



A Deep Dive into Defacement: How Geopolitical Events Trigger Web Attacks

Marco Balduzzi, Ryan Flores, Lion Gu, and Federico Maggi
with Vincenzo Ciancaglini, Roel Reyes, and Akira Urano

Trend Micro Forward-Looking Threat Research (FTR) Team

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Contents

5

Our Approach to the Investigation

7

Targets and Methods of Website Defacers

11

Real World Conflicts Reflected in Cyberspace

54

Auxiliary Activities of Defacement Groups

58

Conclusion

Web attacks—attacks that compromise internet assets like mail servers, cloud infrastructures, and websites—are troubling phenomena. The research community has put considerable effort into investigating these incidents but has mostly focused on detecting attacks and not delving into the *reasons* behind these attacks.

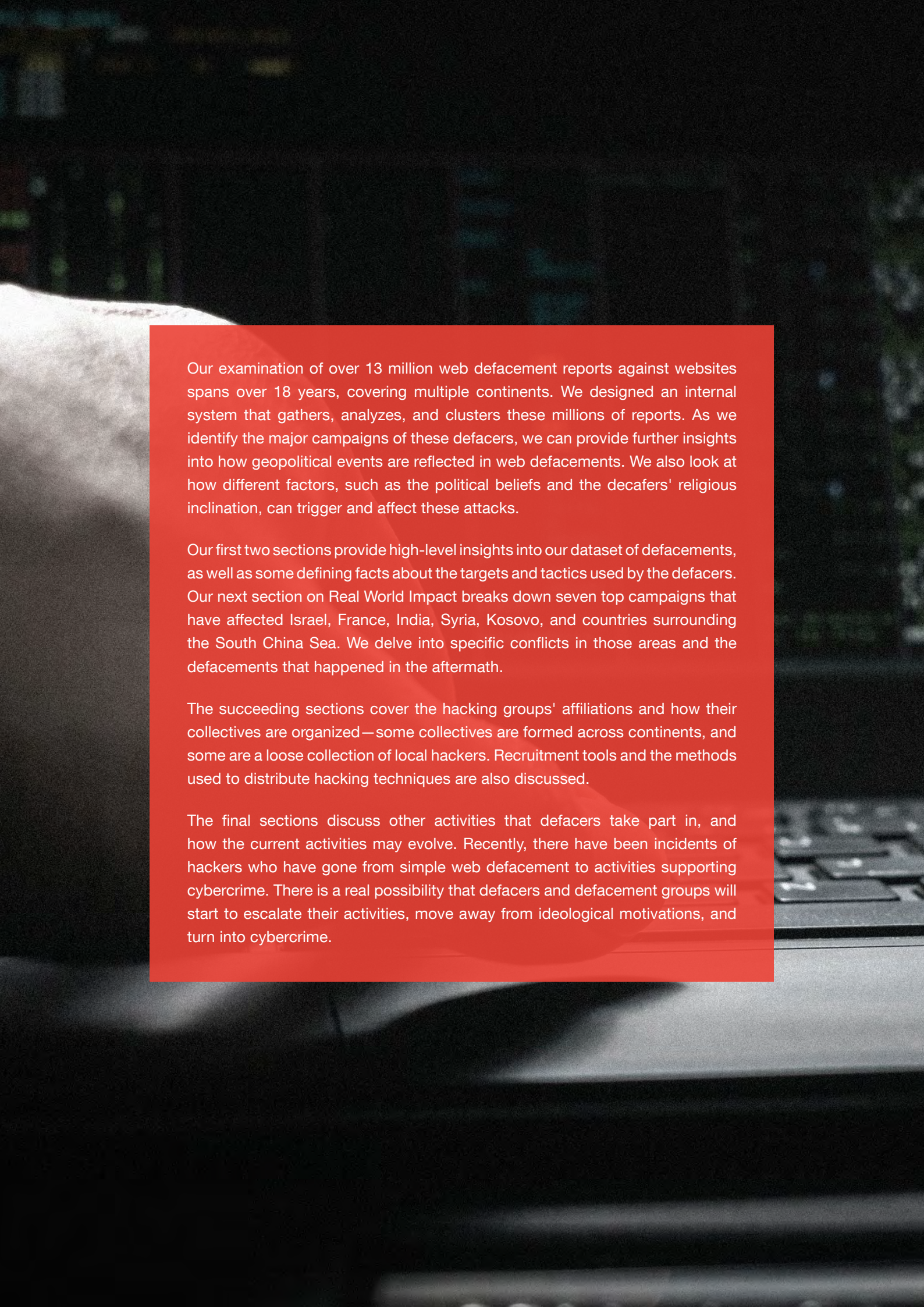
Of course, the typical cybercriminal's goal is to profit. They might compromise websites to push ransomware, or they could try and steal data—recent breaches show that information is an increasingly valuable commodity. But, as this paper discusses, more emotional motivations, such as patriotism, specific real-world events or simply hacktivism, can also trigger compromises.

Web defacement hacktivism is the practice of subverting a website with the goal of promoting a specific agenda or political ideology. Methods may vary, but when hacktivists compromise a website, the usual tactic involves replacing the original page with their version—a practice that is called web defacement.

Hacktivism is mainly linked to web defacement, but a hacktivist (the attacker) can also be involved in traffic redirection (from a legitimate site to an attacker-owned site), denial of service (a form of service disruption), and malware distribution to support their particular cause.

Dedicated websites like Zone-H¹ collect evidence of web defacements and defacers can voluntarily advertise their compromise by submitting a report.

Elaborating on the reasons behind web defacements at scale is not as easy as it seems. While someone could theorize that geopolitical events and conflicts influence cybercriminals' attacks against websites and their choice of victims, corroborating this phenomenon requires large-scale analysis.

A close-up, low-angle shot of a person's hand typing on a laptop keyboard. The background is dark and out of focus, showing some greenery. A semi-transparent red rectangular box is overlaid on the left side of the image, containing white text. The text is arranged in four paragraphs, each separated by a small gap. The overall mood is professional and tech-oriented.

Our examination of over 13 million web defacement reports against websites spans over 18 years, covering multiple continents. We designed an internal system that gathers, analyzes, and clusters these millions of reports. As we identify the major campaigns of these defacers, we can provide further insights into how geopolitical events are reflected in web defacements. We also look at how different factors, such as the political beliefs and the defacers' religious inclination, can trigger and affect these attacks.

Our first two sections provide high-level insights into our dataset of defacements, as well as some defining facts about the targets and tactics used by the defacers. Our next section on Real World Impact breaks down seven top campaigns that have affected Israel, France, India, Syria, Kosovo, and countries surrounding the South China Sea. We delve into specific conflicts in those areas and the defacements that happened in the aftermath.

The succeeding sections cover the hacking groups' affiliations and how their collectives are organized—some collectives are formed across continents, and some are a loose collection of local hackers. Recruitment tools and the methods used to distribute hacking techniques are also discussed.

The final sections discuss other activities that defacers take part in, and how the current activities may evolve. Recently, there have been incidents of hackers who have gone from simple web defacement to activities supporting cybercrime. There is a real possibility that defacers and defacement groups will start to escalate their activities, move away from ideological motivations, and turn into cybercrime.

Our Approach to the Investigation

Our objectives include exploring motivations and influences behind website defacements, focusing on how geopolitical events act as triggers for web defacement activities. To better understand these dynamics globally, we gathered web defacement reports from third-party sources and processed them with an automated system we designed specifically for this purpose.

Each web defacement report consists of:

1. Meta-information on the defacement, such as timestamp, website URL, the defacer's name, vulnerability, and more.
2. The deface page planted by the defacer (or modified, if this is the case). The deface page comes in the form of a source code (HTML/JS/CCS) and may contain small-sized external resources such as images. Additional content is fetched dynamically at analysis-time.

Our system automatically analyzes each deface page via two components:

1. A static-code analyzer that extracts representative features (i.e., characteristics) from the page (like title, length, and encoding) in an offline manner.
2. A dynamic-code analyzer that renders the page with a headless browser and extracts additional features in an online fashion. This analyzer works better with dynamically generated pages (e.g., when a link is generated via JavaScript) or pages with external content like embedded streams of songs.

The output of these components is a set of features that describe the page at high-level. These features are used as input for the following component: the campaign detector.

The campaign detector looks for defacements that—we believe—are conducted by the same actor or criminal group. This is often the case with campaigns wherein multiple actors unite and conduct defacements that relate to each other, such as those with similar target choices or deface pages. In fact, defacers enlisted on the same campaign are usually provided with a template for rendering similar

deface pages. These templates provide consistency in promoting the criminal group and spreading the campaign's propaganda and motivations.

This component groups similar pages accordingly, and represents them in form of clusters of *web defacement campaigns*. For this process, we make use of machine learning. We apply unsupervised learning to a set of features that well represents a summary of the pages — these are received from the static and dynamic analyzers mentioned before. The process automatically detects new campaigns and labels them for inspection. The result of this processing is indexed in an elastic-search back end and visualized via a web console. For each campaign, the console allows the analyst to inspect information like the lifespan of the campaign, the composition of the deface pages, as well as that of their actors. The console also allows analysis on how criminal groups are organized and if/when a certain actor belongs to multiple groups or moves from one to another. We will discuss the details of our system in a follow-up paper that will be released later in the year.

Targets and Methods of Website Defacers

As previously stated, our work is based on a large-scale analysis of 13 million website defacements that we collected from the following data sources:

- Zone-H²: 12,303,240 defacement incidents
- Hack-CN³: 386,705 defacement incidents
- Mirror Zone⁴ (now offline): 195,398 defacement incidents
- Hack Mirror⁵: 68,980 defacement incidents
- MyDeface⁶ (now offline): 37,843 defacement incidents

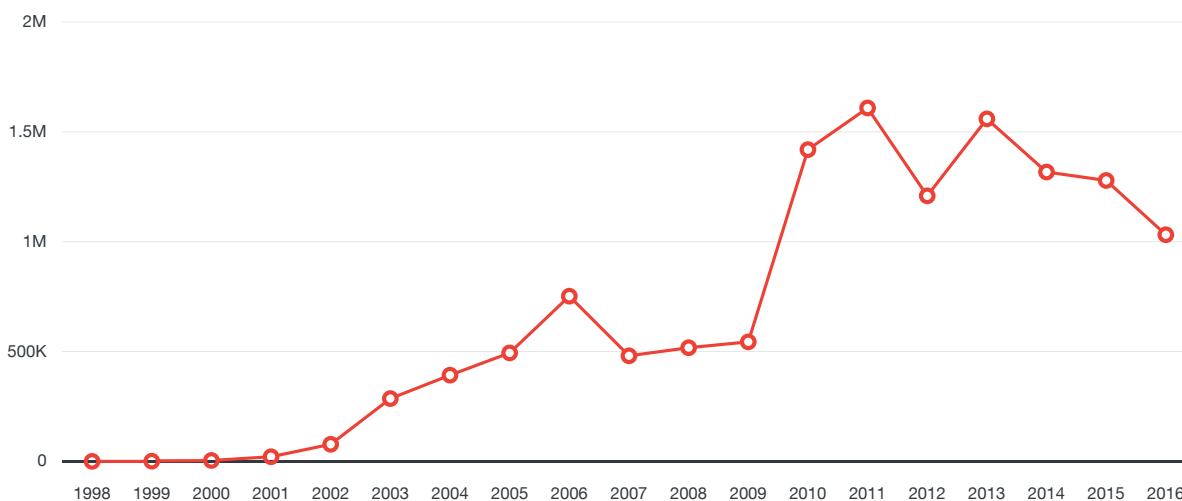


Figure 1. The rate of web defacement records per year

The total number of unique defacers is 104,135, and the total number of unique compromised domains is 9,929,484. Note that one domain can have multiple incidents recorded.

