

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 attackⁱ 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 OpTrump2016ⁱⁱ 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.

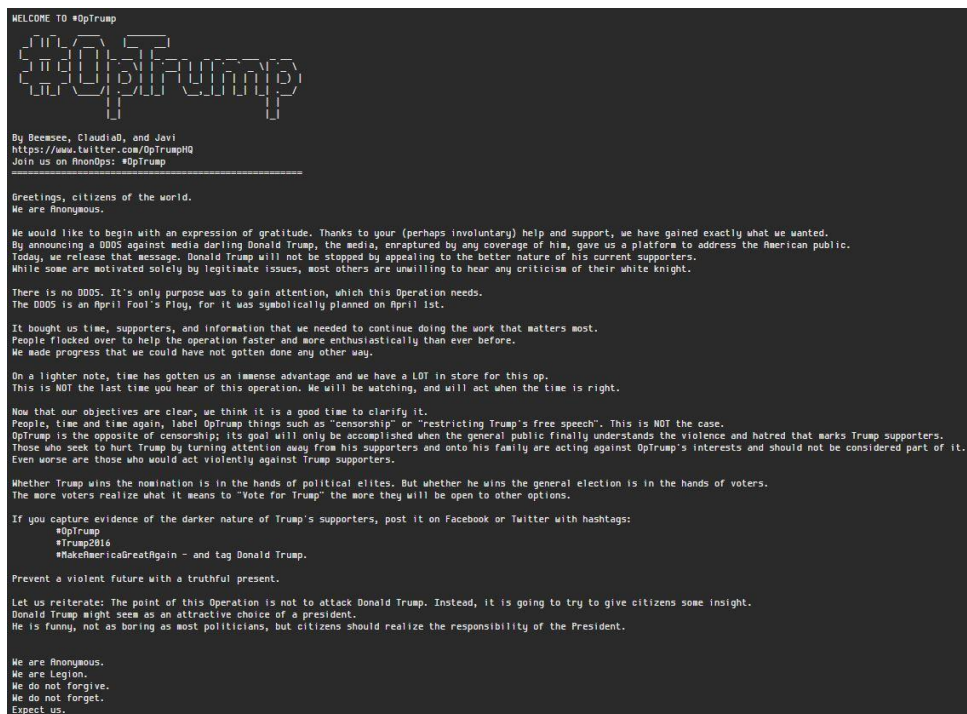


Figure1: OpTrump - April fool's

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 Ghostbinⁱⁱⁱ 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.

```

1 #OpTrump2016
2
3 There was recently an announcement by Beemsee which concludes that the DDOSing factor of this operation was a publicity stunt.
4 This was not the intention when I re-engaged this operation. The original target of www.TrumpChicago.com
5 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
6 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



Error establishing a database connection

Figure 4: CitizensForTrump.com Error

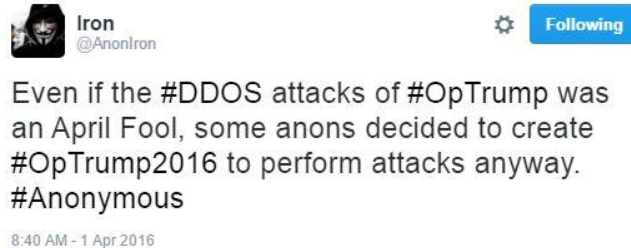


Figure 5: OpTrump2016 replacing OpTrump2016

```
[02:15] <ThaCosmo_> we need either more DoS tools activated or more people lol
[02:16] <goku18> ok my vpn is finally working
[02:16] <multithr3d> Taking longer to load, but still up.
[02:16] == ThaCosmo [webirc@AN-d4g.6r5.dsiqi2.IP] has quit [Ping timeout: 121 seconds]
[02:16] <ThaCosmo_> yay myself left XD
[02:16] <multithr3d> Lololol
[02:16] <AnonymousLoyalist_> ill get more tools
[02:16] == AnonymousLoyalist [webirc@AN-rrv.6op.jd9vvk.IP] has quit [Ping timeout: 121 seconds]
[02:16] <ThaCosmo_> i haxed his account
[02:16] <ThaCosmo_> mwahaha im the new cosmo
[02:16] == AnonMayh3m [webirc@AN-2iv.k6f.incoi9.IP] has quit [Ping timeout: 121 seconds]
[02:17] <goku18> can anyone tell me what number of threads I shoul put hOIC on?
[02:17] == AnonymousLoyalist_ has changed nick to AnonymousLoyalist
[02:17] <ThaCosmo_> i use 1000 for me XD
```

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

