Jun 28 2024

NETMANAGEIT

Intelligence Report

Kimsuky Deploys TRANSLATEXT Chrome Extension

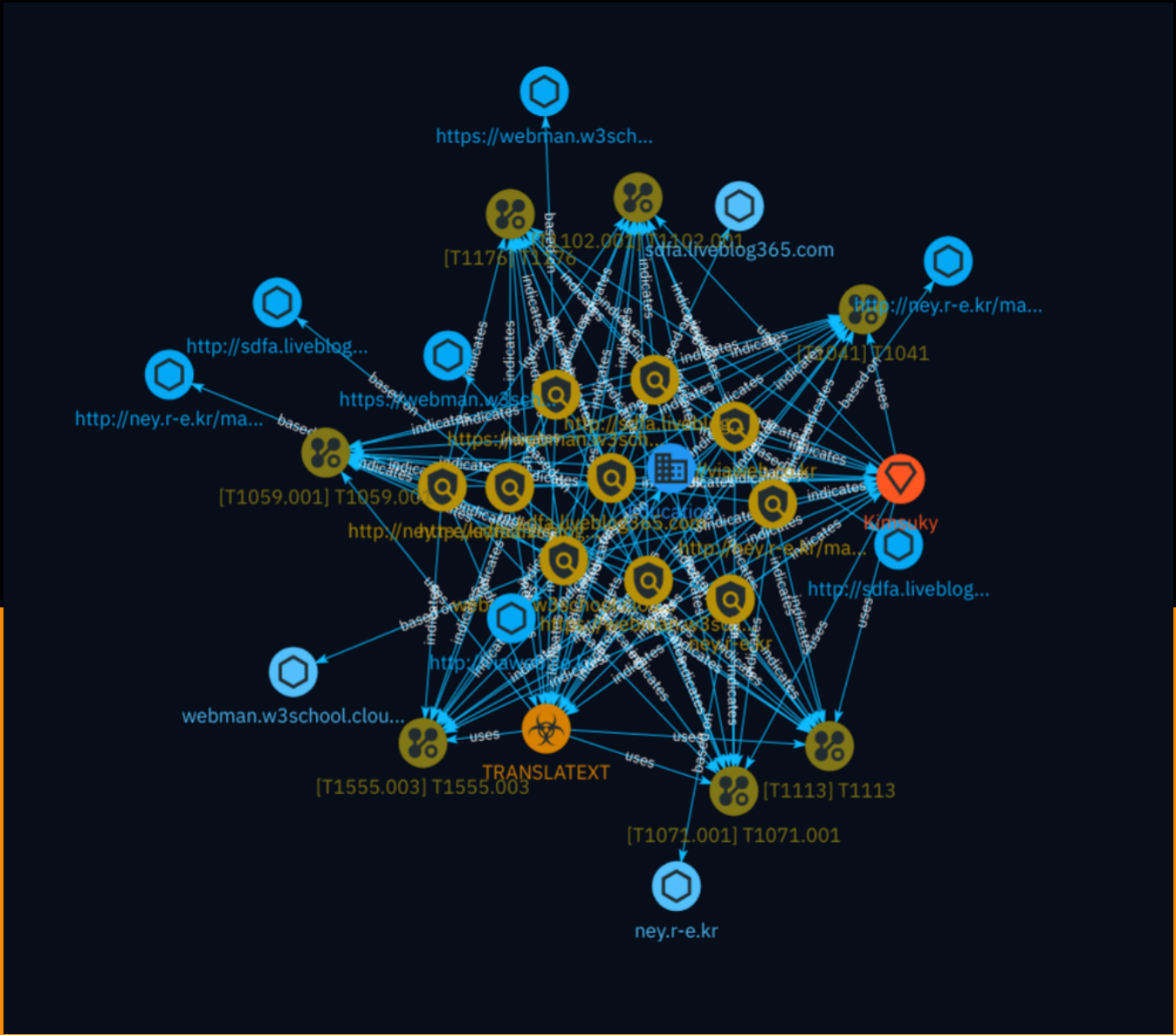

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In March 2024, the cybersecurity firm Zscaler observed a new activity from Kimsuky, a North Korean state-sponsored hacker group. They employed a malicious Google Chrome extension named 'TRANSLATEXT' specifically crafted to steal email addresses, usernames, passwords, cookies, and capture browser screenshots. The primary targets appear to be academic researchers in South Korea specializing in geopolitical issues related to the Korean peninsula. The extension bypassed security measures of prominent email providers and exfiltrated stolen data via a GitHub repository controlled by the threat actors.

