National Cybersecurity and Communications Integration Center

**06 May 2013**

# OpUSA: Potential Tools

***DISCLAIMER:*** *This advisory is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this advisory or otherwise. Further dissemination of this advisory is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.*

## *Executive Summary*

Multiple groups, and individual hacker handles have claimed their intent to attack U.S. websites as part of OpUSA. As seen in many hacktivist operations (Ops), willing participants have posted free tools to assist other like minded individuals in their attack efforts. Often, more coordinated attacks will name a specific tool, target, day and time for the attack. That has not been the case for OpUSA thus far. Individual hacker groups seem to be conducting attacks independently, each claiming responsibility for individual defacements and data breaches that have supposedly recently taken place. Below you will find some of the tools being posted in conversations about OpUSA and links to US-CERT sites which provide background on the vulnerabilities exploited by these tools as well as mitigation advice for computer network defense actions.

## *Structured Query Language (SQL) injection*

The following is a sampling of tools being offered to willing members interested in using SQL attacks during OpUSA.

- **Havij:** Automates SQL Injection attacks. It allows the attacker to 'fingerprint' the database, retrieve Database Management System users and password hashes, dump tables and columns, retrieve specific data from the database, run SQL statements, and access the underlying file system and execute commands on the operating system.
- **SQL Poison:** This exploit scanner tool incorporates automated Google Dorking methods to look for SQL vulnerabilities. Once the vulnerability is discovered, it performs an SQL injection attack.

**The following US-CERT advisories offer further information:**

- US-CERT SQL Injection: http://www.us-cert.gov/security-publications/sql-injection
- US-CERT Securing Your Web Browser: http://www.us-cert.gov/publications/securing-your-web-browser

## *Distributed Denial of Service (DDoS)*

DDoS tools are often used by hacktivist so users may voluntary botnets. These are a list of the available DDoS tools via Open Source:

- **Low Orbit Ion Cannon (LOIC):** Floods servers with TCP or UDP packets with the intention of disrupting service.
- **High Orbit Ion Cannon (HOIC):** Can attack as many as 256 sites simultaneously and can target subdirectories of the main page using "booster packs" that enable traffic with multiple user-agent strings, referrers, and headers.

- **HTTP Unbearable Load King (HULK):** Also referred to as HULK DDoSser. Generates unique requests for each and every request generated, which bypasses caching engines and impacting the server's load directly.[1]
- **Slowloris:** Attempts to keep multiple open connections to the target web server and keep them open as long as possible.
- **DDos Notepad**: Attackers can create a simple Batchfile DDoS echo script using Notepad.
- **ByteDOS:** Windows desktop DOS application that is a standalone executable file and doesn't require any special installation on the attacking machine. It is equipped with embedded IP resolver capabilities that allow the tool to resolve IPs from domain names. It also supports SYN Flood and ICMP flood.
- **Turbinas:** Also referred to as VOLKS TURBINAS.EXE, which are associated with Cloaked Malware group designed to evade security detection systems.[2]
- **Syn Flood DOS:** Attack in which the actor sends a number of consecutive SYN requests to a target attempting to consume server resources.
- **Jays Booter:** A customized shell booter, which can be instructed to attack a specific IP for a period of time in an attempt to boot the target off of the internet. There are three types of shells: POST, GET, and SLOWORIS.
- **HTTPFlooder:** Program that attempts to flood the HTTP layer through GET and POST requests.
- **TORSHAMMER:** A Slow POST DOS tool written in Python. It can be run through the TOR network, which will anonymize the attacker. It can impact unprotected web-servers running Apache and IIS.[3]
- **R.U.D.Y:** Also known as R-U-Dead-Yet. This is an HTTP POST DOS attack that allows the attacker to choose the forms and form fields that they want to use for the POST attack.[4]
- **OWASP HTTP Tool:** A Slow POST DOS tool that allows the attacker to generate a customized number of connections, connection rate, timeouts, and even the content length. [5]
- **Anonymous DOSer:** A customized DOS tool put together in visual basic. It is very simple to use and can be used for HTTP floods or UDP floods.
- **Windows_DNS_Attack_Tool:** DNS Amplification tool. It uses open DNS resolvers and source address spoofing to create large denial of service attacks.
- **Goodbye:** Similar to HTTPFlooder and R-U-Dead-Yet DDoS tools.

**The following US-CERT advisories offer further information:**

- US-CERT Anonymous DDoS Activity: http://www.us-cert.gov/ncas/alerts/TA12-024A
- US-CERT Understanding Denial-of-Service-Attacks: http://www.us-cert.gov/ncas/tips/ST04-015
- US-CERT DNS Amplification Attacks: http://www.us-cert.gov/ncas/alerts/TA13-088A

## *Password Crackers/Stealers*

Several password crackers and stealers were spotted on related forums. Some of which are found below:

- **Backtrack 5: A** Linux based penetration testing tool. The most recent edition was synced up with the new release of KaliLinux. This toolkit provides easy-to-use tools such as port scanners, metasploit, Nmap, Browser Exploitation Framework, Hydra, Aircrack-ng, and Ophcrack. Aircrack and Ophcrack are password crackers.
- **Hash Cracker:** Refers to multiple free applications designed to crack MD2, MD5, SHA-1, SHA-256, SHA384, and SHA-512 using bruteforce techniques or using a rainbow table/dictionary attacks.

