Mar 01 2024

NETMANAGEIT

Intelligence Report

DNS Used to Hide Fake Investment Platform Schemes

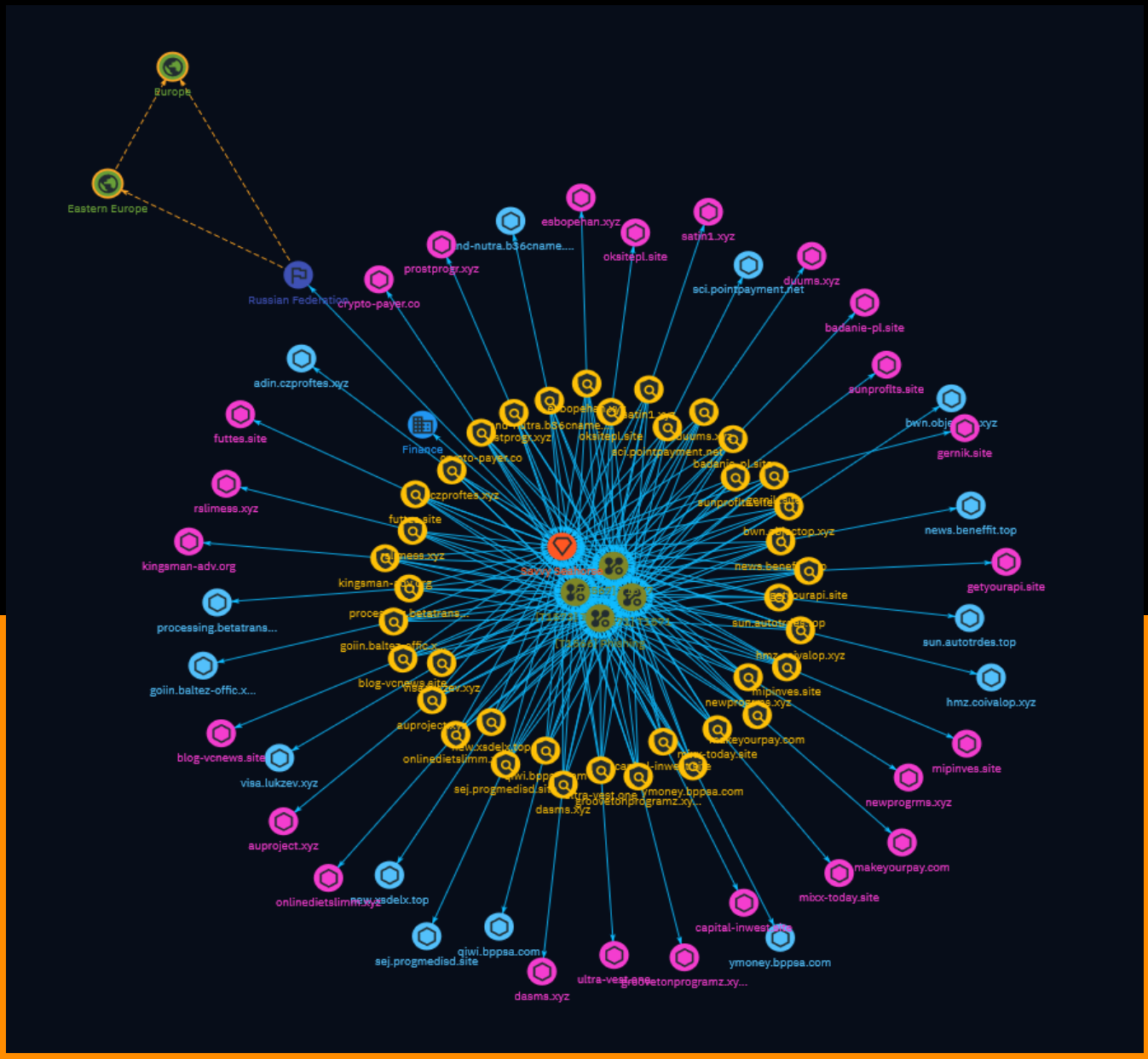

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A threat actor known as Savvy Seahorse is using DNS techniques to create traffic distribution systems that direct victims to fake investment platforms through Facebook ads. The campaigns involve advanced social engineering including fake ChatGPT bots that convince victims to provide personal information and make deposits, with the funds ultimately transferred to Russia.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
ymoney.bppsa.com
Pattern Type
stix
Pattern
[hostname:value = 'ymoney.bppsa.com']
Name
visa.lukzev.xyz
Pattern Type
stix
Pattern
[hostname:value = 'visa.lukzev.xyz']
Name
sci.pointpayment.net

Pattern Type
stix
Pattern
[hostname:value = 'sci.pointpayment.net']
Name
qiwi.bppsa.com
Pattern Type
stix
Pattern
[hostname:value = 'qiwi.bppsa.com']
Name
processing.betatransfer.io
Pattern Type
stix
Pattern
[hostname:value = 'processing.betatransfer.io']
Name
news.beneffit.top

Pattern Type
stix
Pattern
[hostname:value = 'news.beneffit.top']
Name
new.xsdelx.top
Pattern Type
stix
Pattern
[hostname:value = 'new.xsdelx.top']
Name
land-nutra.b36cname.site
Pattern Type
stix
Pattern
[hostname:value = 'land-nutra.b36cname.site']
Name
hmz.coivalop.xyz

