Jul 26 2023

NETMANAGEIT

Intelligence Report

Evolution of Russian APT29 – New Attacks and Techniques Uncovered

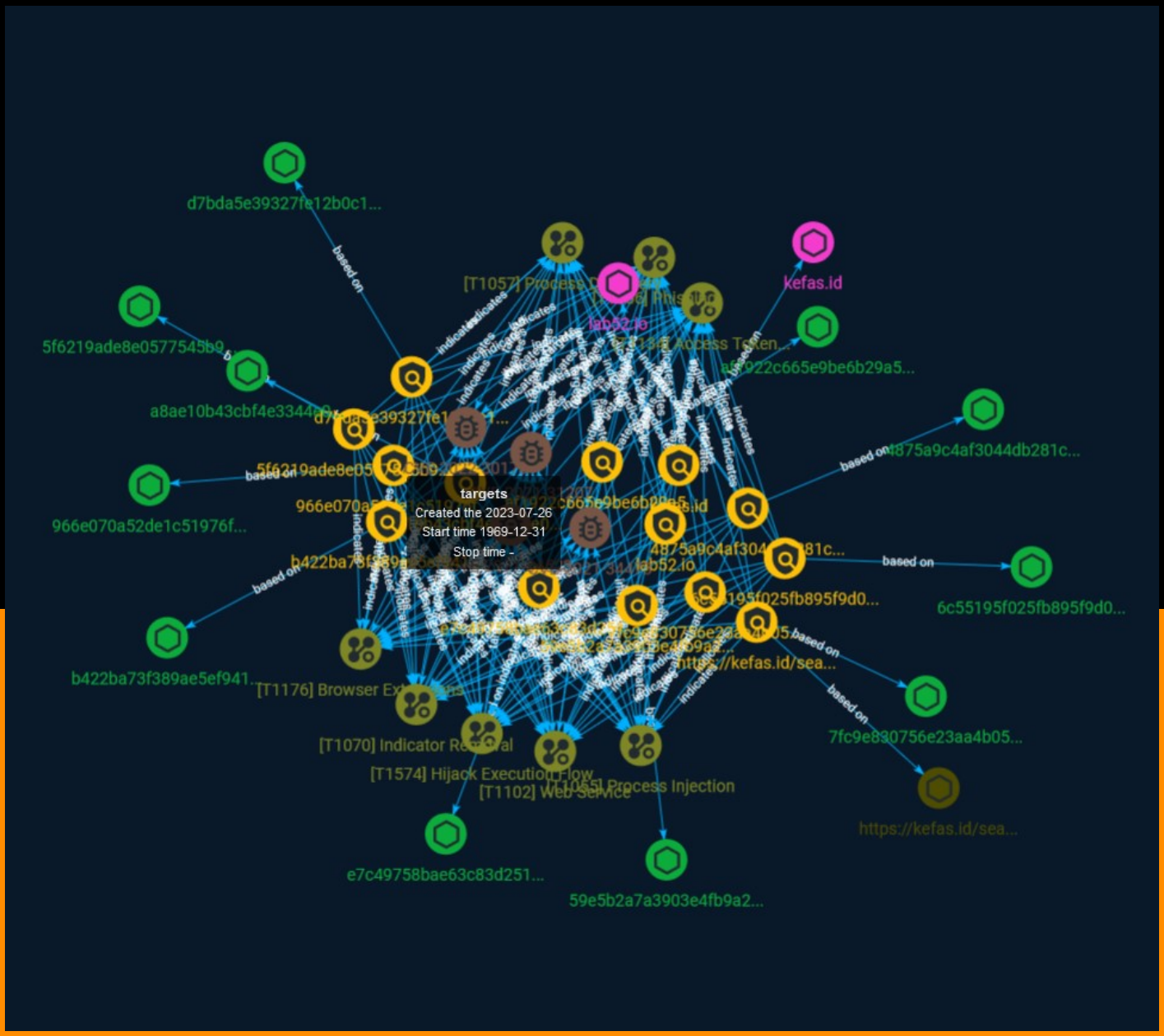

Table of contents

Overview

Entities

Observables

External References

Overview

Description

When it comes to exceptionally sophisticated malware attacks, APT29 stands at the forefront. The SolarWinds breach marked only the beginning of persistent malware attacks carried out by the threat actor. Since the attack on SolarWinds, the APT has relentlessly persisted in its attacks on governments, defense entities, critical manufacturing organizations, and IT service providers. Their latest attacks involve exploiting lesser-known Windows features and specifically targeting diplomats stationed in Ukraine.

Confidence

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

15 / 100

Indicator

Name

966e070a52de1c51976f6ea1fc48ec77f6b89f4bf5e5007650755e9cd0d73281

Description

SHA256 of a61b35a9a9650396223bb82aad02c0ec1f1bb44b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '966e070a52de1c51976f6ea1fc48ec77f6b89f4bf5e5007650755e9cd0d73281']

Name

a8ae10b43cbf4e3344e0184b33a699b19a29866bc1e41201ace1a995e8ca3149

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a8ae10b43cbf4e3344e0184b33a699b19a29866bc1e41201ace1a995e8ca3149']

Name

kefas.id

Pattern Type

stix

Pattern

[domain-name:value = 'kefas.id']

Name

59e5b2a7a3903e4fb9a23174b655adb75eb490625ddb126ef29446e47de4099f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '59e5b2a7a3903e4fb9a23174b655adb75eb490625ddb126ef29446e47de4099f']

Name

b422ba73f389ae5ef9411cf4484c840c7c82f2731c6324db0b24b6f87ce8477d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b422ba73f389ae5ef9411cf4484c840c7c82f2731c6324db0b24b6f87ce8477d']

