Deloitte.

Threat Intelligence
and Analytics

Hacktivism

A defender's playbook

Threat study

Issue date: August 12, 2016 | **TLP:** White | **Serial:** W-TS-EN-16-00735 | **Industry:** All

Abstract

Hacktivism—The act of carrying out malicious cyber activity to promote a political agenda, religious belief, or social ideology.

As the cyber threat landscape continues to evolve, the ability to monitor, detect, and defend against cyberattacks has now become more arduous than ever. These cyberattacks have become more sophisticated, as are the actors behind them, and the tools, techniques, and procedures (TTPs) they use. Of the many cyber threats that our society faces, hacktivism continues to be one of the most significant.

Cyberattacks by hacktivists are at an all-time high. With the use of social media, hacktivists can now spread the word and recruit across the globe with a single tweet or a Facebook post to carry out their agenda driven attack. One of the most well-known hacktivist groups, 'Anonymous,' has been carrying out their cyber campaigns since 2003 and continue to be the most active and prominent hacktivist group. Understanding the mindset of a hacktivist is vital and although they stand for a certain "moral" cause, they are still hackers and some with elite hacking ability.

Because hacktivists attack targets based upon a certain cause, makes them much more unpredictable as attacks may have already commenced before the hacktivist group has announced their attack campaign. Based on previous campaigns, in most cases small and medium-sized organizations are hit the hardest by hacktivism because they aren't ready nor have the security infrastructure or intelligence-gathering capabilities to prepare and defend. Although state and local governments have begun to strengthen their security posture, they still aren't as prepared as they need to be defend against hacktivism.

Attribution of attacks to hacktivists is very difficult. Hacktivist groups such as Anonymous are a leaderless organization and anyone can be a member just by stating that you are a member. In such groups, anonymity is always emphasized to avoid attribution. In conjunction, hacktivists can take on distant causes without the need to travel which enables both individual actions and large-scale distributed attack efforts. Persons of a common nationality or united by a common cause, for example, can join together whether residing in their homeland or in a foreign country to carry out cyberattacks.

Hacktivism continues to be a major cyber threat across the globe. In order to prepare and defend against hacktivism, we must understand how hacktivists operate and the tactics they use to carry out their agenda. The purpose of this tactical guide is to arm your organization with the intelligence needed to know the adversary and their tactics and to implement the right security measures to help mitigate risk in your organization for today and for the future.

Table of contents

Attack Methodology

A Vicious Cycle

Like other cybercriminal groups or nation-state sponsored organizations, hacktivists use their own specific set of tools, techniques, and procedures, known as TTPs. To know the adversary, you need to understand their behaviors and modus operandi. Their TTPs provide the necessary information not only to understand how they operate, but also give you the insight into their cyber weapons, types of targets, and the vectors they use to carry out their attacks.

Understanding the hackvist's TTPs arms you with the ability to monitor, detect, and mitigate cyberattacks that can impact your organization.

In this section we will discuss the types of attacks, vectors, targets, and their intended effects. Hacktivists' attacks usually run a cyclical approach against their target. Although deviations may occur, most campaigns follow an attack cycle.

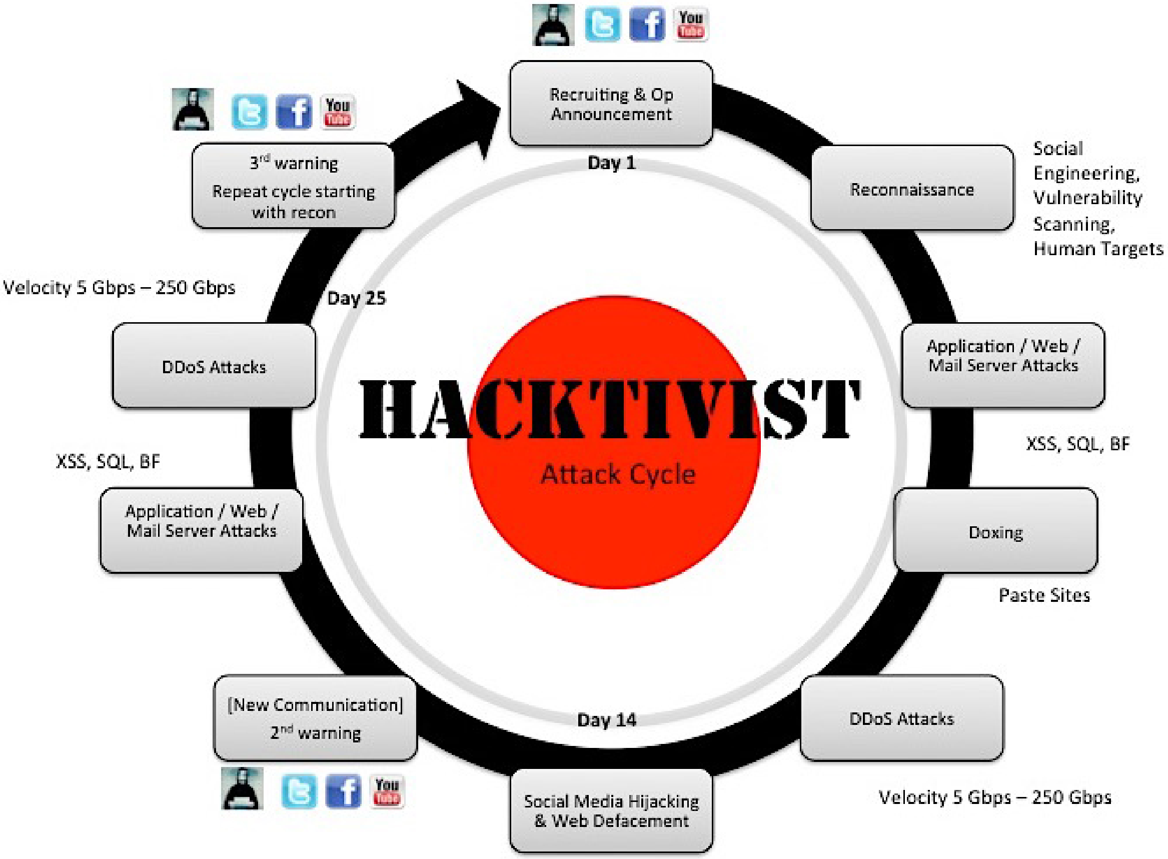

Recruiting & Op Announcement
Day 1
Reconnaissance
Social Engineering, Vulnerability Scanning, Human Targets
Application / Web / Mail Server Attacks
XSS, SQL, BF
Doxing
Paste Sites
DDoS Attacks
Velocity 5 Gbps – 250 Gbps
Social Media Hijacking & Web Defacement
Day 14
[New Communication] 2nd warning
Application / Web / Mail Server Attacks
XSS, SQL, BF
DDoS Attacks
Velocity 5 Gbps – 250 Gbps
Day 25
3rd warning Repeat cycle starting with recon
HACKTIVIST
Attack Cycle

Figure 1 - Average Attack Cycle By Hacktivists [2]

Note: This data is based upon averages of previous hacktivist campaigns. TTPs, timing, and the order they are carried out can change at any time.

