Sep 25 2023

NETMANAGEIT

Intelligence Report

A multi-ransomware cybercriminal group

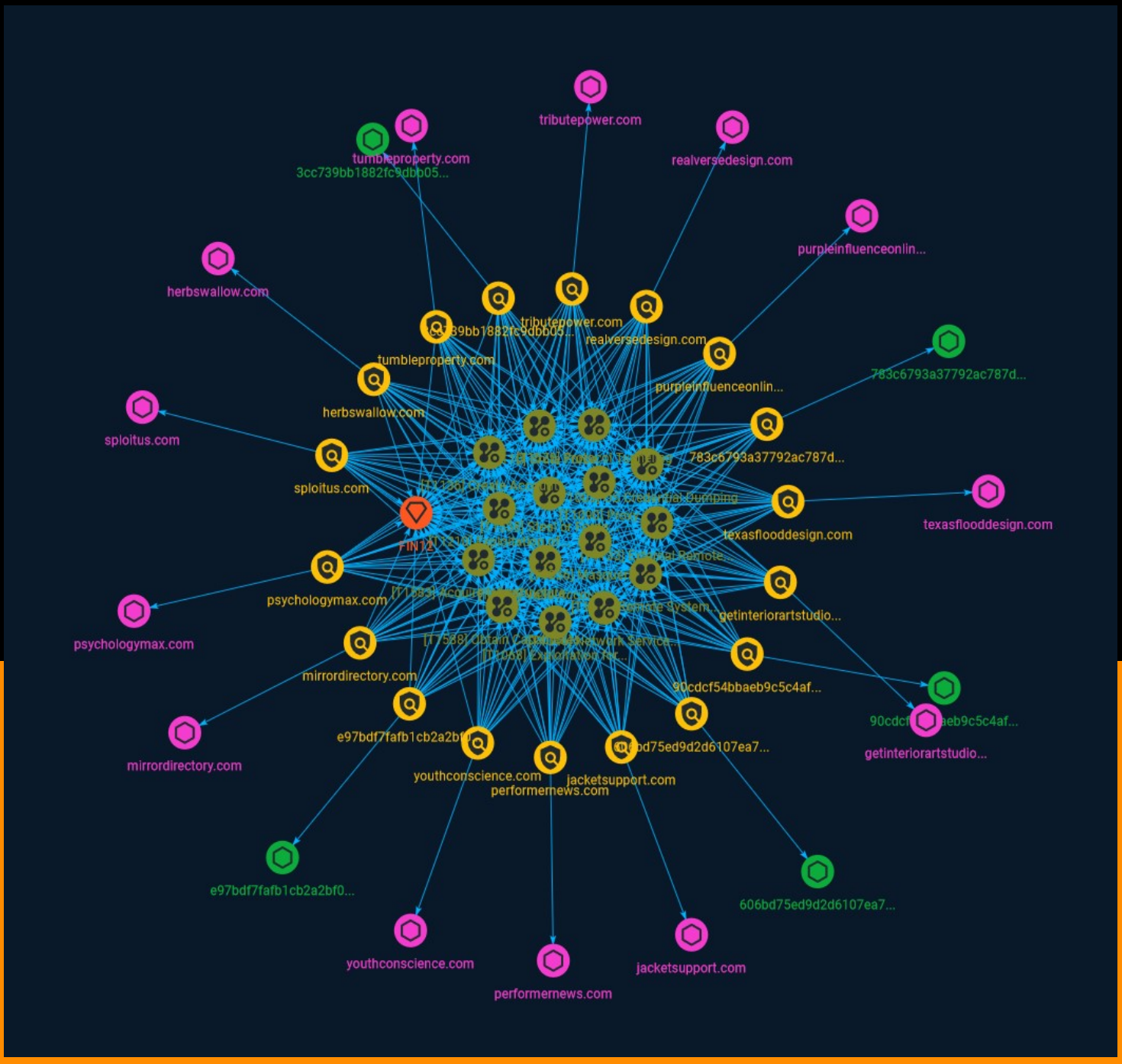

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In March 2023, ANSSI reported to the university hospital in Brest the compromise of one of its servers. The reactivity of the health facility has made it possible to rapidly isolate the Internet's information system (IS) and to hamper the progress of attacker procedures (AMOs) preventing data exfiltration and SI encryption. The discovery of links with a set of incidents observed on the French perimeter and reported in open sources made it possible to link this attack to the FIN12 cybercriminal MOA.

