Jun 10 2023

NETMANAGEIT

Intelligence Report

Recent Satacom campaign delivers cryptocurrency-stealing addon

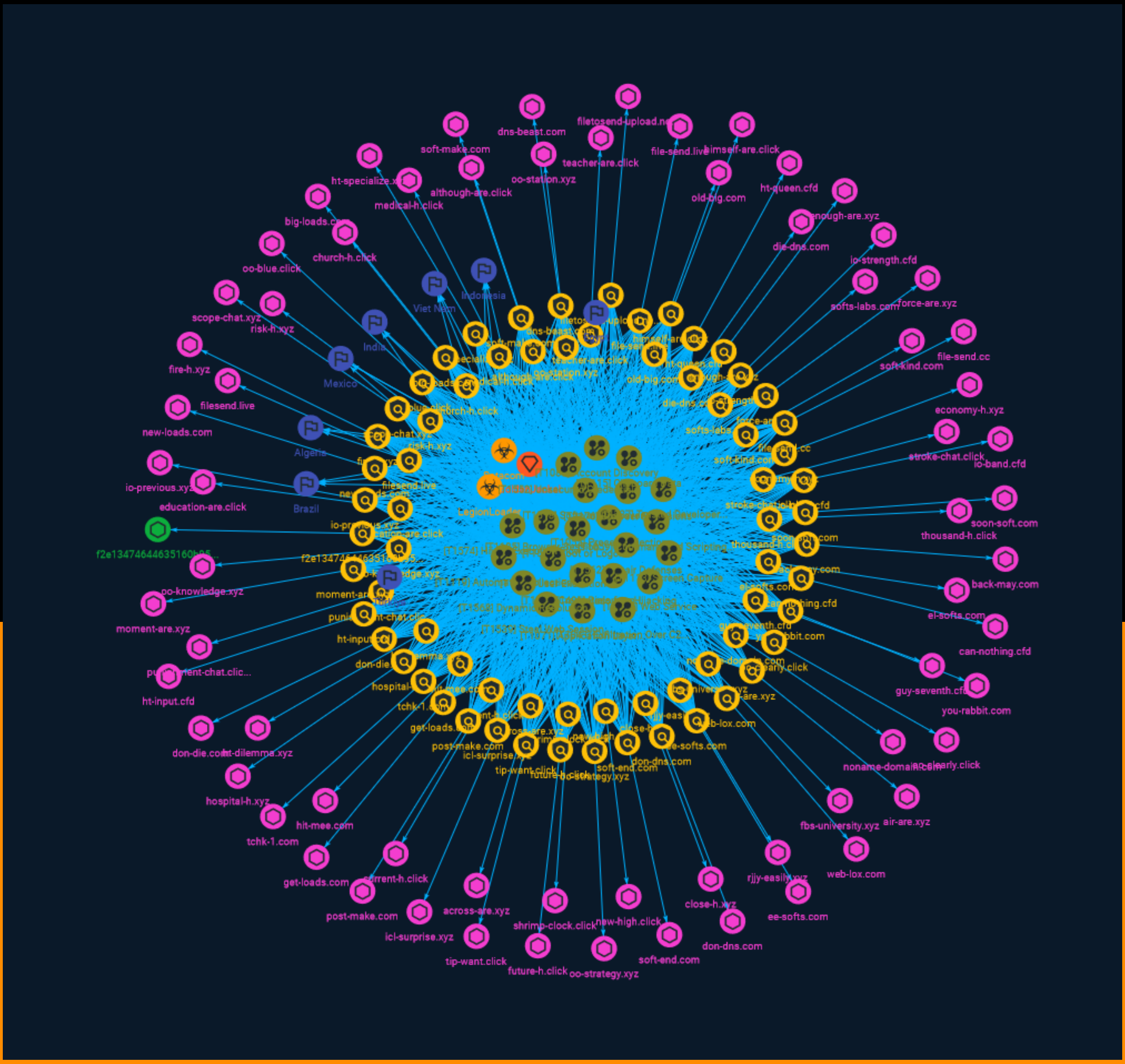

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Satacom downloader, also known as LegionLoader, is a renowned malware family that emerged in 2019. It is known to use the technique of querying DNS servers to obtain the base64-encoded URL in order to receive the next stage of another malware family currently distributed by Satacom. The main purpose of the malware that is dropped by the Satacom downloader is to steal BTC from the victim's account by performing web injections into targeted cryptocurrency websites.

