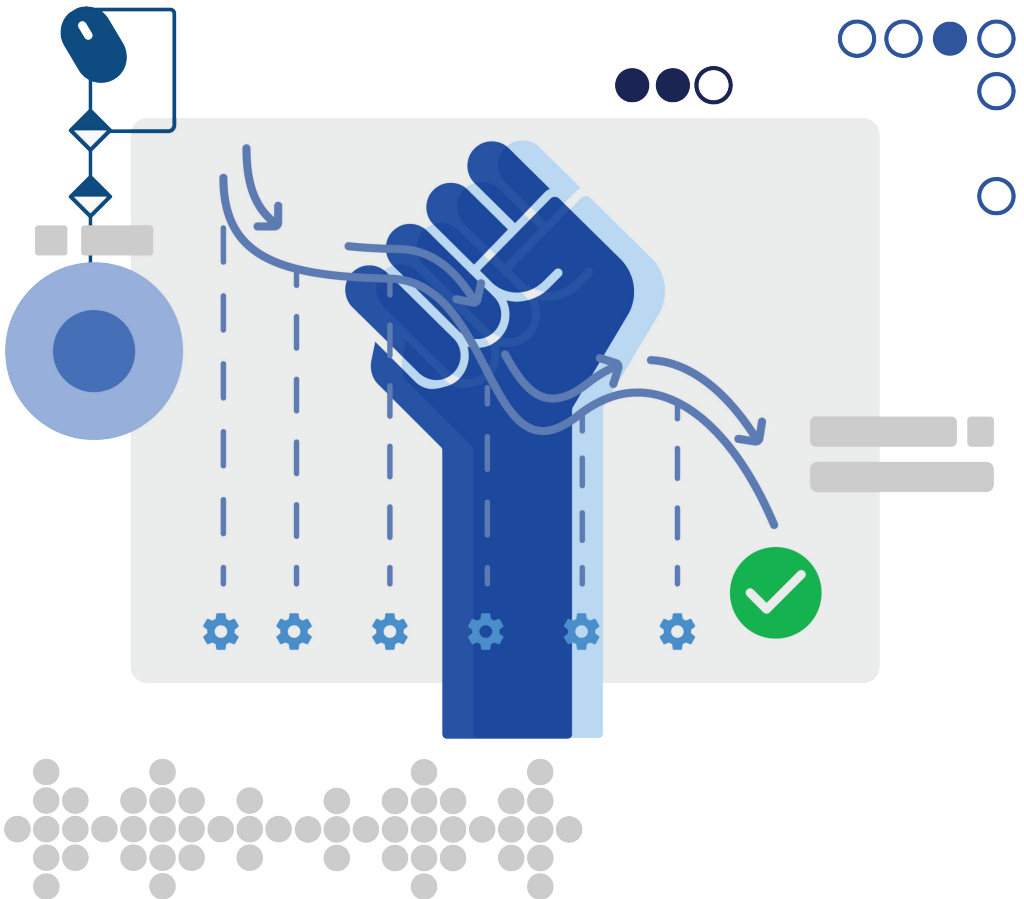
Recorded Future

CYBER THREAT ANALYSIS

Return to Normalcy:

False Flags and the Decline of International Hacktivism

By Insikt Group®



CTA-2019-0821

Groups with the trappings of hacktivism have recently dumped Russian and Iranian state security organization records online, although neither have proclaimed themselves to be hacktivists. In addition, hacktivism has taken a back seat in news reporting, and general mentions seem to be in decline.

Insikt Group utilized the Recorded Future® Platform and reports of historical hacktivism events to analyze the shifting targets and players in the hacktivism space. The target audience of this research includes security practitioners whose enterprises may be targets for hacktivism.

Executive Summary

Hacktivism often brings to mind a loose collective of individuals globally that band together to achieve a common goal. However, Insikt Group research demonstrates that this is a misleading assumption; the hacktivist landscape has consistently included actors reacting to regional events, and has also involved states operating under the guise of hacktivism to achieve geopolitical goals. In the last 10 years, the number of large-scale, international hacking operations most commonly associated with hacktivism has risen astronomically, only to fall off just as dramatically after 2015 and 2016.

This constitutes a return to normalcy, in which hacktivist groups are usually small sets of regional actors targeting specific organizations to protest regional events, or nation-state groups operating under the guise of hacktivism. Attack vectors used by hacktivist groups have remained largely consistent from 2010 to 2019, and tooling has assisted actors to conduct larger-scale attacks. However, company defenses have also become significantly better in the last decade, which has likely contributed to the decline in successful hacktivist operations. Network defenders who have seen, or may in the future see, their organizations targeted by such activities should monitor this changing landscape.

Key Judgments

- Overall hacktivist activity is declining, as the hacktivist landscape shifts away from broad public participation and back toward its origins as a practice of smaller groups of dedicated individuals.
- Improvements over the past decade in the defensive posture of large financial institutions, government agencies, and other popular hacktivist targets have likely rendered the use of unskilled volunteers less effective.
- Insikt Group assesses with high confidence that nation-state entities have increasingly used hacktivism in association with strategic campaigns, by coordinating with legitimate hacktivists of like mind, and have conducted false-flag operations made to appear as unassociated, independent hacktivist activity.
- When targeting a country to protest the actions of its government, hacktivists are also likely to target any organization operating from that country to spread chaos.

Background

Hacktivism, created from the words "hack" and "activism," is largely defined as the conducting of cyberattacks to further the goals of political or social activism. In the early-to-mid 2010s, international groups targeted organizations to protest against everything from anti-piracy measures to the whaling industry. However, while cyberattacks are becoming more widespread, hacktivism seems to be in decline. In addition, multiple threat actors such as Guccifer 2.0, 1937CN, Guardians of Peace, and the Shadow Brokers have conducted cyber operations claiming to be hacktivists, only to be revealed or suspected as groups operating for or connected to nation-states. Most recently, groups like Digital Revolution and Lab Dookhtegan infiltrated and dumped sensitive documents online belonging to Russian and Iranian state security groups, respectively. However, these groups have not gone out of their way to call themselves "hacktivists."

This raised the following questions: What is the current state of hacktivism, and how does it compare to previous years? Who are the current players and how has targeting changed? Finally, what are known links between hacktivism and other types of cyber operations?

This report attempts to answer these questions by laying out a brief history of hacktivism around the globe, data trend analysis of reported hacktivism-based events in the last decade, as well as analysis on specific actors, attack vectors, targets, and events.

History of Hacktivism

During the course of our research, we determined that there are two primary originations for hacktivist groups: international and regional. International hacktivist groups work across borders with hacktivist groups or individuals in other countries to achieve their goals. Regional hacktivist groups primarily originated from political and social missions specific to the climate of certain countries and regions.

