Feb 20 2024

NETMANAGEIT

Intelligence Report

Russia-Aligned TAG-70 Targets European Government and Military Mail Servers in New Espionage Campaig

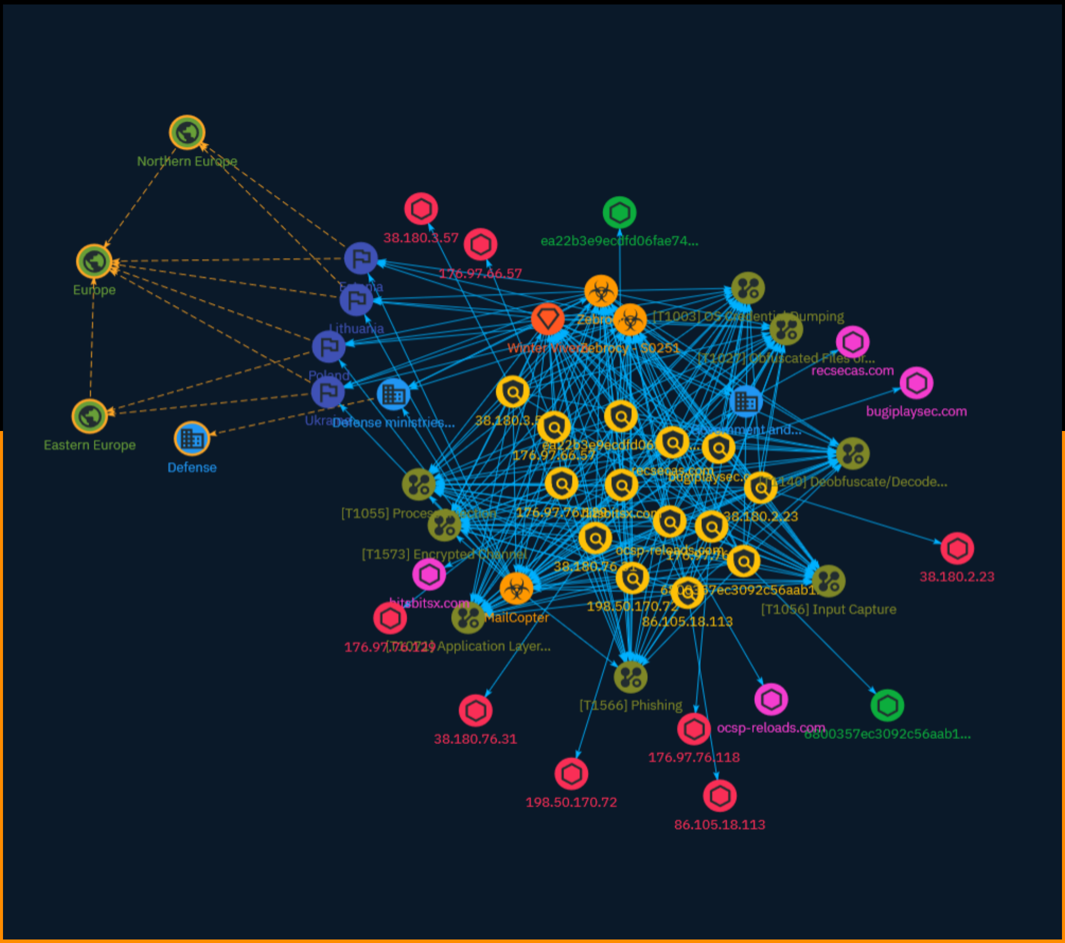

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A new espionage campaign conducted by the Russia-aligned threat actor TAG-70 has been observed targeting European government and military entities. The attackers are exploiting cross-site scripting (XSS) vulnerabilities to compromise Roundcube mail servers and exfiltrate sensitive data.

Confidence

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

15 / 100

Content

N/A

Indicator

Name

ocsp-reloads.com

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '12 months ago', 'timestamp': 1677743106, 'iso': '2023-03-02T02:45:06-05:00'} - **IPQS: Domain:** ocsp-reloads.com - **IPQS: IP Address:** 38.180.2.23

Pattern Type

stix

Pattern

[domain-name:value = 'ocsp-reloads.com']

Name

hitsbitsx.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '10 months ago', 'timestamp': 1680862056, 'iso': '2023-04-07T06:07:36-04:00'} - **IPQS: Domain:** hitsbitsx.com - **IPQS: IP Address:** 38.180.3.57

Pattern Type

stix

Pattern

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

Name

bugiplaysec.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

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

Name

86.105.18.113

Description

- **Zip Code:** N/A - **ISP:** WorldStream - **ASN:** 49981 - **Organization:** WorldStream - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** 86.105.18.113 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:**

False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** NL - **Region:** South Holland - **City:** Naaldwijk - **Latitude:** 52 - **Longitude:** 4.2

Pattern Type

stix

Pattern

[ipv4-addr:value = '86.105.18.113']

Name

38.180.3.57

Description

- **Zip Code:** N/A - **ISP:** Cogent Communications - **ASN:** 9009 - **Organization:** M247 Europe - **Is Crawler:** False - **Timezone:** Europe/Sofia - **Mobile:** False - **Host:** 38.180.3.57 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** BG - **Region:** Sofia - **City:** Sofia - **Latitude:** 42.67 - **Longitude:** 23.8

