SOLUTIONARY®
Relevant | Intelligent | Security

Q2 2013

SERT Quarterly Research Report

Table of Contents

Introduction

This SERT Quarterly Threat Report contains research conducted and highlights the results of analysis performed during the second quarter of 2013 (Q2). The Solutionary Security Engineering Research Team (SERT) focused on several emerging hacktivist campaigns during the quarter. SERT continually performs analysis and intelligence gathering operations to determine if Solutionary clients are targeted and to maintain awareness of the tools and techniques used by hacktivist groups and other malicious attackers, ensuring that SERT maintains constant vigilance.

Quarterly Highlights

- 73% of sites compromised during OpUSA were hosted on Microsoft IIS Web servers
- 17% of the compromised OpUSA targets hosted on Microsoft IIS platforms are running IIS versions 5.0 and 5.1 which are over 10 years old and no longer supported by Microsoft
- 68% of sites compromised by OpUSA attacks were hosted outside of the United States
- Increased malicious DNS request traffic was observed originating from global sources
- NSA PRISM heightens concerns on privacy and data access by the United States Government

Threat Landscape During Q2

Overview

Solutionary SERT focused analysis on hacktivist campaigns that targeted the financial and government sectors during the second quarter. To determine how and why these systems were targeted, SERT researched the techniques used during the attacks and compromises.

Hacktivist Activities

SERT closely monitored events associated with the OpUSA campaign. This planned hacktivist campaign targeted U.S. organizations, including the retail, financial and government sectors. From the first announcement of the OpUSA campaign, support from several hacktivist groups grew rapidly in social media circles. Soon after the campaign was announced, hacktivist groups associated with previous Distributed Denial of Service (DDoS) attacks against financial organizations and the defacement of state and local government websites also announced support of the OpUSA campaign. The motivation behind this attack campaign was claimed to be retaliation for war crimes committed during United States military campaigns in Iraq, Afghanistan and Pakistan. The groups claiming involvement in OpUSA leveraged the following attack techniques:

- SQL Injection
- Cross-Site Scripting (XSS)
- Distributed Denial of Service (DDoS)

While tracking events associated with OpUSA, SERT became aware that hacktivist groups involved in the campaign had actually begun their attacks earlier than the announced launch date of May 7, 2013. SERT discovered evidence of several sites that had been defaced as preliminary “warm-up” compromises for OpUSA.

It appears many of the OpUSA targets were hosted on external hosting providers. Several of the domains targeted and compromised were using vulnerable versions of OpenSSL mod_auth_passthrough and FrontPage extensions. FrontPage extensions have been utilized for many years because of their increased functionality and usability when constructing and deploying websites and have been a popular target of malicious attackers for remotely compromising vulnerable systems. Sites may have been targeted because of their configuration and country affiliation, which may coincide with the OpUSA objective.

The sites that were defaced were predominantly running the following configurations or features:

- Apache 2.2.21 to Apache 2.2.24 (Unix)
- OpenSSL 0.9.8e to OpenSSL 1.0.0
- Mod_auth_passthrough 2.1
- Mod_bwlimited 1.4
- FrontPage/5.0.2.263

On May 7, 2013, Solutionary did not detect, nor receive reports of clients experiencing DDoS attacks usually associated with these types of campaigns. Solutionary has not received any reports to validate that any such targeted attacks took place before, during or after the May 7, 2013 launch date. However, several hundred defaced domains were discovered in posts on or after May 7, 2013 — all of which were associated with OpUSA.

All the domains listed in posts by the hacktivists were defaced with custom graphics stating the hacktivists' message. A majority of the defacements did not follow the conventional methodology of modifying the sites main or index page, but rather a new page was added to the website to promote the hacktivists' message. Some examples of the defacement content are provided in Figure 1[*†].

Based on the apparent scaling back of hacktivist attacks for the OpUSA event, it appears that hacktivists had a genuine interest in conducting a concerted graffiti campaign designed to spread their message and attempt to raise awareness of what they view as injustices. The number of websites compromised was significant, but the overall harm to those systems has, so far, appeared to be relatively low given the level of access that the attackers were able to obtain. However, Solutionary cautions that the true nature of these attacks cannot be verified at this time, so organizations should be aware that the OpUSA event could have been used to gather additional system information and stage future attacks,

Figure 1

[*] http://blog.radware.com/security/2013/04/cyber-attack-against-u-s-based-websites-on-may-7th/
[†] http://blogs.cisco.com/security/the-effects-of-opusa/

The compromised servers hosting the defaced domains targeted in OpUSA are greatly dispersed among many geographic regions as depicted in Figure 2.

