Feb 03 2024

NETMANAGEIT

Intelligence Report

Scaly Wolf uses White Snake stealer against Russian industry

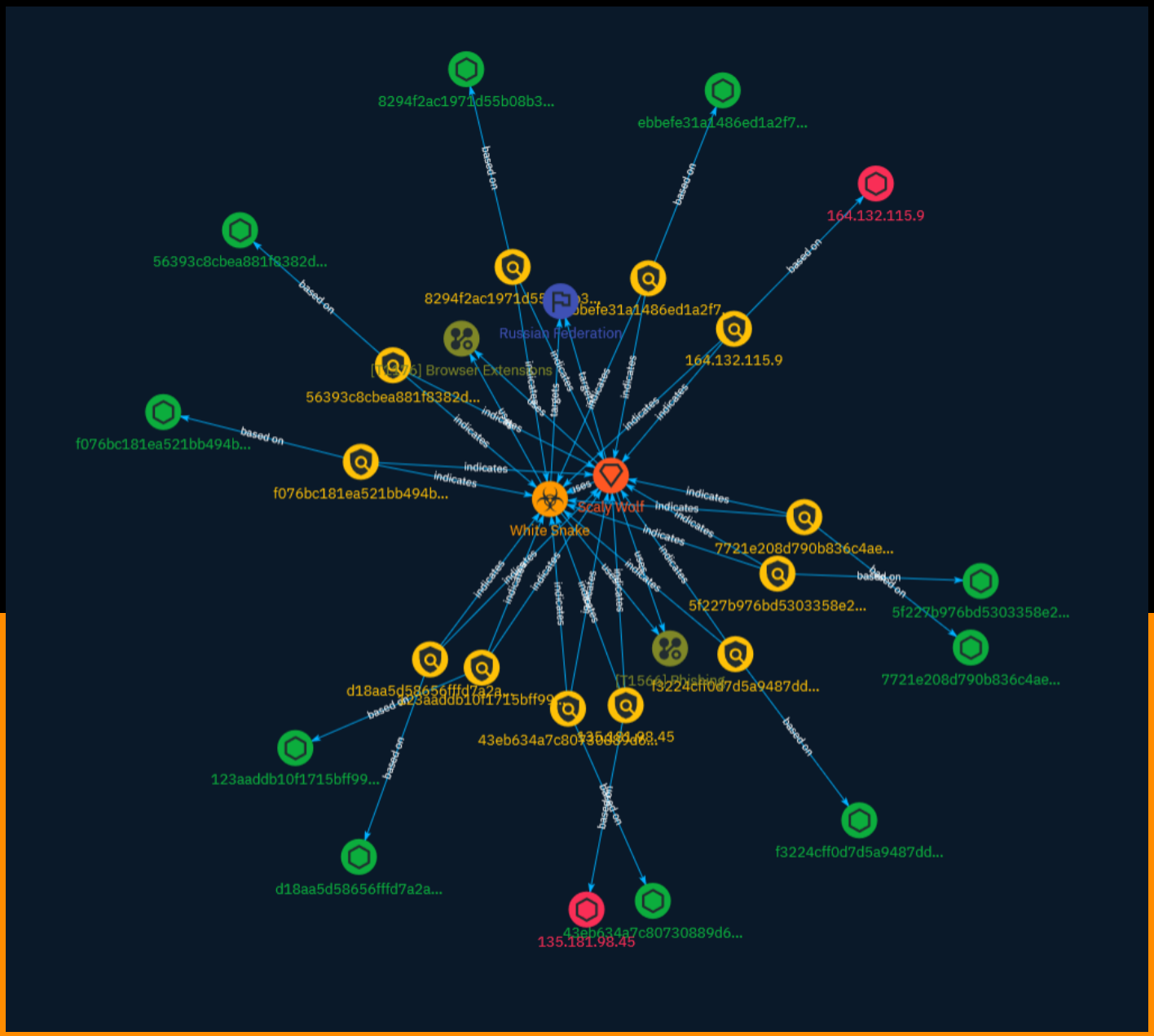

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Scaly Wolf, a group tracked by Bi.ZONE since summer 2023, conducted several phishing campaigns, disguising letters as requests from Russian regulators and law enforcement agencies. In all cases the text of the letter is written correctly from a legal point of view, which makes the mailing convincing, inspires the user's trust and encourages them to launch a malicious file. The implementation of the attack leads to the infection of systems with a payload in the form of the White Snake stealer,

