radware

ERT Threat Alert
#OpSingleGateway – Summer Edition
June 7, 2017

Abstract

In the first week of June there has been a dramatic increase in activity from #OpSingleGateway, an Anonymous operation designed to combat the government of Thailand's strategy to implement central control of the nation's Internet, similar to what has been witnessed in China.

Figure 1: OpSingleGateway

Background

The Thai government along with the Ministry of Information and Communication Technology (MICT) are working on consolidating ten Internet gateways in the country into a single, centralized gateway. The centralized gateway would allow the government to monitor, censor and inspect all Internet traffic in Thailand and would be able to arrest any person not complying with the countries' Internet laws.

Over the weekend of June 3 – 4, media outlets began reporting on an alert from the Thailand Computer Emergency Response Team (ThaiCert) warning state agencies about a possible attack from Anonymous[i]. At the beginning of 2017, Radware issued a similar alert[ii] regarding the same operation, OpSingeGateway. In January, Anonymous targeted Thailand's domain registrar, ISP's and government agencies with DDoS attacks, data dumps and defaces. The Ministry of Foreign Affairs, Thailand's International Cooperation Agency, and Thailand's job portal was leaked on the darknet.

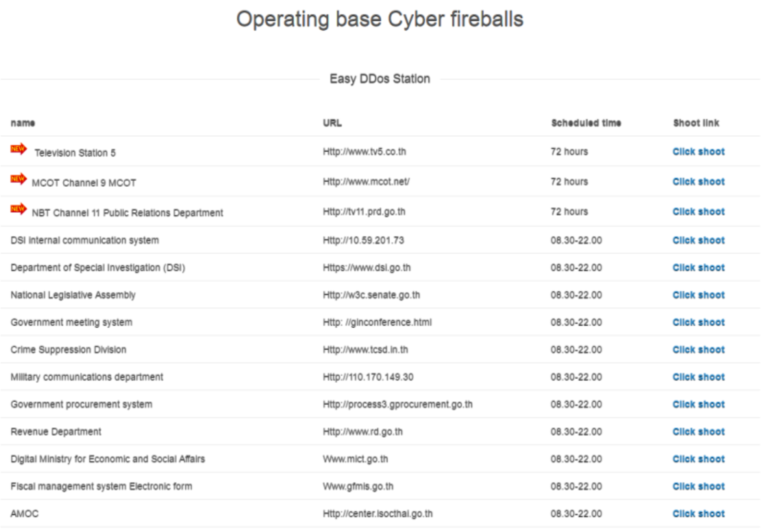
Now Telecoms[iii] along with others are setting up teams to deal with the persistent threat from OpSingleGateway. Anonymous has issued several statements about the plan for a single gateway and has organized a new phase of the operation. "Thailand F-Five Cyber Army" is targeting fourteen sites in a series of attacks and has provided an attack portal for hacktivist. There are also several accounts on Twitter targeting universities, telecoms, media and the government sites in parallel.

Targets

Anonymous is targeting fourteen main sites but has also been observed attacking universities, telecoms, media, government and energy firms in this phase. Attacker @CyberHatSec[iv] recently targeted and dumped data from Siam Fiber Optics company. The database from the dump included website administrator's usernames and passwords[v]. Nic.go.th was also targeted and dumped by Anonymous[vi] after Radware's alert in January. This dump also included usernames and passwords related to nic.go.th[vii]. Most recently Thai.com was hacked by WHT[viii]. Once again, this dump also included username and passwords[ix].

Easy DDos Station for 14 targets

1.	Television Station 5	tv5.co.th
2.	MCOT Channel 9 MCOT	mcot.net/
3.	NBT Channel 11 Public Relations Department	tv11.prd.go.th shoot
4.	DSI internal communication system	10.59.201.73
5.	Department of Special Investigation (DSI)	dsi.go.th
6.	National Legislative Assembly	w3c.senate.go.th
7.	Government meeting system	ginconference.html
8.	Crime Suppression Division	tcsd.in.th
9.	Military communications department	110.170.149.30
10.	Government procurement system	process3.gprocurement.go.th
11.	Revenue Department	www.rd.go.th
12.	Digital Ministry for Economic and Social Affairs	mict.go.th
13.	Fiscal management system Electronic form	gfmis.go.th
14.	AMOC	center.isocthai.go.th



