Abstract

Anonymous plans to officially launch phase 4 of Operation Catalunya in support of Catalan independence, at 8pm Central European Time on Thursday, December 21st.

Figure 1: OpCatalunya Banner

Background

In October 2017, citizens of Catalonia – an autonomous community in Spain - held an independence referendum. This call for independence created a conflict between the Catalan leadership and Spanish government and increased law enforcement presence in Catalonia. As a result, the hacktivist group Anonymous launched a series of cyber-attacks against Spanish institutions in protest. The Anonymous operation has already seen three waves of attacks with a fourth operation staged to begin on December 21, 2017 in parallel with Catalans regional election.

Figure 2: @Scode404 Announcing the official start time for OpCatalunya

Targets

Anonymous hacktivists seek to launch attacks on companies related to the security and telecommunications companies of the Spanish government along with websites associated with the Spanish government.

> #Anonymous is already ready for tomorrow. Time: 20:00 pm in Spanish time. #OpCatalunya #FreeCatalonia #Op21DEC #21D @Scode404 @ANONSPAIN2 @NamaTikure @nonymousNews @AnonPlus_Info @YourAnonNews @LulsecZombie @UnitedSecAnon @AnonXeljomudoX

Figure 3: Notes from Minion Ghost's Github

Attack Vectors

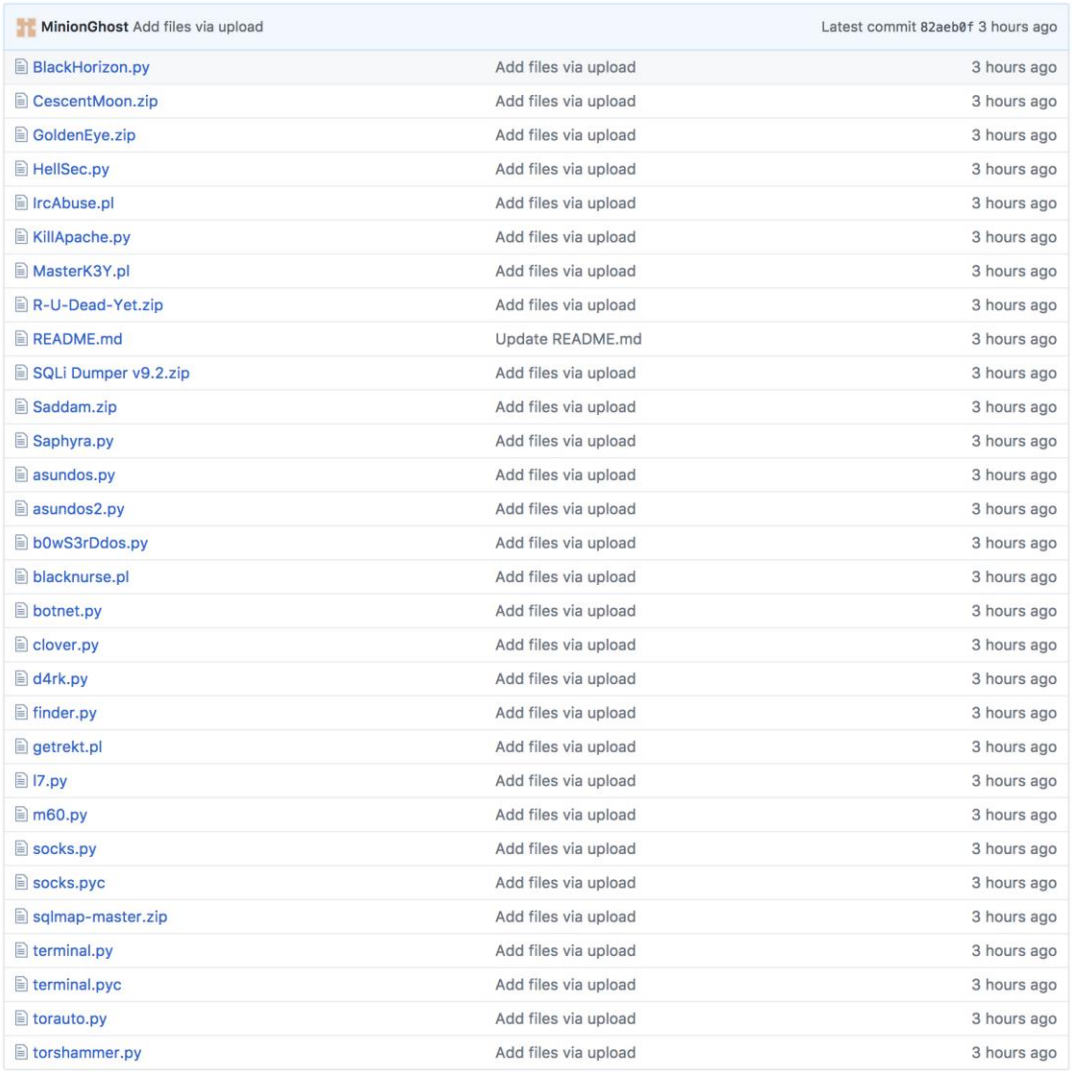
Web Application Attacks

- **Cross-Site Scripting** - In this attack, malicious scripts are injected into websites via a web application flaw where there is no validation of user input used by the application. The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.
- **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

- **ICMP**: Internet Control Message Protocol (ICMP) is a connectionless protocol used for IP operations, diagnostics, and errors. An ICMP Flood - sending an abnormally large number of ICMP packets of any type (especially network latency testing "ping" packets) - can overwhelm a target server that attempts to process every incoming ICMP request, until a denial-of-service condition for the target server.
- **TCP Flood** - One of the oldest, yet still very popular denial-of-service 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
