Dec 22 2023

NETMANAGEIT

Intelligence Report

CALISTO doxxing: Sekoia.io findings concurs to Reuters' investigation on FSB-related Andrey Korinets

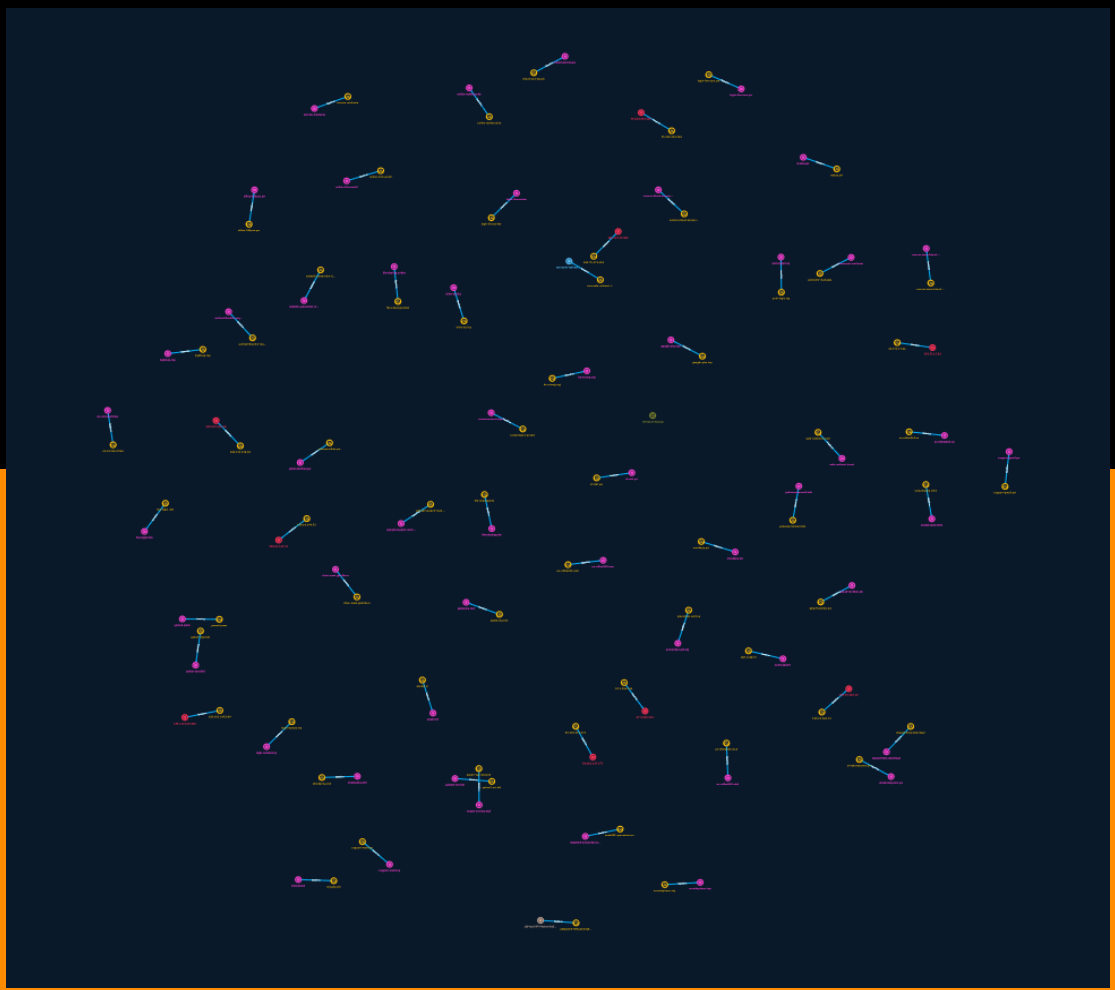

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In the wake of Reuters's sanctions against two Russian nationals, Sekoia.io published a technical investigation that confirmed that Andrey Korinets was linked to a known phishing network.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Phishing
ID
T1566
Description
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Indicator

