Aug 09 2024

NETMANAGEIT

Intelligence Report

Router Roulette: Cybercriminals and Nation-States Sharing Compromised Networks

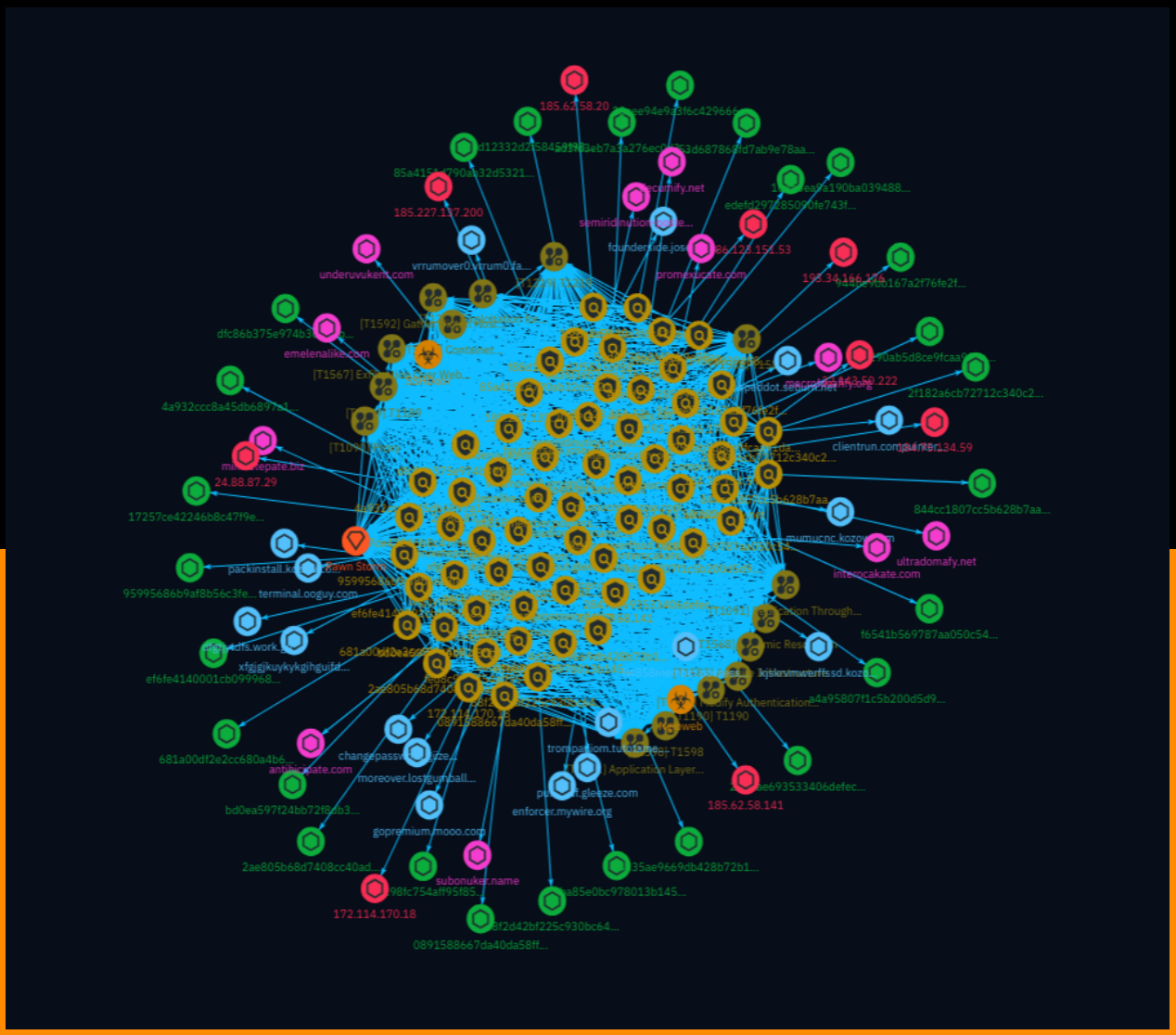

Table of contents

Overview

Entities

Observables

External References

Overview

Description

TrendMicro highlights the dangers of internet-facing routers and elaborates on Pawn Storm's exploitation of EdgeRouters, complementing the FBI's advisory from February 27, 2024. Cybercriminals and nation-state actors share an interest in compromised routers used as an anonymization layer, with cybercriminals renting out compromised routers and nation-state threat actors like Pawn Storm and Sandworm using dedicated proxy botnets. The analysis focuses on a criminal botnet of Ubiquiti EdgeRouters, disrupted by the FBI in January 2024, which Pawn Storm accessed in April 2022 for persistent espionage campaigns.

