Abstract
The infamous Mirai botnet was responsible for the top three DDoS attacks in 2016, against Brian Krebs, OVH and DynDNS. Taking over hundreds of thousands of Internet of Things (IoT) devices, it stunned the IT industry with traffic volumes exceeding 1Tbps. Since its source code became available via a hacker forum, it is only a matter of time until other cyber-delinquents customize it and create new variations to launch new cyber-attacks. Since its debut three months ago, Radware has already tracked improvements by hackers trying to expand Mirai's capabilities.

Background
IoT devices are vulnerable to enslavement because their operating systems are stripped down and are equipped with rudimentary security features. Mirai – as well as other botnets such as Lizkebab, BASHLITE, Torlus and Gafgyt - are all capable of launching massive DDoS attacks via common and known exploits found in devices like default credentials and failure-to-patch known vulnerabilities.

Since the code is widely available on both the clearnet and the darknet, several variants of this botnet have been introduced by different threat actors. The reason is the lack of security around the devices. These devices are rarely updated and feature default passwords which make them vulnerable to botherders. In addition, there are billions of devices available for enslaving. As DDoS-as-a-Service tools go mainstream in the darknet, a cheaper and more powerful option becomes available because IoT devices are not turned off, so attackers have availability at all times. These botnets are so large and powerful they do not need to rely on amplification. They are using sophisticated attack vectors that overwhelm server resources like TCP, GRE and Layer 7 floods.

IoT Bontet Services
New vendors and websites sell Mirai and other IoT botnets on the darknet or offer turnkey setup of the botnet. Some of the slots sell for as low as $50 while other Mirai-based slots with 100,000 infected devices sell for $7,500 (see Figure 1 below).

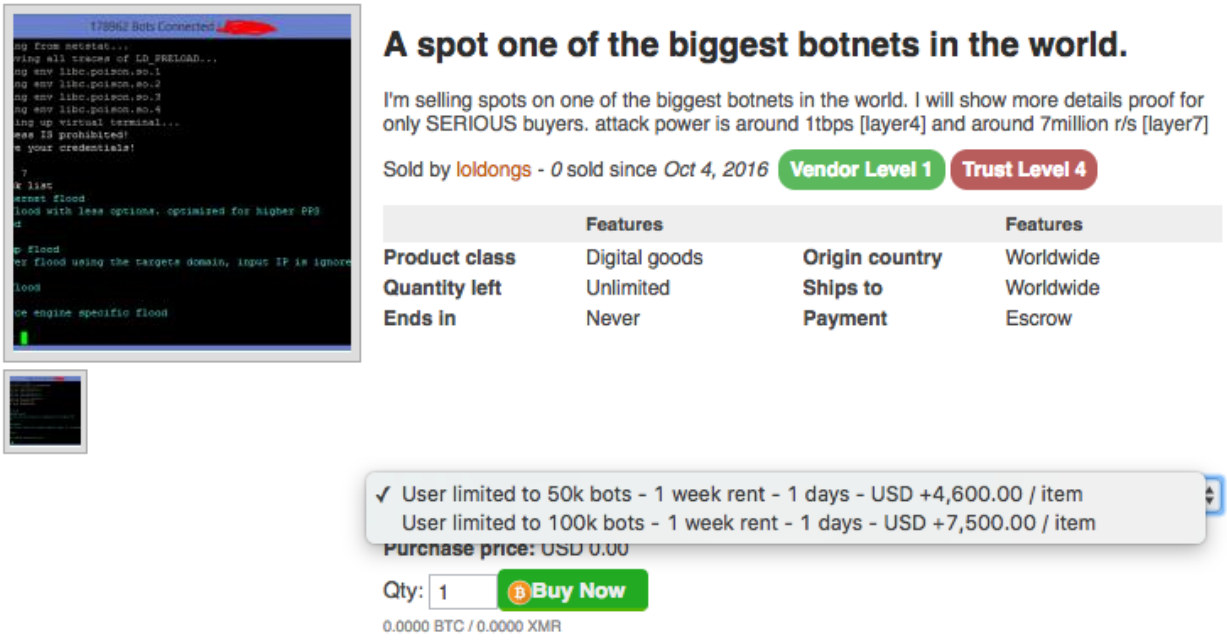

Figure 1: Mirai on AlphaBay

There are also several services that are willing to setup the Mirai botnet for somebody. Package prices for botnet setup range from $30 for a basic setup to $100 for a more advanced setup. The basic setup comes with two servers and 10x pre-infected bots while the advanced package comes with six VPSs and 500 pre-infected devices (see Figure 2 below).

