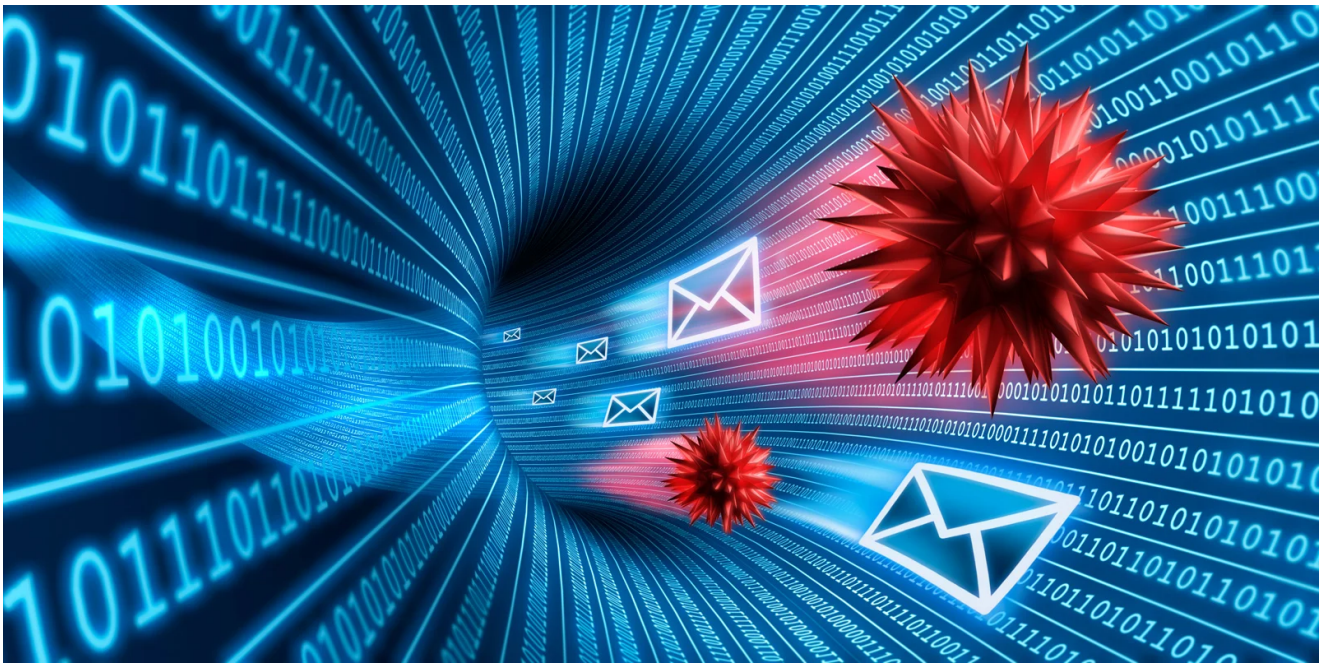
New Meta information stealer distributed in malspam campaign

bleepingcomputer.com/news/security/new-meta-information-stealer-distributed-in-malspam-campaign/

Bill Toulas

By
Bill Toulas

- April 10, 2022
- 11:12 AM
- 0



A malspam campaign has been found distributing the new META malware, a new info-stealer malware that appears to be rising in popularity among cybercriminals.

META is one of the novel info-stealers, along with Mars Stealer and BlackGuard, whose operators wish to take advantage of Raccoon Stealer's exit from the market that left many searching for their next platform.

