Apr 04 2024

NETMANAGEIT

Intelligence Report

"Hey, This Isn't the Right Site!" Distribution of Malware Exploiting Google Ads Tracking

birdarid.org
http://birdarid.org...
https://notione.my-a...
uses
uses
[T1497]...
https://cerisico.net
infostealer
[T1020] T1020
slashidot.org
https://textbin.net...
yogapets.xyz
indicates
[T1574] Hijack Execution Flow
https://yogapets.xyz...
[T1020] Automated Exfiltration
based on
notione.my-apk.com
notione.my-apk.com
[T1055] T1055
alternativebehaviora...
https://alternativeb...
6fdd12c30b3db365214...
cerisico.net
https://bookpool.org...
based on
[T1204] T1204
bookpool.org
Rhadamanthys
[T1566] T1566
[T1195] T1195
6fdd12c30b3db365214a...
https://slashidot.or...
cerisico.net

Table of contents

Overview

Entities

Observables

External References

Overview

Description

AhnLab Security Intelligence Center has detected a malware strain disguised as installers for popular groupware applications like Notion and Slack. The malware is distributed through Google Ads tracking, where clicking on ads redirects users to websites that trick them into downloading and executing malicious files. Once executed, the malware fetches payloads from attacker-controlled servers and injects malicious code into legitimate Windows system files to steal private data.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
slashidot.org
Pattern Type
stix
Pattern
[domain-name:value = 'slashidot.org']
Name
bookpool.org
Pattern Type
stix
Pattern
[domain-name:value = 'bookpool.org']
Name
https://yogapets.xyz/@abcmse1.exe

Pattern Type

stix

Pattern

[url:value = 'https://yogapets.xyz/@abcmse1.exe']

Name

https://textbin.net/raw/oumciccl6b

Pattern Type

stix

Pattern

[url:value = 'https://textbin.net/raw/oumciccl6b']

Name

https://slashidot.org/@abcDP.exe

Pattern Type

stix

Pattern

[url:value = 'https://slashidot.org/@abcDP.exe']

Name

https://cerisico.net/

Pattern Type

stix

Pattern

[url:value = 'https://cerisico.net/']

Name

https://bookpool.org/@Base.exe

Pattern Type

stix

Pattern

[url:value = 'https://bookpool.org/@Base.exe']

Name

https://alternativebehavioralconcepts.org/databack/notwin.php

Pattern Type

stix

Pattern

[url:value = 'https://alternativebehavioralconcepts.org/databack/notwin.php']

Name

http://birdarid.org/@abcDS.exe

Pattern Type

stix

Pattern

[url:value = 'http://birdarid.org/@abcDS.exe']

Name

6fdd12c30b3db365214a0c7bf6e10801c792cfd7fbb791944eaa042355dd2d0b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6fdd12c30b3db365214a0c7bf6e10801c792cfd7fbb791944eaa042355dd2d0b']

Name

https://notione.my-apk.com

Pattern Type

stix

Pattern

[url:value = 'https://notione.my-apk.com']

Name

notione.my-apk.com

Pattern Type

stix

Pattern

[hostname:value = 'notione.my-apk.com']

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']

Malware

Name
Rhadamanthys

Name
infostealer

Attack-Pattern

Name

Hijack Execution Flow

ID

T1574

Description

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution. There are many ways an adversary may hijack the flow of execution, including by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be intercepted. Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads.

Name

Automated Exfiltration

ID

T1020

Description

Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection. When automated exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as [Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1041) and [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048).

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

Virtualization/Sandbox Evasion

ID

T1497

Description

Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) during automated discovery to shape follow-on behaviors.(Citation: Deloitte Environment Awareness) Adversaries may use several methods to accomplish [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) such as checking for security monitoring tools (e.g., Sysinternals, Wireshark, etc.) or other system artifacts associated with analysis or virtualization. Adversaries may also check for legitimate user activity to help determine if it is in an analysis environment. Additional methods include use of sleep timers or loops within malware code to avoid operating within a temporary sandbox. (Citation: Unit 42 Pirpi July 2015)

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

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)

Domain-Name

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

Url

Value
https://yogapets.xyz/@abcmse1.exe
https://textbin.net/raw/oumciccl6b
https://slashidot.org/@abcDP.exe
https://cerisico.net/
https://bookpool.org/@Base.exe
https://alternativebehavioralconcepts.org/databack/notwin.php
http://birdarid.org/@abcDS.exe
https://notione.my-apk.com

StixFile

Value
6fdd12c30b3db365214a0c7bf6e10801c792cfd7fbb791944eaa042355dd2d0b

Hostname

Value
notione.my-apk.com

External References

- https://asec.ahnlab.com/en/63477/
- https://otx.alienvault.com/pulse/660b1c21743577029836e950