ERT Threat Alert
Patriotic Hackivism
April 24, 2018

Abstract

Hacktivists have increased their activities in recent months, expressing social and political agendas via cyber-protests. These uproars have now taken to the digital world where hacktivists are using defacements, injections and denial-of-service attacks. In addition to just spreading their message, organized groups also engage in influential operations as an attempt to not only control the political message, but the leadership itself.

Patriotism is an example of good intentions translated to bad activities when combined with the low entry point for hacking. The amount of publicly available tools found online today allow anyone with enough motivation to spread a message or influence the course of politics. Since a political viewpoint is hard to change, often these campaigns will have a negligible impact, however this type of operation demonstrates the power that a single individual or group possesses over the political process today.

Background

Patriotic hacktivism poses a serious challenge to modern day security when an individual can get their hands on the ability to influence government procedures or disrupt government systems utilizing publicly available toolkits.

Manipulating elections has become an emerging threat for nations and societies over the past years. Cyber-attacks have become powerful tools of influence and are utilized not only by nation states against one another, but also by hacktivist groups and individuals looking to influence government processes or to destabilize a region.

Anonymous – OpIsrael / OpUSA

Anonymous hacktivists launch a yearly campaign on April 7th with the stated goal of “erasing Israel from the internet” in protest against the Israeli Government. The hacktivist attempt to disrupt government websites with denial-of-service attacks and defacements while targeting citizens with harassing messages. Most attackers are anti-Israeli/anti-Semitic activists with some originating from the autonomous Palestinian territories. These attackers normally fail at causing major damages but on occasion they have successfully targeted government systems.

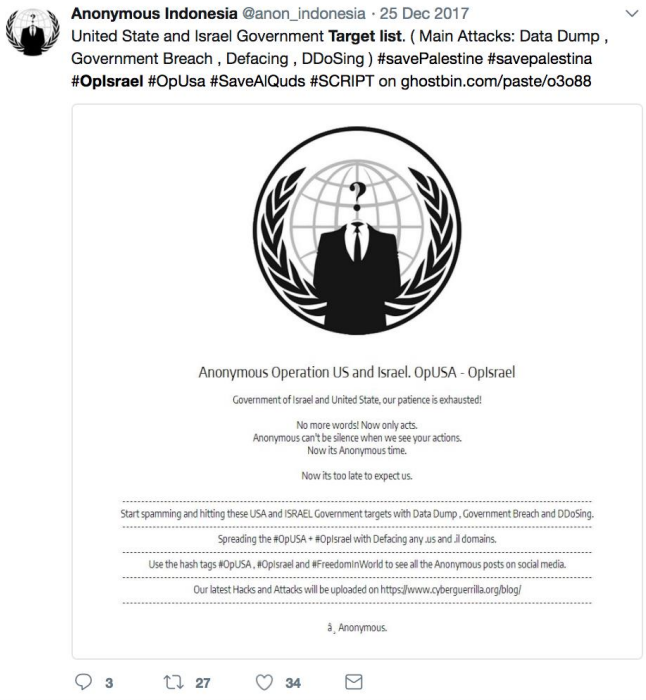

Figure 1: Anonymous OpIsrael and OpUsa

On one side you have pro-Palestinian, non-nation state hackers launching attacks against Israeli systems, and on the other side, you have Israeli citizens, corporations and government agencies defending themselves from this operation. Adding to the confusion, attribution becomes very difficult. Determining if an attack is from an actual protester or a government agency becomes almost impossible.

Figure 2: Indian hackers hit Pakistan. Source TNS

India/Pakistan Conflict

India and Pakistan's conflict dates back to 1947 when India gained independence from Britain and Pakistan was formed. Since then, the conflict between the two countries has spilled onto the internet with attackers ranging from hacktivist groups to sanctioned, state-sponsored attacks. Similar to retaliations conducted by ground forces, hacktivist target government sites with denial-of-service attacks and SQL injections in an attempt to steal data or deface a website following a holiday, political event or military actions. When evolving countries do not have adequate cyber divisions, patriotic hackers normally fill the void.

