New Borat remote access malware is no laughing matter

bleepingcomputer.com/news/security/new-borat-remote-access-malware-is-no-laughing-matter/

Bill Toulas

By
Bill Toulas

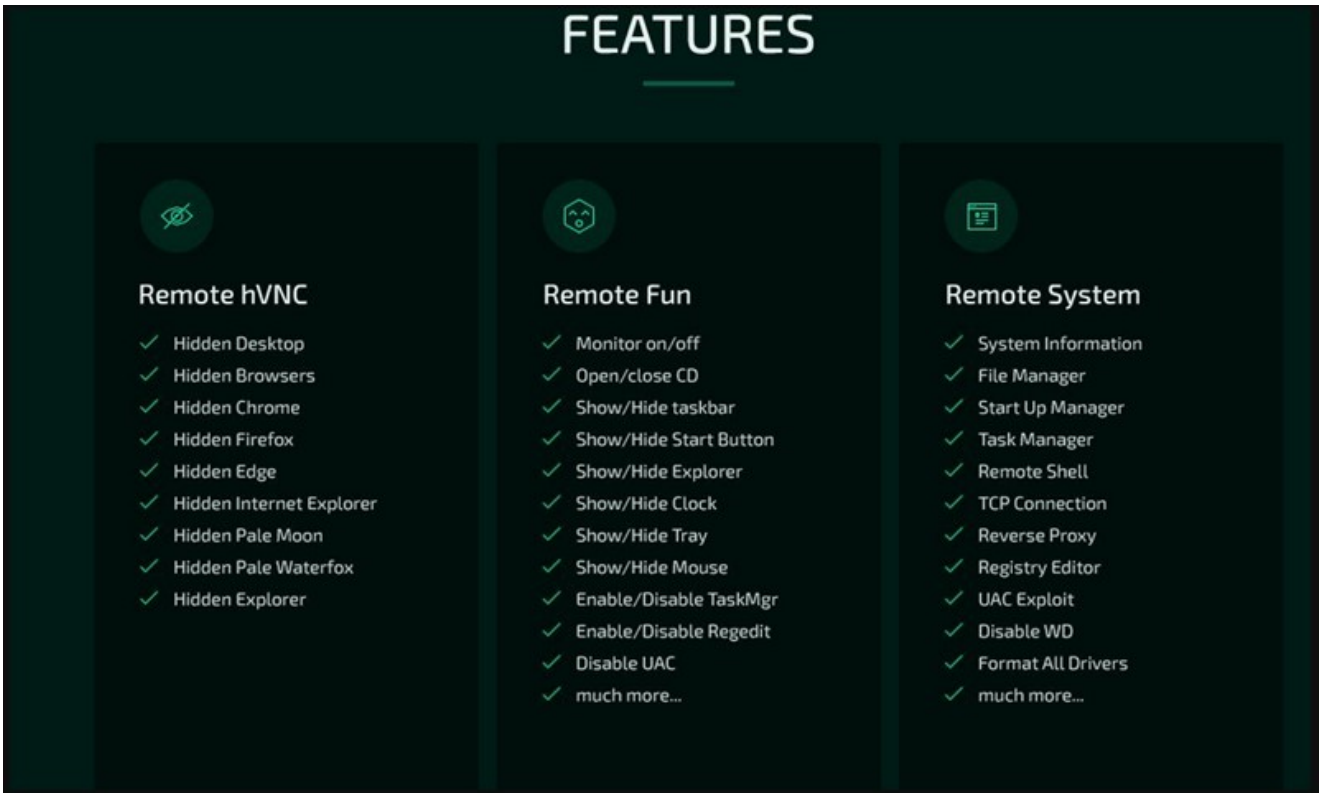
- April 3, 2022
- 10:02 AM
- 0

A new remote access trojan (RAT) named Borat has appeared on darknet markets, offering easy-to-use features to conduct DDoS attacks, UAC bypass, and ransomware deployment.

As a RAT, Borat enables remote threat actors to take complete control of their victim's mouse and keyboard, access files, network points, and hide any signs of their presence.

The malware lets its operators choose their compilation options to create small payloads that feature precisely what they need for highly tailored attacks.

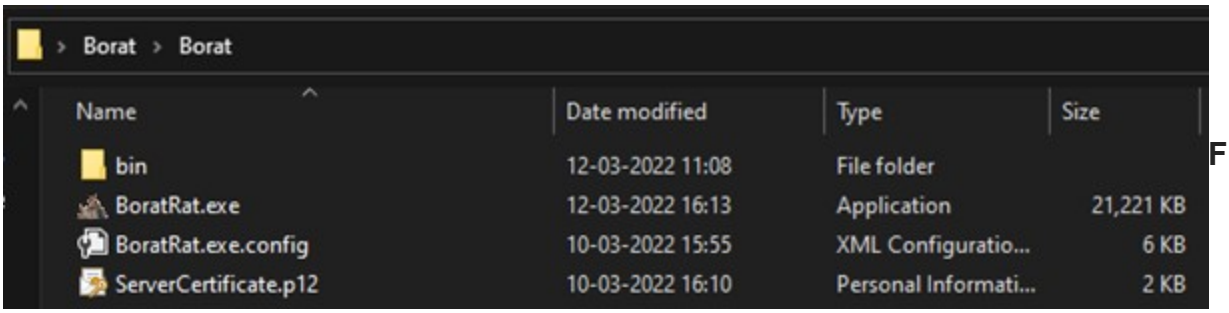
Borat was analyzed by researchers at Cyble, who spotted it in the wild and sampled the malware for a technical study that revealed its functionality.



