Jul 24 2023

NETMANAGEIT

Intelligence Report

The threat level for accountants is increasing: the UAC-0006 group carried out the third cyber attack in 10 days (CERT-UA#7065, CERT-UA#7076)

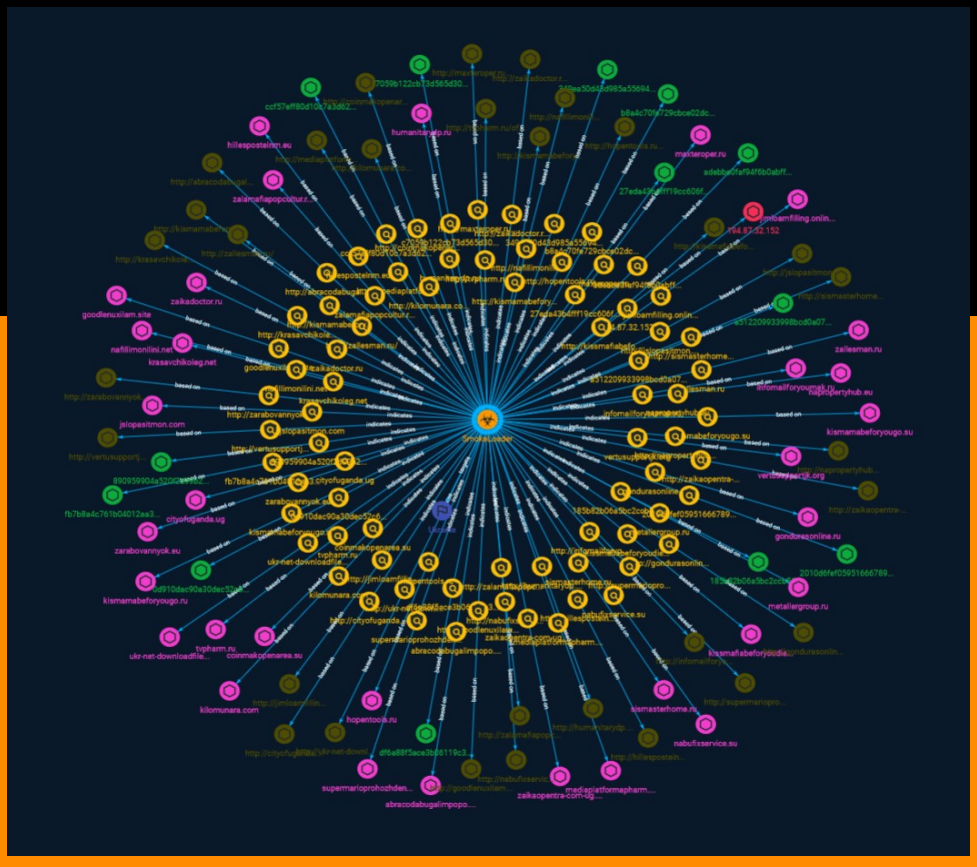

Table of contents

Overview

Entities

Observables

External References

Overview

Description

On 07/21/2023 and 07/24/2023, the Government Computer Emergency Response Team of Ukraine CERT-UA recorded regular attacks by the UAC-0006 group using the SmokeLoader malware.

Confidence

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

15 / 100

Indicator

Name
zarabovannyok.eu
Pattern Type
stix
Pattern
[domain-name:value = 'zarabovannyok.eu']
Name
supermarioprohozhdenie.ru
Pattern Type
stix
Pattern
[domain-name:value = 'supermarioprohozhdenie.ru']
Name
http://zalamafiapopcultur.ru/

Pattern Type

stix

Pattern

[url:value = 'http://zalamafiapopcultur.ru/']

Name

http://tvpharm.ru/officedownloadfile/weboffice.exe

Pattern Type

stix

Pattern

[url:value = 'http://tvpharm.ru/officedownloadfile/weboffice.exe']

Name

kissmafiabeforyoudied.ru

Pattern Type

stix

Pattern

[domain-name:value = 'kissmafiabeforyoudied.ru']

Name

zallesman.ru

Pattern Type

stix

Pattern

[domain-name:value = 'zallesman.ru']

