Apr 19 2024

NETMANAGEIT

Intelligence Report

Analysis of Pupy RAT Used in Attacks Against Linux Systems

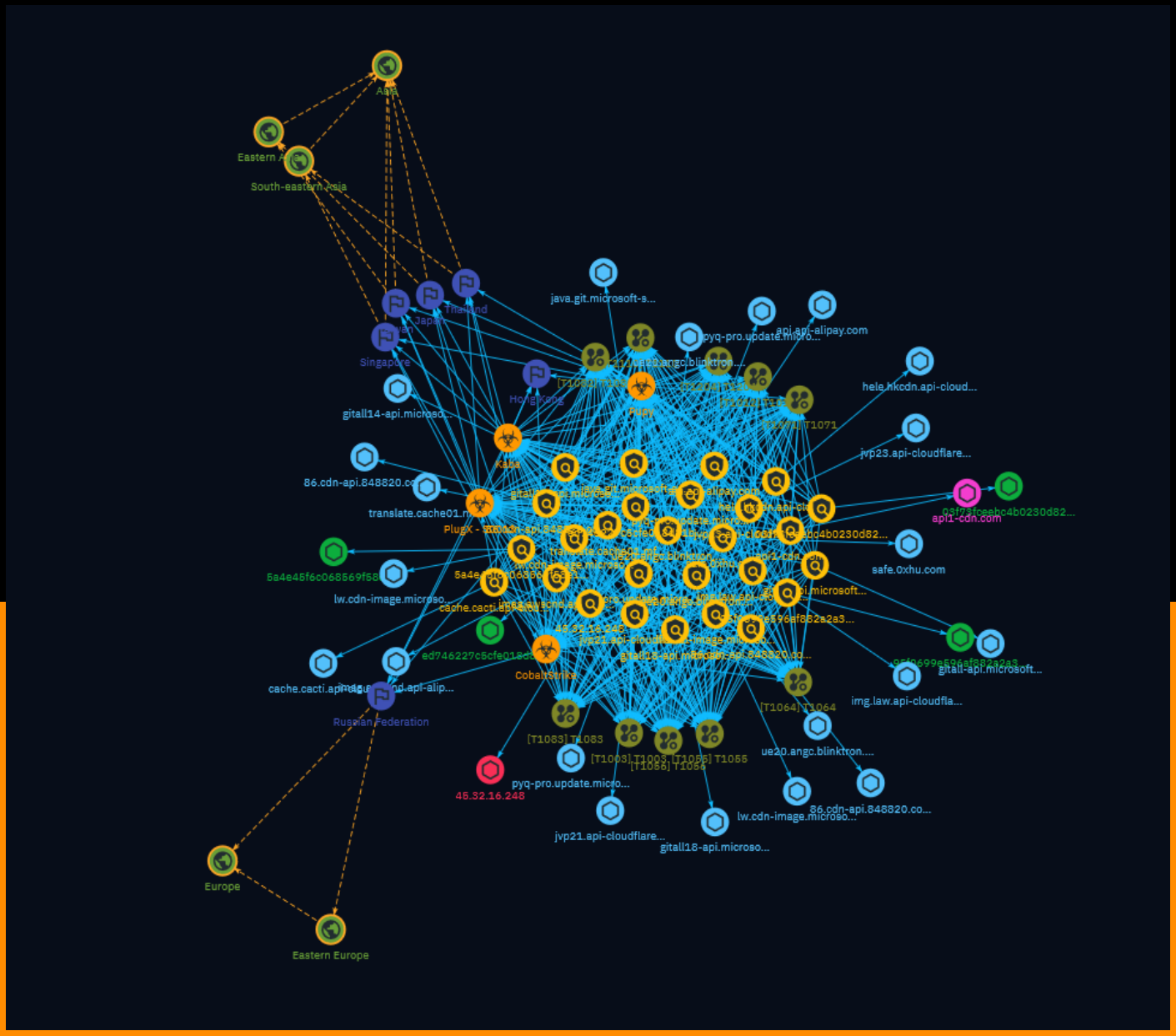

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Pupy RAT is a cross-platform remote access trojan that has been used by various threat actors, including APT groups, to target Linux and Windows systems. It provides features for remote control, information theft, and post-exploitation attacks. Recent examples include distribution alongside PlugX to target South Korea, and updated versions targeting Russia and Eastern Europe. To prevent infection, systems should be kept updated and anti-malware solutions used.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
ue20.angc.blinktron.com.bk1233.com
Pattern Type
stix
Pattern
[hostname:value = 'ue20.angc.blinktron.com.bk1233.com']
Name
ue20.angc.blinktron.com
Pattern Type
stix
Pattern
[hostname:value = 'ue20.angc.blinktron.com']
Name
translate.cache01.mfath.ugliquarie.com