Name
expert-service.tech
Pattern Type
stix
Pattern
[domain-name:value = 'expert-service.tech']
Name
yahoomailfree.pw
Pattern Type
stix
Pattern
[domain-name:value = 'yahoomailfree.pw']
Name
yahoocentermail.info

Pattern Type
stix
Pattern
[domain-name:value = 'yahoocentermail.info']
Name
sykt.support
Pattern Type
stix
Pattern
[domain-name:value = 'sykt.support']
Name
en-office365.club
Pattern Type
stix
Pattern
[domain-name:value = 'en-office365.club']
Name
185.99.134.22

Description

ISP: Korea **OS:** None ---------- Hostnames: - lt.v76540.com - mkt.v76540.com - mkt.76543k.com - lt.76543y.com - www.v76549.com - m.76543g.com - 76543e.com - mkt.76543j.com - 76543r.com - m.s76542.com - m.s76541.com - mkt.76543n.com - s76541.com - m.v76544.com - m.76545.com - mkt.76540.com - 76542.com - lt.76543x.com - 76548.com - 76543.net - www.s76540.com - 76543p.com - m.76543b.com - www.76543q.com - lt.76543i.com - www.76543u.com - v76548.com - mkt.76543l.com - m.v76549.com - www.76543c.com - m.s76540.com - mkt.v76549.com - 76543o.com - 76543k.com - lt.s76541.com - mkt.76543c.com - 76543j.com - v76549.com - 76543a.com - mkt.76543d.com - lt.76543b.com - lt.76543q.com - 76543b.com - lt.76543f.com - lt.76543u.com - v76542.com - m.76543t.com - mkt.76543app.com - lt.76543r.com - lt.76540.com - lt.76543v.com - m.76543u.com - mkt.76543i.com - lt.76543.net - lt.76541.com - v76541.com - 76545.com - m.76542.com - www.76543.com - www.76545.com - lt.76543w.com - m.76543s.com - 76543f.com - www.76540.com - lt.76543n.com - 76543v.com - mkt.s76540.com - mkt.76543h.com - www.76543i.com - 76543h.com - m.76540.com - lt.76549.com - mkt.76543t.com - mkt.v76546.com - lt.76542.com - 76543x.com - mkt.76543m.com - www.v76546.com - 76543c.com - 76543m.com - mkt.76543.com - lt.76545.com - mkt.76543y.com - www.76543y.com - www.s76542.com - m.76543p.com - m.76543r.com - 76543u.com - s76542.com - www.76543e.com - www.76543o.com - lt.76548.com - v76540.com - m.76543m.com - lt.76543s.com - m.v76541.com - m.76543i.com - m.76543z.com - lt.76543j.com - www.76543d.com - m.76548.com - lt.76543p.com - m.v76542.com - www.76543r.com - m.v76545.com - lt.v76544.com - m.76543h.com - mkt.76543z.com - 76543i.com - www.76543s.com - lt.v76548.com - lt.v76545.com - www.76541.com - lt.v76543.com - www.76549.com - mkt.v76541.com - m.76543x.com - m.76543w.com - 76549.com - www.76542.com - lt.76543a.com - www.76543app.com - lt.76543e.com - www.v76540.com - lt.76543k.com - 76543app.com - www.76543m.com - 76543y.com - mkt.76543s.com - 76543z.com - 76543q.com - v76545.com - www.76543n.com - m.76541.com - mkt.76543x.com - lt.v76542.com - www.76543p.com - 76543.com - m.76543.com - www.76543w.com - m.76543y.com - www.76543f.com - m.76543v.com - lt.v76549.com - lt.76543c.com - mkt.s76541.com - m.76543app.com - www.76548.com - m.76549.com - www.76543z.com - www.76543t.com - v76543.com - lt.76543z.com - lt.76543app.com - mkt.76543q.com - mkt.76543b.com - lt.76543d.com - mkt.76543u.com - mkt.76543f.com - m.76543e.com - 76543d.com - m.v76546.com - mkt.s76542.com - m.v76540.com - 76540.com - mkt.76543r.com - mkt.76543v.com - 76543t.com - mkt.76543g.com - mkt.76541.com - lt.76543g.com - 76541.com - mkt.76549.com - 76543w.com - mkt.76543w.com - www.76543g.com - m.76543n.com - m.76543j.com - v76544.com - mkt.v76548.com - m.76543d.com - m.76543o.com - 76543l.com - lt.s76540.com - 76543n.com - lt.s76542.com - lt.76543h.com - www.76543j.com - m.76543a.com - www.v76547.com - lt.v76546.com - lt.76543t.com - mkt.76542.com - mkt.v76542.com - www.v76543.com - m.76543q.com - www.v76545.com - lt.76543m.com - m.v76547.com - lt.76543.com - mkt.76545.com - v76546.com - m.76543.net - m.76543c.com - m.v76548.com - www.76543h.com - www.76543a.com - www.76543l.com - m.76543l.com - 76543s.com - mkt.76548.com - lt.76543o.com - m.76543k.com - m.v76543.com - www.v76548.com - www.76543.net - mkt.76543p.com - mkt.v76547.com - www.v76544.com - www.76543v.com -

