://fashionstylist.za.com/Invoice_82637.html

http://fashionstylist.za.com/Invoice_0020317.html

http://designwebexpress.com/Invoice_5221.html

http://designwebexpress.com/Invoice_4221.html

http://efghij.za.com/Invoice_662243.html

http://www.cttuae.com/ems/page.html

http://lfomessi.za.com/home.html

http://bridgefieldapartmentsapp.ie/home.html

http://172.245.244.118/Quote.html

http://designwebexpress.com/Invoice.html

http://efghij.za.com/Invoice_72638.html

External References

- https://otx.alienvault.com/pulse/64c28bb6fc5889a39639cfc4
- https://www.trellix.com/en-us/about/newsroom/stories/research/beyond-file-search-a-novel-method.html