Jul 12 2023

NETMANAGEIT

Intelligence Report

Attackers Exploit Unpatched Windows Zero-Day Vulnerability

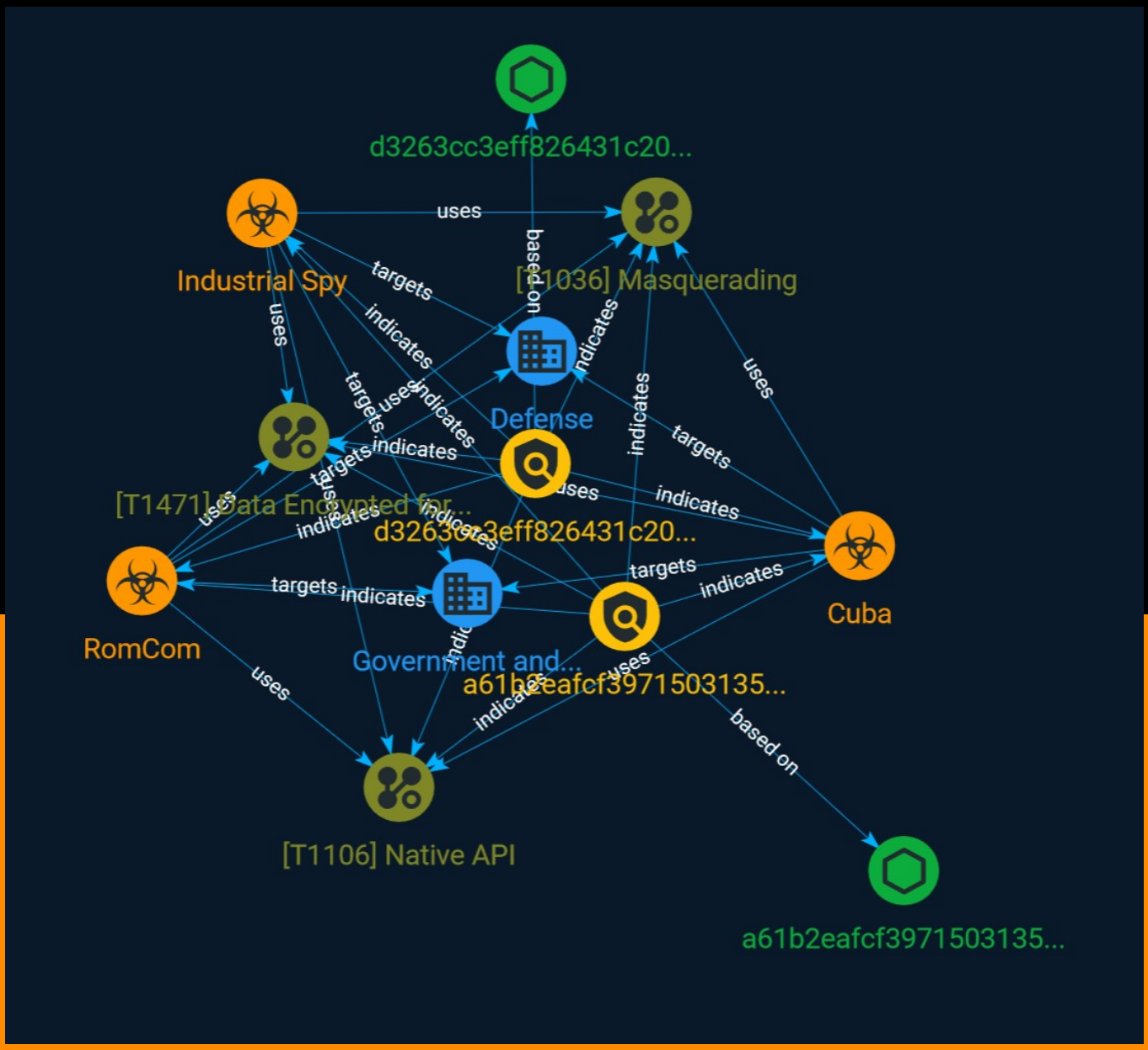

Table of contents

Overview

- Description 4
- Confidence 4

Entities

- Indicator 5
- Malware 7
- Sector 8
- Attack-Pattern 9

Observables

- StixFile 11

External References

- External References 12

Overview

Description

Security firm Symantec has issued an advisory about a zero-day vulnerability in Microsoft Windows that has been used in targeted attacks on government and government targets.. and the cyber-crime group Storm-0978

Confidence

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

15 / 100

Indicator

Name

a61b2eafcf39715031357df6b01e85e0d1ea2e8ee1dfec241b114e18f7a1163f

Description

Rtf.Exploit.CVE_2017_0199-6335035-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a61b2eafcf39715031357df6b01e85e0d1ea2e8ee1dfec241b114e18f7a1163f']

Name

d3263cc3eff826431c2016aee674c7e3e5329bebfb7a145907de39a279859f4a

Pattern Type

stix

Pattern

```
[file:hashes.'SHA-256' =
'd3263cc3eff826431c2016aee674c7e3e5329bebfb7a145907de39a279859f4a']
```

Malware

Name
Industrial Spy
Name
Cuba
Description
[Cuba](https://attack.mitre.org/software/S0625) is a Windows-based ransomware family that has been used against financial institutions, technology, and logistics organizations in North and South America as well as Europe since at least December 2019.(Citation: McAfee Cuba April 2021)
Name
RomCom

Sector

Name
Defense
Description
Public and private entities involved in the conception and production of weapons and the planning and conducting of military operations.
Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Attack-Pattern

Name
Data Encrypted for Impact
ID
T1471
Description
An adversary may encrypt files stored on a mobile device to prevent the user from accessing them. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.
Name
Masquerading
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)

Name

Native API

ID

T1106

Description

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes. (Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations. Native API functions (such as `NtCreateProcess`) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API `CreateProcess()` or GNU `fork()` will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations. (Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC) Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation) Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system. While invoking API functions, adversaries may also attempt to bypass defensive tools (ex: unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001)).

StixFile

Value
d3263cc3eff826431c2016aee674c7e3e5329bebfb7a145907de39a279859f4a
a61b2eafcf39715031357df6b01e85e0d1ea2e8ee1dfec241b114e18f7a1163f

External References

- https://otx.alienvault.com/pulse/64aed329ac23f695c7e2115e
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/microsoft-zeroday-exploit