mkt.v76544.com - 76543g.com - m.76543f.com - www.s76541.com - www.v76542.com - www.76543x.com - mkt.v76543.com - lt.76543l.com - mkt.v76545.com - mkt.76543.net - lt.v76541.com - mkt.76543e.com - v76547.com - www.v76541.com - mkt.76543o.com - www.76543b.com - mkt.76543a.com - s76540.com - www.76543k.com - lt.v76547.com ---------- Domains: - v76544.com - 76543v.com - 76543app.com - 76543l.com - 76543y.com - 76543n.com - 76543h.com - 76543e.com - 76543z.com - 76540.com - 76543q.com - v76545.com - s76541.com - 76543x.com - 76543u.com - 76548.com - 76543.net - 76543.com - 76543c.com - 76543p.com - 76543m.com - v76546.com - 76542.com - v76543.com - 76543o.com - s76542.com - 76543k.com - 76543s.com - 76543j.com - 76543a.com - v76540.com - 76543b.com - 76543d.com - 76543r.com - v76548.com - v76549.com - 76543g.com - 76543t.com - v76542.com - v76541.com - 76545.com - 76541.com - 76543w.com - v76547.com - 76543f.com - 76549.com - s76540.com - 76543i.com ---------- Services: **80:** ``` HTTP/1.1 301 Moved Permanently Server: nginx Date: Tue, 19 Dec 2023 14:03:56 GMT Content-Type: text/html Content-Length: 178 Connection: keep-alive Location: https://cn.aliyun.com/notfound X-Frame-Options: SAMEORIGIN ``` ---------- **443:** ``` HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 08 Dec 2023 16:18:13 GMT Content-Type: text/html Content-Length: 178 Connection: keep-alive Location: https://cn.aliyun.com/notfound X-Frame-Options: SAMEORIGIN ``` HEARTBLEED: 2023/12/08 16:18:47 185.99.134.22:443 - SAFE ---------- **8083:** ``` HTTP/1.1 301 Moved Permanently Server: nginx Date: Sat, 25 Nov 2023 06:08:28 GMT Content-Type: text/html Content-Length: 178 Connection: keep-alive Location: https://cn.aliyun.com/notfound X-Frame-Options: SAMEORIGIN ``` HEARTBLEED: 2023/11/25 06:08:43 185.99.134.22:8083 - SAFE ---------- **8085:** ``` HTTP/1.1 301 Moved Permanently Server: nginx Date: Mon, 11 Dec 2023 13:34:17 GMT Content-Type: text/html Content-Length: 178 Connection: keep-alive Location: https://cn.aliyun.com/notfound X-Frame-Options: SAMEORIGIN ``` HEARTBLEED: 2023/12/11 13:34:42 185.99.134.22:8085 - SAFE ---------- **8086:** ``` HTTP/1.1 400 Bad Request Server: nginx Date: Tue, 19 Dec 2023 01:13:40 GMT Content-Type: text/html; charset=utf-8 Content-Length: 666 Connection: close ``` ---------- **8087:** ``` HTTP/1.1 400 Bad Request Server: nginx Date: Wed, 20 Dec 2023 06:43:10 GMT Content-Type: text/html; charset=utf-8 Content-Length: 166 Connection: close