United States

The term "hacktivist" was coined in 1994 by Cult of the Dead Cow (CDC), a hacker group formed in 1984 in Lubbock, Texas. Two years after CDC was founded, the U.S. Congress enacted the Computer Fraud and Abuse Act (CFAA), making the intentional access of a computer without authorization illegal. Various hacker groups and individuals within the country emerged in the 90s and early 2000s, exploiting bugs in systems to either pressure organizations into creating more secure products, and/or for the ego boost, social capital, or anti-establishment sentiment that came with finding and exploiting a new vulnerability. L0pht Heavy Industries famously did both — in 1998, the group testified in front of Congress about the internet's alarming lack of security. By this time, they were already well known in the Boston security scene for their grey hat hacker activities.

The term hacktivism, however, came into prominence with the growing popularity of 4chan[.]com — a bulletin board system (BBS)-esque online forum established in 2003 by United States teenager Christopher Poole. Modelled after Japanese BBS systems, non-logged in members on this site were by default named "Anonymous." This forum became the birthplace of the Anonymous hacking collective, consisting of members hailing from all over the globe.

China

As laid out in Recorded Future's previous analysis on Chinese and Russian hacking communities, China's first hacktivists were patriotic, initially angered by anti-Chinese riots in Indonesia. Groups such as the Green Army, China Eagle Union, and Hongke (or Honker) Union, emerged from online pro-China BBS. These groups all contributed to early internet defacements, DDoS attacks, and credential thefts targeting the U.S. and other Chinese adversaries. This was especially the case during the China-U.S. Hacker War of 2001, when the Hongke Union DDoSed the White House website and targeted websites of U.S. businesses in retaliation for the collision between a U.S. spy plane and a Chinese fighter jet off of the Hainan Island that occurred a month earlier.

However, all of these initial groups have since splintered, shut themselves down, or integrated into China's rapidly growing cybersecurity industry. More recent Chinese hacktivism events, such as 1937CN's politically motivated attack on Vietnamese targets, were tenuously linked to wider, possibly state-sponsored cyberespionage campaigns. Anti-Chinese hacktivists exist in China's borders as well; one of the oldest Chinese dissident hacking groups was the Hong Kong Blondes, a group with membership both in and outside of China, who claimed to temporarily disable a PRC communications satellite in 1997.

Russia

While politically motivated cyber campaigns have emerged from Russia, most of Russia's "grassroots" hacktivist organizations or operations have been associated with Russian intelligence organizations, or have been linked to Russian government support. One of the first purported hacktivism events emerging from Russia resulted in a series of DDoS attacks and other intrusions targeting Estonian government organizations in 2007. While initially attributed by some to Russian hacktivists, other individuals clearly pointed fingers at the Russian state. In 2014, the hacking group CyberBerkut rose to prominence after they DDoSed NATO websites. While the group initially took on Ukrainian identities, technical links and contextual analysis provided by both Recorded Future and other organizations have linked the group to the Russian state and the GRU, respectively.

In addition, the alleged "lone hacker" behind the U.S. Democratic National Committee breach in 2016 (Guccifer 2.0), as well as the famed leakers of NSA documents (the Shadow Brokers), have been linked to the Russian government. Hacktivist dissidents in Russia include the ranks of Anonymous International, also known as Shaltai B0ltai, or "Humpty Dumpty," a hacktivist group that obtained access to SMS messages, social media accounts, and emails from multiple Russian officials from 2014 until the arrests of several key members in 2016. In addition, in July 2019, a hacking group named 0v1ru$ breached a major FSB contractor, defaced its homepage, and passed sensitive data to hacking group Digital Revolution, who published the data and advertised the dump on social media.

Brazil

As stated in Recorded Future's previous reporting on Brazil's hacking communities, much of Brazil's hacking community initially participated in web defacements. While hacktivist operations were initially conducted for fun (or to chastise website administrators for poor security configurations), Brazilian hackers also targeted organizations involved in political scandals or contributors to environmental disasters, utilizing hacktivism to express outrage. Anonymous activity in Brazil is also strong, and initially involved DDoSing political organizations. Some of this activity even prompted a formal investigation by the Brazilian Federal Police. After DDoS proved ineffective over time, intrusions into target environments to collect and leak data became more common. Groups in Brazil that likely support Anonymous's cause have targeted corrupt politicians, companies involved in corruption scandals, candidates in elections, the 2016 Summer Olympics in Rio de Janeiro, and the 2014 FIFA World Cup in Brazil.

Internationally

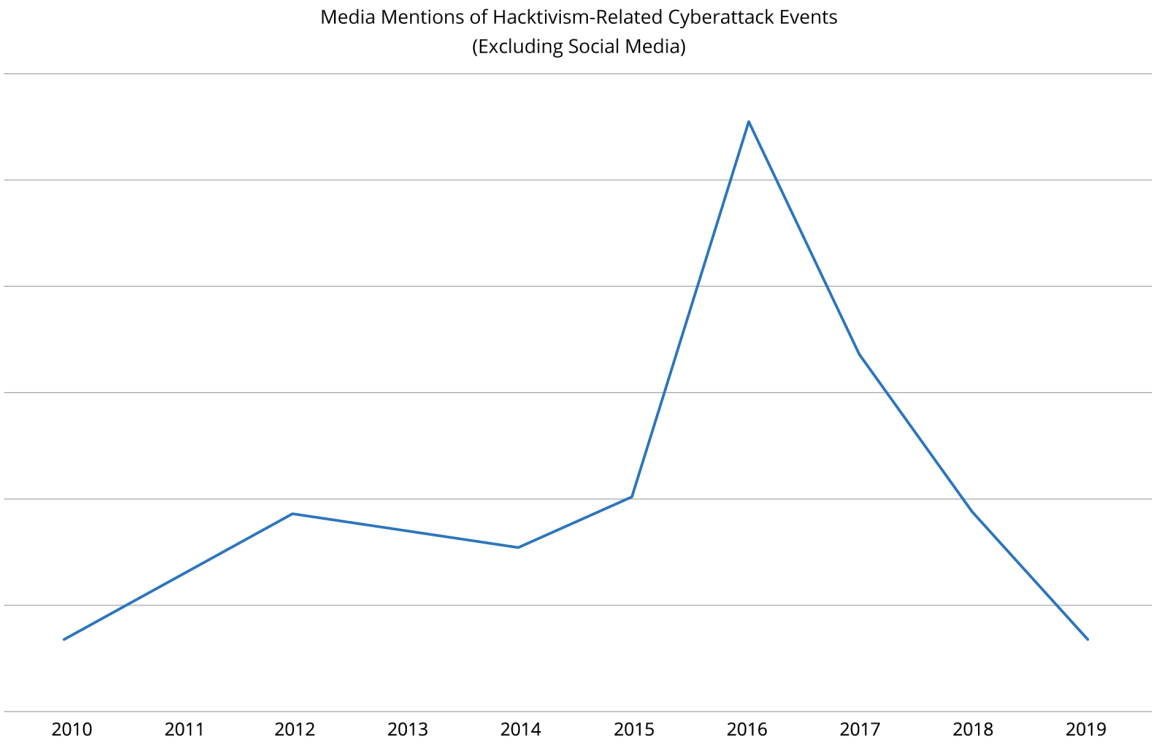
Hacktivist groups in every region have their own unique motives. Hacktivist groups in multiple countries have historically grown out of regional conflicts, state-directed initiatives, general disillusionment with their government, or offending events that go against a group's worldview. Regional conflicts, like those between Israel and Palestine, Serbia and Kosovo, and India and Pakistan, sparked hacktivist groups on various sides that attempted to shut down or deface websites belonging to the opposition from as early as 2008. In addition, various groups of individuals directly employed by state governments, like Iran's Al Qassam Cyber Fighters and the Syrian Electronic Army, have cooperated with other, more organic hacktivist groups to participate in hacktivist operations that are in line with state goals.

