Russian Hacker Pleads Guilty for Role in Infamous Linux Ebury Malware

By Catalin Cimpanu

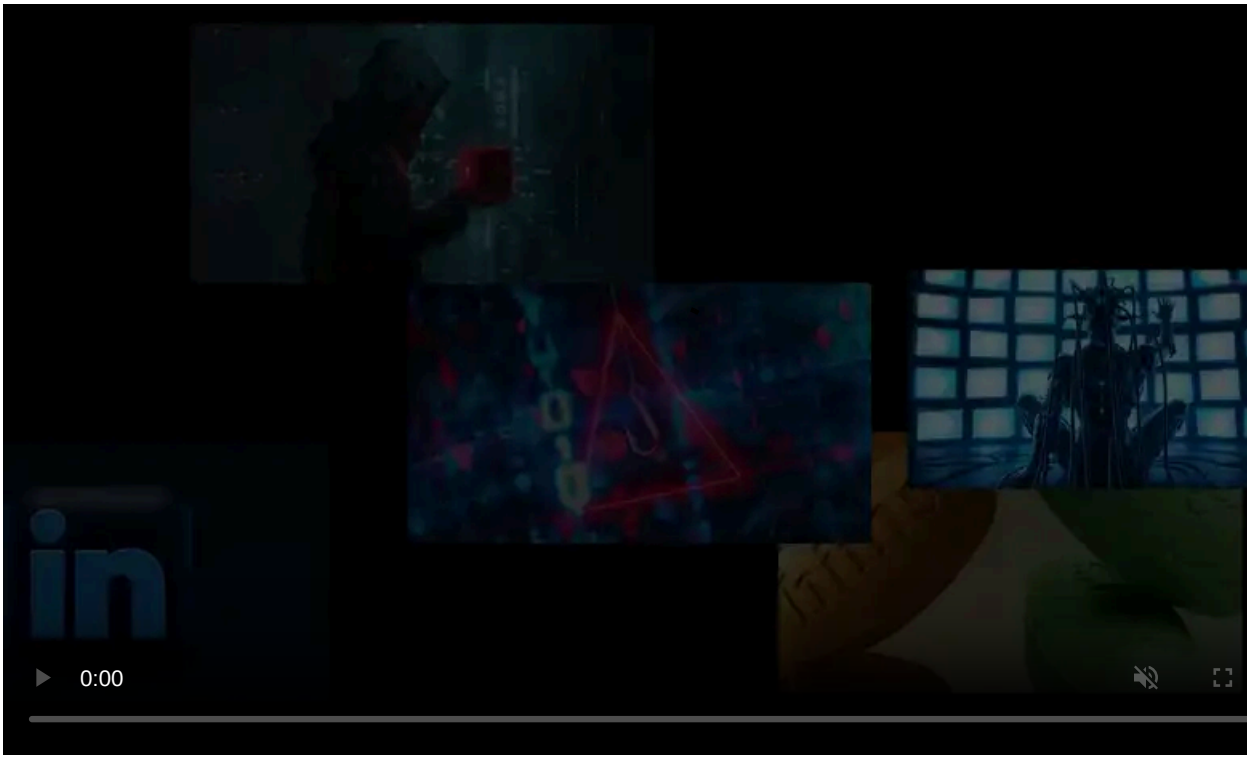
Published: 2017-03-29 · Archived: 2026-04-05 15:54:30 UTC