Name

http://coinmakopenarea.su/

Pattern Type

stix

Pattern

[url:value = 'http://coinmakopenarea.su/']

Name

185b82b06a5bc2ccb5643440227293c7fa123216f7abfb685bdc0dc70dffdc37

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '185b82b06a5bc2ccb5643440227293c7fa123216f7abfb685bdc0dc70dffdc37']

Name

kismamabeforyougo.su

Pattern Type

stix

Pattern

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

Name

http://nabufixservice.su/

Pattern Type

stix

Pattern

[url:value = 'http://nabufixservice.su/']

Name

349ea50d43d985a55694b440ca71062198a3c7a1f7764509970d37a054d04d2a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '349ea50d43d985a55694b440ca71062198a3c7a1f7764509970d37a054d04d2a']

Name
http://jslopasitmon.com/
Pattern Type
stix
Pattern
[url:value = 'http://jslopasitmon.com/']
Name
kismamabeforyougo.ru
Pattern Type
stix
Pattern
[domain-name:value = 'kismamabeforyougo.ru']
Name
http://mediaplatformapharm.ru/officedownloadfile/weboffice.exe
Pattern Type
stix
Pattern
[url:value = 'http://mediaplatformapharm.ru/officedownloadfile/weboffice.exe']

Name
http://maxteroper.ru/
Pattern Type
stix
Pattern
[url:value = 'http://maxteroper.ru/']
Name
krasavchikoleg.net
Pattern Type
stix
Pattern
[domain-name:value = 'krasavchikoleg.net']
Name
http://hillespostelnm.eu/
Pattern Type
stix
Pattern
[url:value = 'http://hillespostelnm.eu/']

Name
coinmakopenarea.su
Pattern Type
stix
Pattern
[domain-name:value = 'coinmakopenarea.su']
Name
http://sismasterhome.ru/
Pattern Type
stix
Pattern
[url:value = 'http://sismasterhome.ru/']
Name
infomailforyoumak.ru
Pattern Type
stix
Pattern
[domain-name:value = 'infomailforyoumak.ru']

Name

b8a4c70fe729cbce02dc67b18ee0f8397834cd2067664363617567a255427242

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b8a4c70fe729cbce02dc67b18ee0f8397834cd2067664363617567a255427242']

Name

df6a88f5ace3b06119c30539048a2d8724c511de287a43201c610ef236ca64b8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'df6a88f5ace3b06119c30539048a2d8724c511de287a43201c610ef236ca64b8']

Name

vertusupportjk.org

Pattern Type

stix

Pattern

[domain-name:value = 'vertusupportjk.org']

Name

http://infomailforyoumak.ru/

Pattern Type

stix

Pattern

[url:value = 'http://infomailforyoumak.ru/']

Name

mediaplatformapharm.ru

Pattern Type

stix

Pattern

[domain-name:value = 'mediaplatformapharm.ru']

Name

194.87.32.152

Description

ISP: HUIZE TELECOM LIMITED **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 301 Moved Permanently Location: http://www.google.com/ Content-Type: text/html; charset=UTF-8 Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-

src 'nonce-VvhMWkwfDA35E2yJEzDKlw' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp Permissions-Policy: unload=() Origin-Trial: Ap+qNlnLzJDKSmEHjzM5ilaa908GuehlLqGb6ezME5lkhelj20qVzfv06zPmQ3LodoeujZuphAolrnhnPA8w4AIAAABfeyJvcmlnaW4iOiJodHRwczovL3d3dy5nb29nbGUuY29tOjQ0MyIsImZlYXR1cmUiOiJQZXJtaXNzaW9uc1BvbGljeVVubG9hZCIsImV4cGlyeSI6MTY4NTY2Mzk5OX0= Origin-Trial: AvudrjMZqL7335p1KLV2lHo1kxdMeIN0dUI15d0CPz9dovVLCcXk8OAqjho1DX4s6NbHbA/AGobuGvcZv0drGgQAAAB9eyJvcmlnaW4iOiJodHRwczovL3d3dy5nb29nbGUuY29tOjQ0MyIsImZlYXR1cmUiOiJCYWNrRm9yd2FyZENhY2hlTm90UmVzdG9yZWRSZWFzb25zIiwiZXhwaXJ5IjoxNjkxNTM5MTk5LCJpc1N1YmRvbWFpbiI6dHJ1ZX0= Date: Sun, 16 Jul 2023 20:53:35 GMT Expires: Tue, 15 Aug 2023 20:53:35 GMT Cache-Control: public, max-age=2592000 Server: gws Content-Length: 219 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Connection: close ```