Other less-patriotic hacktivist groups have turned their cyber capabilities against their own country. Anti-government groups like Turkey's RedHack leaked stolen documents and DDoSed websites belonging to their country's government in 2016. More anti-establishment, international groups like NullCrew react to individual offenses such as the enforcement of anti-piracy laws and the arrest of Julian Assange in 2012, by hacking the offending organizations in order to speak up against actions that they deem "unjust."

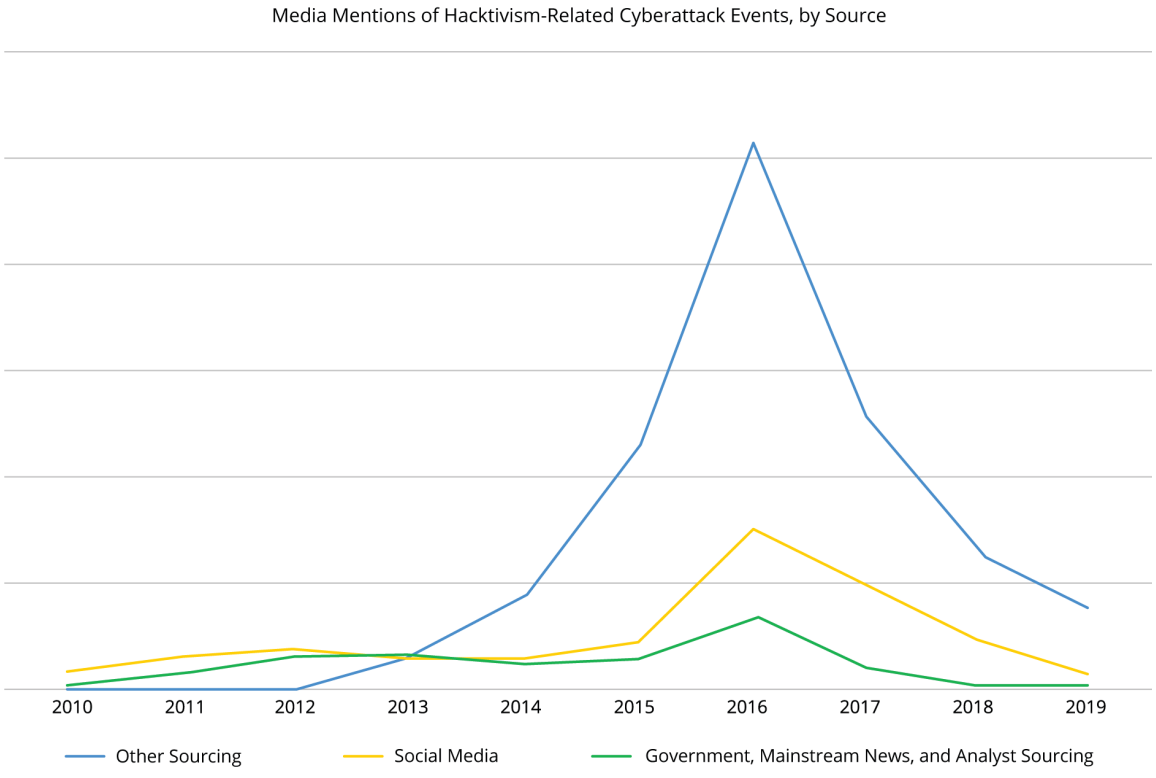
The Anonymous Hacking Collective is one of the few truly international groups of anonymized users whose hacking operations range from targeting political parties and large industry verticals, to non-hacktivist activities that target random organizations "for the lulz." While originating from a forum run by a Western moderator, the group has significant players around the globe. Anonymous's iconography and language has been adopted by multiple regional groups worldwide for different purposes, and has inspired other similar hacking groups, such as GhostShell.

Threat Analysis

Using the Recorded Future Platform, Insikt Group pulled all mentions of hacktivism-related cyberattacks, excluding social media as a source, across all Recorded Future sources over the last nine years. These sources include underground forums, technical blogs, and mainstream news, among other forms of communication. These mentions encompassed underground forum announcements of leaked data, news reporting of publicly disclosed attacks, and reports of individuals or hacktivist groups taking credit for individual attacks. Duplicates exist in the data, as operations can span multiple days, and multiple sources may report on the same issue. However, duplicates counted for a small portion of the data set and were left in. Our data and analysis indicates that, similar to research conducted by others over the past year, chatter surrounding hacktivist attacks has been in steep decline since a peak between 2015 and 2016.



Media mentions of hacktivism-related cyberattacks (2010–2019).



Media mentions of hacktivism-related cyberattacks by source type.