Attack Types

Inside the Arsenal

Doxing—the exposing and publishing of one's identity and their personal information online.

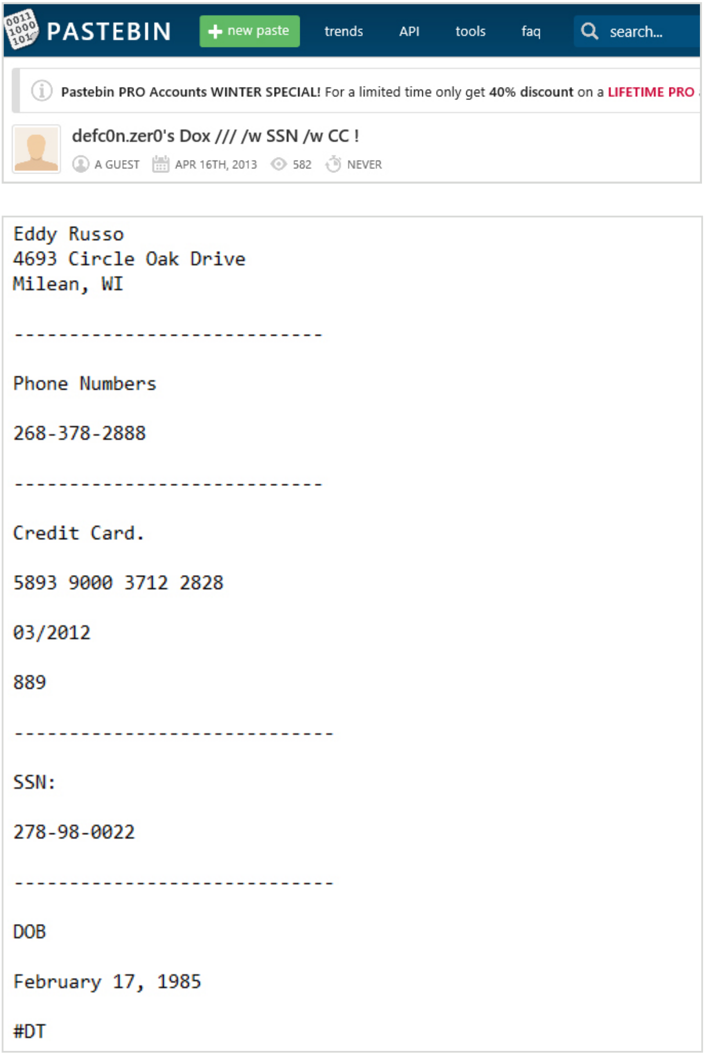
A. **Intended Effect:** The intended effect is multi-faceted as it may be used to embarrass the target or to gather a target's personal information for harassment of individuals or other malicious activities.

B. **Targets:** Usually consist of high profile individuals, or individuals tied to the protested campaign.

C. **Techniques & Procedures:**
   - Social engineering in an attempt to further their doxing efforts
   - Utilizing public social media to obtain info (Facebook, Twitter, Instagram, etc.)
   - Utilize public records (County, State, DMV, marriage certificates, criminal, etc.)
   - Utilization of hacking tools to access websites that host the targeted person's personal information

D. **Tools:**
   - SQL injection tools
   - Cross-site Scripting (XSS)

See sample of a dox posted to a public paste site below



Pastebin PRO Accounts WINTER SPECIAL! For a limited time only get 40% discount on a LIFETIME PRO

defc0n.zer0's Dox /// /w SSN /w CC !

A GUEST APR 16TH, 2013 582 NEVER

```
Eddy Russo
4693 Circle Oak Drive
Milean, WI

----------------------------

Phone Numbers

268-378-2888

----------------------------

Credit Card.

5893 9000 3712 2828

03/2012

889

-----------------------------

SSN:

278-98-0022

-----------------------------

DOB

February 17, 1985

#DT
```

Figure 2 - Public "DOXing" Example

DDoS—Distributed Denial of Service is the use of multiple computers to generate an excessive amount of network traffic towards an Internet-facing asset.

A. **Intended effect:** The intended effect of a DDoS attack is to render a device or multiple devices unusable due to an excessive amount of network traffic targeting the devices, or resource exhaustion. These types of attacks can completely knock out an organization's external-facing network that may be used for banking, e-commerce, distribution, acting company website, etc. Attacks vary in size ranging from single digits in gigabytes per second (Gbps) to over 400 Gbps. The largest recorded DDoS attack in history was an attack carried out against the website of the BBC; the total size of this attack was over 600 Gbps.

B. **Targets:** Usually consist of an external-facing network device that can cause significant

C. **Techniques and procedures:**
   - Single machine DoS attack
   - Multiple machines DDoS attack
   - Booter Service and other pay-for DDoS services (A service offered by cyber criminals that provides paying customers with DDoS attack capabilities on demand. Utilizing this service grants the customer anonymity as they are not the ones carrying out the actual attack, but the booter service is)
   - Obfuscation of traffic by utilizing a Virtual Private Network (VPN) or Tor to hide the origin of the attack
   - Hijacking of multiple machines to create a botnet to carry out attacks