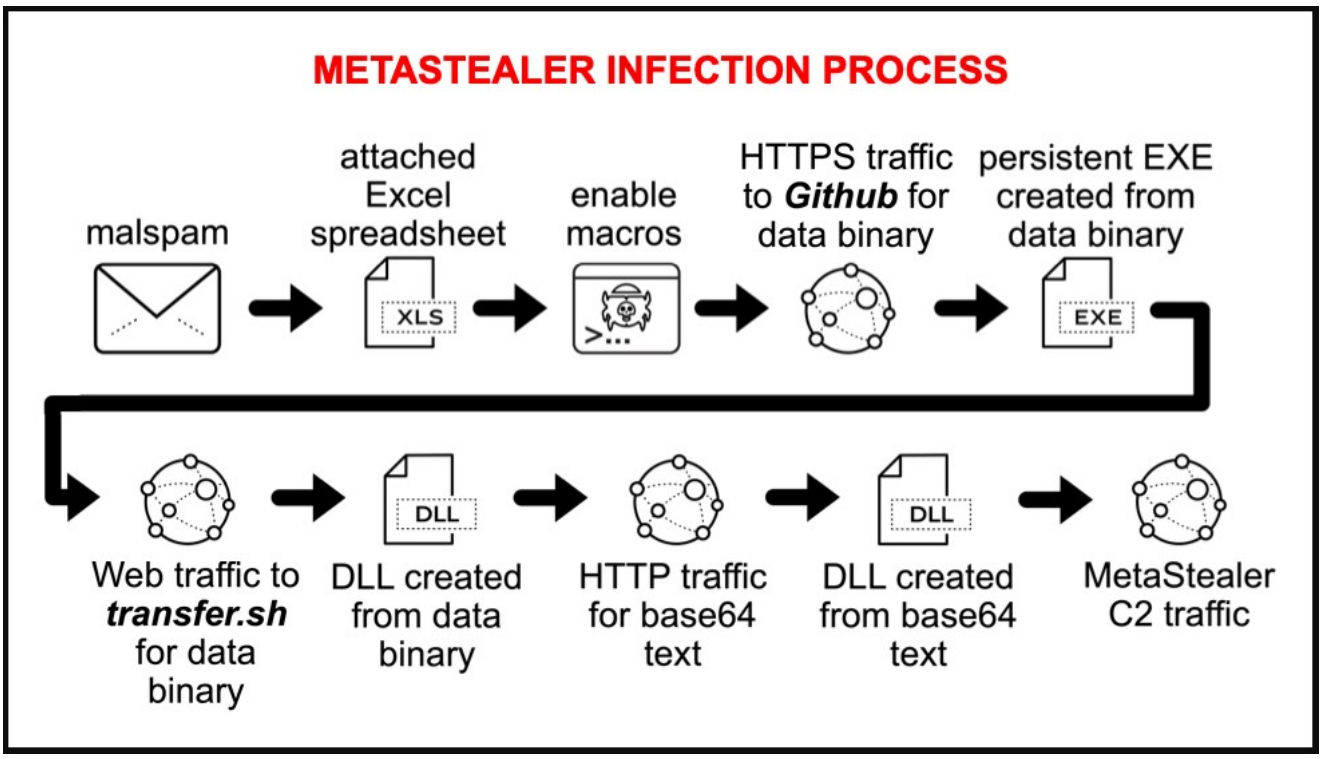
Bleeping Computer first reported about META last month, when analysts at KELA warned about its dynamic entrance into the TwoEasy botnet marketplace.

The tool is sold at $125 for monthly subscribers or $1,000 for unlimited lifetime use and is promoted as an improved version of RedLine.

