The Underground Economist: Volume 3, Issue 12

By Learn More about the Authors Behind The Underground Economist

Archived: 2026-04-05 20:22:16 UTC

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

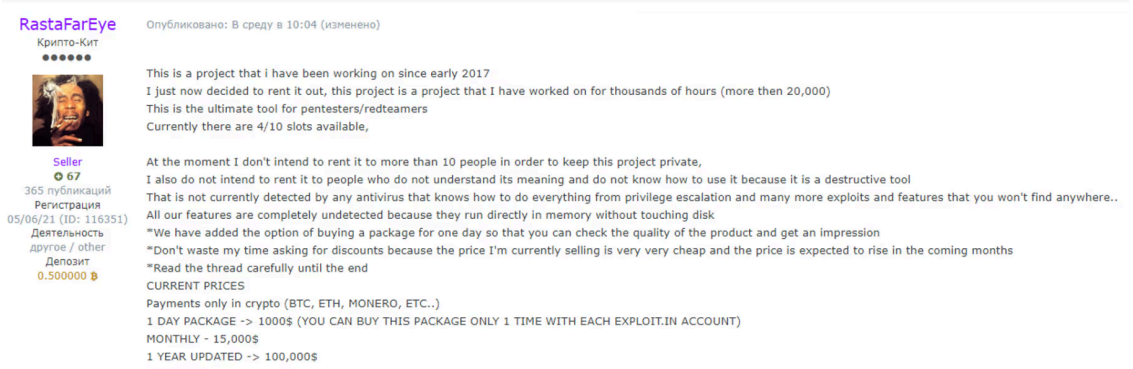
Well-regarded and established threat actor "RastaFarEye" advertised a multi-functional malware, dubbed "DarkGate," on the predominantly Russian language Deep Web forum "Exploit." This privately developed malware would allow threat actors to build their own botnets by compromising and controlling various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



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.”

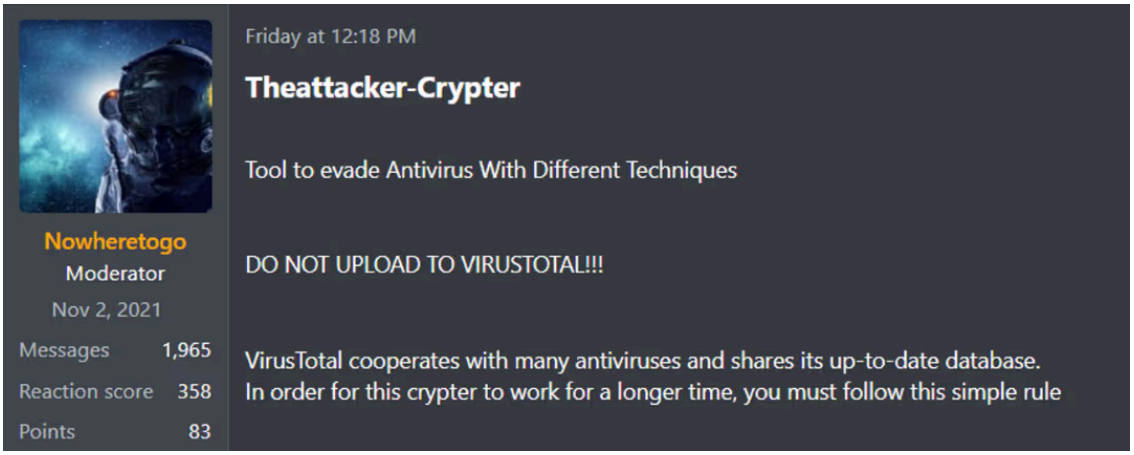
The actor first highlighted a free obfuscation tool, dubbed “Theattacker-Crypter,” on June 9, 2023. The tool allows threat actors to encrypt malicious files to avoid detection by most antivirus products. This is accomplished by injecting payloads into processes on 32-bit or 64-bit Windows machines.