D. **Tools:**
   - **HOIC (High Orbit Ion Cannon):** HOIC is an open-source DDoS application which requires very little training and is one of the tools most commonly used to carry out a DDoS attack. HOIC uses high-speed multi-threaded HTTP flooding against the target.
     - **Mitigation**—Implement firewall filtering policies as well as traffic limiters, and utilize anti-DDoS services (Akamai, Verisign)
   - **Slowloris:** Performs a DoS attack against various types of Apache and other web servers by exhausting the available connections. The tool sends partial HTTP traffic to the server for a long period of time, rendering the server unavailable for new requests because all the threads and processes are consumed.
     - **Mitigation**—Use load balancers and change timeout directive
   - **Ufonet:** Uses Open Redirect vectors on 3rd party web applications such as a botnet to carry out large DDoS attacks.
     - **Mitigation**—Use load balancers, rate limiter, or DDoS prevention service (Akamai, Verisign, etc.)
   - **MDK3:** Specializes in flooding wireless networks by overloading the Access Point (AP). This tool uses methods such as flooding authentication requests to the AP, beacon flood, and de-authentication/dissociation flooding.
     - **Mitigation**—Limit wireless users, disable beaconing, and enable TCP resetting.
   - **Torshammer:** A powerful DoS tool that can be run through the Tor network to be anonymized. Used to target Apache and IIS.
     - **Mitigation**—Keep all web servers fully patched and up to date. Also ingest up-to-date Tor Network exit nodes to implement up-to-date blocks (https://torstatus.blutmagie.de)
   - **Thcssl:** Performs DoS attacks that require a small number of packets to cause a denial of service by initiating SSL handshakes and then immediately requesting a renegotiation of the encryption key. This cycle continues until the server's resources are used up and exhausted
     - **Mitigation**—Limit or disable SSL key renegotiation. Add an SSL accelerator to optimize SSL processing. Implement IPS but may have some difficulty due to encryption of packets
   - **Pyloris:** A configurable tool to perform application-layer DoS attacks. This tool has the ability to utilize SOCKS proxies and SSL connections and can target protocols such as HTTP, FTP, SMTP, IMAP, and Telnet
     - **Mitigation**—Utilization of specialized security platforms for application-layer attacks. Can also implement low timeouts, IP connection limits, data transfer rates, etc. on targeted servers.
   - **Hping3:** A command-line tool that can be configured to generate extremely large and fast ICMP echo requests and supports TCP, UDP, ICMP and RAW-IP protocols. This tool is quick and easy to run. It comes preloaded on Kali Linux and is primarily used to consume the network connection on the target's computer.
     - **Mitigation**—Implement firewall filtering policies as well as traffic limiters, and utilize anti-DDoS services (Akamai, Verisign.)

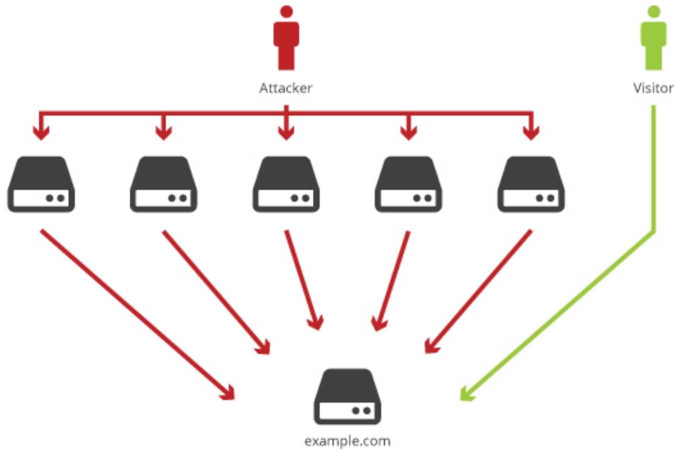
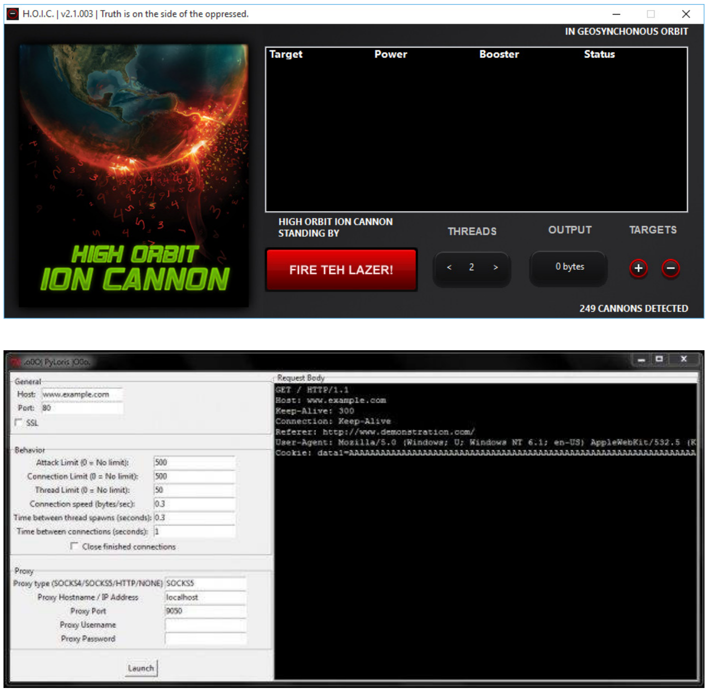


Figure 3—Example of a simple DDoS[3] attack where the attacker is utilizing multiple controlled machines to send a flood of traffic to the intended target, rendering it unusable for the visitor that needs access to it.



General
Host: www.example.com
Port: 80
□ SSL

Behavior
Attack Limit (0 = No limit): 500
Connection Limit (0 = No limit): 500
Thread Limit (0 = No limit): 50
Connection speed (bytes/sec): 0.3
Time between thread spawns (seconds): 0.3
Time between connections (seconds): 1
□ Close finished connections

Proxy
Proxy type (SOCKS4/SOCKS5/HTTP/NONE) SOCKS5
Proxy Hostname / IP Address localhost
Proxy Port 9050
Proxy Username
Proxy Password

