Mar 26 2024

NETMANAGEIT

Intelligence Report

Tycoon 2FA: an in-depth analysis of the latest version of the phishing kit

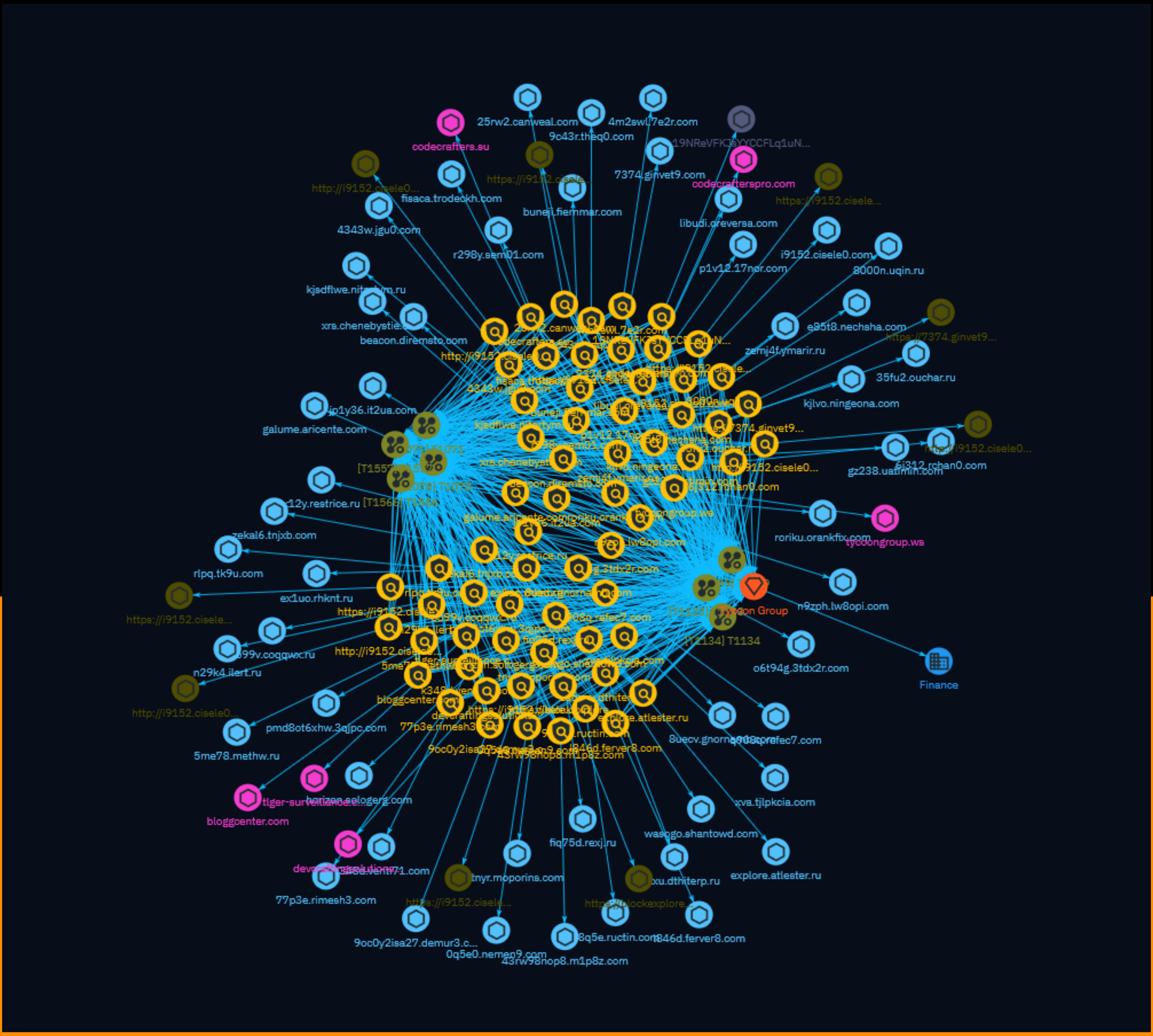

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This report provides an in-depth analysis of Tycoon 2FA, an Adversary-in-The-Middle phishing kit distributed as a Phishing-as-a-Service platform. It became widespread since August 2023 and is currently massively used in phishing campaigns mainly targeting Microsoft 365 accounts. Our analysis revealed recent changes enhancing its stealth capabilities. We identified tracking opportunities to monitor this threat and will continue investigating Tycoon 2FA infrastructure.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
zemj4f.ymarir.ru
Pattern Type
stix
Pattern
[hostname:value = 'zemj4f.ymarir.ru']
Name
zekal6.tnjxb.com
Pattern Type
stix
Pattern
[hostname:value = 'zekal6.tnjxb.com']
Name
zaqaxu.dthiterp.ru