Pattern Type
stix
Pattern
[hostname:value = 'hmz.coivalop.xyz']
Name
goiin.baltez-offic.xyz
Pattern Type
stix
Pattern
[hostname:value = 'goiin.baltez-offic.xyz']
Name
bwn.objectop.xyz
Pattern Type
stix
Pattern
[hostname:value = 'bwn.objectop.xyz']
Name
ultra-vest.one

Pattern Type
stix
Pattern
[domain-name:value = 'ultra-vest.one']
Name
sunproflts.site
Pattern Type
stix
Pattern
[domain-name:value = 'sunproflts.site']
Name
prostprogr.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'prostprogr.xyz']
Name
onlinedietslimm.xyz

Pattern Type
stix
Pattern
[domain-name:value = 'onlinedietslimm.xyz']
Name
oksitepl.site
Pattern Type
stix
Pattern
[domain-name:value = 'oksitepl.site']
Name
mixx-today.site
Pattern Type
stix
Pattern
[domain-name:value = 'mixx-today.site']
Name
kingsman-adv.org

Pattern Type
stix
Pattern
[domain-name:value = 'kingsman-adv.org']
Name
gernik.site
Pattern Type
stix
Pattern
[domain-name:value = 'gernik.site']
Name
dasms.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'dasms.xyz']
Name
crypto-payer.co

Pattern Type
stix
Pattern
[domain-name:value = 'crypto-payer.co']
Name
capital-inwest.site
Pattern Type
stix
Pattern
[domain-name:value = 'capital-inwest.site']
Name
blog-vcnews.site
Pattern Type
stix
Pattern
[domain-name:value = 'blog-vcnews.site']
Name
badanie-pl.site

Pattern Type
stix
Pattern
[domain-name:value = 'badanie-pl.site']
Name
sun.autotrdes.top
Pattern Type
stix
Pattern
[hostname:value = 'sun.autotrdes.top']
Name
adin.czproftes.xyz
Pattern Type
stix
Pattern
[hostname:value = 'adin.czproftes.xyz']
Name
getyourapi.site

Pattern Type
stix
Pattern
[domain-name:value = 'getyourapi.site']
Name
sej.progmedisd.site
Pattern Type
stix
Pattern
[hostname:value = 'sej.progmedisd.site']
Name
esbopehan.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'esbopehan.xyz']
Name
newprogrms.xyz

Pattern Type
stix
Pattern
[domain-name:value = 'newprogrms.xyz']
Name
rslimess.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'rslimess.xyz']
Name
duums.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'duums.xyz']
Name
groovetonprogramz.xyz

Pattern Type
stix
Pattern
[domain-name:value = 'groovetonprogramz.xyz']
Name
futtes.site
Pattern Type
stix
Pattern
[domain-name:value = 'futtes.site']
Name
mipinves.site
Pattern Type
stix
Pattern
[domain-name:value = 'mipinves.site']
Name
auproject.xyz

Pattern Type
stix
Pattern
[domain-name:value = 'auproject.xyz']
Name
satin1.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'satin1.xyz']
Name
makeyourpay.com
Pattern Type
stix
Pattern
[domain-name:value = 'makeyourpay.com']

Intrusion-Set

Name
Savvy Seahorse

Attack-Pattern

Name
T1573
ID
T1573
Description
Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.
Name
T1571
ID
T1571
Description
Adversaries may communicate using a protocol and port pairing that are typically not associated. For example, HTTPS over port 8088(Citation: Symantec Elfin Mar 2019) or port 587(Citation: Fortinet Agent Tesla April 2018) as opposed to the traditional port 443.

Adversaries may make changes to the standard port used by a protocol to bypass filtering or muddle analysis/parsing of network data. Adversaries may also make changes to victim systems to abuse non-standard ports. For example, Registry keys and other configuration settings can be used to modify protocol and port pairings.(Citation: change_rdp_port_conti)

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)

Name

T1567

ID

T1567

Description

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

Country

Name
Russian Federation

Region

Name
Eastern Europe

Name
Europe

Sector

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

Hostname

Value
ymoney.bppsa.com
visa.lukzev.xyz
sci.pointpayment.net
qiwi.bppsa.com
processing.betatransfer.io
news.beneffit.top
new.xsdelx.top
land-nutra.b36cname.site
hmz.coivalop.xyz
goiin.baltez-offic.xyz
bwn.objectop.xyz
sun.autotrdes.top
adin.czproftes.xyz

sej.progmedisd.site

Domain-Name

Value
ultra-vest.one
prostprogr.xyz
sunproflts.site
onlinedietslimm.xyz
oksitepl.site
mixx-today.site
kingsman-adv.org
gernik.site
dasms.xyz
crypto-payer.co
capital-inwest.site
blog-vcnews.site
badanie-pl.site

getyourapi.site

esbopehan.xyz

newprogrms.xyz

rslimess.xyz

duums.xyz

groovetonprogramz.xyz

futtes.site

mipinves.site

auproject.xyz

satin1.xyz

makeyourpay.com

External References

- https://blogs.infoblox.com/cyber-threat-intelligence/beware-the-shallow-waters-savvy-seahorse-lures-victims-to-fake-investment-platforms-through-facebook-ads/
- https://otx.alienvault.com/pulse/65e0cc22a43a74523fa3eae6