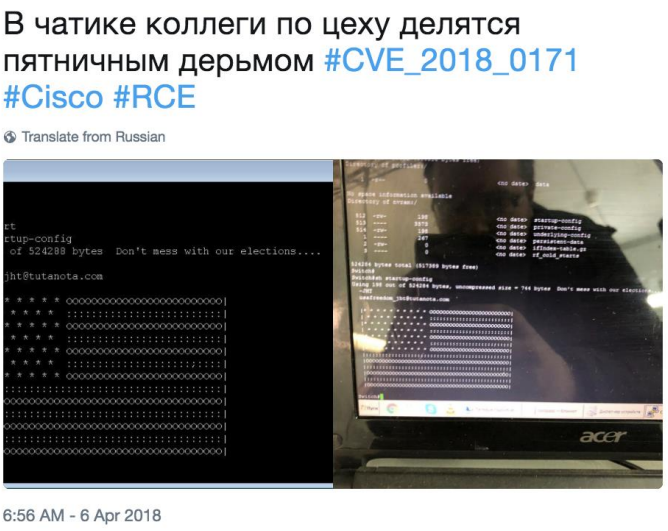

Figure 3: Message displayed on routers across Russia and Iran

Russia/United States Conflict

The rivalry between the United States and Russia goes back to the Cold War. Since then, both sides have been engaged in a persistent proxy war and what appears to be an never-ending war of spies. Technology involved in espionage has evolved with a major focus now on the cyber domain. Both sides have engaged in manipulating political opinions with influence operations mainly driven from the data obtained by breaching government systems.

Similar to the Israeli and the Pakistan/India conflict, local patriotic hackers are involved as well. But unlike the Pakistan/India conflict, Russia and the United States have some of the best government-backed hacking divisions with equally talented hacktivist in the world. With both nation states engaged in digital operations against each other, the hacktivist still engage in operations against each country, leaving room for state-sponsored hackers to operate anonymously.

This presents a problem for government officials who are left to determine if the attack was a sectioned nation state attack or the work of a talented patriotic hacker and what the appropriate response is. Recently, on April 6th, several people across Russia and Iran began reporting that their routers had been compromised and displayed a message from the hacker. This message read "Don't mess with our elections" and had an American flag. This work appeared to be an example of patriotic hacktivist, impacted thousands of devices across both countries and leave Russian and Iran to decide how to respond in accordance to the damage caused by the hack.

Recently the United States government has decided to indict several individuals in both Iran and Russia for digital campaigns carried out on United States targets. These digital campaigns included interfering with the United States political system[1] to cyber theft[2], with President Putin stating that the US election interference may have been the work of patriotic hackers in Russia. Following the recent hack against the Iranian and Russian routers, US-CERT issued an alert[3] stating that Russian state sponsored actors have been targeting network infrastructure devices, primarily in the government and private-sector, critical infrastructure and internet service providers, since 2015.

As far as the election goes, In reality, targeting an election is not that difficult and has been accomplished before by one hacker in nine Latin American countries. Hacker Andres Sepulveda was able to rig elections in Latin America for almost a decade. He and a team of hackers would target campaigns with spyware to look for critical data such as strategies and internal documents and then used that data to manipulate people on social media.

Syria
Other examples of patriotic hacktivism includes past attacks by the Syrian Electronic Army (SEA). SEA is a group of pro-Syrian, pro-Assad hackers who's relationship with the Syrian government is unknown. They have used a number of different attack vectors in the past including phishing, account hijacking, defacements and denial-of-service attacks to target those that oppose the Syrian government and President Bashar al-Assad. Past targets have included the Executive Office of the President and United States Marine Corps. The group also hijacked the Associated Press's twitter account and falsely claimed that President Barack Obama had been injured in a bombing at the White House.

China
China's hacking army is a legitimate division comprised of tens of thousands of highly trained individuals who engage in sanctioned intelligence operations aimed at the United States and other countries. Some hacktivists located inside China mainly focus on targeting their own government, but on occasion launch attacks against other nations. In 2012, hacktivist from both China and the Philippines engaged in operations against each other due to a standoff between the nations over Scarborough Shoal and the Spratly Islands. What began as simple website defacements quickly escalated to denial-of-service attacks and data breaches. The attacks even caused Philippine officials to denounce the attacks and eventually stated that the government does not condone the attacks.