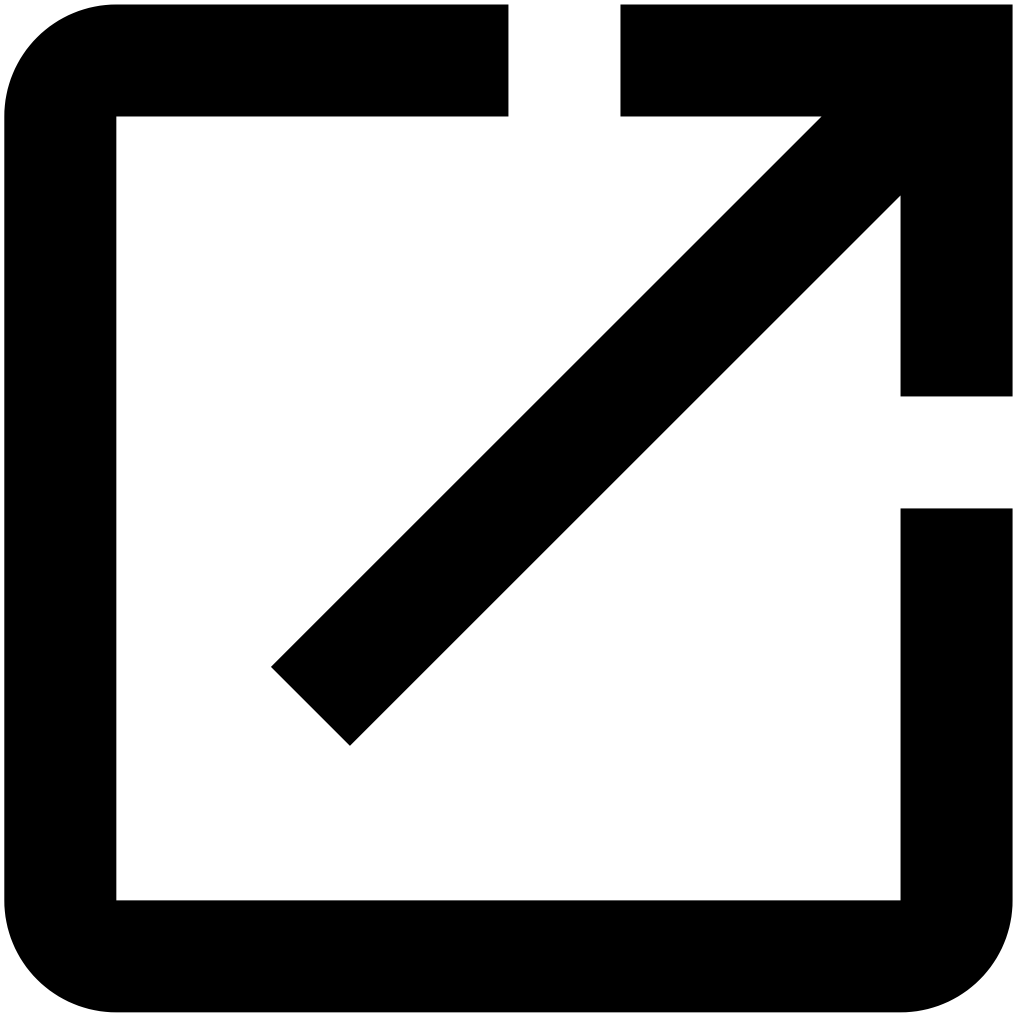
The US Department of Justice announced yesterday that Maxim Senakh, 41, of Velikii Novgorod, Russia, pleaded guilty for his role in the creation of the Ebury malware and for maintaining its infamous botnet.

US authorities indicted Senakh in January 2015, and the law enforcement detained the hacker in Finland in August of the same year.

Finland approved Senakh's extradition to the US in January 2016, but not without the classic rhetoric from Russian authorities who called the extradition process "legal abuse," and the practice of arresting Russian citizens abroad an "illegal practice" and "witch hunt."

After facing legal proceedings in the US, Senakh has now confessed to his role in the creation of the Ebury malware together with other unnamed co-conspirators.

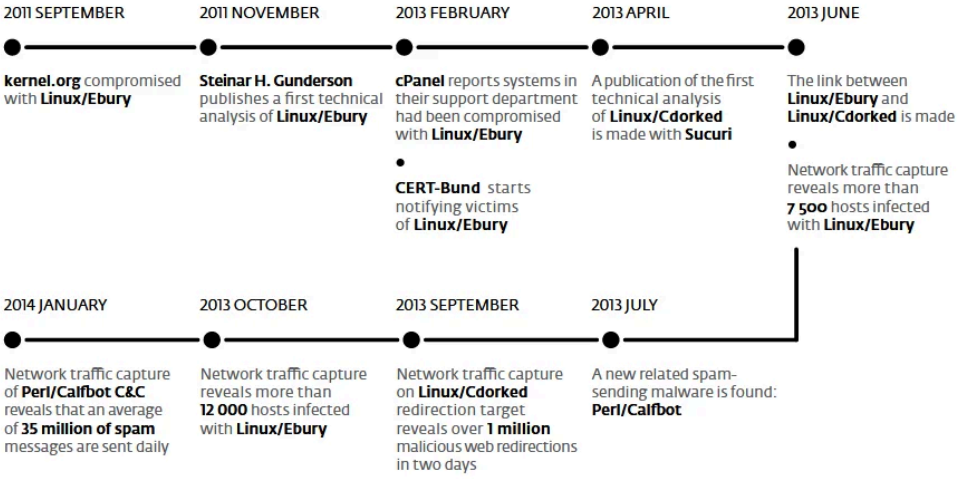

0:00



Ebury malware infected around 25,000 servers

The Ebury malware appeared on the malware scene in 2011, and only targeted UNIX-like operating systems like Linux, FreeBSD, and Solaris.

Crooks installed Ebury on servers left unprotected online. The malware contained a rootkit component to survive between reboots and a backdoor to provide criminals remote access. Hackers also used Ebury to steal SSH login credentials and SSH private keys, which they later used to infect new servers.



Ebury timeline (via ESET)

Crooks assembled servers infected with Ebury in a botnet they used to redirect traffic to paying customers or to send email spam, also for financial gain. During its peak, ESET estimated that Ebury infected 25,000 servers across the world.

Ebury's became famous in 2011 after a Florida man, with no connections to the Ebury crew, installed Ebury on kernel.org servers. In recent years, Ebury activity has died down following aggressive sinkholing, albeit the malware will still pop up in a honeypot once in a while.

Ebury was often used together with other malware such as CDorked, Onimiki, and Calfbot. Coverage of Ebury attacks and features can be found on the sites of Steinar H. Gunderson, ESET [1, 2], CERT-BUND, and Sucuri.

Senakh's sentencing is scheduled for August 3, 2017.