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.87.32.152']

Name

humanitarydp.ru

Pattern Type

stix

Pattern

[domain-name:value = 'humanitarydp.ru']

Name

http://ukr-net-downloadfile.su/summary/php/form/name/267856437856374568797257305680384563486589345630856730443317231095623053892649181 6

496246343234365738465390457389758367465736573894573 86/file/видаткова_накладная_№121_від_18_липня_2023р.html

Pattern Type

stix

Pattern

[url:value = 'http://ukr-net-downloadfile.su/summary/php/form/name/267856437856374568797257305680384563486589345630856730443317231095623053892649181649624634323436573846539045738975836746573657389457386/file/видаткова_накладная_№121_від_18_липня_2023р.html']

Name

cityofuganda.ug

Pattern Type

stix

Pattern

[domain-name:value = 'cityofuganda.ug']

Name

jimloamfilling.online

Pattern Type

stix

Pattern

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

Name

http://abracodabugalimpopo.ru/

Pattern Type

stix

Pattern

[url:value = 'http://abracodabugalimpopo.ru/']

Name

c7059b122cb73d565d30d16ad97bdd412ea9f47292a5e3a30298c1ba5041290c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c7059b122cb73d565d30d16ad97bdd412ea9f47292a5e3a30298c1ba5041290c']

Name

http://cityofuganda.ug/

Pattern Type

stix

Pattern

[url:value = 'http://cityofuganda.ug/']

Name

0d910dac90a30dec52c6484bd7087f4a1d55d827a093a2f43c9dfe59a082aab9

Description

multiple_versions

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0d910dac90a30dec52c6484bd7087f4a1d55d827a093a2f43c9dfe59a082aab9']

Name

http://kismamabeforyougo.ru/

Pattern Type

stix

Pattern

[url:value = 'http://kismamabeforyougo.ru/']

Name

http://kissmafiabeforyoudied.ru/

Pattern Type

stix

Pattern

[url:value = 'http://kissmafiabeforyoudied.ru/']

Name

http://zarabovannyok.eu/

Pattern Type

stix

Pattern

[url:value = 'http://zarabovannyok.eu/']

Name

gondurasonline.ru

Pattern Type

stix

Pattern

[domain-name:value = 'gondurasonline.ru']

Name

http://hopentools.ru/

Pattern Type

stix

Pattern

[url:value = 'http://hopentools.ru/']

Name

metallergroup.ru

Pattern Type

stix

Pattern

[domain-name:value = 'metallergroup.ru']

Name

zaikaopentra-com-ug.su

Pattern Type

stix

Pattern

[domain-name:value = 'zaikaopentra-com-ug.su']

Name

tvpharm.ru

Pattern Type

stix

Pattern

[domain-name:value = 'tvpharm.ru']

Name

http://gondurasonline.ru/

Pattern Type

stix

Pattern

[url:value = 'http://gondurasonline.ru/']

Name

fb7b8a4c761b04012aa384e35b219e1236dfb6639a08bddc85cd006f0ca92d9f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fb7b8a4c761b04012aa384e35b219e1236dfb6639a08bddc85cd006f0ca92d9f']

Name
http://zallesman.ru/
Pattern Type
stix
Pattern
[url:value = 'http://zallesman.ru/']
Name
http://goodlenuxilam.site/
Pattern Type
stix
Pattern
[url:value = 'http://goodlenuxilam.site/']
Name
zalamafiapopcultur.ru
Pattern Type
stix
Pattern
[domain-name:value = 'zalamafiapopcultur.ru']