Confidence

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

15 / 100

Content

N/A

Indicator

Name

f3224cff0d7d5a9487dd405aa53217992c4a11616cc9990ce1745bc1b008c3fe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f3224cff0d7d5a9487dd405aa53217992c4a11616cc9990ce1745bc1b008c3fe']

Name

f076bc181ea521bb494b799203945af4f2db1635b20cef395ad67819dd397f7b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f076bc181ea521bb494b799203945af4f2db1635b20cef395ad67819dd397f7b']

Name

ebbefe31a1486ed1a2f70538380dc899c2b0d704028cde9ba4dbf64b91293e3a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ebbefe31a1486ed1a2f70538380dc899c2b0d704028cde9ba4dbf64b91293e3a']

Name

d18aa5d58656fffd7a2a0a3d7f6f4e011bf0f39b8f89701b0e5263951e1ce90c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd18aa5d58656fffd7a2a0a3d7f6f4e011bf0f39b8f89701b0e5263951e1ce90c']

Name

8294f2ac1971d55b08b3cbed419929c24998d986b8d4ab5a126f6a901646ef99

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8294f2ac1971d55b08b3cbed419929c24998d986b8d4ab5a126f6a901646ef99']

Name

7721e208d790b836c4ae2ac3e7dde1ff799953e62932d9e418acfeecfcff43ca

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7721e208d790b836c4ae2ac3e7dde1ff799953e62932d9e418acfeecfcff43ca']

Name

5f227b976bd5303358e28a62103b7cc15210efdfa640b8e754f757690a716edb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5f227b976bd5303358e28a62103b7cc15210efdfa640b8e754f757690a716edb']

Name

56393c8cbea881f8382d195682787254bb576cc4b370410eb94fd93a00a82ee8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '56393c8cbea881f8382d195682787254bb576cc4b370410eb94fd93a00a82ee8']

Name

43eb634a7c80730889d64e6b13987a5bb4068dd463bc728db08d1eba3499d8d1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '43eb634a7c80730889d64e6b13987a5bb4068dd463bc728db08d1eba3499d8d1']

Name

123aaddb10f1715bff99617342df9cec7bb68d61abbc502f18938a7dcf0a4216

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '123aaddb10f1715bff99617342df9cec7bb68d61abbc502f18938a7dcf0a4216']

Name

164.132.115.9

Description

CC=GB ASN=AS16276 OVH SAS

Pattern Type

stix

Pattern

[ipv4-addr:value = '164.132.115.9']

Name

135.181.98.45

Description

CC=FI ASN=AS24940 Hetzner Online GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '135.181.98.45']

Name

f3224cff0d7d5a9487dd405aa53217992c4a11616cc9990ce1745bc1b008c3fe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f3224cff0d7d5a9487dd405aa53217992c4a11616cc9990ce1745bc1b008c3fe']

Name

f076bc181ea521bb494b799203945af4f2db1635b20cef395ad67819dd397f7b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f076bc181ea521bb494b799203945af4f2db1635b20cef395ad67819dd397f7b']

Name

ebbefe31a1486ed1a2f70538380dc899c2b0d704028cde9ba4dbf64b91293e3a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ebbefe31a1486ed1a2f70538380dc899c2b0d704028cde9ba4dbf64b91293e3a']

Name

d18aa5d58656fffd7a2a0a3d7f6f4e011bf0f39b8f89701b0e5263951e1ce90c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd18aa5d58656fffd7a2a0a3d7f6f4e011bf0f39b8f89701b0e5263951e1ce90c']

Name

8294f2ac1971d55b08b3cbed419929c24998d986b8d4ab5a126f6a901646ef99

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8294f2ac1971d55b08b3cbed419929c24998d986b8d4ab5a126f6a901646ef99']

Name

7721e208d790b836c4ae2ac3e7dde1ff799953e62932d9e418acfeecfcff43ca

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7721e208d790b836c4ae2ac3e7dde1ff799953e62932d9e418acfeecfcff43ca']

Name

5f227b976bd5303358e28a62103b7cc15210efdfa640b8e754f757690a716edb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5f227b976bd5303358e28a62103b7cc15210efdfa640b8e754f757690a716edb']