Operating base Cyber fireballs

Easy DDos Station

name	URL	Scheduled time	Shoot link
NEW Television Station 5	Http://www.tv5.co.th	72 hours	Click shoot
NEW MCOT Channel 9 MCOT	Http://www.mcot.net/	72 hours	Click shoot
NEW NBT Channel 11 Public Relations Department	Http://tv11.prd.go.th	72 hours	Click shoot
DSI internal communication system	Http://10.59.201.73	08.30-22.00	Click shoot
Department of Special Investigation (DSI)	Https://www.dsi.go.th	08.30-22.00	Click shoot
National Legislative Assembly	Http://w3c.senate.go.th	08.30-22.00	Click shoot
Government meeting system	Http: //ginconference.html	08.30-22.00	Click shoot
Crime Suppression Division	Http://www.tcsd.in.th	08.30-22.00	Click shoot
Military communications department	Http://110.170.149.30	08.30-22.00	Click shoot
Government procurement system	Http://process3.gprocurement.go.th	08.30-22.00	Click shoot
Revenue Department	Http://www.rd.go.th	08.30-22.00	Click shoot
Digital Ministry for Economic and Social Affairs	Www.mict.go.th	08.30-22.00	Click shoot
Fiscal management system Electronic form	Www.gfmis.go.th	08.30-22.00	Click shoot
AMOC	Http://center.isocthai.go.th	08.30-22.00	Click shoot

Figure 2: Easy DDoS Station

Attack Methods

First, Anonymous hackers scan the sites with a basic fuzzer looking for possible vulnerabilities. After discovering vulnerabilities in the technology and mapping the network, they select their attack vector, as there is no one-size-fits-all solution.

Web Application Exploits

- **SQL Injection** - This technique takes advantage of poor application coding. When the application inputs are not sanitized it becomes vulnerable. Attackers can modify an application SQL query to gain access to unauthorized data with administrator access, run remote commands on the server, drop or create objects in the database and more.
- **Defacement** – Attacker changes the visual appearance of the website by breaking into a web server and replacing the current website with one of their own. This attack is most commonly associated with SQL.
- **Injection** - This form of an attack allows administrative access and usually involves obtaining user credentials first. It allows hackers to make changes to a website.

- **Data Theft** – compromising sensitive data while data at rest or in transit, via stealing encryption keys, hashed passwords, clear text data off the server, and even from a user's browser.

Denial of Service Attack Vectors

- **TCP flood** - One of the oldest, yet still very popular Denial of Service (DoS) attacks. It involves sending numerous SYN packets to the victim. In many cases, attackers will spoof the SRC IP so the reply (SYN+ACK packet) will not return, thus overwhelming the session/connection tables of the targeted server or one of the network entities on the way (typically the firewall). Servers need to open a state for each SYN packet that arrives and they store this state in tables that have limited size. As big as this table may be it is easy to send sufficient amount of SYN packets that will fill the table, and once this happens the server starts to drop a new request, including legitimate ones. Similar effects can happen on a firewall which also has to process and invest in each SYN packet. Unlike other TCP or application-level attacks the attacker does not have to use a real IP - this is perhaps the biggest strength of the attack.
- **UDP Flood** – In a UDP flood, the attacker sends large UDP packets to a single destination or to random ports. Since the UDP protocol is "connectionless" and does not have any type of handshake mechanism, the main intention of a UDP flood is to saturate the Internet pipe. In most cases the attackers spoof the SRC (source) IP
- **HTTP/S Flood** - An attack method used by hackers to attack web servers and applications. These floods consist of seemingly legitimate session-based sets of HTTP GET or POST requests sent to a targeted web server. HTTP floods do not use spoofing, reflective techniques or malformed packets. These requests are specifically designed to consume a significant amount of the server's resources, and therefore can result in a denial-of-service. Such requests are often sent en masse by means of a botnet, increasing the attack's overall power. HTTP and HTTPS flood attacks are one of the most advanced threats facing web servers today since it is hard for network security devices to distinguish between legitimate and malicious HTTP traffic.

Denial of Service Tools

In addition to the Easy DDoS station provided by F5 Cyber Army Thailand, Anon Thai News has provided a list of suggested tools for this operation[x]. These tools are simple DoS scripts or GUI tools that are easily mitigated with Radware signature based mitigation system.

- DDoSim
- SlowLoris
- ApacheKiller
- PyLoris
- Hping
- Qslowloris
- Tor's Hammer
- Sniper xxXXxx
- Xerxes

VPN's

Anon Thai News is also providing a list of VPN's that are suggested to use while launching a denial of service with the tools previously suggested.

- proXPN
- Cyberghost
- Hotspot Shield
- Free VPN
- Its Hidden

- USA IP
- VPN Tool
- Tor VPN

IRC

In this phase of the operation, the group Op Anonymous Greece has created a Titanpad[xi] for hacktivist to communicate and post target information for the operation. In addition to Titanpad, attackers are also using more traditional methods of communication through IRC's found on Cyber Guerrilla[xii], Anon Plus[xiii] and Anon Ops[xiv].

