Abstract

Since our previous ERT alert outlining the potential cyber-attack against Donald Trump on April fool's day, the presidential candidate was eventually hit and online entities of key Trump properties were taken offline as of Friday, April 1st 2016. The day before, members of the Anonymous collective stated that the planned attack[i] on Donald Trump was a ploy and symbolically planned for April 1st to gain public attention for the operation. Shortly after the paste was posted, another Anonymous member posted a paste to Ghostbin disregarding the previous paste and announcing OpTrump2016[ii] and their plans to DDoS Donald Trump's website.

This alert provides details on the attack tools and vectors as well as guidance on how organizations can keep their networks and applications protected from these types of attacks.

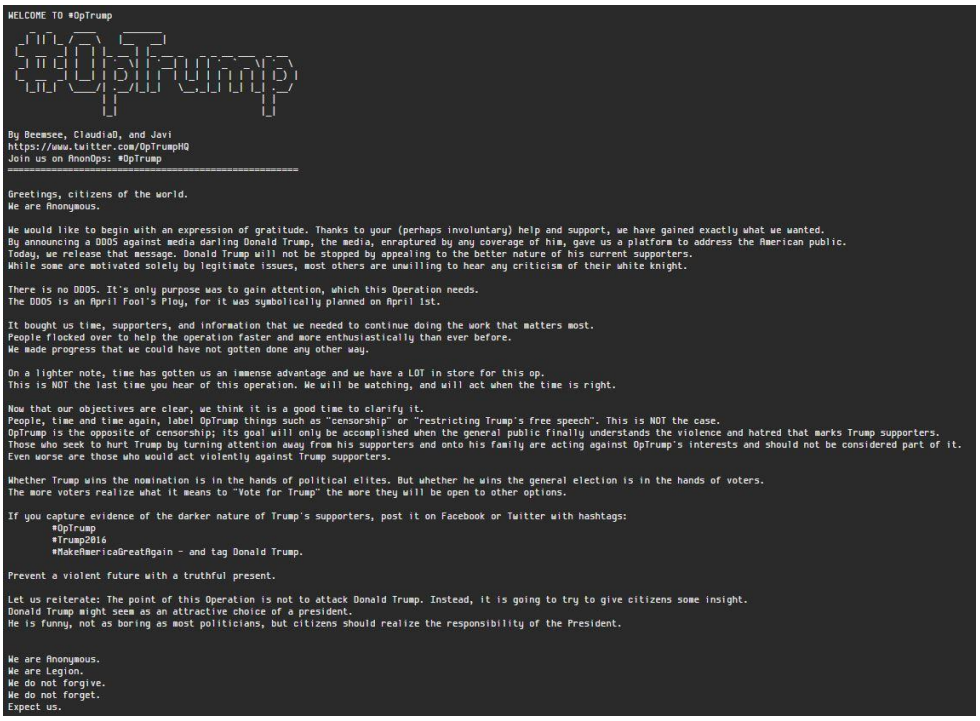

Figure1: OpTrump - April fool's

Background

On March 23, an ERT alert was issued regarding a planned attack against the presidential candidate and how it provoked a debate within the US Anonymous community and the possible outcomes for a planned cyber-assault on April 1st. The original goal was to relaunch OpTrump and specifically target TrumpChicago.com. On March 31st, members of the Anonymous collective posted a paste on Ghostbin[iii] stating the main purpose of the troll was to gain media attention and no DDoS attacks would be conducted. It also stated that this part of the operation bought them time, supporters and information. Attackers have claimed the operation is not over and future attacks are planned. At the end of the paste, authors asked anyone with "evidence of the darker nature of Trump's supporters" post it on Facebook and Twitter with the hashtags #OpTrump, #Trump2016, and #MakeAmericaGreatAgain.

```
#OpTrump2016

There was recently an announcement by Beemsee which concludes that the DDOSing factor of this operation was a publicity stunt.
This was not the intention when I re-engaged this operation. The original target of www.TrumpChicago.com
was briefly taken down yet without the assistance of the the #OpTrump channel the site was up in no time. When/If we get enough
people to join #OpTrump2016 we will attempt to DDOS a given website.
```

Figure 2: OpTrump2016

Shortly after this paste was posted, Anonymous Loyalist, posted a paste on Ghostbin disregarding the previous paste and announced OpTrump2016, an attempt to DDoS Donald Trump's websites. Anonymous Loyalist has organized in the AnonOps IRC channel, #Trump2016, which averages about 30 attackers within the IRC chat at any given time. Within the IRC, discussions include what attack vectors should be used and suggested VPNs. Some of the tools being used for OpTrump2016 include Metasploit, Nmap, Hping3, TorsHammer, UFonet and SlowLoris. Hotspot Shield and Cyber Ghost VPN services have also been mentioned as ways to mask their identities.

