ERT Threat Alert
AnonPlus Italia – Drupalgeddon
May 29, 2018

Abstract
Radware's Emergency Response Team (ERT) has been following AnonPlus Italia, an Anonymous group that has engaged in digital protests throughout April and May. The Anonymous affiliated group has executed numerous web defacements to protest war, religion, politics and financial power while spreading a message about their social network by abusing the content management systems (CMS) of websites that have not been updated to protect against exploits.

Figure 1: AnonPlus Logo

Background
In 2011, AnonPlus was created with the purpose of becoming a social networking service developed for Anonymous members. Shortly after it was announced, AnonPlus was hacked by rival groups and has struggled to maintain a social presence and a secure internet relay chat (IRC) since. AnonPlus Italia is not affiliated with Anonymous Italia. AnonPlus Italia attacks from earlier this year have had a political objective. This group has launched attacks over the past month against government-related websites in Italy and the United States as well as financial institutions.

Previous Operations
AnonPlus has supported multiple hacktivism operations in the past.

OpSingleGateway
Last year, Radware's ERT reported on an Anonymous operation, OpSingleGateway[1] [2]. This Anonymous operation protested the government of Thailand's strategy to implement central control of the nation's internet. The centralized gateway would give the government the ability to control, intercept and arrest any person not complying with internet laws. Under the Computer Crimes Act, a committee is given the power to inspect, block and delete content and anyone entering forged or false information into a computer could face a five-year jail sentence.

[1] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opsingle-gateway/
[2] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opsinglegateway-summer/

Figure 2: @AnonPlus_Info in #OpSingleGateway

OpCatalonia[3]

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 the law enforcement presence in Catalonia. As a result, the hacktivist group Anonymous launched a series of cyberattacks against Spanish institutions by targeting websites and networks of Spanish institutions. In this operation, hacktivists exploited the CMS WordPress. The AnonPlus IRC, webchat.anonplus.org, was used to host channels such as #opcatalunya, #freecatalonia and #catalunya.

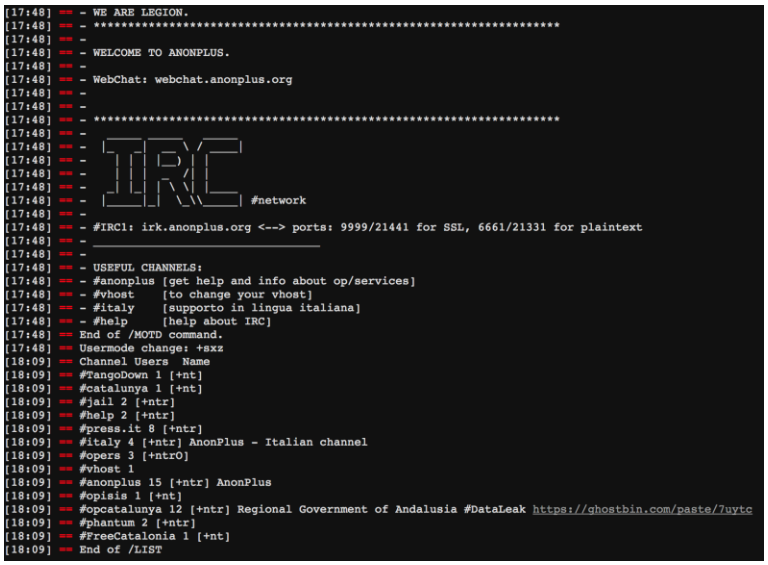

Figure 3: Old AnonPlus IRC hosting OpCatalunya channels

Current Campaign

Since 2018, AnonPlus Italia has been involved in political hacktivism as they target the Italian government. On February 6, AnonPlus attacked the website of Milan and leaked personal data from the Florence Democratic Party. The leak has provoked an internal debate within the Anonymous collective since it contained information of innocent citizens. After the data was posted on the AnonPlus IRC, the server was taken offline.

