NETMANAGEIT

Intelligence Report

One year later, Rhadamanthys is still dropped via malvertising

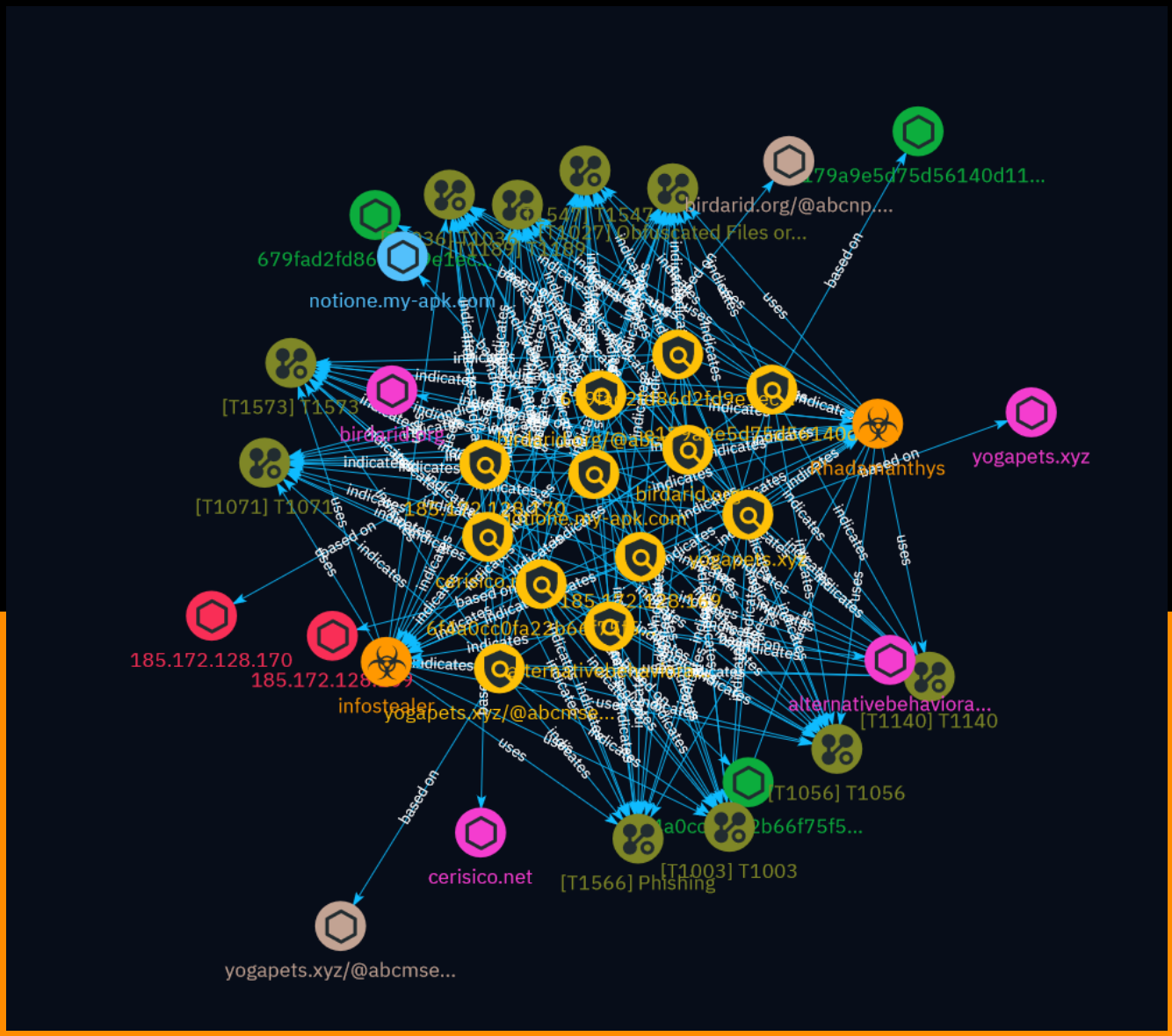

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A recent malvertising campaign is distributing the Rhadamanthys infostealer by impersonating popular software brands in search ads. Clicking the fake ads leads to decoy sites where users are tricked into downloading malware droppers, which retrieve the final payload from a pastebin site.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
notione.my-apk.com
Pattern Type
stix
Pattern
[hostname:value = 'notione.my-apk.com']
Name
yogapets.xyz/@abcmse1.exe
Pattern Type
stix
Pattern
[email-addr:value = 'yogapets.xyz/@abcmse1.exe']
Name
birdarid.org/@abcnp.exe