- **CpanelBruteReiluke:** Bruteforce password cracking tool designed by a developer known as Reiluke. Reiluke also has made his blind SQL, email brute force, and exploit scanner tools available via open source.
- **Gmail_Hacker:** Labeled as a free Gmail-specific password cracking tool which is advertised as taking less than 2 minutes to retrieve passwords.
- **Firefox Password Stealer:** Provides details on how an attacker can turn their Firefox browser into a password stealer. This is not a tool, but rather direction for end users.[6]
- **ICQ Steal0r:** Program seems to be dedicated to stealing passwords of ICQ users. ICQ is an instant messaging application popularized by Mirabilis.

**The following US-CERT advisories offer further information:**

- US-CERT Password Management: https://www.us-cert.gov/sites/default/files/publications/PasswordMgmt2012.pdf

## *Proxy Servers/Anonymizers*

In additional to options like the onion router (TOR), OpUSA members have advertised the following to assist actors in obfuscating their activity.

- **CYBERGHOST:** A Virtual Private Network (VPN) simulator which sets up a proxy server allowing anonymous activity with 128-bit AES encryption. It also has the most server locations available in the US and a number of countries in Europe.
- **TunnelBear:** This VPN simulator also circumvents Geoblocking, which is geographically blocking internet users from certain web services.[7]
- **SumRando:** This VPN simulator allows users to generate random IP addresses, which can obfuscate attribution.
- **Real Hide IP:** Hides the IP address of anyone employing the application.
- **Hotspot Shield:** Hides the IP address of anyone employing the application.

## *Other Tools Mentioned*

Hacker groups have mentioned the following tools among several others that don't fit the above categories.

- **Net Tools:** This could refer to any number of items, but c|net offers a network toolbox that has network sniffing and scanning tools.
- **Pack Del Hacker:** This is a simplified, online-based file-sharing service.
- **EmailScraperWizardv06b:** This is noted as one of the more successful email scrapers on the internet. It can extract email addresses from websites.
- **IP Port Scanner:** This could refer to multiple tools dedicated to scanning, mapping and discovering open ports.
- **IP Scanner:** These types of tools can scan networks, detect devices, wireless devices, routers, and can find HTTP, HTTPS, and FTP folders.
- **DHCP_IP_Forcer:** This allows an attacker to essentially scan a network and detect IP addresses and MAC addresses on a network. Some DHCP Force components allow the attacker to reconfigure modems.

## Summary

While it is difficult to assess the specific tools that may be used against targeted organizations, this product is intended to provide organizations with an idea of the type of free tools that may be employed against them, so they may better prepare mitigation strategies during OpUSA or similar hacktivist operations.  As always, NCCIC reminds users and administrators of the importance of best practices to strengthen the security posture of their organization's systems. Critical Infrastructure Key Resource (CIKR) owners and operators should work toward a resilient network model that assumes such an attack will occur against their enterprise. The goal is to minimize damage, and provide pathways for restoration of critical business functions in the shortest amount of time possible.

## Points of Contact

For all inquiries pertaining to this product, please contact the NCCIC Duty Officer at NCCIC@hq.dhs.gov or 1(800) 282-0870. NCCIC Watch & Warning and Analysis can be contacted at NCCIC_WatchandWarning@hq.dhs.gov.

## Can I share this product?

- Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

## References

[1] http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CC4QFjAA&url=http%3A%2F%2Fwww.sectorix.com%2F2012%2F05%2F17%2Fhulk-web-server-dos-tool%2F&ei=Fd2HUaH6MYPS9AS734GIDQ&usg=AFQjCNGeKinhk9P1JUToNeltsoS5ZkOhzw&sig2=UDG5gLtbCFl_5khc30iZxQ&bvm=bv.45960087,d.eWU
[2] http://www.prevx.com/filenames/X2439093139683158502-X1/VOLKS+TURBINAS.EXE.html
[3] http://franx47.wordpress.com/2013/02/04/using-torshammer-as-a-dos-denial-of-service-tool/
[4] http://code.google.com/p/r-u-dead-yet/
[5] https://www.owasp.org/index.php/OWASP_HTTP_Post_Tool
[6] http://www.hackersthirst.com/2011/01/turn-firefox-into-password-stealer.html
[7] http://www.pcworld.com/article/260236/tunnelbear_vpn_circumvents_geoblocking.html