Confidence

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

15 / 100

Attack-Pattern

Name

Boot or Logon Autostart Execution

ID

T1547

Description

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

Name

Browser Session Hijacking

ID

T1185

Description

Adversaries may take advantage of security vulnerabilities and inherent functionality in browser software to change content, modify user-behaviors, and intercept information as part of various browser session hijacking techniques.(Citation: Wikipedia Man in the Browser) A specific example is when an adversary injects software into a browser that allows them to inherit cookies, HTTP sessions, and SSL client certificates of a user then use the browser as a way to pivot into an authenticated intranet.(Citation: Cobalt Strike Browser Pivot)(Citation: ICEBRG Chrome Extensions) Executing browser-based behaviors such as pivoting may require specific process permissions, such as `SeDebugPrivilege` and/or high-integrity/administrator rights. Another example involves pivoting browser traffic from the adversary's browser through the user's browser by setting up a proxy which will redirect web traffic. This does not alter the user's traffic in any way, and the proxy connection can be severed as soon as the browser is closed. The adversary assumes the security context of whichever browser process the proxy is injected into. Browsers typically create a new process for each tab that is opened and permissions and certificates are separated accordingly. With these permissions, an adversary could potentially browse to any resource on an intranet, such as [Sharepoint](https://attack.mitre.org/techniques/T1213/002) or webmail, that is accessible through the browser and which the browser has sufficient permissions. Browser pivoting may also bypass security provided by 2-factor authentication.(Citation: cobaltstrike manual)

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

Credentials from Password Stores

ID

T1555

Description

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

Name

Software Discovery

ID

T1518

Description

Adversaries may attempt to get a listing of software and software versions that are installed on a system or in a cloud environment. Adversaries may use the information from [Software Discovery](https://attack.mitre.org/techniques/T1518) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Adversaries may attempt to enumerate software for a variety of reasons, such as figuring out what security measures are present or if the compromised system has a version of software that is vulnerable to [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).

Name

Impair Defenses

ID

T1562

Description

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

Name

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) 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). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

Browser Extensions

ID

T1176

Description

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

Name

Resource Hijacking

ID

T1496

Description

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

Name

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

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution.(Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Steal Web Session Cookie

ID

T1539

Description

An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials. Web applications and services often use session cookies as an authentication token after a user has authenticated to a website. Cookies are often valid for an extended period of time, even if the web application is not actively used. Cookies can be found on disk, in the process memory of the browser, and in network traffic to remote systems. Additionally, other applications on the targets machine might store sensitive authentication cookies in memory (e.g. apps which authenticate to cloud services). Session cookies can be used to bypasses some multi-factor authentication protocols.(Citation: Pass The Cookie) There are several examples of malware targeting cookies from web browsers on the local system.(Citation: Kaspersky TajMahal April 2019)(Citation: Unit 42 Mac Crypto Cookies January 2019) There are also open source frameworks such as Evilginx 2 and Muraena that can gather session cookies through a malicious proxy (ex: [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557)) that can be set up by an adversary and used in phishing campaigns.(Citation: Github evilginx2)(Citation: GitHub Mauraena) After an adversary acquires a valid cookie, they can then perform a [Web Session Cookie](https://attack.mitre.org/techniques/T1550/004) technique to login to the corresponding web application.