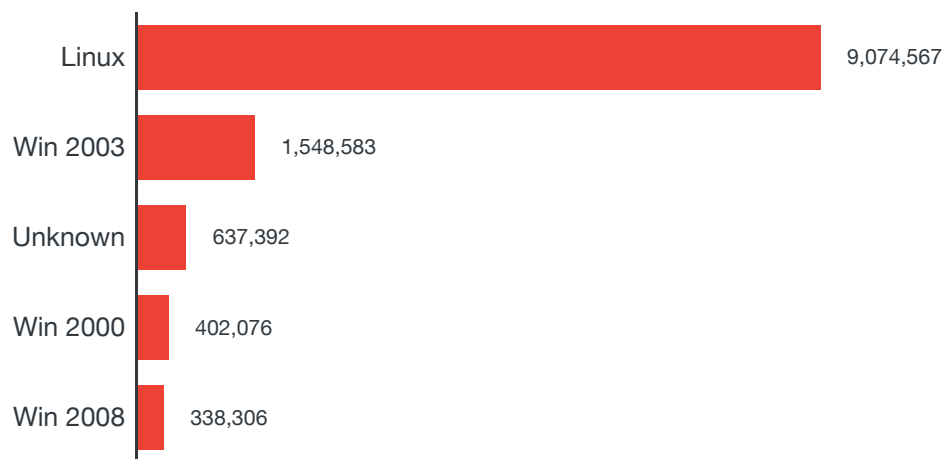


Figure 2. Operating systems of defaced web sites

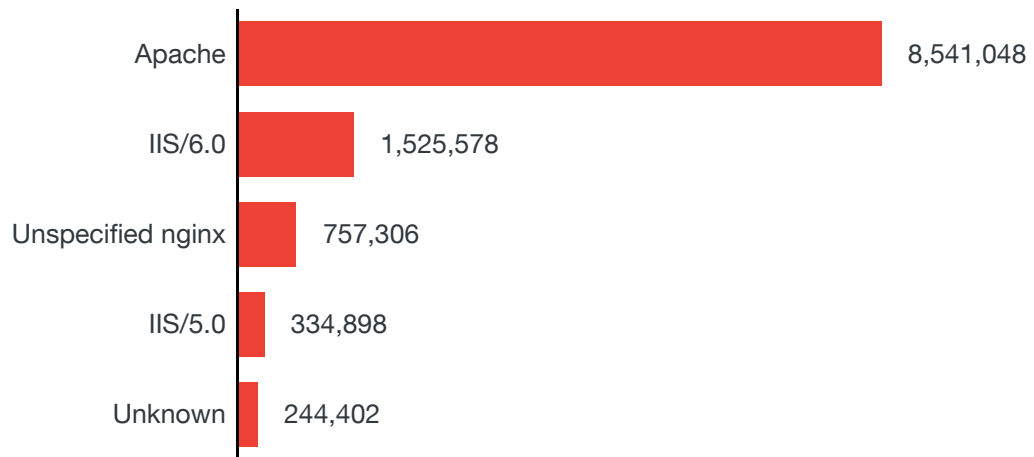


Figure 3. Web servers of defaced websites

Based on the metadata voluntarily provided by the defacers (which we cannot validate), here is a visual representation of the class of vulnerabilities leveraged by the attackers:

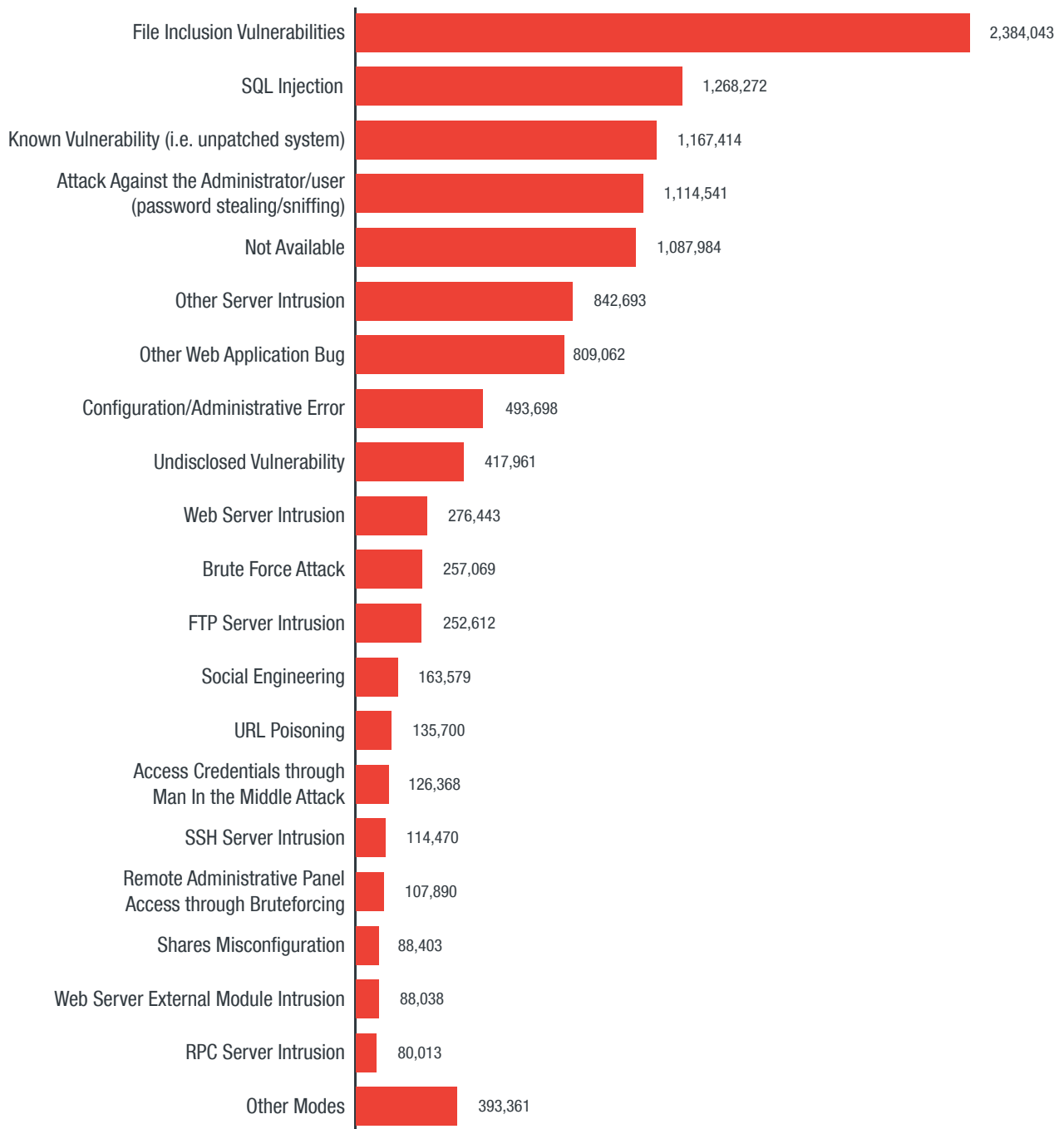


Figure 4. The methods of hacking as reported by defacers, based on defacement ID Information

The Role of Social Media

We observed that defacers voluntarily leave contact information upon compromise, based on the features (i.e., characteristics) automatically extracted during the analysis of the deface pages. It seems to be common practice for attackers that push propaganda to advertise their beliefs and refer their “viewers” to social networking sites or provide contact emails of the group.

Overall, we found that emails and Twitter are the primary forms of advertisement, with 25% (email) and 8% (Twitter) of pages displaying at least one of these. In fact, 6% of pages have multiple contact emails. In contrast, the telephone seems to be an unloved form of contact—only 3% of our attack records have telephone information. Not a surprising percentage since it may expose the defacer to attribution.

Another interesting aspect of propaganda-driven attacks on websites is the addition of streaming—songs played in the background of the page or even visual aspects. Our data found that 32% of the defacements have an embedded URL referencing either a streaming provider (like YouTube) or an audio file hosted on an external resource that is most likely another compromised machine. We manually investigated some of these cases and confirmed that most of these songs are related to religion.

Real-World Conflicts Reflected in Cyberspace

Mass attacks, or attacks that typically use automated hacking tools to compromise as many websites as possible indiscriminately, are common across the web. But in the course of our research, we noted a more coordinated form of attack that we labeled “campaigns”. In a campaign, the attackers launch specific attacks as a reaction to certain events, to push an agenda, make known their grievances, or spread political messages.

Our system allowed us to identify the top seven campaigns connected to and motivated by real-world conflicts. In the graph below, the horizontal (X) axis pertains to the number of attackers participating in a particular campaign, while the vertical (Y) axis maps the number of hacktivism-related defacements on record. The data shows that the #OpIsrael campaign garnered the most number of attackers, while Free Kashmir has the most number of defacements. We will delve deeper into these campaigns in the succeeding sections.

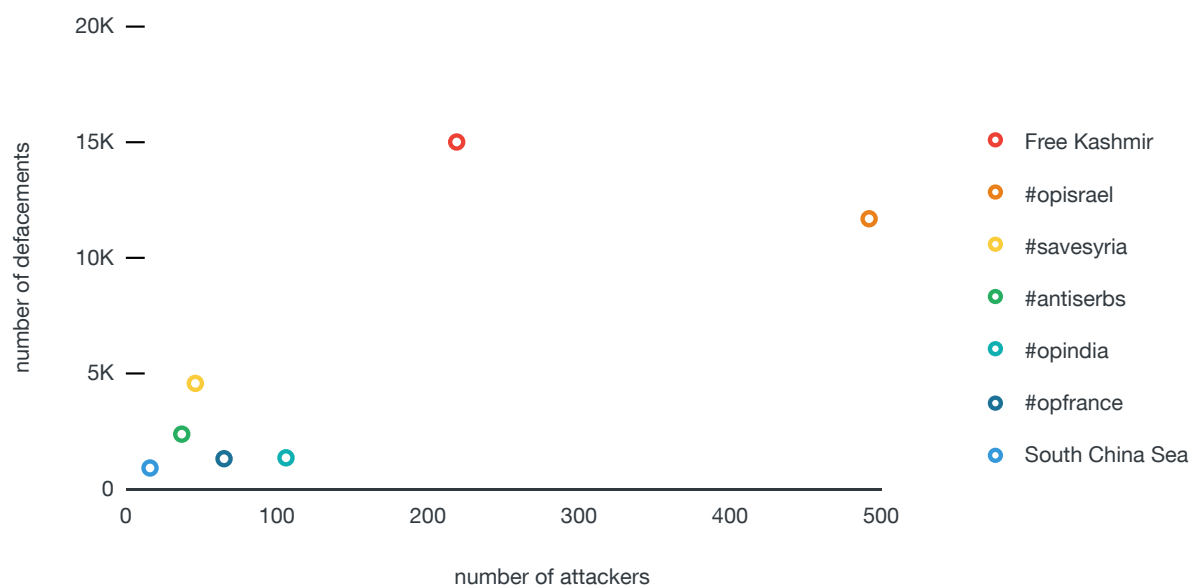


Figure 5. Overview of the top seven defacement campaigns from collected data

Conflicts Spark Anti-Israel Defacement Campaigns

So far, we've identified three major anti-Israel web defacement campaigns. The first (and the longest) is #OpIsrael, which is composed of several campaigns supported by different groups. Then there is the #OpSaveGaza campaign, which is a short, but highly effective defacement campaign in reaction to Israel's Operation Protective Edge. Last is #OpBader / #ElectronicBader / #BaderOperation, a loosely organized campaign with multiple groups participating that has gained traction since May 2016.

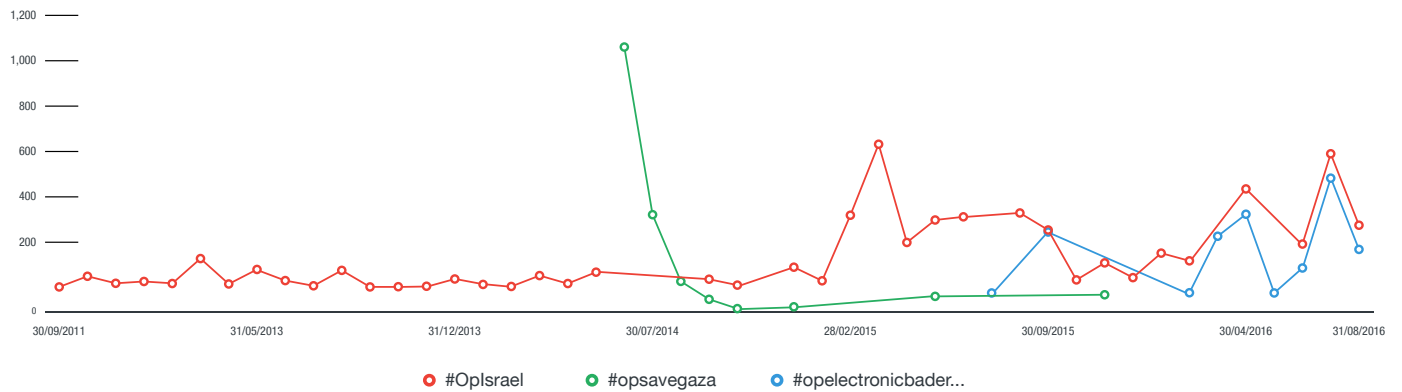


Figure 6. #OpIsrael, #opsavegaza and #opbader / #electronicbader / #baderoperation timelines

The struggle between Israel and Palestine is one of the longest modern-day conflicts, starting in 1948 and continuing to this day⁷. Israel's continued occupation of the West Bank and military operations in Gaza only serve as fuel to the anger of Palestinians and other groups sympathetic to Palestine.

Target TLDs of #OpIsrael Defacements

These defacements are not random. As much as possible, the hacking groups target Israeli websites, as co.il and org.il top-level domains (TLDs) rank second and sixth respectively in the distribution of defaced websites carrying anti-Israel messages.

