ERT Threat Alert
Operation Trump

Operation Trump Background

On December 11, 2015 Anonymous announced Operation Trump (#OpTrump), a three phase hacking campaign[1] to “expose the real Donald Trump” and take down the presidential candidate’s online footprint.[2]

Campaign Phases

Phase 1: Ideological Hacking ─ An important aspect of this operation used to directly impact voter opinions. "Trolling" will be primarily managed by this sector on social media using the hashtag #OpTrump on Twitter with plans to release additional hashtags in the future. The main goal is to provoke Trump and add doubt to his supporters with memes, mocking, and spamming hashtags. Because of Trump’s Twitter presence, Anonymous will attempt to contact Trump and get him to acknowledge and respond. This sector also plans to concentrate on the creation of media for this op, including management of the official Twitter page: https://twitter.com/OpTrumpOfficial.

Phase 2: Penetration ─ Also an important point, this will be for the more advanced anons who have much more experience in information security. Primarily people working in this aspect will attempt to gather information that Trump would not want publicized. Information gathering includes inspection of public speeches, and extracting emails from personal and enterprise mail servers. The information gathered will be released in the third sector of this operation.

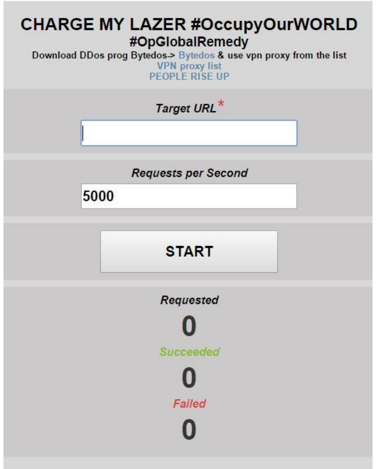
Phase 3: Exposition of Information ─ The most humorous section of this operation will coordinate the information released to the public. This includes coordination, compilation, and eventually release of information that was gathered in section two. Information will be released via YouTube, Twitter, and other social media sites.

“Day of Rage”

In addition, Anonymous is planning a ‘Day of Rage’ on December 18t, 2015 at 9pm UTC. Similar to OpParis and OpISIS, Anonymous will be trolling, attacking and issuing ‘counter propaganda’ about Donald Trump. Details about the attack will not be published until it begins. On December 18 Anonymous will also release formal attack plans along with additional information regarding the Op. Anonymous is looking for public support in trolling Donald Trump that is likely due to the lack of attention the operation has garnered thus far.

Tools Being Used

- Tor
- Pyloris - https://github.com/AnonymousTools/Pyloris-enhanced
- WebHive - hxxp://pastehtml.com/view/ct6qaqwp6.html



CHARGE MY LAZER #OccupyOurWORLD
#OpGlobalRemedy
Download DDos prog Bytedos-> Bytedos & use vpn proxy from the list
VPN proxy list
PEOPLE RISE UP

*Target URL**

Requests per Second
5000

Requested
0
Succeeded
0
Failed
0

Figure 1 WebHive tool

Links

- https://justpaste.it/OpTrump
- https://youtu.be/eSnOwUE5Fro - Offical Video
- https://twitter.com/OpTrumpOfficial
- http://usuncut.com/resistance/anonymous-begins-optrump/ - News
- https://webchat.anonops.com/?channels=OpTrump - IRC

Targets

- www.trumptowerny.com
- https://secure.donaldjtrump.com 104.130.250.119
- www.donaldjtrump.com
- shop.donaldjtrump.com
- www.trumphotelcollection.com
- www.trumphotels.com
- www.trumpinternationalrealty.com
- www.trumpsoho.com
- www.trumpsohohotel.com
- www.thetrumpcard.com
- www.trumpatrium.com
- www.40wallstreet.com
- www.trump.com

Future Op and Targets

#OpHillary / #HillaryClinton

- www.hillaryclinton.com
- shop.hillaryclinton.com
- www.hillary.org

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 potential attack campaigns during the U.S. election period. 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 cycle should proactively prepare networks and have an emergency plan in place for such an incident.

Organizations under Attack Should Consider

- A security solution that can protect its infrastructure from multi-vector attacks including protection from network and application based DDoS attacks as well as volumetric attacks that can saturate the Internet pipe
- 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.
- A solution that provides protection against sophisticated web-based attacks and web site intrusions to prevent defacement and information theft.
- 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.
- Monitor security alerts and examine triggers carefully. Tune existing policies and protections to prevent false positives and allow identification of real threats if and when they occur.

Radware offers a full range of solutions to help networks properly mitigate attacks similar to these. Our attack mitigation solution provides 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.

Sources

1. https://ghostbin.com/paste/ejbsh
2. Wired, Anonymous Launches #OpTrump to Teach Donald a Lesson, December 2015