Name

http://zaikaopentra-com-ug.su/

Pattern Type

stix

Pattern

[url:value = 'http://zaikaopentra-com-ug.su/']

Name

a512209933998bcd0a07a16af04aa7fd05e3c23103978ad250a7e1cb249d4baa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a512209933998bcd0a07a16af04aa7fd05e3c23103978ad250a7e1cb249d4baa']

Name

hillespostelnm.eu

Pattern Type

stix

Pattern

[domain-name:value = 'hillespostelnm.eu']

Name

2010d6fef059516667897371bea5903489887851c08e0f925a5df49731ec9118

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2010d6fef059516667897371bea5903489887851c08e0f925a5df49731ec9118']

Name

jslopasitmon.com

Pattern Type

stix

Pattern

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

Name

napropertyhub.eu

Pattern Type

stix

Pattern

[domain-name:value = 'napropertyhub.eu']

Name

hopentools.ru

Pattern Type

stix

Pattern

[domain-name:value = 'hopentools.ru']

Name

890959904a520f2d99b2aee5763fec2a5cd0e490657aeed9e0a7a9ae60dde517

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '890959904a520f2d99b2aee5763fec2a5cd0e490657aeed9e0a7a9ae60dde517']

Name

http://humanitarydp.ru/

Pattern Type

stix

Pattern

[url:value = 'http://humanitarydp.ru/']

Name

http://jimloamfilling.online/

Pattern Type

stix

Pattern

[url:value = 'http://jimloamfilling.online/']

Name

http://krasavchikoleg.net/

Pattern Type

stix

Pattern

[url:value = 'http://krasavchikoleg.net/']

Name

abracodabugalimpopo.ru

Pattern Type

stix

Pattern

[domain-name:value = 'abracodabugalimpopo.ru']

Name

http://kismamabeforyougo.su/

Pattern Type

stix

Pattern

[url:value = 'http://kismamabeforyougo.su/']

Name

adebbe0faf94f6b0abff96cf9da38d4c845299c7fde240e389553bf847e3d238

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'adebbe0faf94f6b0abff96cf9da38d4c845299c7fde240e389553bf847e3d238']

Name

zaikadoctor.ru

Pattern Type

stix

Pattern

[domain-name:value = 'zaikadoctor.ru']

Name

27eda43b4fff19cc606f87414705cefa7271bd8f998176c2b49a5fc35bee5c21

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '27eda43b4fff19cc606f87414705cefa7271bd8f998176c2b49a5fc35bee5c21']

Name

nabufixservice.su

Pattern Type

stix

Pattern

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

Name

goodlenuxilam.site

Pattern Type

stix

Pattern

[domain-name:value = 'goodlenuxilam.site']

Name

maxteroper.ru

Pattern Type

stix

Pattern

[domain-name:value = 'maxteroper.ru']

Name

sismasterhome.ru

Pattern Type

stix

Pattern

[domain-name:value = 'sismasterhome.ru']

Name

http://kilomunara.com/

Pattern Type

stix

Pattern

[url:value = 'http://kilomunara.com/']

Name

nafillimonilini.net

Pattern Type

stix

Pattern

[domain-name:value = 'nafillimonilini.net']

Name

http://vertusupportjk.org/

Pattern Type

stix

Pattern

[url:value = 'http://vertusupportjk.org/']

Name

ccf57eff80d10c7a3d6236802e91d4f60fbe68a8cca21d670ffdb7c6c6cb897b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ccf57eff80d10c7a3d6236802e91d4f60fbe68a8cca21d670ffdb7c6c6cb897b']

Name

http://supermarioprohozhdenie.ru/

Pattern Type

stix

Pattern

[url:value = 'http://supermarioprohozhdenie.ru/']

Name

ukr-net-downloadfile.su

Pattern Type

stix

Pattern

[domain-name:value = 'ukr-net-downloadfile.su']

Name
http://zaikadoctor.ru/
Pattern Type
stix
Pattern
[url:value = 'http://zaikadoctor.ru/']
Name
kilomunara.com
Pattern Type
stix
Pattern
[domain-name:value = 'kilomunara.com']
Name
http://nafillimonilini.net/
Pattern Type
stix
Pattern
[url:value = 'http://nafillimonilini.net/']