Name

lab52.io

Pattern Type

stix

Pattern

[domain-name:value = 'lab52.io']

Name

e7c49758bae63c83d251cacbfada7c09af0c3038e8ff755c4c04f916385805d8

Description

XOR_embeded_exefile_xored_with_round_256_bytes_key

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e7c49758bae63c83d251cacbfada7c09af0c3038e8ff755c4c04f916385805d8']

Name

af1922c665e9be6b29a5e3d0d3ac5916ae1fc74ac2fe9931e5273f3c4043f395

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'af1922c665e9be6b29a5e3d0d3ac5916ae1fc74ac2fe9931e5273f3c4043f395']

Name

https://kefas.id/search/s.php

Pattern Type

stix

Pattern

[url:value = 'https://kefas.id/search/s.php']

Name

5f6219ade8e0577545b9f13afd28f6d6e991326f3c427d671d1c1765164b0d57

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5f6219ade8e0577545b9f13afd28f6d6e991326f3c427d671d1c1765164b0d57']

Name

4875a9c4af3044db281c5dc02e5386c77f331e3b92e5ae79ff9961d8cd1f7c4f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4875a9c4af3044db281c5dc02e5386c77f331e3b92e5ae79ff9961d8cd1f7c4f']

Name

7fc9e830756e23aa4b050f4ceaeb2a83cd71cfc0145392a0bc03037af373066b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7fc9e830756e23aa4b050f4ceaeb2a83cd71cfc0145392a0bc03037af373066b']

Name

d7bda5e39327fe12b0c1f42c8e27787f177a352f8eebafbe35d3e790724eceff

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd7bda5e39327fe12b0c1f42c8e27787f177a352f8eebafbe35d3e790724eceff']

Name

6c55195f025fb895f9d0ec3edbf58bc0aa46c43eeb246cfb88eef1ae051171b3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6c55195f025fb895f9d0ec3edbf58bc0aa46c43eeb246cfb88eef1ae051171b3']

