ARTICLE

Doxing, DoS, and Defacement: Today's Mainstream Hacktivism Tools

Written by: Ray Pompon

Date: April 12, 2017

The power of technology has forever buried the old means of retail commerce, communication, entertainment, and finance. In a similar way, technology is now empowering a sea of change in politics and protest.

The use of hacking tools is no longer limited to statecraft and cybercrime; hacking tools are weapons available to anyone and everyone. Their use on a highly cyber-connected society means that information itself can now be easily weaponized. These are the perfect tools for civil disobedience because they enable few to stand against many and make a difference.

The Cyberweapons of Hacktivism

Hacktivists use three common offensive cyber techniques to varying degrees to get their messages out there and harass their opponents.

Doxing and Leaking

The first is *doxing* (*dox* being short for documents, or docs), which involves publicizing of private or personal information on the Internet about a hacktivist's opponents to intimidate or embarrass them. On a broader scale, *leaking* is the publication of carefully curated and incriminating emails or confidential documents, which can be effective against organizations or public figures. This is what plays out on the nightly news with WikiLeaks, and it is all too common. However, doxing is more a personal attack. It involves releasing highly personal, identifying information about an individual that includes details like date of birth, family names, phone numbers, social media profiles, and even photographs.

Most insidiously, doxing can be used to hit individual members within a targeted organization. For example, thousands of U.S. law enforcement and government employees have been doxed as part of hacktivist protests.[i] Because of the nature of their jobs, law enforcement personnel can be placed in serious physical danger if their personal information is leaked to the public. It's such a serious problem that the FBI has issued warnings to law enforcement personnel and their family members about possible doxing and cyber-attacks by hacktivists.[ii]

Where are hacktivists getting this information to share? In many cases, they are hacking the police systems directly just for this purpose.[iii] Ironically, even the original restricted warnings on doxing issued internally to the FBI were leaked by hacktivists.[iv]

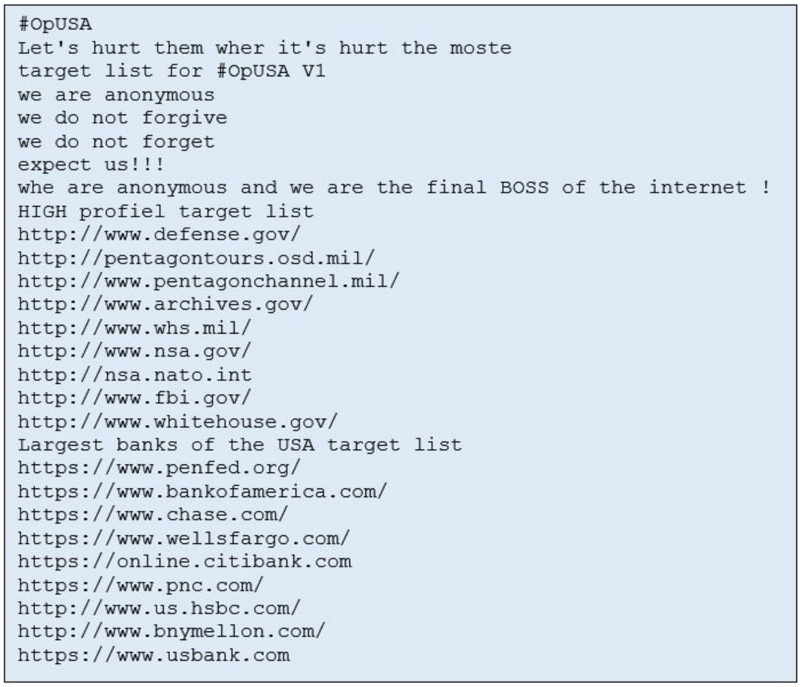
Denial of Service

A fundamental form of physical dissent is the protest march or the sit-in. These are designed to deny usage of some important service and at the same time call attention to the protestors' cause. In the Internet world, the denial-of-service (DoS) attack is an easy, electronic substitute. But, to be effective as a protest tool and draw attention to the cause, hacktivist protest attacks need to be publicized in advance. A good example of this was Anonymous' 2013 OpUSA campaign against U.S. banks and government offices, which was forewarned weeks in advance (see Figure 1).

