



| Flash |

DarkGate Popularity Prompts Pause on New User Support

F-2023-09-15a

Classification: TLP: GREEN

Criticality: Low

Intelligence Requirements: Malware

September 15, 2023

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on September 15, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Flash | DarkGate Popularity Prompts Pause on New User Support

› Key Findings

- The resurgence in popularity of DarkGate malware has prompted its founder to discontinue support for new users—a move that ZeroFox assesses is temporary and will lead to a larger number of threat actors deploying this tool, particularly in light of this malware hitting the news cycle.
- Threat actors continue to praise DarkGate for its effectiveness, which was displayed in a recent phishing campaign using Microsoft Teams as a lure.

Analyst Commentary

The resurgence in the popularity of DarkGate malware has prompted its founder to discontinue support for new users. ZeroFox assesses this move is temporary and will lead to a larger number of threat actors deploying this tool. On September 6, 2023, developer and well-regarded threat actor “RastaFarEye” announced that the DarkGate malware project is popular and has now sold 30 licenses to monthly users. In this update, the threat actor noted that their current team cannot support any additional users and, therefore, the sale of licenses is currently suspended (see Figure 1). Of note, this is 20 more licenses than the original 10 the threat actor advertised in June 2023.

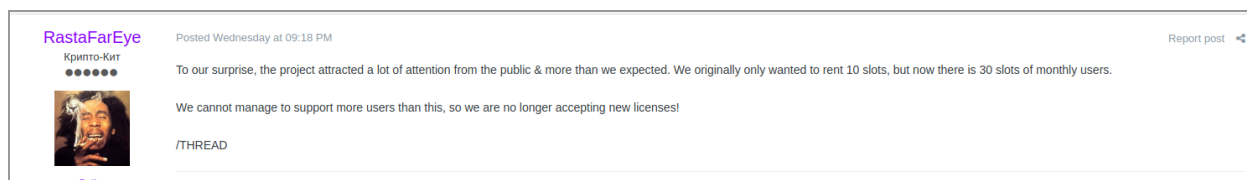


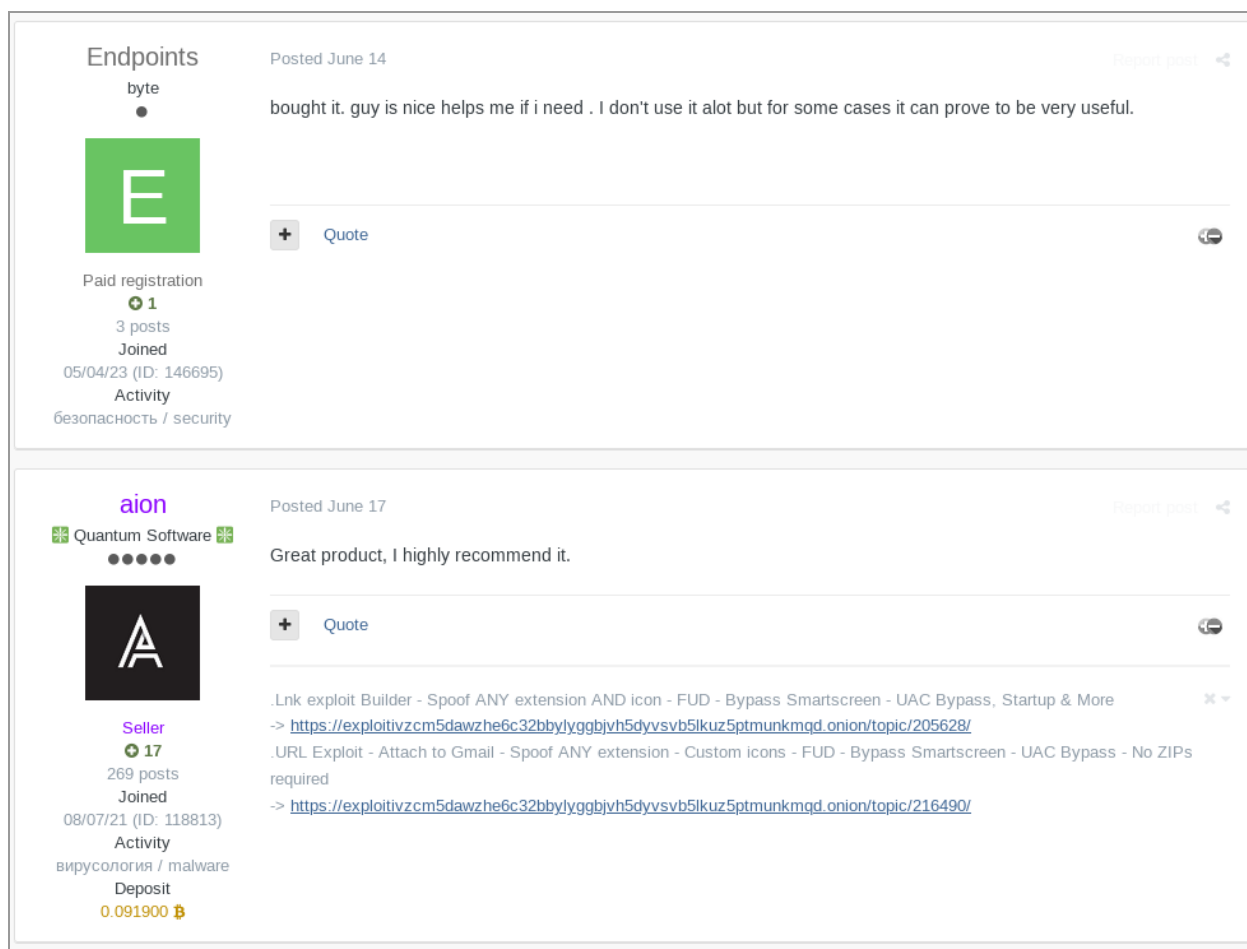
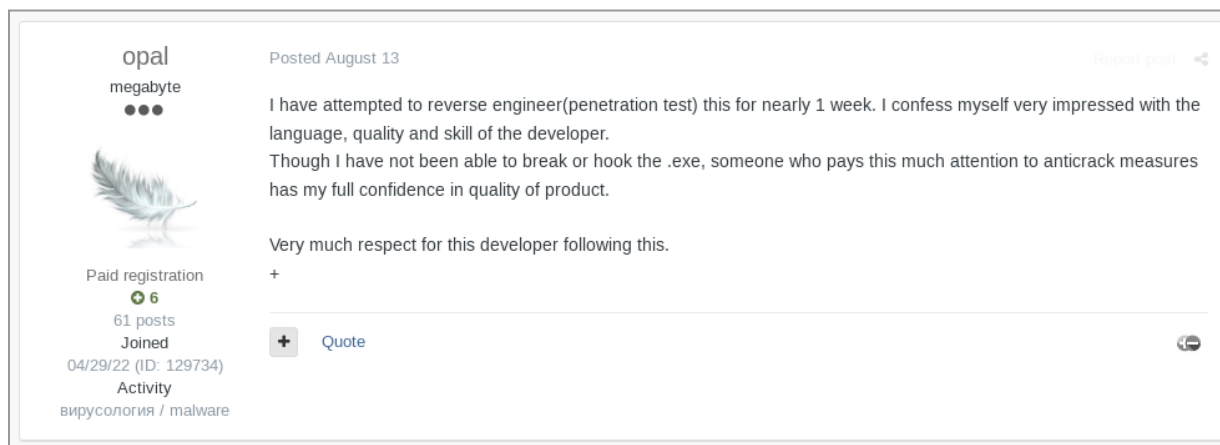
Figure 1. RastaFarEye announced they have 30 monthly users of the DarkGate malware and will not sell additional licenses