Name
Account Discovery
ID
T1087
Description
Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system or within a compromised environment. This information can help adversaries determine which accounts exist, which can aid in follow-on behavior such as brute-forcing, spear-phishing attacks, or account takeovers (e.g., [Valid Accounts](https://attack.mitre.org/techniques/T1078)). Adversaries may use several methods to enumerate accounts, including abuse of existing tools, built-in commands, and potential misconfigurations that leak account names and roles or permissions in the targeted environment. For examples, cloud environments typically provide easily accessible interfaces to obtain user lists. On hosts, adversaries can use default [PowerShell](https://attack.mitre.org/techniques/T1059/001) and other command line functionality to identify accounts. Information about email addresses and accounts may also be extracted by searching an infected system’s files.

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).

Name

Automated Collection

ID

T1119

Description

Once established within a system or network, an adversary may use automated techniques for collecting internal data. Methods for performing this technique could include use of a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) to search for and copy information fitting set criteria such as file type, location, or name at specific time intervals. In cloud-based environments, adversaries may also use cloud APIs, command line interfaces, or extract, transform, and load (ETL) services to automatically collect data. This functionality could also be built into remote access tools. This technique may incorporate use of other techniques such as [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) and [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570) to identify and move files, as well as [Cloud Service Dashboard](https://attack.mitre.org/techniques/T1538) and [Cloud Storage Object Discovery](https://attack.mitre.org/techniques/T1619) to identify resources in cloud environments.

Name

Trusted Developer Utilities Proxy Execution

ID

T1127

Description

Adversaries may take advantage of trusted developer utilities to proxy execution of malicious payloads. There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering.(Citation: engima0x3 DNX Bypass)(Citation: engima0x3 RCSI Bypass)(Citation: Exploit Monday WinDbg)(Citation: LOLBAS Tracker) These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted process that effectively bypasses application control solutions.

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

Unsecured Credentials

ID

T1552

Description

Adversaries may search compromised systems to find and obtain insecurely stored credentials. These credentials can be stored and/or misplaced in many locations on a system, including plaintext files (e.g. [Bash History](https://attack.mitre.org/techniques/T1552/003)), operating system or application-specific repositories (e.g. [Credentials in Registry](https://attack.mitre.org/techniques/T1552/002)), or other specialized files/artifacts (e.g. [Private Keys](https://attack.mitre.org/techniques/T1552/004)).

Name

Screen Capture

ID

T1113

Description

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as `CopyFromScreen`, `xwd`, or `screencapture`.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

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)

Name

Clipboard Data

ID

T1115

Description

Adversaries may collect data stored in the clipboard from users copying information within or between applications. For example, on Windows adversaries can access clipboard data by using `clip.exe` or `Get-Clipboard`.(Citation: MSDN Clipboard)(Citation: clip_win_server)(Citation: CISA_AA21_200B) Additionally, adversaries may monitor then replace users’ clipboard with their data (e.g., [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002)).(Citation: mining_ruby_reversinglabs) macOS and Linux also have commands, such as `pbpaste`, to grab clipboard contents.(Citation: Operating with EmPyre)

Name

Exfiltration Over C2 Channel

ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Indicator

Name
stroke-chat.click
Pattern Type
stix
Pattern
[domain-name:value = 'stroke-chat.click']
Name
current-h.click
Pattern Type
stix
Pattern
[domain-name:value = 'current-h.click']
Name
although-are.click

Pattern Type
stix
Pattern
[domain-name:value = 'although-are.click']
Name
noname-domain.com
Pattern Type
stix
Pattern
[domain-name:value = 'noname-domain.com']
Name
punishment-chat.click
Pattern Type
stix
Pattern
[domain-name:value = 'punishment-chat.click']
Name
die-dns.com

Pattern Type

stix

Pattern

[domain-name:value = 'die-dns.com']

Name

new-high.click

Pattern Type

stix

Pattern

[domain-name:value = 'new-high.click']

Name

risk-h.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'risk-h.xyz']

Name

el-softs.com

Pattern Type

stix

Pattern

[domain-name:value = 'el-softs.com']

Name

hit-mee.com

Pattern Type

stix

Pattern

[domain-name:value = 'hit-mee.com']

Name

teacher-are.click

Pattern Type

stix

Pattern

[domain-name:value = 'teacher-are.click']