Request Body

```
GET / HTTP/1.1
Host: www.example.com
Keep-Alive: 300
Connection: Keep-Alive
Referer: http://www.demonstration.com/
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/532.5 (K
Cookie: data1=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Figure 4—HOIC & Pyloris Interfaces [4]

Web Defacement – Making any unauthorized visual or verbal changes to a targeted website

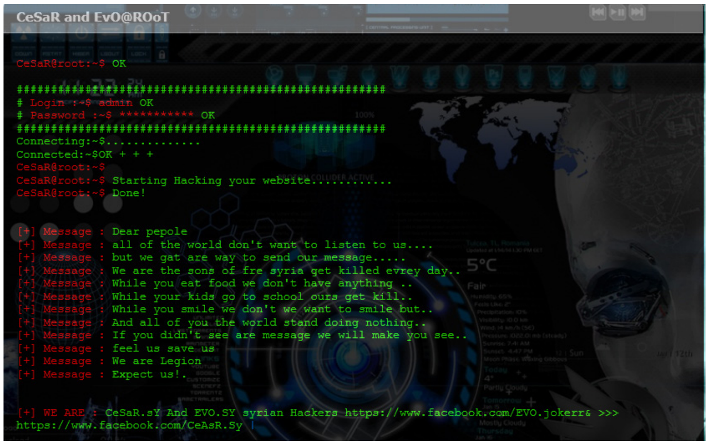
A. **Intended Effect:** The intended effect is to "vandalize" the target's website and post the hacktivist's visual or verbal propaganda, which can also result in reputational damage.

B. **Targets:** Usually consist of corporate, government, and religious sites tied to the protested campaign.

C. **Techniques & Procedures:**
   - Social engineering in an attempt to gather credential information for the targeted website
   - Exploiting vulnerabilities or misconfigurations of targeted website
   - Exploiting backdoor entry (open port / path, another connection which allows the attacker to pivot to the webserver)
   - Utilization of security tools to perform reconnaissance to determine path of least resistance to targeted web server

D. **Tools:**
   - Cross-site Scripting (XSS)
   - Metasploit
   - Havji
   - Acunteix
   - Nitko
   - Others

See samples images of web defacements below. (Note the styles and threat actor groups)


CeSaR and EvO@ROoT

```
CeSaR@root:~$ OK

#####################################################
# Login :~$ admin OK
# Password :~$ *********** OK
#####################################################
Connecting:~$..............
Connected:~$OK + + +
CeSaR@root:~$
CeSaR@root:~$ Starting Hacking your website...........
CeSaR@root:~$ Done!


[+] Message : Dear pepole
[+] Message : all of the world don't want to listen to us....
[+] Message : but we gat are way to send our message.....
[+] Message : We are the sons of fre syria get killed evrey day..
[+] Message : While you eat food we don't have anything ..
[+] Message : While your kids go to school ours get kill..
[+] Message : While you smile we don't we want to smile but..
[+] Message : And all of you the world stand doing nothing..
[+] Message : If you didn't see are message we will make you see..
[+] Message : feel us save us
[+] Message : We are Legion
[+] Message : Expect us!.


