(U//FOUO) OpUSA: Criminal Hackers Planning Cyber Attacks Against US Websites

1 May 2013

(U//FOUO) Prepared by the Office of Intelligence and Analysis (I&A), Cyber Intelligence Analysis Division. Coordinated with the US-Computer Emergency Readiness Team (US-CERT), the Industrial Control Systems Cyber Emergency Response Team, and the National Cybersecurity and Communications Integration Center.

(U) Scope

(U//FOUO) This Note describes ongoing efforts by mostly Middle East- and North Africa-based criminal hackers and cyber actors to plan and launch cyber attacks aimed at US Government agencies, financial institutions, and commercial organizations in a campaign known as “OpUSA.” This information is provided to inform the Department and federal, state, local, tribal, territorial, and private sector partners in order to identify priorities for protective and support measures regarding emerging threats to cybersecurity.

(U) Key Findings

(U//FOUO) On 7 May 2013, a group of mostly Middle East- and North Africa-based criminal hackers are preparing to launch a cyber attack campaign known as "OpUSA" against websites of high-profile US Government agencies, financial institutions, and commercial entities. The attacks likely will result in limited disruptions and mostly consist of nuisance-level attacks against publicly accessible webpages and possibly data exploitation. Independent of the success of the attacks, the criminal hackers likely will leverage press coverage and social media to propagate an anti-US message.

(U) Source Summary Statement

(U//FOUO) The analysis in this Note is based on US-CERT reporting and open source reporting. The reliability of this reporting is excellent, giving us **high confidence** in our judgments. This Note also is supported by US media reporting; as this information may contain political or journalistic bias and may be intended to influence as well as inform, we have **medium confidence** in the analytic judgments derived from this reporting.

(U//FOUO) Middle East- and North Africa-Based Criminal Hackers Planning Cyber Campaign Targeting US Websites

(U//FOUO) A group of Middle East- and North Africa-based criminal hackers are planning a 7 May 2013 cyber attack campaign, known as "OpUSA," against US Government, financial, and commercial institutions. Since mid-April 2013, the campaign's members have used social media and web forums hosting violent extremist content to attract additional participants and raise awareness of the efforts.

- (U//FOUO) According to US-CERT, the OpUSA campaign has publicized hundreds of high-profile US Government agencies, local government, and law enforcement agencies, and local and regional financial institutions as likely targets.

- (U//FOUO) On 10 April 2013, one of the alleged organizers announced the campaign through a social media outlet and listed various criminal hacking teams he claimed would participate in the attacks, according to open source reporting. Approximately 40 individuals and groups have been identified as likely participants in OpUSA, including some who have expressed support for violent extremism.

- (U//FOUO) According to US media reporting, although OpUSA officially is scheduled for 7 May 2013, two separate criminal hacking groups linked to the campaign already have defaced at least 17 US websites. Another associated individual claimed to have hacked social network accounts and posted 40,000 user names, e-mail addresses, and passwords.

- (U//FOUO) Open source reporting indicates that the criminal hackers behind the OpUSA campaign previously organized and claimed responsibility for an early April 2013 cyber campaign known as "OpIsrael," which targeted Israeli Government and commercial websites.

(U//FOUO) Several individuals linked to websites that host violent extremist content have promoted OpUSA and called on like-minded individuals to support the effort, indicating the campaign has gained the attention of at least some violent extremist sympathizers.

- (U//FOUO) A member of a web forum that hosts al-Qa'ida-inspired content posted messages on the forum and social media encouraging supporters of violent extremism to participate in the cyber attacks, according to open source reporting.

- (U//FOUO) Several members of key web forums that host violent extremist content openly called on sympathizers to access the expertise of non-ideologically motivated individuals by collaborating with them on the campaign.

- (U//FOUO) According to US media reporting, the criminal hackers behind the OpUSA campaign have accused the United States of committing multiple war crimes in Afghanistan, Iraq, and Pakistan, as well as within the United States. In a 16 April 2013 message, the group's members also accused the US Government of blaming Muslims for the 15 April 2013 Boston Marathon bombings and promised retribution.