Name

rjjy-easily.xyz

Pattern Type
stix
Pattern
[domain-name:value = 'rjjy-easily.xyz']
Name
education-are.click
Pattern Type
stix
Pattern
[domain-name:value = 'education-are.click']
Name
softs-labs.com
Pattern Type
stix
Pattern
[domain-name:value = 'softs-labs.com']
Name
across-are.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'across-are.xyz']

Name

church-h.click

Pattern Type

stix

Pattern

[domain-name:value = 'church-h.click']

Name

guy-seventh.cfd

Pattern Type

stix

Pattern

[domain-name:value = 'guy-seventh.cfd']

Name

oo-knowledge.xyz

Pattern Type	stix
Pattern	[domain-name:value = 'oo-knowledge.xyz']
Name	old-big.com
Pattern Type	stix
Pattern	[domain-name:value = 'old-big.com']
Name	close-h.xyz
Pattern Type	stix
Pattern	[domain-name:value = 'close-h.xyz']
Name	fire-h.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'fire-h.xyz']

Name

thousand-h.click

Pattern Type

stix

Pattern

[domain-name:value = 'thousand-h.click']

Name

post-make.com

Pattern Type

stix

Pattern

[domain-name:value = 'post-make.com']

Name

oo-station.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'oo-station.xyz']

Name

fbs-university.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'fbs-university.xyz']

Name

moment-are.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'moment-are.xyz']

Name

io-strength.cfd

Pattern Type

stix

Pattern

[domain-name:value = 'io-strength.cfd']

Name

shrimp-clock.click

Pattern Type

stix

Pattern

[domain-name:value = 'shrimp-clock.click']

Name

oo-blue.click

Pattern Type

stix

Pattern

[domain-name:value = 'oo-blue.click']

Name

back-may.com

Pattern Type

stix

Pattern

[domain-name:value = 'back-may.com']

Name

ht-dilemma.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'ht-dilemma.xyz']

Name

file-send.live

Pattern Type

stix

Pattern

[domain-name:value = 'file-send.live']

Name

ee-softs.com

Pattern Type

stix

Pattern

[domain-name:value = 'ee-softs.com']

Name

filesend.live

Pattern Type

stix

Pattern

[domain-name:value = 'filesend.live']

Name

soft-kind.com

Pattern Type

stix

Pattern

[domain-name:value = 'soft-kind.com']

Name

tip-want.click

Pattern Type

stix

Pattern

[domain-name:value = 'tip-want.click']

Name

ht-specialize.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'ht-specialize.xyz']

Name

you-rabbit.com

Pattern Type

stix

Pattern

[domain-name:value = 'you-rabbit.com']

Name

don-die.com

Pattern Type

stix

Pattern

[domain-name:value = 'don-die.com']

Name

ht-queen.cfd

Pattern Type

stix

Pattern

[domain-name:value = 'ht-queen.cfd']

Name

soft-end.com

Pattern Type

stix

Pattern

[domain-name:value = 'soft-end.com']

Name

scope-chat.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'scope-chat.xyz']

Name

io-band.cfd

Pattern Type

stix

Pattern

[domain-name:value = 'io-band.cfd']

Name

get-loads.com

Pattern Type

stix

Pattern

[domain-name:value = 'get-loads.com']

Name

dns-beast.com

Pattern Type
stix
Pattern
[domain-name:value = 'dns-beast.com']
Name
air-are.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'air-are.xyz']
Name
f2e13474644635160b9534db20d60ccc625e0cd6e3aceb1e5e706b75f82d3ecc
Description
Win32:Evo-gen\ [Trj] SHA256 of 199017082159b23decdf63b22e07a7a1
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = 'f2e13474644635160b9534db20d60ccc625e0cd6e3aceb1e5e706b75f82d3ecc']

Name

force-are.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'force-are.xyz']

Name

future-h.click

Pattern Type

stix

Pattern

[domain-name:value = 'future-h.click']

Name

medical-h.click

Pattern Type

stix

Pattern
[domain-name:value = 'medical-h.click']