Attack Methods

Distributed Denial-of-Service - A distributed denial-of-service attacks is when an attacker or a group of attackers employ multiple machines to carry out a DoS attack using multiple distributed machines simultaneously, therefore increasing its effectiveness and strength. The army of infected machines carrying out the attacks are mostly often composed of infected IoT devices controlled by the attacker via a Command and Control Server.

---

[1] https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere
[2] https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary
[3] https://www.us-cert.gov/ncas/alerts/TA18-106A

SQL Injection - This technique takes advantage of poor application coding. When the application inputs are not sanitized it becomes vulnerable. Attackers can modify an application SQL query to gain access to unauthorized data with administrator access, run remote commands on the server, drop or create objects in the database, and more.

Cross-Site Scripting - In this attack, malicious scripts are injected into websites through a web application flaw where there is no validation of user input used by the application. The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.

Remote Code Execution – A remote attacker can construct a request with malicious content to exploit the vulnerability. A successful exploitation may lead to remote code injection of a Drupal server, which may lead to the server becoming completely compromised. Remote code execution attacks, which describes an attacker's ability to execute malicious code or command on a targets machine in order to extract sensitive information and/or abuse the system functionality, which finally may result in taking full control of over the server.

Phishing - A digital attempt to obtain sensitive information from a victim by using a malicious email or website. The attacker solicits personal information by posing as a trustworthy organization or the company itself. These attempts are either sent out to everyone in the company or designed to specifically target key associates. Once an associate falls victim to these the hacker will then have the sensitive information required to gain access to certain systems.

Social Engineering - A process of psychological manipulation, more commonly known as human hacking. The goal is to have the targeted victim divulge confidential information or give you unauthorized access because you have played off their natural human emotion of wanting to help or provide them with something. Most of the time the attacker's motives are to either gather information for future cyber-attacks, to commit fraud or to gain system access for malicious activity.

Targets

Government – Government agencies and those who do business with the government are often the first targets selected by patriotic hacktivist. Normally these attacks manifest as denial-of-service attacks in combination with defacements. If the hacktivist are skilled, they will focus on targeting government databases and contractors for information through social engineering and phishing attacks designed to give the attacker remote access. With access to government data they normally leak the data publicly in an attempt to shame the administration or they use the data to influence a political event such as an election or legislation.

Corporations – Corporations that do business with government agencies are also targeted by patriotic hacktivist for several reasons. Attackers targeting government agencies typically target contractors and corporations who do business with the government during the reconnaissance phase of an operation. Often times attacker will find weaker defense outside of government networks and will choose to target their data. Another reason corporations are targeted by patriotic hackers is due to their association or involvement with a political or social event. Often times, these are defense contractors and large corporations. Corporations are typically the target of network and application attacks including denial-of-service, SQL injection, cross-site scripting as well as social engineering in the form of phishing attacks designed to deliver malware allowing the attacker remote access.

Citizens – Citizens are normally targeted by patriotic hacktivist with political messages and propaganda designed to influence emotional reactions in a specific way. This typically involves spreading fake news via the use of bot accounts designed to target notable citizens. Attackers will use current political topics as bait to target citizens with social engineering attack designed to profile and collection data for future use.

Reasons for Concern

Technology can provide a more immersive and rewarding experience, but as more government and processes become digitized, any machine being connected to the internet will create new challenges for those managing the security of the targeted networks. These are risks that both nation state hackers and hacktivist will take advantage of. One of the biggest concern around political affairs is the loss of connectivity during pivotal moments that results in the loss of visibility of real time data to the public.

While attribution is difficult, hackers will use this opportunity to their advantage in an attempt to destabilize a government by promoting a certain political view point or candidate. Adding to the confusion of an attack, attribution can be almost impossible making it difficult for certain victims to determine if the attack came from an individual or a nation state.

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

For further network and application protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Effective Web Application Security Essentials

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate –** using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options -** on-premise, out-of-path, virtual or cloud-based

Under Attack and in Need of Emergency Assistance? Radware Can Help

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

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.