Confidence

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

15 / 100

Attack-Pattern

Name
OS Credential Dumping
ID
T1003
Description
Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.
Name
Valid Accounts
ID
T1078
Description
Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised

credentials 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, network devices, and remote desktop.(Citation: volexity_0day_sophos_FW) Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence. In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account.(Citation: CISA MFA PrintNightmare) The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.(Citation: TechNet Credential Theft)

Name

Brute Force

ID

T1110

Description

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes. Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy Discovery](https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access.

Name

Masquerading

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)

Name

Exploitation of Remote Services

ID

T1210

Description

Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software 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. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system. An adversary may need to determine if the remote system is in a vulnerable state, which may be done through [Network Service Discovery](https://attack.mitre.org/techniques/T1046) or other Discovery methods looking for common, vulnerable software that may be deployed in the network, the lack of certain patches that may indicate vulnerabilities, or security software that may be used to detect or contain

remote exploitation. Servers are likely a high value target for lateral movement exploitation, but endpoint systems may also be at risk if they provide an advantage or access to additional resources. There are several well-known vulnerabilities that exist in common services such as SMB (Citation: CIS Multiple SMB Vulnerabilities) and RDP (Citation: NVD CVE-2017-0176) as well as applications that may be used within internal networks such as MySQL (Citation: NVD CVE-2016-6662) and web server services.(Citation: NVD CVE-2014-7169) Depending on the permissions level of the vulnerable remote service an adversary may achieve [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068) as a result of lateral movement exploitation as well.

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

Exploitation for Privilege Escalation

ID

T1068

Description

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software 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. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

Name

Steal or Forge Kerberos Tickets

ID

T1558

Description

Adversaries may attempt to subvert Kerberos authentication by stealing or forging Kerberos tickets to enable [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003). Kerberos is an authentication protocol widely used in modern Windows domain environments. In Kerberos environments, referred to as “realms”, there are three basic participants: client, service, and Key Distribution Center (KDC).(Citation: ADSecurity Kerberos Ring Decoder) Clients request access to a service and through the exchange of Kerberos tickets, originating from KDC, they are granted access after having successfully authenticated. The KDC is responsible for both authentication and ticket granting. Adversaries may attempt to abuse Kerberos by stealing tickets or forging tickets to enable unauthorized access. On Windows, the built-in `klist` utility can be used to list and analyze cached Kerberos tickets.(Citation: Microsoft Klist) Linux systems on Active Directory domains store Kerberos credentials locally in the credential cache file referred to as the "ccache". The credentials are stored in the ccache file while they remain valid and generally while a user's session lasts.(Citation: MIT ccache) On modern Redhat Enterprise Linux systems, and derivative distributions, the System Security Services Daemon (SSSD) handles Kerberos tickets. By default SSSD maintains a copy of the ticket database that can be found in `/var/lib/sss/secrets/secrets.ldb` as well as the corresponding key located in `/var/lib/sss/secrets/.secrets.mkey`. Both files require root access to read. If an adversary is able to access the database and key, the credential cache Kerberos blob can be extracted and converted into a usable Kerberos ccache file that adversaries may use for [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003). The ccache file may also be converted into a Windows format using tools such as Kekeo.(Citation: Linux Kerberos Tickets)(Citation: Brining MimiKatz to Unix)(Citation: Kekeo) Kerberos tickets on macOS are stored in a standard ccache format, similar to Linux. By default, access to these ccache entries is federated through the KCM daemon process via the Mach RPC protocol, which uses the caller's environment to determine access. The storage location for these ccache entries is influenced by the `/etc/krb5.conf` configuration file and the `KRB5CCNAME` environment variable which can specify to save them to disk or keep them protected via the KCM daemon. Users can interact with ticket storage using `kinit`, `klist`, `ktutil`, and `kcc` built-in binaries or via Apple's native Kerberos framework. Adversaries can use open source tools to interact with the ccache files directly or to use the Kerberos framework to call lower-level APIs for extracting the user's TGT or Service Tickets.(Citation: SpectorOps Bifrost Kerberos macOS 2019)(Citation: macOS kerberos framework MIT)

