ERT Threat Alert
OpCatalonia
October 31, 2017

Abstract

At the beginning of 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 has launched a series of cyber-attacks against Spanish institutions in protest. The Anonymous operation has already seen two waves of attacks with a third lingering as Spanish authorities impose direct rule on Catalonia using Article 155 of the Spanish Constitution. More is expected as the government convoke new elections to the Parliament of Catalonia on December 21 of this year.

Figure 1: An Anonymous propaganda image for OpFreeCatalonia

Background

Ahead of the referendum in Catalonia, Anonymous began building support for Catalonia's independence in September when they announced Operation Free Catalonia. Ever since, Anonymous has been targeting websites and networks of Spanish institutions, including the Constitutional Court of Spain and other government agencies. A number of other organizations – mainly ISPs, corporations, private businesses and schools - all suffered collateral impact.

Reasons for Concern

Anonymous is leveraging their common arsenal of cyber assaults, including network- and application-based attacks, defacements, data dumps and denial-of-service attempts. The first wave of attacks came after Spanish police violently ended the reference by forcefully removing ballet boxes. The second wave followed actions by the Spanish government on October 17 to regain control of Catalonia. Any government agency, corporation or organization in Spain is considered a target and should prepare. Anonymous is attacking a number of large organizations in an attempt to spread their message. The attackers are mainly defacing Spanish-based websites with a message for independence in Catalonia. In addition, the attackers launched denial-of-service attacks and application-based attacks resulting in data dumps from SQL Injections.

Targets

Data Dumps

- sanjavier.es
- uhu.es
- lavozdealmeria.es
- juntadeandalucia.es
- sgic.udc.es
- rac.es
- juntadeandalucia.es
- ayuntamientodeguadarrama.es
- bibdigital.rjb.csic.es
- ua.es
- proteccioncivil.es
- etsii.upv.es
- newsespana.es
- votoaccesible.com
- pagina.jccm.es
- madrid.org
- biblioteca.uca.es
- sscc.es
- aperturas.org

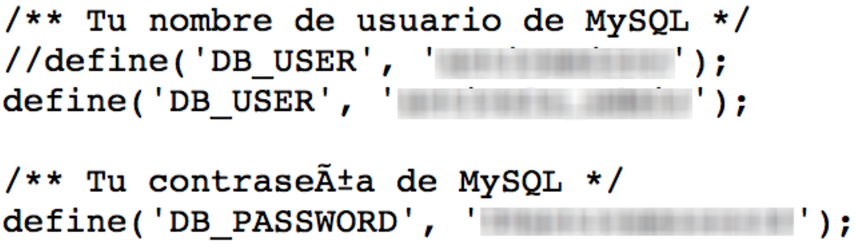
DDoS

- dsn.gob.es
- cni.es
- fomento.gob.es
- mjusticia.gob.es
- telitec.com
- flexinet.es
- internet4spain.com
- linerentalspain.com
- unlimited3gspain.com
- mjusticia.gob.es
- bancamarch.es
- policia.es
- mineco.gob.es
- pp.es
- tribunalconstitucional.es
- casaral.es

Attack Vectors

Web Application Attacks

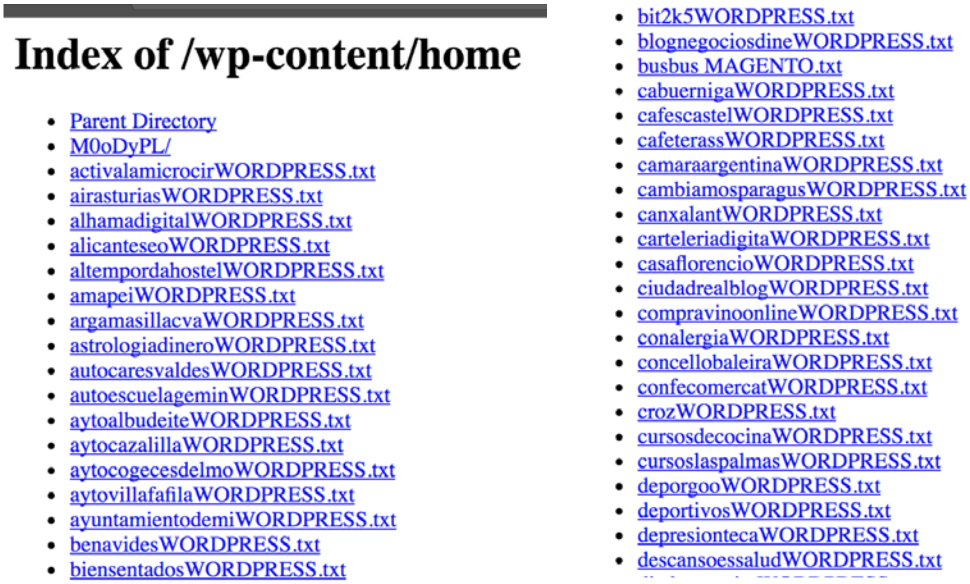
SQL Injection - This technique takes advantage of poor application coding. When the application inputs are not properly sanitized, it becomes vulnerable. Attackers can modify an application SQL query to gain access to unauthorized data with administrator access, run remote commands on the server, drop or create objects in the database, and more.



```
/** Tu nombre de usuario de MySQL */
//define('DB_USER', '[redacted]');
define('DB_USER', '[redacted]');

/** Tu contraseÃ±a de MySQL */
define('DB_PASSWORD', '[redacted]');
```

