Aug 31 2023

NETMANAGEIT

Intelligence Report

UAC-0173: judicial authorities and notaries "under the gun"

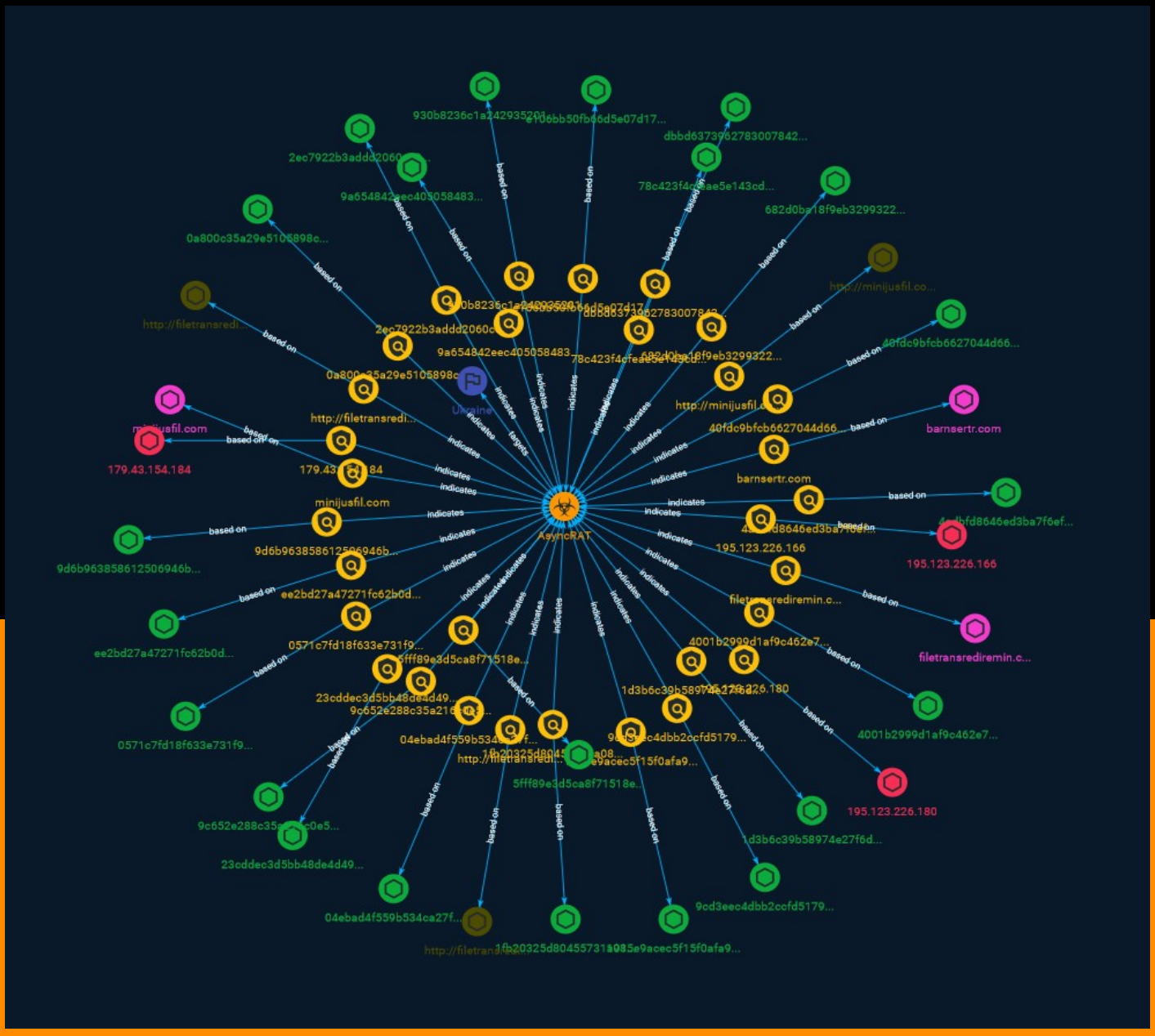

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Since the first quarter of 2023, the government computer emergency response team of Ukraine CERT-UA has been monitoring targeted malicious activity, which consists in the distribution of messages with attachments in the form of BZIP, GZIP, RAR archives containing BAT files created by with the help of the ScrubCrypt cryptor (cost - from USD 249), the launch of which will ensure that the computer is affected by the malicious program AsyncRAT (the source code is published on GitHub).