400 Bad Request

---

nginx

``` ----------
```

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.99.134.22']

Name

86.110.117.172

Description

CC=RU ASN=AS3267 Federal State Institution Federal Scientific Research Institute for System Analysis of the Ru

Pattern Type

stix

Pattern

[ipv4-addr:value = '86.110.117.172']

Name

secure-icloud.accountant

Pattern Type

stix

Pattern

[domain-name:value = 'secure-icloud.accountant']

Name

emailapp.pw

Pattern Type

stix

Pattern

[domain-name:value = 'emailapp.pw']

Name

online-redirect.site

Pattern Type

stix

Pattern

[domain-name:value = 'online-redirect.site']

Name

drive-aoi.icu

Pattern Type

stix

Pattern

[domain-name:value = 'drive-aoi.icu']

Name

37.1.206.114

Description

ISP: Scalaxy B.V. **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDOplhFnxEpb7TIAHlJ3/wSnvubhbQp9f4t+jvdldzzPHJ3tuG414A8HqSCQyIZxY67zqpVapV/jGZH9Y6GbGkxPdynzFKMvM5PFGLEcWHm3KzGwTTuKM/uFq5Y qF81clxXiUodPvLf6pPTYXrflZvlWF9OmkQfQf4T8atPMA0u18r2AMmYzK084hZz2E8NnF6jySqa ENZONSOsqAKeR0KiKhzESesr5K8sAPw3Xb/tj1GBTrtcSelgI6rALQGgpQYNv+D7nPYewK7XoMb/T2VWdzP8BumSmh73BCYBRXpz0o6np7vNpWvRdn9JLQqb3GjPeM+7WOiqoUDTab4l9OvKNXaysBrt MRs/ 4UDnyNVm4MSjqGMLh6JLNSR5gm5tCfAfPfsHTZDASRmDyOiAmWHxOTyxcAeji75jROHgGZxbmo8fZc4+AiRMc348PSulSA3uTrQfCERhHsLOpmcbmsGxyrv5Zobqd1uDEO1B6kwzoZ8w95utmG1z uwIT8uacXnM= Fingerprint: ca:4e:2b:dd:61:20:b3:41:65:bb:01:c3:4a:b2:aa:89 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '37.1.206.114']

Name
auth-login.top
Pattern Type
stix
Pattern
[domain-name:value = 'auth-login.top']
Name
login-access.top
Pattern Type
stix
Pattern
[domain-name:value = 'login-access.top']
Name
safe-redirect.in.net
Pattern Type
stix
Pattern
[domain-name:value = 'safe-redirect.in.net']

Name

google-plus.top

Pattern Type

stix

Pattern

[domain-name:value = 'google-plus.top']

Name

185.72.179.132

Description

CC=DE ASN=AS51417 TBits.net GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.72.179.132']

Name

file-sharing.online

Pattern Type

stix

Pattern

[domain-name:value = 'file-sharing.online']

Name

185.212.128.28

Description

CC=VG ASN=AS200313 IT WEB LTD

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.212.128.28']

Name

hghshop.top

Pattern Type

stix

Pattern

[domain-name:value = 'hghshop.top']

Name

qooqle-support-mail.pw

Pattern Type
stix
Pattern
[domain-name:value = 'qooqle-support-mail.pw']
Name
authentification-request.top
Pattern Type
stix
Pattern
[domain-name:value = 'authentification-request.top']
Name
prevention-aol.top
Pattern Type
stix
Pattern
[domain-name:value = 'prevention-aol.top']
Name
yahoo2-srv.bid

Pattern Type

stix

Pattern

[domain-name:value = 'yahoo2-srv.bid']

Name

login-live.review

Pattern Type

stix

Pattern

[domain-name:value = 'login-live.review']