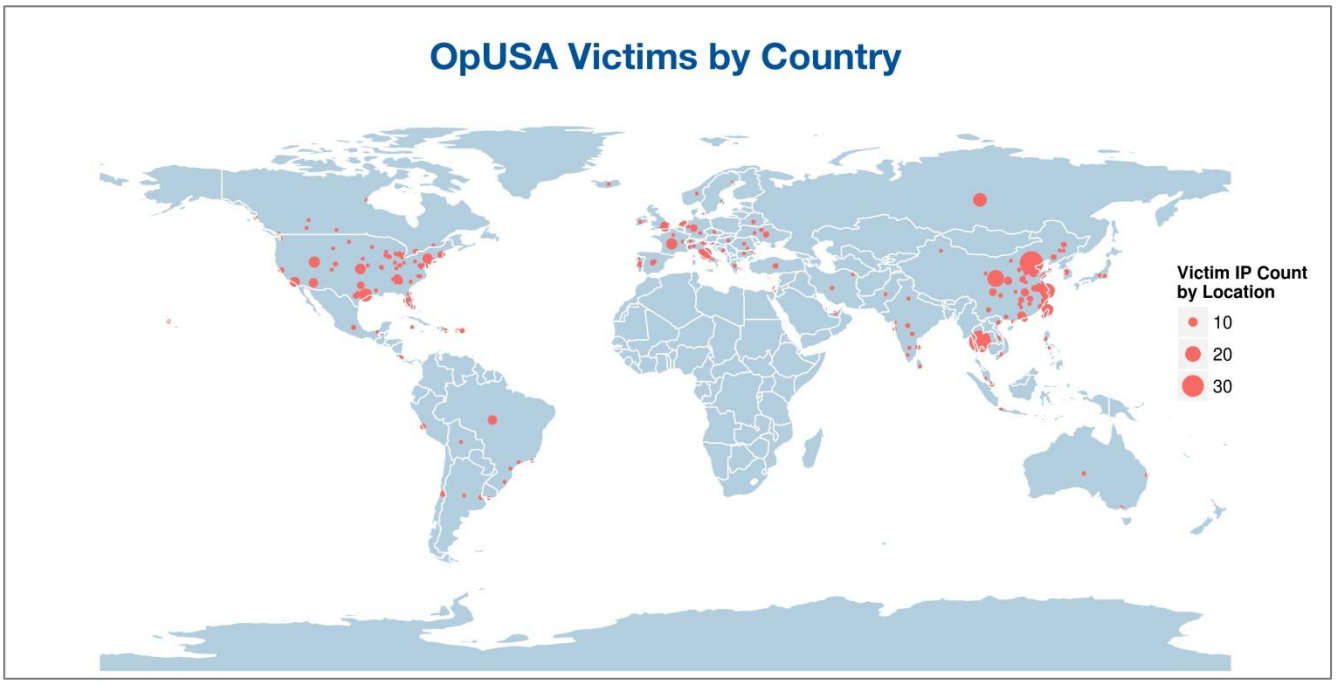

Figure 2

Figure 3 represents the total distribution hosted in other countries in relation to those in the U.S.

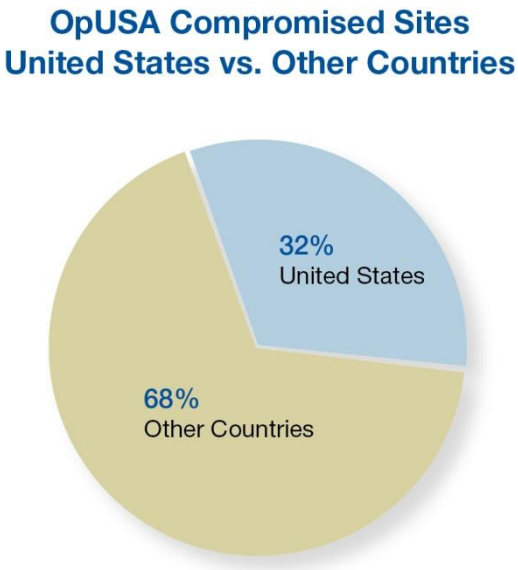

Figure 3

As seen in Figures 3 and 4, the country with the largest number of affected servers by country was the United States. The counts associated with each country are representative of the total number of websites defaced as reported by the hacktivist groups in Pastebin posts by the groups during the attack. All of these servers share a common theme —hosting providers maintain the majority of the compromised servers.