Vulnerability

Name
CVE-2022-30170
Name
CVE-2021-34523
Name
CVE-2021-31207
Name
CVE-2021-34473

Country

Name
Norway
Name
Poland
Name
Ukraine

Attack-Pattern

Name
Browser Extensions
ID
T1176
Description
Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition) Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions. Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `.mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install configuration profiles, however `.mobileconfig` files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS) Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence. (Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension) There

have also been instances of botnets using a persistent backdoor through malicious Chrome extensions.(Citation: Stantinko Botnet) There have also been similar examples of extensions being used for command & control.(Citation: Chrome Extension C2 Malware)

Name

Access Token Manipulation

ID

T1134

Description

Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token. An adversary can use built-in Windows API functions to copy access tokens from existing processes; this is known as token stealing. These token can then be applied to an existing process (i.e. [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001)) or used to spawn a new process (i.e. [Create Process with Token](https://attack.mitre.org/techniques/T1134/002)). An adversary must already be in a privileged user context (i.e. administrator) to steal a token. However, adversaries commonly use token stealing to elevate their security context from the administrator level to the SYSTEM level. An adversary can then use a token to authenticate to a remote system as the account for that token if the account has appropriate permissions on the remote system.(Citation: Pentestlab Token Manipulation) Any standard user can use the `runas` command, and the Windows API functions, to create impersonation tokens; it does not require access to an administrator account. There are also other mechanisms, such as Active Directory fields, that can be used to modify access tokens.

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

Process Discovery

ID

T1057

Description

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. In Windows environments, adversaries could obtain details on running processes using the [Tasklist](https://attack.mitre.org/software/S0057) utility via [cmd](https://attack.mitre.org/software/S0106) or `Get-Process` via [PowerShell](https://attack.mitre.org/techniques/T1059/001). Information about processes can also be extracted from the output of [Native API](https://attack.mitre.org/techniques/T1106) calls such as `CreateToolhelp32Snapshot`. In Mac and Linux, this is accomplished with the `ps` command. Adversaries may also opt to enumerate processes via /proc. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/

T1059/008) commands such as `show processes` can be used to display current running processes.(Citation: US-CERT-TA18-106A)(Citation: show_processes_cisco_cmd)

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

Indicator Removal

ID

T1070

Description

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary’s actions. Typically these artifacts are

used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

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
Web Service
ID
T1102
Description
Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

Domain-Name

Value
lab52.io
kefas.id

StixFile

Value
b422ba73f389ae5ef9411cf4484c840c7c82f2731c6324db0b24b6f87ce8477d
d7bda5e39327fe12b0c1f42c8e27787f177a352f8eebafbe35d3e790724eceff
af1922c665e9be6b29a5e3d0d3ac5916ae1fc74ac2fe9931e5273f3c4043f395
966e070a52de1c51976f6ea1fc48ec77f6b89f4bf5e5007650755e9cd0d73281
7fc9e830756e23aa4b050f4ceaeb2a83cd71cfc0145392a0bc03037af373066b
59e5b2a7a3903e4fb9a23174b655adb75eb490625ddb126ef29446e47de4099f
a8ae10b43cbf4e3344e0184b33a699b19a29866bc1e41201ace1a995e8ca3149
4875a9c4af3044db281c5dc02e5386c77f331e3b92e5ae79ff9961d8cd1f7c4f
e7c49758bae63c83d251cacbfada7c09af0c3038e8ff755c4c04f916385805d8
5f6219ade8e0577545b9f13afd28f6d6e991326f3c427d671d1c1765164b0d57
6c55195f025fb895f9d0ec3edbf58bc0aa46c43eeb246cfb88eef1ae051171b3

Url

Value
https://kefas.id/search/s.php

External References

- https://otx.alienvault.com/pulse/64c131d13447ec7826c8ac6f
- https://www.avertium.com/resources/threat-reports/evolution-of-russian-apt29-new-attacks-and-techniques-uncovered