

NETMANAGEIT

Intelligence Report

New Go loader pushes Rhadamanthys stealer

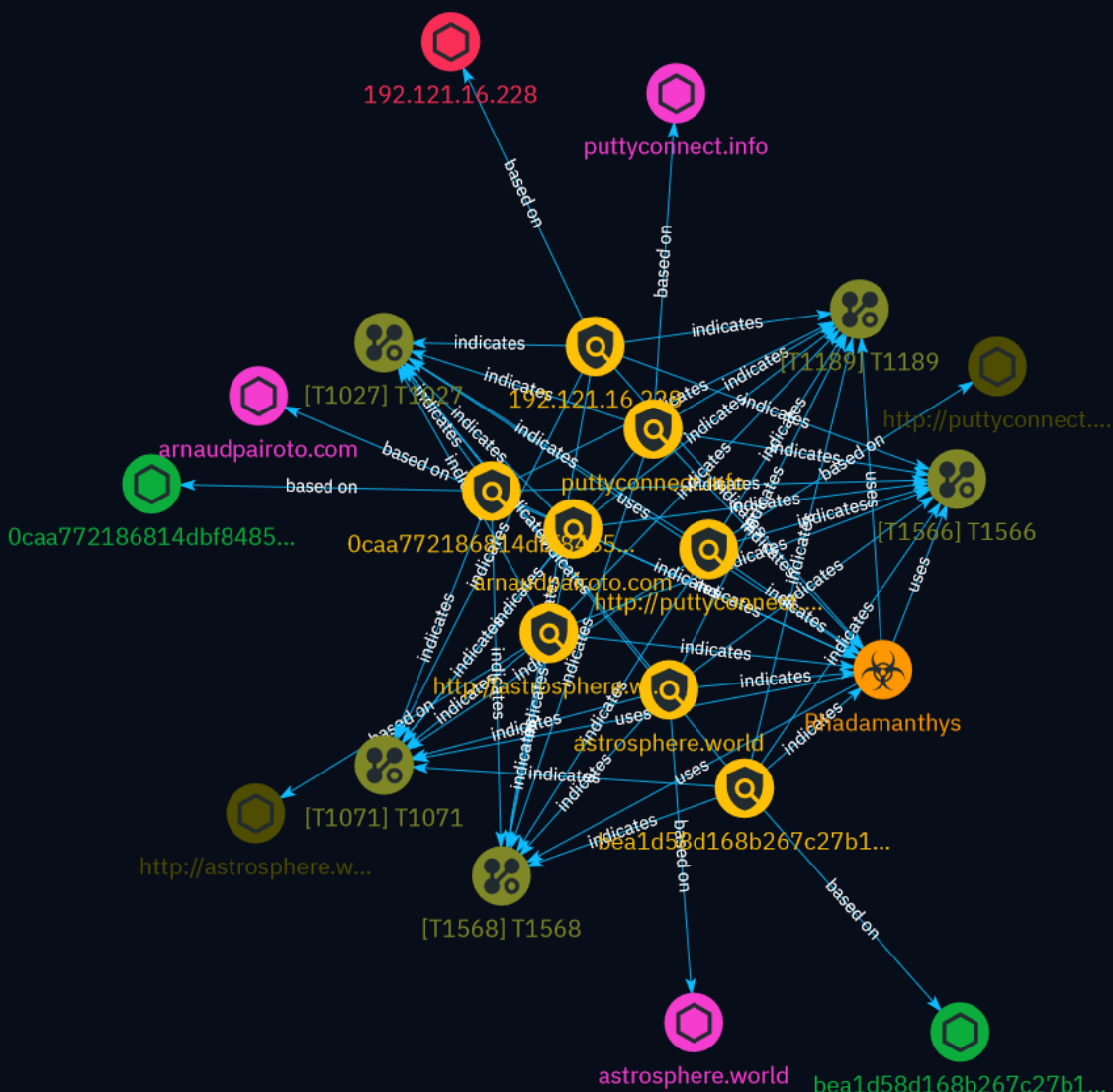


Table of contents

Overview

● Description	4
● Confidence	4
● Content	5

Entities

● Indicator	6
● Malware	10
● Attack-Pattern	11

Observables

● Domain-Name	15
● Url	16
● IPv4-Addr	17
● StixFile	18



External References

- External References

19

Overview

Description

A recent malvertising campaign targeted system administrators by impersonating the PuTTY website. Clicking on the fake download deployed a new Go-based malware loader that retrieved the Rhadamanthys stealer payload. The threat actor likely controls both the malvertising and loader infrastructure to enable end-to-end deployment of malware.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

puttyconnect.info

Pattern Type

stix

Pattern

[domain-name:value = 'puttyconnect.info']

Name

astrosphere.world

Pattern Type

stix

Pattern

[domain-name:value = 'astrosphere.world']

Name

arnaudpairoto.com

Pattern Type

stix

Pattern

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

Name

http://puttyconnect.info/1.php

Pattern Type

stix

Pattern

[url:value = 'http://puttyconnect.info/1.php']

Name

http://astrosphere.world/onserver3.php

Pattern Type

stix

Pattern

[url:value = 'http://astrosphere.world/onserver3.php']

Name

192.121.16.228

Description

CC=NL ASN=AS57169 EDIS GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.121.16.228']

Name

bea1d58d168b267c27b1028b47bd6ad19e249630abb7c03cfffede8568749203

Pattern Type

stix

Pattern

[file:hashes:'SHA-256' =
'bea1d58d168b267c27b1028b47bd6ad19e249630abb7c03cfffede8568749203']

Name

0caa772186814dbf84856293f102c7538980bcd31b70c1836be236e9fa05c48d

Pattern Type

stix

Pattern

[file:hashes!'SHA-256' =
'0caa772186814dbf84856293f102c7538980bcd31b70c1836be236e9fa05c48d']

Malware

Name

Rhadamanthys

Attack-Pattern

Name

T1189

ID

T1189

Description

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](<https://attack.mitre.org/techniques/T1550/001>). Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](<https://attack.mitre.org/techniques/T1608/004>)), including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting * Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary * Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising](<https://attack.mitre.org/techniques/T1583/008>)) * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable

version. * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. * In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](<https://attack.mitre.org/techniques/T1190>), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](<https://attack.mitre.org/techniques/T1528>), like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

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

T1027

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

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

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.

Domain-Name

Value

puttyconnect.info

astrosphere.world

arnaudpairoto.com

Url

Value

<http://puttyconnect.info/1.php>

<http://astrosphere.world/onserver3.php>

IPv4-Addr

Value

192.121.16.228

StixFile

Value

bea1d58d168b267c27b1028b47bd6ad19e249630abb7c03cfffede8568749203

0caa772186814dbf84856293f102c7538980bcd31b70c1836be236e9fa05c48d

External References

-
- <https://www.malwarebytes.com/blog/threat-intelligence/2024/03/new-go-loader-pushes-rhadamanthys>
-
- <https://otx.alienvault.com/pulse/66017db30442d5ba6d624260>