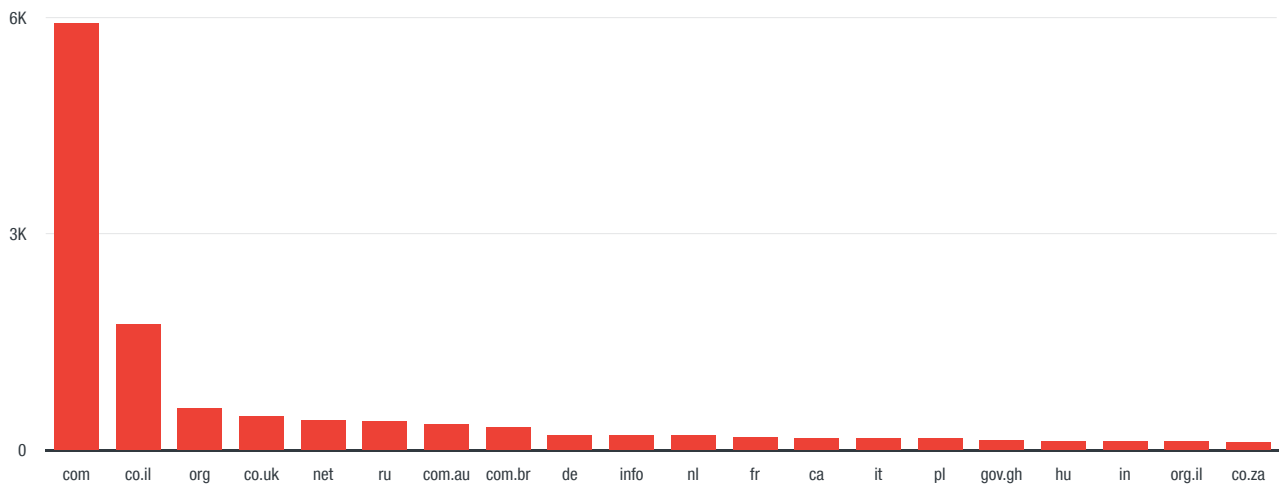


Figure 7. Target sites for #OpIsrael

#OpIsrael

The very first #OpIsrael web defacement was made by "imLulzPirate" on August 26, 2012. The website myisrael.us fell victim to the defacement, with the main page of the website altered to display a politically charged message against Israel and Zionism. The defacement embeds a YouTube video uploaded by Canadians for Justice and Peace in the Middle East, condemning the Gaza War in December 2007 – January 2008.



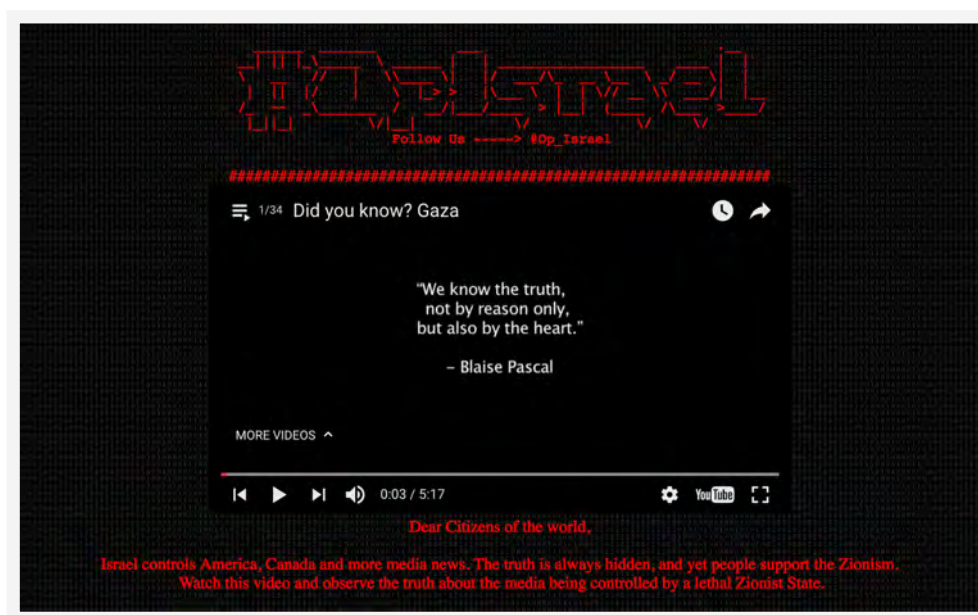


Figure 8. The first #OpIsrael defacement made by imLulzPirate

#OpIsrael did not gain any traction after the initial defacement made by imLulzPirate. It took several months for members of the Anonymous collective to support the cause and organize a campaign against Israeli websites.

The first organized large-scale defacement campaign happened on April 7, 2013, a date chosen because it coincides with Holocaust Remembrance Day. This attack has been repeated every year since then, with 326 defacers executing 11,000 plus defacements on more than 5,400 domains.

#OpIsrael Sub-campaigns

#OpIsrael Engaged is a sub-campaign that started in 2015 and continued up to 2016. Similar to the main #OpIsrael campaign, it peaked every April 7. The AnonGhost team, a tight-knit group that claims to have members from Mauritania, Morocco, Malaysia, Indonesia, Tunisia, USA, and Ireland, mostly did the 2015 campaign. Anonymous Arabe, a loose group of hackers from Arabic-speaking countries in the Middle East and North Africa, was responsible for the majority of the 2016 campaign.



Figure 9. Defaced pages by AnonGhost Team and Anonymous Arabe showing identical wording for the #OpIsrael Engaged campaign

It is worth noting that AnonGhost seems to have either branched out to other countries or has sub-groups, with AnonGhost being the umbrella group. So far we've seen AnonGhostDz, which is the Algerian sub-group, AnonGhost Indonesia, AnongGhost Gaza, AnonGhost Tunisia, AnonGhost Maldives, and AnonGhost Vietnamese.

#OpIsrael Decided is another sub-campaign that started around the same time as #OpIsrael Engaged, and uses a similar message. It is supported mostly by an AnonCoders team that is a loose association of hackers from Albania, Tunisia, Morocco, Lebanon, Bangladesh, Indonesia, and France, among others.



Figure 10. #OpIsrael Decided defacement pages shows similar wording to #OpIsrael Engaged

#OpBader / #ElectronicBader / #BaderOperation

This is a larger campaign with 2,759 defacement records, which is as many as the #OpIsrael Engaged and #OpIsrael Decided sub-campaigns combined. While #OpIsrael Engaged and #OpIsrael Decided had standard templates (and the participating hackers did not do much to alter these templates), #OpBader is loosely organized, with templates and messages that vary quite significantly.

The only common identifiable string we can find related to this campaign is the use of these hashtags:

#opisrael #alfallagaTeam #fallaga #fallagatteam #tunisianfallagatteam #opbader #electronicBader #baderoperation #hackers #fallagahackers

"Bader" is a reference to the Battle of Badr, a significant battle won by the Prophet Muhammad in the early years of Islam⁸. These historical references strongly indicate that these hacking groups view themselves as cyber-jihadists, viewing their actions as part of a digital jihad.

#OpSaveGaza

The #OpSaveGaza/#SaveGaza campaign is related to #OpIsrael since both target Israel and Israeli actions in Palestinian territories, but #OpSaveGaza/#SaveGaza is mostly influenced by events in the Gaza region specifically.

On July 2014, Israel launched Operation Protective Edge, which included airstrikes and a land invasion aimed at destroying tunnels from Gaza to Israel⁹. Not surprisingly, the first instance of #OpSaveGaza/#SaveGaza appeared in response to the land invasion. The defacements continued until October, and only when hostilities in the Gaza strip subsided significantly did the 2014 campaign die down. #OpSaveGaza had 3,415 defacements within that short period, making it one of the most active web defacement campaigns.



Figure 11. Sample defacement pages of the #OpSaveGaza campaign

#Save Gaza

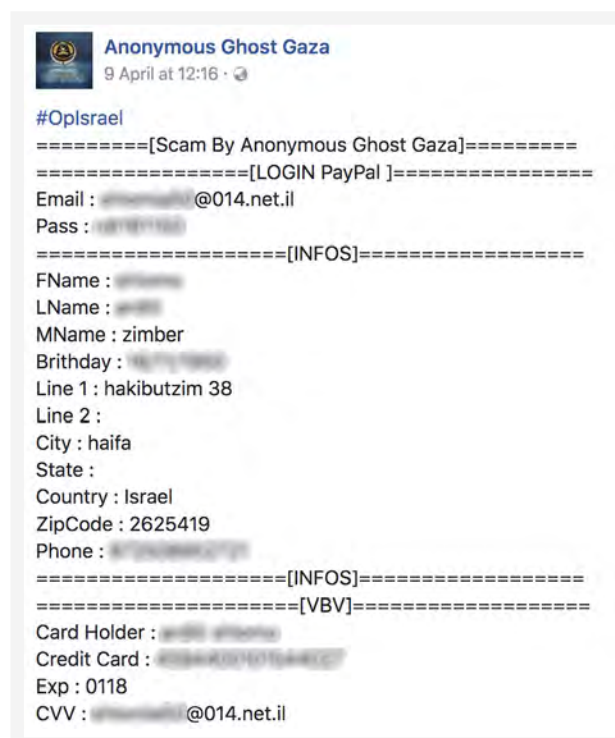
#Save Gaza started in July of 2016 as a sub-campaign under #opBader, primarily driven by Anonymous Ghost Gaza. Among the sub-campaigns discussed, it has been the most vocal and the most forceful.

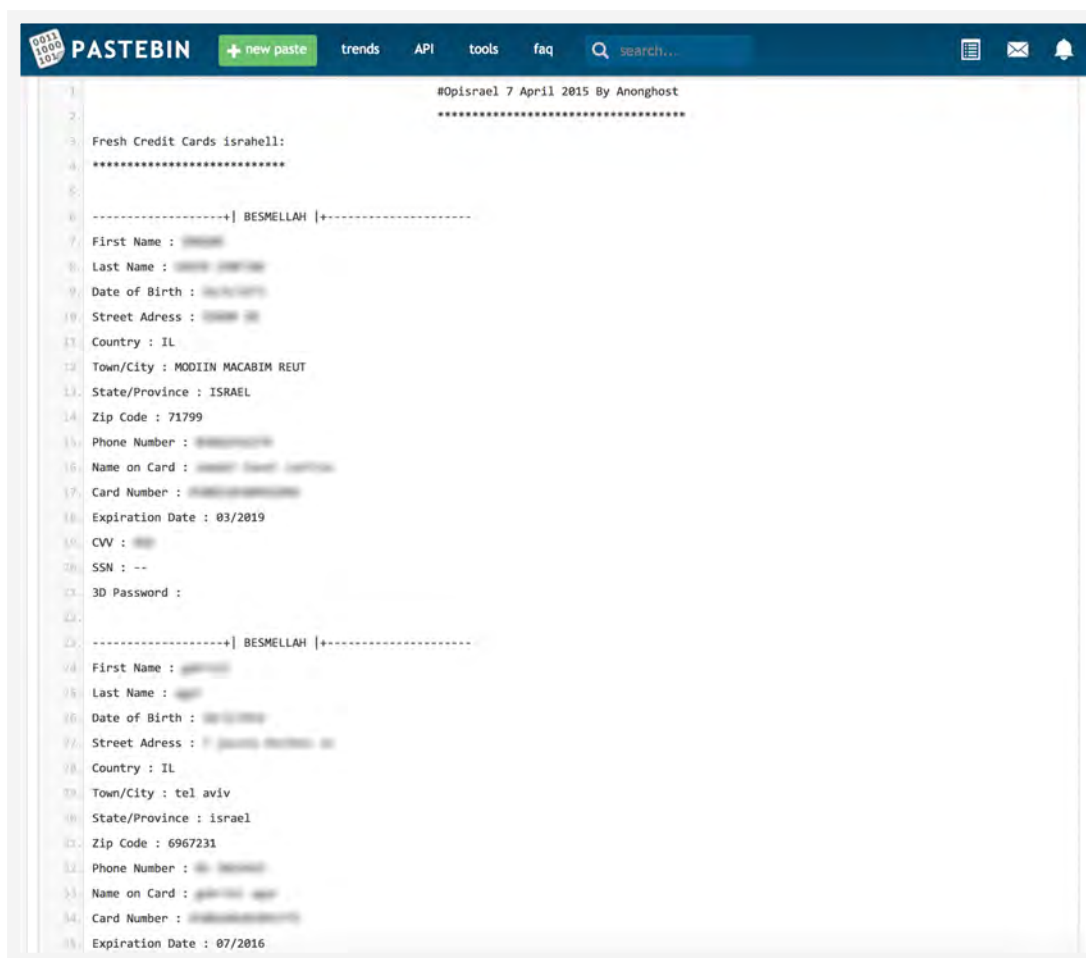
While #OpIsrael Decided and #OpIsrael Engaged use relatively tame language, #Save Gaza incites violence and puts direct pressure on Israelis, threatening to steal credit card information, bank credentials, and other website credentials.



Figure 12. Forceful language in the defacement campaign #Save Gaza

It is worth noting that Anonymous Ghost Gaza followed through on their threat to steal the personal information of Israeli citizens. Members of Anonymous Ghost Gaza posted Israeli citizens' credit card information and online account credentials on their Facebook page and Pastebin.





