Sep 16 2023

NETMANAGEIT

Intelligence Report

Email campaigns leverage updated DBatLoader to deliver RATs, stealers

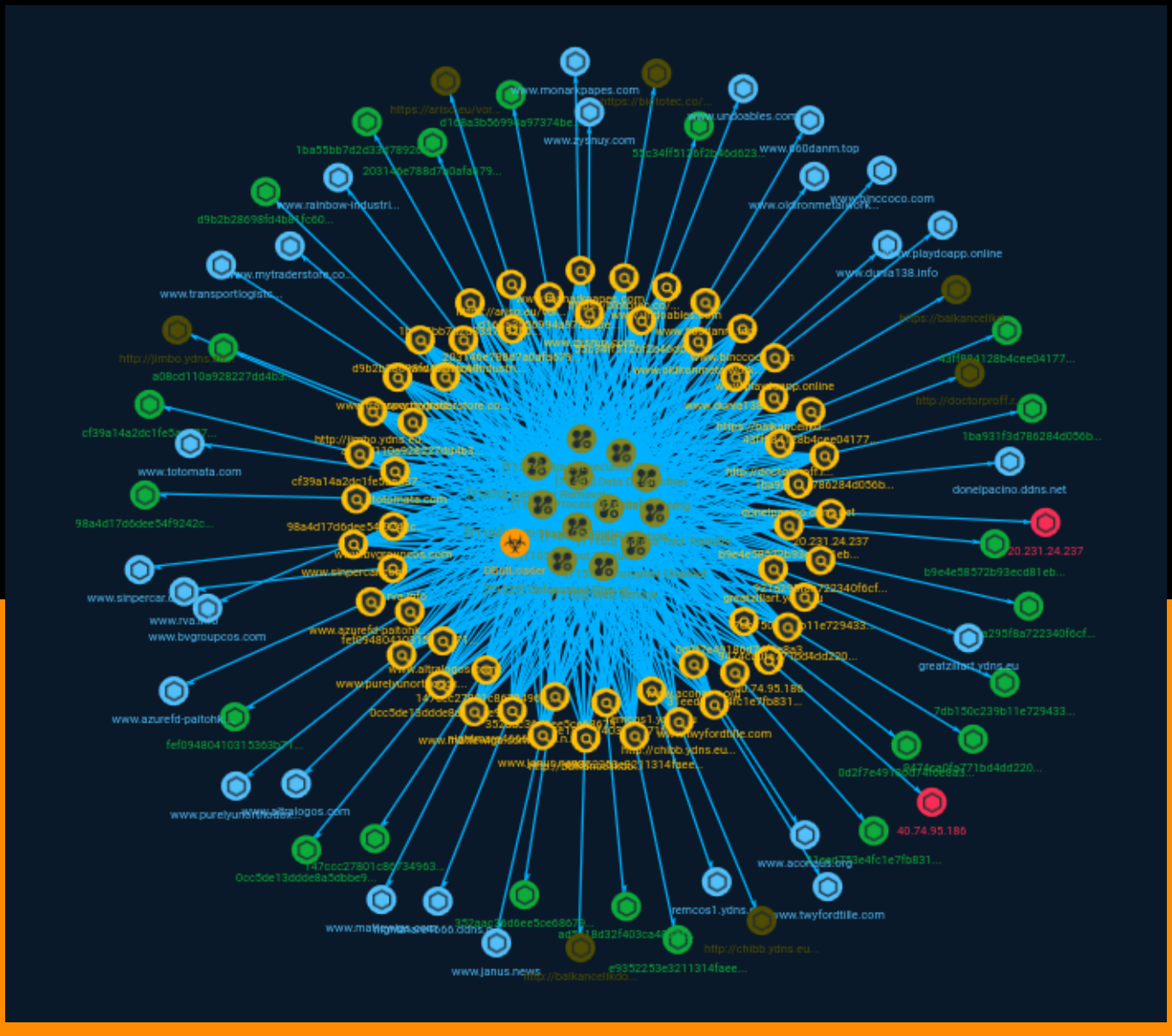

Table of contents

Overview

Entities

Observables

External References

Overview

Description

IBM X-Force has identified new capabilities in DBatLoader malware samples delivered in recent email campaigns, signaling a heightened risk of infection from commodity malware families associated with DBatLoader activity. X-Force has observed nearly two dozen email campaigns since late June leveraging the updated DBatLoader loader to deliver payloads such as Remcos, Warzone, Formbook, and AgentTesla. DBatLoader malware has been used since 2020 by cybercriminals to install commodity malware remote access Trojans (RATs) and infostealers, primarily via malicious spam (malspam).