New Meta malspam campaign

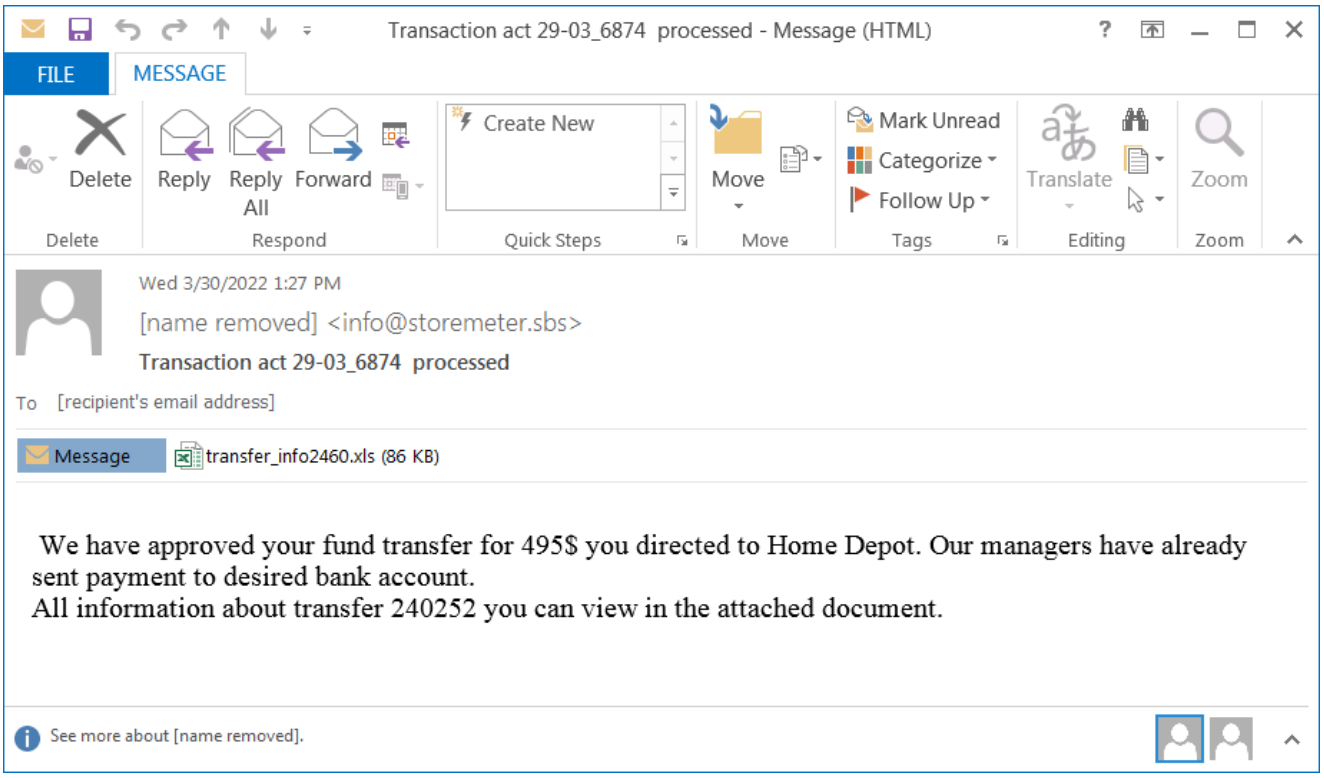
A new spam campaign seen by security researcher and ISC Handler Brad Duncan is proof that META is actively used in attacks, being deployed to steal passwords stored in Chrome, Edge, and Firefox, as well as cryptocurrency wallets.

The infection chain in the particular campaign follows the "standard" approach of a macro-laced Excel spreadsheet arriving in prospective victims' inboxes as email attachments.