Confidence

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

15 / 100

Indicator

Name
4adbfd8646ed3ba7f6ef8dc615377e4abe320f5ebe670e3894b439152df68422
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '4adbfd8646ed3ba7f6ef8dc615377e4abe320f5ebe670e3894b439152df68422']
Name
http://filetransrediremin.com/calc.exe
Pattern Type
stix
Pattern
[url:value = 'http://filetransrediremin.com/calc.exe']
Name

2ec7922b3addd2060cc8d6346194cef5f7d4255243293ad9d20488234ae5a31c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2ec7922b3addd2060cc8d6346194cef5f7d4255243293ad9d20488234ae5a31c']

Name

04ebad4f559b534ca27fd29b45ecc96b2e8e5a04205f05ef186f1d0e08ad0b07

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '04ebad4f559b534ca27fd29b45ecc96b2e8e5a04205f05ef186f1d0e08ad0b07']

Name

40fdc9bfcb6627044d6643ad42c6523e399de2941c982943162f8f561893265e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '40fdc9bfcb6627044d6643ad42c6523e399de2941c982943162f8f561893265e']

Name

e106bb50fb66d5e07d17c2e99d2c009f4573444b51bf2023341bca31f0abeedd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e106bb50fb66d5e07d17c2e99d2c009f4573444b51bf2023341bca31f0abeedd']

Name

1fb20325d80455731a0849675b0a863d550014b3162d28148c702a52348ae3a4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1fb20325d80455731a0849675b0a863d550014b3162d28148c702a52348ae3a4']

Name

1915e9acec5f15f0afa975bf2eec577acd9a0ae48ce96c4161decdaa88f0547a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1915e9acec5f15f0afa975bf2eec577acd9a0ae48ce96c4161decdaa88f0547a']

Name

4001b2999d1af9c462e792996e45ee8e515d075fe19deb758348dd65af37e40a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4001b2999d1af9c462e792996e45ee8e515d075fe19deb758348dd65af37e40a']

Name

1d3b6c39b58974e27f6dabd4fd4827c67ebb323acf72f9eec268d0e7c37a68f1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1d3b6c39b58974e27f6dabd4fd4827c67ebb323acf72f9eec268d0e7c37a68f1']

Name

9a654842eec405058483efdd893171161e437fb1086772b3eaacd91059b23cfe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9a654842eec405058483efdd893171161e437fb1086772b3eaacd91059b23cfe']

Name

9c652e288c35a216c0e5a5a4e952e4cd276522b4be4a8e5fdf8eb908c208896d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9c652e288c35a216c0e5a5a4e952e4cd276522b4be4a8e5fdf8eb908c208896d']

Name

0a800c35a29e5105898ca274b12dda114e08f23da75dcec3b16a809f1d0109ad

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0a800c35a29e5105898ca274b12dda114e08f23da75dcec3b16a809f1d0109ad']

Name

http://minijusfil.com/c.cmd

Pattern Type

stix

Pattern

[url:value = 'http://minijusfil.com/c.cmd']

Name

9d6b963858612506946b88d8597d67c5092588058986f98b09e84e4133555bc1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9d6b963858612506946b88d8597d67c5092588058986f98b09e84e4133555bc1']

Name

dbbd6373962783007842b7d3a39b9ae9b93a1f709692018f0a3b2d58896f161b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dbbd6373962783007842b7d3a39b9ae9b93a1f709692018f0a3b2d58896f161b']

Name

78c423f4cfeae5e143cd2756b663bdee3ef455cb2d7ba4e89d604200d5c638f8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '78c423f4cfeae5e143cd2756b663bdee3ef455cb2d7ba4e89d604200d5c638f8']

Name

23cddec3d5bb48de4d49e9cf772512733e8d860a886817b54d0f5576ec150f43

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '23cddec3d5bb48de4d49e9cf772512733e8d860a886817b54d0f5576ec150f43']

Name

682d0ba18f9eb32993222bb686b53d6ec0d3255ca11b3c2dac929098651c7164

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '682d0ba18f9eb32993222bb686b53d6ec0d3255ca11b3c2dac929098651c7164']