Confidence

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

100 / 100

Content

N/A

Attack-Pattern

Name
T1102.001
ID
T1102.001
Description
Adversaries may use an existing, legitimate external Web service to host information that points to additional command and control (C2) infrastructure. Adversaries may post content, known as a dead drop resolver, on Web services with embedded (and often obfuscated/encoded) domains or IP addresses. Once infected, victims will reach out to and be redirected by these resolvers. 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 a dead drop resolver 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).
Name
T1555.003
ID

T1555.003

Description

Adversaries may acquire credentials from web browsers by reading files specific to the target browser.(Citation: Talos Olympic Destroyer 2018) Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future. Web browsers typically store the credentials in an encrypted format within a credential store; however, methods exist to extract plaintext credentials from web browsers. For example, on Windows systems, encrypted credentials may be obtained from Google Chrome by reading a database file, `AppData\Local\Google\Chrome\User Data\Default\Login Data` and executing a SQL query: `SELECT action_url, username_value, password_value FROM logins;`. The plaintext password can then be obtained by passing the encrypted credentials to the Windows API function `CryptUnprotectData`, which uses the victim's cached logon credentials as the decryption key.(Citation: Microsoft CryptUnprotectData April 2018) Adversaries have executed similar procedures for common web browsers such as FireFox, Safari, Edge, etc. (Citation: Proofpoint Vega Credential Stealer May 2018)(Citation: FireEye HawkEye Malware July 2017) Windows stores Internet Explorer and Microsoft Edge credentials in Credential Lockers managed by the [Windows Credential Manager](https://attack.mitre.org/techniques/T1555/004). Adversaries may also acquire credentials by searching web browser process memory for patterns that commonly match credentials.(Citation: GitHub Mimikittenz July 2016) After acquiring credentials from web browsers, adversaries may attempt to recycle the credentials across different systems and/or accounts in order to expand access. This can result in significantly furthering an adversary's objective in cases where credentials gained from web browsers overlap with privileged accounts (e.g. domain administrator).

Name

T1071.001

ID

T1071.001

Description

Adversaries may communicate using application layer protocols associated with web traffic 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. Protocols such as HTTP/S(Citation: CrowdStrike Putter Panda) and WebSocket(Citation: Brazking-Websockets) that carry web traffic may be very common in environments. HTTP/S packets have many fields and headers in which data can be concealed. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.

Name

T1059.001

ID

T1059.001

Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack) PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

Name

T1176

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 for [Command and Control](https://attack.mitre.org/tactics/TA0011). (Citation: Stantinko Botnet)(Citation: Chrome Extension C2 Malware) Adversaries may also use browser extensions to modify browser permissions and components, privacy settings, and other security controls for [Defense Evasion](https://attack.mitre.org/tactics/TA0005). (Citation: Browers FriarFox)(Citation: Browser Adrozek)

Name

T1113

ID

T1113

Description

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as `CopyFromScreen`, `xwd`, or `screencapture`.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

Name

T1041

ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Sector

Name
Education

Indicator

Name
https://webman.w3school.cloudns.nz/config.php
Pattern Type
stix
Pattern
[url:value = 'https://webman.w3school.cloudns.nz/config.php']
Name
webman.w3school.cloudns.nz
Pattern Type
stix
Pattern
[hostname:value = 'webman.w3school.cloudns.nz']
Name
http://sdfa.liveblog365.com/ares/babyhades.txt