- **SYN:** A SYN flood overwhelms a target machine by sending thousands of connection requests to it using spoofed IP addresses. This causes the target machine to attempt to open a connection for each malicious request and subsequently wait for an ACK packet that never arrives. A server under a SYN flood attack will continue to wait for a SYN-ACK packet for each connection request, as the delay could be normal and related to network congestion. However, because a SYN-ACK packet never arrives for any of the connection requests; the massive number of half-open connections quickly fills up the server's TCB table before it can time any connections out. This process continues for as long as the flood attack continues.

- **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.



MinionGhost Add files via upload		Latest commit 82aeb0f 3 hours ago
BlackHorizon.py	Add files via upload	3 hours ago
CescentMoon.zip	Add files via upload	3 hours ago
GoldenEye.zip	Add files via upload	3 hours ago
HellSec.py	Add files via upload	3 hours ago
IrcAbuse.pl	Add files via upload	3 hours ago
KillApache.py	Add files via upload	3 hours ago
MasterK3Y.pl	Add files via upload	3 hours ago
R-U-Dead-Yet.zip	Add files via upload	3 hours ago
README.md	Update README.md	3 hours ago
SQLi Dumper v9.2.zip	Add files via upload	3 hours ago
Saddam.zip	Add files via upload	3 hours ago
Saphyra.py	Add files via upload	3 hours ago
asundos.py	Add files via upload	3 hours ago
asundos2.py	Add files via upload	3 hours ago
b0wS3rDdos.py	Add files via upload	3 hours ago
blacknurse.pl	Add files via upload	3 hours ago
botnet.py	Add files via upload	3 hours ago
clover.py	Add files via upload	3 hours ago
d4rk.py	Add files via upload	3 hours ago
finder.py	Add files via upload	3 hours ago
getrekt.pl	Add files via upload	3 hours ago
l7.py	Add files via upload	3 hours ago
m60.py	Add files via upload	3 hours ago
socks.py	Add files via upload	3 hours ago
socks.pyc	Add files via upload	3 hours ago
sqlmap-master.zip	Add files via upload	3 hours ago
terminal.py	Add files via upload	3 hours ago
terminal.pyc	Add files via upload	3 hours ago
torauto.py	Add files via upload	3 hours ago
torshammer.py	Add files via upload	3 hours ago