Pattern Type

stix

Pattern

[hostname:value = 'zaqaxu.dthiterp.ru']

Name

xva.tjlpkcia.com

Pattern Type

stix

Pattern

[hostname:value = 'xva.tjlpkcia.com']

Name

xrs.chenebystie.com

Pattern Type

stix

Pattern

[hostname:value = 'xrs.chenebystie.com']

Name

x12y.restrice.ru

Pattern Type

stix

Pattern

[hostname:value = 'x12y.restrice.ru']

Name

wasogo.shantowd.com

Pattern Type

stix

Pattern

[hostname:value = 'wasogo.shantowd.com']

Name

tnyr.moporins.com

Pattern Type

stix

Pattern

[hostname:value = 'tnyr.moporins.com']

Name

roriku.orankfix.com

Pattern Type

stix

Pattern

[hostname:value = 'roriku.orankfix.com']

Name

rlpq.tk9u.com

Pattern Type

stix

Pattern

[hostname:value = 'rlpq.tk9u.com']

Name

r298y.sem01.com

Pattern Type

stix

Pattern

[hostname:value = 'r298y.sem01.com']

Name

pmd8ot6xhw.3qjpc.com

Pattern Type

stix

Pattern

[hostname:value = 'pmd8ot6xhw.3qjpc.com']

Name

q908q.refec7.com

Pattern Type

stix

Pattern

[hostname:value = 'q908q.refec7.com']

Name

p1v12.17nor.com

Pattern Type

stix

Pattern

[hostname:value = 'p1v12.17nor.com']

Name

oo99v.coqqwx.ru

Pattern Type

stix

Pattern

[hostname:value = 'oo99v.coqqwx.ru']

Name

o6t94g.3tdx2r.com

Pattern Type

stix

Pattern

[hostname:value = 'o6t94g.3tdx2r.com']

Name

n9zph.lw8opi.com

Pattern Type

stix

Pattern

[hostname:value = 'n9zph.lw8opi.com']

Name

n29k4.ilert.ru

Pattern Type

stix

Pattern

[hostname:value = 'n29k4.ilert.ru']

Name

libudi.oreversa.com

Pattern Type

stix

Pattern

[hostname:value = 'libudi.oreversa.com']

Name

l846d.ferver8.com

Pattern Type

stix

Pattern

[hostname:value = 'l846d.ferver8.com']

Name

kjsdflwe.nitertym.ru

Pattern Type

stix

Pattern

[hostname:value = 'kjsdflwe.nitertym.ru']

Name

kjlvo.ningeona.com

Pattern Type

stix

Pattern

[hostname:value = 'kjlvo.ningeona.com']

Name

k348d.venti71.com

Pattern Type

stix

Pattern

[hostname:value = 'k348d.venti71.com']

Name

i9152.cisele0.com

Pattern Type

stix

Pattern

[hostname:value = 'i9152.cisele0.com']

Name

jp1y36.it2ua.com

Pattern Type

stix

Pattern

[hostname:value = 'jp1y36.it2ua.com']

Name

galume.aricente.com

Pattern Type

stix

Pattern

[hostname:value = 'galume.aricente.com']

Name

gz238.uatimin.com

Pattern Type
stix

Pattern
[hostname:value = 'gz238.uatimin.com']

Name
horizon.sologerg.com

Pattern Type
stix

Pattern
[hostname:value = 'horizon.sologerg.com']

Name
fisaca.trodeckh.com

Pattern Type
stix

Pattern
[hostname:value = 'fisaca.trodeckh.com']

Name
explore.atlester.ru

Pattern Type

stix

Pattern

[hostname:value = 'explore.atlester.ru']