Source: ZeroFox Intelligence

Threat actors continue to praise DarkGate for its effectiveness, which was displayed in a recent phishing campaign using Microsoft Teams as a lure. RastaFarEye's original advertisement continues to receive high praise and an above-average amount of interest from peer threat actors. ZeroFox researchers assess that the positive feedback was partially generated by the threat actor's continual updates to the DarkGate malware project that have provided additional features and bug fixes.

Attention from peer threat actors is a significant metric in the underground. Positive reviews from other threat actors further reinforce an offering's perceived value in the underground. Given that threat actors operate in an environment full of deception, these testimonials could add weight to the malware's credibility. The above-average engagement on the thread likely indicates its prominence in threat actor circles. ZeroFox researchers observed feedback from peer threat actors stating (see Figures 2-3):

- The malware works as advertised.
- The threat actor is quick to respond and reputable.
- The malware is difficult to reverse.

**Figure 2. Peer threat actor praising DarkGate malware and threat actor RastaFarEye***Source: ZeroFox Intelligence***Figure 3. Peer threat actor praising DarkGate malware, claiming it is difficult to reverse engineer***Source: ZeroFox Intelligence*

ZeroFox researchers have identified channels the threat actor uses to market the malware. Initially, updates were advertised on both the deep web Russian-language forums, Exploit and XSS. This multi-platform approach increases visibility and the potential customer base. Researchers observed a shift in this trend, with the latest updates exclusively being promoted on Exploit.