Following the leak, AnonPlus's main twitter account, @AnonPlus_info, was suspended and they decided to stop using social networks all together. Instead, they created their own website and on March 11, 2018, AnonPlus Italia announced their return with a new manifesto posted on their domains, Anonplus.tk and Anonplus.rf.gd. Today they use these domains to host information about recent attacks. Their new IRC now resides at webchat.anonplus.cf.

[3] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opcatalunya-phase4/

AnonPlus Italia defaced two websites on April 20, including a new manifesto and advertisement for their new IRC. Over the next six days, AnonPlus Italia would claim responsibility for defacing 21 websites, 20 of which use the CMS Drupal.

The Drupal (a popular open-source CMS) security team released a patch for a critical remote code execution (RCE) against Drupal on March 29, 2018 that allows attackers to execute arbitrary code on unpatched servers as a result of an issue affecting multiple subsystems with default or common module configurations in Drupal[4]. A remote attacker can construct a request with malicious content to exploit the vulnerability. A successful exploitation may lead to remote code injection on a Drupal server.

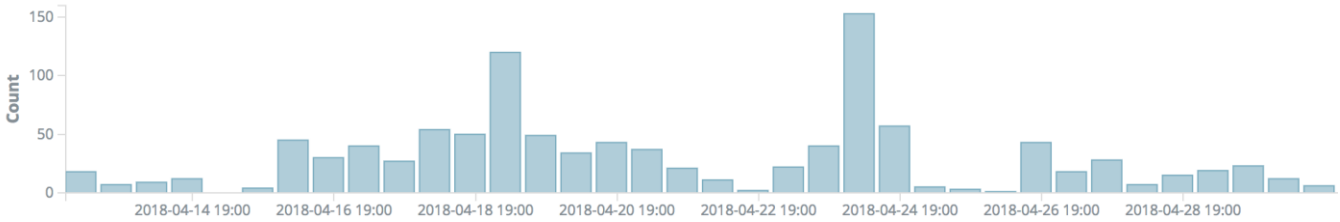

Figure 4: Activity following publication of exploit for CVE-2018-7600 on April 13th

Exploited Vulnerabilities and CVEs

Exploits for CVE-2018-7600[5] were posted to Github and Exploit-DB under the guise of education purposes only. The first PoC was posted to Exploit DB[6] on April 13, 2018. On April 14, Legion B0mb3r, a member of the Bangladesh-based hacking group Err0r Squad, posted a video to YouTube[7] demonstrating how to use this CVE-2018-7600[8] exploit to deface an unpatched version of Drupal. On April 17, a Metasploit[9] module was also released to the public.

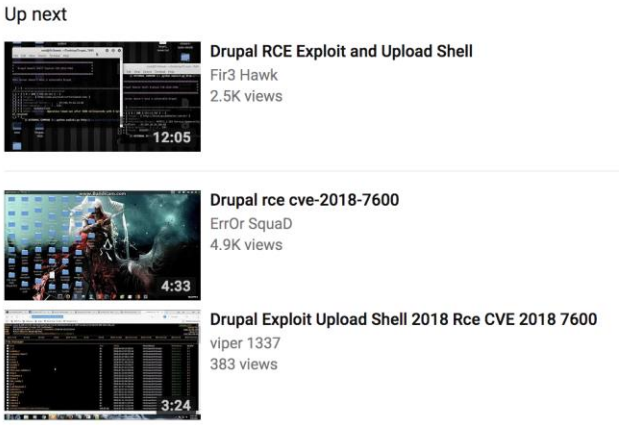

Figure 5: Tutorials on YouTube

Running an RCE attack for the purpose of defacing a Drupal website is easy. All the attacker requires is a predefined list of targeted websites that have not updated to the latest version of Drupal. Google advance search locates a CMS based on key terms and refines the search to a specific region. Once the attacker creates a list, they run an attack script that automates the rest of the process. The script will exploit the list of outdated Drupal websites and upload the defaced content.