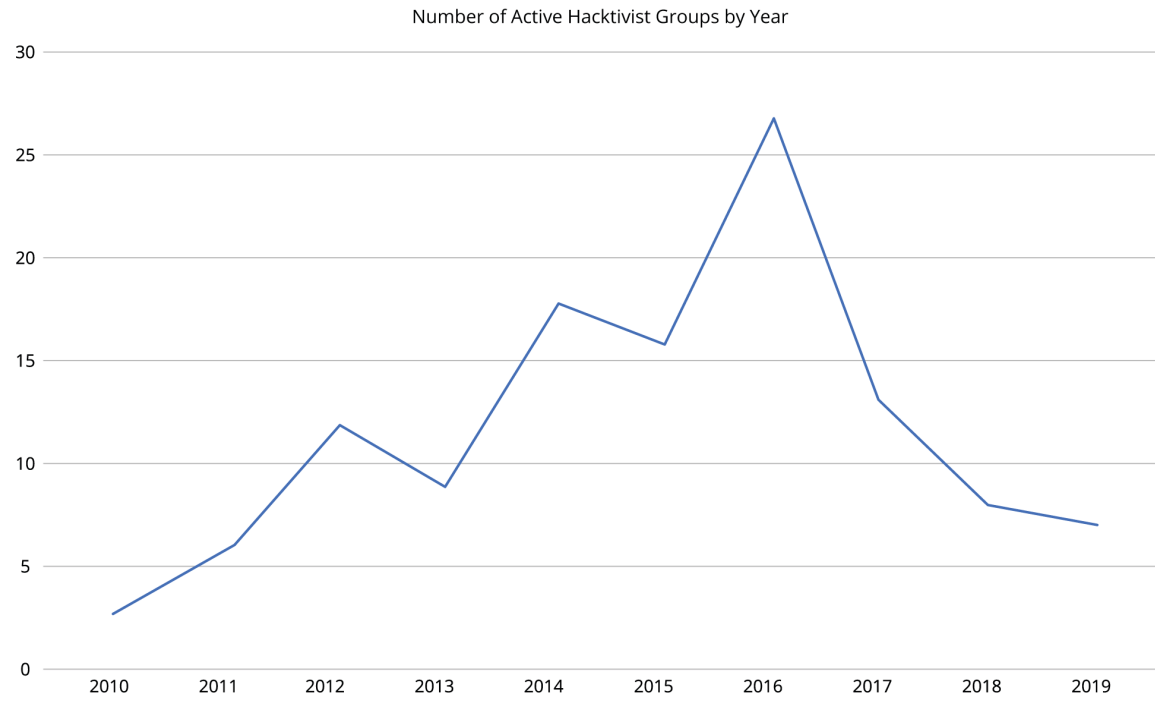
When including mentions of hacktivism-related cyberattacks on social media into the dataset, the social media mentions clearly dwarfed mentions elsewhere. Some of these mentions were found in other social media announcements of future attacks, or individuals claiming responsibility for attacks. However, mentions were just as frequently amplifications of the same announcements, or reposts of old news. The interest of many hacktivists in public recognition of their acts, whether legitimate or not, can result in an amplification effect on social media. This was especially the case in 2016. Recorded Future data shows that mentions of hacktivism-related cyberattacks have declined steeply across multiple media sources, including social media, over the last four years. Insikt Group assesses with medium confidence that this is in part due to a decline in amplifying discussions (e.g., news articles and social media shares) around hacktivism-related cyberattacks.

Trends by Attacker

Using the Recorded Future Platform, Insikt Group collected information on 81 hacktivist groups active over the last 10 years (listed in Appendix A). We included all threat groups with sociopolitical agendas under the "hacktivism" umbrella.. This grouping included the anti-establishment NullCrew, hacking crews associated with known terrorist organizations or nation-states, as well as the team behind the Ashley Madison breach.

While singular operations have involved the participation of 20 or more separate groups, we also defined active groups that were the primary force behind a widely reported upon operation that year as hacktivist groups. While we primarily defined members of certain hacktivist groups to be from a specific region (like the Middle East), we recognize that attribution and direct identification of hacktivists can be difficult for researchers and the media. An example is the group New World Hackers, which purportedly consisted of members from Russia, China, and India, but was later reported to primarily consist of a core group of college students from the U.S., the U.K., and Australia. Moreover, in certain cases, hacktivists from other countries have become involved in more international operations, or operations not associated with their particular region.

As illustrated in the graph below, Insikt Group observed that the number of active hacktivist groups per year has declined since 2016.



Number of active hacktivist groups by year.

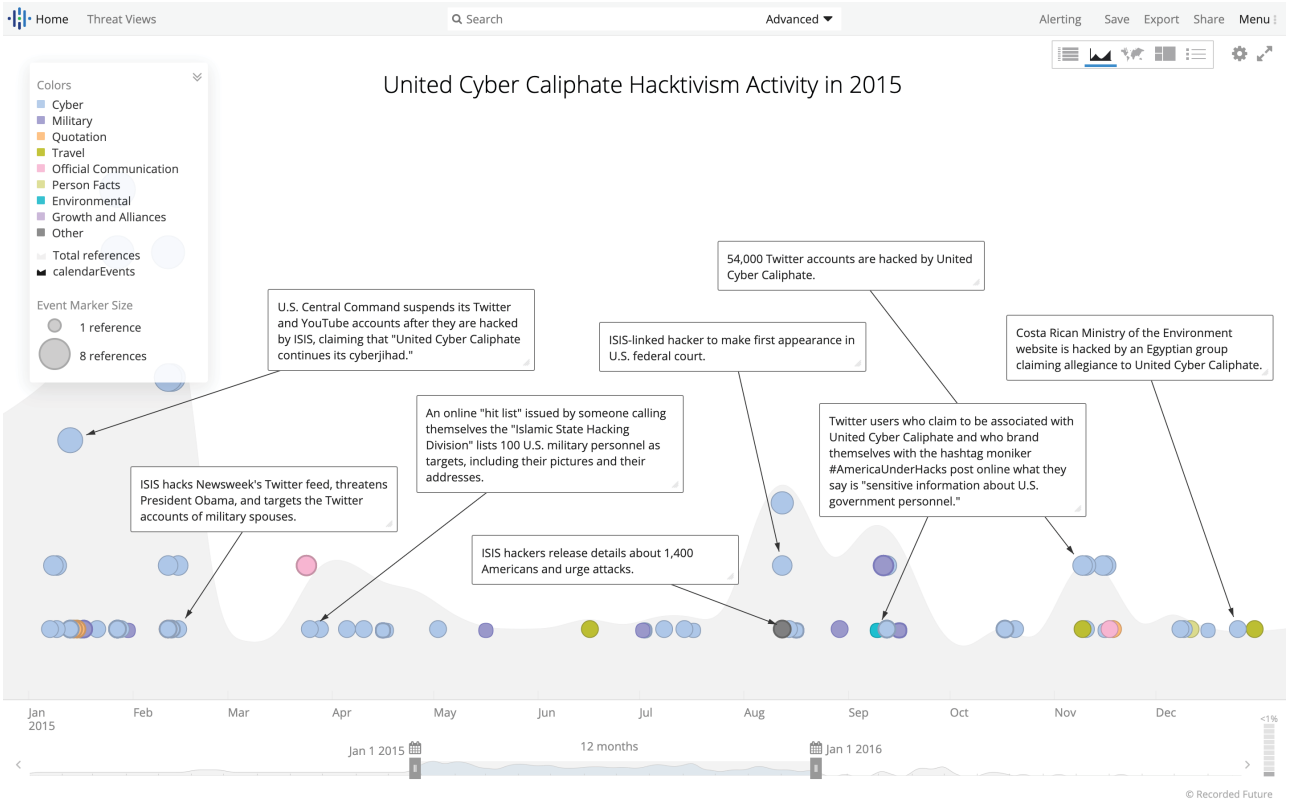
2013 saw a decline in active hacktivist groups, attributed by some to increased arrests and convictions deterring hacktivists from conducting sustained operations. There was also a decline in the number of successful campaigns in 2012. The cooperation of LulzSec leader Hector Monsegur with the FBI resulted in the arrests of multiple LulzSec members in 2012. In addition, charges were brought against members of Anonymous in Singapore in 2013. Separate to the public prosecutions, reports of Anonymous infighting started as early as 2011 and continued into 2013, suggesting that there was likely a fracturing of Anonymous during this time.