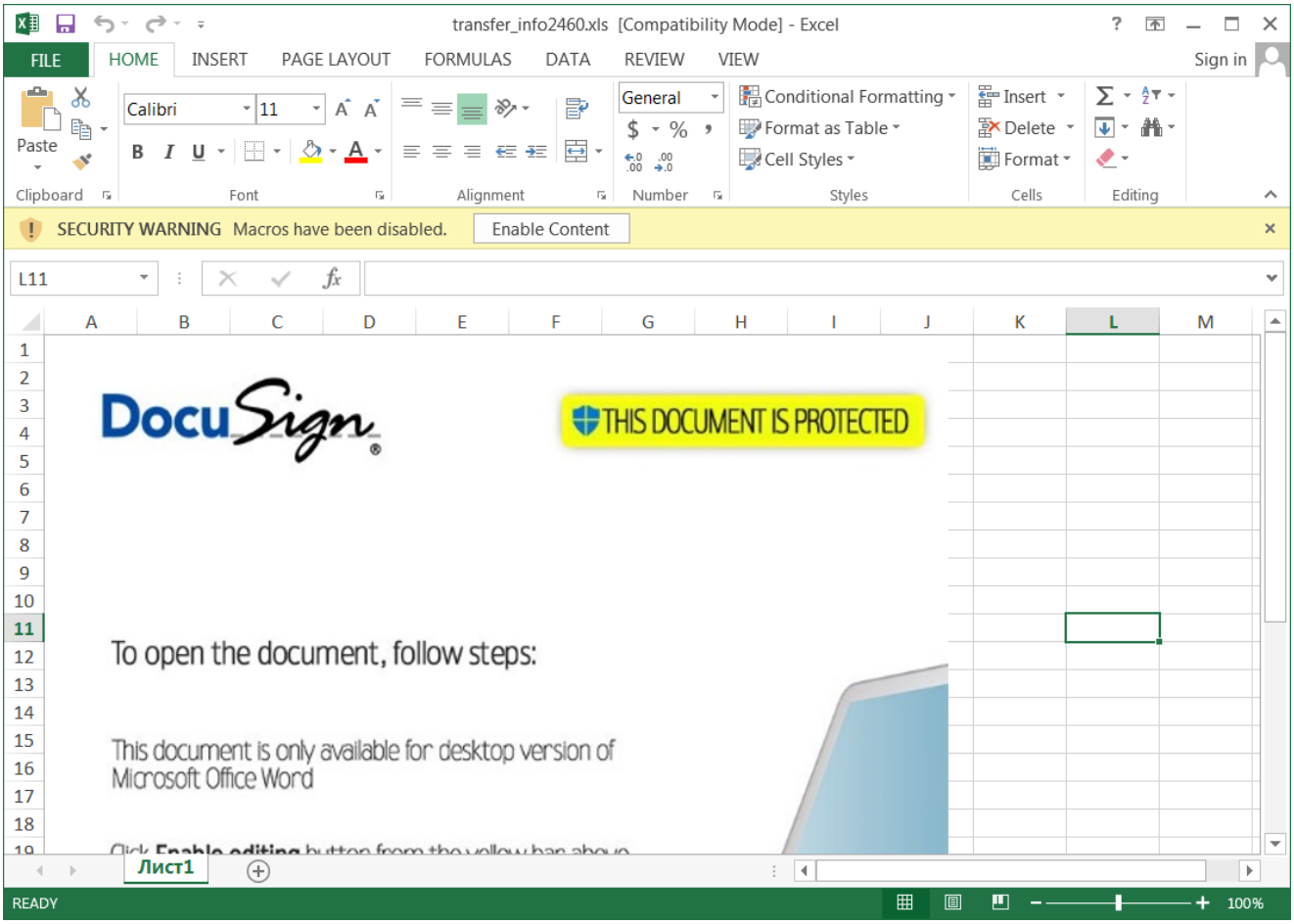
META infection chain on the spotted campaign *(isc.sans.edu)*

The messages make bogus claims of fund transfers that are not particularly convincing or well-crafted but can still be effective against a significant percentage of recipients.



