Apr 10 2024

NETMANAGEIT

Intelligence Report

Active Nitrogen campaign delivered via malicious ads for PuTTY, FileZilla

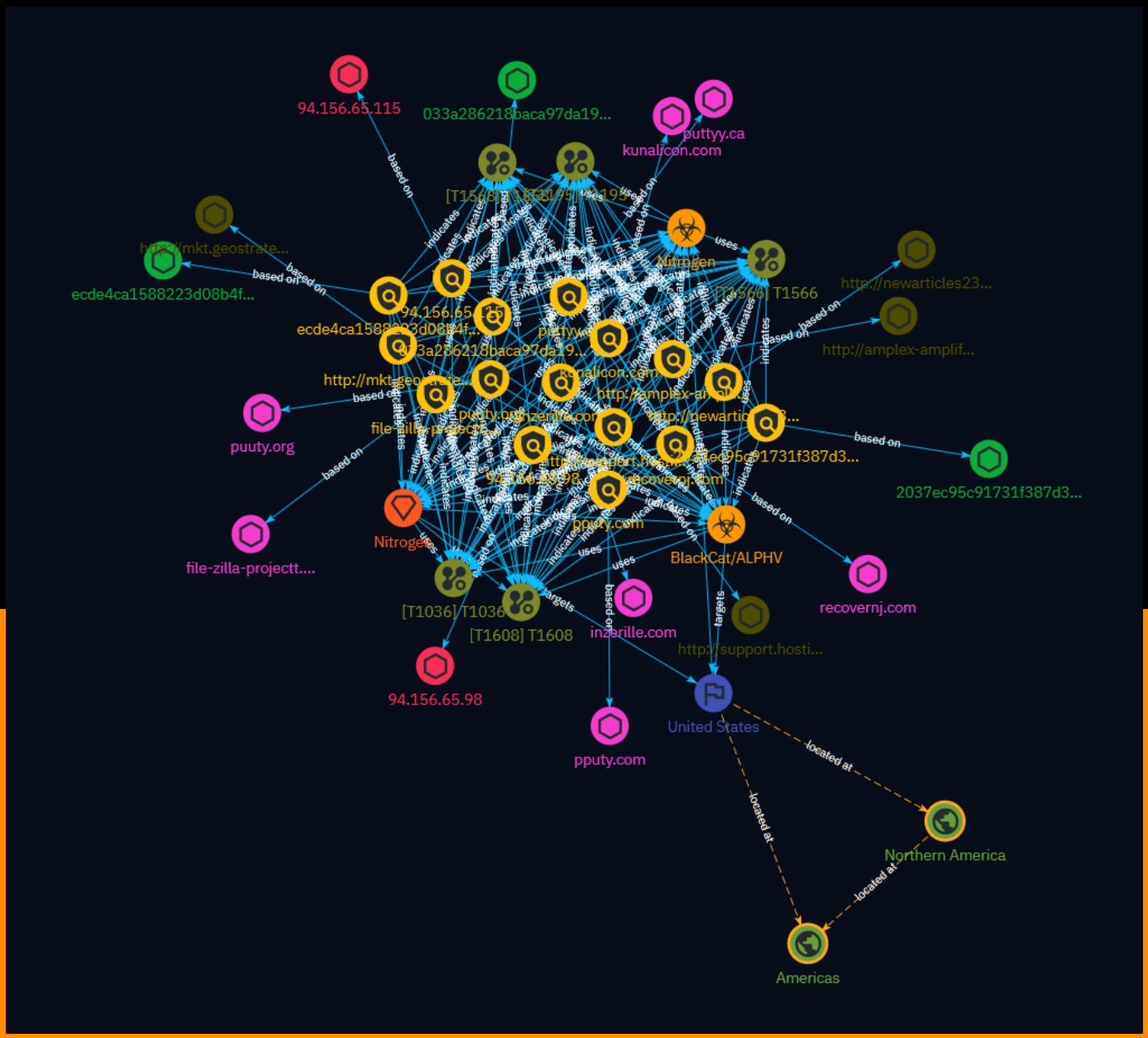

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This report describes an ongoing malicious campaign targeting system administrators through fraudulent online advertisements for popular utilities like PuTTY and FileZilla. Threat actors are using these ads to trick victims into downloading and running the Nitrogen malware, which is employed to gain initial access to private networks, leading to data theft and deployment of ransomware such as BlackCat/ALPHV. The tactics, techniques, and procedures (TTPs) used in this campaign, as well as indicators of compromise (IOCs), are provided to assist defenders in taking appropriate action.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

recovernj.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Health & fitness - **Domain Age:** {'human': '9 years ago', 'timestamp': 1424371356, 'iso': '2015-02-19T13:42:36-05:00'} - **IPQS: Domain:** recovernj.com - **IPQS: IP Address:** 104.21.31.122