[+] WE ARE : CeSaR.sY And EVO.SY syrian Hackers https://www.facebook.com/EVO.jokerr& >>>
https://www.facebook.com/CeAsR.Sy
```

Figure 5—Web Defacement Example

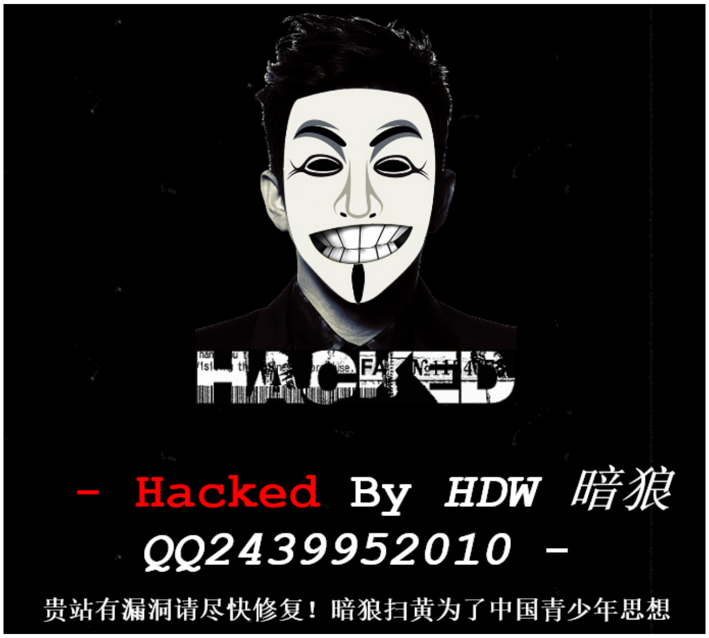


Figure 6—Web Defacement Example

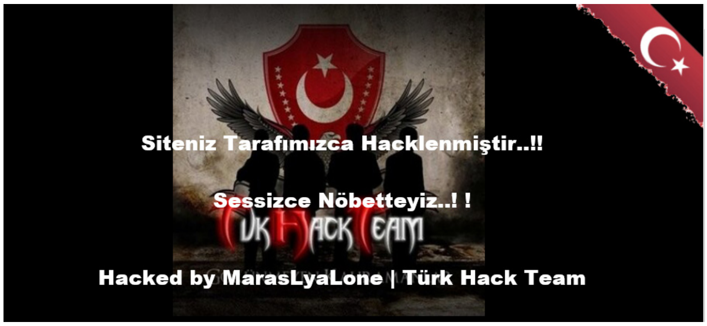
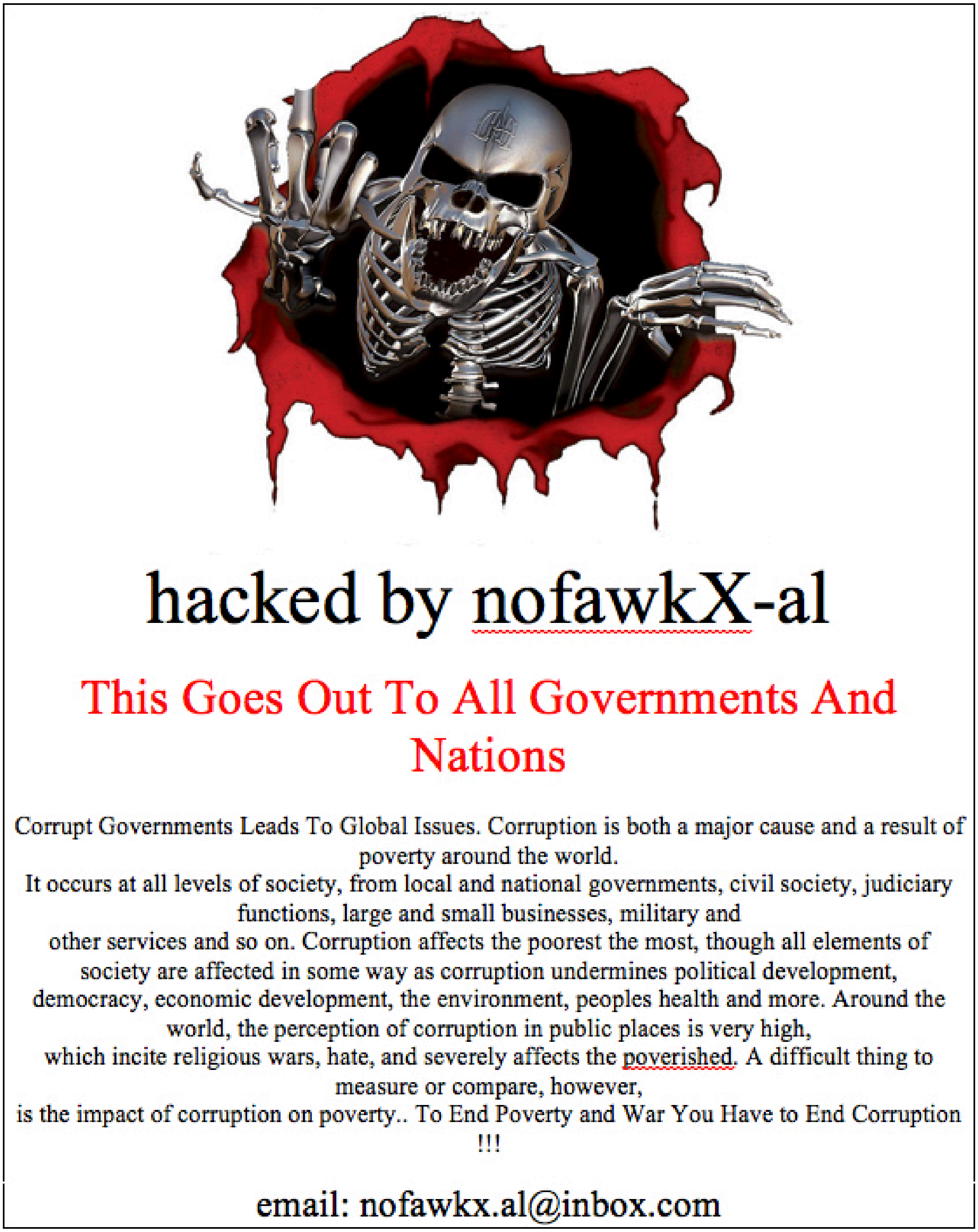

Siteniz Tarafımızca Hacklenmiştir..!!
Sessizce Nöbetteyiz..! !
TÜRK HACK TEAM
Hacked by MarasLyaLone | Türk Hack Team

Figure 7—Web Defacement Example



hacked by nofawkX-al

This Goes Out To All Governments And Nations

Corrupt Governments Leads To Global Issues. Corruption is both a major cause and a result of poverty around the world.
It occurs at all levels of society, from local and national governments, civil society, judiciary functions, large and small businesses, military and
other services and so on. Corruption affects the poorest the most, though all elements of society are affected in some way as corruption undermines political development, democracy, economic development, the environment, peoples health and more. Around the world, the perception of corruption in public places is very high,
which incite religious wars, hate, and severely affects the poverished. A difficult thing to measure or compare, however,
is the impact of corruption on poverty.. To End Poverty and War You Have to End Corruption !!!

email: nofawkx.al@inbox.com

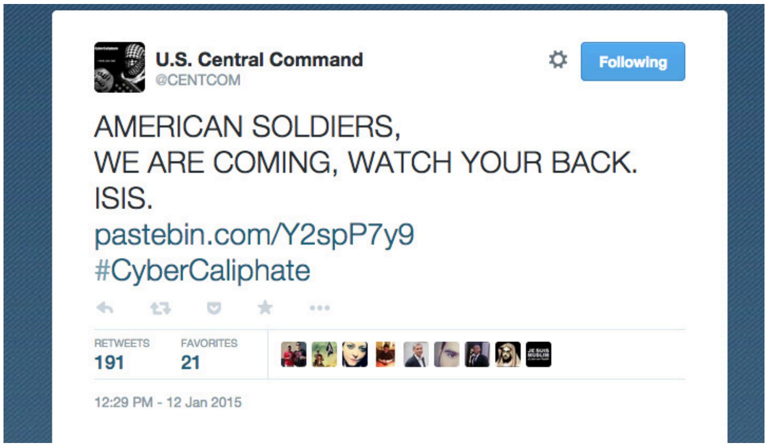
Figure 8—Web defacement example

Social media hijacking—Gaining unauthorized access to social media accounts with the intention of posting data related to the hacktivist's campaign

A. **Intended effect:** The intended effect is to "vandalize" the target's website and post the hacktivist's visual or verbal propaganda, which can also result in reputational damage

B. **Targets:** Targets consist primarily of public-facing assets owned, controlled by or affiliated with the entity, including but not limited to:
   - Social media accounts belonging to target entities and individuals closely associated with target entities:
     - Facebook, Google+
     - Special Internet—Pinterest, Yelp, LinkedIn
     - Photo and Media—Vine, Soundcloud, Instagram, YouTube
     - Communication—Snapchat, Twitter, Skype, WhatsApp, Gmail, Google Voice
   - Public-facing assets
     - Public web sites
     - Corporate intranet
     - Messaging/email
     - File and other electronic data transfer
     - Home internet services
   - Non-public assets that may still be publicly exposed
     - E911 services
     - Telephone services
     - Voicemail services

C. **Techniques and procedures:**
   - Social engineering to gather credential information for the user's social media account
   - Insider threat actor with access to company's social media accounts
   - Sending messages containing malware to your social media accounts with subjects intended to evoke the reader's interest; when clicked, the messages may grant threat actor access to accounts
   - Phishing emails which contain malware or imitate emails from the social media site asking you to log in and change your credentials, claiming your social media account has been compromised



U.S. Central Command
@CENTCOM

AMERICAN SOLDIERS,
WE ARE COMING, WATCH YOUR BACK.
ISIS.
pastebin.com/Y2spP7y9
#CyberCaliphate

RETWEETS 191
FAVORITES 21

12:29 PM - 12 Jan 2015

Figure 9 [5]—US Central Command Twitter account hijacked by Cyber Caliphate in 2015

D. **Tools**
   - Spammer technology
   - Password dictionary
   - Malicious Code (Malware)

E. **Securing social media**—With potential social media targets identified, proactive steps can be taken so that additional exposure associated with regular use does not increase the attack surface.
   - **Publishing**—All social media publishing for high-profile individuals and entity accounts needs to be controlled via a workflow tool such as Sprinkler or HootSuite.
   - **Access**—Social media account access should exclusively use two-factor authentication.
   - **Footprint**—Proactively register social media accounts with the proper name and identification on popular social media venues, if they are not already extant and/or are not already controlled by the organization.
   - **Monitoring**—Enhance monitoring of existing social media accounts to detect compromise.
   - **Communication/Response**—Identify and establish proper abuse contacts for social media venues to enable rapid takedown of rogue accounts or to recover from account takeover.
   - **Brand**—Identify any rogue, look-alike, or other unauthorized social media accounts that may be used to socially engineer targets, publish false information, or discredit targets. Monitor such accounts or request that they be taken down.

F. **Additional notes**
   - Additionally, for high-profile individuals and/or dependents, it is recommended that social media accounts be disabled/suspended during any ongoing crisis so that accounts not directly under the control of the target entity cannot be compromised.
   - Social engineering is often used to hijack social media accounts. Crafted spear-phishing emails, telephone calls, and other similar attack vectors can be used to gain additional information which can be used to further both doxing and social media hijacking attacks. Proper communication to staff, especially those charged with maintaining social media access, should include enhanced training on the proper response to suspicious attempts to gain access (phone calls or emails), exposures, or compromises.

Monitoring and detection

Eyes and ears