Figure 2: Username and Passwords found in text file



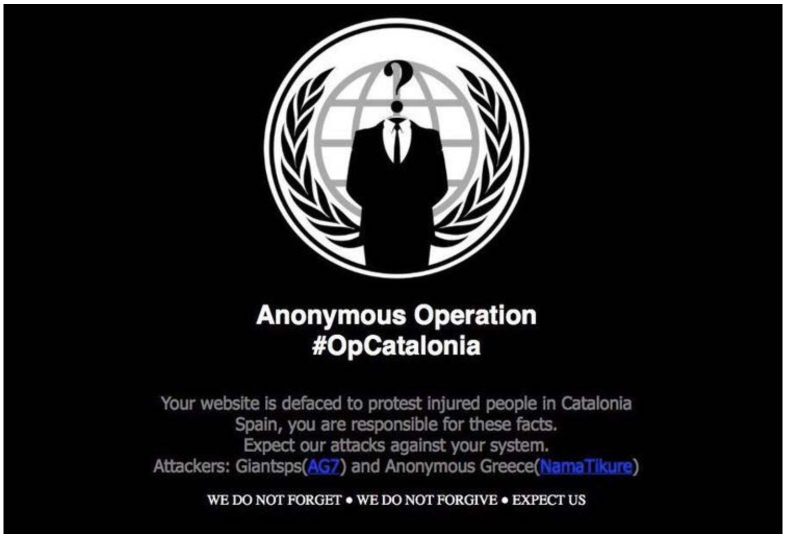
Index of /wp-content/home

- Parent Directory
- M0oDyPL/
- activalamicrocirWORDPRESS.txt
- airasturiasWORDPRESS.txt
- alhamadigitalWORDPRESS.txt
- alicanteseoWORDPRESS.txt
- altempordahostelWORDPRESS.txt
- amapeiWORDPRESS.txt
- argamasillacvaWORDPRESS.txt
- astrologiadineroWORDPRESS.txt
- autocaresvaldesWORDPRESS.txt
- autoescuelageminWORDPRESS.txt
- aytoalbudeiteWORDPRESS.txt
- aytocazalillaWORDPRESS.txt
- aytocogecesdelmoWORDPRESS.txt
- aytovillafafilaWORDPRESS.txt
- ayuntamientodemiWORDPRESS.txt
- benavidesWORDPRESS.txt
- biensentadosWORDPRESS.txt

- bit2k5WORDPRESS.txt
- blognegociosdineWORDPRESS.txt
- busbus MAGENTO.txt
- cabuernigaWORDPRESS.txt
- cafescastelWORDPRESS.txt
- cafeterassWORDPRESS.txt
- camaraargentinaWORDPRESS.txt
- cambiamosparagusWORDPRESS.txt
- canxalantWORDPRESS.txt
- carteleriadigitaWORDPRESS.txt
- casaflorencioWORDPRESS.txt
- ciudadrealblogWORDPRESS.txt
- compravinoonlineWORDPRESS.txt
- conalergiaWORDPRESS.txt
- concellobaleiraWORDPRESS.txt
- confecomercatWORDPRESS.txt
- crozWORDPRESS.txt
- cursosdecocinaWORDPRESS.txt
- cursoslaspalmasWORDPRESS.txt
- deporgooWORDPRESS.txt
- deportivosWORDPRESS.txt
- depresiontecaWORDPRESS.txt
- descansoessaludWORDPRESS.txt

Figures 3 & 4: OpCatalonia staging server – text files contained credentials for targeted sites

Defacement – A website defacement is like digital graffiti. An attacker will change 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 Injections. This form of an attack allows administrative access so that the hacker can make the changes required. Another way this is preformed is via FTP if the user’s credentials have been obtained.