Name

fiq75d.rexj.ru

Pattern Type

stix

Pattern

[hostname:value = 'fiq75d.rexj.ru']

Name

e85t8.nechsha.com

Pattern Type

stix

Pattern

[hostname:value = 'e85t8.nechsha.com']

Name

ex1uo.rhknt.ru

Pattern Type

stix

Pattern

[hostname:value = 'ex1uo.rhknt.ru']

Name

buneji.fiernmar.com

Pattern Type

stix

Pattern

[hostname:value = 'buneji.fiernmar.com']

Name

beacon.diremsto.com

Pattern Type

stix

Pattern

[hostname:value = 'beacon.diremsto.com']

Name

9oc0y2isa27.demur3.com

Pattern Type

stix

Pattern

[hostname:value = '9oc0y2isa27.demur3.com']

Name

9c43r.theq0.com

Pattern Type

stix

Pattern

[hostname:value = '9c43r.theq0.com']

Name

98q5e.ructin.com

Pattern Type

stix

Pattern

[hostname:value = '98q5e.ructin.com']

Name

8uecv.gnornamb.com

Pattern Type

stix

Pattern

[hostname:value = '8uecv.gnornamb.com']

Name

8000n.uqin.ru

Pattern Type

stix

Pattern

[hostname:value = '8000n.uqin.ru']

Name

77p3e.rimesh3.com

Pattern Type

stix

Pattern

[hostname:value = '77p3e.rimesh3.com']

Name

7374.ginvet9.com

Pattern Type
stix
Pattern
[hostname:value = '7374.ginvet9.com']
Name
6j312.rchan0.com
Pattern Type
stix
Pattern
[hostname:value = '6j312.rchan0.com']
Name
5me78.methw.ru
Pattern Type
stix
Pattern
[hostname:value = '5me78.methw.ru']
Name
4m2swl.7e2r.com

Pattern Type
stix
Pattern
[hostname:value = '4m2swl.7e2r.com']
Name
43rw98nop8.m1p8z.com
Pattern Type
stix
Pattern
[hostname:value = '43rw98nop8.m1p8z.com']
Name
4343w.jgu0.com
Pattern Type
stix
Pattern
[hostname:value = '4343w.jgu0.com']
Name
35fu2.ouchar.ru

Pattern Type

stix

Pattern

[hostname:value = '35fu2.ouchar.ru']

Name

0q5e0.nemen9.com

Pattern Type

stix

Pattern

[hostname:value = '0q5e0.nemen9.com']

Name

25rw2.canweal.com

Pattern Type

stix

Pattern

[hostname:value = '25rw2.canweal.com']

Name

tycoongroup.ws

Pattern Type

stix

Pattern

[domain-name:value = 'tycoongroup.ws']

Name

tlger-surveillance.com

Pattern Type

stix

Pattern

[domain-name:value = 'tlger-surveillance.com']

Name

codecrafterspro.com

Pattern Type

stix

Pattern

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

Name

devcraftingsolutions.com

Pattern Type

stix

Pattern

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

Name

codecrafters.su

Pattern Type

stix

Pattern

[domain-name:value = 'codecrafters.su']

Name

https://i9152.cisele0.com/NOZcbtTxxEiGj/X

Pattern Type

stix

Pattern

[url:value = 'https://i9152.cisele0.com/NOZcbtTxxEiGj/X']

Name

bloggcenter.com

Pattern Type

stix

Pattern

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

Name

https://i9152.cisele0.com/NOZcbtTxxEiGj/?r

Pattern Type

stix

Pattern

[url:value = 'https://i9152.cisele0.com/NOZcbtTxxEiGj/?r']

Name

https://i9152.cisele0.com/NOZcbtTxxEiGj/?rr

Pattern Type

stix

Pattern

[url:value = 'https://i9152.cisele0.com/NOZcbtTxxEiGj/?rr']

Name

https://i9152.cisele0.com/NOZcbtTxxEiGj/

Pattern Type

stix

Pattern

[url:value = 'https://i9152.cisele0.com/NOZcbtTxxEiGj/']

Name

https://7374.ginvet9.com/

Pattern Type

stix

Pattern

[url:value = 'https://7374.ginvet9.com/']