In order to be successful in reducing the likelihood of becoming a victim of hacktivism, your organization must have a strong monitoring and detection capability. A good monitoring and detection program includes technical resources and skilled personnel, as well as the ability to utilize these two necessities efficiently. Strong monitoring and detection cannot work without these two necessities. If a security monitoring device triggers an alert, and there is no one to analyze the alert, the monitoring and detection capability has failed; people and technology are both critical.

Another key to having a strong monitoring and detection program is knowing what to monitor and what thresholds are in place to eliminate false positives, as well as ensuring you are detecting legitimate malicious behavior. Out of all of the key elements discussed, the most important takeaway is to be proactive.

Being in a proactive monitoring state puts you ahead of the game and ahead of the adversary. It can give you better insight into your infrastructure, baselines, and vulnerable target areas.

Proactive monitoring should include the following key components:

- Social media account and publication monitoring
- Website integrity monitoring—notifies key individuals on changes to critical assets and their content
- Site availability monitoring—provides baseline performance measures and notifies key individual of any severe deviation
- Open-Source Monitoring
  - Paste sites
  - Social media sites
- Closed-Source Monitoring
  - Dark Web (Tor, I2P)
  - Deep Web (Unindexed sites, password-protected forums, BitTorrent, IRC)
- Perimeter Internet Connection Monitoring
- Monitor perimeter router bandwidth on uplinks
- Firewall, IPS, load-balancer monitoring
- Host integrity monitoring (file changes, access monitoring)

Remediation and prevention

Clear and protect

Trying to stop a leaderless group of faceless individuals without geographic borders from attacking your systems is extremely difficult if not impossible. Because hacktivists are socially or politically motivated, an attack can materialize in a few hours and without warning; hacktivists may launch attacks in reaction to a news item which relates to your organization only tangentially. While it may be difficult to stop an attack from taking place, your organization can prepare for attacks and have the ability to monitor, detect, and mitigate them with the proper security controls in place. Below is a list of recommendations to strengthen your organization's security posture and reduce the attack surface of your organization

A. **Vulnerability management program status check**

B. **Identify current patch state of Internet-facing assets and priorities for immediate patching**
   - 48 hour target list
   - 72 hour target list
   - 1 week target list
   - 2 week target list
   - Immediate vulnerability assessment recommended
   - Assess and harden Internet-facing systems
     - Shut down unnecessary ports and services
     - Shut down old/unused assets
     - Accelerate any security technology deployment (AV, IPS, etc.)
     - Consider shifting critical services to cloud providers (DNS, email, spam control)
     - Identify key assets and implement DDoS protection for these assets
       - DDoS shield technologies, like CloudFlare are less effective, especially if the adversary has already mapped your infrastructure
       - Based on our analysis, we find that BGP (Border Gateway Protocol) based DDoS scrubbing like Neustar, Verisgn or Akamai are more effective

C. **Public-facing attack surface**
   - **Access—**Web channels should be secured via SSL when possible. Two-factor authentication should be used for all remote-access and remote-management systems.
   - **Footprint**—All authorized web channels should be accounted for, including IP address, location, group ownership, and backup strategy. Critical internal assets, such as intranet systems, should be moved internally so that they are only available on VPN/remote-access when feasible.
   - **Monitoring**—All authorized web channels should be monitored consistently for DDoS, brute-force attempts, and web-application attacks such as SQL injection. Additionally, external site availability and integrity monitoring should be added to every critical asset to detect resource exhaustion attacks against them, where bandwidth is not depleted but webserver resources are.
   - **Communications/Response—**Changes to web content should proceed via a publishing workflow system so that only authorized content is published to websites by authorized individuals.
   - **Brand**—Associated domains must be further protected; all communications to domains, IP registrars, and registries should be authenticated prior to responding so that domain-hijacking cannot be successful.

D. **Additional notes**
   - In general, public network interfaces, dial-in interfaces, and management systems for telephony systems, PBX, E911, and electronic voicemail systems should be heavily monitored. If these systems are secured using a single-factor authentication system (shared password), these passwords should be updated. If a vendor has remote access to these systems, it should be considered a vulnerability and shut down for the duration of an attack.
   - Building management systems facing the Internet—in many cases, systems running content in elevators or controlling building environment controls and alarm systems—are public-facing and poorly secured. Short of shutting these systems down, disabling remote access to these systems should be considered for the duration of an attack.
   - Consider other control networks as targets as well—this could include any entity-run control network in an industrial facility such as a water treatment plant, municipal utility, security system, or similar. Steps need to be taken to protect these assets or remove their exposure for the duration of an attack.