Accounts

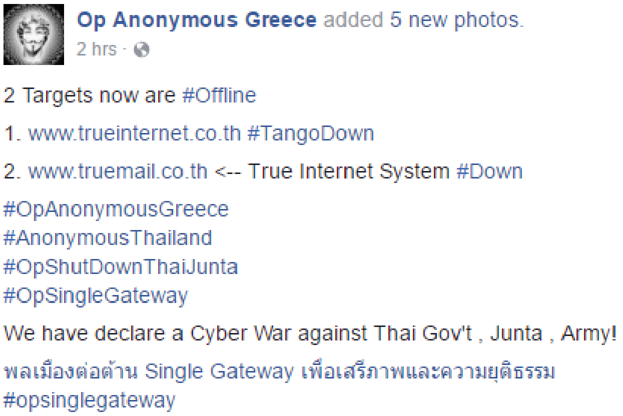
Twitter	Facebook
• https://twitter.com/AnonPlus_Info • https://twitter.com/CyberHatSec • https://twitter.com/AnonThailand	• https://www.facebook.com/opanonymousgreece • https://www.facebook.com/AnonThaiNewsV2 • https://www.facebook.com/OpSingleGateway/ • https://www.facebook.com/ThailandF5CyberArmy • https://www.facebook.com/PeopleCyberTh/

YouTube

Thailand Censorship #OpSingleGateway (May 8th, 2017) - https://youtu.be/k7ggPrrHJcA

Reasons for Concern

Anonymous has been targeting Thailand at a persistent rate since the announcement in 2015 to consolidate the Internet gateways. This announcement not only drew the attention of hacktivist like Anonymous but also privacy and security advocates around the world. Security professionals are concerned with Thailand's plans to centralize the country's gateways into a single point. This would ultimately become a single point of failure. This would also allow the government to easily intercept and preform deep packet inspection on the country's traffic. The Bangkok Post reported[xv] that the Central Investigation Bureau (CIB), the agency tasked with monitoring the Internet for content deemed offensive, is taking steps to target those that view the material. The agency is reportedly in the process of acquiring tools to help them identify users who view questionable material so they can confront the user and warn them.



Op Anonymous Greece added 5 new photos.
2 hrs ·

2 Targets now are #Offline

1. www.trueinternet.co.th #TangoDown

2. www.truemail.co.th <-- True Internet System #Down

#OpAnonymousGreece
#AnonymousThailand
#OpShutDownThaiJunta
#OpSingleGateway

We have declare a Cyber War against Thai Gov't , Junta , Army!

พลเมืองต่อต้าน Single Gateway เพื่อเสรีภาพและความยุติธรรม
#opsinglegateway

Figure 3: OpSingleGate Continues on June 5th – Target: True Internet

Because of these actions, hacktivists around the world are launching attacks against Thailand. After OpSingleGateway was revamped in December 2016, Anonymous began targeting sites all over Thailand in a number of different verticals. These attacks will continue as long as the Thai government continues with their plans to centralize and monitor the country's Internet.

Effective DDoS Protection Essentials:

- **Hybrid DDoS Protection** - (on-premise + cloud) – for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - to quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - to promptly protect from unknown threats and 0-day attacks
- **A cyber-security emergency response plan** - that includes a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Effective Web Application Security Essentials

- **Full OWASP Top-10 application vulnerabilities coverage**– against defacements, injections, etc.
- **Low false positive rate** – using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options** - on-premise, out-of-path, virtual or cloud-based

For further security measures, Radware urges companies to inspect and patch their network in order to defend against 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.

[i] http://www.bangkokpost.com/news/general/1261507/state-agencies-warned-against-cyberattacks
[ii] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opsingle-gateway/
[iii] http://www.bangkokpost.com/news/general/1261455/nbtc-braces-for-anonymous-attacks
[iv] https://twitter.com/CyberHatSec/status/871321726042296320
[v] https://ghostbin.com/paste/3u9py
[vi] https://www.cyberguerrilla.org/blog/anonymous-hacks-nic-go-th-for-opsinglegateway/
[vii] http://ruqay5morumo3tcg.onion/?60e061f70ef21204#aCR3WSA4R+YkKI2UAjDSr4Ft2NJzAdXQrDjKRZcXqUU=
[viii] https://www.cyberguerrilla.org/blog/anonymous-hacks-thai-com-for-opsinglegateway/
[ix] https://zerobin.net/?5cf6199fad0b3e57#pIn3LU7xOTfPeb3LZUsHlkjkpFO7Cy6i9TiHlwLM5bU=

[x] https://www.facebook.com/AnonThaiNewsV2/posts/1382434288492095
[xi] https://titanpad.com/P2l3KB4qPk
[xii] www.webchat.cyberguerrilla.org
[xiii] http://webchat.anonplus.org/
[xiv] https://webchat.anonops.com
[xv] http://www.bangkokpost.com/news/general/1253246/lese-majeste-drive-targets-web-viewers