[4] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/ert-alert-drupalgeddon/
[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7600
[6] https://www.exploit-db.com/exploits/44448/
[7] https://www.youtube.com/watch?v=45eJEGes2K8
[8] https://www.exploit-db.com/exploits/44448/
[9] https://www.exploit-db.com/exploits/44482/

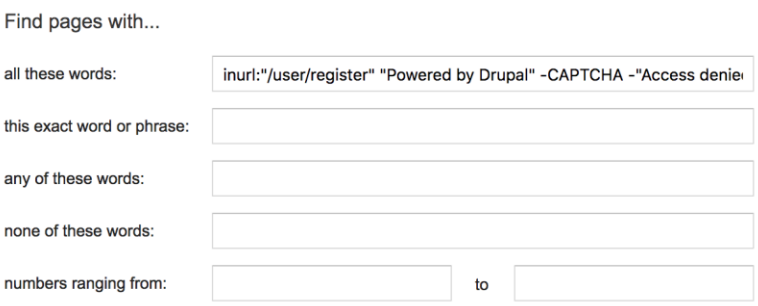

Figure 6: Google Dork for Drupal

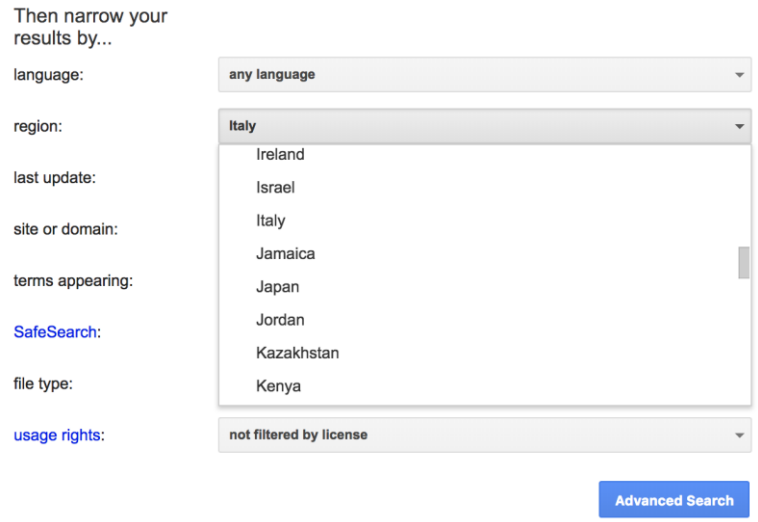

Figure 7: Refining search to a region

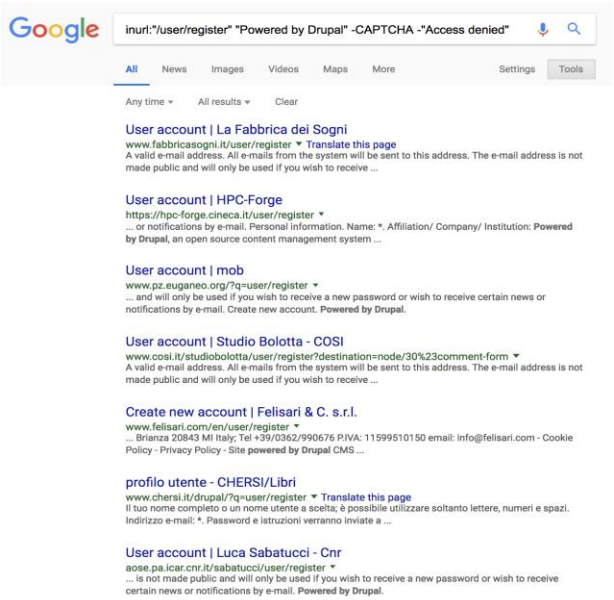

Figure 8: List of Drupal sites in Italy

In May, AnonPlus Italia executed 27 more defacements, of which 19 were Drupal. AnonPlus's May campaign started on May 2 and is ongoing as of this writing. One day prior to the end of their April campaign, Drupalgeddon 3 was disclosed. CVE-2018-7602 / SA-CORE-2018-004[10] is a remote code execution vulnerability[11] that exists within multiple subsystems of Drupal 7.x and 8.x. It allows the attacker to control the Drupal site[12]. Content management systems like WordPress and Joomla are normally abused by Anonymous hacktivists to target other web servers. In this recent string of defacements, the group AnonPlus Italia is abusing misconfigured or unpatched CMS instances with remote code exploits, allowing them to upload shells and deface unmaintained websites. Over the last 60 days, AnonPlus is targeting websites that use Drupal.

