Sep 07 2023

NETMANAGEIT

Intelligence Report

How an APT technique turns to be a public Red Team Project

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A report by Yoroi's Malware ZLab and Palo Alto Networks explores the art of DLL Sideloading, as well as the evolving tactics of the APT29 cyber-espionage team.

Confidence

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

15 / 100

Indicator

Name
bcc7c41209afcf67858b3ef80f0afa1eabf2e4faadcaa23bacc9aa5d57b9d836
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'bcc7c41209afcf67858b3ef80f0afa1eabf2e4faadcaa23bacc9aa5d57b9d836']
Name
c8ca2199aabae9af5c59e658d11a41f76af4576204c23bf5762825171c56e5e8
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'c8ca2199aabae9af5c59e658d11a41f76af4576204c23bf5762825171c56e5e8']
Name

4240201a9d957a01676ab7165d112d03c7dbdba7b34778407e7b73344b3fd158

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4240201a9d957a01676ab7165d112d03c7dbdba7b34778407e7b73344b3fd158']

Name

ffd5114ffb3a2f66757cecb2fb0079cceaa42a4b42ded566e76b7d58b4effac5

Description

ConventionEngine_Term_Users

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ffd5114ffb3a2f66757cecb2fb0079cceaa42a4b42ded566e76b7d58b4effac5']

Name

5e352c8f55ed9be1142b09e13df7b3efac7ea9e6173b6792d9a5c44dedc3a4ee

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5e352c8f55ed9be1142b09e13df7b3efac7ea9e6173b6792d9a5c44dedc3a4ee']

Name

311372f5957d95231e50389495c6dc506c57aea4

Description

Rule for OneDriveUpdate EXE Repackage

Pattern Type

yara

Pattern

rule onedriveupdate_exe_repackage { /* 4240201a9d957a01676ab7165d112d03c7dbdba7b34778407e7b73344b3fd158 */ meta: author = "Yoroi Malware ZLab" description = "Rule for OneDriveUpdate EXE Repackage" last_updated = "2023-07-27" tlp = "WHITE" category = "informational" strings: $1 = {4? 83 f8 ?? 4? 8d 52 01 4? 8b ?? 4? 0f 45 c8 4? ff c0 0f b6 84 ?? ?? ?? ?? ?? 30 4? ?? 4? 8d 41 01 4? 81 f8 ?? ?? ?? ??} /* .text:0000000140001660 48 83 F8 1C cmp rax, 1Ch .text:0000000140001664 48 8D 52 01 lea rdx, [rdx+1] .text:0000000140001668 48 8B CE mov rcx, rsi .text:000000014000166B 48 0F 45 C8 cmovnz rcx, rax .text:000000014000166F 41 FF C0 inc r8d .text:0000000140001672 0F B6 84 0D 18 01 00 00 movzx eax, [rbp+rcx+480h+var_368] .text:000000014000167A 30 42 FF xor [rdx-1], al .text:000000014000167D 48 8D 41 01 lea rax, [rcx+1] .text:0000000140001681 41 81 F8 28 03 00 00 cmp r8d, 328h */ condition: $1 }

Name

02214c0c7ee94e8efebd3bebe6f788ef3390d8a9

Description

Rule for OneDriveUpdate DLL Repackage

Pattern Type

yara

Pattern

rule onedriveupdate_dll_repackage { /* 6f08ce39072bdacf4a98578ca6b508b68b2c78ed2a378c73a1c87595f9d0c591 a855012a9e198837eae04295de56d28e9258da1e933c56805b39b1f8d0d03c56 bcc7c41209afcf67858b3ef80f0afa1eabf2e4faadcaa23bacc9aa5d57b9d836 c8ca2199aabae9af5c59e658d11a41f76af4576204c23bf5762825171c56e5e8 f62e0ec08b15f9a4f3178c77ad540bd7369d1341472fdcbc88aecc0ed29c0387 */ meta: author = "Yoroi Malware ZLab" description = "Rule for OneDriveUpdate DLL Repackage" last_updated = "2023-07-27" tlp = "WHITE" category = "informational" strings: $1 = {4? 83 f8 ?? 4? 8d 5? ?? 4? 8b cf 4? 0f 45 c8 4? ff c1 0f b6 84 0d 18 01 00 00 4? 8d 41 01 30 42 ff 4? 63 c1 4? 3b c7} /* .text:00000001800012E0 49 83 F8 1C cmp r8, 1Ch .text:00000001800012E4 48 8D 52 01 lea rdx, [rdx+1] .text:00000001800012E8 49 8B CF mov rcx, r15 .text:00000001800012EB 49 0F 45 C8 cmovnz rcx, r8 .text:00000001800012EF 41 FF C1 inc r9d .text:00000001800012F2 0F B6 84 0D 18 01 00 00 movzx eax, [rbp+rcx+150h+var_38] .text:00000001800012FA 4C 8D 41 01 lea r8, [rcx+1] .text:00000001800012FE 30 42 FF xor [rdx-1], al .text:0000000180001301 49 63 C1 movsxd rax, r9d .text:0000000180001304 48 3B C7 cmp rax, rdi */ condition: $1 }