The image shows a screenshot of a Pastebin page. The header is dark blue with the 'PASTEBIN' logo, a 'new paste' button, and navigation links for 'trends', 'API', 'tools', and 'faq'. A search bar is on the right. The main content area is white with a line-numbered list of text. The text is a list of personal and financial details for two individuals, separated by a header line that reads '#Opisrael 7 April 2015 By Anonghost' followed by a line of asterisks. The first individual's details include: First Name, Last Name, Date of Birth, Street Address, Country (IL), Town/City (MODIIN MACABIM REUT), State/Province (ISRAEL), Zip Code (71799), Phone Number, Name on Card, Card Number, Expiration Date (03/2019), CW, SSN, and 3D Password. The second individual's details include: First Name, Last Name, Date of Birth, Street Address, Country (IL), Town/City (tel aviv), State/Province (israel), Zip Code (6967231), Phone Number, Name on Card, Card Number, and Expiration Date (07/2016).

```
1. #Opisrael 7 April 2015 By Anonghost
2. *****
3. Fresh Credit Cards israhell:
4. *****
5.
6. -----+| BESMELLAH |+-----
7. First Name :
8. Last Name :
9. Date of Birth :
10. Street Address :
11. Country : IL
12. Town/City : MODIIN MACABIM REUT
13. State/Province : ISRAEL
14. Zip Code : 71799
15. Phone Number :
16. Name on Card :
17. Card Number :
18. Expiration Date : 03/2019
19. CW :
20. SSN : --
21. 3D Password :
22.
23. -----+| BESMELLAH |+-----
24. First Name :
25. Last Name :
26. Date of Birth :
27. Street Address :
28. Country : IL
29. Town/City : tel aviv
30. State/Province : israel
31. Zip Code : 6967231
32. Phone Number :
33. Name on Card :
34. Card Number :
35. Expiration Date : 07/2016
```

Figure 13. Hacking groups publicly expose Israeli citizens' information and financial details

Groups behind the Campaigns

Hackers and hacking groups participating in #OpIsrael campaigns are mostly from Arabic-speaking countries in the Middle East and North Africa, with other groups from Bangladesh, Malaysia, and Indonesia also participating. Note that these are countries that do not recognize the validity of Israel as a state.

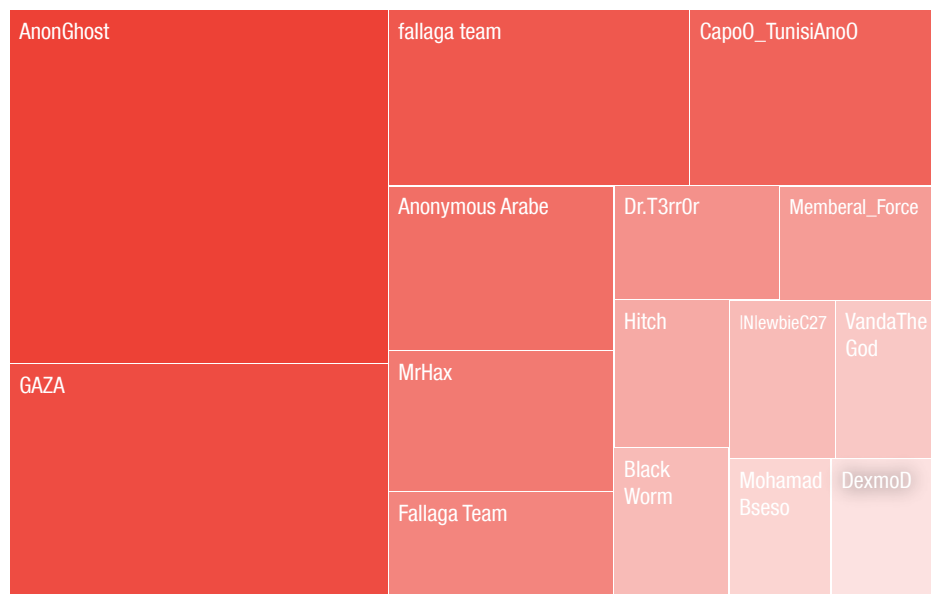


Figure 14. Top 15 participating hacking groups and hackers

The common use of the name "fallaga" by hackers and hacking groups in North Africa is a reference to "felaghas" or "fellagha", armed groups that were instrumental in driving out the French from Algeria in the Algerian War that lasted from the 1950s to early 1960s.

Charlie Hebdo Aftermath Results in #OpFrance

On January 7, 2015, two men attacked Charlie Hebdo, a French magazine that caused controversy several times in the past through its satirical cartoons about Islam and the prophet Muhammad. The attack left 12 people dead and 11 injured¹⁰. In the aftermath, France was a target of other attacks, this time in cyberspace. The smaller campaigns under #OpFrance include #OpCharlie, #OPCHARLIEHEBDO, and #AntiCharlieHebdo.

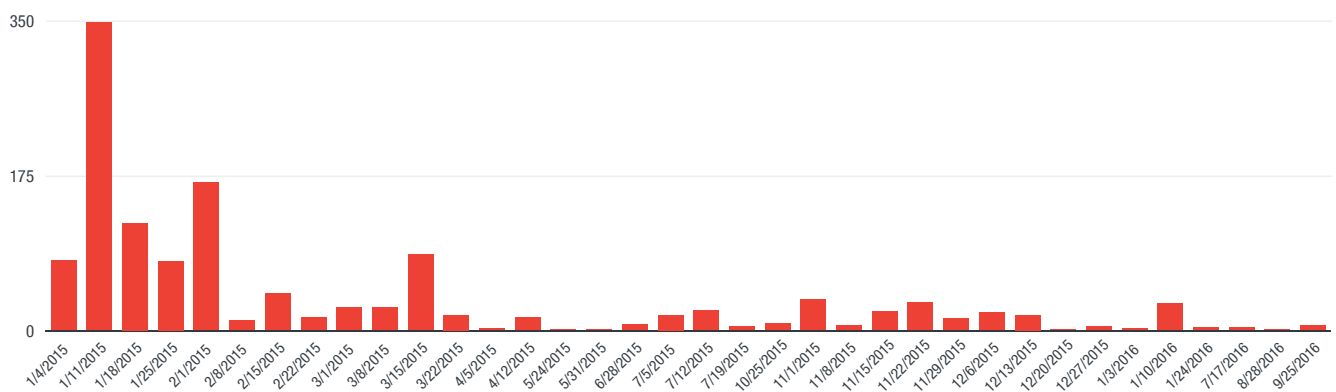


Figure 15. Timeline of #OpFrance—activity peaked January to March 2015, right after the Charlie Hebdo attacks

Target TLDs of #OpFrance Defacements

Similar to the attacks against Israel, #OpFrance hackers were trying to target French websites, as evidenced by .fr domains having the second-most domains that had sites defaced.

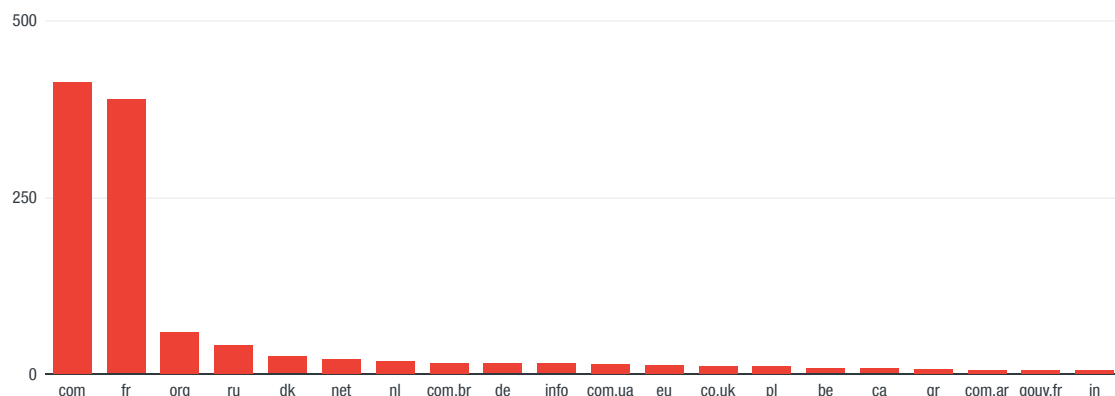


Figure 16. Target sites for #OpFrance

This campaign focused on French websites, with defacers targeting sites of companies like the French supermarket Carrefour, or sites with .fr TLDs. From our data, 36% of #OpFrance defacements have .fr TLDs.

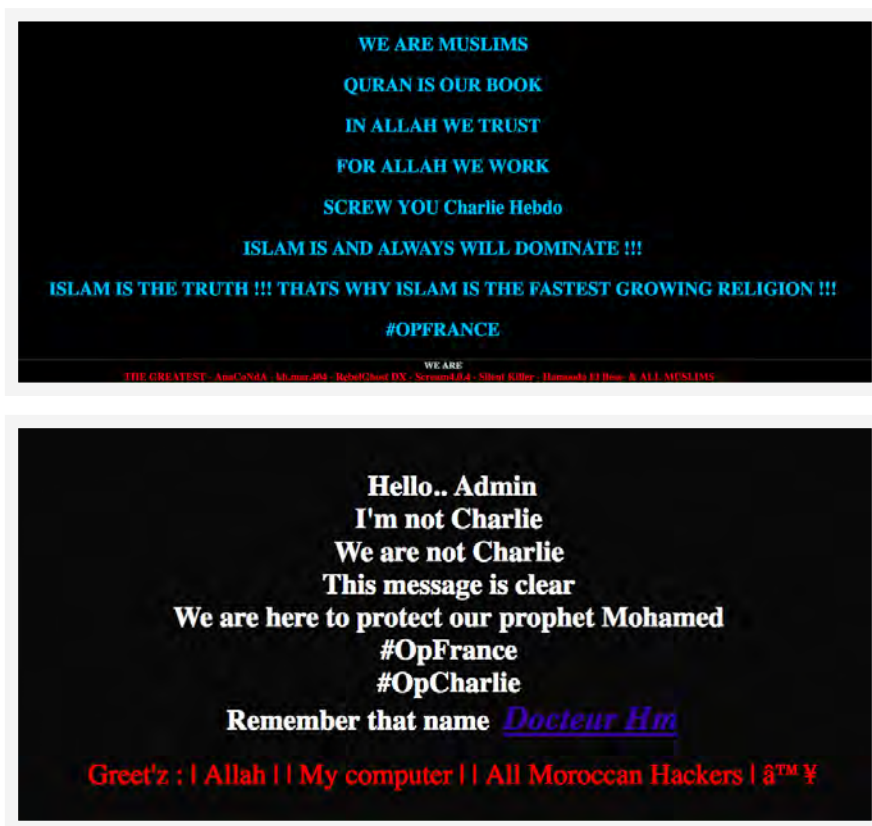


Figure 17. Defacement pages for the #OpFrance campaign

Hacking groups from Muslim-majority countries such as Tunisia, Syria, Mauritania, Morocco, Bangladesh and Indonesia began targeting French websites in an #OpFrance web defacement campaign that appear to be in support of the attacks. Some of the defacements even paraphrased Saudi-Australian Islamic preacher Junaid Thorne's statement on the matter, "If you want to enjoy 'freedom of speech' with no limits, expect others to exercise 'freedom of action.'"

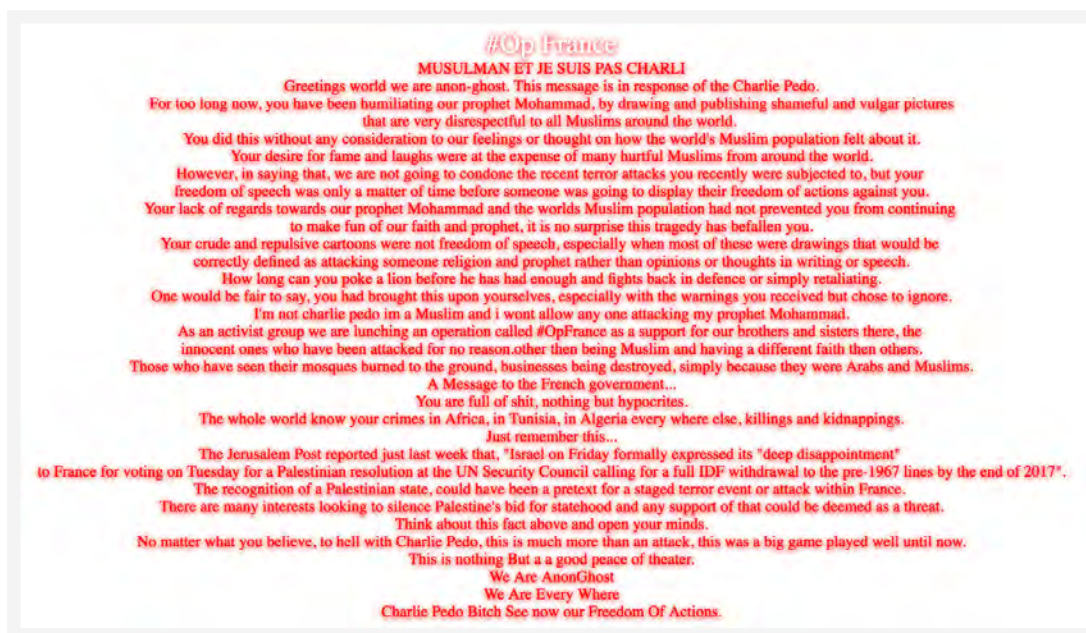


Figure 18. Defaced page promoting Islamic preachers' statement on Charlie Hebdo

Even though several groups were part of #OpFrance, the Middle East Cyber Army was particularly active and did the majority of the defacements. This group includes members that belong to other hacking groups such as Anonymous Arabe and some hackers from North Africa.

It is worth noting that one suspected member of the Middle East Cyber Army was arrested several months after the January – March #OpFrance campaign. The Bulgarian police arrested a 21-year-old Syrian student residing in Bulgaria, believed to be the leader of the group¹¹. Based on the defacement pages of Middle East Cyber Army, the hacker with the alias "The Greatest" was arrested. The group modified their defacement pages to include #OPSaveTheGreatest after the arrest.