Name

95.213.194.163

Description

ISP: OOO "Network of data-centers "Selectel" **OS:** Ubuntu ---------- Hostnames: - www.689.spb.ru - 689.spb.ru ---------- Domains: - spb.ru ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDgtClvs+TfB3u0IGVXbqzQCRX9dJRxxHtfuJe47VFyPKF6 KtqABLoebHuWTLmUmYK0BHv0FFWlByBhdxLkLpwBhl5+OOCE8n0/ v6GSD4HFIrm5EB4AeU6Cfb0g SHoLOairUI6p6CdEL+sTmti509eBdNN1j1y1q0ml0e3tIi98s7umSr7ieBPPOCTQwgtpLggxwze/ FxA+jvQo8t29lCcnD43LJVT49QVzEJxKOLcF8Fo5uI1CDeeADlgrUSaXOfqGjLxJMYKN/b1FDSNe NktkpOK9YFDh7Eqo5O/aFjw6HH6K6veqdztepCUB9N9yyPkiAGCfT/exdSM2r8kOcvN1 Fingerprint: 0b:42:69:76:93:70:fe:34:f5:a6:a3:29:d7:ef:71:27 Kex Algorithms: curve25519-sha256

curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Wed, 20 Dec 2023 06:29:28 GMT Content-Type: text/html Content-Length: 1026 Last-Modified: Wed, 22 Feb 2023 09:50:40 GMT Connection: keep-alive ETag: "63f5e570-402" Accept-Ranges: bytes ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Mon, 04 Dec 2023 14:03:20 GMT Content-Type: text/html Content-Length: 161416 Last-Modified: Tue, 06 Dec 2022 14:28:49 GMT Connection: keep-alive ETag: "638f51a1-27688" Accept-Ranges: bytes ``` HEARTBLEED: 2023/12/04 14:03:36 95.213.194.163:443 - SAFE ---------- **3000:** ``` ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '95.213.194.163']

Name

139.162.145.184

Description

CC=DE ASN=AS63949 Akamai Connected Cloud

Pattern Type

stix

Pattern

[ipv4-addr:value = '139.162.145.184']

Name

158.69.149.52

Description

CC=CA ASN=AS16276 OVH SAS

Pattern Type

stix

Pattern

[ipv4-addr:value = '158.69.149.52']

Name

serv.safe-redirect.in.net

Pattern Type

stix

Pattern

[hostname:value = 'serv.safe-redirect.in.net']

Name

en-microsofl.live

Pattern Type
stix
Pattern
[domain-name:value = 'en-microsofl.live']
Name
node03-prevention-icloud.link
Pattern Type
stix
Pattern
[domain-name:value = 'node03-prevention-icloud.link']
Name
drive-meet-goodle.ru
Pattern Type
stix
Pattern
[domain-name:value = 'drive-meet-goodle.ru']
Name
office-356pro.pw

Pattern Type
stix
Pattern
[domain-name:value = 'office-356pro.pw']
Name
secure-store-lcloud.top
Pattern Type
stix
Pattern
[domain-name:value = 'secure-store-lcloud.top']
Name
yamail.press
Pattern Type
stix
Pattern
[domain-name:value = 'yamail.press']
Name
online-1drv.world

Pattern Type
stix
Pattern
[domain-name:value = 'online-1drv.world']
Name
ukroboronprom.pw
Pattern Type
stix
Pattern
[domain-name:value = 'ukroboronprom.pw']
Name
anabol.in
Pattern Type
stix
Pattern
[domain-name:value = 'anabol.in']
Name
screenname.click

Pattern Type
stix
Pattern
[domain-name:value = 'screenname.click']
Name
be-strong.org
Pattern Type
stix
Pattern
[domain-name:value = 'be-strong.org']
Name
icloud-service.pw
Pattern Type
stix
Pattern
[domain-name:value = 'icloud-service.pw']
Name
shared-docs.download

Pattern Type
stix
Pattern
[domain-name:value = 'shared-docs.download']
Name
ukrpharma.ovh
Pattern Type
stix
Pattern
[domain-name:value = 'ukrpharma.ovh']
Name
accounts-mail.asia
Pattern Type
stix
Pattern
[domain-name:value = 'accounts-mail.asia']
Name
y8j4po1ih74l9akzmkq8@r.o-w-o.info