Pattern Type

stix

Pattern

[url:value = 'http://sdfa.liveblog365.com/ares/babyhades.txt']

Name

http://ney.r-e.kr/mar/tys.php

Pattern Type

stix

Pattern

[url:value = 'http://ney.r-e.kr/mar/tys.php']

Name

ney.r-e.kr

Pattern Type

stix

Pattern

[hostname:value = 'ney.r-e.kr']

Name

http://viaweb.co.kr

Pattern Type

stix

Pattern

[url:value = 'http://viaweb.co.kr']

Name

sdfa.liveblog365.com

Pattern Type

stix

Pattern

[hostname:value = 'sdfa.liveblog365.com']

Name

http://sdfa.liveblog365.com/ares/hades.txt

Pattern Type

stix

Pattern

[url:value = 'http://sdfa.liveblog365.com/ares/hades.txt']

Name

http://ney.r-e.kr/mar/tys.txt

Pattern Type
stix
Pattern
[url:value = 'http://ney.r-e.kr/mar/tys.txt']
Name
https://webman.w3school.cloudns.nz
Pattern Type
stix
Pattern
[url:value = 'https://webman.w3school.cloudns.nz']

Intrusion-Set

Name

Kimsuky

Description

[Kimsuky](https://attack.mitre.org/groups/G0094) is a North Korea-based cyber espionage group that has been active since at least 2012. The group initially focused on targeting South Korean government entities, think tanks, and individuals identified as experts in various fields, and expanded its operations to include the United States, Russia, Europe, and the UN. [Kimsuky](https://attack.mitre.org/groups/G0094) has focused its intelligence collection activities on foreign policy and national security issues related to the Korean peninsula, nuclear policy, and sanctions.(Citation: EST Kimsuky April 2019)(Citation: BRI Kimsuky April 2019)(Citation: Cybereason Kimsuky November 2020)(Citation: Malwarebytes Kimsuky June 2021)(Citation: CISA AA20-301A Kimsuky) [Kimsuky](https://attack.mitre.org/groups/G0094) was assessed to be responsible for the 2014 Korea Hydro & Nuclear Power Co. compromise; other notable campaigns include Operation STOLEN PENCIL (2018), Operation Kabar Cobra (2019), and Operation Smoke Screen (2019).(Citation: Netscout Stolen Pencil Dec 2018)(Citation: EST Kimsuky SmokeScreen April 2019)(Citation: AhnLab Kimsuky Kabar Cobra Feb 2019) North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups.

Malware

Name
TRANSLATEXT

indicates

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name
Name

uses

Name
Description
[Kimsuky](https://attack.mitre.org/groups/G0094) has used browser extensions including Google Chrome to steal passwords and cookies from browsers. [Kimsuky](https://attack.mitre.org/groups/G0094) has also used Nirsoft's WebBrowserPassView tool to dump the passwords obtained from victims.(Citation: Zdnet Kimsuky Dec 2018)(Citation: CISA AA20-301A Kimsuky)(Citation: Netscout Stolen Pencil Dec 2018)(Citation: Talos Kimsuky Nov 2021)
Name
Name
Name
Name
Description

[Kimsuky](https://attack.mitre.org/groups/G0094) has executed a variety of PowerShell scripts.(Citation: EST Kimsuky April 2019)(Citation: CISA AA20-301A Kimsuky)(Citation: Talos Kimsuky Nov 2021)(Citation: KISA Operation Muzabi)

Name

Name

Name

Description
[Kimsuky](https://attack.mitre.org/groups/G0094) has used HTTP GET and POST requests for C2.(Citation: Talos Kimsuky Nov 2021)

Name

based-on

Name
Name
Name
Name
Name
Name
Name
Name

targets

Name

Hostname

Value
ney.r-e.kr
sdfa.liveblog365.com
webman.w3school.cloudns.nz

External References

- https://www.zscaler.com/blogs/security-research/kimsuky-deploys-translatext-target-south-korean-academia
- https://otx.alienvault.com/pulse/667e6a3f7625d7dc706f0d31