However, the number of hacktivist groups doubled in 2014 from the year prior. Recorded Future data shows that a majority of new hacktivist groups that emerged or were active during this year originated from the Middle East. Countries in this region during this time were experiencing periods of instability and conflict following the Arab Spring, known as the Arab Winter.

Various regional Anonymous Groups from Palestine, Syria, Jordan, and Lebanon paired up with AnonGh0st, the Gaza Hacker Team, Parastoo, Fallaga Team Tunisia, the Syrian Electronic Army, and the Al Qassam Cyber Fighters to participate in the second annual OpIsrael (also known as OpIsraeliBirthday). This operation targeted Israeli government and private sector websites, and encouraged hacktivists to deface and DDoS any and all Israeli organizations. In retaliation, the Israeli Elite Force hacktivism group published personally identifiable information (PII) belonging to multiple regional Anonymous group participants, uploading documents containing real names, locations, and photos of the attackers to Dropbox. At that time, there was a splintering of Anonymous organizations, with other Anonymous factions seemingly "at war" with the Syrian Electronic Army and affiliated groups, illustrating the factional quality of a nebulous organization such as Anonymous and similar hacktivist organizations. During this time, pro-ISIS activity within underground forums such as Shamukh Forum was also occurring, as laid out in Recorded Future's previous research.

Outside of the Middle East, multiple pro-Russian and pro-Ukrainian hacktivist and claimed hacktivist activity emerged in the wake of the annexation of Crimea in 2014. A pro-Russian hacking group calling themselves "Anonymous Ukraine" dumped emails of the Ukranian Democratic Alliance for Reform online, while CyberBerkut (a hacking group more closely tied to the Kremlin), took down websites of NATO and the Ukranian Ministry of Defense. On the pro-Ukrainian side, groups like the Ukraine Cyber Alliance and InfoNapalm have also released emails from top Kremlin officials and DDoSed or defaced Russian government websites.

In addition, 2014 and 2015 saw the rise of a hacktivist organization claiming to be linked to ISIS, but was in fact linked to the Russian government's GRU. The United Cyber Caliphate started out by breaking into the Youtube accounts of the U.S. Central Military Command (CENTCOM) during this time. While the compromised accounts dumped multiple U.S. Army files containing officer rosters, campaign models, and several war scenarios, these proved to be previously available, unclassified documents. The Cyber Caliphate also doxxed thousands of U.S. military personnel that same year.



Timeline of United Cyber Caliphate activity in 2015. (Source: Recorded Future)

A diverse collection of attackers and international operations emerged in 2015 and 2016. Operations were spurred by regional events ranging from the Flint Michigan water crisis to global campaigns to shut down escort service websites. Attacks originated from a variety of Anonymous chapters including Brazil, Poland, and the Philippines, as well as coordinated international pro-Islamic collectives and other international and regional groups. Major international Anonymous campaigns in this time period included Operation Isis, an attempt to counter ISIS and Operation Icarus, targeting the international finance system. Other attacks included

DDoS attacks on the BBC and Donald Trump's campaign website by the New World Hackers group, and attacks on universities conducted by GhostShell. Disputes between nations continued to spur nationalist actions such as the Turk Hack Team shutting down various U.S. Congress websites and hacktivist tit-for-tat between India and Pakistan.

Code for the Mirai botnet, one of the most effective DDoS botnets in history, was used by hacktivist groups after its source code was posted on Github by its original, non-hacktivist authors in October 2016. The Mirai botnet was able to send traffic to a target at speeds of up to 1 terabyte per second, enabling the DDoSing of a target more effectively than any other prior botnet. Multiple sets of actors utilized the source code to create their own botnets; groups attempted to use Mirai-variant botnets to target the campaign websites of Donald Trump and Hillary Clinton, as well as take out ISPs in Britain and LIberia.

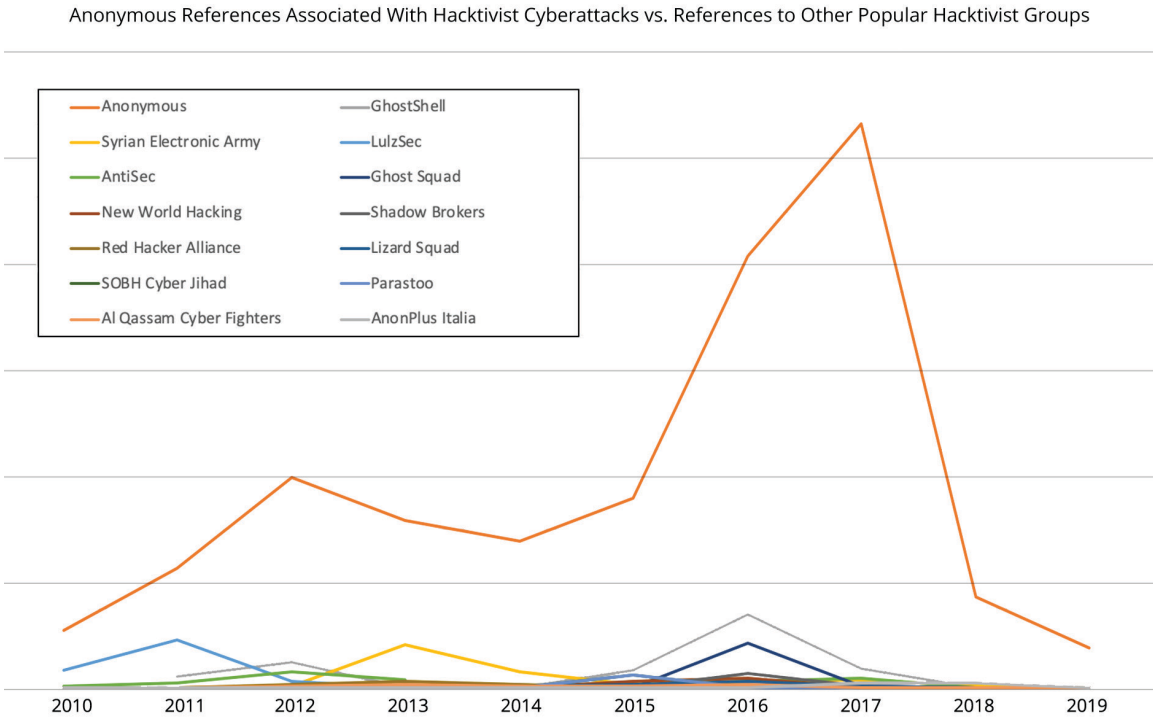
Anonymous also advertised the tool during Operation Icarus, a campaign targeting the global financial industry. Their initial actions in February 2016 included physical protests and DDoS attacks on bank infrastructure. Participants were also encouraged to use the Low Orbit Ion Cannon (LOIC), an open source DDoS tool previously used by Anonymous in successful DDoS flood attacks. In addition, the creation of the Mirai botnet itself also spurred further hacktivist operations; BrickerBot was malware created by a hacktivist to "brick" vulnerable IoT devices and routers in order to prevent the active device from becoming a new addition to future botnets.

