ESET Research: Ebury botnet alive & growing; 400k Linux servers compromised for cryptocurrency theft and financial gain

DUBAI , DUBAI, UNITED ARAB EMIRATES, May 17, 2024 /EINPresswire.com/ -- ESET Research released today its deep-dive investigation into one of the most advanced server-side malware campaigns, which is still growing and has seen hundreds of thousands of compromised servers in its at least 15-year-long operation. Among the activities of the infamous Ebury group and botnet over the years has been the spread of spam, web traffic redirections, and credential stealing. In recent years it has diversified to credit card and cryptocurrency theft. Additionally, Ebury has been deployed as a backdoor to compromise almost 400,000 Linux, FreeBSD, and OpenBSD servers; more than 100,000 were still compromised as of late 2023. In many cases, Ebury operators were able to gain full access to large servers of ISPs and well-known hosting providers.

Ten years ago, ESET published a white paper about Operation Windigo, which uses multiple malware families working in combination, with the Ebury malware family at its core. In late 2021, the Dutch National High Tech Crime Unit (NHTCU), part of the Netherlands national police, reached out to ESET regarding servers in the Netherlands suspected of being compromised with Ebury malware. Those suspicions turned out to be well-founded and with NHTCU's assistance, ESET Research has gained considerable visibility into operations run by the Ebury threat actors.

“Following the release of the Windigo paper in early 2014, one of the perpetrators was arrested at the Finland-Russia border in 2015, and later extradited to the United States. While initially claiming innocence, he eventually pleaded guilty to the charges in 2017, a few weeks before his trial at the U.S. District Court in Minneapolis was set to proceed, and where ESET researchers were scheduled to testify,” says Marc-Etienne M. Léveillé, the ESET researcher who investigated Ebury for more than a decade.

Ebury, active since at least 2009, is an OpenSSH backdoor and credential stealer. It is used to deploy additional malware to: monetize the botnet (such as modules for web traffic redirection), proxy traffic for spam, perform adversary-in-the-middle attacks (AitM), and host supporting malicious infrastructure. In AitM attacks, ESET has observed over 200 targets across more than 75 networks in 34 different countries between February 2022 and May 2023.

Its operators have used the Ebury botnet to steal cryptocurrency wallets, credentials, and credit card details. ESET has uncovered new malware families authored and deployed by the gang for financial gain, including Apache modules and a kernel module to perform web traffic redirection. Ebury operators also used zero-day vulnerabilities in administrator software to compromise servers in bulk.

After a system is compromised, a number of details are exfiltrated. Using the known passwords and keys obtained on that system, credentials are reused to try logging into related systems. Each new major version of Ebury introduces some important change and new features and obfuscation techniques.

“We have documented cases where the infrastructure of hosting providers was compromised by Ebury. In these cases, we have seen Ebury being deployed on servers rented out by those providers, with no warning to the lessees. This resulted in cases where the Ebury actors were able to compromise thousands of servers at once,” says Léveillé. There is no geographical boundary to Ebury; there are servers compromised with Ebury in almost all countries in the world. Whenever a hosting provider was compromised, it led to a vast number of compromised servers in the same data centers.

At the same time, no verticals appear more targeted than others. Victims include universities, small and large enterprises, internet service providers, cryptocurrency traders, Tor exit nodes, shared hosting providers, and dedicated server providers, to name a few.

In late 2019, the infrastructure of a large and popular US-based domain registrar and web hosting provider was compromised. In total, approximately 2,500 physical and 60,000 virtual servers were compromised by the attackers. A very large portion, if not all, of these servers are shared between multiple users to host the websites of more than 1.5 million accounts. In another incident, a total of 70,000 servers from that hosting provider were compromised by Ebury in 2023. Kernel.org, hosting the source code of the Linux kernel, had been a victim of Ebury too.

“Ebury poses a serious threat and a challenge to the Linux security community. There is no simple fix that would make Ebury ineffective, but a handful of mitigations can be applied to minimize its spread and impact. One thing to realize is that it doesn’t only happen to organizations or individuals that care less about security. A lot of very tech-savvy individuals and large organizations are among the list of victims,” concludes Léveillé.

For more technical information and a set of tools and indicators to help system administrators determine whether their systems are compromised by Ebury, read the full white paper “Ebury is alive but unseen: 400k Linux servers compromised for cryptocurrency theft and financial gain”.

Ebury deployments per month using two different scales on the Y axis, according to the database of compromised servers maintained by the perpetrators.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here