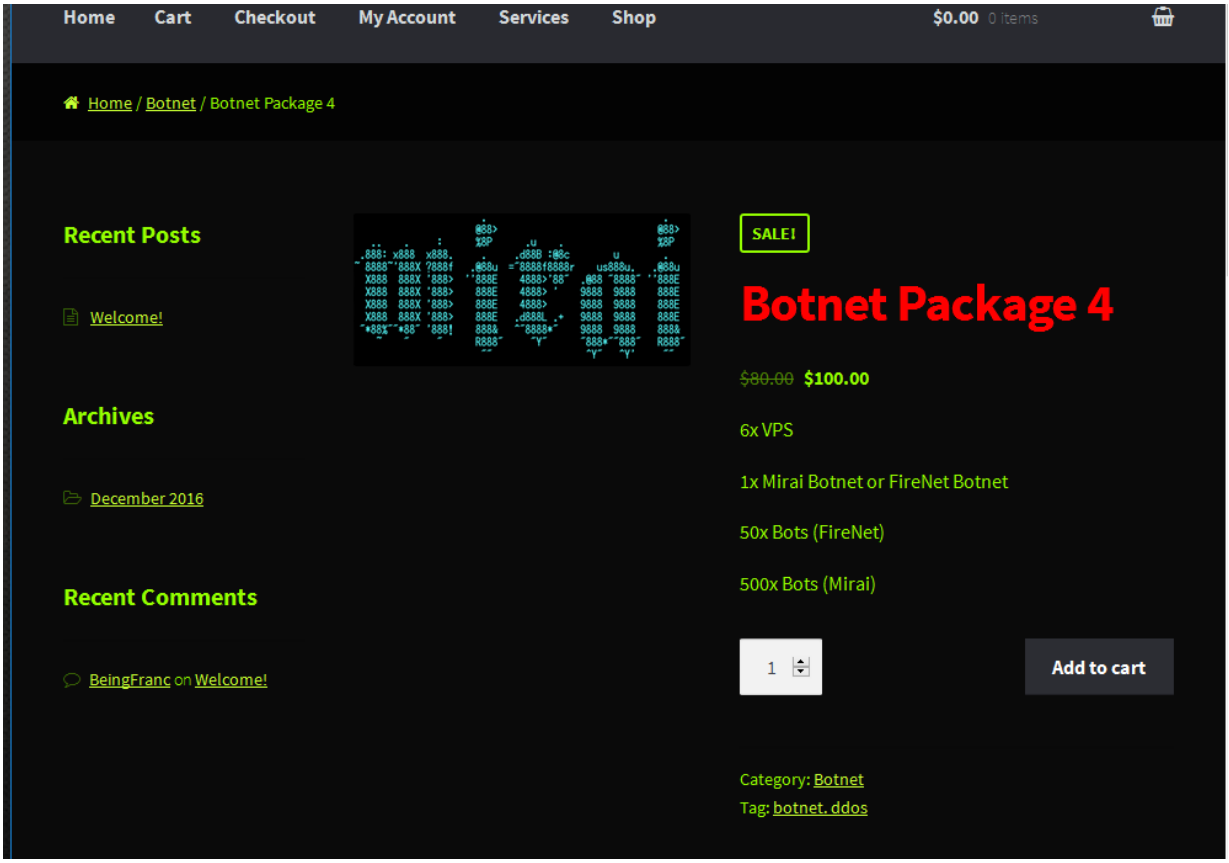

Figure 2: Mirai Setup Service

Bot herders have been seen using Mirai in combination with a new vulnerability in an attempt to enslave more devices for their DDoS-as-a-Service business. This attempt was most notably publicized with the recent outage at Deutsche Telekom, with an unsuccessful takeover ~900,000 routers. With a simple remote code execution (RCE), a hacker took advantage of a SOAP (an XML-based application communication protocol) vulnerability in DSL modems with port 7547 opened designed for communication with third parties. This remote code execution attack is exploiting a vulnerability found in the TR-069 configuration protocol in combination with the Mirai IoT botnet and has been seen in the wild in Germany, United Kingdom and Brazil.

Recent industry reports provide insight into what bot herders are now focusing on:

1. Sony IPELA IP cameras[i]. These types of devices (released March 2012) are being exploited by an OS level backdoor account with SSH/Telnet access. The backdoor password hash was identified as far back as October 2012 on a forum. These cameras have been vulnerable for 4 years.

Figure 3:
https://forum.insidepro.com/viewtopic.php?p=121234&sid=adf940d0ab3ffa770c09215ac9f6f2e1

2. Disabling software updates to hundreds of thousands of white label Internet cameras to keep them vulnerable to newly discovered authentication and web server command injection 0-day exploits. [ii]

3. A new strain of the Mirai botnet using a domain generator algorithm (DGA)[iii], improving its original code from hard-coded command-and-control domains to dynamically generated, daily rotating domains. As Mirai matures and its ecosystem of vulnerable devices is growing, we are witnessing a shift from Telnet's common ports 23 and 2323 to targeting additional ones such as 7547, 5555 (tr069).

Attack vectors

- UDP
- VSE
- DNS Water Torture
- SYN with options
- ACK + bypass
- GRE
- HTTP

What's Expected Next

IoT devices will continue to be hijacked at alarming rates and most likely used to carry out political activism or extortion attempts.

DDoS Protection Considerations for Organizations Under Threat

- **Hybrid DDoS Protection** – on premise and cloud-based solutions for real-time protection that also addresses high volume attacks and protects from pipe saturation.
- **Behavioral-Based Detection** - to quickly and accurately identify and block anomalies while allowing legitimate traffic through.
- **Real-Time Signature Creation** - to promptly protect from unknown threats and zero-day attacks.
- **Cyber-Security Emergency Response Plan** - that includes a dedicated emergency team of experts.

Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools, visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

---

[i] http://blog.sec-consult.com/2016/12/backdoor-in-sony-ipela-engine-ip-cameras.html

[ii] https://www.cybereason.com/zero-day-exploits-turn-hundreds-of-thousands-of-ip-cameras-into-iot-botnet-slaves/

[iii] http://blog.netlab.360.com/new-mirai-variant-with-dga/