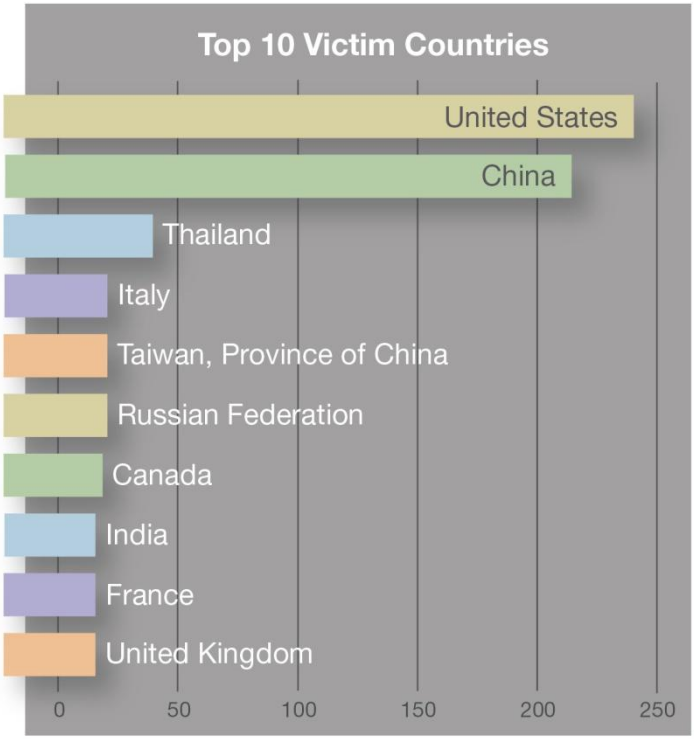

Figure 4

The distribution of attacks against sites hosted on Microsoft IIS and Apache are illustrated in Figure 5.a. Deeper dives into specific versions of the platforms are explored in Figures 5.b and 5.c.

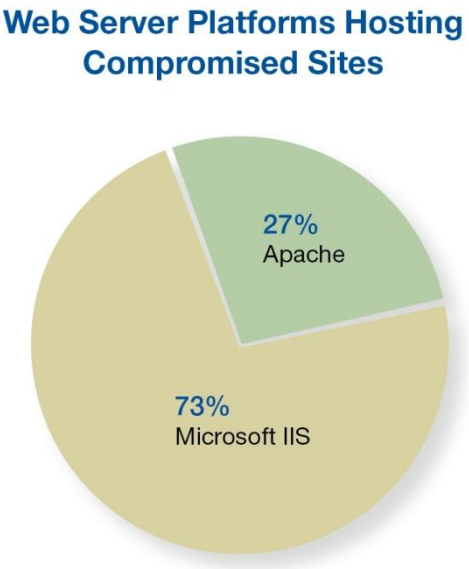

Figure 5.a

As illustrated in Figure 5.b, a significant number of the targets were hosted on older versions of the Microsoft IIS Web server. Some of these included versions that are over 10 years old and are no longer supported by the vendor with security patches or updates. Microsoft IIS 5.1 was distributed with Microsoft Windows XP Professional following IIS 5.0, which was distributed with Microsoft Windows 2000. Furthermore, IIS 6.0 is included with Windows Server 2003, which was removed from Mainstream Support in July 2010 transitioning to extended support, which is planned to end in 2015.

It is important to note the large percentage of compromised sites running old and unsupported operating systems. These systems are often more vulnerable than newer systems because they are no longer patched or updated leaving many security vulnerabilities available for exploitation.

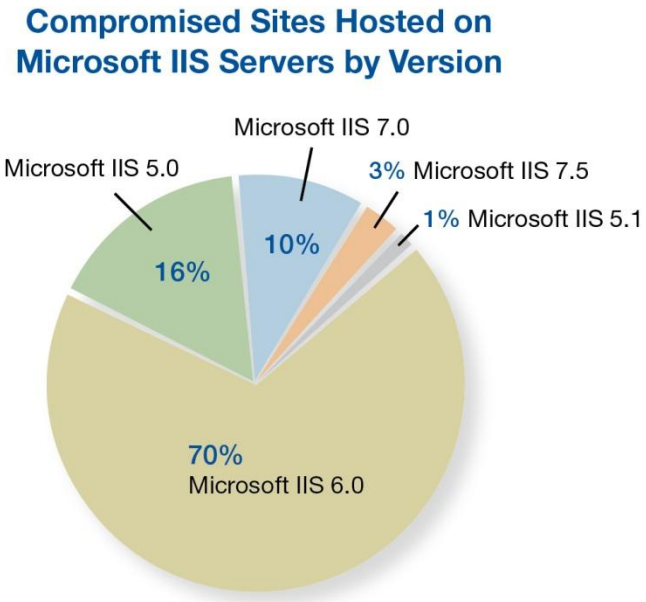

Figure 5.b

Additional servers most often observed in the list of compromised sites were versions of Apache 2.X.X as shown in Figure 5.c below.