Email carrying the malicious Excel attachment *(isc.sans.edu)*

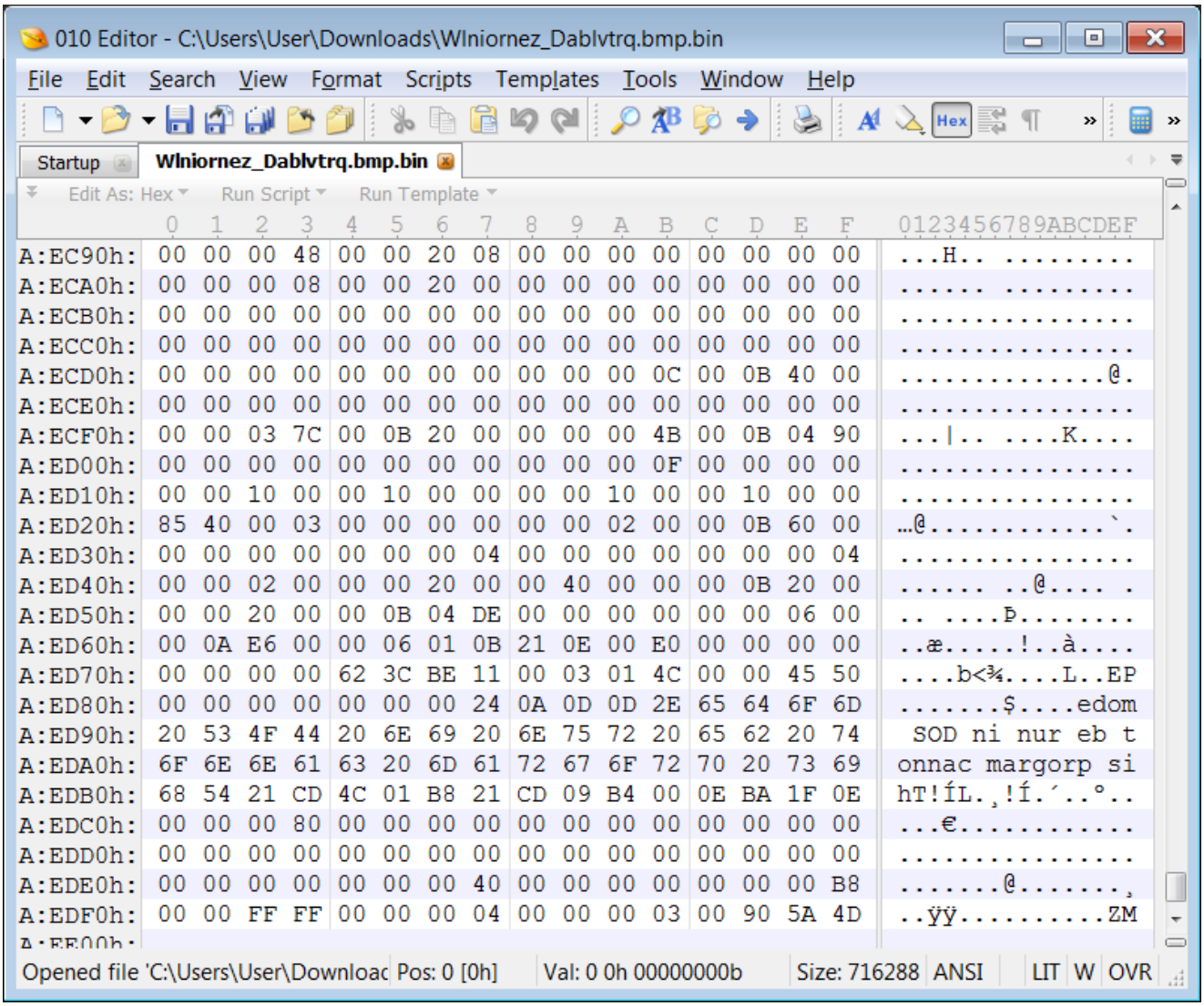
The spreadsheet files feature a DocuSign lure that urges the target to "enable content" required to run the malicious VBS macro in the background.