Some of Borat's features *(Cyble)*

Extensive features

It is unclear if the Borat RAT is sold or freely shared among cybercriminals, but Cycle says it comes in the form of a package that includes a builder, the malware's modules, and a server certificate.

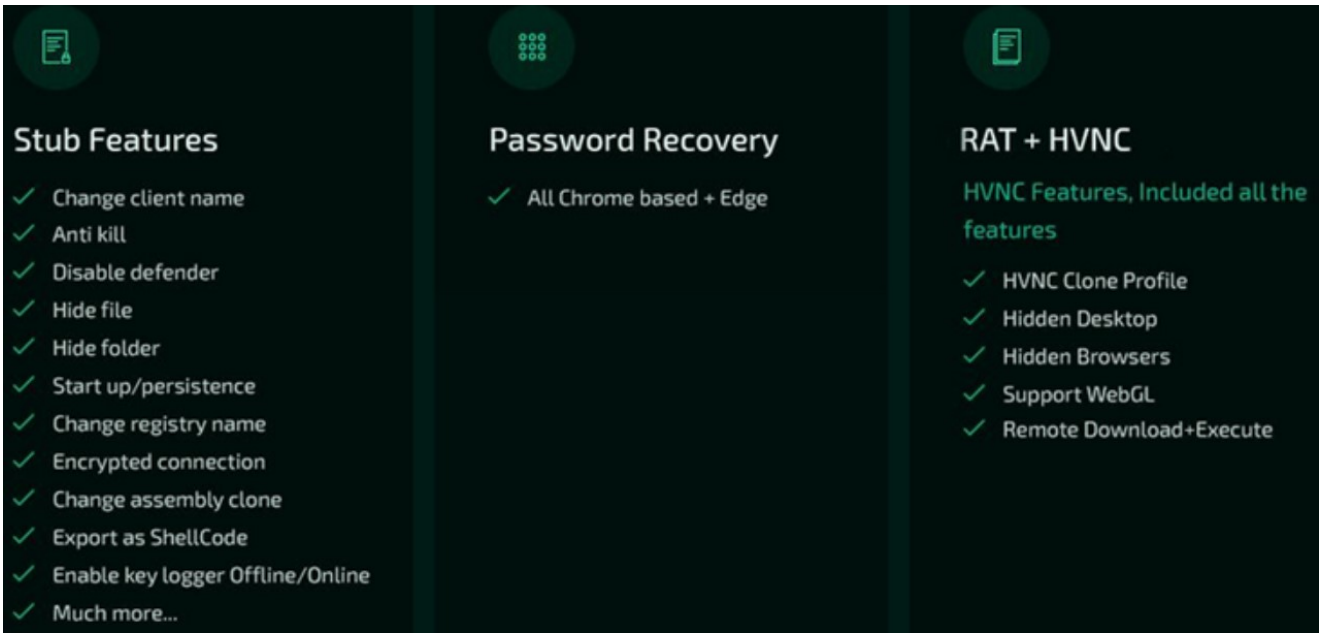


Files in the Borat RAT archive *(Cyble)*

The features of the trojan, each having its own dedicated module, include the following:

- **Keylogging** – monitor and log key presses and store them in a txt file
- **Ransomware** – deploy ransomware payloads onto the victim's machine and automatically generate a ransom note through Borat
- **DDoS** – direct garbage traffic to a target server by using the compromised machine's resources
- **Audio recording** – record audio via the microphone, if available, and store it in a wav file

- **Webcam recording** – record video from the webcam, if available
- **Remote desktop** – start a hidden remote desktop to perform file operations, use input devices, execute code, launch apps, etc.
- **Reverse proxy** – set up a reverse proxy to protect the remote operator from having their identity exposed
- **Device info** – gather basic system information
- **Process hollowing** – inject malware code into legitimate processes to evade detection
- **Credential stealing** – steal account credentials stored in Chromium-based web browsers
- **Discord token stealing** – steal Discord tokens from the victim
- **Other functions** – disrupt and confuse the victim by playing audio, swapping the mouse buttons, hiding the desktop, hiding the taskbar, holding the mouse, turning off the monitor, showing a blank screen, or hanging the system



More of Borat's advertised features *(Cyble)*

As noted in Cyble's analysis, the above features make Borat essentially a RAT, spyware, and ransomware, so it's a potent threat that could conduct a variety of malicious activity on a device.

All in all, even though the RAT's developer decided to name it after the main character of the comedy movie Borat, incarnated by Sacha Baron Cohen, the malware is no joke at all.

By digging deeper trying to find the origin of this malware, Bleeping Computer found that the payload executable was recently identified as AsyncRAT, so it's likely that its author based his work on it.

Typically, threat actors distribute these tools via laced executables or files that masquerade as cracks for games and applications, so be careful not to download anything from untrustworthy sources such as torrents or shady sites.

Related Articles:

Clop ransomware gang is back, hits 21 victims in a single month

New Windows Subsystem for Linux malware steals browser auth cookies

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.