Confidence

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

15 / 100

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
Input Capture
ID
T1056
Description
Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various

different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

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

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

Indicator Removal

ID

T1070

Description

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary.

(Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Hijack Execution Flow

ID

T1574

Description

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

Name

Ingress Tool Transfer

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas)

Name

Multi-Stage Channels

ID

T1104

Description

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

first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

Name

Data Destruction

ID

T1485

Description

Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives.(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)(Citation: Unit 42 Shamoon3 2018)(Citation: Talos Olympic Destroyer 2018) Common operating system file deletion commands such as `del` and `rm` often only remove pointers to files without wiping the contents of the files themselves, making the files recoverable by proper forensic methodology. This behavior is distinct from [Disk Content Wipe](https://attack.mitre.org/techniques/T1561/001) and [Disk Structure Wipe](https://attack.mitre.org/techniques/T1561/002) because individual files are destroyed rather than sections of a storage disk or the disk's logical structure. Adversaries may attempt to overwrite files and directories with randomly generated data to make it irrecoverable.(Citation: Kaspersky StoneDrill 2017)(Citation: Unit 42 Shamoon3 2018) In some cases politically oriented image files have been used to overwrite data.(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017) To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware designed for destroying data may have worm-like features to propagate across a network by leveraging additional techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: Symantec Shamoon 2012)(Citation: FireEye Shamoon Nov 2016)(Citation: Palo Alto Shamoon Nov 2016)(Citation: Kaspersky StoneDrill 2017)(Citation: Talos Olympic Destroyer 2018). In cloud environments, adversaries may leverage access to delete cloud storage, cloud storage accounts, machine images, and other infrastructure crucial to operations to damage an organization or their customers.(Citation: Data Destruction - Threat Post)(Citation: DOJ - Cisco Insider)

Name
Web Service
ID
T1102
Description
Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

Indicator

Name
b9e4e58572b93ecd81ebcb6ef411b6fa447c7c9177a1ea2fdf26558d76e0ca3a
Description
Typical_Malware_String_Transforms
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'b9e4e58572b93ecd81ebcb6ef411b6fa447c7c9177a1ea2fdf26558d76e0ca3a']
Name
0cc5de13ddde8a5dbbe9ce4f14a595e8f8bed743a0f4a7bbdba4d8de44d88b30
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '0cc5de13ddde8a5dbbe9ce4f14a595e8f8bed743a0f4a7bbdba4d8de44d88b30']

Name

www.zysnuy.com

Pattern Type

stix

Pattern

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

Name

31eed753e4fc1e7fb831c38bddd30577a41a727fabb73360fa90a6d93fc61d02

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '31eed753e4fc1e7fb831c38bddd30577a41a727fabb73360fa90a6d93fc61d02']

Name

www.totomata.com

Pattern Type

stix

Pattern

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

Name

www.dunia138.info

Pattern Type

stix

Pattern

[hostname:value = 'www.dunia138.info']

Name

352aac36d6ee5ce68679227aa27b082cbeae8990853a47b3d48ee7bc4cd7c613

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '352aac36d6ee5ce68679227aa27b082cbeae8990853a47b3d48ee7bc4cd7c613']

Name

203146e788d7a0afa679721e1581f5cdcf8e2c4d4367a7ce53c433184d988fcc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '203146e788d7a0afa679721e1581f5cdcf8e2c4d4367a7ce53c433184d988fcc']

Name

greatzillart.ydns.eu

Pattern Type

stix

Pattern

[hostname:value = 'greatzillart.ydns.eu']

Name

www.rva.info

Pattern Type

stix

Pattern

[hostname:value = 'www.rva.info']

Name

55c34ff5126f2b46d623f802d1e0e1d886e671fb8fb7f75294bbf7726f13340d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '55c34ff5126f2b46d623f802d1e0e1d886e671fb8fb7f75294bbf7726f13340d']

