Abstract

Donald Trump and his presidential campaign has gained a new round of attention from the Anonymous collective. Throughout March, a planned cyber-assault against the presidential candidate provoked a debate within the US Anonymous community over political affiliation. The original intention was to attack Donald Trump and "erase his online footprint." While some groups chose to remain unaffiliated, others – such as RedCult - still plan to launch cyber-attacks against the presidential candidate, threatening to re-launch Anonymous's previous OpTrump campaign that took place in December of 2015.

Trump's case suggests that every person with power and influence is the subject to a potential resistance from hacktivists and should have a cyber-attack mitigation plan in place to protect personal and business holdings. By nature, political defiance may result in ongoing, continuous attempts.

This alert outlines the development of the events, describes the intentions and capabilities of the parties involved, and recommends steps of prevention and mitigation.

Background

March 4th 2016

On March 4, a group inside of Anonymous attempted to re-launch OpTrump, an operation that was originally launched on December 11, 2015. The goal was to expose Donald Trump's personal information and take down the presidential candidate's online footprint. The relaunch of the operation was intended to attack Donald Trump's websites, specifically TrumpChicago.com on April 1, with a series of network- and application-layer attacks that would include DDoS and SQL injections. The group behind this operation published a video to YouTube[i] as well several pastes on Pastebin and Ghostbin[ii] (see Figure 1).

Figure 1: Ghostbin paste about OpTrump

Some of the websites on the target lists included:

- https://www.donaldjtrump.com
- http://www.trump.com
- https://www.trumphotelcollection.com
- http://www.trumptowerny.com
- http://www.trumpvegascondos.com
- http://www.trumpchicago.com
- http://www.donaldtrump2016online.com
- http://citizensfortrump.com

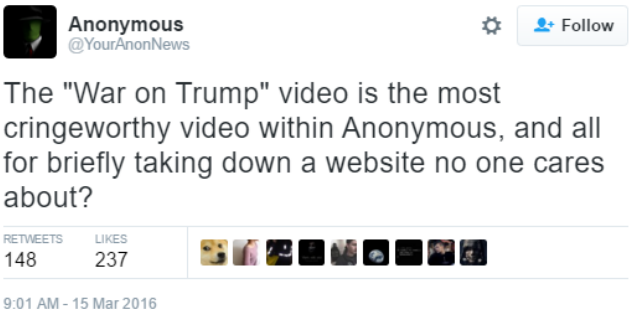

Figure 2: YourAnonNews comments on OpTrump

March 5th – 15th 2016

During this time period, Anonymous began to fight internally about other Anonymous accounts supporting politicians and the legitimacy of certain operations. The main consensus inside Anonymous appears to be that while there is no leader and any Anon can support whoever they want, Anonymous as a whole does not support or endorse any candidate.

Figure 3: Example of an Anonymous member supporting a political figure

March 16th 2016

Main Anonymous accounts began announcing that the re-launch of OpTrump was terminated (see Figure 3). In a video posted to YouTube[iii], Anonymous states that this operation will not accomplish anything and will not remove Donald Trump from the election. They are now asking Anonymous members to redirect and protest against the system as a whole vs a single political candidate.

Figure 4: Sandy, a member of New World Hackers, has called off their threat of a 1Tbps attack.

March 17th 2016

On March 17, an Anonymous group called RedCult[iv] launched OpWhiteRose, a reference to the resistance group that operated during the Second World War. The operational plan was to launch a campaign against Donald Trump and fascism in the US. RedCult is a fairly well known group inside of Anonymous and known for being the originators behind OpISIS. Their release includes a video on YouTube[v], along with Donald Trump's alleged personal information on pase sites. Analysis by Radware has revealed that the released information from the Dox (which included Trump's social security number, date of birth, cellphone, and addresses) was extracted from a previous Dox in 2013 (see Figure 4).[vi]

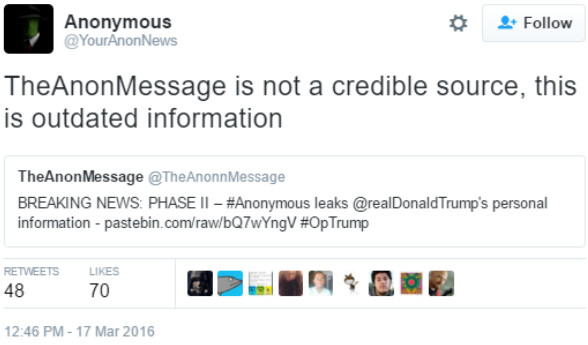

Figure 5: YourAnonNews referencing the outdated dox from RedCult being circulated

Attack Vectors

- **UDP flood**-Sending large UDP packets, in most cases with spoofed SRC IP (fairly easy since the UDP protocol does require a "handshake"). Normally used to saturate the Internet pipe.
- **TCP flood**-Sending numerous SYN packets to the victim with spoofed SRC IP so the reply will not return to the attacker. The intention is to overwhelm the server's session/connection tables.
- **SQL Injection**-Modify an application SQL query in order to gain unauthorized access to data or run malicious programs.
- **Brute-Force**-Compromising encrypted data by systematically checking all possible combinations until the correct encryption key is found.