Name

56393c8cbea881f8382d195682787254bb576cc4b370410eb94fd93a00a82ee8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '56393c8cbea881f8382d195682787254bb576cc4b370410eb94fd93a00a82ee8']

Name

43eb634a7c80730889d64e6b13987a5bb4068dd463bc728db08d1eba3499d8d1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '43eb634a7c80730889d64e6b13987a5bb4068dd463bc728db08d1eba3499d8d1']

Name

123aaddb10f1715bff99617342df9cec7bb68d61abbc502f18938a7dcf0a4216

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '123aaddb10f1715bff99617342df9cec7bb68d61abbc502f18938a7dcf0a4216']

Name

164.132.115.9

Description

CC=GB ASN=AS16276 OVH SAS

Pattern Type

stix

Pattern

[ipv4-addr:value = '164.132.115.9']

Name
135.181.98.45
Description
CC=FI ASN=AS24940 Hetzner Online GmbH
Pattern Type
stix
Pattern
[ipv4-addr:value = '135.181.98.45']

Malware

Name
White Snake

Name
White Snake

Intrusion-Set

Name
Scaly Wolf

Name
Scaly Wolf

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)

Name

Browser Extensions

ID

T1176

Description

Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition) Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions. Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `.mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install configuration profiles, however `.mobileconfig` files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS) Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence. (Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension) There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions.(Citation: Stantinko Botnet) There have also been similar examples of extensions being used for command & control.(Citation: Chrome Extension C2 Malware)

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

Browser Extensions

ID

T1176

Description

Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and

customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition) Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions. Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `.mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install configuration profiles, however `.mobileconfig` files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS) Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence. (Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension) There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions.(Citation: Stantinko Botnet) There have also been similar examples of extensions being used for command & control.(Citation: Chrome Extension C2 Malware)

Country

Name
Russian Federation

Name
Russian Federation

StixFile

Value
f3224cff0d7d5a9487dd405aa53217992c4a11616cc9990ce1745bc1b008c3fe
f076bc181ea521bb494b799203945af4f2db1635b20cef395ad67819dd397f7b
ebbefe31a1486ed1a2f70538380dc899c2b0d704028cde9ba4dbf64b91293e3a
d18aa5d58656fffd7a2a0a3d7f6f4e011bf0f39b8f89701b0e5263951e1ce90c
8294f2ac1971d55b08b3cbed419929c24998d986b8d4ab5a126f6a901646ef99
7721e208d790b836c4ae2ac3e7dde1ff799953e62932d9e418acfeecfcff43ca
56393c8cbea881f8382d195682787254bb576cc4b370410eb94fd93a00a82ee8
5f227b976bd5303358e28a62103b7cc15210efdfa640b8e754f757690a716edb
43eb634a7c80730889d64e6b13987a5bb4068dd463bc728db08d1eba3499d8d1
123aaddb10f1715bff99617342df9cec7bb68d61abbc502f18938a7dcf0a4216
f3224cff0d7d5a9487dd405aa53217992c4a11616cc9990ce1745bc1b008c3fe
f076bc181ea521bb494b799203945af4f2db1635b20cef395ad67819dd397f7b
ebbefe31a1486ed1a2f70538380dc899c2b0d704028cde9ba4dbf64b91293e3a

d18aa5d58656fffd7a2a0a3d7f6f4e011bf0f39b8f89701b0e5263951e1ce90c

8294f2ac1971d55b08b3cbed419929c24998d986b8d4ab5a126f6a901646ef99

7721e208d790b836c4ae2ac3e7dde1ff799953e62932d9e418acfeecfcff43ca

56393c8cbea881f8382d195682787254bb576cc4b370410eb94fd93a00a82ee8

5f227b976bd5303358e28a62103b7cc15210efdfa640b8e754f757690a716edb

43eb634a7c80730889d64e6b13987a5bb4068dd463bc728db08d1eba3499d8d1

123aaddb10f1715bff99617342df9cec7bb68d61abbc502f18938a7dcf0a4216

IPv4-Addr

Value
164.132.115.9
135.181.98.45
164.132.115.9
135.181.98.45

External References

- https://bi.zone/expertise/blog/scaly-wolf-primenyaet-stiler-white-snake-protiv-rossiyskoy-promyshlennosti/
- https://otx.alienvault.com/pulse/65bcd7c264b9df47c21dbd21