Name

remcos1.ydns.eu

Pattern Type

stix

Pattern

[hostname:value = 'remcos1.ydns.eu']

Name

a08cd110a928227dd4b3b42b1801bc1c907dd042bea8494ac701142c5eb345da

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a08cd110a928227dd4b3b42b1801bc1c907dd042bea8494ac701142c5eb345da']

Name

http://doctorproff.ru/194_Hmoczcsvbok

Pattern Type

stix

Pattern

[url:value = 'http://doctorproff.ru/194_Hmoczcsvbok']

Name

147ccc27801c86734963bf547721517bddbc76c4b80225d557c373cd5e16da3d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '147ccc27801c86734963bf547721517bddbc76c4b80225d557c373cd5e16da3d']

Name

d168a3b56994a97374be1c208e6e3aa01e1c512829ee4cceafceeeee1b5ddcc1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd168a3b56994a97374be1c208e6e3aa01e1c512829ee4cceafceeeee1b5ddcc1']

Name
0d2f7e49186d74f6e8a320d41283d88fcd785f4b1e06abd18553ebc14b8c9f17
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '0d2f7e49186d74f6e8a320d41283d88fcd785f4b1e06abd18553ebc14b8c9f17']
Name
www.sinpercar.com
Pattern Type
stix
Pattern
[hostname:value = 'www.sinpercar.com']
Name
www.binccoco.com
Pattern Type
stix
Pattern

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

Name

ad5e18d32f403ca4871f3d4b222c84821a6b6ba74ec858cc99eb00c66bb6bddb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ad5e18d32f403ca4871f3d4b222c84821a6b6ba74ec858cc99eb00c66bb6bddb']

Name

www.mytraderstore.com

Pattern Type

stix

Pattern

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

Name

20.231.24.237

Description

CC=US ASN=AS8075 MICROSOFT-CORP-MSN-AS-BLOCK

Pattern Type

stix

Pattern

[ipv4-addr:value = '20.231.24.237']

Name

fef09480410315363b71b047f1a07100080cb970bae50ee0280586ab778089e8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fef09480410315363b71b047f1a07100080cb970bae50ee0280586ab778089e8']

Name

https://biototec.co/youtubedrivedocumentsuploadgifterssocialiseapartmentsroomsdoors/211_Wbroctgfmht

Description

HTML document, ASCII text
80c3fe2ae1062abf56456f52518bd670f9ec3917b7f85e152b347ac6b6faf880

Pattern Type

stix

Pattern

[url:value = 'https://biototec.co/youtubedrivedocumentsuploadgifterssocialiseapartmentsroomsdoors/211_Wbroctgfmht']

Name

www.aconaus.org

Pattern Type

stix

Pattern

[hostname:value = 'www.aconaus.org']

Name

http://jimbo.ydns.eu/jimboori/inc/def4f4924bdf6e.php

Pattern Type

stix

Pattern

[url:value = 'http://jimbo.ydns.eu/jimboori/inc/def4f4924bdf6e.php']

Name

https://balkancelikdovme.com/work/Elpuxpkilck

Description

HTML document, ASCII text, with CRLF, LF line terminators
37a4e56c497e170de6e152bc479624eb8d7ccb35bad5a190f2fdb17ac699cffa

Pattern Type

stix

Pattern

[url:value = 'https://balkancelikdovme.com/work/Elpuxpkilck']

Name

nightmare4666.ddns.net

Pattern Type

stix

Pattern

[hostname:value = 'nightmare4666.ddns.net']

Name

www.rainbow-industrie.com

Pattern Type

stix

Pattern

[hostname:value = 'www.rainbow-industrie.com']

Name

7db150c239b11e729433ce9ea99939f08bf35aac1dda071917c4a7e694a7258d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7db150c239b11e729433ce9ea99939f08bf35aac1dda071917c4a7e694a7258d']

Name

www.azurefd-paitohk.xyz

Pattern Type

stix

Pattern

[hostname:value = 'www.azurefd-paitohk.xyz']

Name

www.oldironmetalworksllc.com

Pattern Type

stix

Pattern

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

Name

http://chibb.ydns.eu/chibbori/inc/8fcde15698ce9a.php

Pattern Type

stix

Pattern

[url:value = 'http://chibb.ydns.eu/chibbori/inc/8fcde15698ce9a.php']

