[SANS ISC] RedLine Stealer Delivered Through FTP

blog.rootshell.be/2022/01/20/sans-isc-redline-stealer-delivered-through-ftp/

January 20, 2022

I published the following diary on isc.sans.edu: "*RedLine Stealer Delivered Through FTP*":

Here is a piece of malicious Python script that injects a RedLine stealer into its own process. Process injection is a common attacker's technique these days (for a long time already). The difference, in this case, is that the payload is delivered through FTP! It's pretty unusual because FTP is today less and less used for multiple reasons (lack of encryption by default, complex to filter with those passive/active modes). Support for FTP has even been disabled by default in Chrome starting with version 95! But FTP remains a common protocol in the IoT/Linux landscape with malware families like Mirai. My honeypots still collect a lot of Mirai samples on FTP servers. I don't understand why the attacker chose this protocol because, in most corporate environments, FTP is not allowed by default (and should definitely not be!)… [Read more]