Name
http://napropertyhub.eu/
Pattern Type
stix
Pattern
[url:value = 'http://napropertyhub.eu/']

Malware

Name
SmokeLoader

Country

Name
Ukraine

Domain-Name

Value
goodlenuxilam.site
metallergroup.ru
krasavchikoleg.net
kismamabeforyougo.su
coinmakopenarea.su
jslopasitmon.com
zaikaopentra-com-ug.su
kismamabeforyougo.ru
zalamafiapopcultur.ru
kissmafiabeforyoudied.ru
hopentools.ru
zallesman.ru
supermarioprohozhdenie.ru

zaikadoctor.ru

mediaplatformapharm.ru

kilomunara.com

maxteroper.ru

tvpharm.ru

humanitarydp.ru

sismasterhome.ru

abracodabugalimpopo.ru

infomailforyoumak.ru

nabufixservice.su

nafillimonilini.net

vertusupportjk.org

ukr-net-downloadfile.su

jimloamfilling.online

napropertyhub.eu

zarabovannyok.eu

gondurasonline.ru

cityofuganda.ug

hillespostelnm.eu

StixFile

Value
df6a88f5ace3b06119c30539048a2d8724c511de287a43201c610ef236ca64b8
a512209933998bcd0a07a16af04aa7fd05e3c23103978ad250a7e1cb249d4baa
185b82b06a5bc2ccb5643440227293c7fa123216f7abfb685bdc0dc70dffdc37
c7059b122cb73d565d30d16ad97bdd412ea9f47292a5e3a30298c1ba5041290c
b8a4c70fe729cbce02dc67b18ee0f8397834cd2067664363617567a255427242
0d910dac90a30dec52c6484bd7087f4a1d55d827a093a2f43c9dfe59a082aab9
349ea50d43d985a55694b440ca71062198a3c7a1f7764509970d37a054d04d2a
27eda43b4fff19cc606f87414705cefa7271bd8f998176c2b49a5fc35bee5c21
fb7b8a4c761b04012aa384e35b219e1236dfb6639a08bddc85cd006f0ca92d9f
adebbe0faf94f6b0abff96cf9da38d4c845299c7fde240e389553bf847e3d238
890959904a520f2d99b2aee5763fec2a5cd0e490657aeed9e0a7a9ae60dde517
ccf57eff80d10c7a3d6236802e91d4f60fbe68a8cca21d670ffdb7c6c6cb897b
2010d6fef059516667897371bea5903489887851c08e0f925a5df49731ec9118

IPv4-Addr

Value
194.87.32.152

Url

Value
http://goodlenuxilam.site/
http://maxteroper.ru/
http://supermarioprohozhdenie.ru/
http://kismamabeforyougo.ru/
http://kissmafiabeforyoudied.ru/
http://zalamafiapopcultur.ru/
http://tvpharm.ru/officedownloadfile/weboffice.exe
http://zaikaopentra-com-ug.su/
http://humanitarydp.ru/
http://jslopasitmon.com/
http://nabufixservice.su/
http://krasavchikoleg.net/
http://hopentools.ru/

http://ukr-net-downloadfile.su/summary/php/form/name/
267856437856374568797257305680384563486589345630856730443317231095623053892649181649624634323436573846539045738975836746573657389457386/file/
видаткова_накладная_№121_від_18_липня_2023р.html

http://coinmakopenarea.su/

http://gondurasonline.ru/

http://mediaplatformapharm.ru/officedownloadfile/weboffice.exe

http://napropertyhub.eu/

http://infomailforyoumak.ru/

http://vertusupportjk.org/

http://nafillimonilini.net/

http://zallesman.ru/

http://abracodabugalimpopo.ru/

http://hillespostelnm.eu/

http://zarabovannyok.eu/

http://sismasterhome.ru/

http://jimloamfilling.online/

http://zaikadoctor.ru/

http://kilomunara.com/

http://cityofuganda.ug/

http://kismamabeforyougo.su/

External References

- https://otx.alienvault.com/pulse/64be7b3dbe9c2467c5461227