Confidence

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

100 / 100

Content

N/A

Attack-Pattern

Name

Replication Through Removable Media

ID

T1091

Description

Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system. In the case of Initial Access, this may occur through manual manipulation of the media, modification of systems used to initially format the media, or modification to the media's firmware itself. Mobile devices may also be used to infect PCs with malware if connected via USB.(Citation: Exploiting Smartphone USB) This infection may be achieved using devices (Android, iOS, etc.) and, in some instances, USB charging cables.(Citation: Windows Malware Infecting Android)(Citation: iPhone Charging Cable Hack) For example, when a smartphone is connected to a system, it may appear to be mounted similar to a USB-connected disk drive. If malware that is compatible with the connected system is on the mobile device, the malware could infect the machine (especially if Autorun features are enabled).

Name

Proxy

ID

T1090

Description

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

Name

Container Administration Command

ID

T1609

Description

Adversaries may abuse a container administration service to execute commands within a container. A container administration service such as the Docker daemon, the Kubernetes API server, or the kubelet may allow remote management of containers within an environment.(Citation: Docker Daemon CLI)(Citation: Kubernetes API)(Citation: Kubernetes Kubelet) In Docker, adversaries may specify an entrypoint during container deployment that executes a script or command, or they may use a command such as `docker exec` to execute a command within a running container.(Citation: Docker Entrypoint)(Citation: Docker Exec) In Kubernetes, if an adversary has sufficient permissions, they may gain remote execution in a container in the cluster via interaction with the Kubernetes API

server, the kubelet, or by running a command such as `kubectl exec`.(Citation: Kubectl Exec Get Shell)

Name

Acquire Infrastructure

ID

T1583

Description

Adversaries may buy, lease, rent, or obtain infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services.(Citation: TrendmicroHideoutsLease) Some infrastructure providers offer free trial periods, enabling infrastructure acquisition at limited to no cost.(Citation: Free Trial PurpleUrchin) Additionally, botnets are available for rent or purchase. Use of these infrastructure solutions allows adversaries to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contacting third-party web services or acquiring infrastructure to support [Proxy] (https://attack.mitre.org/techniques/T1090), including from residential proxy services. (Citation: amnesty_nso_pegasus)(Citation: FBI Proxies Credential Stuffing)(Citation: Mandiant APT29 Microsoft 365 2022) Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.

Name

T1190

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211) or [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

Name

Gather Victim Host Information

ID

T1592

Description

Adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding its configuration (ex: operating system, language, etc.). Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about hosts 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)). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [External Remote Services](https://attack.mitre.org/techniques/T1133)).

Name

T1219

ID

T1219

Description

An adversary may use legitimate desktop support and remote access software to establish an interactive command and control channel to target systems within networks. These services, such as `VNC`, `Team Viewer`, `AnyDesk`, `ScreenConnect`, `LogMein`, `AmmyyAdmin`, and other remote monitoring and management (RMM) tools, are commonly used as legitimate technical support software and may be allowed by application control within a target environment.(Citation: Symantec Living off the Land)(Citation: CrowdStrike 2015 Global Threat Report)(Citation: CrySyS Blog TeamSpy) Remote access software may be installed and used post-compromise as an alternate communications channel for redundant access or as a way to establish an interactive remote desktop session with the target system. They may also be used as a component of malware to establish a reverse connection or back-connect to a service or adversary-controlled system. Adversaries may similarly abuse response features included in EDR and other defensive tools that enable remote access. Installation of many remote access software may also include persistence (e.g., the software's installation routine creates a [Windows Service](https://attack.mitre.org/techniques/T1543/003)). Remote access modules/features may also exist as part of otherwise existing software (e.g., Google Chrome’s Remote Desktop).(Citation: Google Chrome Remote Desktop)(Citation: Chrome Remote Desktop)