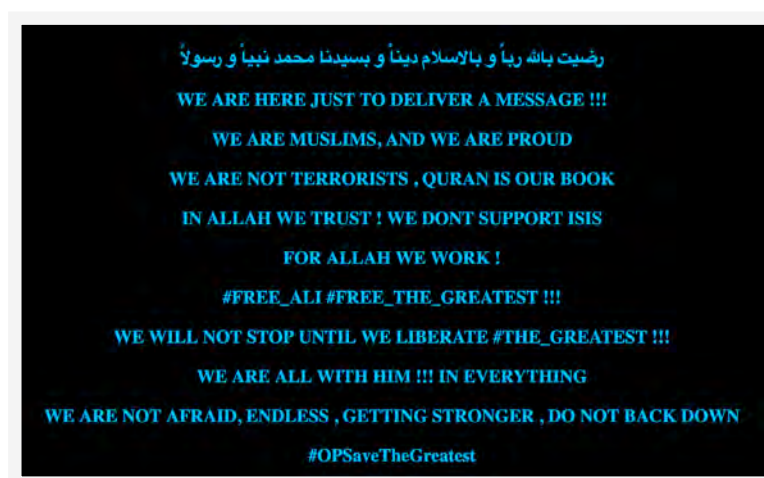


Figure 19. Defaced page modified to support "The Greatest", who was supposedly arrested in Bulgaria

Groups Behind the Campaigns

The visualization below shows the Middle East Cyber Army to be the most active group behind #OpFrance. AnonGhost, which was active in the anti-Israel defacements, also widely participated, as well as hackers from Mauritius (Mauritania Coder), and some from Bangladesh and Indonesia.

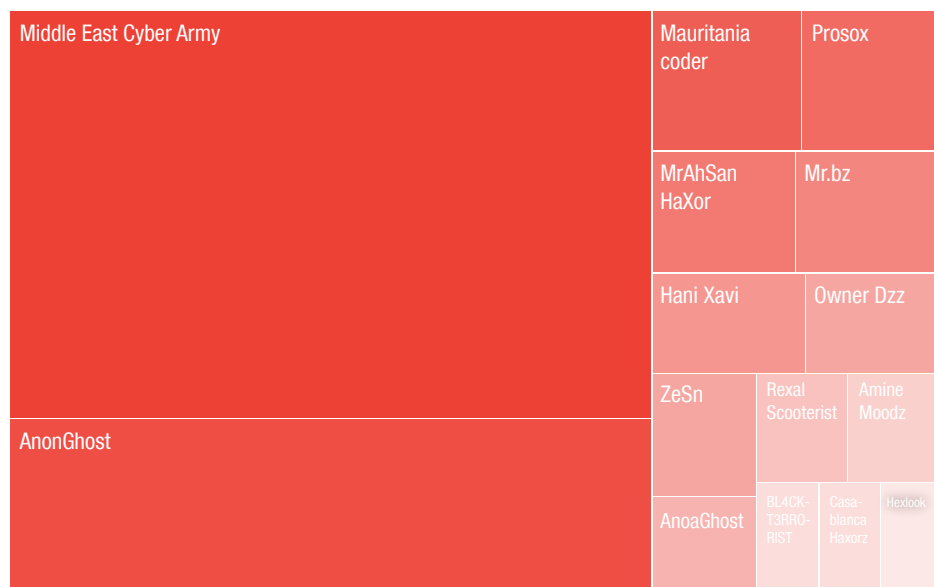


Figure 20. Top 15 participating hacking groups and hackers

Indian Border Disputes Trigger Campaigns

Like Israel, India has unresolved territorial disputes with its neighbors and sees frequent clashes along its borders. The unresolved dispute with Pakistan regarding Kashmir and Jammu, as well as the challenges of patrolling and enforcing the border between India and Bangladesh (the fifth longest land border in the world), makes for a volatile situation. It's further exacerbated by constant defacements between Pakistani and Indian hacking groups, and between Bangladeshi and Indian hacking groups.

Target TLD's of #OpIndia

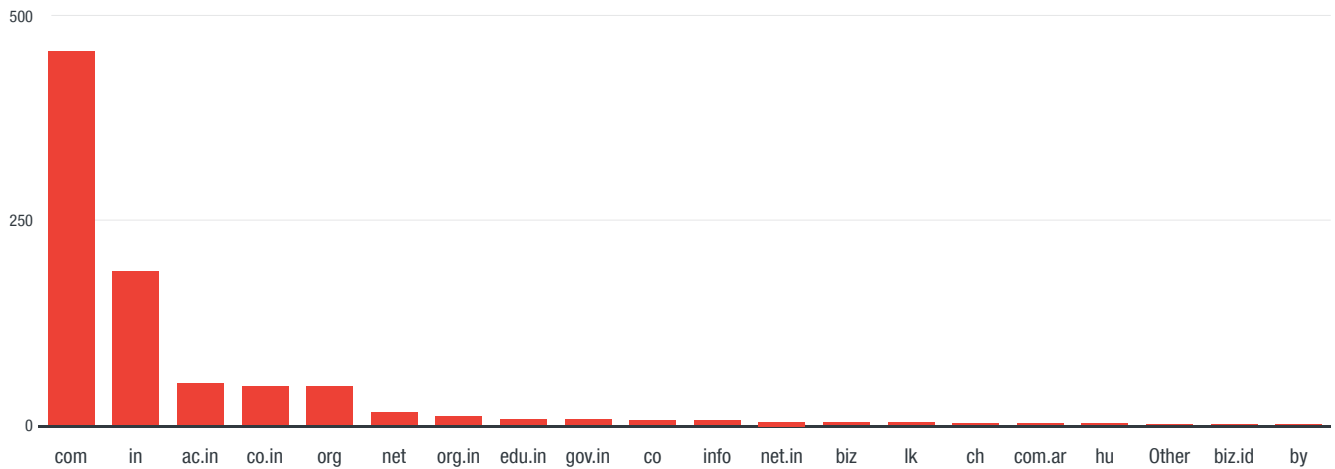


Figure 21. Target sites of #OpIndia

The hackers targeted Indian websites, as evidenced by the TLD's .in, ac.in, co.in, org.in, edu.in and gov. being in the top nine domains with websites defaced.

Cricket leads to #riseofthetigers

Even cricket teams became a trigger for defacement campaigns, illustrating the degree of tension between India and its two neighbors.

The campaign #OpIndia started on March 2015, executed by Bangladeshi hackers, after Indian politician Shashi Tharoor tweeted that he preferred to face the Bangladesh cricket team (called The Tigers) in the Cricket World Cup quarterfinals. Tharoor reportedly felt Bangladesh was a weaker team that would give India an easier path to the finals.



Figure 22. Defacement page for #OpIndia with an image of the Bangladesh cricket team featured



Figure 23. The Tharoor tweet that started the controversy

Free Kashmir

Led by Pakistani hacking groups ZCompany Hacking Crew (ZHC) and Muslim Liberation Army, Free Kashmir is a long-standing campaign that started in 2011. The attacks began with the calling out of the illegal occupation and human rights abuses the Indian Armed Forces committed against Kashmiris¹². Free Kashmir has the most number of defacements out of all the campaigns studied, despite having only around half the number of attackers that #OpIsrael had.

Pakistan is India's rival claimant to the disputed territory of Kashmir, and the defacement pages of both ZHC and Muslim Liberation Army commonly quote India's Penal Code Act No. 45 of 1860, which does not include the State of Jammu and Kashmir as part of India. However, the ruler of Jammu and Kashmir, Maharaja Hari Singh, acceded both territories to India in 1947¹³.



Figure 24. Free Kashmir campaign defacements

The messages of ZHC and the Muslim Liberation Army have a Pakistani slant and do not necessarily reflect the sentiments of the Kashmiri people. However, they may gain traction with younger Kashmiris as ZHC and Muslim Liberation Army also highlight the human rights abuses and disappearances of Kashmiri activists and militants¹⁴, an issue that has not received international attention.

Nationalism Inspires Retaliatory Hacking

It is also quite common for hacking groups in India, Pakistan, and Bangladesh to start defacement campaigns against their rival country's websites. The presence of active hacking groups in neighboring, conflicting countries makes for a volatile situation, and these "turf wars" or "nationalistic defacements" can easily be triggered, and in a lot of cases, get out of hand.

One such incident happened in 2015 when a Pakistani hacker named Faisal 1337 hacked into multiple Indian websites. The government website of the state of Kerala was the most prominent website defaced.



Figure 25. Indian local government websites hacked

Immediately, hacking groups from India launched #op_pak_cyber_space, defacing hundreds of Pakistani websites in retaliation.

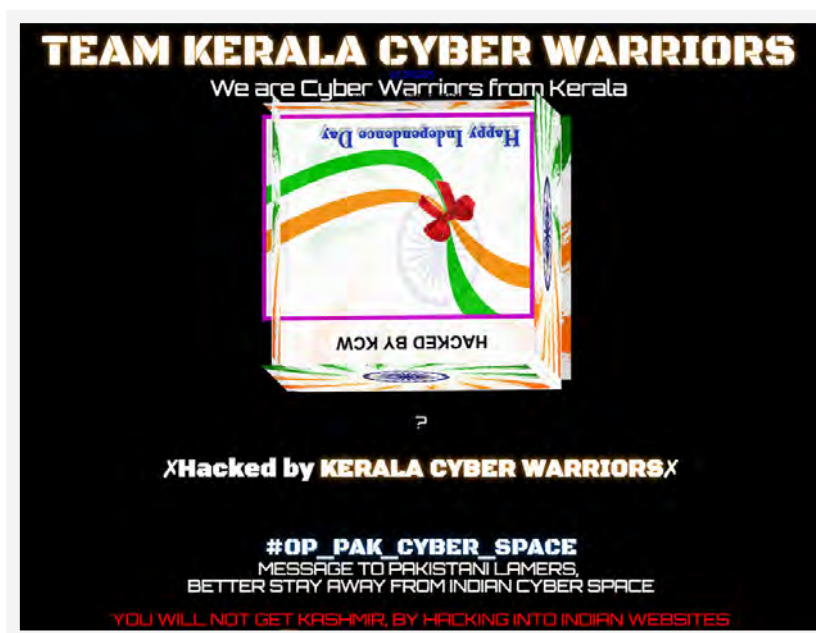


Figure 26. Retaliatory attack from Indian hackers

The defacement of Mumbai Airport Customs website by Pakistani defacer Alone Injector is another example. After the incident, Indian hackers retaliated with a campaign defacing the websites for Islamabad, Peshawar, Multan and Karachi airports in Pakistan.



Figure 27. Mumbai Airport Customs defacement



Figure 28. The defacement page seen on Islamabad, Peshawar, Multan and Karachi airport websites

Fallout of the Attacks between India and its Neighbors

Aside from ongoing campaigns by Indian, Pakistani and Bangladeshi hackers (against or in response to each other's hacking), the real-world conflict between the three countries has significantly increased in the past two years.

One event happened on January 2, 2016, when several terrorists attacked India's Pathankot Air Force base, killing several Indian military men and one civilian. The attack was later claimed and attributed to Jaish-e-Mohammed, a separatist group in Kashmir¹⁵. After the attack, Indian hacking groups retaliated by targeting Pakistani websites.



Figure 29. Retaliatory defacements made by Team Indian Black Hats aka Indian Cyber Devils

On September 18, 2016, attackers from Jaish-e-Mohammed, the same terror group responsible for the Pathankot Air Base attack a few months prior, launched another attack on an Indian army headquarters in Uri that left 17 army members dead, as well as all four attackers¹⁶. A few days later, the Indian government launched surgical strikes targeting locations in Kashmir.

These series of incidents sparked back and forth campaigns between Indian and Pakistani hacking groups, with defacements containing politically charged messages, freedom slogans, or just plain hate speech.





Figure 30. Defacements generated by conflict with India

Another event that triggered a sizeable defacement campaign was the drafting of Nepal's new constitution in September 2015. Some in India believed that the constitution marginalized certain ethnic groups; an issue that was highlighted when the Indian Express reported that India requested Nepal to make seven amendments to its constitution¹⁷. The report triggered an outrage in Nepal, as the message was seen as a foreign country meddling in the internal affairs of an independent sovereignty.

The outrage triggered the #BackOffIndia campaign during October 2015, supported by DQN hacker and craXerbikash from Nepal, BloodSecurity from the Philippines, and several Pakistani hackers.



Figure 31. A campaign triggered by India's involvement with Nepalese matters

Groups behind the Attacks

The most prominent anti-India defacements came from RiseOfTheTigers, a collective that was created just for the #OpIndia campaign in March 2015. Several Bangladeshi hacking groups joined RiseOfTheTigers: Bangladesh Grey Hat Hackers, Bangladesh Cyber Army, Team_CC, Bangladesh Script Kiddie Hackers, Blacksmith Hackers Team, 3xp1re Cyber Army, Bangladesh Black Hat Hackers, and others.