Groups like the New World Hackers are using booters capable of pushing over 150Gbps in network capacity. These attackers are also able to resolve and locate the origin server's IP address. This operation's first target was CitizensForTrump.com. The group was able to take the site offline for 45 minutes. Since then they have also managed to target and take down TrumpHotelCollection.com and TrumpInitiative.com.

Figure 3: CitizensForTrump.com Down

Figure 4: CitizensForTrump.com Error

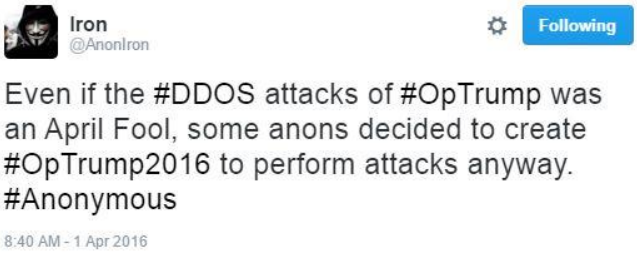

Figure 5: OpTrump2016 replacing OpTrump2016

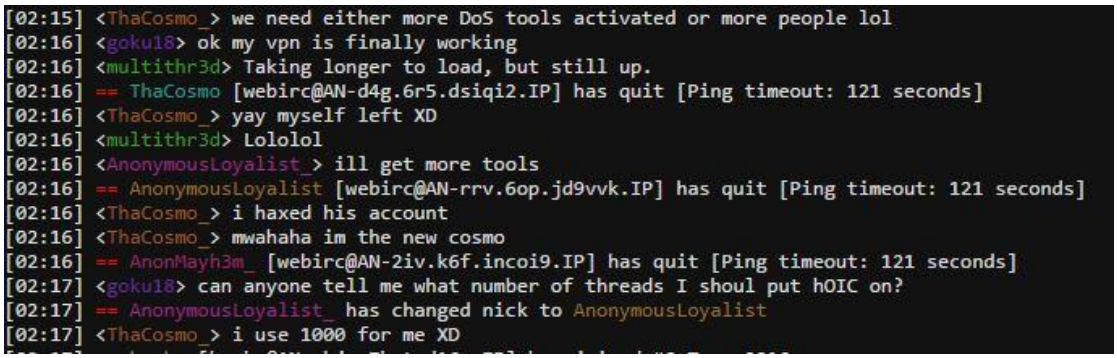

Figure 6: #OpTrump2016 IRC chat about the use of HOIC

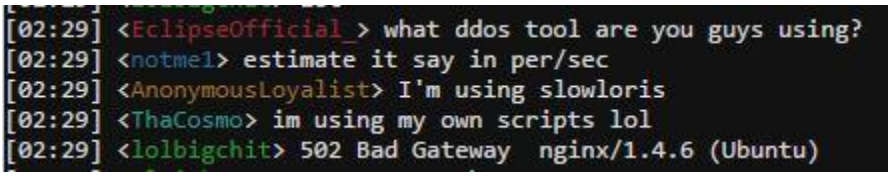

Figure 7: #OpTrump2016 IRC chat about the use of SlowLoris

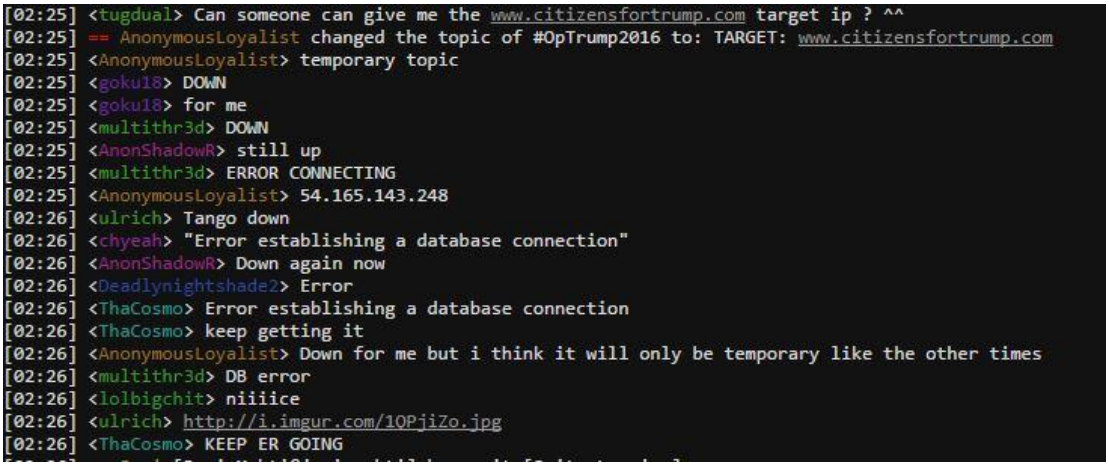

Figure 8: #OpTrump2016 IRC chat about targeting CitizensForTrump.com

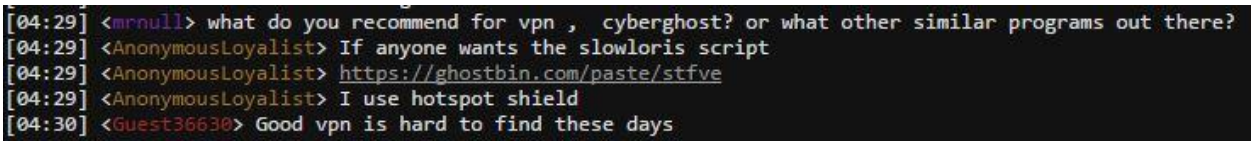

Figure 9: #OpTrump2016 IRC chat about suggested VPN services

Figure 10: New World Hacking claims to have taken down Trump.com

