Abstract

In a move to combat the government of Thailand's strategy to implement central control of the nation's Internet, Anonymous has launched OpSingleGateway. OpSingleGateway is in reaction to the Thai government's plan to consolidate 10 Internet gateways in the country into a single, centralized gateway controlled by the government. The centralized gateway would give the government the ability to control, intercept and arrest any person not complying with Internet laws. The campaign was revamped in December 2016 following amendments to the Computer Crimes Act of 2007. Under these new laws, a committee is given the power to inspect, block and delete content, and anyone entering forged or false information into a computer deemed a threat to national security and could face a five-year jail sentence.[1]

Recent Attacks and Targets

Since this announcement, Thailand's government agencies - nationally and abroad - have faced severe DDoS attacks resulting in Internet outages, website defacements and data dumps.

- **DDoS Attacks** - National Security Agency, Ministry of Defense, Ministry of Digital Economy and Ministry of Foreign Affairs were all targeted. Dozens of other websites knocked offline:
  - https://twitter.com/DeepLUser/status/821351906656325632
  - https://twitter.com/LonelyCloudss/status/820973091807297536
  - https://twitter.com/maxiedakitten/status/820629767540051969
  - https://twitter.com/anonymousAsia/statuses/821074694036135937
- **Data Dumps** - personal data about government employees: names, work history, financial information, phone numbers, emails, user names and passwords.
  - Leaks found on the Clearnet:
    - thahadyaw.go.th - https://ghostbin.com/paste/bx9wp
    - thaisoung.co.th - https://ghostbin.com/paste/qh7d8
    - thaiveterans.mod.go.th - https://ghostbin.com/paste/n48y6

  - Leaks found on the Darknet:
    - ID's of MFA (Ministry of Foreign Affairs) & TICA (Thailand International Cooperation Agency) employees. http://qkjscem7kksghlux.onion/
    - Details from Thailand's government job portal on PrivateBin. http://264nglqbtqlabsxl.onion/opsinglegateway-anonymous-hacks-thai-gov-job-portal-to-protest-cyber-law-and-censorship/

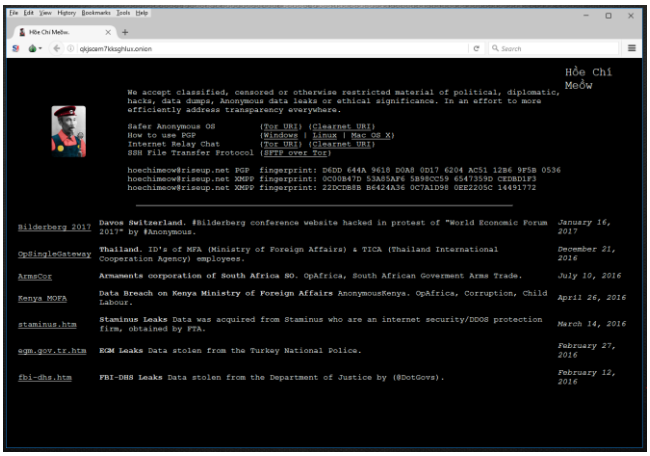

Figure 1: OpSingleGateway MFA (Ministry of Foreign Affairs) dump on the Darknet

[1] http://aa.com.tr/en/asia-pacific/junta-appointed-thai-assembly-passes-cyber-control-bill/707774

Target List:

https://ghostbin.com/paste/hc7tm

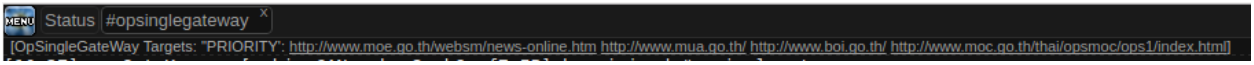

Figure 2: Current Targets for the week post in the #OpSingleGateway Channel

Communication Channels:

- IRC -
  http://webchat.anonplus.org
  http://webchat.anonops.org
- Twitter - https://twitter.com/AnonThailand

Figure 3: Anonymous announcing that all .go.th and .mi.th are targets for #OpSingleGateway

- YouTube - https://www.youtube.com/watch?v=xlbk8noxuZ4 (New)
- Facebook-
  https://www.facebook.com/OpSingleGateway/
  https://www.facebook.com/ThailandF5CyberArmy/

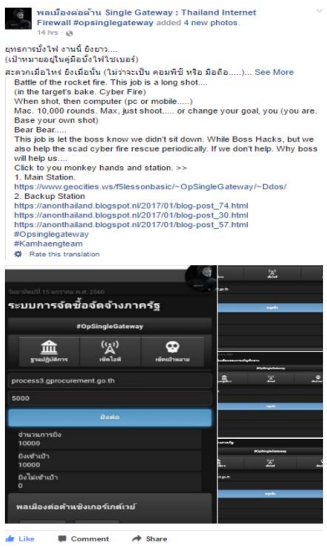

Figure 4: Instructions on Facebook for participating in the DoS attack

Attack Methods

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

Web Application Exploits

- **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.

Figure 5: Hacker shows that they have root access on ssps4.go.th

- **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.

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.

Effective DDoS Protection Essentials

As civil protests are more and more often accompanied with cyber-attacks, authorities and corporations have to adjust their protection strategies to prevent possible network outages, data leakage and reputation loss.

- **Hybrid DDoS Protection** – on premise and cloud-based solutions for real-time protection 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.
- **Cyber-Security Emergency Response Plan** - that includes a dedicated team of security experts.

Effective Web Application Protection Essentials

- **Full coverage of OWASP Top-10** application vulnerabilities
- **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
- **IP-agnostic device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Flexible deployment options -** on-premise, out-of-path, virtual or cloud-based

Radware's hybrid attack mitigation solution provides a set of patented technologies designed to detect, mitigate and report todays most advanced threats. Dedicated hardware and cloud based DDoS protection solutions seamlessly integrated with a Web Application Firewall protect against network and application attacks in real time and help ensure continuous service availability.

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.