Name

Remote System Discovery

ID

T1018

Description

Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as [Ping](https://attack.mitre.org/software/S0097) or `net view` using [Net](https://attack.mitre.org/software/S0039). Adversaries may also analyze data from local host files (ex: `C:\Windows\System32\Drivers\etc\hosts` or `/etc/hosts`) or other passive means (such as local [Arp](https://attack.mitre.org/software/S0099) cache entries) in order to discover the presence of remote systems in an environment. Adversaries may also target discovery of network infrastructure as well as leverage [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands on network devices to gather detailed information about systems within a network (e.g. `show cdp neighbors`, `show arp`).(Citation: US-CERT-TA18-106A)(Citation: CISA AR21-126A FIVEHANDS May 2021)

Name

Acquire Infrastructure

ID

T1583

Description

Adversaries may buy, lease, or rent 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) 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).(Citation: amnesty_nso_pegasus) 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

Protocol Tunneling

ID

T1572

Description

Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection/network filtering and/or enable access to otherwise unreachable systems. Tunneling involves explicitly encapsulating a protocol within another. This behavior may conceal malicious traffic by blending in with existing traffic and/or provide an outer layer of encryption (similar to a VPN). Tunneling could also enable routing of network packets that would otherwise not reach their intended destination, such as SMB, RDP, or other traffic that would be filtered by network appliances or not routed over the Internet. There are various means to encapsulate a protocol within another protocol. For example, adversaries may perform SSH tunneling (also known as SSH port forwarding), which involves forwarding arbitrary data over an encrypted SSH tunnel. (Citation: SSH Tunneling) [Protocol Tunneling](https://attack.mitre.org/techniques/T1572) may also be abused by adversaries during [Dynamic Resolution](https://attack.mitre.org/techniques/T1568). Known as DNS over HTTPS (DoH), queries to resolve C2 infrastructure may be encapsulated within encrypted HTTPS packets.(Citation: BleepingComp Godlua JUL19) Adversaries may also leverage [Protocol Tunneling](https://attack.mitre.org/techniques/T1572) in conjunction with [Proxy](https://attack.mitre.org/techniques/T1090) and/or [Protocol Impersonation](https://attack.mitre.org/techniques/T1001/003) to further conceal C2 communications and infrastructure.

Name

Network Service Discovery

ID

T1046

Description

Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port and/or vulnerability scans using tools that are brought onto a system.(Citation: CISA AR21-126A FIVEHANDS May 2021) Within cloud environments, adversaries may attempt to discover services running on other cloud hosts. Additionally, if the cloud environment is connected to a on-premises environment, adversaries may be able to identify services running on non-cloud systems as well. Within macOS environments, adversaries may use the native Bonjour application to discover services running on other macOS hosts within a network. The Bonjour mDNSResponder daemon automatically registers and advertises a host's registered services on the network. For example, adversaries can use a mDNS query (such as `dns-sd -B _ssh._tcp .`) to find other systems broadcasting the ssh service.(Citation: apple doco bonjour description)(Citation: macOS APT Activity Bradley)

Name

Create Account

ID

T1136

Description

Adversaries may create an account to maintain access to victim systems. With a sufficient level of access, creating such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system. Accounts may be created on the local system or within a domain or cloud tenant. In cloud environments, adversaries may create accounts that only have access to specific services, which can reduce the chance of detection.