Pattern Type
stix
Pattern
[email-addr:value = 'y8j4po1ih74l9akzmkq8@r.o-w-o.info']
Name
eu-office365.com
Pattern Type
stix
Pattern
[domain-name:value = 'eu-office365.com']
Name
eu-office365.co
Pattern Type
stix
Pattern
[domain-name:value = 'eu-office365.co']
Name
muscle.ovh

Pattern Type
stix
Pattern
[domain-name:value = 'muscle.ovh']
Name
service-mail.asia
Pattern Type
stix
Pattern
[domain-name:value = 'service-mail.asia']
Name
node005-prevention-aol.link
Pattern Type
stix
Pattern
[domain-name:value = 'node005-prevention-aol.link']
Name
support-mail.top

Pattern Type

stix

Pattern

[domain-name:value = 'support-mail.top']

Name

95.171.17.36

Description

CC=RU ASN=AS48822 Universum bit Ltd.

Pattern Type

stix

Pattern

[ipv4-addr:value = '95.171.17.36']

Name

musclepharm.top

Pattern Type

stix

Pattern

[domain-name:value = 'musclepharm.top']

Name
live-login.info
Pattern Type
stix
Pattern
[domain-name:value = 'live-login.info']
Name
support-gmail.pw
Pattern Type
stix
Pattern
[domain-name:value = 'support-gmail.pw']
Name
ukrnet.pw
Pattern Type
stix
Pattern
[domain-name:value = 'ukrnet.pw']

Name
login-live-com.pw
Pattern Type
stix
Pattern
[domain-name:value = 'login-live-com.pw']
Name
screenname-aol.pw
Pattern Type
stix
Pattern
[domain-name:value = 'screenname-aol.pw']
Name
yahoo-user.bid
Pattern Type
stix
Pattern
[domain-name:value = 'yahoo-user.bid']

Name
massa.pw
Pattern Type
stix
Pattern
[domain-name:value = 'massa.pw']
Name
gmail-techdoc.pw
Pattern Type
stix
Pattern
[domain-name:value = 'gmail-techdoc.pw']
Name
file-sharing.site
Pattern Type
stix
Pattern
[domain-name:value = 'file-sharing.site']

Name
platforma.link
Pattern Type
stix
Pattern
[domain-name:value = 'platforma.link']

Domain-Name

Value
yamail.press
login-live.review
file-sharing.site
online-1drv.world
eu-office365.co
node005-prevention-aol.link
google-plus.top
ukroboronprom.pw
hghshop.top
auth-login.top
ukrpharma.ovh
office-356pro.pw
emailapp.pw

yahoo2-srv.bid

massa.pw

musclepharm.top

drive-meet-goodle.ru

accounts-mail.asia

yahoo-user.bid

drive-aoi.icu

eu-office365.com

qooqle-support-mail.pw

login-live-com.pw

anabol.in

authentification-request.top

yahoocentermail.info

live-login.info

secure-icloud.accountant

shared-docs.download

node03-prevention-icloud.link

ukrnet.pw

expert-service.tech

screenname-aol.pw

screenname.click

yahoomailfree.pw

icloud-service.pw

en-office365.club

file-sharing.online

support-gmail.pw

muscle.ovh

online-redirect.site

sykt.support

platforma.link

secure-store-lcloud.top

support-mail.top

service-mail.asia

safe-redirect.in.net

login-access.top

be-strong.org

prevention-aol.top

en-microsofl.live

gmail-techdoc.pw

Email-Addr

Value
y8j4po1ih74l9akzmkq8@r.o-w-o.info

Hostname

Value
serv.safe-redirect.in.net

IPv4-Addr

Value
185.99.134.22
139.162.145.184
185.72.179.132
86.110.117.172
185.212.128.28
95.171.17.36
158.69.149.52
95.213.194.163
37.1.206.114

External References

- https://otx.alienvault.com/pulse/65845530e91ba2f86699a818
- https://blog.sekoia.io/calisto-doxxing-sekoia-io-findings-concurs-to-reuters-investigation-on-fsb-related-andrey-korinets/