Name

https://blockexplorer.one/bitcoin/mainnet/address/19NReVFKJsYYCCFLq1uNKYrUqQE2bB4Jwx

Pattern Type

stix

Pattern

[url:value = 'https://blockexplorer.one/bitcoin/mainnet/address/19NReVFKJsYYCCFLq1uNKYrUqQE2bB4Jwx']

Name

http://i9152.cisele0.com/web6socket/socket.io/?type=User&appnum=1&EIO=4&transport=websocket

Pattern Type

stix

Pattern

[url:value = 'http://i9152.cisele0.com/web6socket/socket.io/?type=User&appnum=1&EIO=4&transport=websocket']

Name

http://i9152.cisele0.com/lbuakdidnqmytlcBiVbomCGYTSPFFZAABOLJGWUCZHXZKPGZOQRAVFAAF?317727838333203306556902opEXJOOmXGJPZNFTJIXPAAFUILTKKRQQEFFSNIABRZNUPXEUOAKDATDS

Pattern Type

stix

Pattern

[url:value = 'http://i9152.cisele0.com/lbuakdidnqmytlcBiVbomCGYTSPFFZAABOLJGWUCZHXZKPGZOQRAVFAAF?317727838333203306556902opEXJOOmXGJPZNFTJIXPAAFUILTKKRQQEFFSNIABRZNUPXEUOAKDATDS']

Name

http://i9152.cisele0.com/34S7EHRE0DB8QrFfvijoRMsX632e0GRF8rZ89110

Pattern Type

stix

Pattern

[url:value = 'http://i9152.cisele0.com/34S7EHRE0DB8QrFfvijoRMsX632e0GRF8rZ89110']

Name

19NReVFKJsYYCCFLq1uNKYrUqQE2bB4Jwx

Pattern Type

stix

Pattern

[cryptocurrency-wallet:value = '19NReVFKJsYYCCFLq1uNKYrUqQE2bB4Jwx']

Intrusion-Set

Name
Tycoon Group

Attack-Pattern

Name
T1134

ID
T1134

Description
Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token. An adversary can use built-in Windows API functions to copy access tokens from existing processes; this is known as token stealing. These token can then be applied to an existing process (i.e. [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001)) or used to spawn a new process (i.e. [Create Process with Token](https://attack.mitre.org/techniques/T1134/002)). An adversary must already be in a privileged user context (i.e. administrator) to steal a token. However, adversaries commonly use token stealing to elevate their security context from the administrator level to the SYSTEM level. An adversary can then use a token to authenticate to a remote system as the account for that token if the account has appropriate permissions on the remote system.(Citation: Pentestlab Token Manipulation) Any standard user can use the \`runas\` command, and the Windows API functions, to create impersonation tokens; it does not require access to an administrator account. There are also other mechanisms, such as Active Directory fields, that can be used to modify access tokens.

Name

T1078

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

T1559

ID

T1559

Description

Adversaries may abuse inter-process communication (IPC) mechanisms for local code or command execution. IPC is typically used by processes to share data, communicate with each other, or synchronize execution. IPC is also commonly used to avoid situations such as deadlocks, which occurs when processes are stuck in a cyclic waiting pattern. Adversaries may abuse IPC to execute arbitrary code or commands. IPC mechanisms may differ depending on OS, but typically exists in a form accessible through programming languages/libraries or native interfaces such as Windows [Dynamic Data Exchange](https://attack.mitre.org/techniques/T1559/002) or [Component Object Model](https://attack.mitre.org/techniques/T1559/001). Linux environments support several different IPC mechanisms, two of which being sockets and pipes.(Citation: Linux IPC) Higher level execution mediums, such as those of [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059)s, may also leverage underlying IPC mechanisms. Adversaries may also use [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) to facilitate remote IPC execution.(Citation: Fireeye Hunting COM June 2019)