Pattern Type
stix
Pattern
[email-addr:value = 'birdarid.org/@abcnp.exe']
Name
yogapets.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'yogapets.xyz']
Name
cerisico.net
Pattern Type
stix
Pattern
[domain-name:value = 'cerisico.net']
Name
birdarid.org

Pattern Type

stix

Pattern

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

Name

alternativebehavioralconcepts.org

Pattern Type

stix

Pattern

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

Name

185.172.128.170

Description

ISP: TNSECURITY LTD **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAZbTeIU6HquogznmvASFA8k e3frGg2Lcj2GA2WwdaqD0HiHP6KZ15A07xHtS9g/PMy2CdPg/JQxBcAfpWlF7OE= Fingerprint: 4a:3d:b4:0c:9a:3b:c1:5e:a2:cb:60:c0:c2:39:fa:ad Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com

aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK X-Powered-By: Express Content-Type: text/html; charset=utf-8 Content-Length: 5817 ETag: W/"16b9-P4FO4C1Sw7102MABOYgW6QVW0wI" Date: Fri, 23 Feb 2024 19:49:03 GMT Connection: keep-alive Keep-Alive: timeout=5 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.172.128.170']

Name

e179a9e5d75d56140d11cbd29d92d8137b0a73f964dd3cfd46564ada572a3109

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e179a9e5d75d56140d11cbd29d92d8137b0a73f964dd3cfd46564ada572a3109']

Name

6f4a0cc0fa22b66f75f5798d3b259d470beb776d79de2264c2affc0b5fa924a2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6f4a0cc0fa22b66f75f5798d3b259d470beb776d79de2264c2affc0b5fa924a2']

Name

679fad2fd86d2fd9e1ec38fa15280c1186f35343583c7e83ab382b8c255f9e18

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '679fad2fd86d2fd9e1ec38fa15280c1186f35343583c7e83ab382b8c255f9e18']

Name

185.172.128.169

Description

ISP: TNSECURITY LTD **OS:** - ---------- Services: **21:** ``` 220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220-You are user number 1 of 50 allowed. 220-Local time is now 04:26. Server port: 21. 220-This is a private system - No anonymous login 220-IPv6 connections are also welcome on this server. 220 You will be disconnected after 15 minutes of inactivity. 421 Unable to read the indexed puredb file (or old format detected) - Try pure-pw mkdb 211-Extensions supported: UTF8 EPRT IDLE MDTM SIZE MFMT REST STREAM MLST type*;size*;sizd*;modify*;UNIX.mode*;UNIX.uid*;UNIX.gid*;unique*; MLSD PRET AUTH TLS PBSZ PROT TVFS ESTA PASV EPSV SPSV ESTP 211 End. ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Tue, 27 Feb 2024 22:22:59 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Fri, 14 Jan 2022 07:23:06 GMT Connection: keep-alive ETag: "61e124da-267" Accept-Ranges: bytes ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx Date: Sun, 25 Feb 2024 21:32:25 GMT Content-Type: text/html Content-Length: 831 Last-Modified: Fri, 23 Feb 2024 09:56:46 GMT Connection: keep-alive

ETag: "65d86bde-33f" Strict-Transport-Security: max-age=31536000 Accept-Ranges: bytes ```
HEARTBLEED: 2024/02/25 21:32:47 185.172.128.169:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.172.128.169']

Malware

Name
Rhadamanthys

Name
infostealer

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)s, 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

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

T1573

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

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

T1140

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

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

T1547

ID

T1547

Description

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending

features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

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.

Hostname

Value
notione.my-apk.com

Email-Addr

Value
birdarid.org/@abcnp.exe
yogapets.xyz/@abcmse1.exe

Domain-Name

Value
yogapets.xyz
cerisico.net
birdarid.org
alternativebehavioralconcepts.org

IPv4-Addr

Value
185.172.128.170
185.172.128.169

StixFile

Value
e179a9e5d75d56140d11cbd29d92d8137b0a73f964dd3cfd46564ada572a3109
6f4a0cc0fa22b66f75f5798d3b259d470beb776d79de2264c2affc0b5fa924a2
679fad2fd86d2fd9e1ec38fa15280c1186f35343583c7e83ab382b8c255f9e18

External References

- https://www.malwarebytes.com/blog/threat-intelligence/2024/02/one-year-later-rhadamanthys-is-still-dropped-via-malvertising
- https://otx.alienvault.com/pulse/65e0cd34e59d92040eea0de7