Forkbombus
Threat Intelligence and Deception Technologies LABS

Forkbombus Labs Assists FBI in Click Fraud Botnet Disruption

August 7th, 2017 - FOR IMMEDIATE RELEASE

On August 4th, 2017, Fabio Gasperini, an Italian citizen, was found guilty by jury trial on one charge of Computer Intrusion for his involvement in the orchestration and propagation of a global botnet used to perform click fraud activity. Forkbombus Labs is proud to announce its pivotal role in the discovery and investigation of the botnet and click fraud activity.

“Forkbombus Labs is committed not only to providing immediate defenses, but to working with the global law enforcement community to enable and ensure long term remediation of cyber criminal activity. We take great pride in our role in the disruption and discontinuation of these malicious acts - as well as the identification and apprehension of the suspected parties.” said James Ward, CEO and Co-Founder of Forkbombus Labs.

The Click Fraud Botnet

On December 5th, 2014, Forkbombus Labs was alerted by its Hivemind technology to the existence of a new botnet being propagated by the Shellshock vulnerability (CVE-2014-6271[1]), specifically targeting QNAP NAS devices which were accessible on the public internet via TCP port 80. Analysis of these attacks revealed the ultimate motivation of perpetrating advertisement click fraud. In addition to the click fraud, the malicious code served several purposes, including but not limited to:

- Adding a backdoor administrator user account.
- Creation of a publicly accessible unauthenticated webshell.
- Configuring an SSH daemon on port 26.
- Patching the infected QNAP NAS Device for the Shellshock vulnerability, preventing further exploitation.
- Downloading and execution of a Lightaidra IRC Bot.
- Further (worm like) Botnet propagation.
- Visiting advertisements in a fraudulent manner meant to emulate legitimate human activity.

“Our researchers quickly identified long standing related activity and the motivation behind these attacks. This allowed our users to quickly identify the appropriate response for this activity and their needs. Through our combined efforts with the FBI, we were able to engage in root cause remediation of this activity, preventing millions of attacks from affecting our clients and the internet as a whole.” said Stu Gorton, Chief Science Officer and Co-Founder of Forkbombus Labs.

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271

Victim Resources

QNAP NAS Devices which were susceptible to the Shellshock Vulnerability[2], and accessible via port 80 to the public internet may be infected. Using our Hivemind technology, Forkbombus Labs has identified over 2,500 infected QNAP NAS devices in more than 70 countries. If you suspect you may be a victim of the aforementioned QNAP NAS Botnet, or other cyber criminal activity, please contact Forkbombus Labs at information@forkbomb.us.

Hivemind Intelligent Deception

Forkbombus Labs' Hivemind is the first intelligent deception technology to instantly react to and reconfigure for each individual actor, portraying itself as being valuable and vulnerable to what they will target. Hivemind draws attackers in and entices them into divulging high fidelity details of their campaigns. These details uncover assets, intentions, motivations, capabilities, and even the identities of attackers. Hivemind and its investigation platform automatically performs deep enrichment and cognitive analysis on observed events and indicators. This deep indicator enrichment allows the Hivemind platform to identify and relate activity, assets, and infrastructure used by actors even before they can be utilized against a network. HIVEMIND correlates discovered relations with other activity, new and old, tracking threats as they evolve. Hivemind's historical intelligence of attackers and associated offensives allow analysts to spearhead their investigations - promoting an understanding of why an attack occurred, and preventing false positives, alert numbness, and alert fatigue.

For more information and demonstrations of Hivemind, contact information@forkbomb.us.

[2] https://www.qnap.com/en/news/2014/qnap-releases-qfix-v1-0-2-to-fix-shellshock-for-non-qts-4-1-1-build-1003-users

The information in this article is provided as is and without warranty and does not represent professional advice or services. Forkbombus Labs is not responsible for any loss or damages from actions taken based on information within this publication.

Media Relations: press@forkbomb.us