```
[02:29] <EclipseOfficial_> what ddos tool are you guys using?
[02:29] <notme1> estimate it say in per/sec
[02:29] <AnonymousLoyalist> I'm using slowloris
[02:29] <ThaCosmo> im using my own scripts lol
[02:29] <lolbigchit> 502 Bad Gateway nginx/1.4.6 (Ubuntu)
```

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

```
[02:25] <tugdual> Can someone can give me the www.citizensfortrump.com target ip ? ^^
[02:25] == AnonymousLoyalist changed the topic of #OpTrump2016 to: TARGET: www.citizensfortrump.com
[02:25] <AnonymousLoyalist> temporary topic
[02:25] <goku18> DOWN
[02:25] <goku18> for me
[02:25] <multithr3d> DOWN
[02:25] <AnonShadowR> still up
[02:25] <multithr3d> ERROR CONNECTING
[02:25] <AnonymousLoyalist> 54.165.143.248
[02:26] <ulrich> Tango down
[02:26] <chyeah> "Error establishing a database connection"
[02:26] <AnonShadowR> Down again now
[02:26] <Deadlynightshade2> Error
[02:26] <ThaCosmo> Error establishing a database connection
[02:26] <ThaCosmo> keep getting it
[02:26] <AnonymousLoyalist> Down for me but i think it will only be temporary like the other times
[02:26] <multithr3d> DB error
[02:26] <lolbigchit> niiice
[02:26] <ulrich> http://i.imgur.com/10PjiZo.jpg
[02:26] <ThaCosmo> KEEP ER GOING
```

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

