Jun 11 2024

NETMANAGEIT

Intelligence Report

Cybercriminals attack banking customers in EU with V3B phishing kit

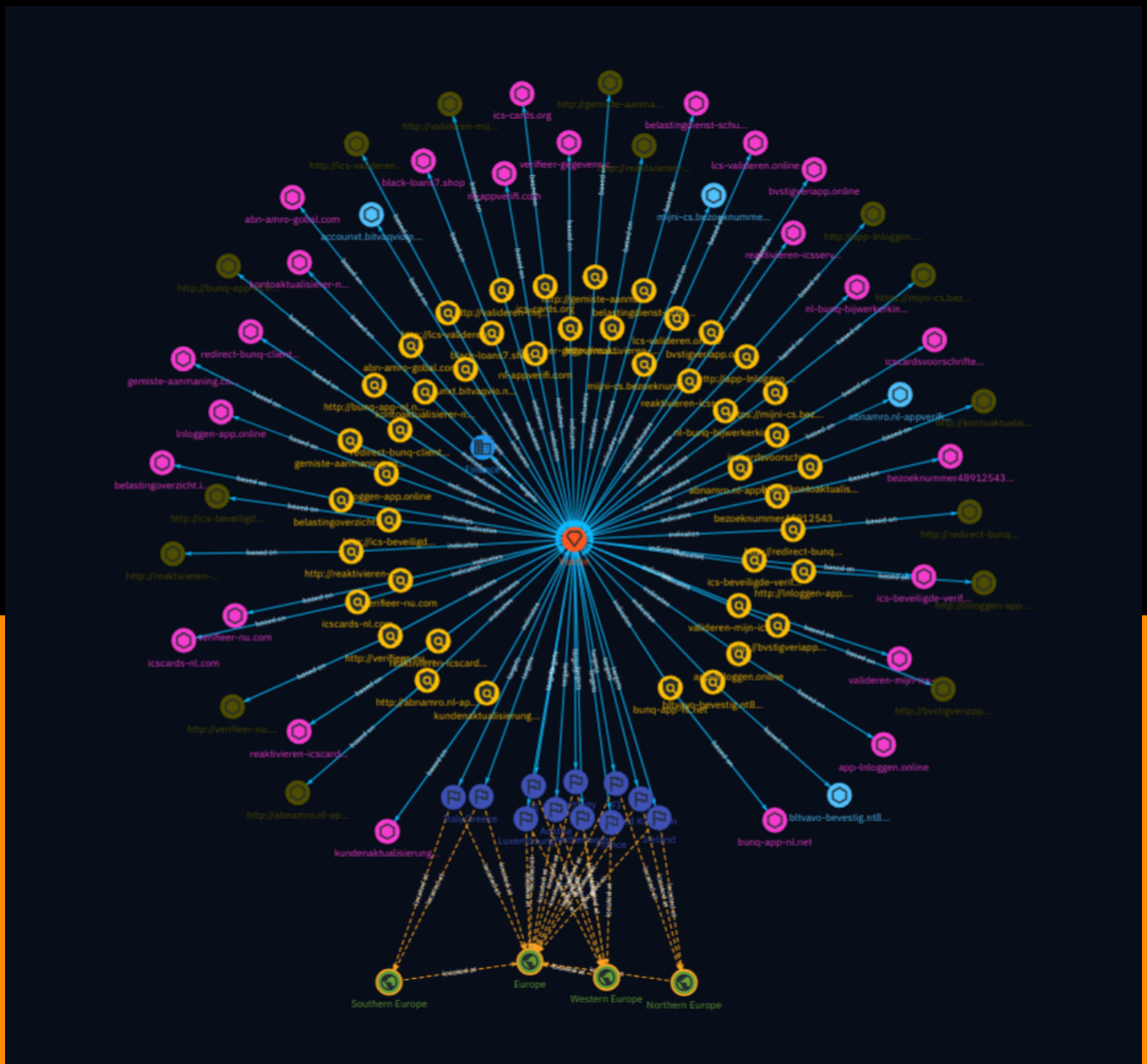

Table of contents

Overview

Entities

Observables

External References

Overview

Description

An analysis reveals that a cybercriminal group is distributing sophisticated phishing kits to target banking customers in the European Union. These kits, designed to steal sensitive information like credentials and OTP codes, utilize social engineering tactics to deceive victims into revealing personal data. The kit, called 'V3B,' is available through a Phishing-as-a-Service model and can be self-hosted. It supports over 54 financial institutions, featuring customized templates that mimic online banking and e-commerce systems across multiple European countries. The threat actors employ advanced techniques like encrypted code, anti-bot measures, live chat interactions, and support for features like QR Codes, PhotoTAN, and Smart ID for authentication bypass. The phishing kit has gained a significant user base, estimated at hundreds of cybercriminals, resulting in substantial financial losses for banking customers across the EU.