Pattern Type

stix

Pattern

[ipv4-addr:value = '38.180.3.57']

Name

38.180.2.23

Description

- **Zip Code:** N/A - **ISP:** Cogent Communications - **ASN:** 9009 - **Organization:** M247 Europe - **Is Crawler:** False - **Timezone:** Europe/Sofia - **Mobile:** False - **Host:** 38.180.2.23 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** BG - **Region:** Sofia - **City:** Sofia - **Latitude:** 42.67 - **Longitude:** 23.8

Pattern Type

stix

Pattern

[ipv4-addr:value = '38.180.2.23']

Name

198.50.170.72

Description

- **Zip Code:** N/A - **ISP:** OVH SAS - **ASN:** 16276 - **Organization:** OVH SAS - **Is Crawler:** False - **Timezone:** America/Montreal - **Mobile:** False - **Host:** 198.50.170.72 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** CA - **Region:** Quebec - **City:** Montreal - **Latitude:** 45.51 - **Longitude:** -73.59

Pattern Type

stix

Pattern

[ipv4-addr:value = '198.50.170.72']

Name

176.97.76.129

Description

- **Zip Code:** N/A - **ISP:** M247 Europe - **ASN:** 9009 - **Organization:** M247 Europe - **Is Crawler:** False - **Timezone:** Europe/Bucharest - **Mobile:** False - **Host:** 176.97.76.129 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** RO - **Region:** Bucuresti - **City:** Bucharest - **Latitude:** 44.43 - **Longitude:** 26.11

Pattern Type

stix

Pattern

[ipv4-addr:value = '176.97.76.129']

Name

176.97.76.118

Description

- **Zip Code:** N/A - **ISP:** M247 Europe - **ASN:** 9009 - **Organization:** M247 Europe - **Is Crawler:** False - **Timezone:** Europe/Bucharest - **Mobile:** False - **Host:** 176.97.76.118 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** RO - **Region:** Bucuresti - **City:** Bucharest - **Latitude:** 44.43 - **Longitude:** 26.11

Pattern Type

stix

Pattern

[ipv4-addr:value = '176.97.76.118']

Name

176.97.66.57

Description

- **Zip Code:** N/A - **ISP:** M247 Europe - **ASN:** 9009 - **Organization:** M247 Europe - **Is Crawler:** False - **Timezone:** Asia/Dubai - **Mobile:** False - **Host:** 176.97.66.57 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** True - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** AE - **Region:** Dubai - **City:** Dubai - **Latitude:** 25.07 - **Longitude:** 55.3

Pattern Type

stix

Pattern

[ipv4-addr:value = '176.97.66.57']

Name

ea22b3e9ecdfd06fae74483deb9ef0245aefdc72f99120ae6525c0eaf37de32e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ea22b3e9ecdfd06fae74483deb9ef0245aefdc72f99120ae6525c0eaf37de32e']

Name

6800357ec3092c56aab17720897c29bb389f70cb49223b289ea5365314199a26

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6800357ec3092c56aab17720897c29bb389f70cb49223b289ea5365314199a26']

Name

38.180.76.31

Description

CC=NO ASN=AS9009 M247 Europe SRL

Pattern Type

stix

Pattern

[ipv4-addr:value = '38.180.76.31']

Name

recsecas.com

Pattern Type

stix

Pattern

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

Malware

Name

Zebrocy - S0251

Name

MailCopter

Name

Zebrocy

Description

[Zebrocy](https://attack.mitre.org/software/S0251) is a Trojan that has been used by [APT28](https://attack.mitre.org/groups/G0007) since at least November 2015. The malware comes in several programming language variants, including C++, Delphi, AutoIt, C#, VB.NET, and Golang. (Citation: Palo Alto Sofacy 06-2018)(Citation: Unit42 Cannon Nov 2018)(Citation: Unit42 Sofacy Dec 2018)(Citation: CISA Zebrocy Oct 2020)

Intrusion-Set

Name
Winter Vivern

Attack-Pattern

Name
Input Capture
ID
T1056
Description
Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).
Name
Encrypted Channel
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

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

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

Process Injection

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Name

Application Layer Protocol

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

OS Credential Dumping

ID

T1003

Description

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

Country

Name
Lithuania

Name
Estonia

Name
Ukraine

Name
Poland

Region

Name
Northern Europe

Name
Eastern Europe

Name
Europe

Sector

Name	Description
Government and administrations	Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.
Defense ministries (including the military)	Includes the military and all defense related-space activities.
Defense	Public and private entities involved in the conception and production of weapons and the planning and conducting of military operations.

Domain-Name

Value
ocsp-reloads.com
hitsbitsx.com
bugiplaysec.com
recsecas.com

IPv4-Addr

Value
86.105.18.113
38.180.3.57
38.180.2.23
198.50.170.72
176.97.66.57
176.97.76.129
176.97.76.118
38.180.76.31

StixFile

Value
ea22b3e9ecdfd06fae74483deb9ef0245aefdc72f99120ae6525c0eaf37de32e
6800357ec3092c56aab17720897c29bb389f70cb49223b289ea5365314199a26

External References

- https://go.recordedfuture.com/hubfs/reports/cta-2024-0217.pdf
- https://otx.alienvault.com/pulse/65d472a0c6c172be11812240