Quorum Cyber

Threat Intelligence DarkGate Malware

TLP Status: CLEAR

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft Solutions Partner

Table of Contents

Document Control 3

Revision History 3

Related Documents 3

DarkGate Malware 4

Overview 4

Impact 4

Incident Detection 4

Targeted Products 4

Containment, Mitigations & Remediations 5

Indicators of Compromise 5

Threat Actor 6

Threat Landscape 6

Mitre Methodologies 6

Further Information 6

Document Control

Revision History

Version	Date	Summary of Changes
0.1	14/09/2023	Initial Report Drafted
1.0	15/09/2023	PDF Formatting

Related Documents

The following documents are either referenced within, or are related to, the content of this document:

Document Name	Date	Version
	dd/mm/yyyy	

DarkGate Malware

Overview

DarkGate is a malware family that has been active since 2017 but has recently been associated with a significant surge in operations and targeting. DarkGate is a multi-purpose malware toolkit that includes features for evading detection, escalating privileges, remote code execution, keylogging, and data theft from web browsers and Discord. The malware applies various techniques such as obfuscating malicious code in AutoIT scripts and the utilisation of shellcode to decrypt and launch the final payload.

Throughout recent months, the rate of DarkGate malware deployment has increased via several cyber-attack vectors, including phishing and malvertising. Intelligence has revealed that phishing campaigns linked to the deployment of DarkGate malware contains a malicious VBScript that triggers the infection chain leading to the installation of the loader.

The malware was initially advertised for rent by a threat actor named 'RastaFarEye', with cryptocurrency being the only accepted form of payment. As of the time of writing, the price for renting DarkGate ranges from US$1,000 for one day to US$100,000 per year.

A new Microsoft Teams phishing campaign was recently detected that was associated with the delivery of malicious attachments, resulting in the installation of the DarkGate Loader malware. As with previous campaigns, the attack chain involved the phishing messages being sent by compromised external Office 365 accounts to target organisations [1]. It has been assessed to be highly likely that the recent spike in DarkGate operations is to be attributed to the developer renting the malware to a limited number of affiliates.

Impact

DarkGate is a potent malware that supports a wide range of malicious operations, including cryptocurrency mining, reverse shell establishment, keylogging, clipboard and system information stealing. As such, installation of the malware on target systems will almost certainly result in the compromise of the integrity of data

Incident Detection

Recent campaigns have shown that DarkGate is continually developing via the addition of new components and obfuscation techniques to conceal its infection chain. However, a comprehensive endpoint detection and response (EDR) solution, such as Microsoft Defender, can provide additional protection against malware threats like that implemented by DarkGate. EDR solutions can alert system users of potential breaches and prevent further progress prior to the malware implementing significant damage.

Targeted Products

Windows OS.

[1] Phishing campaign via Microsoft Teams targeting public sector (quorumcyber.com)

Containment, Mitigations & Remediations

As mentioned previously, a primary method of reducing the threat of DarkGate malware is to detect it in the early stages via the implementation of an effective and monitored EDR solution. An effective EDR tool, such as the Microsoft Defender suite, will block any associated malware attempts upon detection.

With regards to the Microsoft Teams phishing campaigns involving the deployment of DarkGate malware the only way to prevent this attack vector is to only allow Microsoft Teams chat requests from specific external domains.

Indicators of Compromise

DarkGate Malware Associated Domain:

- uc11fe6137f8efa3654a6ebed384[.]dl[.]dropboxusercontent[.]com
- a-1bcdn[.]com
- avayacloud[.]com[.]global[.]prod[.]fastly[.]net
- drkgatevservicceoffice[.]net
- intranet[.]mcasavaya[.]com
- onlysportsfitnessam[.]com
- reactervnamnat[.]com
- sanibroadbandcommunicton[.]duckdns[.]org
- xfirecovery[.]pro

DarkGate Malware Associated File Hash (SHA-256):

- 711b9ebcf9aca14620ede45cff8bdf14f7a7e6943c9917fb9cfc91f3c272c7c2

DarkGate Malware Associated URL:

- hxxps[://]uc11fe6137f8efa3654a6ebed384[.]dl[.]dropboxusercontent[.]com/cd/0/get/CDt45nEqDc48WirxbT-40wtB--dO1NHaFqNOgN1lwYIGg7_MJ6ew50FzJnetseIa5LSJpr0LI0ZjjACGzO4SSeK4-03Mwut0gqeelg_5WVh18aUNmINSsryrc5UHQas7osmvaPnvMy7zZ09GyK5aXj3c/file?dl=1#

DarkGate Malware Associated IP Addresses:

- 149[.]248[.]0[.]82
- 179[.]60[.]149[.]3
- 185[.]143[.]223[.]64
- 185[.]8[.]106[.]231
- 45[.]89[.]65[.]198
- 5[.]34[.]178[.]21

- 80[.]66[.]88[.]145
- 89[.]248[.]193[.]66

Threat Actor

DarkGate was initially advertised for rent by a threat actor named RastaFarEye, with cryptocurrency being the only accepted form of payment. RastaFarEye is an active member of the top-tier underground forum, Exploit, and has previously been involved in numerous malicious operations, primarily involving the targeting of macOS and Windows systems. The threat actor has also been detected to have sold exploits, malware loaders, trojans, fraudulent certificates, and source codes for malware programmes, in addition to offering a range of services and tools that enable threat actors to bypass security measures and deploy malware.

Threat Landscape

Throughout recent months, the rate of DarkGate malware deployment has increased via several cyber-attack vectors, including phishing and malvertising. Although at the time of writing, DarkGate has yet to emerge as a widespread threat, the expanded targeting trends as well as the recruitment of numerous infection vectors has resulted in an assessment that it is likely that the prevalence of this threat will continue to surge in the coming months.

Mitre Methodologies

Initial Access
T1566 - Phishing[2]

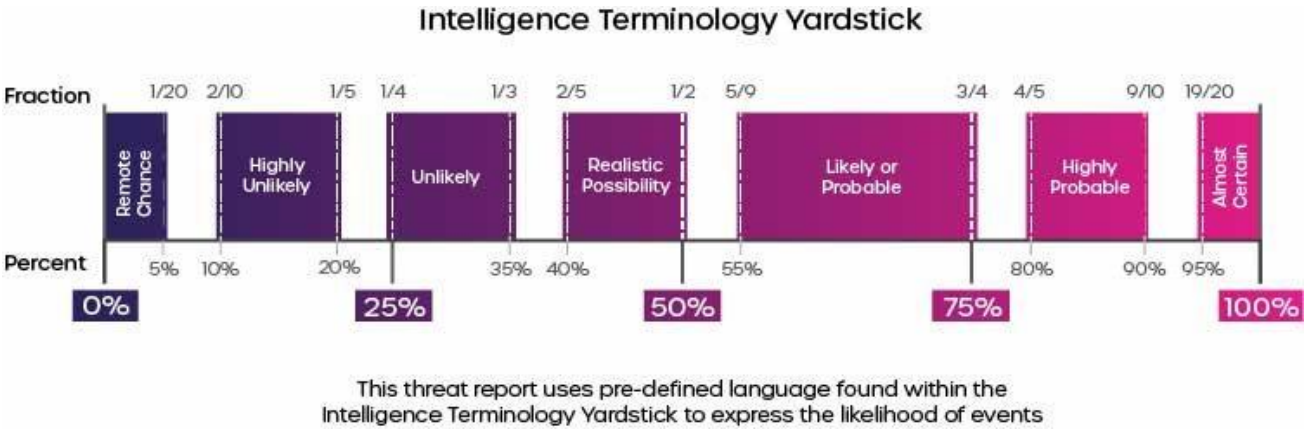
Execution
T1204.001 - User Execution: Malicious Link[3]
T1204.002 - User Execution: Malicious File[4]

Further Information

- Quorum Cyber Threat Intelligence Security Blog - Microsoft Phishing with DarkGate Malware
- Truesec Analysis - DarkGate Microsoft Teams Campaign
- Telekom DarkGate Malware Analysis

Intelligence Cut-off Date (ICoD): 14/09/2023 10:00 UTC

[2] Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®
[3] User Execution: Malicious Link, Sub-technique T1204.001 - Enterprise | MITRE ATT&CK®
[4] User Execution: Malicious File, Sub-technique T1204.002 - Enterprise | MITRE ATT&CK®



This threat report uses pre-defined language found within the Intelligence Terminology Yardstick to express the likelihood of events