Name
can-nothing.cfd

Pattern Type
stix

Pattern
[domain-name:value = 'can-nothing.cfd']

Name
hospital-h.xyz

Pattern Type
stix

Pattern
[domain-name:value = 'hospital-h.xyz']

Name
himself-are.click

Pattern Type
stix

Pattern
[domain-name:value = 'himself-are.click']

Name
don-dns.com

Pattern Type
stix

Pattern
[domain-name:value = 'don-dns.com']

Name
new-loads.com

Pattern Type
stix

Pattern
[domain-name:value = 'new-loads.com']

Name
economy-h.xyz

Pattern Type
stix

Pattern

[domain-name:value = 'economy-h.xyz']

Name

icl-surprise.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'icl-surprise.xyz']

Name

soft-make.com

Pattern Type

stix

Pattern

[domain-name:value = 'soft-make.com']

Name

oo-clearly.click

Pattern Type

stix

Pattern

[domain-name:value = 'oo-clearly.click']

Name

ht-input.cfd

Pattern Type

stix

Pattern

[domain-name:value = 'ht-input.cfd']

Name

enough-are.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'enough-are.xyz']

Name

oo-strategy.xyz

Pattern Type

stix

Pattern
[domain-name:value = 'oo-strategy.xyz']
Name
big-loads.com
Pattern Type
stix
Pattern
[domain-name:value = 'big-loads.com']
Name
soon-soft.com
Pattern Type
stix
Pattern
[domain-name:value = 'soon-soft.com']
Name
tchk-1.com
Pattern Type
stix

Pattern

[domain-name:value = 'tchk-1.com']

Name

filetosend-upload.net

Pattern Type

stix

Pattern

[domain-name:value = 'filetosend-upload.net']

Name

web-lox.com

Pattern Type

stix

Pattern

[domain-name:value = 'web-lox.com']

Name

io-previous.xyz

Pattern Type

stix

Pattern
[domain-name:value = 'io-previous.xyz']

Name
file-send.cc

Pattern Type
stix

Pattern
[domain-name:value = 'file-send.cc']

Intrusion-Set

Name
GoldenJackal

Country

Name
Brazil

Name
India

Name
Egypt

Name
Algeria

Name
Viet Nam

Name
Türkiye

Name
Mexico

Name
Indonesia

Malware

Name
LegionLoader

Name
Satacom

Domain-Name

Value
new-high.click
filesend.live
old-big.com
stroke-chat.click
ht-dilemma.xyz
back-may.com
future-h.click
hospital-h.xyz
file-send.cc
ht-queen.cfd
big-loads.com
oo-blue.click
medical-h.click

can-nothing.cfd
risk-h.xyz
oo-clearly.click
icl-surprise.xyz
church-h.click
new-loads.com
file-send.live
ht-input.cfd
rjjy-easily.xyz
soft-end.com
ee-softs.com
die-dns.com
enough-are.xyz
soft-make.com
current-h.click
punishment-chat.click
dns-beast.com
don-die.com

don-dns.com
io-band.cfd
tip-want.click
although-are.click
io-previous.xyz
you-rabbit.com
soon-soft.com
hit-mee.com
teacher-are.click
noname-domain.com
ht-specialize.xyz
guy-seventh.cfd
across-are.xyz
tchk-1.com
fbs-university.xyz
oo-knowledge.xyz
air-are.xyz
filetosend-upload.net

oo-station.xyz
shrimp-clock.click
web-lox.com
thousand-h.click
himself-are.click
soft-kind.com
close-h.xyz
fire-h.xyz
oo-strategy.xyz
economy-h.xyz
scope-chat.xyz
el-softs.com
moment-are.xyz
get-loads.com
post-make.com
softs-labs.com
force-are.xyz
education-are.click

io-strength.cfd

StixFile

Value
f2e13474644635160b9534db20d60ccc625e0cd6e3aceb1e5e706b75f82d3ecc

External References

- https://otx.alienvault.com/pulse/647e0775cc54787894ba6c87
- https://securelist.com/satacom-delivers-cryptocurrency-stealing-browser-extension/109807/