2024-05-30

HUNTER

EMERGING THREATS

DARKGATE MALWARE

DarkGate malware variant was first observed in the wild in 2018 (seemingly in production since 2017), evolving into a more dangerous and widespread version of itself in recent years - more notably after the takedown of the Qbot infrastructure, there has been a surge in cases involving the variant. **DarkGate** is a malicious toolkit that operates under the Malware-as-a-Service model (meaning it is sold or rented to threat actors), and understood to have the functionality of both a loader and a RAT (Remote Access Trojan).

THREAT SUMMARY

DarkGate malware variant was first observed in the wild in 2018 (seemingly in production since 2017), evolving into a more dangerous and widespread version of itself in recent years - more notably after the takedown of the Qbot infrastructure, there has been a surge in cases involving the variant. **DarkGate** is a malicious toolkit that operates under the Malware-as-a-Service model (meaning it is sold or rented to threat actors), and understood to have the functionality of both a loader and a RAT (Remote Access Trojan).
In recent events, **DarkGate** was involved in a campaign during January of 2024, exploiting a vulnerability in Microsoft Windows SmartScreen bypass (CVE-2024-21412) in order to deliver and proliferate the malware on vulnerable machines. These attacks employed the masquerading of legitimate software installers in order to infect users with the payload.

With the variant continuously evolving, recent attacks and the observed proliferation of the use of **DarkGate** in the wild, it is important to assess, understand and prepare for this malicious toolkit in our environments.

Intel 471 References:

[TITAN Malware Campaign Report]
(https://titan.intel471.com/malware/5e3f56b5f6a0042895cf200b1bebc397)Â

[TITAN Info Report: Actor Bordislav offers to lease DarkGate multifunctional loader malware]
(https://titan.intel471.com/report/inforep/8f30102b5633f1e7c520e2bb44366a6e)

SYNOPSIS

DarkGate is a malicious toolkit, that allows operators (in its newest versioning) to fully compromise a victimâ€™s system - allowing the ability to conduct malicious acts such as remote code execution, defense evasion, information stealing/data exfiltration and further malware deployment. Utilizing [Intel 471] (https://intel471.com/)'s reliable and timely threat intelligence, it has been observed to be delivered via phishing emails/malicious attachments, vulnerability exploitations, and malvertising/SEO (search engine optimization) poisoning campaigns - with researchers seeing the delivery taking place with file types such as malicious Windows Installer packages (.msi), VBscript or PDF files (PDF instances were observed to exploit CVE-2024-21412 containing a redirect to a malicious .URL internet shortcut file). It is worthy to note that most recently, Proofpoint researchers observed delivery being associated with a malicious HTML file.

After initial access is gained, **DarkGate** will abuse LOLBINS (Living Off the Land Binaries) in order to pull the next stage payload, which then utilizes DLL side loading in order to drop AutoIT3.exe and AutoIT scripts associated. It is worthy to note that the infection chain can vary depending on the initial payload file type, however the part of the chain that includes AutoIT is common throughout. At this juncture, it will invoke the Autoit3 binary to execute the malicious scripts that deploy the loader and ultimately leads to the main **DarkGate** payload execution.

HUNT PACKAGES

DIRECT TO IP ADDRESS IN EXECUTION OF WEBDAV DLL VIA RUNDLL32 – MALICIOUS LINK OR EXPLOITATION
https://hunter.cyborgsecurity.io/research/hunt-package/d020807d-8833-460f-ac88-b004b74ecea4

WMIC WINDOWS INTERNAL DISCOVERY AND ENUMERATION
https://hunter.cyborgsecurity.io/research/hunt-package/bc0fd59c-4217-46a7-a167-764727118567

HTTP REQUEST AND SHELL EXECUTION COMMANDS – POTENTIAL DOWNLOAD AND EXECUTE COMMAND
https://hunter.cyborgsecurity.io/research/hunt-package/ffe470ec-87b2-49c9-a2b4-a776050e2537

COMMON SUSPICIOUS POWERSHELL EXECUTION ARGUMENT TECHNIQUES
https://hunter.cyborgsecurity.io/research/hunt-package/9762067d-ac45-450e-b1f0-bea9d2e219d7

POWERSHELL DOWNLOAD AND EXECUTE DROPPER BEHAVIOR – SEPARATE COMMAND CALLS
https://hunter.cyborgsecurity.io/research/hunt-package/a669df93-4b21-45d9-bbb6-e9c987587cef

WINDOWS CMD.EXE LAUNCHING SCRIPT INTERPRETER
https://hunter.cyborgsecurity.io/research/hunt-package/a5c2a987-f7cd-479f-a77e-f992f1be2ea6

POTENTIALLY ABNORMAL PARENT PROCESS FOR CMD.EXE OR REGEDIT.EXE
https://hunter.cyborgsecurity.io/research/hunt-package/332e1055-ae60-4e27-853b-b0b9ee02dcc0

ABNORMAL EXECUTION OF WEBDAV DLL VIA RUNDLL32 – POTENTIALLY MALICIOUS LINK OR EXPLOITATION
https://hunter.cyborgsecurity.io/research/hunt-package/062ae7c6-3e3d-401c-8797-1df3218f3e47

RELATED LINKS
Sign up for free HUNTER access
DarkGate Malware Emerging Threat Collection

MITRE CONTEXT

- Tactic Names:
  - Defense Evasion
  - Initial Access
  - Discovery
  - Command and Control
  - Lateral Movement
  - Execution
  - Credential Access
- Technique Names:
  - Windows Command Shell
  - System Network Configuration Discovery
  - Visual Basic
  - Non-Standard Port
  - Malicious Link
  - Command and Scripting Interpreter
  - Ingress Tool Transfer
  - PowerShell
  - Web Protocols
  - Rundll32
  - Remote Services
  - Phishing
  - Malicious File
  - Exploitation for Credential Access
  - Windows Management Instrumentation
- Threat Names:
  - DarkGate

REFERENCES

1. https://titan.intel471.com/malware/5e3f56b5f6a0042895cf200b1bebc397
2. https://titan.intel471.com/report/inforep/8f30102b5633f1e7c520e2bb44366a6e
3. https://www.trendmicro.com/en_us/research/24/c/cve-2024-21412--darkgate-operators-exploit-microsoft-windows-sma.html
4. https://www.logpoint.com/en/blog/inside-darkgate/