As previously reported in [Volume 3: Issue 12 of ZeroFox's The Underground Economist](#), the threat actor has updated the DarkGate malware 17 times (see Figures 4-8). The most notable updates the malware has received:

- Enhance the rootkit
- Establish persistence on a machine even when files are removed from the installation folder
- Contain hidden startup methods
- Enhance obfuscation that most antivirus products, including Windows Defender, do not detect as malicious
- Bind multiple files into generated stub for easier distribution of malware
- Scan for open ports specified by the operator
- Prevent the malware from running on machines in CIS countries
- Bypass Cloudflare headers to show real IP addresses

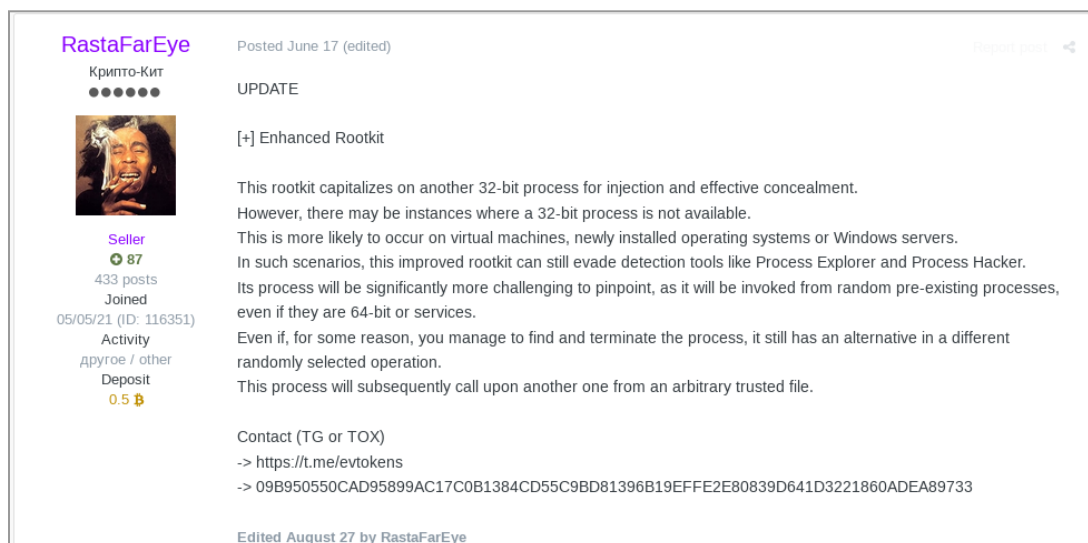


Figure 4. Post by RastaFarEye announcing update featuring enhanced rootkit

Source: ZeroFox Intelligence

RastaFarEye

Крипто-Кит

●●●●●●



Seller

87

433 posts

Joined

05/05/21 (ID: 116351)

Activity

другое / other

Deposit

0.5

Posted June 29 (edited)

Report post

UPDATE

[+] Enhanced Loader Stability: Several internal changes to improve functionality.

The Loader is now capable of supporting up to 10,000 bots (70\$/mo Server) by each port (up to 65535), with a ping rate of once every 4 seconds.

If you require more capacity, you can simply tweak the ping configuration or launch additional DarkGate instances. Moreover, DarkGate Global now has the ability to handle an unlimited number of simultaneous connections.

[+] Persistence Module:

In the event you discover and delete the files from the installation folder, they are designed to automatically restore themselves. Plus another hidden startup method will stay in use.

[+] BSOD Protect:

If somehow the user/AV will find the installation folder and delete the files or the entire folder, not only will the files be restored, but a system critical error will also occur. In addition, the files will be installed in an alternative location. This feature operates without needing administrator privileges or any form of UAC bypass.