AnonPlus Manifesto and Defacement

Figure 9: The mission statement of AnonPlus

Application Attack Methods

Remote Code Execution – In an RCE 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.

[10] https://www.drupal.org/sa-core-2018-004
[11] https://www.exploit-db.com/exploits/44542/
[12] https://www.bleepingcomputer.com/news/security/hackers-dont-give-site-owners-time-to-patch-start-exploiting-new-drupal-flaw-within-hours/

Data Theft – Compromising sensitive data while data at rest or in transit by stealing encryption keys, hashed passwords, or by clearing text data off the server or a user's browser.

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 and RCE attacks.

Recently Targeted Sites

- https://registro-gts.vvf.to.it/
- https://www.gsnmagazine.com/
- http://www.telugudesam.org/
- https://www.lollandsbank.dk/
- https://www.csb.co.in/
- https://www.ghana.accessbankplc.com
- https://kr-binary.bknbank.com/
- http://www.deliverthepost.com/
- http://www.workerscomp.state.nm.us/
- http://workerscomp.newmexico.gov/
- https://workerscomp.nm.gov/
- https://fondosicurezzainterna.interno.gov.it/it
- http://www.vvftrento.it/
- https://legislature.idaho.gov/sessioninfo/2009/legislation/h0176/anonplus.html
- https://infragard-ct.org/
- https://secure.infragard-ct.org/
- http://www.suacalabria.it/
- http://legislature.idaho.gov
- https://icourt.idaho.gov/
- http://www.fisascat.it/
- https://www.dovesiamonelmondo.it/
- http://www.k9webprotection.com
- http://www.confind.emr.it/
- http://www.confindustrialiguria.it/
- http://www.cal.liguria.it/
- http://istruzione.provincia.genova.it/
- http://www.cittametropolitana.genova.it/

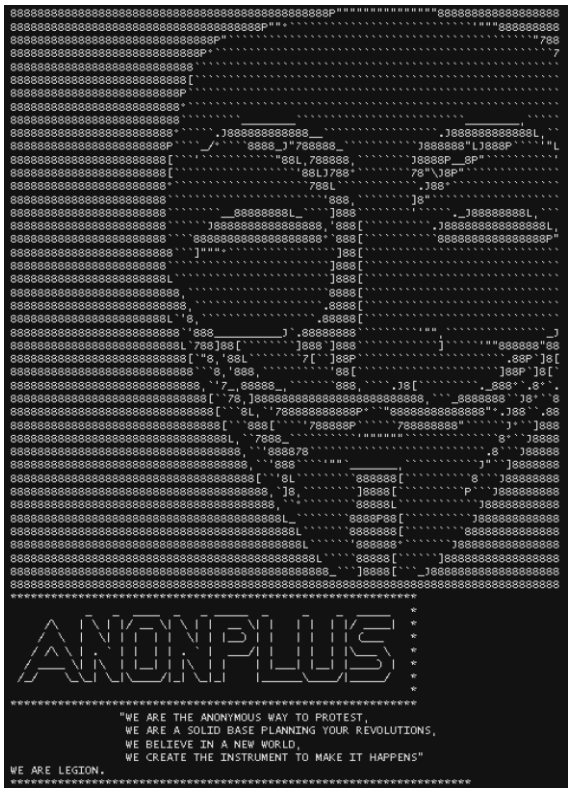

Figure 10: AnonPlus IRC: http://webchat.anonplus.cf

Recommendations

Radware's recommendation is to upgrade to the patched release most closely related to your current version.

- The current stable version of Drupal for Drupal 8 users at the time of writing is Drupal 8.5.3.
- The current stable version of Drupal for Drupal 7 users at the time of writing is Drupal 7.59.

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 network and application 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 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.