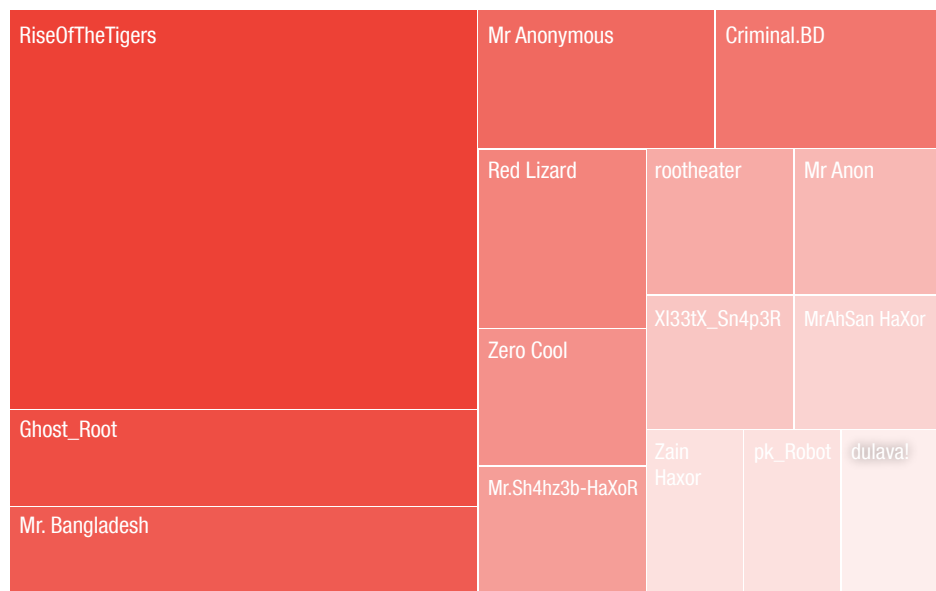


Figure 32. Top 15 participating hacking groups and hackers

Military Actions prompt a #SaveSyria Campaign

On April 22, 2016, the Syrian government launched airstrikes targeting residential areas in Aleppo during Friday scheduled prayers. The attacks happened despite a ceasefire agreement by both sides in February 2016. There were several more airstrikes, the worst of which hit the al-Quds hospital, killing 50 people¹⁸. The incident inspired a #SaveSyria campaign that exposed graphic images of wounded civilians in Aleppo.

Target TLDs of #SaveSyria

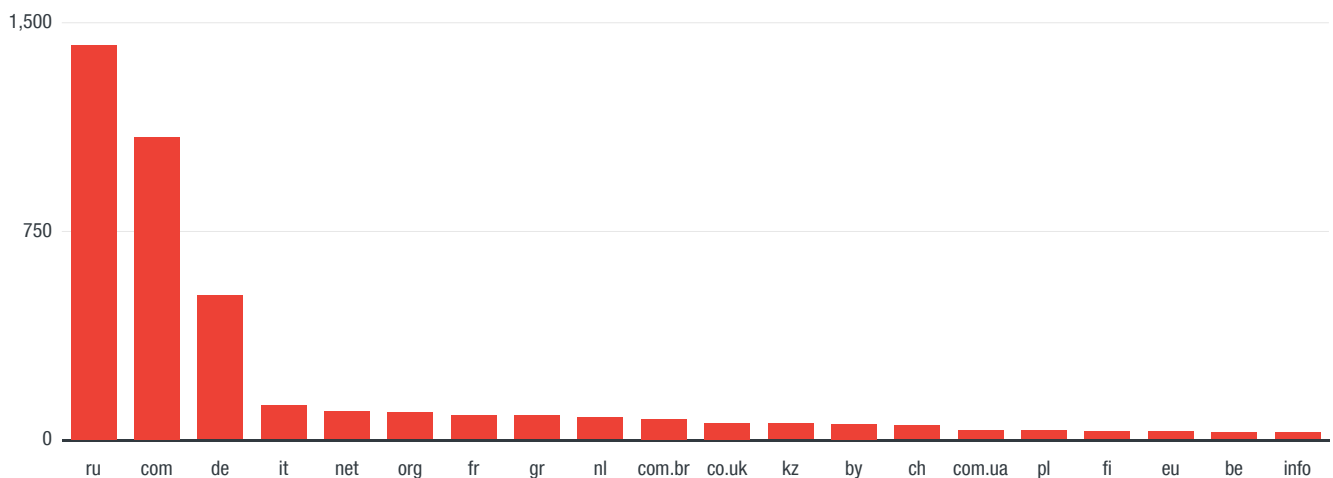


Figure 33. Targeted domains of #SaveSyria

Most of the #SaveSyria defacements targeted Russian websites because many suspected that Russia was behind the April 2016 airstrikes. Russia is seen as supportive of Syrian president Bashar al-Assad, and the country has reinforced Assad's regime through air superiority assets.

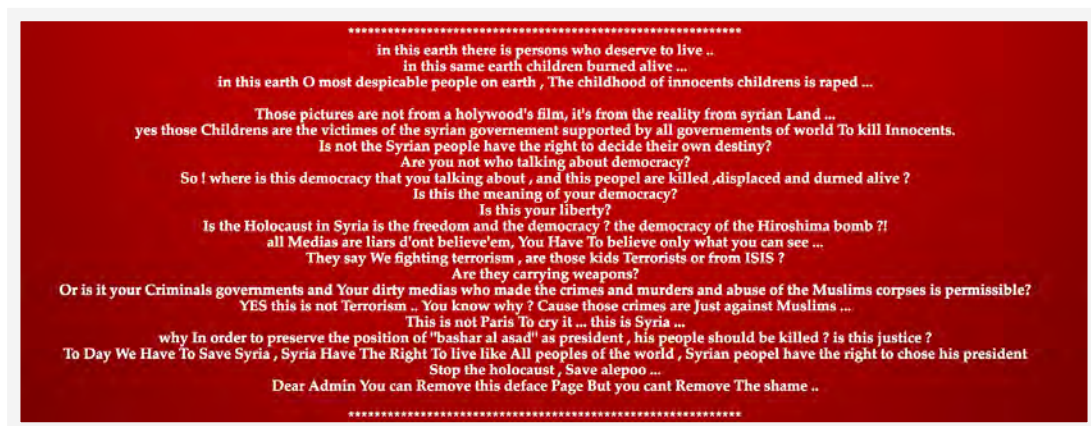
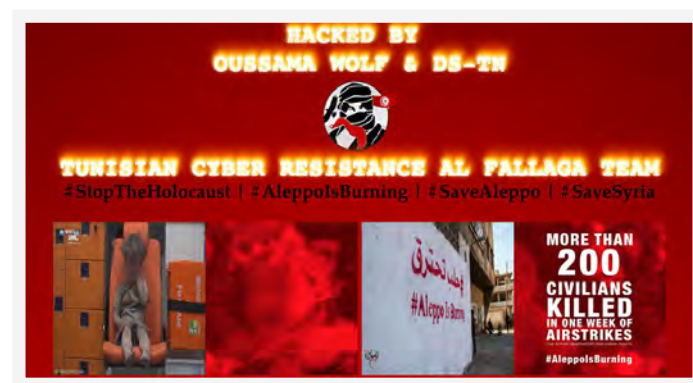


Figure 34. Defaced sites showing graphic images of Aleppo

The Fallaga Team formed a loose collective called the Tunisian Cyber Resistance Al Fallaga Team, composed of Tunisian hackers and actively supported by hackers from Anonymous Arabe, Algeria, and Indonesia. They launched a defacement campaign with the hashtags #StopTheHolocaust, #AleppolsBurning, #SaveAleppo and #SaveSyria.

Campaigns Provoked by Kosovo Disputes

Kosovo is a disputed territory and partially recognized state that declared its independence from Serbia in 2008. The majority of its population is of Albanian descent, and the country enjoys friendly relations with Albania stemming from common history and traditions. In Northern Kosovo, near Serbia, there are communities of Serbian descent that refuse to acknowledge Kosovo's independence. This tension reached a boiling point in 2011 when Kosovo Police clashed with ethnic Serbian rioters who refused to remove roadblocks going into enclaves of Serbian control¹⁹.

Albanian hacking groups KSG-CREW, kwgdeface and AlbanianHackers launched the #AntiSerbs campaign a few months after the initial clashes. The campaign died down before the Brussels Agreement, which involved the integration of Northern Kosovo into Kosovo and had Kosovo Serbs manning the police and judiciary, was concluded.

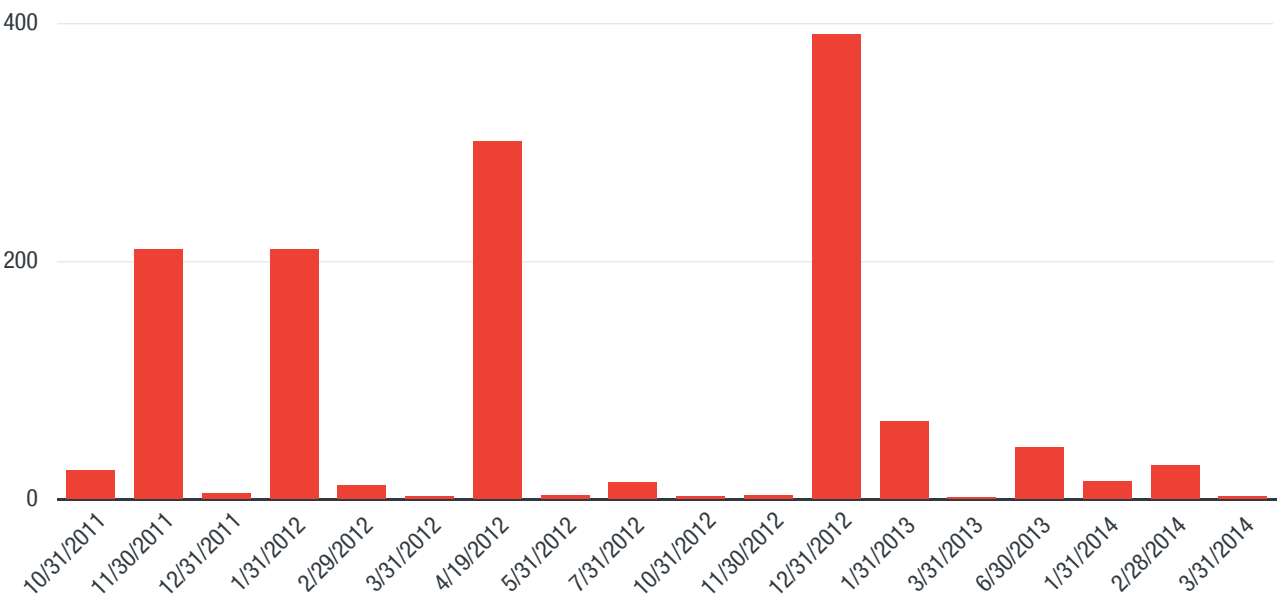


Figure 35. Timeline of anti-Serbs campaign

The defacement pages showed support for Kosovo independence, and also mentioned contested towns commonly involved in civil unrest. They listed Serbian-controlled territories bordering Kosovo with an Albanian majority and declared their desire to separate from Serbia and join Kosovo.

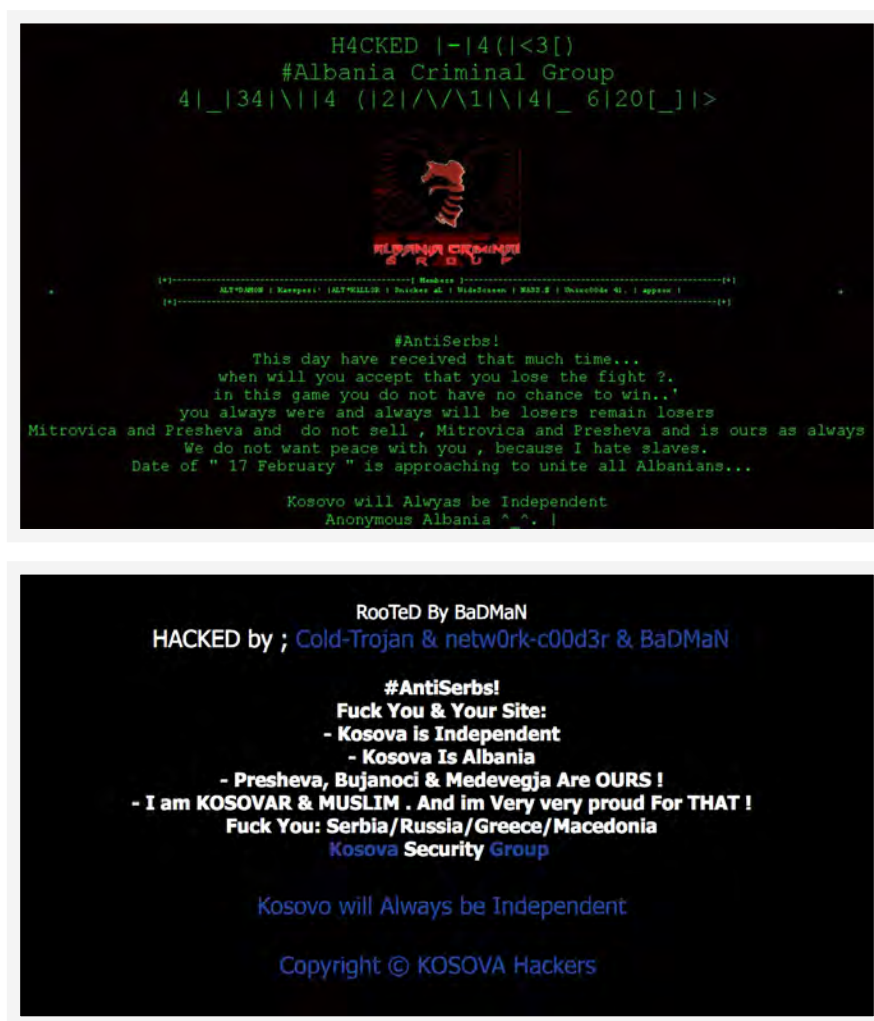


Figure 36. Web defacement pages supporting Kosovo

Disputes in the South China Sea

OpPhilippines and OpTaiwan

On May 9, 2013, a maritime incident involving the Taiwanese fishing boat Guang Da Xing No. 28 and the Philippine Coast Guard resulted in the death of Taiwanese fisherman Hung Shih-cheng (洪石成)²⁰. This incident led to many consequences, including sanctions and a military drill from Taiwan government, protests in Taiwan, and several cyberattacks.

