Contents

MetaStealer, a newly emerged information stealer malware coming into prominence across the cyber threat landscape, has been proliferating through a malspam campaign. The infostealer gained visibility among the security professionals from this malspam campaign; however, KELA threat hunters identified it for the first time, appearing to be a similar or improved version of RedLine stealer.

MetaStealer was launched at the start of March, and sold for USD125 per month or USD1000 for unlimited usage. It is implanted to run in the background of the target's system to steal a host of information, such as collecting login information, credit card details, and other sensitive information. Its dynamic entrance into the TwoEasy botnet marketplace facilitates the selling of stolen details.

###MetaStealer distributed via malspam in an attack flow

MetaStealer is distributed through a new spam campaign involving a phishing email sent to all the targets with a malicious attachment of a Microsoft Excel document named transfer "info2460.xls" (its name may vary) disguising as a letter regarding an approved transaction.

This confirms that MetaStealer, aka META still remains actively instrumental in the exploitation campaign to collect keystrokes (record keyboard input), exfiltrate steal login credentials mostly saved in the web browser, steal clipboard details, two-factor authentication data, cryptocurrency wallets information, system information, and other data. The malspam campaign was detected by security researcher and ISC Handler Brad Duncan.

The mail content somehow manages to convince the targeted recipient with too good to be true claims of fund transfers.

Here the chain of infection follows a series of standard approaches of a macro-laced Malicious Microsoft Excel document arriving as an email attachment featuring a DocuSign for tricking to "enable content" required to run the malicious VBS macro in the background.

However, it is essential to note that malicious documents accessed with MS Office versions released before 2010 do not require a user to enable macros commands to infect computers manually.

Upon file execution, it starts to load malicious scripts that can enable the initialization of various MetaStealer Malware payloads, including DLLs & executables, from multiple sites, such as GitHub.

While a few of the downloaded files are either base64 encoded or have their bytes reversed to bypass detection by security software.

All the payloads are assembled eventually on the targeted system under a random name "qwveqwveqw.exe", and a new registry key is added for persistence.

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

MetaStealer also modifies Windows Defender via PowerShell to evade .exe files from scanning in order to protect its files from getting detected.