Figure 11: New World Hacking claims to have taken down TrumpChicago.com

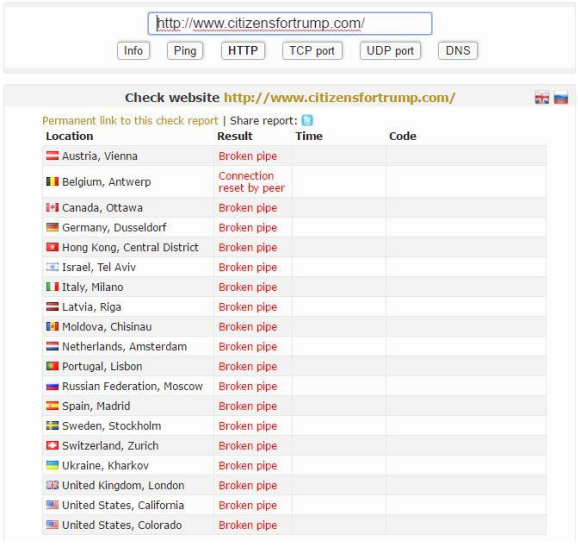

Figure 12: CitizensForTrump.com Down

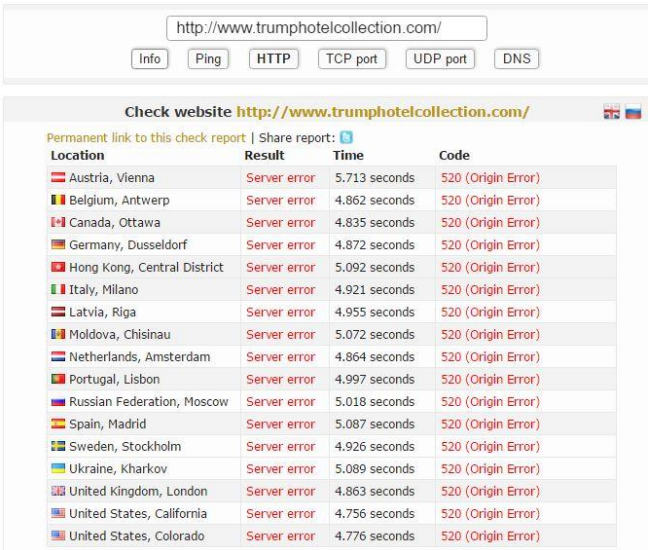

Figure 13: TrumpHotelCollection.com Down

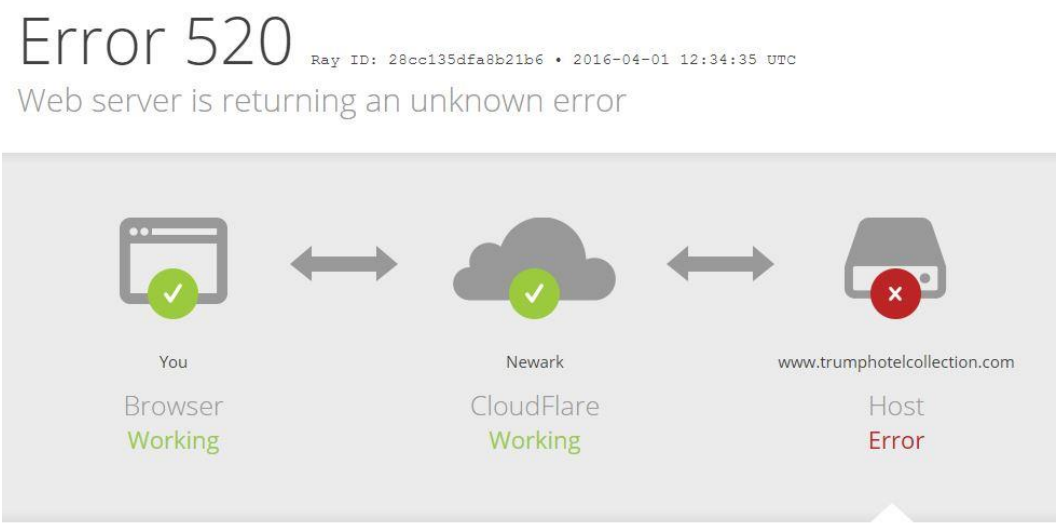

Figure 14: TrumpHotelCollection.com Down

Targets[iv] [v] [vi]

- Trump.com
- TrumpChicago.com
- Mail.trump.com
- Mail.trumpac.com
- DonaldJTrump.com
- CitizensForTrump.com
- TrumpHotelCollection.com
- Trumpinitiative.com
- Trumporg.com

Attack Tools

- Metasploit
- LOIC
- HOIC
- Hping3
- TorsHammer
- SlowLoris
- UFonet
- Booter/Stresser (+150gbps)

IRC Chat

- https://webchat.anonops.com/ #OpTrump2016

Reasons for Concern

Anonymous has a very strong influence on over-sensationalized hacktivists looking for a cause. Even after the planned attack for April 1st was called off, Anon's formed a new Operation, OpTrump2016, and followed through on the threat to attack Trump's websites.

