Doctor Web detected Linux Trojan written in Go

news.drweb.com/news/

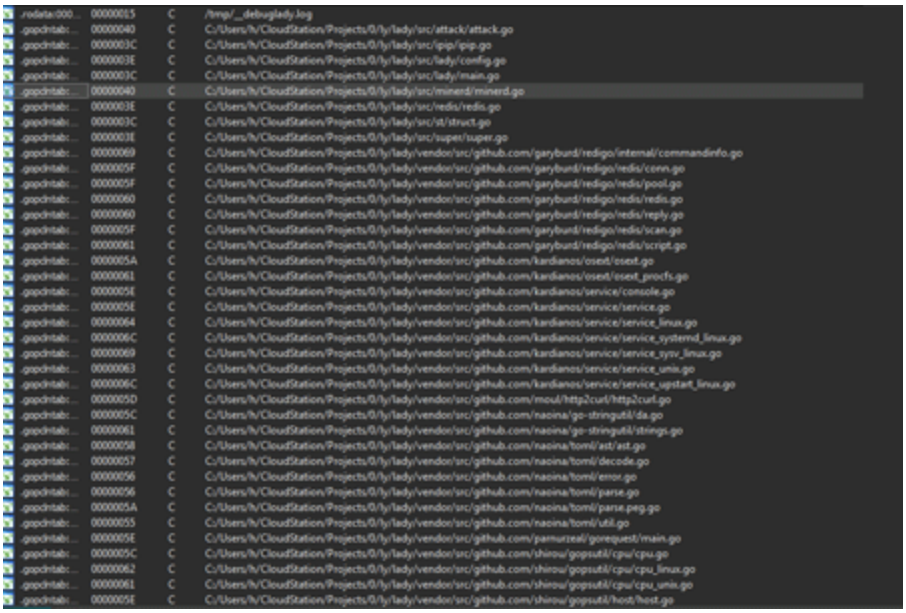
Doctor Web

Back to news

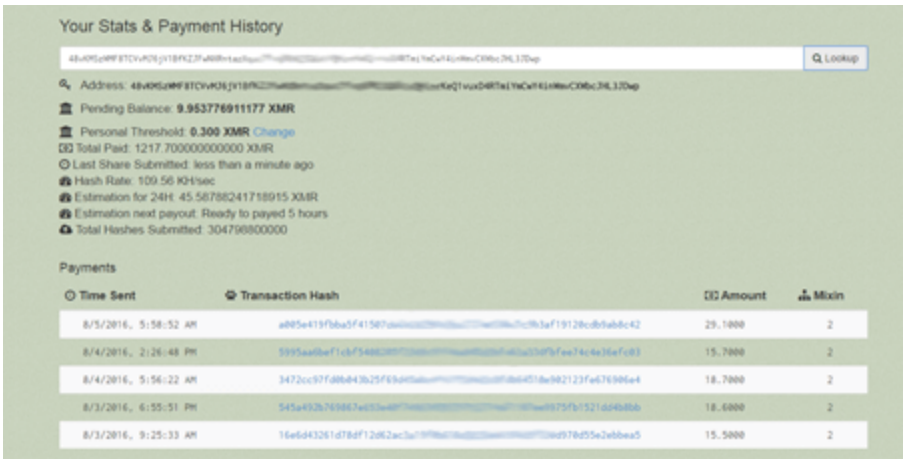
August 8, 2016

Doctor Web analysts have detected and examined a new Linux Trojan which is able to run a cryptocurrency mining program on an infected computer. Its key feature lies in the fact that it is written in Go, a language developed by Google.

A Trojan, named **Linux.Lady.1**, can execute a limited range of actions such as to determine an external IP address of the infected computer, to attack other computers, and to download and launch a cryptocurrency mining software. **Linux.Lady.1** is written in the Google developed programming language—Go. Although Doctor Web security researchers have already encountered Trojans written in Go, such malware programs are not frequently detected in the wild. The architecture of the Trojan consists of numerous libraries published on GitHub—the most popular collaborative application development service.



Once **Linux.Lady.1** is launched, it sends the following information to the command and control server: the current Linux version and the name of the operating system family it belongs to, a number of CPUs, names and a number of running processes, and so on. The Trojan receives a configuration file necessary for downloading and launching of a cryptocurrency mining program in order to generate income which is then transferred to the cybercriminals' e-wallet.



Linux.Lady.1 can also determine an external IP address of the infected computer using special websites, specified in the configuration file, and attack other computers of the network. The Trojan tries to connect to the remote servers via a port used by the Redis (remote dictionary server) data structure store, without entering a password in expectation that the system has not been configured correctly. If the connection is established, the malware adds a downloader script, named **Linux.DownLoader.196**, to the cron scheduler. The script downloads a copy of **Linux.Lady.1** and installs it on the compromised host. Then the Trojan adds a key for connection to the computer over SSH protocol to the list of authorized keys.

Dr.Web for Linux successfully detects and removes **Linux.Lady.1** and **Linux.DownLoader.196**, therefore, these malicious programs pose no threat to our users.

More about this Trojan

What is the benefit of having an account?

Tell us what you think

To ask Doctor Web's site administration about a news item, enter @admin at the beginning of your comment. If your question is for the author of one of the comments, put @ before their names.

Other comments