Name

External Remote Services

ID

T1133

Description

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management] (https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

Name

Obtain Capabilities

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)

Indicator

Name
tumbleproperty.com
Pattern Type
stix
Pattern
[domain-name:value = 'tumbleproperty.com']
Name
getinteriorartstudio.com
Pattern Type
stix
Pattern
[domain-name:value = 'getinteriorartstudio.com']
Name
mirrordirectory.com

Pattern Type
stix
Pattern
[domain-name:value = 'mirrordirectory.com']
Name
realversedesign.com
Pattern Type
stix
Pattern
[domain-name:value = 'realversedesign.com']
Name
jacketsupport.com
Pattern Type
stix
Pattern
[domain-name:value = 'jacketsupport.com']
Name
sploitus.com

Pattern Type

stix

Pattern

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

Name

783c6793a37792ac787dfb45005ca178506e56c9d9f33e8db0924b57a97c2530

Description

SHA256 of 536734aa6ec0f0b1ba8e43088edc6857eca42667

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '783c6793a37792ac787dfb45005ca178506e56c9d9f33e8db0924b57a97c2530']

Name

youthconscience.com

Pattern Type

stix

Pattern

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

Name

3cc739bb1882fc9dbb056f39ebe4965771aeca0ceb44e85da39d1ba7dade693f

Description

ALF:Trojan:Win32/Cevarast.A SHA256 of 8291929d6f3ede6ec025c21d1559a7fe9d30a9ce

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3cc739bb1882fc9dbb056f39ebe4965771aeca0ceb44e85da39d1ba7dade693f']

Name

90cdcf54bbaeb9c5c4afc9b74b48b13e293746ee8858c033fc9d365fd4074018

Description

SHA256 of 1e0ec6994400413c7899cd5c59bdbd6397dea7b5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '90cdcf54bbaeb9c5c4afc9b74b48b13e293746ee8858c033fc9d365fd4074018']

Name
psychologymax.com
Pattern Type
stix
Pattern
[domain-name:value = 'psychologymax.com']
Name
purpleinfluenceonline.com
Pattern Type
stix
Pattern
[domain-name:value = 'purpleinfluenceonline.com']
Name
performernews.com
Pattern Type
stix
Pattern
[domain-name:value = 'performernews.com']

Name
herbswallow.com
Pattern Type
stix
Pattern
[domain-name:value = 'herbswallow.com']
Name
texasflooddesign.com
Pattern Type
stix
Pattern
[domain-name:value = 'texasflooddesign.com']
Name
e97bdf7fafb1cb2a2bf0a4e14f51e18a34f3ff2f6f7b99731e93070d50801bef
Description
ConventionEngine_Term_Desktop SHA256 of 28400c267815762e49c200e8b481a592c67f9cf7
Pattern Type
stix

Pattern

[file:hashes.'SHA-256' = 'e97bdf7fafb1cb2a2bf0a4e14f51e18a34f3ff2f6f7b99731e93070d50801bef']

Name

tributepower.com

Pattern Type

stix

Pattern

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

Name

606bd75ed9d2d6107ea7ee67063d1761a99f2fb5e932c8344d11395d24587dd6

Description

#Lowfi:HSTR:VirTool:MSIL/GeneralPacker.E SHA256 of 292629c6ab33bddf123d26328025e2d157d9e8fc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '606bd75ed9d2d6107ea7ee67063d1761a99f2fb5e932c8344d11395d24587dd6']

Intrusion-Set

Name
FIN12

Domain-Name

Value
performernews.com
tributepower.com
sploitus.com
texasflooddesign.com
youthconscience.com
jacketsupport.com
tumbleproperty.com
getinteriorartstudio.com
herbswallow.com
realversedesign.com
purpleinfluenceonline.com
mirrordirectory.com
psychologymax.com

StixFile

Value
e97bdf7fafb1cb2a2bf0a4e14f51e18a34f3ff2f6f7b99731e93070d50801bef
783c6793a37792ac787dfb45005ca178506e56c9d9f33e8db0924b57a97c2530
3cc739bb1882fc9dbb056f39ebe4965771aeca0ceb44e85da39d1ba7dade693f
90cdcf54bbaeb9c5c4afc9b74b48b13e293746ee8858c033fc9d365fd4074018
606bd75ed9d2d6107ea7ee67063d1761a99f2fb5e932c8344d11395d24587dd6

External References

- https://otx.alienvault.com/pulse/6511e8782e1cee84a0784001
- https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-007.pdf
- https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-007/