Malware seen turning systems into proxies without consent

December 31 2015, by Nancy Owano

Credit: George Hodan/Public Domain

A cybersecurity company has spotted malware which sets up anonymous proxies on infected personal computers. Lee Mathews in *Geek.com* said the strain turns infected machines into anonymous proxy hosts.

Palo Alto Networks is the company that made the discovery. Jeff White posted the report, talking about the behavior of a recent sample.

"Anonymous proxies play an important role in protecting one's privacy while on the Internet; however, when unsuspecting individuals have their systems turned into proxies without their consent, it can create a dangerous situation."

He said this is actually a family of malware, designated as ProxyBack. Palo Alto Networks observed over 20 versions used to infect systems as far back as March 2014, said White. Most targets belong to educational institutions.

Obstacles that might normally derail proxy traffic such as software and hardware firewalls are no problem for ProxyBack. Why?

The malware is creating a reverse tunnel on a compromised system, said Mathews, which allows requests to pass through undetected. "Some of the more nefarious traffic originated from an automated system that was setting up bogus accounts on sites," he said.
(The problem for a non-legitimate proxy is that the network traffic destined to reach the proxy server, which is a compromised system, will usually not be able to reach it because of firewalls or other network based restrictions put in place to protect systems, said White.)

Softpedia described how the malware works—"by infecting a PC, establishing a connection with a proxy server controlled by the attackers, from where it receives instructions, and later the traffic it needs to route to actual Web servers." Each machine infected with ProxyBack works as a bot inside a larger network controlled by the attackers, who send commands and update instructions via simple HTTP requests, said *Softpedia*.

White wrote: "It was clear that there were legitimate, benign, users of the SOCKS proxy, along with malicious users as well, further adding weight to the conclusion that this is a proxy service." He said the legitimate

traffic included sites like eBay, Twitter, Craigslist, Wikipedia and more.

Palo Alto Networks, meanwhile, released the IPS signature 14864 to detect and block ProxyBack traffic. White said that WildFire properly classifies ProxyBack executables as malicious and AutoFocus users can track this threat using the ProxyBack tag.

Doug Bonderud in *Security Intelligence* commented: "Here's the takeaway when it comes to ProxyBack: Malware creators have moved beyond a smash-and-grab mentality to one that focuses on quietly infecting systems and then using them to further seemingly legitimate business aims. In other words, desktops are quickly becoming the newest cybercriminal currency as server potential—rather than stored data—becomes the big value-add for attackers."

More information: researchcenter.paloaltonetwork … ies-without-consent/