Pattern Type
stix
Pattern
[hostname:value = 'translate.cache01.mfath.ugliquarie.com']
Name
safe.0xhu.com
Pattern Type
stix
Pattern
[hostname:value = 'safe.0xhu.com']
Name
pyq-pro.update.microsoft-shop.com.bk1233.com
Pattern Type
stix
Pattern
[hostname:value = 'pyq-pro.update.microsoft-shop.com.bk1233.com']
Name
pyq-pro.update.microsoft-shop.com

Pattern Type

stix

Pattern

[hostname:value = 'pyq-pro.update.microsoft-shop.com']

Name

lw.cdn-image.microsoft-shop.com.bk1233.com

Pattern Type

stix

Pattern

[hostname:value = 'lw.cdn-image.microsoft-shop.com.bk1233.com']

Name

lw.cdn-image.microsoft-shop.com

Pattern Type

stix

Pattern

[hostname:value = 'lw.cdn-image.microsoft-shop.com']

Name

jvp23.api-cloudflare.com

Pattern Type
stix
Pattern
[hostname:value = 'jvp23.api-cloudflare.com']
Name
jvp21.api-cloudflare.com
Pattern Type
stix
Pattern
[hostname:value = 'jvp21.api-cloudflare.com']
Name
java.git.microsoft-shop.com
Pattern Type
stix
Pattern
[hostname:value = 'java.git.microsoft-shop.com']
Name
img.law.api-cloudflare.com

Pattern Type
stix
Pattern
[hostname:value = 'img.law.api-cloudflare.com']
Name
imag.awscnd.api-alipay.com
Pattern Type
stix
Pattern
[hostname:value = 'imag.awscnd.api-alipay.com']
Name
hele.hkcdn.api-cloudflare.com
Pattern Type
stix
Pattern
[hostname:value = 'hele.hkcdn.api-cloudflare.com']
Name
gitall18-api.microsoft-shop.com

Pattern Type
stix
Pattern
[hostname:value = 'gitall18-api.microsoft-shop.com']
Name
gitall14-api.microsoft-shop.com
Pattern Type
stix
Pattern
[hostname:value = 'gitall14-api.microsoft-shop.com']
Name
gitall-api.microsoft-shop.com
Pattern Type
stix
Pattern
[hostname:value = 'gitall-api.microsoft-shop.com']
Name
cache.cacti.api-cloudflare.com

Pattern Type
stix
Pattern
[hostname:value = 'cache.cacti.api-cloudflare.com']
Name
api.api-alipay.com
Pattern Type
stix
Pattern
[hostname:value = 'api.api-alipay.com']
Name
86.cdn-api.848820.com.bk1233.com
Pattern Type
stix
Pattern
[hostname:value = '86.cdn-api.848820.com.bk1233.com']
Name
86.cdn-api.848820.com

Pattern Type

stix

Pattern

[hostname:value = '86.cdn-api.848820.com']

Name

api1-cdn.com

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '1 day ago', 'timestamp': 1713449073, 'iso': '2024-04-18T10:04:33-04:00'} - **IPQS: Domain:** api1-cdn.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'api1-cdn.com']

Name

45.32.16.248

Description

- **Zip Code:** N/A - **ISP:** Vultr - **ASN:** 20473 - **Organization:** Vultr - **Is Crawler:** False - **Timezone:** Asia/Tokyo - **Mobile:** False - **Host:**

45.32.16.248.vultrusercontent.com - **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:** JP - **Region:** Tokyo - **City:** Tokyo - **Latitude:** 35.69 - **Longitude:** 139.75

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.32.16.248']

Name

ed746227c5cfe018d81b53f37f74fe0f64496503ec23d2b65b67244b1d1a26fd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ed746227c5cfe018d81b53f37f74fe0f64496503ec23d2b65b67244b1d1a26fd']

Name

95f0699e596af882a2a3869c2f3f76ffd9382bf7e3686b28961128869e2c515f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '95f0699e596af882a2a3869c2f3f76ffd9382bf7e3686b28961128869e2c515f']

Name

5a4e45f6c068569f58e191a306119159181d23d8864a04d125c7a8119198f35e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5a4e45f6c068569f58e191a306119159181d23d8864a04d125c7a8119198f35e']

Name

03f73fceebc4b0230d82cc26509aa32f36c1b34494ad2ed297b2e65eebbdb31a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '03f73fceebc4b0230d82cc26509aa32f36c1b34494ad2ed297b2e65eebbdb31a']