The DocuSign lure that entices users to enable content *(isc.sans.edu)*

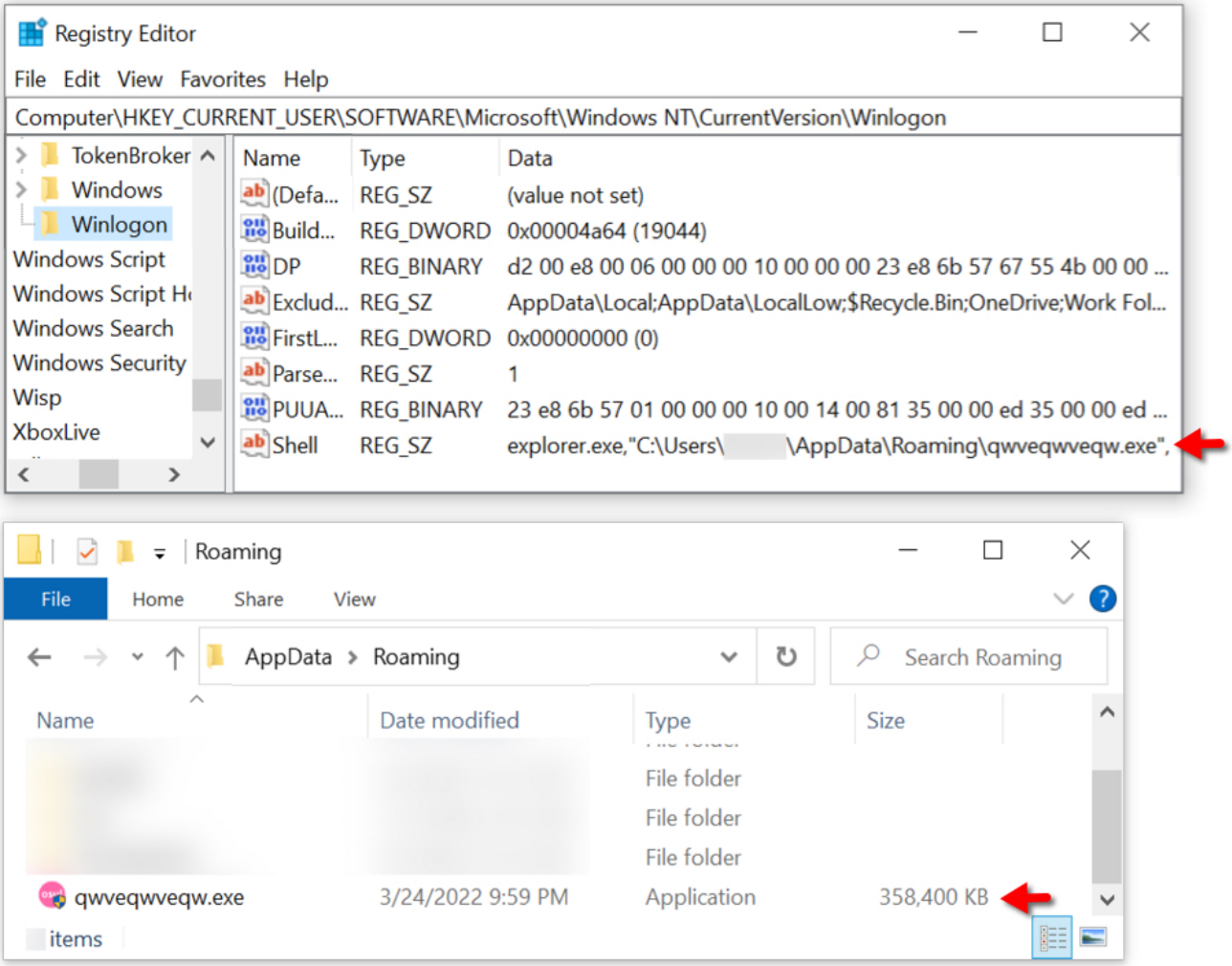
When the malicious script runs, it will download various payloads, including DLLs and executables, from multiple sites, such as GitHub.

Some of the downloaded files are base64 encoded or have their bytes reversed to bypass detection by security software. For example, below is one of the samples collected by Duncan that has its bytes reversed in the original download.