Multiple state-sponsored hacktivism groups were also active during 2016. The Shadow Brokers began dumping classified NSA files online in the summer of 2016, and alleged "lone-wolf" Guccifer 2.0 stole emails from the U.S. Democratic National Committee, the Clinton Foundation, and the inbox of Former White House Chief of Staff John Podesta, subsequently sending the documents to DCLeaks[.]com. Both the Shadow Brokers and Guccifer 2.0 have been linked to the Russian state and to Russia's GRU, respectively. These groups joined the ranks of "hacking groups" linked to nation-states, previously comprised of North Korea's Guardians of Peace (responsible for the Sony hack in 2014), Iran's Cutting Sword of Justice (who claimed credit for the cyberattack on Saudi Aramco in 2015), Russia's CyberBerkut, and the Syrian Electronic Army, among others.

Our research indicates that since 2016, the number of hacktivist groups (state-linked or otherwise) publicly conducting cyber campaigns has steadily declined, which correlates with the decline in mentions of hacktivism-based cyberattacks in the previous section. In addition, we assess that large-scale international campaigns have also occurred less frequently. Regardless of the decline, however, Recorded Future analysis demonstrates that regional Anonymous chapters have been consistently active, being referenced alongside hacktivist cyberattack mentions over a hundred times more than other hacktivist groups in certain years.

In fact, Anonymous's peak number of references occured in 2017, when overall mentions of hacktivism were in decline. We assess that there are three possible (not mutually exclusive) drivers for this trend:

1. Anonymous's history as one of the first, completely decentralized hacktivist groups allows individuals to create regional branches under the Anonymous banner, and attracts hacktivists in that region who are familiar with the Anonymous name.
2. Due to its (and other hacktivist groups') decentralized nature, any individual conducting hacktivism on the internet can claim that their activity is directed by Anonymous.
3. Different Anonymous regional branches can have different missions and targets. The majority of our data surrounding Anonymous hacktivism after 2014 referenced Anonymous chapters outside the United States (such as Anonymous International and Anonymous Italia), and different chapters have focused on targeting different organizations.



References to Anonymous being associated with hacktivist cyberattacks versus references to other groups.

Trends by Attack Vector

While multiple hacktivist groups have risen and fallen in the last decade, attack vectors surrounding hacktivist cyberattacks have remained consistent. Hacktivism-related attacks usually result in one of the four following effects:

1. Denial of service
2. Defacement of public facing websites and accounts
3. Release of sensitive data
4. Takeover of key accounts

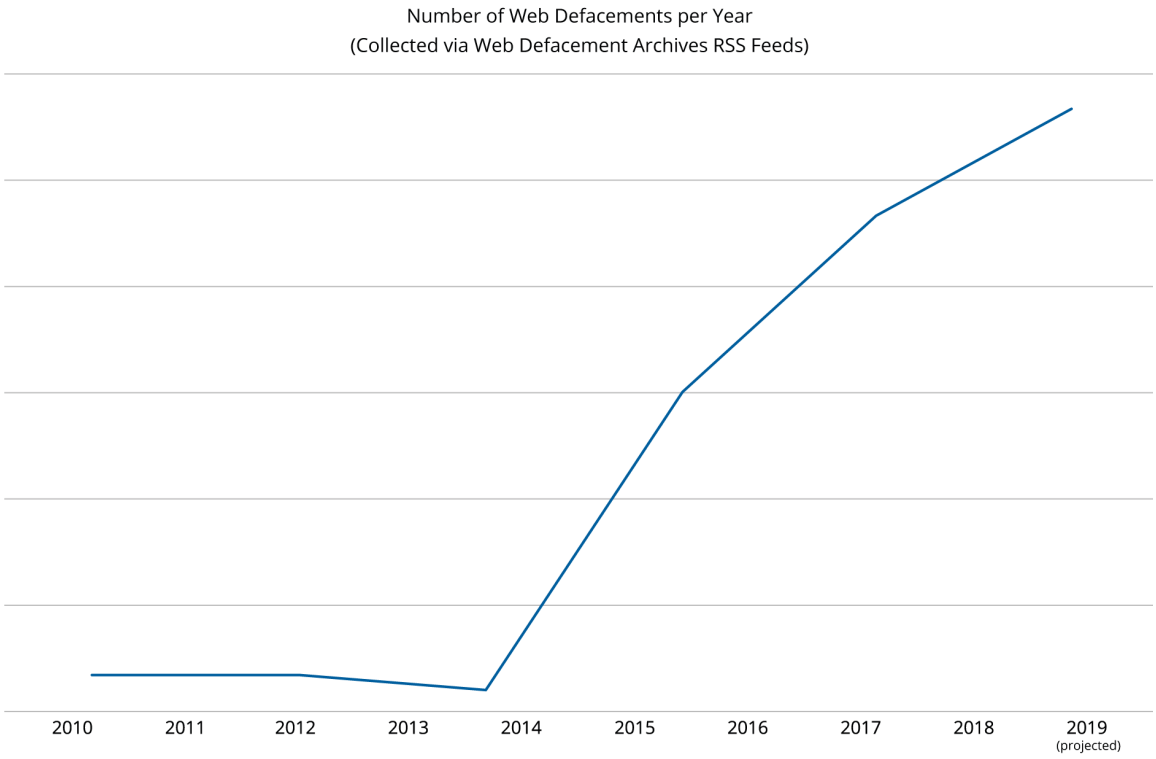
In certain cases, hacktivist groups have even wiped internal data belonging to target organizations, like RedHack's erasure of over $670 billion in electricity bills belonging to Turkish citizens. Most of these attacks are conducted to prevent availability or integrity of certain services, publicly shame users of the services, or to publicly shame the services themselves. These measures may be attempted all at once, as in the 2011 incident in which Antisec (an offshoot of Anonymous) breached the network of the private intelligence firm Stratfor, resulting in the theft of approximately 200GB of data that was subsequently provided to Wikileaks to dox the firm and its clients, while the company website was also shut down.

Insikt Group has listed common attack vectors associated with hacktivist operations resulting in the aforementioned desired effects in the following table. Based on the analysis of Recorded Future data and other publicly available reporting, Insikt Group assesses with high confidence that these attack vectors have remained popular over the last decade and are still popular today. However, quality of commodity spyware, credibility of spearphishing websites, and DDoS capabilities have all risen in the last decade as well, with the dissemination of the LOIC and Mirai, as well as other widely available tools.

Desired Effect	Attack Vectors
Denial of Service	Single-Machine DoS Attack Multiple-Machine DDoS Attack
Defacement, Release of Sensitive Data, or Destruction of Sensitive Data	Cross-Site Scripting (XSS) Brute-Forcing Credentials SQL/noSQL Injection Metasploit/Openly Available Penetration Testing Tools Spearphishing With Malicious Links or Attachments Watering-Hole Attacks Social Engineering to Obtain Accounts Utilization of Commodity Spyware or Other Malware
Theft of Key Accounts	Brute-Forcing Credentials Credential Stuffing Attacks Spearphishing With Malicious Links Social Engineering/OSINT

Commonly utilized attack vectors to achieve hacktivism-related cyber effects.