These notifications give defenders a chance to prepare their response. Without them, a hacktivist runs the risk of the affected organization attributing the attack to criminals or equipment outages. For a hacktivist, that's a fail—the attention is just as important to them as the shutdown.

The real problem with hacktivists perpetrating DoS attacks is the use of illegally subverted computers (*pwned* bots) woven into distributed denial-of-service (DDoS) botnets. It's much harder to claim the moral high ground when you DDoS someone using stolen computing resources. Some hacktivists have tried to frame DDoS attacks as legitimate forms of protest although, so far, this hasn't held any water as a legal defense.[v]

We have come to expect the mostly symbolic protest gestures from groups like Anonymous, such as their DDoS attacks on Holocaust Remembrance Day[vi] or Canada Day.[vii] What is new is groups like New World Hackers claiming responsibility for the largest DDoS attack in the history of the Internet.[viii] The California State Threat Assessment Center (STAC) has issued warnings of a ramp-up of several different hacktivist groups that are planning DDoS attacks against government sites.[ix] DDoS as a protest tool is normalizing and spreading.



```
#OpUSA
Let's hurt them wher it's hurt the moste
target list for #OpUSA V1
we are anonymous
we do not forgive
we do not forget
expect us!!!
whe are anonymous and we are the final BOSS of the internet !
HIGH profiel target list
http://www.defense.gov/
http://pentagontours.osd.mil/
http://www.pentagonchannel.mil/
http://www.archives.gov/
http://www.whs.mil/
http://www.nsa.gov/
http://nsa.nato.int
http://www.fbi.gov/
http://www.whitehouse.gov/
Largest banks of the USA target list
https://www.penfed.org/
https://www.bankofamerica.com/
https://www.chase.com/
https://www.wellsfargo.com/
https://online.citibank.com
https://www.pnc.com/
http://www.us.hsbc.com/
http://www.bnymellon.com/
https://www.usbank.com
```

Figure 1. Anonymous pre-announced its 2013 OpUSA campaign against U.S. banks and government offices

Defacement

Website defacement—changing the visual appearance of a site—was also an early and popular form of hacktivism, essentially taking the form of political graffiti across Internet. It reached an early apex of popularity in 2001 when a mid-air collision between a Chinese fighter plane and a U.S. spy plane occurred. Chinese hackers retaliated by hacking into and defacing nearly a thousand U.S. websites, and American hacktivists responding in kind.[x] Website defacement still happens, often to take the hacktivist's message directly to "the people."

But, stepping back from tampering with the visual appearance of websites, there are more insidious forms of hacktivist defacement. In its purest form, defacement is what we security professionals call an attack against data integrity; that is, someone has corrupted our systems by electronic tampering. But, defacement can go beyond websites. Many other kinds of electronic systems can be subverted to send a political message.

Online polls have been hacked to skew results, although most of the time it has been done as a prank.[xi] This calls into question any online political polling. Followers of social media such as Twitter[xii] or Facebook[xiii] are also easily subverted, further corrupting the viability of any online political campaigns. Political Bots, a research team that investigates the impact of automated propaganda on the public, explains, "Bots are social media accounts that automate interaction with other users, and political bots have been particularly active on public policy issues, political crises, and elections."[xiv] In a separate post, the research team noted that in the week prior to the 2016 U.S. presidential election, 19 million bot accounts sent tweets. "The U.S. election saw perhaps the most pervasive use of bots in attempts to manipulate public opinion in the short history of these automated political tools."[xv] Entire platforms for political communication and discourse are being defaced, notably sometimes *invisibly*, to skew influence.