Anonymous Operation
#OpCatalonia

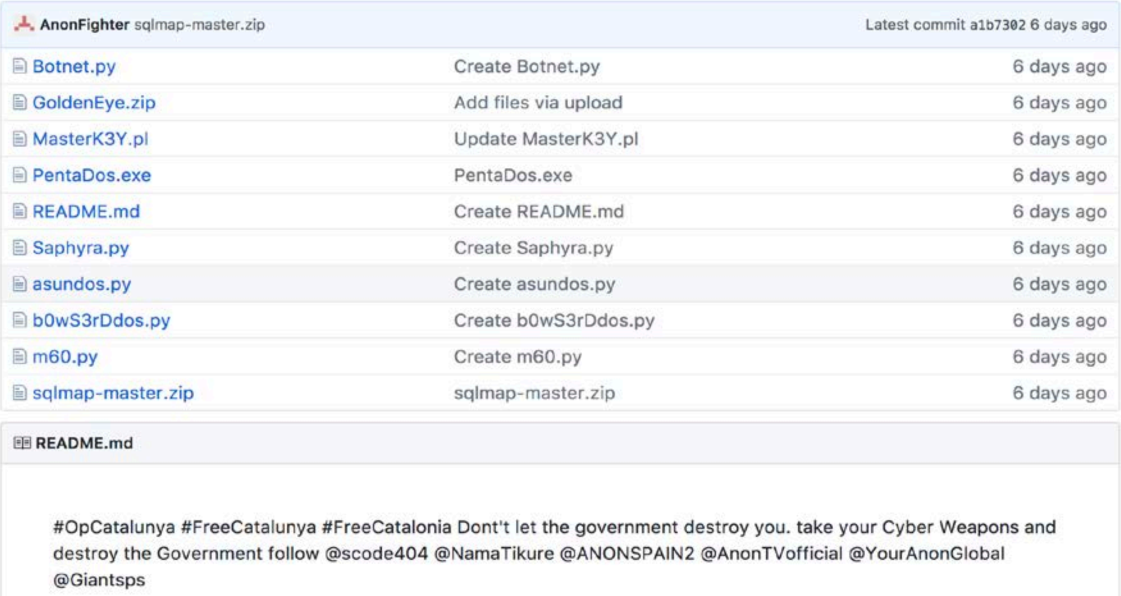
Your website is defaced to protest injured people in Catalonia
Spain, you are responsible for these facts.
Expect our attacks against your system.
Attackers: Giantsps(AG7) and Anonymous Greece(NamaTikure)

WE DO NOT FORGET • WE DO NOT FORGIVE • EXPECT US

Figure 5: OpCatalonia Defacement

Network-Level DDoS Attacks

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 a sufficient amount of SYN packets to 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.



AnonFighter sqlmap-master.zip | Latest commit a1b7302 6 days ago

Botnet.py	Create Botnet.py	6 days ago
GoldenEye.zip	Add files via upload	6 days ago
MasterK3Y.pl	Update MasterK3Y.pl	6 days ago
PentaDos.exe	PentaDos.exe	6 days ago
README.md	Create README.md	6 days ago
Saphyra.py	Create Saphyra.py	6 days ago
asundos.py	Create asundos.py	6 days ago
b0wS3rDdos.py	Create b0wS3rDdos.py	6 days ago
m60.py	Create m60.py	6 days ago
sqlmap-master.zip	sqlmap-master.zip	6 days ago

README.md

#OpCatalunya #FreeCatalunya #FreeCatalonia Dont't let the government destroy you. take your Cyber Weapons and destroy the Government follow @scode404 @NamaTikure @ANONSPAIN2 @AnonTVofficial @YourAnonGlobal @Giantsps

Figure 6: OpCatalonia GitHub Page with DoS Scripts

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.