Name

0571c7fd18f633e731f93e93f82260c89157e2e014152b1d909cfbc1c7d68570

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0571c7fd18f633e731f93e93f82260c89157e2e014152b1d909cfbc1c7d68570']

Name

barnsertr.com

Pattern Type

stix

Pattern

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

Name

9cd3eec4dbb2ccfd5179b14c10f3dd2e92c6e9d2804aadab31eaeaf428b970c3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9cd3eec4dbb2ccfd5179b14c10f3dd2e92c6e9d2804aadab31eaeaf428b970c3']

Name

5fff89e3d5ca8f71518e29491341b09ea37516a91daab793030ae093358bb82a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5fff89e3d5ca8f71518e29491341b09ea37516a91daab793030ae093358bb82a']

Name

930b8236c1a242935201df7a6a133c5fa0274966e9fc82ff507871e147ea8499

Description

RAR_Archive

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '930b8236c1a242935201df7a6a133c5fa0274966e9fc82ff507871e147ea8499']

Name

195.123.226.166

Description

ISP: ITL LLC **OS:** None ---------- Hostnames: - www.filetransrediremin.com - vps.hostry.com - filetransrediremin.com - sb4.giohap.site ---------- Domains: - filetransrediremin.com - giohap.site - hostry.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDHD8kU9mD1b0c6ZTQ3Ayt7UTOBWWJ7kHGYw1nJb8AiFHDo 4LLDg+eSZ4XZlvhaYsE4a1Dopwb1Yb2Y1zZZjwM3C4GoASpX00GCJZDe3p5BYskacU6sSy0dIfBP RSNFwwokKzsfetjpyTf2WCGfn/KMpy1ukkWfuaY/hY8p22rVcAXoydXl4B+Kjlx+r5L2nfPz18jY ItUEM6lBDrS56hOXMq95sQiwuRIEoU0qkDHVYjuywscl6FTHZ4OT58HM2RBpxbFBoqBYs03Wh/ NB xmvwF7vvbs3k10mItiJUef2Xs16nz96V/KlH5Z8F/YYR6E/t86Ez1TSf5UzPjU10kra9 Fingerprint: 4e:00:5d:df:90:48:97:6b:ff:10:8f:35:04:9b:a8:6c Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **25:** ``` 220 dom4.com ESMTP service ready 250-dom4.com says hello 250-ENHANCEDSTATUSCODES 250-PIPELINING 250-CHUNKING 250-8BITMIME 250-AUTH CRAM-MD5 250-AUTH=CRAM-MD5 250-XACK 250-SIZE 0 250-VERP 250 DSN ``` ---------- **80:** ``` HTTP/1.1 403 Forbidden Date: Wed, 23 Aug 2023 21:52:15 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips Last-Modified: Thu, 16 Oct 2014 13:20:58 GMT ETag: "1321-5058a1e728280" Accept-Ranges: bytes Content-Length: 4897 Content-Type: text/html; charset=UTF-8 ``` ---------- **443:** ``` HTTP/1.1 403 Forbidden Date: Thu, 24 Aug 2023 15:37:45 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips Last-Modified:

Thu, 16 Oct 2014 13:20:58 GMT ETag: "1321-5058a1e728280" Accept-Ranges: bytes Content-Length: 4897 Content-Type: text/html; charset=UTF-8 ``` HEARTBLEED: 2023/08/24 15:38:08 195.123.226.166:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.123.226.166']

Name

ee2bd27a47271fc62b0da3d8b4139746eae3deada5acecda7c4f502a162b9d11

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ee2bd27a47271fc62b0da3d8b4139746eae3deada5acecda7c4f502a162b9d11']

Name

filetransrediremin.com

Pattern Type

stix

Pattern

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

Name

minijusfil.com

Pattern Type

stix

Pattern

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

Name

179.43.154.184

Description

ISP: Private Layer INC **OS:** None ------------------------- Hostnames: - hostedby.privatelayer.com ------------------------- Domains: - privatelayer.com ------------------------- Services: **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10 (version 1607)/Windows Server 2016 (version 1607) OS Build: 10.0.14393 Target Name: WIN-D2B8VC1E9I0 NetBIOS Domain Name: WIN-D2B8VC1E9I0 NetBIOS Computer Name: WIN-D2B8VC1E9I0 DNS Domain Name: WIN-D2B8VC1E9I0 FQDN: WIN-D2B8VC1E9I0 ; Administrator SES ``` ------------------ **3389:** ``` \x0b\x12\x7f\x15\x00@\x10\x05\xaa\xe0\x15\x8f\x04\xd0\x04\xd0\x00\x01\x00\x02\x00\x0