Communication plan

Know your audience

Having a communication plan is critical in the event of an incident by hacktivists. Having a communication plan in place allows for the incident to be effectively communicated to all appropriate stakeholders. Information needs to be forthcoming so certain stakeholders know where the incident stands. Response times may be delayed if proper communication isn't taking place or if communication to the wrong audience occurs during an incident. One of the most important aspects of a strong communication plan is knowing who the right contacts are and what their role is. Listed below are the key contacts your organization should know in the event of an incident.

A. **Identify key contacts for the following:**
   - Social media abuse contacts
   - Domain and IP registrars and registries
   - Internet service providers
   - Internet hosting providers
   - Cloud services providers
   - Technology partners

B. **Situation Room (War Room) planning:**
   - Identify agency partners
     - State National Guard
     - State and federal law enforcement
     - State technology organizations
   - Logistics and personnel scheduling
     - Extended shift protocols and overtime policies
     - Groups required for staffing war room
     - Ad-hoc communications and collaboration plan
     - Technology collaboration plan (group ware, messaging, data handling protocol, privacy)
   - Event communications to media
     - Criteria for acknowledging an event
     - Designated spokespersons
     - Key media contacts

Summary

Like any cyber threat group, hacktivists will always continue to evolve and remain a present danger to individuals, groups, governments, and corporations worldwide. We as cyber defenders must recognize the capabilities of hacktivists and the damages hacktivism can cause. So many times have we focused on cyber criminals selling stolen data or nation-states that specialise in advance persistent threats (APTs), that we ignore another hacktivist group that can cause just as much damage to your organization both from a cyber and public relations perspective. As discussed previously, most hacktivists are ideologically motivated rather than profit-driven, making future attacks by a hacktivist group somewhat unpredictable.

Hacktivist groups benefit directly from publicity generated in response to their campaigns. This publicity may attract new group members or draw attention to the group's selected cause. Leveraging this publicity is critical, as it can provide clues to help prepare, defend, and mitigate possible cyberattacks against your organization.

Anonymous remains one of the largest decentralized hacktivist groups in the world; however, newer hacktivist groups have varying modus operandi. Some hacktivist groups are sponsored by kinetic armies, nation-states, or are individuals carrying out malicious activity on their own. This trend is an indicator that future attacks may have better funding and capabilities and may be more difficult to defend against.

Remember that social media may be your best source of intelligence. Join social media sites such as Twitter, Facebook, etc. Look for different hacktivist groups that could pose a potential threat based upon previous campaigns, and track or subscribe to sources of information regarding such campaigns The more you can monitor these social media platforms, the better your cyber threat intelligence regarding hacktivism will be.

In closing, the best offense is a prepared defense. Your goal is not to strike back at the enemy; but to protect your castle. Utilize this playbook to help plan, prepare, and defend that castle from the enemy. And most importantly, never underestimate them.

Appendix

A hacktivism campaign

Date: August 11 2014

Hacktivist Group: Anonymous

Operation: OpFerguson, #OpFerguson

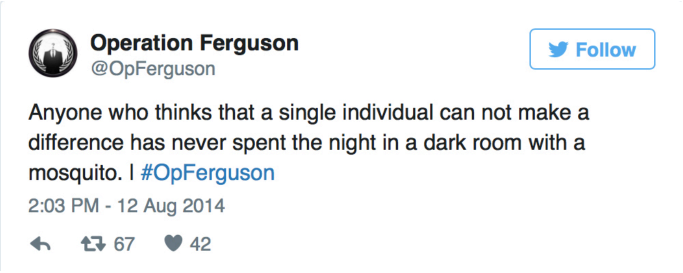
Motivation: To protest against the shooting of unarmed 18-year-old Michael Brown in Ferguson, Missouri.

TTPs: Doxing, DDoS, SQL Injection, Insider Threat, Vulnerability Scanning, Social Media Advertising

Effects:

01. DDoS attacks against the city's servers, websites, and police website (Some were full throttle, and some utilized slow Layer 7 attacks to keep traffic unnoticed while exhausting the target machine's resources)
02. Doxing of Police Chief John Belmar
03. City and police department servers taken offline
04. Hours of police dispatch tapes were accessed and released on YouTube; the release was announced on the Twitter account @ TheAnonMessage
05. An insider and Anonymous supporter was identified (had a Guy Fawkes mask)
06. Malicious social media tactics such as creating dummy Facebook accounts to friend individuals associated with the city.
07. Duration of this campaign was three and a half months, which came in waves depending on what key factors were happening since the shooting.

Social media samples



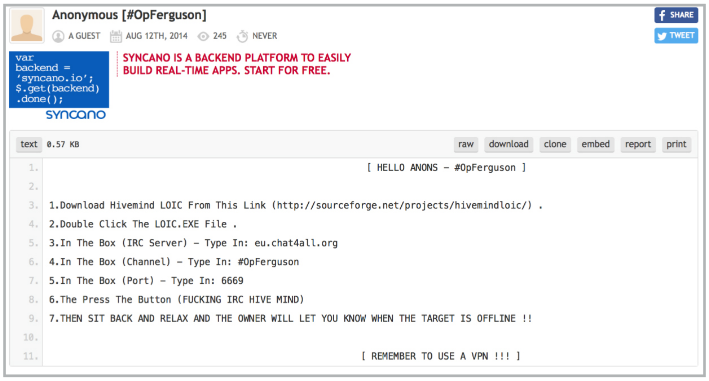
Operation Ferguson
@OpFerguson

Anyone who thinks that a single individual can not make a difference has never spent the night in a dark room with a mosquito. | #OpFerguson

2:03 PM - 12 Aug 2014

@OpFerguson Twitter[6] Post

Home page image for Operation Ferguson[7]



Anonymous [#OpFerguson]

A GUEST AUG 12TH, 2014 245 NEVER

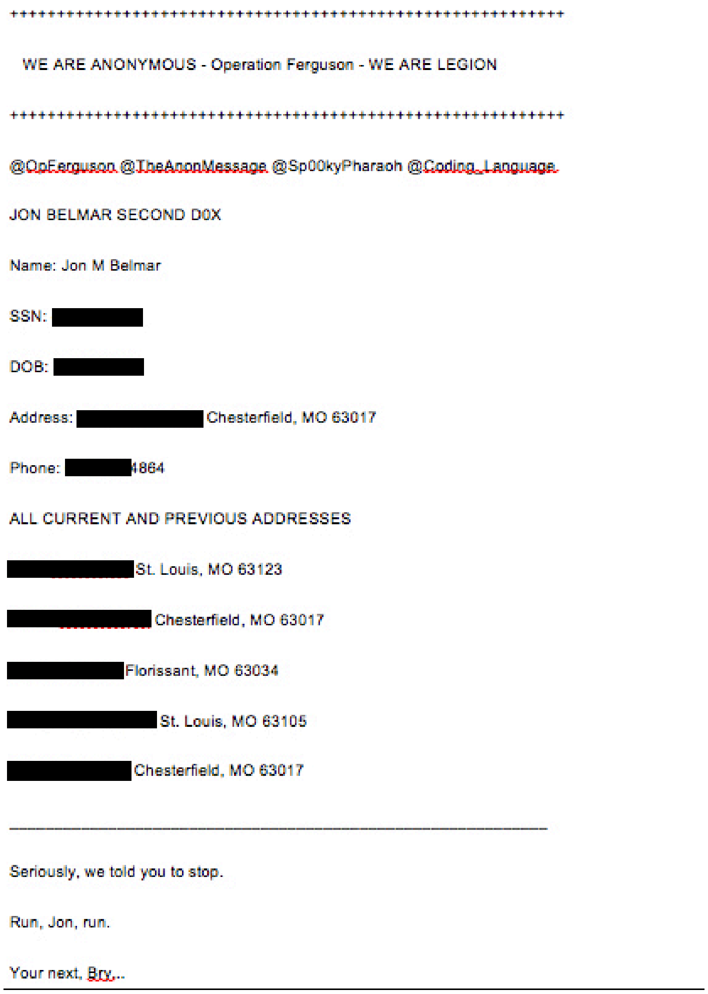
SHARE
TWEET
var backend = 'syncano.io'; $.get(backend) .done();
syncano
SYNCANO IS A BACKEND PLATFORM TO EASILY BUILD REAL-TIME APPS. START FOR FREE.
text
0.57 KB
raw
download
clone
embed
report
print