Pattern Type

stix

Pattern

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

Name

puuty.org

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:**

{'human': '1 week ago', 'timestamp': 1712063537, 'iso': '2024-04-02T09:12:17-04:00'} - **IPQS: Domain:** puuty.org - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

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

Name

puttyy.ca

Description

- **Unsafe:** False - **Server:** LiteSpeed - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '5 days ago', 'timestamp': 1712324564, 'iso': '2024-04-05T09:42:44-04:00'} - **IPQS: Domain:** puttyy.ca - **IPQS: IP Address:** 82.221.129.44

Pattern Type

stix

Pattern

[domain-name:value = 'puttyy.ca']

Name

pputy.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '6 days ago', 'timestamp': 1712239346, 'iso': '2024-04-04T10:02:26-04:00'} - **IPQS: Domain:** pputy.com - **IPQS: IP Address:** 95.216.74.46

Pattern Type

stix

Pattern

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

Name

inzerille.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '12 years ago', 'timestamp': 1327078498, 'iso': '2012-01-20T11:54:58-05:00'} - **IPQS: Domain:** inzerille.com - **IPQS: IP Address:** 104.21.27.223

Pattern Type

stix

Pattern

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

Name

kunalicon.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Business - **Domain Age:** {'human': '14 years ago', 'timestamp': 1264410095, 'iso': '2010-01-25T04:01:35-05:00'} - **IPQS: Domain:** kunalicon.com - **IPQS: IP Address:** 172.67.204.2

Pattern Type

stix

Pattern

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

Name

file-zilla-projectt.org

Description

- **Unsafe:** False - **Server:** ESF - **Domain Rank:** 4 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Movies - **Domain Age:** {'human': '1 week ago', 'timestamp': 1712078297, 'iso': '2024-04-02T13:18:17-04:00'} - **IPQS: Domain:** youtube.com - **IPQS: IP Address:** 173.194.219.91

Pattern Type

stix

Pattern

[domain-name:value = 'file-zilla-projectt.org']

Name

http://support.hosting-hero.com/wp-includes/putty-64bit-0.80-installer.zip

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Business - **Domain Age:** {'human': '2 years ago', 'timestamp': 1649698747, 'iso': '2022-04-11T13:39:07-04:00'} - **IPQS: Domain:** support.hosting-hero.com - **IPQS: IP Address:** 51.89.21.67

Pattern Type

stix

Pattern

[url:value = 'http://support.hosting-hero.com/wp-includes/putty-64bit-0.80-installer.zip']

Name

http://newarticles23.com/wp-includes/putty-64bit-0.80-installer.zip

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 year ago', 'timestamp': 1673435590, 'iso': '2023-01-11T06:13:10-05:00'} - **IPQS: Domain:** newarticles23.com - **IPQS: IP Address:** 154.29.74.51

Pattern Type

stix

Pattern

[url:value = 'http://newarticles23.com/wp-includes/putty-64bit-0.80-installer.zip']

Name

http://mkt.geostrategy-ec.com/installer.zip

Description

- **Unsafe:** False - **Server:** Apache - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1620491643, 'iso': '2021-05-08T12:34:03-04:00'} - **IPQS: Domain:** mkt.geostrategy-ec.com - **IPQS: IP Address:** 192.254.189.58

Pattern Type

stix

Pattern

[url:value = 'http://mkt.geostrategy-ec.com/installer.zip']

Name

http://amplex-amplification.com/wp-includes/FileZilla_3.66.1_win64.zip

Description

- **Unsafe:** False - **Server:** Apache/2 - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Web Tracker - **Domain Age:**

{'human': '8 years ago', 'timestamp': 1461155353, 'iso': '2016-04-20T08:29:13-04:00'} - **IPQS: Domain:** amplex-amplification.com - **IPQS: IP Address:** 149.210.250.206

Pattern Type

stix

Pattern

[url:value = 'http://amplex-amplification.com/wp-includes/FileZilla_3.66.1_win64.zip']

Name

94.156.65.98

Description

- **Zip Code:** N/A - **ISP:** LIMENET - **ASN:** 394711 - **Organization:** LIMENET - **Is Crawler:** False - **Timezone:** Europe/Sofia - **Mobile:** False - **Host:** 94.156.65.98 - **Proxy:** True - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** BG - **Region:** Plovdiv - **City:** Karlovo - **Latitude:** 42.63 - **Longitude:** 24.8

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.156.65.98']