You Can't Punch a Swarm of Bees

Hacking allows anonymous attacks from small groups or individuals to command an unprecedented level of attention in society. Part of that power is in the protestors' ability to blend into a faceless, amorphous group. Beyond the Anonymous group, which revels in striking from the shadows, there are many other protest movements banding together solely based on goals and a set of techniques. These include Resist, BLM, Occupy, and Arab Spring. While some of these groups have some leadership, involvement is more about hashtags than membership cards. Online tools not only facilitate, they also encourage ad-hoc associations and actions around a cause.

An inability to point to a specific leadership in an offending organization can make retribution, containment, and negotiation very difficult. For example, even when a large crackdown against hacktivists occurs, it still represents a small fraction of the actual movement. When the FBI arrested 14 members of Anonymous, the movement quickly regrouped and began taunting law enforcement anew.[xvi] These flash mob style swarms of attacks can be quite exasperating for targeted organizations and, for the same reason, can be very attractive for protestors who want to modulate their involvement in the cause. The deployment of opt-in DDoS tools like the Low Orbit Ion Cannon (LOIC)[xvii] can provide hacktivist movements with a way to arm spur-of-the-moment protestors with powerful cyber-weapons.

Digital crowdsourced protests also provide deniability for egregious actions taken. If the movement wants to preserve some legitimacy, it can also easily disavow any illegal actions by these spontaneous hacktivists. That's just as well, because there are some hacktivists who truly don't believe in any particular cause beyond causing general mayhem to authority figures. Unfortunately, these vandals can easily slip in and out of hacktivist movements to harass and sabotage under the aegis of "making the world a better place."

One can also look at these as situations in which the respective governments are either encouraging (or not discouraging) the hacktivist actions. Hacktivism can be seen as a form of slightly firmer political "soft power"—a way of flexing muscles without actually causing any permanents damage. The web defacements regarding a politically charged sports ruling could easily fit this paradigm.[xviii]

Conclusion

The problem with cyber protesting is that anything technological can be automated and mass-scaled, which means grassroots campaigns can be quickly co-opted into AstroTurf campaigns—usually by the very authorities being protested.

CISOs, build your threat models accordingly. Anyone can get angry at you. Hacktivists won't play fair and merely picket your building and sue you in court. Be sure you have done adequate risk analysis around leaks of email and doxing attacks against staff, sustained DDoS attacks, and defacement of Internet applications.

[i] https://motherboard.vice.com/en_us/article/teenage-hackers-say-theyve-doxxed-more-than-3500-government-employees

[ii] https://www.ic3.gov/media/2015/150421.aspx

[iii] https://www.theguardian.com/uk-news/2016/jan/28/fraternal-order-of-police-hacked-fbi-investigation-data-servers

[iv] https://publicintelligence.net/ufouo-fbi-threat-to-law-enforcement-from-doxing/

[v] https://www.dailydot.com/layer8/ddos-attack-political-protest/

[vi] https://en.wikipedia.org/wiki/OpIsrael

[vii] https://motherboard.vice.com/en_us/article/anonymous-is-celebrating-canada-day-in-protest-with-attacks-on-government-sites

[viii] https://www.theregister.co.uk/2016/10/24/hacktivists_claim_dyn_ddos_responsibility/

[ix] http://www.caloes.ca.gov/cal-oes-divisions/state-threat-assessment-center

[x] http://www.foxnews.com/story/2001/05/01/it-all-out-cyber-war-as-us-hackers-fight-back-at-china.html

[xi] http://mentalfloss.com/article/52524/15-polls-hijacked-internet

[xii] https://arxiv.org/abs/1703.03107

[xiii] https://bits.blogs.nytimes.com/2014/04/20/friends-and-influence-for-sale-online/

[xiv] http://politicalbots.org/?p=719

[xv] http://politicalbots.org/?p=797

[xvi] http://www.nytimes.com/2011/07/26/technology/for-suspected-hackers-a-sense-of-social-protest.html

[xvii] https://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon

[xviii] https://www.nytimes.com/2016/08/23/sports/olympics/weight-lifting-website-hacked-as-iranian-fans-protest-judgment.html

F5 Networks, Inc. | f5.com

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan:f5j-info@f5.com