Sep 11 2023

NETMANAGEIT

Intelligence Report

DarkGate Loader Malware Delivered via Microsoft Teams

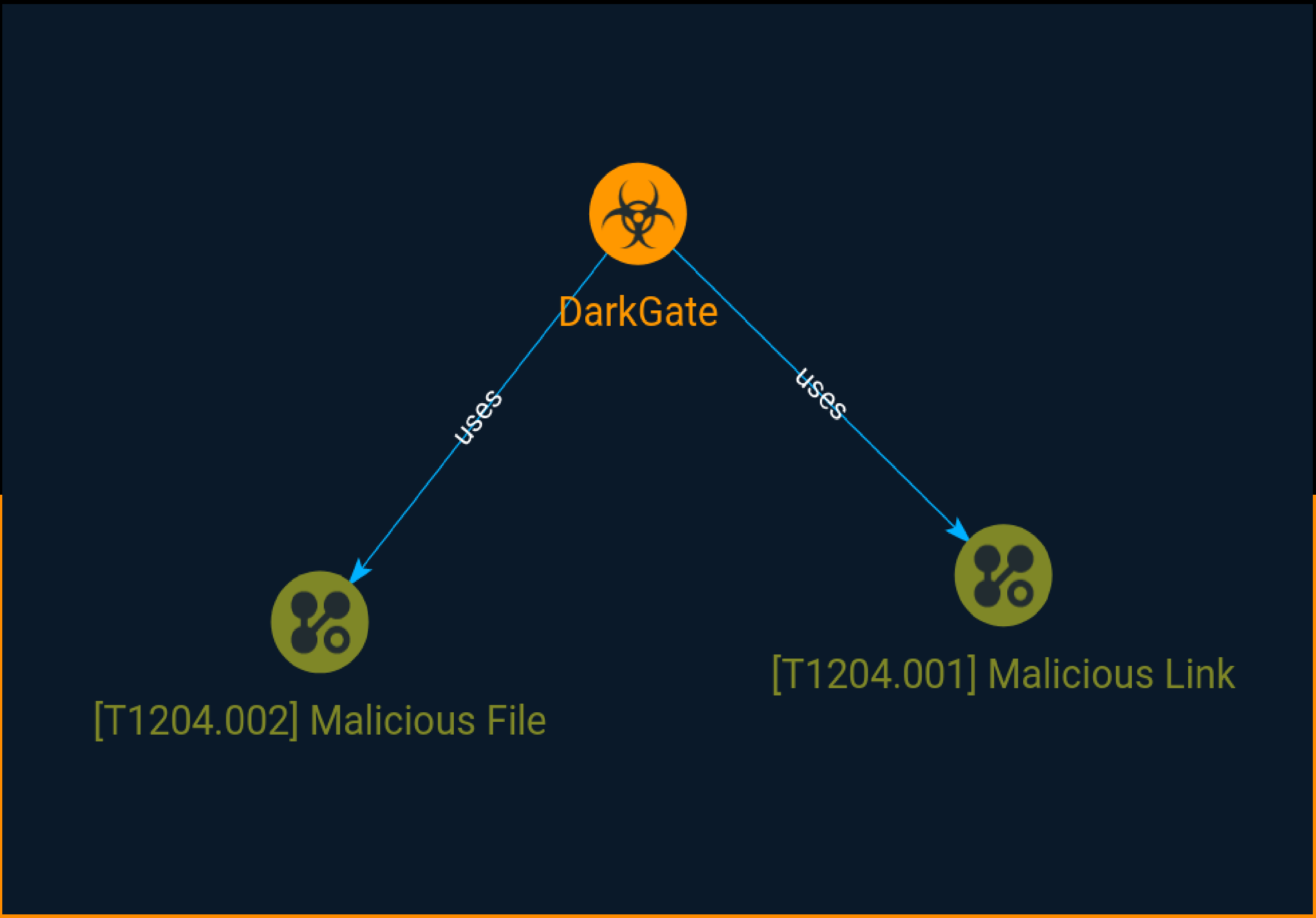

Table of contents

Overview

Entities

External References

Overview

Description

Malspam campaigns involving DarkGate Loader have been on the rise since its author started advertising it as a Malware-as-a-Service offering on popular cybercrime forums in June 2023. Until now DarkGate Loader was seen delivered via traditional email malspam campaigns similar to those of Emotet. In August an operator started using Microsoft Teams to deliver the malware via HR-themed social engineering chat messages.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Malware

Name
DarkGate

Attack-Pattern

Name
Malicious Link
ID
T1204.001
Description
An adversary may rely upon a user clicking a malicious link in order to gain execution. Users may be subjected to social engineering to get them to click on a link that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Clicking on a link may also lead to other execution techniques such as exploitation of a browser or application vulnerability via [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203). Links may also lead users to download files that require execution via [Malicious File](https://attack.mitre.org/techniques/T1204/002).
Name
Malicious File
ID
T1204.002
Description

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001). Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl. Adversaries may employ various forms of [Masquerading](https://attack.mitre.org/techniques/T1036) and [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to increase the likelihood that a user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying instructions to a user on how to open it.(Citation: Password Protected Word Docs) While [Malicious File](https://attack.mitre.org/techniques/T1204/002) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534).

External References

- https://otx.alienvault.com/pulse/64ff2147a9c6a0ac000ebf2f
- https://www.truesec.com/hub/blog/darkgate-loader-delivered-via-teams