Additionally, Insikt Group pulled all archived web defacement events collected by Recorded Future in the last six years. As seen in the following graph, the number of web defacements has increased over the last three years, even though mentions of hacktivism have slowly declined. However, because web defacement sites catalogue defacements from both cybercriminals and hacktivists, it is uncertain how much of this is hacktivist activity. Regardless, the number of successful web defacements demonstrate the ever present effectiveness of this attack vector. The presence of newer, automated web defacement tools have likely also scaled up the number of websites targeted in the last decade.



Recorded events from web defacement archives, separated by year.

Trends by Target

Insikt Group used the Recorded Future Platform to pull all mentions of countries and companies named as victims of hacktivism, and manually processed the data to pull out the victims of hacktivist campaigns associated with the 81 active hacktivist groups mentioned above.

We discovered that, while the occasional international company or industry has been targeted due to general mistrust or upset, organizations local to or involved in regional conflicts important to dissident groups have been primary targets for hacktivists every year since 2010. Among those organizations targeted, most resulted from controversial or annual international events. For example, LulzSec targeted the Arizona Police Department and other organizations in the Arizona state government over a controversial immigration bill in 2011, and also broke into systems belonging to the Atlanta chapter of FBI affiliate InfraGard.

In 2012, after disputes over the Senkaku Islands caused tensions between China and Japan, China's Hongke Union hacktivist group listed over 300 Japanese websites for targeted attacks on message boards. In 2014, #OpFrance was created by Muslim hacktivists in support of the attack on French satirical magazine Charlie Hebdo, and multiple subsequent similar operations followed it. Elections and local politics can also be a trigger for hacktivist activity. In 2019, data affecting German political parties (except the far-right "Alternative for Germany" party) was leaked. In addition, multiple United States alt-right organizations have been targeted by Anonymous since 2017. One operation, #OpDomesticTerrorism, specifically called out Donald Trump's presidency for bigotry.

While national and regional government websites were also consistent targets, hacktivists will occasionally target any organization operating from a country to spread chaos. #OpSudan was an operation kicked off by hacktivism Sudanese dissidents and other groups in June 2019, targeting the Sudanese government. The groups participating in the operation announced their targets on Pastebin, stating that the operation was in protest of the Sudanese government's crackdown on free speech and internet access. The target list released on Pastebin, however, contained not only gov[.]sd domains, but also domains of multiple universities, internet service providers, and even the website of a flour producer.

While operations targeting specific industries do occur (such as #OpSaveTheArctic and #OpPetrol, targeting major oil companies in 2012 and 2014, respectively), they have not occurred as frequently as attacks against government websites (from both domestic and regional hacktivist groups), or as frequently as attacks against organizations who have been involved in an emerging conflict.

Overall Trends

From 2010 to 2015, Insikt Group observed the emergence of online hacking groups following regional conflicts and trends, as well as the growth of more decentralized international groups like Anonymous. However, after a spike in international operations conducted by large groups of hacktivists around 2015, Insikt Group observed a return to regional hacking groups as the number of groups and operations began to decline. Insikt Group also assesses that the following trends in hacktivist activity will continue in the near term.

Improved Security of Targets Combined With Static Attack Vector Evolution

In the past decade, since the heyday of Anonymous, many potential hacktivist targets have significantly improved their security controls. The number of large enterprises susceptible to SQL injection attacks or DDoS floods have decreased, likely due to more mature website structures and the use of DDoS protection services like Akamai and Cloudflare. Although some hacktivist actors are highly skilled, more often than not many members of a hacktivist organization are not skilled and are forced to rely upon simple and outdated tools and techniques that are easily defeated by competent network defenders. There are still many targets susceptible to common hacktivist attack methodologies, but historic targets such as multinational financial institutions and large federal government organizations have in general made improvements to their security posture over the years.

Hacktivism as a False Flag

As nation-states and other advanced entities have been observed shifting to common tools and malware to obscure their activities, some operations have been similarly identified as conducted under the false flag of hacktivist or lone hacker activity. Some of the most widely known examples of such are the use of the Guccifer 2.0 identity by Russian intelligence, the use of the "Guardians of Peace" subterfuge by North Korea in its attack on Sony, and the Iranian-sponsored DDoS attacks on U.S. banks claimed as the work of Cyber Fighters of Izz ad-Din al-Qassam hacktivists. Although espionage operations have made use of false-flag tactics for a long time, the

rise of voluntary hacktivist organizations allows an operator to easily claim an affiliation or identification with hacktivist activity, which may be difficult to disprove.

There is also evidence that criminals have used insecure hacktivist or hacker infrastructure to further their aims. The security firm TrendMicro reported in 2018 that the systems of those involved in website defacement were infected with the banking trojan Ramnit, after which they had their defacement templates altered to include a malicious VBscript that spread Ramnit via subsequently defaced websites.

Prosecution as an Effective Deterrent

Publicized law enforcement efforts led by Western governments (such as the British prosecution of Kane Gamble for sharing stolen data with WikiLeaks and the cooperation of LulzSec leader Hector Monsegur with the FBI) have likely lead to a reduction in the numbers of "volunteers" who previously saw little downside in participating in hacktivist operations. Outside of the Western Hemisphere, charges have been brought against members of Anonymous in Singapore, the Muslim Cyber Army in Indonesia, and others. Recorded Future assesses that the pressures of potential legal repercussions, as well as infighting and distrust among group members, has lead to a decrease in activity by the most prolific group, Anonymous. The loose association of members inherent in many hacktivist organizations allows group members to simply cease participation, or easily splinter into factions. As the number of casual participants declines, the percentage of highly motivated actors remaining in the groups increases and may result in more aggressive, but less broadly supported, activity.

Hacktivism by Terrorist Groups

The definition of hacktivism (cyberattacks for political or social activism) also applies to more extreme activism. Multiple terrorist groups on the United States Foreign Terrorist Organizations list have conducted attacks commonly associated with hacktivism to further their message online. Moreover, one country's freedom

fighter is another country's cyber terrorist when it comes to regional conflicts; #OpIsrael and Anonymous have been referred to by pro-Israeli newspapers as "cyber terrorism" on multiple occasions.

Regardless, we expect that hacktivist-sourced "terrorist" activity currently and in the near future will involve multimodal operations, such as the online release of the stolen PII of numerous military and government employees with the encouragement to conduct physical attacks by ISIS-affiliated actors. This resulted in the conviction of Kosovo resident Ardit Ferizi on both hacking and terrorism charges for his involvement in the scheme. We believe that entities such as ISIS which are involved both in military and cyber conflict can be motivated to conduct more destructive cyberattacks.