```
                        [ HELLO ANONS - #OpFerguson ]

1.Download Hivemind LOIC From This Link (http://sourceforge.net/projects/hivemindloic/) .
2.Double Click The LOIC.EXE File .
3.In The Box (IRC Server) - Type In: eu.chat4all.org
4.In The Box (Channel) - Type In: #OpFerguson
5.In The Box (Port) - Type In: 6669
6.The Press The Button (FUCKING IRC HIVE MIND)
7.THEN SIT BACK AND RELAX AND THE OWNER WILL LET YOU KNOW WHEN THE TARGET IS OFFLINE !!

                        [ REMEMBER TO USE A VPN !!! ]
```

Anonymous educating users on what attack tool and IRC channel [8] to use



++

WE ARE ANONYMOUS - Operation Ferguson - WE ARE LEGION

++

@OpFerguson @TheAnonMessage @Sp00kyPharaoh @Coding_Language

JON BELMAR SECOND D0X

Name: Jon M Belmar

SSN: [redacted]

DOB: [redacted]

Address: [redacted] Chesterfield, MO 63017

Phone: [redacted]4864

ALL CURRENT AND PREVIOUS ADDRESSES

[redacted] St. Louis, MO 63123

[redacted] Chesterfield, MO 63017

[redacted] Florissant, MO 63034

[redacted] St. Louis, MO 63105

[redacted] Chesterfield, MO 63017

____

Seriously, we told you to stop.

Run, Jon, run.

Your next, Bry...

Publicly released DOX on Jon Belmar (Chief of Police for St. Louis County[9])

OpFerguson Campaign Links

- https://www.youtube.com/watch?v=XCIiw6Vwo4I
- http://www.operationferguson.cf
- https://twitter.com/OpFerguson/media
- http://pastebin.com/p72YBVZZ
- http://pastebin.com/82UtBT46
- http://pastebin.com/EeLZgTgr

Recipients may share TLP: White[1] information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

References

[1] TLP: WHITE information is subject to standard copyright rules, and may be distributed freely, without restriction.

[2] This data is based upon averages of previous hacktivist campaigns. TTPs, timing, and the order they are carried out can change at any time.

[3] https://commons.wikimedia.org/wiki/File:HOIC_INTERFACE.png

[4] http://null-byte.wonderhowto.com/how-to/hack-like-pro-denial-service-dos-tools-techniques-0165699

[5] https://www.google.com/search?q=centcom+cyber+caliphate&rls=com.microsoft:en-US:IE-Address&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjdrKSQ_6jNAhVLJlIKHURqCuIQ_AUICSgC&biw=1463&bih=645#imgrc=YudCUGwCO_12SM%3A

[6] twitter.com

[7] https://www.google.com/search?q=anonymous+operation+ferguson&rls=com.microsoft:en-US:IE-Address&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjOpLm-_qjNAhVBGFIKHTdpCHgQ_AUICigD&biw=1463&bih=645#imgrc=UWExY2wuDk8DYM%3A

[8] www.pastebin.com

[9] All Fake Data…we can't use real dox data

About Deloitte Threat Studies

These studies are the result of detailed research conducted by our Threat Analysis & Research (TAR) team on an ongoing threat or emerging threat trend, typically focusing on a specific threat actor or a specific technical issue that is persistent over time. It contains detailed information on adversary TTPs and IOCs.

About Deloitte's Threat Analysis & Research

TAR is delivered as an annual subscription service that provides client-specific threat insights and business impact through collection & analysis of data across numerous sources of information including darkweb, criminal forums, third-party intelligence or other sources. Our professionals have advanced language skills and regional knowledge, and extensive intelligence experience from law enforcement, government, military, and cyber intelligence companies.

Secure.Vigilant.Resilient.™

To grow, streamline and innovate, many organizations have difficulty keeping pace with the evolution of cyber threats. The traditional discipline of IT security, isolated from a more comprehensive risk-based approach, may no longer be enough to protect you. Through the lens of what's most important to your organization, you must invest in cost-justified security controls to protect your most important assets, and focus equal or greater effort on gaining more insight into threats, and responding more effectively to reduce their impact. A Secure.Vigilant.Resilient. cyber risk program can help you become more confident in your ability to reap the value of your strategic investments.

- BEING SECURE means having risk-focused defenses around what matters most to your mission.
- BEING VIGILANT means having threat awareness to know when a compromise has occurred, or may be imminent.
- BEING RESILIENT means having the ability to regain ground when an incident does occur.

This document contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this document, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this document.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not pr HYPERLINK "http://www.deloitte.com/about"ovide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.