Name

www.transportlogistcs.com

Pattern Type

stix

Pattern

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

Name

1ba931f3d786284d056bd83659afabe498c61c999fd5d64837da8c2b737e3746

Description

Win.Trojan.Sinowal-9756760-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1ba931f3d786284d056bd83659afabe498c61c999fd5d64837da8c2b737e3746']

Name

www.mattewigs.com

Pattern Type

stix

Pattern

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

Name

www.monarkpapes.com

Pattern Type

stix

Pattern

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

Name

40.74.95.186

Description

ISP: Microsoft Corporation **OS:** Windows (build 10.0.14393) ---------- Hostnames: ---------- Domains: ---------- 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: window NetBIOS Domain Name: window NetBIOS Computer Name: window DNS Domain Name: window FQDN: window ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '40.74.95.186']

Name

www.bvgroupcos.com

Pattern Type

stix

Pattern

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

Name

www.playdoapp.online

Pattern Type

stix

Pattern

[hostname:value = 'www.playdoapp.online']

Name

http://balkancelikdovme.com/hjghgynyvbtvyugjhbugvdveksk/Xezdxpgykmk

Description

Threat: malware_download - Reporter: abuse_ch - Status: offline

Pattern Type

stix

Pattern

[url:value = 'http://balkancelikdovme.com/hjghgynyvbtvyugjhbugvdveksk/Xezdxpgykmk']

Name

1ba55bb7d2d33d7892669c2e96c351fe59ce60144429508d6251d5dcbfc5ff86

Description

Delphi

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1ba55bb7d2d33d7892669c2e96c351fe59ce60144429508d6251d5dcbfc5ff86']

Name

921a295f8a722340f6cf979c9e3fb0f9a762fe45c94407d1e1a32a4dc35e2854

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '921a295f8a722340f6cf979c9e3fb0f9a762fe45c94407d1e1a32a4dc35e2854']

Name

www.altralogos.com

Pattern Type

stix

Pattern

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

Name

www.undoables.com

Pattern Type

stix

Pattern

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

Name

www.twyfordtille.com

Pattern Type

stix

Pattern

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

Name

cf39a14a2dc1fe5aa487b6faf19c63bc97103db670fa24c62832895e3002eca2

Description

Typical_Malware_String_Transforms

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cf39a14a2dc1fe5aa487b6faf19c63bc97103db670fa24c62832895e3002eca2']

Name

43ff884128b4cee041776015abb9692e42db2cbf8b5a4364859d346c809ec5cd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '43ff884128b4cee041776015abb9692e42db2cbf8b5a4364859d346c809ec5cd']

Name

www.janus.news

Pattern Type

stix

Pattern

[hostname:value = 'www.janus.news']

Name

https://ariso.eu/vorpruefung/255_Pbtrfmfsxud

Pattern Type

stix

Pattern

[url:value = 'https://ariso.eu/vorpruefung/255_Pbtrfmfsxud']

Name

9474ca0fa771bd4dd2202e312ada0090f6890635b9039b5be855cc7cb8eab6ee

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9474ca0fa771bd4dd2202e312ada0090f6890635b9039b5be855cc7cb8eab6ee']

Name

98a4d17d6dee54f9242c704af627da853d978d6d37738f875d08ea0e7eaca373

Description

Typical_Malware_String_Transforms

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '98a4d17d6dee54f9242c704af627da853d978d6d37738f875d08ea0e7eaca373']

Name

www.660danm.top

Pattern Type

stix

Pattern

[hostname:value = 'www.660danm.top']

Name

e9352253e3211314faee670cf457e3f6732d7d93eb52f46aebf4f79cb22cbf7e

Description

Delphi

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e9352253e3211314faee670cf457e3f6732d7d93eb52f46aebf4f79cb22cbf7e']

Name

d9b2b28698fd4b81fc602305bd73e060dc35acb6b72264e75ba9bee47a3501e2

Description

Win.Dropper.LokiBot-9938605-0

Pattern Type

stix

Pattern
[file:hashes.'SHA-256' = 'd9b2b28698fd4b81fc602305bd73e060dc35acb6b72264e75ba9bee47a3501e2']
Name
donelpacino.ddns.net
Pattern Type
stix
Pattern
[hostname:value = 'donelpacino.ddns.net']
Name
www.purelyunorthodox.com
Pattern Type
stix
Pattern
[hostname:value = 'www.purelyunorthodox.com']