0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0

0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00 ``` ------------------ **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Mon, 28 Aug 2023 05:41:46 GMT Connection: close Content-Length: 315 ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '179.43.154.184']

Name

195.123.226.180

Description

ISP: ITL LLC **OS:** Windows (build 10.0.17763) -------------------------- Hostnames: - 193270.example.com -------------------------- Domains: - example.com -------------------------- Services: **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10 (version 1809)/Windows Server 2019 (version 1809) OS Build: 10.0.17763 Target Name: WIN-LIVFRVQFMKO NetBIOS Domain Name: WIN-LIVFRVQFMKO NetBIOS Computer Name: WIN-LIVFRVQFMKO DNS Domain Name: WIN-LIVFRVQFMKO FQDN: WIN-LIVFRVQFMKO ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.123.226.180']

Name

http://filetransrediremin.com/cry/11rota

Pattern Type

stix

Pattern

[url:value = 'http://filetransrediremin.com/cry/11rota']

Malware

Name
AsyncRAT

Country

Name
Ukraine

Domain-Name

Value
filetransrediremin.com
minijusfil.com
barnsertr.com

StixFile

Value
dbbd6373962783007842b7d3a39b9ae9b93a1f709692018f0a3b2d58896f161b
9cd3eec4dbb2ccfd5179b14c10f3dd2e92c6e9d2804aadab31eaeaf428b970c3
2ec7922b3addd2060cc8d6346194cef5f7d4255243293ad9d20488234ae5a31c
1d3b6c39b58974e27f6dabd4fd4827c67ebb323acf72f9eec268d0e7c37a68f1
04ebad4f559b534ca27fd29b45ecc96b2e8e5a04205f05ef186f1d0e08ad0b07
930b8236c1a242935201df7a6a133c5fa0274966e9fc82ff507871e147ea8499
1915e9acec5f15f0afa975bf2eec577acd9a0ae48ce96c4161decdaa88f0547a
9d6b963858612506946b88d8597d67c5092588058986f98b09e84e4133555bc1
5fff89e3d5ca8f71518e29491341b09ea37516a91daab793030ae093358bb82a
23cddec3d5bb48de4d49e9cf772512733e8d860a886817b54d0f5576ec150f43
78c423f4cfeae5e143cd2756b663bdee3ef455cb2d7ba4e89d604200d5c638f8
4adbfd8646ed3ba7f6ef8dc615377e4abe320f5ebe670e3894b439152df68422
9c652e288c35a216c0e5a5a4e952e4cd276522b4be4a8e5fdf8eb908c208896d

0a800c35a29e5105898ca274b12dda114e08f23da75dcec3b16a809f1d0109ad

1fb20325d80455731a0849675b0a863d550014b3162d28148c702a52348ae3a4

0571c7fd18f633e731f93e93f82260c89157e2e014152b1d909cfbc1c7d68570

682d0ba18f9eb32993222bb686b53d6ec0d3255ca11b3c2dac929098651c7164

ee2bd27a47271fc62b0da3d8b4139746eae3deada5acecda7c4f502a162b9d11

e106bb50fb66d5e07d17c2e99d2c009f4573444b51bf2023341bca31f0abeedd

4001b2999d1af9c462e792996e45ee8e515d075fe19deb758348dd65af37e40a

9a654842eec405058483efdd893171161e437fb1086772b3eaacd91059b23cfe

40fdc9bfcb6627044d6643ad42c6523e399de2941c982943162f8f561893265e

IPv4-Addr

Value
179.43.154.184
195.123.226.166
195.123.226.180

Url

Value
http://filetransrediremin.com/cry/11rota
http://minijusfil.com/c.cmd
http://filetransrediremin.com/calc.exe

External References

- https://otx.alienvault.com/pulse/64ee03cb197c460023fb73ad
- https://cert.gov.ua/article/5628441