Name

ecde4ca1588223d08b4fc314d6cf4bce82989f6f6a079e3eefe8533222da6281

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ecde4ca1588223d08b4fc314d6cf4bce82989f6f6a079e3eefe8533222da6281']
Name
2037ec95c91731f387d3c0c908db95184c93c3b8412b6b3ca3219f9f8ff60945
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '2037ec95c91731f387d3c0c908db95184c93c3b8412b6b3ca3219f9f8ff60945']
Name
033a286218baca97da19810446f9ebbaf33be6549a5c260889d359e2062778cf
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '033a286218baca97da19810446f9ebbaf33be6549a5c260889d359e2062778cf']

Name

94.156.65.115

Description

- **Zip Code:** N/A - **ISP:** LIMENET - **ASN:** 394711 - **Organization:** LIMENET - **Is Crawler:** False - **Timezone:** Europe/Sofia - **Mobile:** False - **Host:** 94.156.65.115 - **Proxy:** False - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** BG - **Region:** Plovdiv - **City:** Karlovo - **Latitude:** 42.63 - **Longitude:** 24.8

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.156.65.115']

Malware

Name
BlackCat/ALPHV

Name
Nitrogen

Intrusion-Set

Name
Nitrogen

Attack-Pattern

Name
T1608
ID
T1608
Description
Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting. To support their operations, an adversary may need to take capabilities they developed ([Develop Capabilities](https://attack.mitre.org/techniques/T1587)) or obtained ([Obtain Capabilities](https://attack.mitre.org/techniques/T1588)) and stage them on infrastructure under their control. These capabilities may be staged on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)). Capabilities may also be staged on web services, such as GitHub or Pastebin, or on Platform-as-a-Service (PaaS) offerings that enable users to easily provision applications.(Citation: Volexity Ocean Lotus November 2020)(Citation: Dragos Heroku Watering Hole)(Citation: Malwarebytes Heroku Skimmers)(Citation: Netskope GCP Redirection)(Citation: Netskope Cloud Phishing) Staging of capabilities can aid the adversary in a number of initial access and post-compromise behaviors, including (but not limited to): * Staging web resources necessary to conduct [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) when a user browses to a site.(Citation: FireEye CFR Watering Hole 2012)(Citation: Gallagher 2015)(Citation: ATT ScanBox) * Staging web resources for a link target to be used with spearphishing.(Citation: Malwarebytes Silent Librarian October 2020)(Citation: Proofpoint TA407 September 2019) * Uploading malware or tools to a location accessible to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105).(Citation: Volexity Ocean Lotus November 2020) * Installing a previously acquired SSL/TLS certificate to use to encrypt

command and control traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with [Web Protocols](https://attack.mitre.org/techniques/T1071/001)).(Citation: DigiCert Install SSL Cert)

Name

T1568

ID

T1568

Description

Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control. Adversaries may use dynamic resolution for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ dynamic resolution as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)

Name

T1566

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

T1036

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

T1195

ID

T1195

Description

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including: * Manipulation of development tools * Manipulation of a development environment * Manipulation of source code repositories (public or private) * Manipulation of source code in open-source dependencies * Manipulation of software update/distribution mechanisms * Compromised/infected system images (multiple cases of removable media infected at the factory)(Citation: IBM Storwize)(Citation: Schneider Electric USB Malware) * Replacement of legitimate software with modified versions * Sales of modified/counterfeit products to legitimate distributors * Shipment interdiction While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.(Citation: Avast CCleaner3 2018)(Citation: Microsoft Dofoil 2018)(Citation: Command Five SK 2011) Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Symantec Elderwood Sept 2012)(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011) Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

Country

Name
United States

Region

Name
Northern America

Name
Americas

Domain-Name

Value
recovernj.com
puuty.org
puttyy.ca
pputy.com
kunalicon.com
inzerille.com
file-zilla-projectt.org

Url

Value
http://newarticles23.com/wp-includes/putty-64bit-0.80-installer.zip
http://support.hosting-hero.com/wp-includes/putty-64bit-0.80-installer.zip
http://mkt.geostrategy-ec.com/installer.zip
http://amplex-amplification.com/wp-includes/FileZilla_3.66.1_win64.zip

IPv4-Addr

Value
94.156.65.98
94.156.65.115

StixFile

Value
2037ec95c91731f387d3c0c908db95184c93c3b8412b6b3ca3219f9f8ff60945
ecde4ca1588223d08b4fc314d6cf4bce82989f6f6a079e3eefe8533222da6281
033a286218baca97da19810446f9ebbaf33be6549a5c260889d359e2062778cf

External References

- https://www.malwarebytes.com/blog/threat-intelligence/2024/04/active-nitrogen-campaign-delivered-via-malicious-ads-for-putty-filezilla
- https://otx.alienvault.com/pulse/66169113d5c8fae81c4f80ea