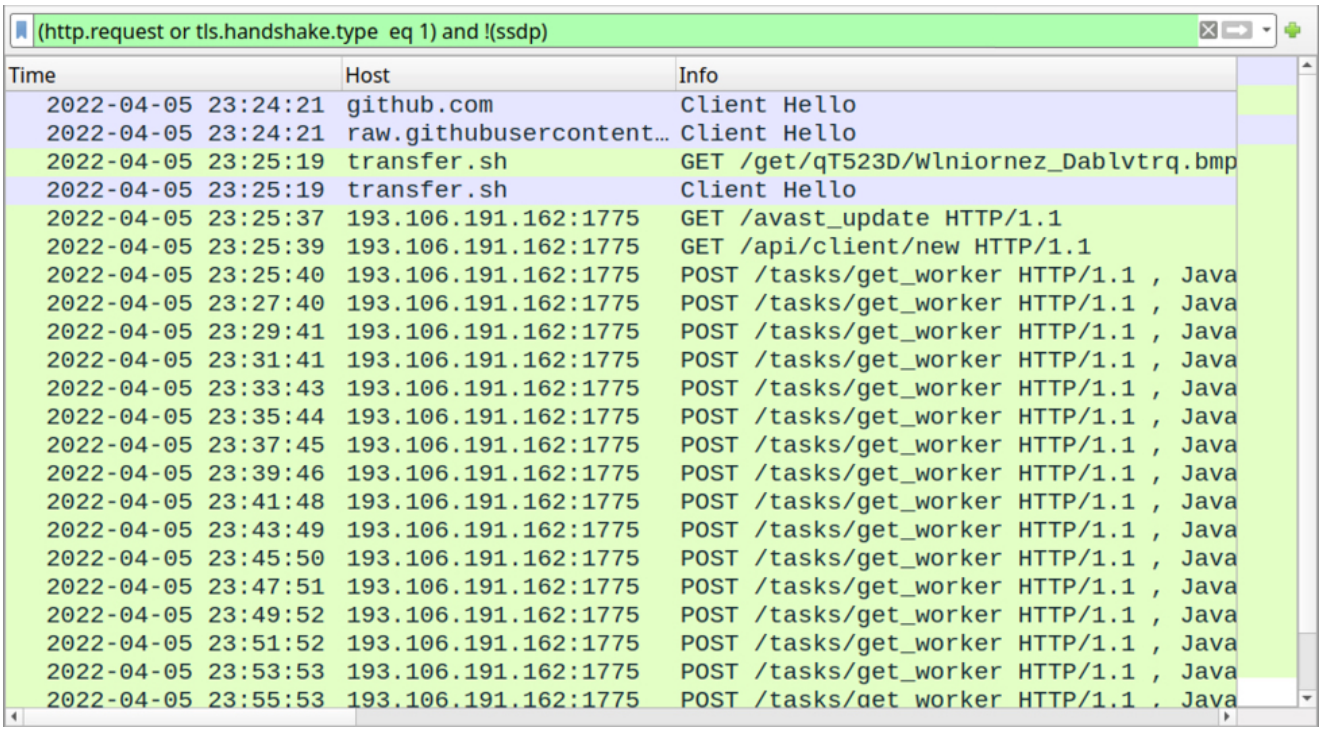
DLL saved in reverse byte order *(isc.sans.edu)*

Eventually, the final payload is assembled on the machine under the name "qwveqwveqw.exe," which is likely random, and a new registry key is added for persistence.



New registry key and the malicious executable *(isc.sans.edu)*

A clear and persistent sign of the infection is the EXE file generating traffic to a command and control server at 193.106.191[.]162, even after the system reboots, restarting the infection process on the compromised machine.



Malicious traffic captured in Wireshark *(isc.sans.edu)*

One thing to note is that META modifies Windows Defender via PowerShell to exclude .exe files from scanning, to protect its files from detection.

If you'd like to dive deeper into the malicious traffic details for detection purposes or curiosity, Duncan has published the PCAP of the infection traffic here.

Related Articles:

German automakers targeted in year-long malware campaign

Ukraine warns of “chemical attack” phishing pushing stealer malware

Pixiv, DeviantArt artists hit by NFT job offers pushing malware

New powerful Prynt Stealer malware sells for just $100 per month

PDF smuggles Microsoft Word doc to drop Snake Keylogger malware

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.