On May 10, 2013, people in Taiwan called for DDoS attacks against .gov.ph to force the Philippine government into issuing an official apology. Many hackers responded, attacking more than 30 .gov.ph sites²¹.



Figure 37. Forum post mobilizing visitors to launch DDoS attack

On May 11, Filipino hacker "Pinoy Vendetta"²² sent a warning message to Taiwanese hackers by defacing one Taiwan government site and several commercial sites. In response, AnonTaiwan launched #OpPhilippines the next day.



Figure 38. Web defacement page from "PinoyVendetta"

After the attack, AnonTaiwan posted leaked data from .gov.ph sites on Pastebin. One noteworthy victim was dns.gov.ph, which is the .gov.ph domain registry website. More than 2,300 accounts, which were possible admin accounts for .gov.ph domains, were leaked. These government sites faced a huge risk. Potentially, attackers could change the name servers of domain names, government domain names would have resolved to invalid IP addresses, and important sites would have been inaccessible to the public.

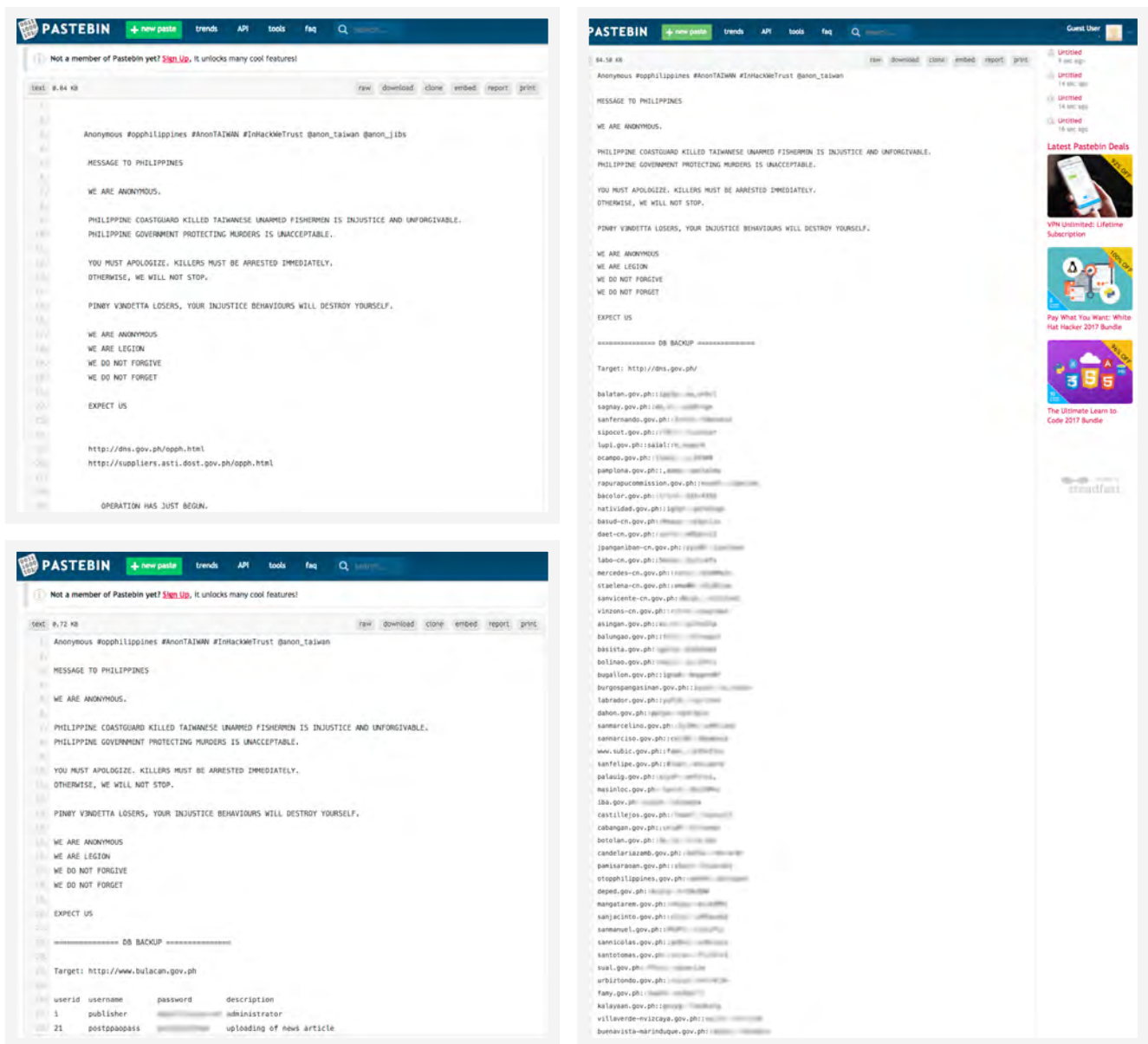


Figure 39. Information leaked on Pastebin

On May 25, 2013, Filipino hackers attacked 31 .tw sites in a campaign titled #OpTaiwan as a response to #OpPhilippines. The defaced pages displayed the messages, "Stop attacking our cyberspace" and "Let our government handle this problem."

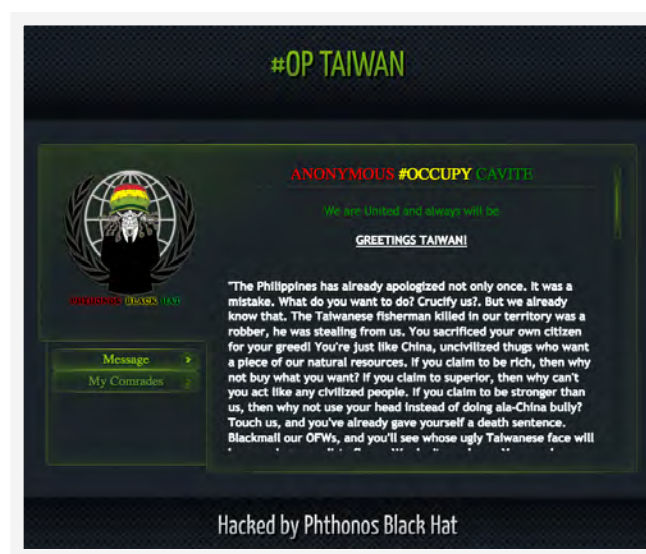


Figure 40. Web defacement pages for #OpTaiwan

Defacements over Territory

Six countries—China, Taiwan, Philippines, Vietnam, Malaysia, and Brunei—are contesting several islands and features, rock outcrops, sandbars, and reefs in the South China Sea.

Over the last few years, the tension between China and Vietnam, and China and Philippines has increased. China has taken aggressive action, from coast guard patrols to building facilities and installations in various contested areas. This has sparked defacement activities by several groups from Philippines, Vietnam, and China against their rival countries' websites.

Attacker	Team
越南国宰相	1937cn
oaddah	1937cn
ZeSn	Anonymous Philippines
YoCo Smart	Silic Group
Nama Defacer	Anonymous Philippines
AnonReaper	Anonymous Philippines
BloodSecurity	BloodSecurity
HukbalaHack	Anonymous Philippines
Anonymous Philippines	Anonymous Philippines
AlfabetoVirtual	1937cn

Figure 41. Top defacers participating in South China Sea defacements, and the groups they belong to

Early Attacks in 2011

Chinese marine surveillance vessels cut the cables of Vietnamese oil survey vessels in the South China Sea²³. This incident triggered defacement attacks that started on June 3, 2011. A Vietnamese defacer 'Mr.N - Cubi11' attacked Chinese government websites. The page displayed Vietnamese patriotic slogans like "Vietnamese People is Willing to Sacrifice to Protect the Sea, Sky, and Nation." More Vietnamese defacers joined this campaign after²⁴.



Figure 42. Vietnamese defacer page

From June 4, 2011, Chinese defacers started to retaliate by attacking .vn websites. Hongke Union (HUC), a well-known Chinese hacktivist group, mobilized its members and launched a series of attacks. Over 30 .gov.vn sites were defaced.

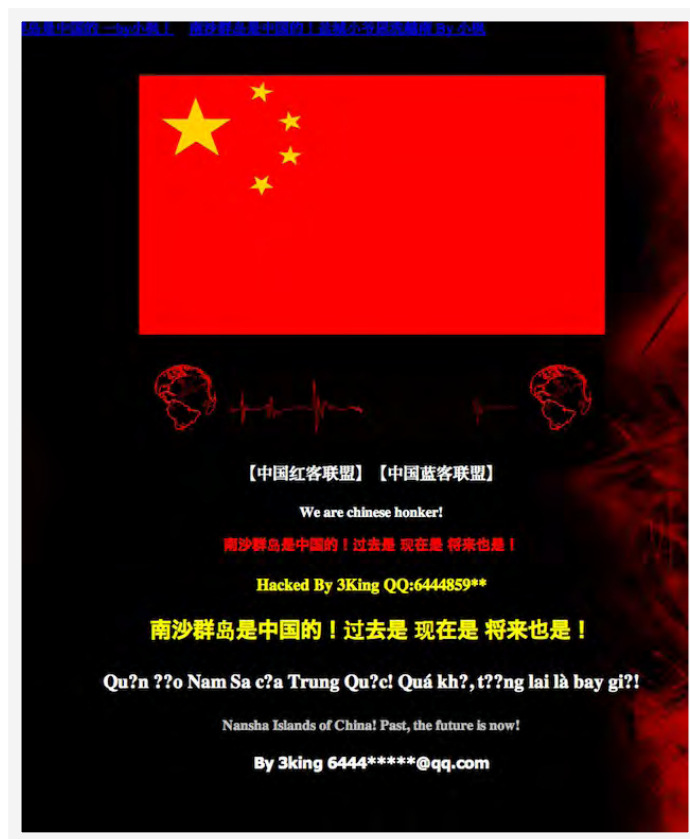


Figure 43. Chinese defacers retaliate

After completing the attacks, the HUC sent out a summary reporting that their attacks were from June 4 to June 5, two function groups were created (one for DDoS, one for defacement), and several QQ chat groups and YY chat channels were created to coordinate attacks²⁵.

Some non-HUC hackers also joined the attack, compromising over 1,000 sites. Most of the victims suffered DDoS attacks and defacement. One popular Vietnamese search engine site was inaccessible for five hours. During the attacks, HUC found Vietnamese defacers attacking .cn sites.

Chinese hacker group Silic also joined the retaliation. In their deface pages, Silic claimed that "(Vietnamese defacers) first stir up trouble, we just attack back." This group attacked 98 .vn websites on June 8. Most victims were .gov.vn sites²⁶.



Figure 44. Silic Group defacement page

OpChinaDown, 2012

On April 10, 2012, a standoff between the Philippine Navy and Chinese maritime surveillance ships over the disputed Scarborough Shoal (Huangyan in Chinese) in the South China Sea caused tension between the two countries. In response, Chinese defacers compromised the website of the University of the Philippines on April 20, 2012, leaving a message that claimed, “We come from China! Huangyan Island is Ours”.



Figure 45. Defaced page of University of the Philippines

The defacer group "Anonymous #OccupyPhilippines" responded on the same day, compromising several .cn sites. The statement "Scarborough Shoal is ours!" was prominent on the deface page²⁷.

Three days later, on April 23, the government of the Philippines claimed that two of its sites suffered DDoS attacks coming from Chinese IP addresses—an apparent retaliatory attack from China. Defacements escalated quickly, triggered by the DDoS attacks²⁸.

