Abstract

Anonymous has initiated the third and final phase of OpIcarus: "Project Mayhem" – a systematic cyber-assault against worldwide stock exchanges. The global hacktivist group opened its attacks with a takedown of the London Stock Exchange website on June 5, 2016 (see Figure 1).

OpIcarus initially started in February with limited success. Following this subpar launch, the attackers then returned, better organized and better prepared via new cyber-attack tools, and launched Phase 2: a 30-day campaign during which network outages were caused at dozens of sites worldwide, including the Bank of Greece, the Bank of Jordan and the Bank of South Korea (see Figure 2).

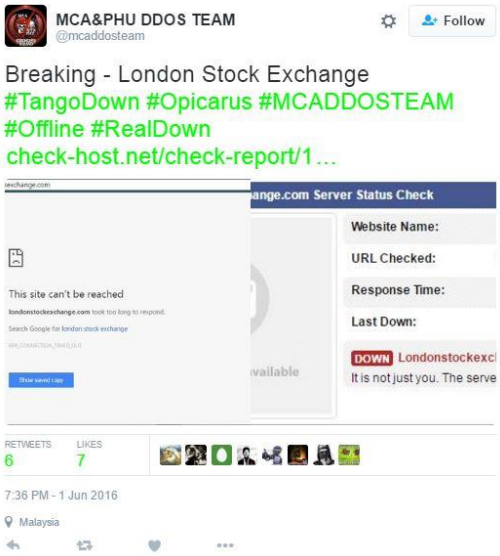

Figure 1: London Stock Exchange website down

Figure 2: Sites targeted during the 2nd phase of OpIcarus

For the third phase, Anonymous has designated all stock exchanges listed on this site as potential targets.

Attack Tools

- **TorsHammer** – A slow-rate HTTP POST (Layer 7) DoS tool that transmits HTML POST fields in slow rates under the same session, thus causing the web server application threads to await the

end of boundless posts until they are exhausted. The new version features a native socks proxy that enables the attack to be launched from random source IP addresses.

- **SlowLoris** - Opening multiple connections sending a partial request, holding them open. Then adding HTTP headers but never completing the request
- **PyLoris** - Enables the attacker to craft its own HTTP request headers (packet header, cookies, packet size, timeout and CRLF) to keep TCP connections open for as long as possible between the attacker and the victims' servers.
- **Slowhttptest** - sends incomplete HTTP requests at a very low transfer rate, keeping server resources waiting (see Figure 3).
- **Xerxes** - an extremely efficient DDoS attack automation tool that provides the capacity to launch multiple independent attacks against several target sites without necessarily requiring a botnet.
- **Ufonet** – This tool leverages 'Open Redirect' vectors on third-party web applications to cause a denial-of-service state.
- **GoldenEye** – Another Layer 7 DoS tool that keeps connections open until the destination server crashes. It features cache control options.

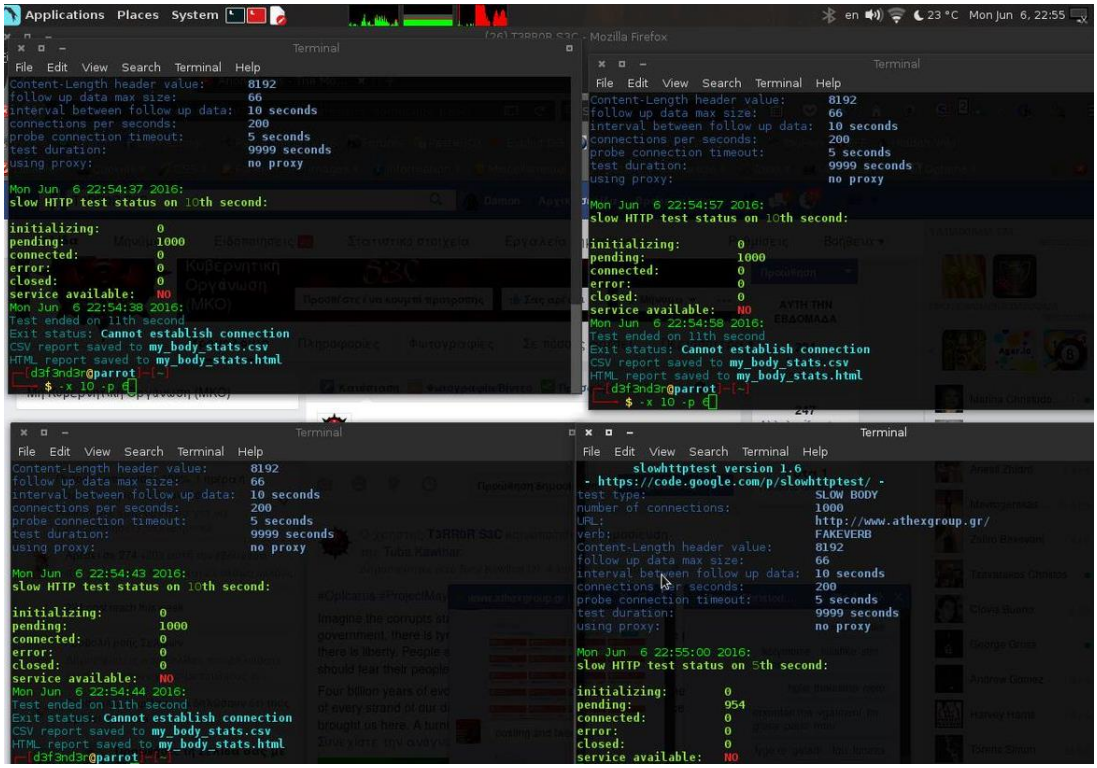

Figure 3: Attackers use ParrotOS plus slowhttptest to launch an attack.

Organizations Under Threat Should Consider

- A security solution that can protect its infrastructure from multi-vector attacks, including protection from network and application-based DDoS attacks as well as volumetric attacks that can saturate the Internet pipe

- A hybrid solution that includes on-premise detection and mitigation with cloud-based protection for volumetric attacks. This provides quick detection, immediate mitigation and protects networks from volumetric attacks that aim to saturate the Internet pipe.
- A solution that provides protection against sophisticated web-based attacks and website intrusions to prevent defacement and information theft.
- A cyber security emergency response plan that includes an emergency response team and process in place. Identify areas where help is needed from a third party.
- Monitor security alerts and examine triggers carefully. Tune existing policies and protections to prevent false positives and allow identification of real threats if and when they occur.

In addition to Radware products, we recommend that you review your network and patch your system accordingly. Maintaining and inspecting your network is necessary in order to defend against these types of 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.