Although no attack conducted directly via computer networks has been documented to have caused deaths, the targeting of industrial safety systems such as TRISIS and ransomware attacks on hospitals, which could result in physical injury, have been observed. Such attacks to date have not been identified as the work of hacktivist groups, however, and are more likely to be conducted by nation-state actors or criminals.

Outlook

We assess that hacktivism as a technique will persist and will be conducted by more motivated and often more capable actors. Non-state-sponsored volunteer hacktivist groups in the future may also consist of more dedicated and skilled members. With an increase in operations from nation-states involving coordinated campaigns with hacktivists of like mind or government operators acting as hacktivists, the use of advanced techniques and more persistent activity may be expected from purported hacktivists.

Our analysis concludes that government agencies and enterprises involved in regional flashpoints such as the Middle East, in politically sensitive endeavors, or in often-targeted sectors including finance and the defense industrial base, should consider themselves potential targets of hacktivist action. Other critical sectors (e.g., healthcare, information technology, transportation, and energy) may also find themselves targets of opposing nationalist and militant hacktivists.

We recommend that mitigation of hacktivist attacks include appropriate defenses against the typical techniques used by these actors, which include phishing, credential theft, website compromise, DDoS, and others. Further observing and understanding the broad threat environment and any hacktivist groups that may take action against an organization will allow defenders to identify new tactics and techniques, and subsequently, employ more effective defensive measures.

Appendix A — List of Key Hacktivist Groups Analyzed

1937CN	Indian hackers	TeaMp0isoN
Afghan Hackers	Indonesian Cyber Freedom	TeaMp0isoN
Al Qassam Cyber Fighters	Indonesian hackers	Team Digi7al
AnonGh0st	Islamic State in Iraq and the Levant	Telecomix
AnonPlus	Israeli Elite Force	The Impact Team
AnonPlus Italia	Lab Dookhtegan	Turkish hackers
Anonsec	Legion	United Cyber Caliphate
Anonymous	Lizard Squad	
Anonymous Brasil	LulzSec	
Anonymous Cambodia	LulzSec Italy	
Anonymous International	LulzSec Philippines	
Anonymous Italy	Moroccan Agent Secret	
Anonymous Jordan	Moroccan hackers	
Anonymous Lebanon	n0sis	
Anonymous Philippines	New Romanic Army	
Anonymous Poland	New World Hacking	
Anonymous Syria	Nigerian hackers	
Anonymous Syria	Nightmare	
Anonymous Ukraine	NullCrew	
AntiSec	Pak Cyber Attackers	
Asor Hack Team	Pakistani hackers	
Asor Hack Team	Pakistani hackers	
Bangladeshi hackers	Parastoo	
Brazilian hackers	Phantom Squad	
CtrlSec	Phineas Fisher	
CyberBerkut	Pro-Israeli hackers	
Digital Revolution	pyknic	
Fallaga Team Tunisia	Red Hacker Alliance	
FancyBear Hackers	RedHack	
Gaza Hacker Team	RedHack	
Ghost Squad	Romanian Hackers	
Ghost Squad	SOBH Cyber Jihad	
GhostSec	Shad0wS3C	
GhostShell	Shadow Brokers	
Guccifer 2.0	Shadow Brokers	
Hack the Planet	Syrian Electronic Army	
IDF-Team	TeaM System Dz	

Appendix B — MITRE ATT&CK Techniques

MITRE ATT&CK Mapping

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port	Data Destruction
Exploit Public-Facing Application ●	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media	Data Encrypted for Impact
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy	Defacement ●
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol	Disk Content Wipe ●
Spearphishing Attachment ●	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol	Disk Structure Wipe
Spearphishing Link ●	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding	Endpoint Denial of Service ●
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels	Network Denial of Service ●
Valid Accounts ●	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-Stage Channels	Resource Hijacking
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy	Runtime Data Manipulation
	LSASS Driver	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	SSH Hijacking	Screen Capture		Multiband Communication	Service Stop ●
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	Keychain	Remote System Discovery	Shared Webroot	Video Capture		Multilayer Encryption	Stored Data Manipulation
	Local Job Scheduling	Create Account	Launch Daemon	DLL Side-Loading	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking	Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Deobfuscate/Decode Files or Information	Network Sniffing	System Information Discovery	Third-party Software			Remote Access Tools	
	PowerShell	Dylib Hijacking	Path Interception	Disabling Security Tools	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares			Remote File Copy	
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management			Standard Application Layer Protocol	
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery				Standard Cryptographic Protocol	
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication Interception	System Service Discovery				Standard Non-Application Layer Protocol	
	Scheduled Task	Hooking	SID-History Injection	File Permissions Modification		System Time Discovery				Uncommonly Used Port	
	Scripting	Hypervisor	Scheduled Task	File System Logical Offsets						Web Service	
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Gatekeeper Bypass							
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	HISTCONTROL							
	Signed Script Proxy Execution	LC_LOAD_DYLIB Addition	Startup Items	Hidden Files and Directories							
	Source	LSASS Driver	Sudo Caching	Hidden Users							
	Space after Filename	Launch Agent	Sudo	Hidden Window							
	Third-party Software	Launch Daemon	Valid Accounts	Image File Execution Options Injection							
	Trap	Launchctl	Web Shell	Indicator Blocking							
	Trusted Developer Utilities	Local Job Scheduling		Indicator Removal from Tools							
	User Execution	Login Item		Indicator Removal on Host							
	Windows Management Instrumentation	Logon Scripts		Indirect Command Execution							
	Windows Remote Management	Modify Existing Service		Install Root Certificate							
	XSL Script Processing	Netsh Helper DLL		InstallUtil							
		New Service		LC_MAIN Hijacking							
		Office Application Startup		Launchctl							
		Path Interception		Masquerading							
		Plist Modification		Modify Registry							
		Port Knocking		Mshta							
		Port Monitors		NTFS File Attributes							
		Rc.common		Network Share Connection Removal							
		Re-opened Applications		Obfuscated Files or Information							
		Redundant Access		Plist Modification							
		Registry Run Keys / Startup Folder		Port Knocking							
		SIP and Trust Provider Hijacking		Process Doppelgänging							
		Scheduled Task		Process Hollowing							
		Screensaver		Process Injection							
		Security Support Provider		Redundant Access							
		Service Registry Permissions Weakness		Regsvcs/Regasm							
		Setuid and Setgid		Regsvr32							
		Shortcut Modification		Rootkit							
		Startup Items		Rundll32							
		System Firmware		SIP and Trust Provider Hijacking							
		Time Providers		Scripting							
		Trap		Signed Binary Proxy Execution							
		Valid Accounts		Signed Script Proxy Execution							
		Web Shell		Software Packing							
		Windows Management Instrumentation Event Subscription		Space after Filename							
		Winlogon Helper DLL		Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Web Service							
				XSL Script Processing							

LEGEND

● Common Initial Access Vectors and Impact from Hacktivist Campaigns

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.