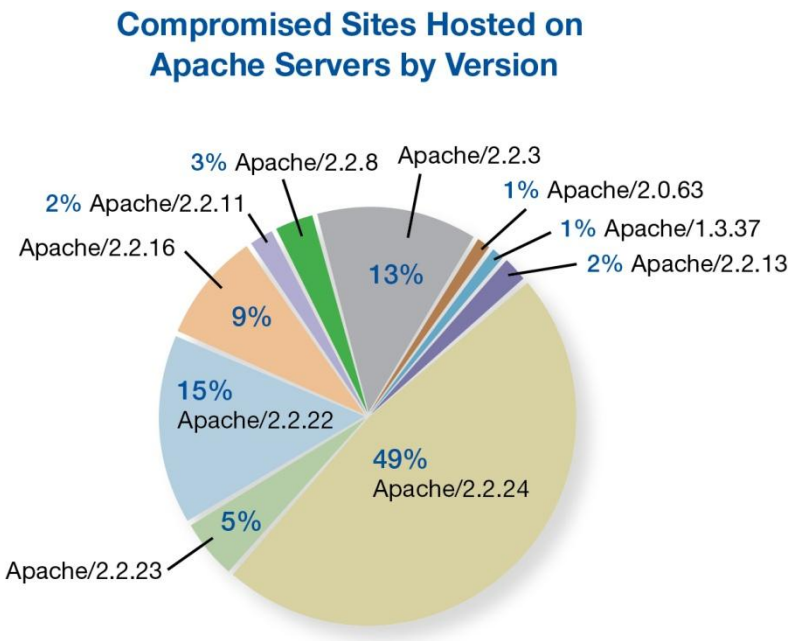

Figure 5.c

It is important to remember that with the level of access gained, attackers could have used these systems to expand an existing botnet or deploy exploit kits, using the compromised sites as landing pages containing additional malicious code used for phishing attacks. Attacks of this nature can also be used in preparation for a future hacktivist campaigns making use of successful compromises from earlier campaigns – effectively making this more of a "staging" attack. It is still unknown if the underlying reason for these attacks was anything other than the primary motivation that was publicly announced by the hacktivists involved.

DNS Request and Denial of Service Activities

During the last part of the quarter, SERT detected a dramatic increase in DNS request traffic originating from sources all around the world. At the time this report was written, the United States and China were the top two originating countries as depicted in Figure 6.

Figure 6

The top requested resource records observed with the recursion flag set are depicted in Figure 7.

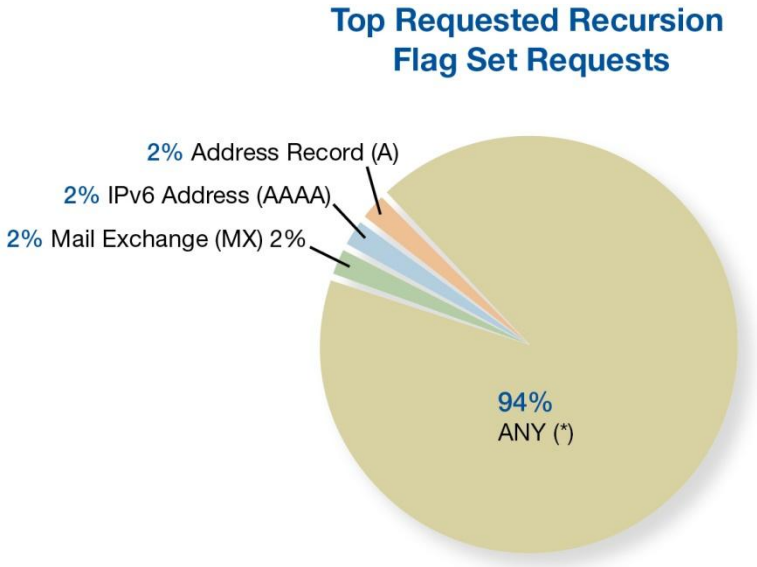

Figure 7

For a majority of the ISP or business provider networks identified, almost all of the domestic sources were private or commercial hosting providers. Based on the aforementioned information it appears the identified systems are performing reconnaissance in search of open DNS servers, specifically servers that are recursively responding to all queries. During a harvesting campaign, "Any" and "TXT" records are usually requested, but the methodology varies from attacker to attacker.