Confidence

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

100 / 100

Content

N/A

Sector

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

Indicator

Name
http://reaktivieren-icsservice.nl/icscard.nl-v1/
Pattern Type
stix
Pattern
[url:value = 'http://reaktivieren-icsservice.nl/icscard.nl-v1/']
Name
https://mijni-cs.bezoeknummer0734859938.info/sca/7a970cab144c3e89685550829fe62941/login
Pattern Type
stix
Pattern
[url:value = 'https://mijni-cs.bezoeknummer0734859938.info/sca/7a970cab144c3e89685550829fe62941/login']
Name

http://gemiste-aanmaning.com/belasting

Pattern Type

stix

Pattern

[url:value = 'http://gemiste-aanmaning.com/belasting']

Name

accounxt.bitvaqvio.nl-csdki.com

Pattern Type

stix

Pattern

[hostname:value = 'accounxt.bitvaqvio.nl-csdki.com']

Name

verifieer-nu.com

Pattern Type

stix

Pattern

[domain-name:value = 'verifieer-nu.com']

Name

lnloggen-app.online

Pattern Type

stix

Pattern

[domain-name:value = 'lnloggen-app.online']

Name

http://abnamro.nl-appverifi.com/3/jjfosp/o34432fpo/index4.php

Pattern Type

stix

Pattern

[url:value = 'http://abnamro.nl-appverifi.com/3/jjfosp/o34432fpo/index4.php']

Name

black-loans7.shop

Pattern Type

stix

Pattern

[domain-name:value = 'black-loans7.shop']

Name

ics-cards.org

Pattern Type

stix

Pattern

[domain-name:value = 'ics-cards.org']

Name

reaktivieren-icsservice.nl

Pattern Type

stix

Pattern

[domain-name:value = 'reaktivieren-icsservice.nl']

Name

http://lnloggen-app.online/

Pattern Type

stix

Pattern

[url:value = 'http://lnloggen-app.online/']

Name

http://ics-beveiligde-verificatie.com/sqi.php

Pattern Type

stix

Pattern

[url:value = 'http://ics-beveiligde-verificatie.com/sqi.php']

Name

http://valideren-mijn-ics-web1.online/sq0.php?session=664483b236193

Pattern Type

stix

Pattern

[url:value = 'http://valideren-mijn-ics-web1.online/sq0.php?session=664483b236193']

Name

http://app-lnloggen.online/authenticatie/inloggen/nl

Pattern Type

stix

Pattern

[url:value = 'http://app-lnloggen.online/authenticatie/inloggen/nl']

Name

http://kontoaktualisierer-nl.com/icscard.nl-v1

Pattern Type

stix

Pattern

[url:value = 'http://kontoaktualisierer-nl.com/icscard.nl-v1']

Name

kundenaktualisierungen.cc

Pattern Type

stix

Pattern

[domain-name:value = 'kundenaktualisierungen.cc']

Name

belastingdienst-schuld.nl

Pattern Type

stix

Pattern

[domain-name:value = 'belastingdienst-schuld.nl']

Name

ics-beveiligde-verificatie.com

Pattern Type

stix

Pattern

[domain-name:value = 'ics-beveiligde-verificatie.com']

Name

bvstigveriapp.online

Pattern Type

stix

Pattern

[domain-name:value = 'bvstigveriapp.online']

Name

app-lnloggen.online

Pattern Type

stix

Pattern

[domain-name:value = 'app-lnloggen.online']

Name

http://lcs-valideren.online/ics/sca-app/663e0152c96c0

Pattern Type

stix

Pattern

[url:value = 'http://lcs-valideren.online/ics/sca-app/663e0152c96c0']

Name

kontoaktualisierer-nl.com

Pattern Type

stix

Pattern

[domain-name:value = 'kontoaktualisierer-nl.com']

Name

mijni-cs.bezoeknummer0734859938.info

Pattern Type

stix

Pattern

[hostname:value = 'mijni-cs.bezoeknummer0734859938.info']

Name

reaktivieren-icscard.nl

Pattern Type

stix

Pattern

[domain-name:value = 'reaktivieren-icscard.nl']

Name

icscards-nl.com

Pattern Type

stix

Pattern

[domain-name:value = 'icscards-nl.com']

