Security Leftovers

By *Roy Schestowitz*
Created *30/09/2015 - 10:18am*
Submitted by Roy Schestowitz on Wednesday 30th of September 2015 10:18:43 AM Filed under Security [1]

- **Tuesday's security advisories [2]**

- **Security updates for Monday [3]**

- **Our First Certificate Is Now Live [4]**

  > Our cross signature is not yet in place, however this certificate is fully functional for clients with the ISRG root in their trust store. When we are cross signed, approximately a month from now, our certificates will work just about anywhere while our root propagates. We submitted initial applications to the root programs for Mozilla, Google, Microsoft, and Apple today.

- **Botnet preying on Linux computers delivers potent DDoS attacks [5] [Ed: Dan Goodin's FUD du jour focuses on cracking that guesses passwords (weak passwords), not back doors in proprietary software. Compare to Microsoft's back doors [6]]**

- **A Linux botnet is launching crippling DDoS attacks in excess of 150Gbps [7]**

- **Security firm discovers Linux botnet that hits with 150 Gbps DDoS attacks [8]**

Akamai announced on Tuesday that its Security Intelligence Response Team has discovered a massive Linux-based botnet that's reportedly capable of downing websites under a torrent of DDoS traffic exceeding 150 Gbps. The botnet spreads via a Trojan variant dubbed XOR DDoS. This malware infects Linux systems via embedded devices like network routers then brute forces SSH access. Once the malware has Secure Shell credentials, it secretly downloads and installs the necessary botnet software, then connects the newly-infected computer to the rest of the hive.

- **Notes on Linux/Xor.DDoS [9]**
- **Linux botnet observed launching powerful DDoS attacks [10]**
- **XOR: Linux-based botnet pushing 20 attacks a day [11]**
- **Linux-powered botnet generates giant denial of service attacks [12]**
- **Akamai XOR DDoS warning [13]**
- **XOR DDoS Botnet Launching 20 Attacks a Day From Compromised Linux Machines, Says Akamai [14]**
- **Linux-powered botnet lets rip on victims with 180Gbps network floods [15]**
- **XOR DDoS Botnet Uses Compromised Linux Machines to Launch 150+ Gbps Attacks [16]**
- **XOR DDoS Attack Tool Being Used to Launch Over 20 Daily Attacks [17]**
-

XOR DDoS Botnet Launches 20 Attacks Per Day via Linux **[18]**

- **Akamai detail powerful botnet cyber security threat** **[19]**

- **Gigantic botnet attacks 20 websites per day ? consists of Linux computers** **[20]**

- **A New Botnet Hits Servers With 150 Gbps DDoS Attacks** **[21]**

Security

Source URL: http://www.tuxmachines.org/node/80494

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] http://lwn.net/Articles/658713/rss
[3] http://lwn.net/Articles/658592/rss
[4] https://letsencrypt.org/2015/09/14/our-first-cert.html
[5] http://arstechnica.com/security/2015/09/botnet-preying-on-linux-computers-delivers-potent-ddos-attacks/
[6] http://techrights.org/wiki/index.php/Microsoft_and_the_NSA
[7] http://www.pcworld.com/article/2987580/security/a-linux-botnet-is-launching-crippling-ddos-attacks-at-more-than-150gbps.html
[8] http://www.engadget.com/2015/09/29/linux-botnet-hits-with-150-gbps-ddos/
[9] http://bartblaze.blogspot.com/2015/09/notes-on-linuxxorddos.html
[10] http://www.scmagazine.com/linux-botnet-observed-launching-powerful-ddos-attacks/article/441750/
[11] http://www.csoonline.com/article/2986869/vulnerabilities/xor-linux-based-botnet-pushing-20-attacks-a-day.html
[12] http://www.zdnet.com/article/linux-powered-botnet-generates-giant-denial-of-service-attacks/
[13] http://isurfpaducah.com/2015/09/30/akamai-xor-ddos-warning16449/
[14] http://www.itbusinessnet.com/article/XOR-DDoS-Botnet-Launching-20-Attacks-a-Day-From-Compromised-Linux-Machines-Says-Akamai-4090211
[15] http://www.theregister.co.uk/2015/09/29/linux_xor_ddos_botnet/
[16] http://news.softpedia.com/news/xor-ddos-botnet-uses-compromised-linux-machines-to-launch-150-plus-gbps-attacks-493139.shtml
[17] https://securityintelligence.com/news/xor-ddos-attack-tool-being-used-to-launch-over-20-daily-attacks/
[18] http://www.infosecurity-magazine.com/news/xor-ddos-botnet-20-attacks-per-day/
[19] http://www.cbronline.com/news/cybersecurity/business/akamai-detail-powerful-botnet-cyber-security-threat-4681768
[20] http://www.myce.com/news/gigantic-botnet-attacks-20-websites-per-day-consists-of-linux-computers-77421/
[21] http://gizmodo.com/a-new-botnet-hits-servers-with-150-gbps-ddos-attacks-1733743786