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.



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

New ‘Meduza’ Stealer Malware Announced

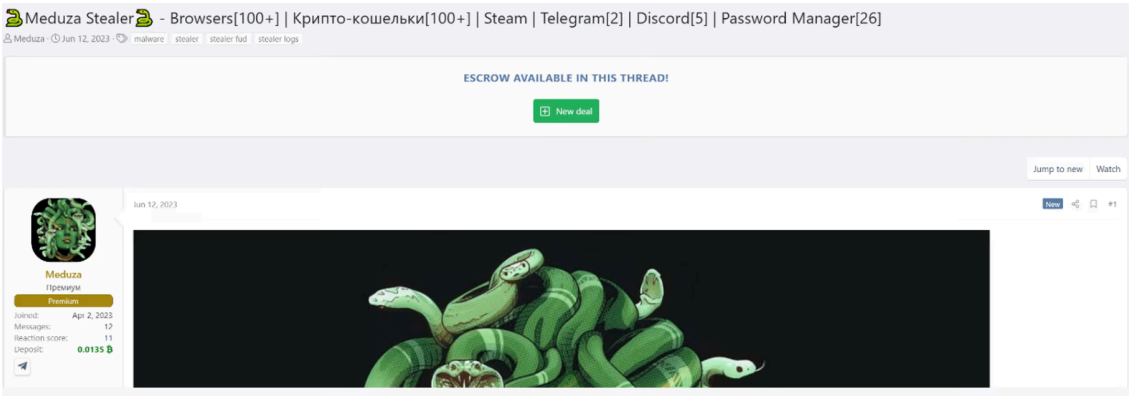
Well-regarded threat actor “Meduza” announced a new stealer malware, dubbed “Meduza,” on the predominantly Russian language Deep Web forum “XSS.” In addition to stealing login credentials and other browser information from victims, the malware collects sensitive data from:

- 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.



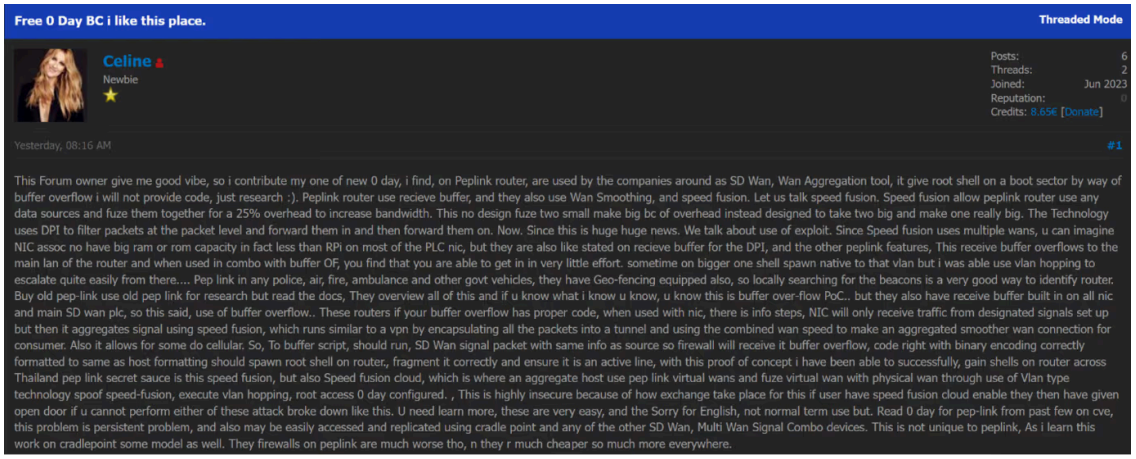
Original screenshot from threat actor “Meduza” announcing new stealer malware dubbed “Meduza”

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.



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.

Source: https://www.zerofox.com/blog/the-underground-economist-volume-3-issue-12/