Name

nl-bunq-bijwerkerking.com

Pattern Type

stix

Pattern

[domain-name:value = 'nl-bunq-bijwerkerking.com']

Name

http://bunq-app-nl.net/K8IjL9/1M3k/lgn

Pattern Type

stix

Pattern

[url:value = 'http://bunq-app-nl.net/K8IjL9/1M3k/lgn']

Name

belastingoverzicht.info

Pattern Type

stix

Pattern

[domain-name:value = 'belastingoverzicht.info']

Name

http://bvstigveriapp.online/pay/664130fb17583

Pattern Type

stix

Pattern

[url:value = 'http://bvstigveriapp.online/pay/664130fb17583']

Name

http://reaktivieren-icsservice.nl/icscard.nl-v1/ics-log.php

Pattern Type

stix

Pattern

[url:value = 'http://reaktivieren-icsservice.nl/icscard.nl-v1/ics-log.php']

Name

bltvavo-bevestig.nt8zd3.ru

Pattern Type

stix

Pattern

[hostname:value = 'bltvavo-bevestig.nt8zd3.ru']

Name

icscardsvoorschriften.nl

Pattern Type

stix

Pattern

[domain-name:value = 'icscardsvoorschriften.nl']

Name

gemiste-aanmaning.com

Pattern Type

stix

Pattern

[domain-name:value = 'gemiste-aanmaning.com']

Name

verifieer-gegevens.com

Pattern Type

stix

Pattern

[domain-name:value = 'verifieer-gegevens.com']

Name

redirect-bunq-client.ru

Pattern Type

stix

Pattern

[domain-name:value = 'redirect-bunq-client.ru']

Name

nl-appverifi.com

Pattern Type

stix

Pattern

[domain-name:value = 'nl-appverifi.com']

Name

valideren-mijn-ics-web1.online

Pattern Type

stix

Pattern

[domain-name:value = 'valideren-mijn-ics-web1.online']

Name

abnamro.nl-appverifi.com

Pattern Type

stix

Pattern

[hostname:value = 'abnamro.nl-appverifi.com']

Name

lcs-valideren.online

Pattern Type

stix

Pattern

[domain-name:value = 'lcs-valideren.online']

Name

http://redirect-bunq-client.ru/account/321/

Pattern Type

stix

Pattern

[url:value = 'http://redirect-bunq-client.ru/account/321/']

Name

bunq-app-nl.net

Pattern Type

stix

Pattern

[domain-name:value = 'bunq-app-nl.net']

Name

abn-amro-gobal.com

Pattern Type

stix

Pattern

[domain-name:value = 'abn-amro-gobal.com']

Name

http://verifieer-nu.com/verificatie/66422f472f10c

Pattern Type

stix

Pattern

[url:value = 'http://verifieer-nu.com/verificatie/66422f472f10c']

Name

bezoeknummer48912543221.info

Pattern Type

stix

Pattern

[domain-name:value = 'bezoeknummer48912543221.info']

Intrusion-Set

Name
Vssrtje

Region

Name
Europe
Name
Northern Europe
Name
Southern Europe
Name
Western Europe

Country

Name
Ireland
Name
FI
Name
BE
Name
Austria
Name
Netherlands
Name
Germany
Name
United Kingdom

Name
Luxembourg
Name
Greece
Name
France
Name
Italy

indicates

Name
Name
Name
Name
Name

based-on

Name
Name
Name

targets

Name

located-at

Name

Domain-Name

Value
ics-cards.org
bunq-app-nl.net
reaktivieren-icscard.nl
belastingdienst-schuld.nl
lnloggen-app.online
icscards-nl.com
lcs-valideren.online
gemiste-aanmaning.com
verifieer-nu.com
nl-appverifi.com
valideren-mijn-ics-web1.online
belastingoverzicht.info
reaktivieren-icsservice.nl

verifieer-gegevens.com

app-lnloggen.online

bvstigveriapp.online

abn-amro-gobal.com

kontoaktualisierer-nl.com

redirect-bunq-client.ru

bezoeknummer48912543221.info

black-loans7.shop

ics-beveiligde-verificatie.com

kundenaktualisierungen.cc

icscardsvoorschriften.nl

nl-bunq-bijwerkerking.com

Hostname

Value
mijni-cs.bezoeknummer0734859938.info
accounxt.bitvaqvio.nl-csdki.com
abnamro.nl-appverifi.com
bltvavo-bevestig.nt8zd3.ru

External References

- https://www.resecurity.com/blog/article/cybercriminals-attack-banking-customers-in-eu-with-v3b-phishing-kit
- https://otx.alienvault.com/pulse/6666e16598de923f59eb5c07