Contact (TG or TOX)

-> <https://t.me/evtokens>

-> 09B950550CAD95899AC17C0B1384CD55C9BD81396B19EFFE2E80839D641D3221860ADEA89733

Edited August 27 by RastaFarEye

+

Quote

Figure 5. Post by RastaFarEye announcing update featuring persistence module*Source: ZeroFox Intelligence*

RastaFarEye

Крипто-Кит

●●●●●●



Seller

👍 87

433 posts

Joined

05/05/21 (ID: 116351)

Activity

другое / other

Deposit

0.5 ₿

Posted July 12 (edited)

Report post

UPDATE - AV Cleaning

[!] Bypass Sophos EDR + Sophos AV detection in au3 (main module)

[!] Updated au3 script apis morpher to fix detection by Kaspersky & Avast in vbs/msi

[!] Fixed Symantec & Avast detection in a few methods from PE Injection library

[*] Windows Defender NOT triggering any detections on delivery

Contact (TG or TOX)

-> <https://t.me/evtokens>

-> 09B950550CAD95899AC17C0B1384CD55C9BD81396B19EFFE2E80839D641D3221860ADEA89733

Edited August 27 by RastaFarEye

+

Quote

--> Желаю каждому чтоб извелись его мечты. Всем несчастливым, поле анаше <--

FUD DarkGate Loader -> <https://exploitvzcm5dawzhe6c32bbylyggbjvh5dyvsvb5lkuz5ptmunkmqd.onion/topic/226166/> ->

\$15,000 month / в месяц

Figure 6. Post by RastaFarEye announcing the non-detectability of malicious nature of malware by most commercial antivirus products

Source: ZeroFox Intelligence

RastaFarEye

Крипто-Кит

●●●●●●



Seller

 87

433 posts

Joined

05/05/21 (ID: 116351)

Activity

другое / other

Deposit

0.5 

Posted July 8 (edited)

Report post

UPDATE

[+] Added unique obfuscator to vbs downloader builder to bypass Windefender without issue when downloaded from internet

[+] Improved user-bug reporting system to detect issues in real-time in case they occur

Contact (TG or TOX)

-> <https://t.me/evtokens>

-> 09B950550CAD95899AC17C0B1384CD55C9BD81396B19EFFE2E80839D641D3221860ADEA89733

Edited August 27 by RastaFarEye

 Quote



-> Желаю каждому чтоб извелись его мечты. Всем несчастливым, поле анаше <--



FUD DarkGate Loader -> <https://exploitvzcm5dawzhe6c32bbylyggbjvh5dyvsvb5lkuz5ptmunkmqd.onion/topic/226166/> -> \$15,000 month / в месяц

See how it works -> <https://0xtoxin.github.io/threat-breakdown/DarkGate-Campaign-Analysis/>

In the news -> <https://github.security.telekom.com/2023/08/darkgate-loader.html>

Windows Secure-Websocket HVNC -> <https://exploitvzcm5dawzhe6c32bbylyggbjvh5dyvsvb5lkuz5ptmunkmqd.onion/topic/202662/> -> \$15,000 lifetime / на всегда

MacOS Secure-Websocket HVNC -> <https://exploitvzcm5dawzhe6c32bbylyggbjvh5dyvsvb5lkuz5ptmunkmqd.onion/topic/223196/> -> \$60,000 lifetime / на всегда

SecurityLab.ru wrote about it -> <https://www.securitylab.ru/news/540559.php>

<https://exploitvzcm5dawzhe6c32bbylyggbjvh5dyvsvb5lkuz5ptmunkmqd.onion/topic/223196/>

Figure 7. Post by RastaFarEye announcing that Windows Defender will not detect downloads made by the malware as malicious

Source: ZeroFox Intelligence

robber666

megabyte

●●●



Paid registration
👤 3

79 posts

Joined

04/04/21 (ID: 103432)

Activity

фрикинг / phreaking

Posted July 9

Report post

Works pretty good. RT results are good af.

+ Quote

RastaFarEye

Крипто-Кит

●●●●●●



Seller

👤 87

433 posts

Joined

05/05/21 (ID: 116351)

Activity

другое / other

Deposit

0.5 ₿

Posted July 10 (edited)

Report post

UPDATE

[+] Binder added onto builder

[!] You can bind multiple files into your generated stub and select the mode it operates with command line support:

- Once Execute in memory
- Always Execute in memory
- Once Execute on disk
- Always Execute on disk
- Once Drop
- Always Drop

[+] Listen on Multiple ports (when opening darkgate, select a port range to allow multiple botnets in a single panel)

- You can specify 2351-2355 for example, and when you make a build you can mark an individual port to connect to

Contact (TG or TOX)

-> <https://t.me/evtokens>

-> 09B950550CAD95899AC17C0B1384CD55C9BD81396B19EFFE2E80839D641D3221860ADEA89733

**Figure 8. Post by RastaFarEye announcing file binder
and positive feedback from peer threat actor “robber666”**

Source: ZeroFox Intelligence

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%