Malware

Name
DBatLoader

StixFile

Value
0d2f7e49186d74f6e8a320d41283d88fcd785f4b1e06abd18553ebc14b8c9f17
43ff884128b4cee041776015abb9692e42db2cbf8b5a4364859d346c809ec5cd
d9b2b28698fd4b81fc602305bd73e060dc35acb6b72264e75ba9bee47a3501e2
fef09480410315363b71b047f1a07100080cb970bae50ee0280586ab778089e8
921a295f8a722340f6cf979c9e3fb0f9a762fe45c94407d1e1a32a4dc35e2854
352aac36d6ee5ce68679227aa27b082cbeae8990853a47b3d48ee7bc4cd7c613
31eed753e4fc1e7fb831c38bddd30577a41a727fabb73360fa90a6d93fc61d02
203146e788d7a0afa679721e1581f5cdcf8e2c4d4367a7ce53c433184d988fcc
0cc5de13ddde8a5dbbe9ce4f14a595e8f8bed743a0f4a7bbdba4d8de44d88b30
d168a3b56994a97374be1c208e6e3aa01e1c512829ee4cceafceeeee1b5ddcc1
147ccc27801c86734963bf547721517bddbc76c4b80225d557c373cd5e16da3d
98a4d17d6dee54f9242c704af627da853d978d6d37738f875d08ea0e7eaca373
b9e4e58572b93ecd81ebcb6ef411b6fa447c7c9177a1ea2fdf26558d76e0ca3a

a08cd110a928227dd4b3b42b1801bc1c907dd042bea8494ac701142c5eb345da

7db150c239b11e729433ce9ea99939f08bf35aac1dda071917c4a7e694a7258d

55c34ff5126f2b46d623f802d1e0e1d886e671fb8fb7f75294bbf7726f13340d

1ba931f3d786284d056bd83659afabe498c61c999fd5d64837da8c2b737e3746

e9352253e3211314faee670cf457e3f6732d7d93eb52f46aebf4f79cb22cbf7e

ad5e18d32f403ca4871f3d4b222c84821a6b6ba74ec858cc99eb00c66bb6bddb

1ba55bb7d2d33d7892669c2e96c351fe59ce60144429508d6251d5dcbfc5ff86

cf39a14a2dc1fe5aa487b6faf19c63bc97103db670fa24c62832895e3002eca2

9474ca0fa771bd4dd2202e312ada0090f6890635b9039b5be855cc7cb8eab6ee

Hostname

Value
www.aconaus.org
www.mytraderstore.com
nightmare4666.ddns.net
www.monarkpapes.com
www.azurefd-paitohk.xyz
www.transportlogistcs.com
www.altralogos.com
www.rainbow-industrie.com
www.dunia138.info
www.660danm.top
www.totomata.com
www.janus.news
www.zysnuy.com

donelpacino.ddns.net

www.binccoco.com

www.purelyunorthodox.com

www.mattewigs.com

www.twyfordtille.com

remcos1.ydns.eu

www.bvgroupcos.com

www.sinpercar.com

www.rva.info

www.undoables.com

greatzillart.ydns.eu

www.playdoapp.online

www.oldironmetalworksllc.com

IPv4-Addr

Value
20.231.24.237
40.74.95.186

Url

Value
https://biototec.co/youtubedrivedocumentsuploadgifterssocialiseapartmentsroomsdoors/211_Wbroctgfmht
http://chibb.ydns.eu/chibbori/inc/8fcde15698ce9a.php
http://balkancelikdovme.com/hjghgynyvbtvyugjhbugvdveksk/Xezdxpgykmk
http://jimbo.ydns.eu/jimboori/inc/def4f4924bdf6e.php
https://ariso.eu/vorpruefung/255_Pbtrfmfsxud
https://balkancelikdovme.com/work/Elpuxpkilck
http://doctorproff.ru/194_Hmoczcsvbok

External References

- https://otx.alienvault.com/pulse/6503fb29e81f4b7d817bfed2
- https://securityintelligence.com/posts/email-campaigns-leverage-updated-dbatloader-deliver-rats-stealers