The information gathered during the reconnaissance could be used in DNS Amplification Attacks to create a Denial of Service (DoS) against a specific target. By sending domain specific queries, the attacker can cause DNS to become part of, or amplify the effect of, a wider DDoS attack on a particular target. Solutionary has no indication this broader attack has yet taken place, but given the high volume of DNS traffic during the last quarter; it would not be surprising to see this threat escalate in the near future.

NSA's PRISM Project Exposed

News of the National Security Agency's (NSA) PRISM project dominated early June. Since the United Kingdom publication *The Guardian* first broke the story, reaction among security professionals, industry and the public has been mixed. An NSA statement claims, in part, that PRISM collects data directly from the servers of the following U.S. service providers: Microsoft, Yahoo!, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple.

For the most part, the organizations listed vigorously deny supporting NSA intelligence gathering with direct, ongoing access to organizational systems. At the same time, these organizations have acted in response to formal legal requests, based on subpoenas and warrants, when they have been presented by law enforcement.

Solutionary has seen indications of skepticism on the part of non-U.S. companies, and some non-US companies have been outspoken about their wishes for a lack of interference by the United States Government. At this time, Solutionary has not seen indications that any organizations have been breached as part of, or in retaliation for, the PRISM data collection program.

Given that PRISM is a classified NSA project, news is still developing about the effectiveness of the project, and any details about how and what information was actually collected. Solutionary will continue to monitor developments, and currently expects that PRISM will have limited impact on client operations.

Recommendations

With the vast diversity of cyber threats that organizations face each day Solutionary diligently provides clients with actionable intelligence through a detailed and proactive research methodology. This helps to ensure the security of client networks and provides actionable recommendations for threat defense and mitigation.

System Compromise and Domain Defacement Mitigation

Solutionary recommends verifying that appropriate security patches are applied to systems and Web servers in a timely manner. Ensuring that patch management process and procedures are developed and followed significantly reduces the likelihood of a successful attack against these resources.

Solutionary advises organizations with Web applications being hosted on external providers to contact and work with the provider to ensure proper patches are implemented and applications are migrated to updated servers as appropriate to further limit the risk of compromise.

References:

http://www.solutionary.com/resource-center/blog/tags/OpUSA

DNS Amplification Attack Defense

Recommended preventive measures for DNS Amplification attack mitigation include logging and reviewing DNS activity as well as limiting recursive query access to authorized networks. If hosting an authoritative DNS server, recursion should be disabled completely. If hosting a recursive server, it should restrict queries to required entities.

Additionally, all customer premise equipment (CPE) devices should be configured not to listen for DNS packets from the incoming WAN interface from *network* and *broadcast* addresses. Solutionary recommends reviewing the procedures in the Internet Engineering Task Force Document 38 for proper implementation of network ingress filtering.

References:

http://tools.ietf.org/html/bcp38

http://www.solutionary.com/resource-center/white-papers/in-denialfollow-seven-steps-for-better-dos-and-ddos-protection

http://www.solutionary.com/resource-center/blog/tags/DDoS

Proactive Privacy Defenses for Information Disclosure

References:

http://www.solutionary.com/resource-center/blog/2013/06/does-prism-really-change-our-view-on-privacy

About SERT

The Solutionary Security Engineering Research Team (SERT) protects and informs Solutionary clients through security threat research, vulnerability analysis and the development of effective countermeasures. For more information, including Vulnerability Disclosures and Threat Reports, visit the research page on solutionary.com, the Solutionary Minds blog or download related whitepapers.

About Solutionary

Solutionary is the leading pure-play managed security service provider (MSSP), focused on delivering managed security services and global threat intelligence. Comprehensive Solutionary security monitoring and security device management services protect traditional and virtual IT infrastructures, cloud environments and mobile data. Solutionary clients are able to optimize current security programs, make informed security decisions, achieve regulatory compliance and reduce costs. The patented, cloud-based ActiveGuard® service platform uses multiple detection technologies and advanced analytics to protect against advanced threats. The Solutionary Security Engineering Research Team (SERT) researches the global threat landscape, providing actionable threat intelligence, enhanced threat detection and mitigating controls. Experienced, certified Solutionary security experts act as an extension of clients' internal teams, providing industry-leading client service to global enterprise and mid-market clients in a wide range of industries, including financial services, healthcare, retail and government. Services are delivered 24/7 through multiple state-of-the-art Security Operations Centers (SOCs).

For additional information: info@solutionary.com | 866-333-2133 | **www.solutionary.com**.