Figure 4: DoS Tools for the operationMinion Ghost

Other Attacks

- **Phishing -** A digital attempt to obtain sensitive information from a victim by using a malicious email or website. The attacker solicits personal information by posing as a trustworthy organization or the company itself. These attempts are either sent out to everyone in the company or designed to specifically target key associates. Once an associate falls victim to these

cyber-attacks, the hacker will then have the sensitive information required to gain access to certain systems.

- **Social Engineering -** A process of psychological manipulation, more commonly known as human hacking. The goal is to have the targeted victim divulge confidential information or give you unauthorized access because you have played off their natural human emotion of wanting to help or provide them with something. Most of the time the attacker's motives are to either gather information for future cyber-attacks, to commit fraud or to gain system access for malicious activity.

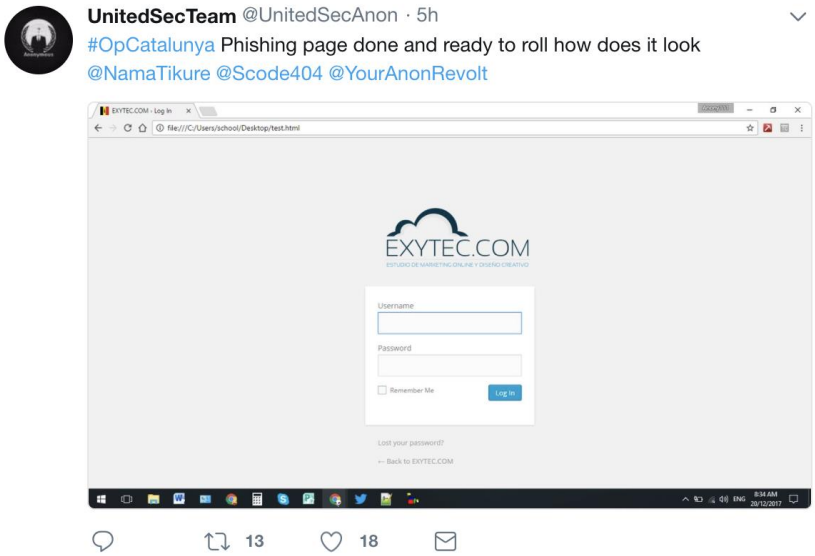


Figure 5: @UnitedSecAnon allegedly preparing a phishing site

Hashtags

- #OpCatalunya
- #FreeCatalonia
- #Op21Dec

Cyber Guerrilla Blog

https://www.cyberguerrilla.org/blog/anonymous-a-freecatalonia-remember-the-21th-of-december/

IRC Channel

http://webchat.anonplus.org/ - #OpCatalunya

YouTube

Operation Video: https://youtu.be/uISLSP0TCKc

Figure 6: Operational Video

Social Media

Organization that are concerned may consider following the following attackers on Twitter

- @AnonXeljomudoX
- @Scode404
- @UnitedSecAnon
- @Anonspain2
- @NamaTikure

What's Expected Next

The crisis between the Spanish and the Catalan governments continues to escalate as Anonymous enters the fourth phase of operations under OpCatalunya. It's expected that Spanish government websites and ISPs will be the main focus for this phase. In addition, cyber security firms protecting these networks could be attacked for their indirect support of the Spanish government. Victims could be targeted by SQL injections, cross-site scripting (XSS), data dumps and service outages caused by denial-of-service attacks. It is expected that these attacks will continue through the rest of December and into 2018.

Organizations Under Attack Should Consider

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through

- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

For further DDoS protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Effective Web Application Security Essentials

- **Full OWASP Top-10** 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

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.