```
[04:29] <mrnull> what do you recommend for vpn , cyberghost? or what other similar programs out there?
[04:29] <AnonymousLoyalist> If anyone wants the slowloris script
[04:29] <AnonymousLoyalist> https://ghostbin.com/paste/stfve
[04:29] <AnonymousLoyalist> I use hotspot shield
[04:30] <Guest36636> Good vpn is hard to find these days
```

Figure 9: #OpTrump2016 IRC chat about suggested VPN services

Trump.com is now #TangoDown as expected.
#OpTrump
#AnonFamily
#IntelGroup
#Nulled
#NwHackers

Location	Result	Time	Code
Austria, Vienna	Server error	0.327 seconds	403 (Forbidden)
Belgium, Antwerp	Server error	0.120 seconds	403 (Forbidden)
Canada, Ottawa	Server error	0.851 seconds	502 (Origin Error)
Germany, Dusseldorf	Server error	0.158 seconds	403 (Forbidden)
Hong Kong, Central District	Server error	0.161 seconds	403 (Forbidden)
Israel, Tel Aviv	Server error	0.364 seconds	403 (Forbidden)
Italy, Milano	Server error	0.250 seconds	403 (Forbidden)
Latvia, Riga	Server error	0.283 seconds	502 (Origin Error)
Moldova, Chisinau	Server error	0.190 seconds	403 (Forbidden)
Netherlands, Amsterdam	Server error	0.289 seconds	403 (Forbidden)
Portugal, Lisbon	Server error	0.477 seconds	403 (Forbidden)
Russian Federation, Moscow	Server error	0.481 seconds	403 (Forbidden)
Spain, Madrid	Server error	0.124 seconds	403 (Forbidden)
Sweden, Stockholm	Server error	0.380 seconds	403 (Forbidden)
Switzerland, Zurich	Server error	0.283 seconds	403 (Forbidden)
Ukraine, Kharkov	Server error	0.372 seconds	403 (Forbidden)
United Kingdom, London	Server error	0.128 seconds	502 (Origin Error)

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

TrumpChicago.com is now #TangoDown as expected.
#OpTrump
#AnonFamily
#IntelGroup
#NwHackers

Location	Result	Time	Code
Austria, Vienna	Server error	0.309 seconds	502 (Origin Error)
Belgium, Antwerp	Server error	0.120 seconds	502 (Origin Error)
Canada, Ottawa	Server error	0.726 seconds	502 (Origin Error)
Germany, Dusseldorf	Server error	0.178 seconds	502 (Origin Error)
Hong Kong, Central District	Server error	0.423 seconds	502 (Origin Error)
Israel, Tel Aviv	Server error	1.021 seconds	502 (Origin Error)
Italy, Milano	Server error	0.106 seconds	502 (Origin Error)
Latvia, Riga	Server error	0.285 seconds	502 (Origin Error)
Moldova, Chisinau	Server error	0.217 seconds	502 (Origin Error)
Netherlands, Amsterdam	Server error	0.175 seconds	502 (Origin Error)
Portugal, Lisbon	Server error	0.467 seconds	502 (Origin Error)
Russian Federation, Moscow	Server error	0.506 seconds	502 (Origin Error)
Spain, Madrid	Server error	0.120 seconds	502 (Origin Error)
Sweden, Stockholm	Server error	0.187 seconds	502 (Origin Error)
Switzerland, Zurich	Server error	0.126 seconds	502 (Origin Error)

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

Check website <http://www.citizensfortrump.com/>

Location	Result	Time	Code
Austria, Vienna	Broken pipe		
Belgium, Antwerp	Connection reset by peer		
Canada, Ottawa	Broken pipe		
Germany, Dusseldorf	Broken pipe		
Hong Kong, Central District	Broken pipe		
Israel, Tel Aviv	Broken pipe		
Italy, Milano	Broken pipe		
Latvia, Riga	Broken pipe		
Moldova, Chisinau	Broken pipe		
Netherlands, Amsterdam	Broken pipe		
Portugal, Lisbon	Broken pipe		
Russian Federation, Moscow	Broken pipe		
Spain, Madrid	Broken pipe		
Sweden, Stockholm	Broken pipe		
Switzerland, Zurich	Broken pipe		
Ukraine, Kharkov	Broken pipe		
United Kingdom, London	Broken pipe		
United States, California	Broken pipe		
United States, Colorado	Broken pipe		

Figure 12: CitizensForTrump.com Down

Check website <http://www.trumphotelcollection.com/>

Location	Result	Time	Code
Austria, Vienna	Server error	5.713 seconds	520 (Origin Error)
Belgium, Antwerp	Server error	4.862 seconds	520 (Origin Error)
Canada, Ottawa	Server error	4.835 seconds	520 (Origin Error)
Germany, Dusseldorf	Server error	4.872 seconds	520 (Origin Error)
Hong Kong, Central District	Server error	5.092 seconds	520 (Origin Error)
Italy, Milano	Server error	4.921 seconds	520 (Origin Error)
Latvia, Riga	Server error	4.955 seconds	520 (Origin Error)
Moldova, Chisinau	Server error	5.072 seconds	520 (Origin Error)
Netherlands, Amsterdam	Server error	4.864 seconds	520 (Origin Error)
Portugal, Lisbon	Server error	4.997 seconds	520 (Origin Error)
Russian Federation, Moscow	Server error	5.018 seconds	520 (Origin Error)
Spain, Madrid	Server error	5.087 seconds	520 (Origin Error)
Sweden, Stockholm	Server error	4.926 seconds	520 (Origin Error)
Ukraine, Kharkov	Server error	5.089 seconds	520 (Origin Error)
United Kingdom, London	Server error	4.863 seconds	520 (Origin Error)
United States, California	Server error	4.756 seconds	520 (Origin Error)
United States, Colorado	Server error	4.776 seconds	520 (Origin Error)

Figure 13: TrumpHotelCollection.com Down

Error 520

Ray ID: 28cc135dfa8b21b6 • 2016-04-01 12:34:35 UTC

Web server is returning an unknown error



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.

```
Once we have successfully bypassed cloudflare, we will then launch the attack this will be done via the links posted, botnets and other scripts, EXCLUDING: LOIC, HOIC or any thing related. Please make sure to use a VPN! Idiots get arrested! If you have the network power to support a high power Hping based attack, we would greatly appreciate your help, in order for us to perform a effective attack we need to exceed the traffic quota, 100GB's per website, but once this traffic hits the web server, it will cripple VERY quickly.  
~AnonymousLoyalist  
~SIRAIexLx
```

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 today's 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 today's 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>