Name

T1566

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

T1071

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

T1133

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

T1557

ID

T1557

Description

Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as [Network Sniffing](https://attack.mitre.org/techniques/T1040), [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002), or replay attacks ([Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212)). By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.(Citation: Rapid7 MiTM Basics) For example, adversaries may manipulate victim DNS settings to enable other malicious activities such as preventing/redirecting users from accessing legitimate sites and/or pushing additional malware.(Citation: ttint_rat)(Citation: dns_changer_trojans)(Citation: ad_blocker_with_miner) Adversaries may also manipulate DNS and leverage their position in order to intercept user credentials and session cookies.(Citation: volexity_0day_sophos_FW) [Downgrade Attack](https://attack.mitre.org/techniques/T1562/010)s can also be used to establish an AiTM position, such as by negotiating a less secure, deprecated, or weaker version of communication protocol (SSL/TLS) or encryption algorithm.(Citation: mitm_tls_downgrade_att)(Citation:

taxonomy_downgrade_att_tls)(Citation: tlseminar_downgrade_att) Adversaries may also leverage the AiTM position to attempt to monitor and/or modify traffic, such as in [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002). Adversaries can setup a position similar to AiTM to prevent traffic from flowing to the appropriate destination, potentially to [Impair Defenses](https://attack.mitre.org/techniques/T1562) and/or in support of a [Network Denial of Service](https://attack.mitre.org/techniques/T1498).

Sector

Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.

Hostname

Value
zemj4f.ymarir.ru
zaqaxu.dthiterp.ru
zekal6.tnjxb.com
xva.tjlpkcia.com
x12y.restrice.ru
xrs.chenebystie.com
wasogo.shantowd.com
rlpq.tk9u.com
roriku.orankfix.com
tnyr.moporins.com
r298y.sem01.com
q908q.refec7.com
pmd8ot6xhw.3qjpc.com

p1v12.17nor.com
o6t94g.3tdx2r.com
oo99v.coqqwx.ru
n9zph.lw8opi.com
n29k4.ilert.ru
libudi.oreversa.com
l846d.ferver8.com
kjsdflwe.nitertym.ru
kjlvo.ningeona.com
k348d.venti71.com
jp1y36.it2ua.com
i9152.cisele0.com
horizon.sologerg.com
galume.aricente.com
gz238.uatimin.com
fisaca.trodeckh.com
fiq75d.rexj.ru
explore.atlester.ru

ex1uo.rhknt.ru
e85t8.nechsha.com
beacon.diremsto.com
buneji.fiernmar.com
9oc0y2isa27.demur3.com
9c43r.theq0.com
8uecv.gnornamb.com
98q5e.ructin.com
7374.ginvet9.com
8000n.uqin.ru
77p3e.rimesh3.com
6j312.rchan0.com
5me78.methw.ru
4m2swl.7e2r.com
35fu2.ouchar.ru
43rw98nop8.m1p8z.com
4343w.jgu0.com
0q5e0.nemen9.com

25rw2.canweal.com

Domain-Name

Value
tycoongroup.ws
codecrafterspro.com
devcraftingsolutions.com
tlger-surveillance.com
codecrafters.su
bloggcenter.com

Url

Value
https://i9152.cisele0.com/NOZcbtTxxEiGj/X
https://i9152.cisele0.com/NOZcbtTxxEiGj/?rr
https://i9152.cisele0.com/NOZcbtTxxEiGj/?r
https://i9152.cisele0.com/NOZcbtTxxEiGj/
https://blockexplorer.one/bitcoin/mainnet/address/19NReVFKJsYYCCFLq1uNKYrUqQE2bB4Jwx
https://7374.ginvet9.com/
http://i9152.cisele0.com/web6socket/socket.io/?type=User&appnum=1&EIO=4&transport=websocket
http://i9152.cisele0.com/lbuakdidnqmytlcBiVbomCGYTSPFFZAABOLJGWUCZHXZKPGZOQRAVFAAF?317727838333203306556902opEXJOOmXGJPZNFTJIXPAAFUILTKKRQQEFFSNIABRZNUPXEUOAKDATDS
http://i9152.cisele0.com/34S7EHRE0DB8QrFfvijoRMsX632e0GRF8rZ89110

Cryptocurrency-Wallet

Value
19NReVFKJsYYCCFLq1uNKYrUqQE2bB4Jwx

External References

- https://blog.sekoia.io/tycoon-2fa-an-in-depth-analysis-of-the-latest-version-of-the-aitm-phishing-kit/
- https://otx.alienvault.com/pulse/6602e304dfdc004f73c12a6e