مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

DarkGate Malware Campaign

Tracking #:432315802

Date:30-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council observed McAfee Labs has uncovered a novel infection chain associated with the DarkGate Remote Access Trojan (RAT).

TECHNICAL DETAILS:

McAfee Labs recently discovered a new infection chain linked to the DarkGate malware, a Remote Access Trojan (RAT) marketed as Malware-as-a-Service (MaaS) on cybercrime forums since at least 2018. DarkGate exhibits sophisticated functionalities including process injection, file download and execution, data theft, shell command execution, and keylogging capabilities. It notably bypasses Microsoft Defender SmartScreen and incorporates evasion tactics to avoid detection. The infection chain begins with an HTML-based entry point or an XLS file, each leading to the execution of malicious scripts, eventually culminating in the deployment of the DarkGate payload.

The malware exploits vulnerabilities such as CVE-2023-36025 and CVE-2024-21412, allowing the execution of malicious commands on unpatched Windows systems. Furthermore, DarkGate maintains persistence by dropping a .lnk file in the startup folder and exfiltrates data to a Command and Control (C2) server located at IP address 5.252.177.207.

The HTML-based infection chain tricks users into interacting with malicious content by masquerading as a cloud view of a Word document, ultimately leading to the execution of a VBScript file to download and execute the DarkGate payload. On the other hand, the XLS-based infection chain prompts users to open the file, leading to the execution of a VBS file and subsequent download and execution of the DarkGate payload, highlighting the malware's multi-vector approach.

The DarkGate payload, a Delphi-compiled executable, maintains persistence by dropping a .lnk file in the startup folder and communicates with a C2 server for exfiltration. It leverages AutoHotkey scripts to automate tasks on the infected system, demonstrating its sophisticated and multifaceted nature.

Indicators of Compromise:

File	Hash
Html file	196bb36f7d63c845afd40c5c17ce061e320d110f28ebe8c7c998b9e6b3fe1005
URL file	2b296ffc6d173594bae63d37e2831ba21a59ce385b87503710dc9ca439ed7833
VBS	038db3b838d0cd437fa530c001c9913a1320d1d7ac0fd3b35d974a806735c907
autohotkey.exe	897b0d0e64cf87ac7086241c86f757f3c94d6826f949a1f0fec9c40892c0cecb
AHK script	dd7a8b55e4b7dc032ea6d6aed6153bec9b5b68b45369e877bb66ba21acc81455
test.txt	4de0e0e7f23adc3dd97d498540bd8283004aa131a59ae319019ade9ddef41795
DarkGate exe	6ed1b68de55791a6534ea96e721ff6a5662f2aefff471929d23638f854a80031
IP	5[.]252.177.207
XLS file	1a960526c132a5293e1e02b49f43df1383bf37a0bbadd7ba7c106375c418dad4
VBS	2e34908f60502ead6ad08af1554c305b88741d09e36b2c24d85fd9bac4a11d2f
LNK file	10e362e18c355b9f8db9a0dbbc75cf04649606ef96743c759f03508b514ad34e
IP	103[.]124.106.237

RECOMMENDATIONS:

- Block the IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Keep Windows and security software's up to date to mitigate vulnerabilities and exploits.
- Verify sender information and be cautious with email content to avoid falling victim to phishing schemes.
- Use email spam filters to reduce the risk of receiving suspicious emails.
- Delete suspicious emails and avoid interacting with their contents.
- Check for secure HTTP connections to ensure the safety of web browsing activities.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/the-darkgate-menace-leveraging-autohotkey-attempt-to-evade-smartscreen/