Name

2d866ccf2b24e3b922abb3d3980c2ed752d86b6c017bc2bf7a1c209aa9464643

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2d866ccf2b24e3b922abb3d3980c2ed752d86b6c017bc2bf7a1c209aa9464643']

Name

664b8fbd825db53ccfc5712f7cd54c71bf53f0791b1bd42af8517729653ae7ae

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '664b8fbd825db53ccfc5712f7cd54c71bf53f0791b1bd42af8517729653ae7ae']

Name

dda686d6fda52c6ab3c084b7024cfc68dba60ae2143a1095659b795f84cf2329

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dda686d6fda52c6ab3c084b7024cfc68dba60ae2143a1095659b795f84cf2329']

Name

a855012a9e198837eae04295de56d28e9258da1e933c56805b39b1f8d0d03c56

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a855012a9e198837eae04295de56d28e9258da1e933c56805b39b1f8d0d03c56']

Name

6f08ce39072bdacf4a98578ca6b508b68b2c78ed2a378c73a1c87595f9d0c591

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6f08ce39072bdacf4a98578ca6b508b68b2c78ed2a378c73a1c87595f9d0c591']

Name

17494a7687c8e57be6fcd486bc34aaa120105729196474ccffd078d8aa256f87

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '17494a7687c8e57be6fcd486bc34aaa120105729196474ccffd078d8aa256f87']

Name

f62e0ec08b15f9a4f3178c77ad540bd7369d1341472fdcbc88aecc0ed29c0387

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f62e0ec08b15f9a4f3178c77ad540bd7369d1341472fdcbc88aecc0ed29c0387']

Intrusion-Set

Name

APT29

Description

[APT29](https://attack.mitre.org/groups/G0016) is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).(Citation: White House Imposing Costs RU Gov April 2021)(Citation: UK Gov Malign RIS Activity April 2021) They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. [APT29](https://attack.mitre.org/groups/G0016) reportedly compromised the Democratic National Committee starting in the summer of 2015.(Citation: F-Secure The Dukes)(Citation: GRIZZLY STEPPE JAR)(Citation: Crowdstrike DNC June 2016)(Citation: UK Gov UK Exposes Russia SolarWinds April 2021) In April 2021, the US and UK governments attributed the [SolarWinds Compromise](https://attack.mitre.org/campaigns/C0024) to the SVR; public statements included citations to [APT29](https://attack.mitre.org/groups/G0016), Cozy Bear, and The Dukes.(Citation: NSA Joint Advisory SVR SolarWinds April 2021)(Citation: UK NSCS Russia SolarWinds April 2021) Industry reporting also referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, Dark Halo, and SolarStorm.(Citation: FireEye SUNBURST Backdoor December 2020)(Citation: MSTIC NOBELIUM Mar 2021)(Citation: CrowdStrike SUNSPOT Implant January 2021)(Citation: Volexity SolarWinds)(Citation: Cybersecurity Advisory SVR TTP May 2021)(Citation: Unit 42 SolarStorm December 2020)

Attack-Pattern

Name
Subvert Trust Controls
ID
T1553
Description
Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site. Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [Modify Registry](https://attack.mitre.org/techniques/T1112) in support of subverting these controls. (Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)
Name
Boot or Logon Autostart Execution