Name

Exploitation for Defense Evasion

ID

T1211

Description

Adversaries may exploit a system or application vulnerability to bypass security features. Exploitation of a vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Vulnerabilities may exist in defensive security software that can be used to disable or circumvent them. Adversaries may have prior knowledge through reconnaissance that security software exists within an environment or they may perform checks during or shortly after the system is compromised for [Security Software Discovery](https://attack.mitre.org/techniques/T1518/001). The security software will likely be targeted directly for exploitation. There are examples of antivirus software being targeted by persistent threat groups to avoid detection. There have also been examples of vulnerabilities in public cloud infrastructure of SaaS applications that may bypass defense boundaries (Citation: Salesforce zero-day in facebook phishing attack), evade security logs (Citation: Bypassing CloudTrail in AWS Service Catalog), or deploy hidden infrastructure.(Citation: GhostToken GCP flaw)

Name

T1598

ID

T1598

Description

Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from [Phishing](https://attack.mitre.org/techniques/T1566) in that the objective is gathering data from the victim rather than executing malicious code. 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 credential harvesting campaigns. Adversaries may also try to obtain information directly through the exchange of emails, instant messages, or other electronic conversation means.(Citation: ThreatPost Social Media Phishing)(Citation: TrendMictro Phishing)(Citation: PCMag FakeLogin)(Citation: Sophos Attachment)(Citation: GitHub Phishery) Victims may also receive phishing messages that direct them to call a phone number where the adversary attempts to collect confidential information.(Citation: Avertium callback phishing) Phishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) and/or sending multiple, seemingly urgent messages. 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) Phishing for information may also involve 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)

Name

T1189

ID

T1189

Description

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting * Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary * Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising]

(https://attack.mitre.org/techniques/T1583/008)) * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version. * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. * In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

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.(Citation: Mandiant APT29 Eye Spy Email Nov 22)

Name

T1588

ID

T1588

Description

Adversaries may buy and/or steal capabilities that can be used during targeting. Rather than developing their own capabilities in-house, adversaries may purchase, freely download, or steal them. Activities may include the acquisition of malware, software (including licenses), exploits, certificates, and information relating to vulnerabilities. Adversaries may obtain capabilities to support their operations throughout numerous phases of the adversary lifecycle. In addition to downloading free malware, software, and exploits from the internet, adversaries may purchase these capabilities from third-party entities. Third-party entities can include technology companies that specialize in malware and exploits, criminal marketplaces, or from individuals.(Citation: NationsBuying)(Citation: PegasusCitizenLab) In addition to purchasing capabilities, adversaries may steal capabilities from third-party entities (including other adversaries). This can include stealing software licenses, malware, SSL/TLS and code-signing certificates, or raiding closed databases of vulnerabilities or exploits.(Citation: DiginotarCompromise)

Name

Modify Authentication Process

ID

T1556

Description

Adversaries may modify authentication mechanisms and processes to access user credentials or enable otherwise unwarranted access to accounts. The authentication process is handled by mechanisms, such as the Local Security Authentication Server (LSASS) process and the Security Accounts Manager (SAM) on Windows, pluggable authentication modules (PAM) on Unix-based systems, and authorization plugins on MacOS systems, responsible for gathering, storing, and validating credentials. By modifying an authentication process, an adversary may be able to authenticate to a service or system without using [Valid Accounts](https://attack.mitre.org/techniques/T1078). Adversaries may maliciously modify a part of this process to either reveal credentials or bypass authentication mechanisms. Compromised credentials or access may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop.

Name

Exfiltration Over Web Service

ID

T1567

Description

Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to compromise. Firewall rules may also already exist to permit traffic to these services. Web service providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Name

Dynamic Resolution

ID

T1568

Description

Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control. Adversaries may use dynamic resolution for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ dynamic resolution as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)

Indicator

Name
clientrun.compuinter.com
Pattern Type
stix
Pattern
[hostname:value = 'clientrun.compuinter.com']
Name
ad3fd3eb7a3a276ec0d384afb5b75fe7d9fc047bb0dab40f9d55870d4520c1f3
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ad3fd3eb7a3a276ec0d384afb5b75fe7d9fc047bb0dab40f9d55870d4520c1f3']
Name

24.88.87.29

Pattern Type

stix

Pattern

[ipv4-addr:value = '24.88.87.29']