Malware

Name
PlugX - S0013
Name
Pupy
Name
CobaltStrike
Name
Kaba
Description
[PlugX](https://attack.mitre.org/software/S0013) is a remote access tool (RAT) with modular plugins that has been used by multiple threat groups.(Citation: Lastline PlugX Analysis)(Citation: FireEye Clandestine Fox Part 2)(Citation: New DragonOK)(Citation: Dell TG-3390)

Country

Name
Hong Kong
Name
Russian Federation
Name
Singapore
Name
Thailand
Name
Taiwan
Name
Japan

Attack-Pattern

Name
T1012
ID
T1012
Description
Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. The Registry contains a significant amount of information about the operating system, configuration, software, and security.(Citation: Wikipedia Windows Registry) Information can easily be queried using the [Reg](https://attack.mitre.org/software/S0075) utility, though other means to access the Registry exist. Some of the information may help adversaries to further their operation within a network. Adversaries may use the information from [Query Registry](https://attack.mitre.org/techniques/T1012) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.
Name
T1056
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

T1110

ID

T1110

Description

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes. Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), [Account Discovery](https://attack.mitre.org/techniques/T1087), or [Password Policy Discovery](https://attack.mitre.org/techniques/T1201). Adversaries may also combine brute forcing activity with behaviors such as [External Remote Services](https://attack.mitre.org/techniques/T1133) as part of Initial Access.

Name

T1064

ID

T1064

Description

This technique has been deprecated. Please use [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) where appropriate. Adversaries may use scripts to aid in operations and perform multiple actions that would otherwise be manual. Scripting is useful for speeding up operational tasks and reducing the time required to gain access to critical resources. Some scripting languages may be used to bypass process monitoring mechanisms by directly interacting with the operating system at an API level instead of calling other programs. Common scripting languages for Windows include VBScript and [PowerShell](https://attack.mitre.org/techniques/T1086) but could also be in the form of command-line batch scripts. Scripts can be embedded inside Office documents as macros that can be set to execute when files used in [Spearphishing Attachment](https://attack.mitre.org/techniques/T1193) and other types of spearphishing are opened. Malicious embedded macros are an alternative means of execution than software exploitation through [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203), where adversaries will rely on macros being allowed or that the user will accept to activate them. Many popular offensive frameworks exist which use forms of scripting for security testers and adversaries alike. Metasploit (Citation: Metasploit_Ref), Veil (Citation: Veil_Ref), and PowerSploit (Citation: Powersploit) are three examples that are popular among penetration testers for exploit and post-compromise operations and include many features for evading defenses. Some adversaries are known to use PowerShell. (Citation: Alperovitch 2014)

Name

T1083

ID

T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the

information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A)

Name

T1204

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

T1055

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

T1082

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example,

adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

Name

T1071

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

T1003

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.

Region

Name
Eastern Europe
Name
Europe
Name
South-eastern Asia
Name
Eastern Asia
Name
Asia

Hostname

Value
ue20.angc.blinktron.com.bk1233.com
ue20.angc.blinktron.com
translate.cache01.mfath.ugliquarie.com
safe.0xhu.com
pyq-pro.update.microsoft-shop.com.bk1233.com
pyq-pro.update.microsoft-shop.com
lw.cdn-image.microsoft-shop.com.bk1233.com
lw.cdn-image.microsoft-shop.com
jvp23.api-cloudflare.com
jvp21.api-cloudflare.com
java.git.microsoft-shop.com
img.law.api-cloudflare.com
imag.awscnd.api-alipay.com

hele.hkcdn.api-cloudflare.com
gitall18-api.microsoft-shop.com
gitall14-api.microsoft-shop.com
gitall-api.microsoft-shop.com
cache.cacti.api-cloudflare.com
api.api-alipay.com
86.cdn-api.848820.com.bk1233.com
86.cdn-api.848820.com

Domain-Name

Value
api1-cdn.com

IPv4-Addr

Value
45.32.16.248

StixFile

Value
ed746227c5cfe018d81b53f37f74fe0f64496503ec23d2b65b67244b1d1a26fd
95f0699e596af882a2a3869c2f3f76ffd9382bf7e3686b28961128869e2c515f
03f73fceebc4b0230d82cc26509aa32f36c1b34494ad2ed297b2e65eebbdb31a
5a4e45f6c068569f58e191a306119159181d23d8864a04d125c7a8119198f35e

External References

- https://asec.ahnlab.com/en/64258/
- https://otx.alienvault.com/pulse/6622761dcbaadd6c53fd281f