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

Process Injection

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

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

Inhibit System Recovery

ID

T1490

Description

Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.(Citation: Talos Olympic Destroyer 2018) (Citation: FireEye WannaCry 2017) This may deny access to available backups and recovery options. Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Data Encrypted for Impact] (https://attack.mitre.org/techniques/T1486).(Citation: Talos Olympic Destroyer 2018) (Citation: FireEye WannaCry 2017) Furthermore, adversaries may disable recovery notifications, then corrupt backups.(Citation: disable_notif_synology_ransom) A number of native Windows utilities have been used by adversaries to disable or delete system recovery features: * `vssadmin.exe` can be used to delete all volume shadow copies on a system - `vssadmin.exe delete shadows /all /quiet` * [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) can be used to delete volume shadow copies - `wmic shadowcopy delete` * `wbadmin.exe` can be used to delete the Windows Backup Catalog - `wbadmin.exe delete catalog -quiet` * `bcdedit.exe` can be used to disable automatic Windows recovery features by modifying boot configuration data - `bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no` * `REAgentC.exe` can be used to disable Windows Recovery Environment (WinRE) repair/recovery options of an infected system On network devices, adversaries may leverage [Disk Wipe](https://attack.mitre.org/techniques/T1561) to delete backup firmware images and reformat the file system, then [System Shutdown/Reboot] (https://attack.mitre.org/techniques/T1529) to reload the device. Together this activity may leave network devices completely inoperable and inhibit recovery operations. Adversaries may also delete “online” backups that are connected to their network – whether via network storage media or through folders that sync to cloud services.(Citation: ZDNet Ransomware Backups 2020) In cloud environments, adversaries may disable versioning and backup policies and delete snapshots, machine images, and prior versions of objects designed to be used in disaster recovery scenarios.(Citation: Dark Reading Code Spaces Cyber Attack)(Citation: Rhino Security Labs AWS S3 Ransomware)

Name

Proxy

ID

T1090

Description

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

Name

Exploitation for Privilege Escalation

ID

T1068

Description

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a

virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

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

Drive-by Compromise

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

System Network Connections Discovery

ID

T1049

Description

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network. An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which their virtual networks operate.(Citation: Amazon AWS VPC Guide)(Citation: Microsoft Azure Virtual Network Overview)(Citation: Google VPC Overview) Similarly, adversaries who gain access to network devices may also perform similar discovery activities to gather information about connected systems and services. Utilities and commands that acquire this information include [netstat](https://attack.mitre.org/software/S0104), "net use," and "net session" with [Net](https://attack.mitre.org/software/S0039). In Mac and Linux, [netstat](https://attack.mitre.org/software/S0104) and `lsof` can be used to list current connections. `who -a` and `w` can be used to show which users are currently logged in, similar to "net session". Additionally, built-in features native to network devices and [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) may be used (e.g. `show ip sockets`, `show tcp brief`).(Citation: US-CERT-TA18-106A)

StixFile

Value
a855012a9e198837eae04295de56d28e9258da1e933c56805b39b1f8d0d03c56
5e352c8f55ed9be1142b09e13df7b3efac7ea9e6173b6792d9a5c44dedc3a4ee
ffd5114ffb3a2f66757cecb2fb0079cceaa42a4b42ded566e76b7d58b4effac5
f62e0ec08b15f9a4f3178c77ad540bd7369d1341472fdcbc88aecc0ed29c0387
bcc7c41209afcf67858b3ef80f0afa1eabf2e4faadcaa23bacc9aa5d57b9d836
2d866ccf2b24e3b922abb3d3980c2ed752d86b6c017bc2bf7a1c209aa9464643
c8ca2199aabae9af5c59e658d11a41f76af4576204c23bf5762825171c56e5e8
4240201a9d957a01676ab7165d112d03c7dbdba7b34778407e7b73344b3fd158
17494a7687c8e57be6fcd486bc34aaa120105729196474ccffd078d8aa256f87
6f08ce39072bdacf4a98578ca6b508b68b2c78ed2a378c73a1c87595f9d0c591
664b8fbd825db53ccfc5712f7cd54c71bf53f0791b1bd42af8517729653ae7ae
dda686d6fda52c6ab3c084b7024cfc68dba60ae2143a1095659b795f84cf2329

External References

- https://otx.alienvault.com/pulse/64fa08504be8677a0a799ef1
- https://yoroi.company/research/how-an-apt-technique-turns-to-be-a-public-red-team-project/