Reasons for Concern

Currently, it's unclear how OpTrump will play out. The attempt by Anonymous to terminate OpTrump can play out in two different ways. First, those that have committed to the operation will fully commit and successfully take down the site, even if its temporary, without the main collective's support. Second is the complete abandonment resulting in a failed operation.

Anonymous is no stranger to failed operations. OpFacebook[vii] failed to be a day that "went down in history" and most recently OpParis deteriorated quickly as Anonymous lacked the ability to verify suspected ISIS accounts. This led to non-ISIS accounts being reported incorrectly as terrorist.

Sometimes operations have ulterior motives, resulting in failure. Some of these motives include driving membership towards an attack service like booters and stressers run by the operator or subverting others into carrying out an attack for them (see Figure 5). If the operator is unable to persuade others into joining the operation its will ultimately fail.

Figure 6: Comment about operations leading to booter membership

What's Expected Next

This year, government and political candidates have been targeted and threatened via various campaigns carried out by both hacktivist and terrorist groups responding to political change. Attacks on government and political sites are not always politically motivated; many attacks are launched so that attackers gain notoriety for publically shaming the government or a political site.

Modern day protests take place as aggressively online in the form of network and application attacks as they do in person. 2016 presidential campaigns should expect and be prepared for cyber-attack.

It is expected that as the United States presidential election continues, nominees for each party will see an increase in cyber-attacks against selected candidates. These threats could include DDoS attacks via booters and stressers and application layer attacks via SQL injections.

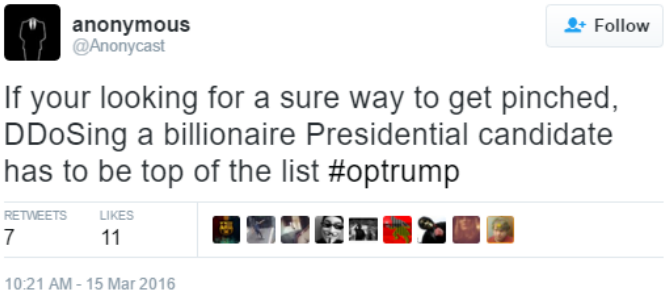

Figure 7: Comment about OpTrump

How to Prepare

While it is impossible to predict the next target of an ideological group such as Anonymous, expect to see more activity and further attack campaigns during the U.S. election. Candidates and political figures should be on high alert and make sure campaign websites and online assets are protected. In addition, organizations involved in supporting, hosting or delivering IT services to political figures in the U.S. election should proactively prepare their networks and have an emergency plan in place for such an incident.

Organizations Under Threat Should Consider

Effective **DDoS protection** elements:

- A hybrid solution that includes on premise detection and mitigation with cloud-based protection for volumetric attacks. This provides quick detection, immediate mitigation and protects networks from volumetric attacks that aim to saturate the Internet pipe.
- Solution must distinguish between legitimate and malicious packets, protecting the SLA while rejecting attack traffic
- An integrated, synchronized solution that can protect from multi-vector attacks combining DDoS with web-based exploits such as website scraping, Brute Force and HTTP floods.
- A cyber-security emergency response plan that includes an emergency response team and process in place. Identify areas where help is needed from a third party.

Effective Web Application protection elements (against web intrusions, defacement and data leakage):

- IP-agnostic device fingerprinting – Having the ability to detect attacks beyond source-IP using by developing a device fingerprint that enables precise activity tracking over time
- Automatic and real time generation of policies to protect from 0-day, unknown attacks
- Shortest time from deployment to a full coverage of OWASP Top-10

Radware's hybrid attack mitigation solution provides a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced threats. Dedicated hardware and cloud solutions protect against attacks in real time and help ensure service availability.

Need an Expert Emergency Assistance?

Radware offers a full range of solutions to help networks properly mitigate attacks similar to these. Our attack mitigation solutions provide a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced DDoS attacks and cyber threats. With dedicated hardware, fully managed services and cloud solutions that protect against attacks, Radware can help ensure service availability. To understand how Radware's attack mitigation solutions can better protect your network contact us today.

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. Radware does not condone any illegal use of anyone's information.

---

[i] https://youtu.be/Ciavyc6bE7A
[ii] https://ghostbin.com/paste/28abm
[iii] https://youtu.be/KE0vMsR87ww
[iv] https://www.facebook.com/anonymousredcultofficial/
[v] https://youtu.be/3UXQpfm_Ytw
[vi] http://pastie.org/pastes/7928699
[vii] https://youtu.be/h6dBZQfpQao