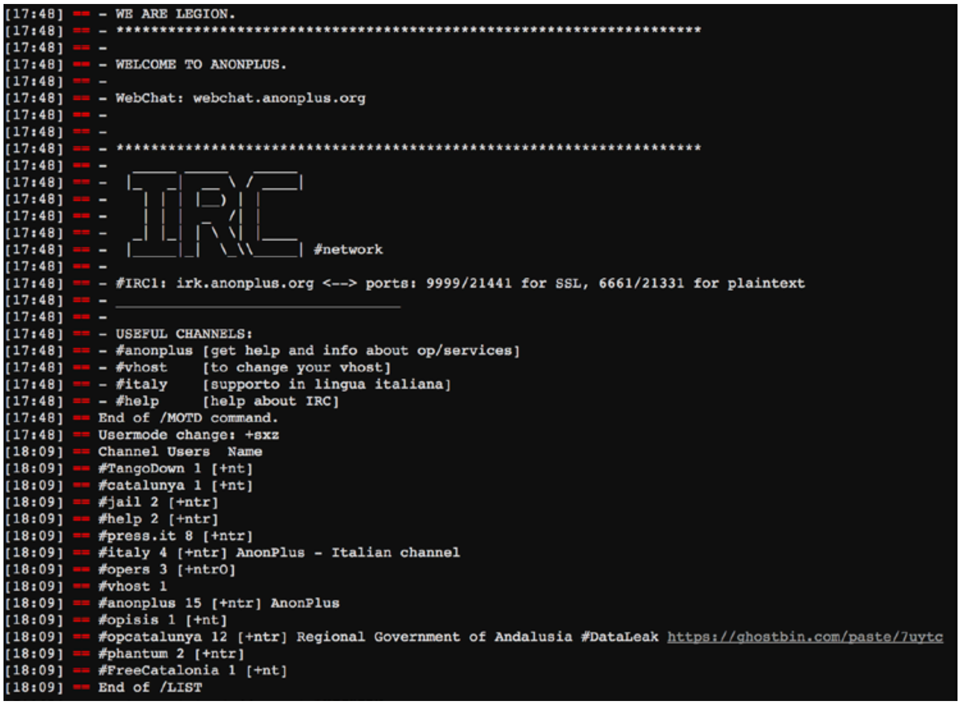
HTTP/S Flood - An attack method used by hackers to attack web servers and applications. These floods consist of seemingly legitimate session-based sets of HTTP GET or POST requests sent to a targeted web server. HTTP floods do not use spoofing, reflective techniques or malformed packets. These requests 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.

Social Media

Organizations that are concerned may consider following the following attackers on Twitter:

- @AnonPlus_info
- @ANONSPAIN2
- @NamaTikure
- @AnonOpsAL
- @Arm_Legi

Operational Video: https://youtu.be/f4cAkfTYDrA
OpCatalonia live hack video - https://twitter.com/Giantsps/status/923914603821707264



```
[17:48] == - WE ARE LEGION.
[17:48] == - *******************************************************************
[17:48] == -
[17:48] == - WELCOME TO ANONPLUS.
[17:48] == -
[17:48] == - WebChat: webchat.anonplus.org
[17:48] == -
[17:48] == -
[17:48] == - *******************************************************************
[17:48] == -   _____ _____   _____
[17:48] == -  |_   _|  __ \ / ____|
[17:48] == -    | | | |__) | |
[17:48] == -    | | |  _  /| |
[17:48] == -   _| |_| | \ \| |____
[17:48] == -  |_____|_|  \_\\_____| #network
[17:48] == -
[17:48] == - #IRC1: irk.anonplus.org <--> ports: 9999/21441 for SSL, 6661/21331 for plaintext
[17:48] == - ________________________________
[17:48] == -
[17:48] == - USEFUL CHANNELS:
[17:48] == - #anonplus [get help and info about op/services]
[17:48] == - #vhost    [to change your vhost]
[17:48] == - #italy    [supporto in lingua italiana]
[17:48] == - #help     [help about IRC]
[17:48] == End of /MOTD command.
[17:48] == Usermode change: +sxz
[18:09] == Channel Users  Name
[18:09] == #TangoDown 1 [+nt]
[18:09] == #catalunya 1 [+nt]
[18:09] == #jail 2 [+ntr]
[18:09] == #help 2 [+ntr]
[18:09] == #press.it 8 [+ntr]
[18:09] == #italy 4 [+ntr] AnonPlus - Italian channel
[18:09] == #opers 3 [+ntrO]
[18:09] == #vhost 1
[18:09] == #anonplus 15 [+ntr] AnonPlus
[18:09] == #opisis 1 [+nt]
[18:09] == #opcatalunya 12 [+ntr] Regional Government of Andalusia #DataLeak https://ghostbin.com/paste/7uytc
[18:09] == #phantum 2 [+ntr]
[18:09] == #FreeCatalonia 1 [+nt]
[18:09] == End of /LIST
```

Figure 7: IRC WebChat http://webchat.anonplus.org

What's Expected Next

The crisis between the Spanish and the Catalan governments is not going to end soon. This operation is expected to escalate in correlation with the conflict. In the near term, there are unverified reports that the third phase will begin on November 12 following the annual Million Mask March on November 5 by Anonymous, as well as a wave of attacks as the December 21 Catalan Parliament elections approach.

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.