Name

founderside.joseulloa.cl

Pattern Type

stix

Pattern

[hostname:value = 'founderside.joseulloa.cl']

Name

decumify.net

Pattern Type

stix

Pattern

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

Name

95995686b9af8b56c3fed1dadccf8b2ed5f417bb4eb8947a406a6e943cca33c6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '95995686b9af8b56c3fed1dadccf8b2ed5f417bb4eb8947a406a6e943cca33c6']

Name

2ae805b68d7408cc40ad058bc0b8b2b5c29d77760084a5230448e47cec1c43f4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2ae805b68d7408cc40ad058bc0b8b2b5c29d77760084a5230448e47cec1c43f4']

Name

underuvukent.com

Pattern Type

stix

Pattern

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

Name
enforcer.mywire.org
Pattern Type
stix
Pattern
[hostname:value = 'enforcer.mywire.org']
Name
moreover.lostgumball.com
Pattern Type
stix
Pattern
[hostname:value = 'moreover.lostgumball.com']
Name
53d687868fd7ab9e78aa09f696923bd3c057e4e50432d07210080474a8d879cb
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '53d687868fd7ab9e78aa09f696923bd3c057e4e50432d07210080474a8d879cb']

Name

17257ce42246b8c47f9ec639a6ffaca2bc14c21a22c4419bf468e3f1d491e330

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '17257ce42246b8c47f9ec639a6ffaca2bc14c21a22c4419bf468e3f1d491e330']

Name

f6541b569787aa050c54ad85976ac5b729697a022be188b0040d37aa91e49ae2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f6541b569787aa050c54ad85976ac5b729697a022be188b0040d37aa91e49ae2']

Name

semiridinution-postepudency.com

Pattern Type

stix

Pattern

[domain-name:value = 'semiridinution-postepudency.com']

Name

32.143.50.222

Pattern Type

stix

Pattern

[ipv4-addr:value = '32.143.50.222']

Name

fed8c98fc754aff95f8538b5bebce558eb274256b0265d4482a675b74e93cc93

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fed8c98fc754aff95f8538b5bebce558eb274256b0265d4482a675b74e93cc93']

Name

antihicipate.com

Pattern Type

stix

Pattern

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

Name

172.114.170.18

Description

Agressive IP known malicious on AbuseIPDB - countryCode: US - abuseConfidenceScore: 100 - lastReportedAt: 2024-02-26T23:06:06+00:00

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.114.170.18']

Name

4d35ae9669db428b72b1aaadd21dbed44ad2fc678efc8110d89ff723e0497406

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4d35ae9669db428b72b1aaadd21dbed44ad2fc678efc8110d89ff723e0497406']

Name

f88d12332d2f58459f989c7c41b5381e8aed9c8c30c1d11373f0d1eb0b340b9a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f88d12332d2f58459f989c7c41b5381e8aed9c8c30c1d11373f0d1eb0b340b9a']

Name

speddot.seburn.net

Pattern Type

stix

Pattern

[hostname:value = 'speddot.seburn.net']

Name

104e3ea9a190ba039488f5200824fe883b98f6fe01d05a1b55e15ed2199c807a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '104e3ea9a190ba039488f5200824fe883b98f6fe01d05a1b55e15ed2199c807a']

Name

trompadiom.tutotame.bigbox.info

Pattern Type

stix

Pattern

[hostname:value = 'trompadiom.tutotame.bigbox.info']

Name

bd0ea597f24bb72f8db34b6b6d2c0bc70eb53df9eae40cdb216a13521145ab03

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bd0ea597f24bb72f8db34b6b6d2c0bc70eb53df9eae40cdb216a13521145ab03']

Name

c290ab5d8ce9fcaa91da3b488c93dee1a4d0581c1335f19cb48027a5a03fe525

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c290ab5d8ce9fcaa91da3b488c93dee1a4d0581c1335f19cb48027a5a03fe525']

Name

dfc86b375e974b3092bbff41eb24db3281fb4fc104f1043a7afbf95f85a2c1d5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dfc86b375e974b3092bbff41eb24db3281fb4fc104f1043a7afbf95f85a2c1d5']

Name

85a4151d790ab32d5321c6e71748b2446032e1775aedd0168be25f76bf4fe93f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '85a4151d790ab32d5321c6e71748b2446032e1775aedd0168be25f76bf4fe93f']