OpTrump is not the only anti-Trump operation currently running. The Anonymous group Redcult is also running OpWhiteRose in parallel. It is expected that these attacks will continue throughout the day. Donald Trump's websites could expect to see an increase in DDoS attacks via booters and stresser as more attackers come online. These websites could also see application layer attacks via SQL injections.

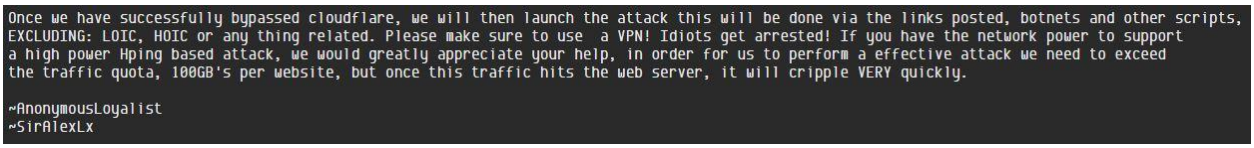

Figure 15: OpTrump2016 now recommending not to use LOIC, HOIC or anything related.

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 attacks during the day. Donald Trump, as well as other 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 Attack 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.

Under Attack and in Need of 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.

---

[i] https://ghostbin.com/paste/exs77
[ii] https://ghostbin.com/paste/cohqo
[iii] https://ghostbin.com/paste/b24pu
[iv] https://ghostbin.com/paste/3ebpe
[v] https://ghostbin.com/paste/zy3gr
[vi] https://ghostbin.com/paste/9bddm