

The Underground Economist: Volume 3, Issue 12

 zerofox.com/blog/the-underground-economist-volume-3-issue-12/

June 27, 2023



5 minute read

Welcome back to The Underground Economist: Volume 3, Issue 12, an intelligence focused blog series illuminating dark web findings in digestible tidbits from our [ZeroFox Dark Ops intelligence team](#). The Dark Ops team scours the dark web, extending visibility and engagement into places traditional security teams can't reach to share meaningful and insightful intelligence on the trends and tactics threat actors are leveraging across the dark web and criminal underground. Here's the latest for the week of June 26, 2023.

Multifunctional Malware Dubbed 'DarkGate' Advertised

Well-regarded and established threat actor "RastaFarEye" advertised a multi-functional malware, dubbed "DarkGate," on the predominantly Russian language Deep Web forum "Exploit." This privately developed malware would allow threat actors to build their own botnets by compromising and controlling various Windows machines.

Additional features of the malware include:

- Generates malicious .lnk files

- Small build size (490kb)
- Runs in memory
- Obfuscates payloads to avoid detection by most antivirus products' dynamic scans
- Maintains access to compromised machines across system restarts
- Steals sensitive data from web browsers
- Logs keystrokes
- Gains higher-level permissions on compromised machines
- Uses the resources of compromised machines for cryptocurrency mining

Prices for the malware vary depending on the length of the license, including:

- \$100,000 USD per year
- \$15,000 USD per month
- \$1,000 USD per day

The screenshot shows a forum post by a user named 'RastaFarEye' with a profile picture of a man. The post is titled 'Крипто-Кит' and has a rating of 67. The text of the post describes a multi-functional malware tool that has been working on since early 2017. It claims to be undetected by any antivirus and offers various features like privilege escalation and data theft. The post lists current prices for different license durations: 1 day for 1000\$, monthly for 15,000\$, and 1 year for 100,000\$. The post also includes a warning to read the thread carefully and a note that the price is expected to rise in the coming months.

Original screenshot from threat actor “RastaFarEye” advertising a multi-functional malware dubbed “DarkGate”

Actor Highlights Free GitHub Projects That Facilitate Cyber Crime

Well-regarded threat actor and moderator “Nowheretogo” advertised two free GitHub projects that facilitate cyber crime on the Russian language Dark Web forum “RAMP.”

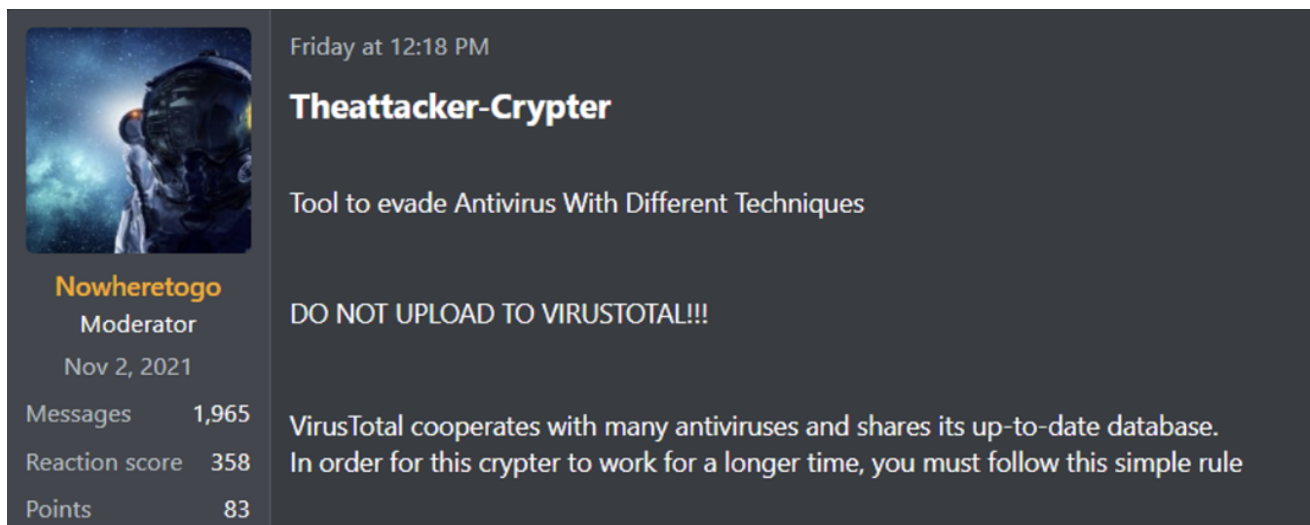
The actor first highlighted a free obfuscation tool, dubbed “Theattacker-Crypter,” on June 9, 2023. The tool allows threat actors to encrypt malicious files to avoid detection by most antivirus products. This is accomplished by injecting payloads into processes on 32-bit or 64-bit Windows machines.