Name

minixetepate.biz

Pattern Type

stix

Pattern

[domain-name:value = 'minixetepate.biz']

Name

dfgtjytdfs.work.gd

Pattern Type

stix

Pattern

[hostname:value = 'dfgtjytdfs.work.gd']

Name

ultradomafy.net

Pattern Type

stix

Pattern

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

Domain-Name

Value
interocakate.com
minixetepate.biz
emelenalike.com
semiridinution-postepudency.com
promexucate.com
subonuker.name
underuvukent.com
antihicipate.com
decumify.net
macrofocafify.org
ultradomafy.net

StixFile

Value
f88d12332d2f58459f989c7c41b5381e8aed9c8c30c1d11373f0d1eb0b340b9a
fed8c98fc754aff95f8538b5bebce558eb274256b0265d4482a675b74e93cc93
681a00df2e2cc680a4b68bdb6fe7d55c34d6d3fc35d462c78ebb659f9cb2cd60
edefd297285090fe743f5c3b111bce54da40f43a32e15d8fa87b8a2c243f6d47
f6541b569787aa050c54ad85976ac5b729697a022be188b0040d37aa91e49ae2
28aee94e9a3f6c4296663bb853a5af5817ae109f066c88b7a245316a9a1e4712
c290ab5d8ce9fcaa91da3b488c93dee1a4d0581c1335f19cb48027a5a03fe525
53d687868fd7ab9e78aa09f696923bd3c057e4e50432d07210080474a8d879cb
944be9bb167a2f76fe2f539d3860bbf26301830c479bc68509af46e047993c8c
17257ce42246b8c47f9ec639a6ffaca2bc14c21a22c4419bf468e3f1d491e330
ad3fd3eb7a3a276ec0d384afb5b75fe7d9fc047bb0dab40f9d55870d4520c1f3
85a4151d790ab32d5321c6e71748b2446032e1775aedd0168be25f76bf4fe93f
ef6fe4140001cb099968acd5772452859adbe7b57496389fbbf2342f9047b962

4d35ae9669db428b72b1aaadd21dbed44ad2fc678efc8110d89ff723e0497406

4a932ccc8a45db6897a11de118cdbf67062569112f1caa69793669c5c24be708

104e3ea9a190ba039488f5200824fe883b98f6fe01d05a1b55e15ed2199c807a

a4a95807f1c5b200d5d94e3e811a7c4af2d0d9ca88ca4d7f9d02015574f4716f

2ae805b68d7408cc40ad058bc0b8b2b5c29d77760084a5230448e47cec1c43f4

95995686b9af8b56c3fed1dadccf8b2ed5f417bb4eb8947a406a6e943cca33c6

88f2d42bf225c930bc644f82bbd229e170d53dd1072e846e2883265a7ac33301

844cc1807cc5b628b7aa807ef3b682d051c8ad5427df3d3e36c7e7633bfc5768

dfc86b375e974b3092bbff41eb24db3281fb4fc104f1043a7afbf95f85a2c1d5

e3ba85e0bc978013b145ebb4c2d583b33422da93787ab8fb2185b55478652d91

2f182a6cb72712c340c2adb43843cfccb5916d236485de1c62fb40c883570824

bd0ea597f24bb72f8db34b6b6d2c0bc70eb53df9eae40cdb216a13521145ab03

0891588667da40da58ffaa8fedcddb0a9a172646ec12e6d0b9ce2acc2caa302b

2847ae693533406defecb226bfe6d62dd36905ff07add4e773426bde83e85ddc

Hostname

Value
packinstall.kozow.com
dfgtjytdfs.work.gd
puffypuf.gleeze.com
trompadiom.tutotame.bigbox.info
moreover.lostgumball.com
mumucnc.kozow.com
clientrun.compuinter.com
li4858member.possessed.us
enforcer.mywire.org
xfgjgjkuykykgihguifdt.mywire.org
kjskrvmwerffssd.kozow.com
speddot.seburn.net
terminal.ooguy.com

gopremium.mooo.com
founderside.joseulloa.cl
vrrumover0.vrrum0.farted.net
changepassword.giize.com

External References

- https://otx.alienvault.com/pulse/66b39de921cdfe8b6ebcc220