(U//FOUO) Commercial Tool Use Suggests Limited Technical Skills

(U//FOUO) The criminal hackers behind the OpUSA campaign most likely will rely on commercial tools to exploit known vulnerabilities, rather than developing indigenous tools or exploits. This suggests some of the participants possess only rudimentary hacking skills capable of causing only temporary disruptions of targeted websites. Nevertheless, OpUSA participants likely will exaggerate the scope and impact of their attacks as a way to attract additional press and draw more capable criminal hackers to future hacking efforts.

- (U//FOUO) According to US media reporting, the attackers probably will use a variety of nuisance-level criminal hacking techniques, such as distributed denial of service (DDoS) attacks, website defacements, and data leaks. The OpUSA campaign has provided potential supporters with the links to various DDoS tools, hacking applications, and resource forums.

- (U//FOUO) US media reporting indicates that on 22 April 2013, the criminal hackers behind the OpUSA campaign described their previous attack, OpIsrael, as a major success. They claimed the attack caused more than $3 billion in damages and accused Israeli officials of downplaying the severity of the attacks. The attackers almost certainly exaggerated the operation's success with claims of having hacked more than 100,000 Israeli websites and 45,000 Israeli social network accounts, in addition to leaking data linked to 30,000 Israeli bank accounts.

- (U//FOUO) According to US-CERT, a private security firm received 706 website defacement claims associated with OpIsrael, some of which have been confirmed. These claims probably are a small portion of the total number of hacked websites, which the security firm assesses may have numbered as many as several thousand.

(U) Implications

(U//FOUO) OpUSA poses a limited threat of temporarily disrupting US websites. It may, however, signal an emerging trend of Middle East- and North Africa-based criminally motivated hackers collaborating with others regardless of their motivation.

(U//FOUO) Middle East- and North-Africa-based criminal hackers will continue issuing public statements to announce cyber attack plans against high-profile targets to attract media attention to their cause. These statements may provide insight into whether these groups are radicalizing toward violence and whether they would potentially partner with or conduct attacks on behalf of violent extremists. The OpUSA campaign's perceived success might lead other individuals—including those with advanced technical skills—to undertake similar efforts and attempt more threatening cyber attacks targeting US Government and commercial websites.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us-cert.gov/report/ and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

(U) I&A would like to invite you to participate in a brief customer feedback survey regarding this product. Your feedback is extremely important to our efforts to improve the quality and impact of our products on your mission. Please click below to access the form and then follow a few simple steps to complete and submit your response. Thank you.

Survey

(U) Tracked by: HSEC-1.1, HSEC-1.2, HSEC-1.3, HSEC-1.4, HSEC-1.5, HSEC-1.6, HSEC-1.8

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) OpUSA: Criminal Hackers Planning Cyber Attacks Against US Websites

1. (U//FOUO) Please select partner type: Select One **and function:** Select One

2. (U//FOUO) Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	○	○	○	○	○	○
Product's relevance to your mission	○	○	○	○	○	○
Product's timeliness	○	○	○	○	○	○
Product's responsiveness to your intelligence needs	○	○	○	○	○	○

3. (U//FOUO) How do you plan to use this product in support of your mission? ***(Check all that apply.)***

- ☐ Integrate into one of my own organization's finished information or intelligence products
- ☐ Share contents with partners outside my organization
- ☐ Share within my organization
- ☐ Improve situational awareness
- ☐ Incorporate into training
- ☐ Incorporate into planning and preparedness efforts
- ☐ Do not plan to use
- ☐ Other:

4. (U//FOUO) How does this product add value to your mission? ***(Please portion mark comments.)***

5. (U//FOUO) How could this product be improved? ***(Please portion mark comments.)***

6. (U//FOUO) Which of the following intelligence sources do you regularly rely on to perform your homeland security mission? ***(Check all that apply.)***

☐ Internal security/intelligence element ☐ NCTC ☐ FBI ☐ Other DHS Component (e.g. CBP, TSA, or USCG)
☐ Other federal agency ☐ Intelligence fusion center ☐ News media ☐ DHS I&A ☐ None of the above

7. (U//FOUO) What is the primary intelligence source you rely on to perform your homeland security mission? Select One

To help us understand more about your organization so we can better tailor future products, please provide:

Name:		*Position:*	
Organization:		*State:*	
Contact Number:		*E-mail:*	

Submit Feedback

Privacy Act Statement

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Product Serial Number: IA-0112-13 REV: 1 April 2013

12-415-IA