The tool also contains several post-exploitation modules, including:

- Bypasses AMSI to run PowerShell commands
- Deletes malicious .exe file from target machine after process injection
- Notifies user when payload executed

The actor advertised a second project, dubbed “ShadowByte-Botnet,” on June 16, 2023. This project allows a threat actor to build their own botnet by compromising and controlling both Windows and Linux machines. In addition to malicious .exe files, the project contains the resources for threat actors to host their own command-and-control (C2) servers.

ZeroFox researchers assess the presence of these free tools will likely facilitate an increase in cyber-attacks because they lower the barrier to entry for threat actors.



The screenshot shows a forum post on a dark background. On the left, there is a profile card for the user 'Nowheretogo', a Moderator, with a profile picture of a person in a space helmet. The card shows the user's name in orange, their role, the date 'Nov 2, 2021', and statistics: Messages (1,965), Reaction score (358), and Points (83). The main post content is on the right, starting with a timestamp 'Friday at 12:18 PM' and the title 'Theattacker-Crypter' in white. Below the title is the subtitle 'Tool to evade Antivirus With Different Techniques'. A warning in white text reads 'DO NOT UPLOAD TO VIRUSTOTAL!!!'. The main body of the post contains the text: 'VirusTotal cooperates with many antiviruses and shares its up-to-date database. In order for this crypter to work for a longer time, you must follow this simple rule'.

Original screenshots from threat actor “Nowheretogo” advertising two free GitHub projects that facilitate cyber crime.

New ‘Meduza’ Stealer Malware Announced

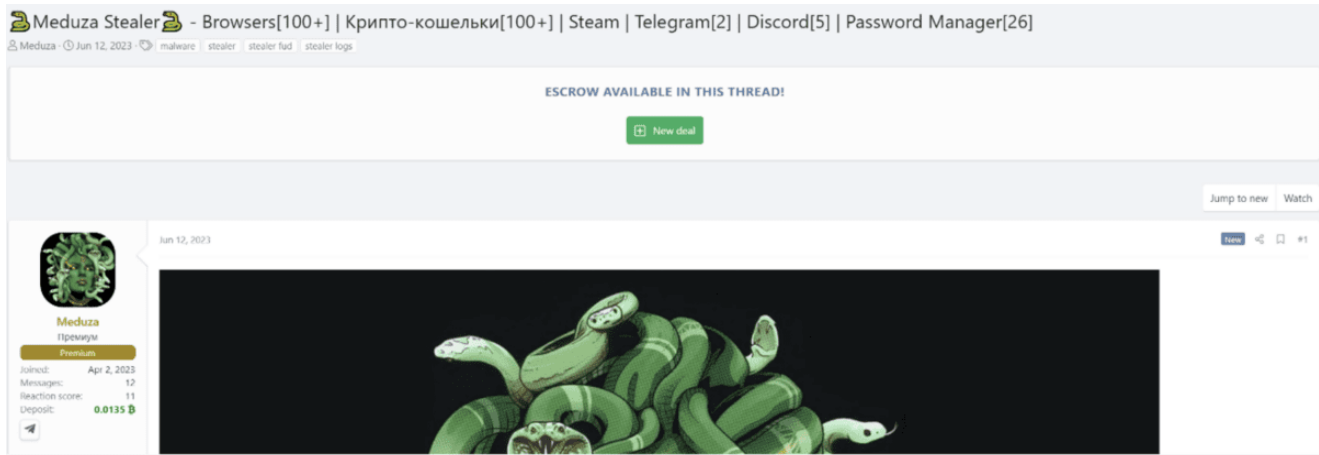
Well-regarded threat actor “Meduza” announced a new stealer malware, dubbed “Meduza,” on the predominantly Russian language Deep Web forum “XSS.” In addition to stealing login credentials and other browser information from victims, the malware collects sensitive data from:

- Various cryptocurrency wallets
- Password managers
- Discord
- Telegram
- Steam
- OpenVPN

The malware also comes with a secure web panel that would allow threat actors to exfiltrate the stolen data and view statistics about the compromised machines.

The actor charged \$200 USD per month for the stealer malware.

ZeroFox researchers assess this new stealer is likely to gain traction among threat actors on the criminal underground because several well-regarded peers have already vouched for the malware.



Original screenshot from threat actor “Meduza” announcing new stealer malware dubbed “Meduza”


Zero-Day Exploit For Vulnerability In Peplink Routers Alleged

New and untested threat actor “Celine” announced an alleged exploit for a zero-day buffer overflow vulnerability in Peplink routers on the English language Dark Web forum “Onniforums.” The alleged exploit would give threat actors administrator access to the compromised devices. The actor claims they successfully tested the exploit on routers based in Thailand.

ZeroFox highlights the impact of this alleged zero-day exploit would likely be significant because many public safety agencies leverage Peplink routers, including police, fire, and emergency medical services.

Our researchers note it is unclear how credible the actor’s claim is without conducting further analysis.

Free 0 Day BC i like this place. Threaded Mode



Celine
Newbie

Posts: 6
Threads: 2
Joined: Jun 2023
Reputation: 0
Credits: 8.69€ [Donate]

Yesterday, 08:16 AM #1

This Forum owner give me good vibe, so i contribute my one of new 0 day, i find, on Peplink router, are used by the companies around as SD Wan, Wan Aggregation tool, it give root shell on a boot sector by way of buffer overflow i will not provide code, just research :). Peplink router use receive buffer, and they also use Wan Smoothing, and speed fusion. Let us talk speed fusion. Speed fusion allow peplink router use any data sources and fuze them together for a 25% overhead to increase bandwidth. This no design fuze two small make big bc of overhead instead designed to take two big and make one really big. The Technology uses DPI to filter packets at the packet level and forward them in and then forward them on. Now. Since this is huge huge news. We talk about use of exploit. Since Speed fusion uses multiple wans, u can imagine NIC assoc no have big ram or rom capacity in fact less than RPi on most of the PLC nic, but they are also like stated on receive buffer for the DPI, and the other peplink features, This receive buffer overflows to the main lan of the router and when used in combo with buffer OF, you find that you are able to get in in very little effort. sometime on bigger one shell spawn native to that vlan but i was able use vlan hopping to escalate quite easily from there.... Pep link in any police, air, fire, ambulance and other govt vehicles, they have Geo-fencing equipped also, so locally searching for the beacons is a very good way to identify router. Buy old pep-link use old pep link for research but read the docs, They overview all of this and if u know what i know u know, u know this is buffer over-flow PoC.. but they also have receive buffer built in on all nic and main SD wan plc, so this said, use of buffer overflow.. These routers if your buffer overflow has proper code, when used with nic, there is info steps, NIC will only receive traffic from designated signals set up but then it aggregates signal using speed fusion, which runs similar to a vpn by encapsulating all the packets into a tunnel and using the combined wan speed to make an aggregated smoother wan connection for consumer. Also it allows for some do cellular. So, To buffer script, should run, SD Wan signal packet with same info as source so firewall will receive it buffer overflow, code right with binary encoding correctly formatted to same as host formatting should spawn root shell on router, fragment it correctly and ensure it is an active line, with this proof of concept i have been able to successfully, gain shells on router across Thailand pep link secret sauce is this speed fusion, but also Speed fusion cloud, which is where an aggregate host use pep link virtual wans and fuze virtual wan with physical wan through use of Vlan type technology spoof speed-fusion, execute vlan hopping, root access 0 day configured. , This is highly insecure because of how exchange take place for this if user have speed fusion cloud enable they then have given open door if u cannot perform either of these attack broke down like this. U need learn more, these are very easy, and the Sorry for English, not normal term use but. Read 0 day for pep-link from past few on cve, this problem is persistent problem, and also may be easily accessed and replicated using cradle point and any of the other SD Wan, Multi Wan Signal Combo devices. This is not unique to peplink, As i learn this work on cradlepoint some model as well. They firewalls on peplink are much worse tho, n they r much cheaper so much more everywhere.

Learn More about the Authors Behind The Underground Economist

The ZeroFox Dark Ops team is embedded in the underground economy, offering dark web intelligence, direct threat actor engagement, and unmatched visibility into the dark web. Our global threat hunting and dark web intelligence team extends the reach of your security resources, engaging with the underground community. We give you an advantage over emerging threats and stop active threats before damage can be done. Integrated into hundreds of dark web communities and places where most can't infiltrate, we combine open-source and human intelligence to fight back, engage with adversaries, triage threats and curate intelligence specific to you. [Learn more here.](#)



Take a tour of the dark web, guided by facts – not fear.

START NOW

Tags: [Deep & Dark Web](#) , [Threat Intelligence](#)