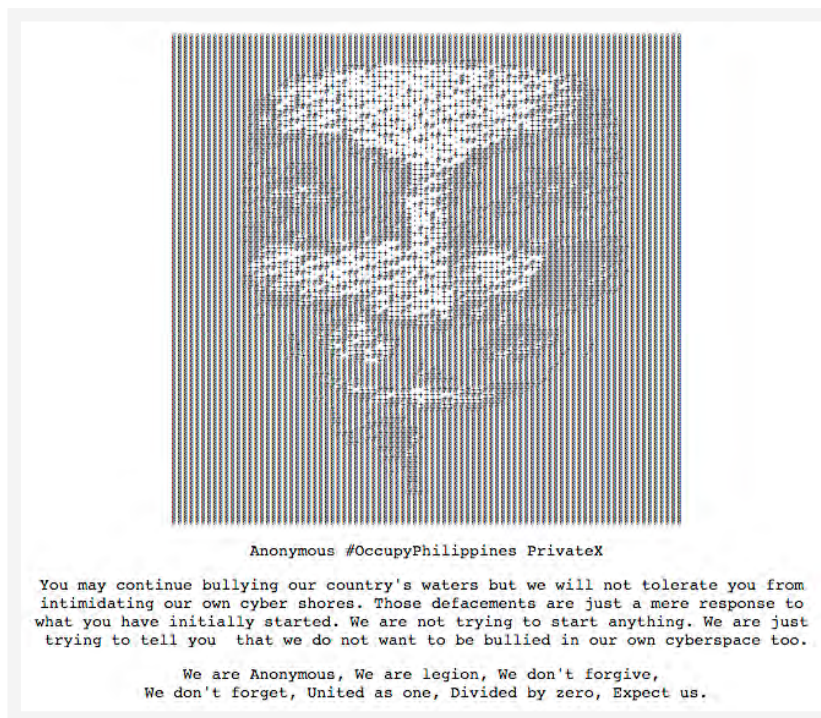


Figure 46. Page from #OccupyPhilippines

On the same day, OccupyPhilippines and PrivateX launched a joint attack operation "#OpChinaDown". They attacked .gov.cn sites and posted DB schema and login credentials of victim sites on Pastebin.

On April 25, the Silic group (the same organization that attacked .vn sites in 2011) joined the web defacement campaign and targeted .gov.ph sites. Besides derogatory statements against Philippine defacers, the page allowed visitors to leave messages on it. Over the course of 3 hours, over 30 visitors left messages on the defaced pages²⁹.



Figure 47. Silic defacement page, where you can leave messages

Chinese hacktivism group 1937cn joined the defacement war on June 1, 2012. This group created a very long deface page to convince viewers to believe in their message. 1937cn spread that page across 173 sites in five days.

StopReclamation and OpChina, 2015

China started reclamation and building on the Spratly archipelago of the South China Sea in April 2015³⁰. This action caused a wave of defacement attacks. BloodSec, a Philippine defacer group, launched a #StopReclamation campaign on April 26, 2015.



Figure 48. BloodSec defacement page

Tensions escalated a month later. Posting on Pastebin³¹, defacers from the Philippines and Vietnam declared the beginning of an #OpChina campaign on May 28, 2015. In the announcement, they called themselves "the united hackers from the Philippines and Vietnam," aiming to "protest your (China) unjust actions over the South China Sea". At the end of the announcement, they left a note that read "Expect us! 5/30/2015".



Figure 49. Joint message from Vietnamese and Filipino hackers, and their defacement pages

This is the first time defacers from the two South East Asian countries united for a common political cause.

A series of attacks hit .cn sites on the date stated in their warning message—August 30, 2015. Most of the victims were .gov.cn sites. The message left by the group Anonymous Philippines asked the Chinese

government to "stop the reclamation, do not put or establish any structure in that location." At the same time, "AnonGhost" from Vietnam put out the message, "Stop the infringements of sovereignty island."



Figure 50. Retaliation from Chinese hackers

On the same day, Chinese defacer team "1937cn" retaliated by defacing .vn sites, and blamed it on the joint action of defacers from Philippines and Vietnam. 1937cn also claimed that "South China Sea is China's inherent territory." 1937cn's response was very quick—they likely noted the joint announcement of the defacers from the Philippines and Vietnam, and carefully prepared the retaliation.

Attacks on Vietnamese Airports, 2016

On July 12, 2016, the Hague Permanent Court of Arbitration ruled in favor of the Philippines against China in an arbitration case about the disputes in the South China Sea. The ruling triggered a series of cyberattacks against Vietnam³².

On July 29, 2016, the Chinese hacker group 1937cn attacked two major airports in Vietnam and the website of Vietnam Airlines³³. They defaced the home page with the same page used in 2015 during the #OpChina defacement campaign. Then the hacker group leaked client information of Vietnam Airlines³⁴. This was not the first time 1937cn attacked Vietnam Airlines; the group also launched a similar attack on May 30, 2015.

I	ID NUMBER	FIRST NAME	MIDDLE NAME	LAST NAME	DOB	GENDER	CREATE DATE	EMBOSSED STATUS	CY PREFERENCE	NAMING	CTITLE	SALUTATION	CAGE
410019	9.3E+09					F	2014/11/2	đinh thi	ACTIVE	VN	SF	MS	Dear MS
410020	9.5E+07					M	2010/08/1	NGUYEN QU	ACTIVE	VN	SF	ONG	THUA ONG
410021	9.6E+07					M	2010/08/1	CHUI LU	ACTIVE	EN	FS	MR	DEAR MR
410022	9.7E+09					M	2015/03/1	JAECKLE E	ACTIVE	VN	SF	MR	Dear MR
410023	9.4E+09					F	2015/09/1	IVAN DUON	ACTIVE	VN	SF	MRS	Dear MRS
410024	9.6E+09					F	2015/09/1	NGUYEN VI	ACTIVE	VN	SF	MRS	Dear MRS
410025	9.4E+07					M	2013/05/1	MINH DUC	ACTIVE	EN	FS	MR	DEAR MR N
410026	9.4E+07					M	2012/07/1	CHIKAYUKI	ACTIVE	JP	FS	MR	DEAR MR N
410027	9E+07					F	2011/08/1	NGUYEN TH	ACTIVE	VN	SF	BA	THUA BA N
410028	9.2E+09					M	2013/10/1	CU HUY BI	ACTIVE	VN	SF	MR	Dear MR
410029	9.7E+07					M	2010/11/1	SHUY NGUY	ACTIVE	EN	FS	MR	DEAR MR N
410030	9.8E+09					F	2014/07/1	STRAN THI	ACTIVE	VN	SF	MRS	Dear MRS
410031	9E+07					M	2013/07/1	NGUYEN DA	ACTIVE	VN	SF	MR	Dear MR
410032	9.8E+09					M	2015/07/1	YU QUOC	ACTIVE	VN	SF	MR	Dear MR
410033	9.2E+09					F	2015/05/1	DANG THI	ACTIVE	VN	SF	MS	Dear MS
410034	9.3E+07					M	2010/06/1	LUONG HU	ACTIVE	VN	SF	ONG	THUA ONG
410035	9.1E+07					F	2010/08/1	NGUYEN TH	ACTIVE	VN	SF	BA	THUA BA
410036	9.2E+07					F	2013/03/1	PHAM THI	ACTIVE	VN	SF	CO	THUA CO N

I	ENROLLMENT	TIER	START	TIER	END	NATIONALITY	LIFE	AMOUNT	POINTS	EXP. DATE	POINTS	EXP. DATE	POINTS	EXP. DATE	POINTS	EXP. DATE	POINTS	EXP. DATE
410019	2014/11/2	1R	2016/02/1	2017/02/28				101	2016/11/30		101	2016/11/30		101	2016/11/30		101	2016/11/30
410020	2010/08/1	CS	2015/06/1	2065/06/30	VIETNAMESE			15712	2016/09/31		2337	2016/09/31		2337	2016/09/31		2337	2016/09/31
410021	2010/08/1	IS	2015/06/1	2065/06/30	CHINA			9771	2016/08/31		3186	2016/08/31		3186	2016/08/31		3186	2016/08/31
410022	2015/03/1	IS	2015/06/1	2016/06/30				2111	2020/03/31		2111	2020/03/31		2111	2020/03/31		2111	2020/03/31
410023	2015/09/1	IS	2015/10/1	2016/10/31				0			0			0			0	
410024	2015/09/1	IS	2015/12/1	2016/12/31				3914	2020/09/30		3914	2020/09/30		3914	2020/09/30		3914	2020/09/30
410025	2013/05/1	IS	2015/10/1	2016/10/31	OTHER			8252	2019/03/31		8252	2019/03/31		8252	2019/03/31		8252	2019/03/31
410026	2012/07/1	IS	2015/10/1	2016/10/31	JAPAN			106880	2017/07/31		106880	2017/07/31		106880	2017/07/31		106880	2017/07/31
410027	2011/08/1	IS	2015/06/1	2065/06/30	OTHER			40089	2016/08/31		41089	2016/08/31		41089	2016/08/31		41089	2016/08/31
410028	2013/10/1	IS	2015/12/1	2016/12/31				0			0			0			0	
410029	2010/11/2	IS	2016/01/1	2017/01/31	VIETNAMESE			28437	2017/11/30		3914	2017/11/30		3914	2017/11/30		3914	2017/11/30
410030	2014/07/1	IS	2015/10/1	2016/10/31				0			0			0			0	
410031	2013/07/1	IS	2015/10/1	2016/10/31				16301	2018/07/31		16301	2018/07/31		16301	2018/07/31		16301	2018/07/31
410032	2016/07/1	IS	2015/08/1	2016/08/31				13306	2020/07/31		13306	2020/07/31		13306	2020/07/31		13306	2020/07/31
410033	2015/05/1	IS	2015/06/1	2016/06/30				4661	2020/03/31		4661	2020/03/31		4661	2020/03/31		4661	2020/03/31
410034	2010/05/1	IS	2015/06/1	2065/06/30	VIETNAMESE			26496	2015/06/30		20652	2015/06/30		20652	2015/06/30		20652	2015/06/30
410035	2010/08/1	IS	2015/06/1	2065/06/30	VIETNAMESE			2750	2016/08/31		770	2016/08/31		770	2016/08/31		770	2016/08/31
410036	2013/03/1	IS	2015/06/1	2016/06/30	OTHER			15417	2019/03/31		15417	2019/03/31		15417	2019/03/31		15417	2019/03/31
410037	2010/07/1	IS	2015/08/1	2016/08/31	VIETNAMESE			39369	2016/07/31		23650	2016/07/31		23650	2016/07/31		23650	2016/07/31

Figure 51. Client information from Vietnam Airlines

The Civil Aviation Administration of Vietnam reported several attacks, supposedly from 1937cn team, on two Vietnam airports within the same day. The IT system for the check-ins of Vietnam Airlines at Tan Son Nhat International Airport was attacked and stopped working. The deface page, which was the same page used on the Vietnam Airlines website, replaced the flight information screens at Noi Bai International Airport. The speaker system at Noi Bai airport was also compromised by hackers for a few minutes, during which the speakers broadcast an announcement against territory dispute. According to the Civil Aviation Administration of Vietnam, the attack caused the delay of 100 flights, affecting thousands of passengers³⁵.

This incident might hint at future hacktivism trends: to reach a wider audience, hacktivists could potentially broaden their targets from traditional websites to critical infrastructures such as airports.

Hacking Groups' Connections and Campaigns

Deface groups are formed by a loose affiliation between hackers. They can be defined as "loose" since hackers can be affiliated with one or more of these hacking groups, even across territories.

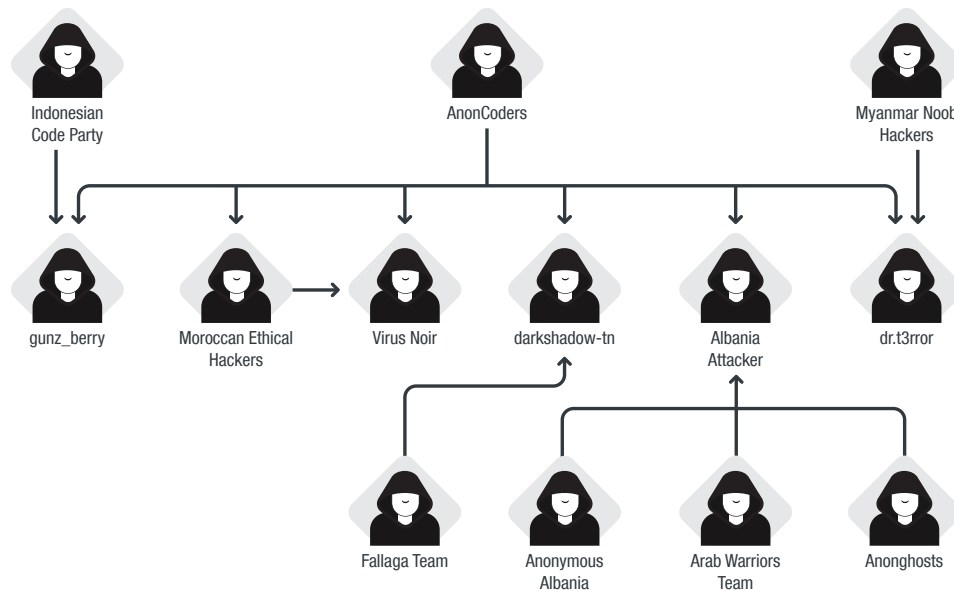


Figure 52. The hacking group AnonCoders

As an example, see the group AnonCoders, which lists gunz_berry, Virus Noir, darkshadow-tn, Albania Attacker and dr.t3rr0r as its core members. However, gunz_berry is also affiliated with Indonesian Code Party, while Virus Noir is affiliated with Moroccan Ethical Hackers, darkshadow-tn with Fallaga Team, and dr.t3rr0r with Myanmar Noob Hackers. Albania Attacker is affiliated with three other groups—Anonymous Albania, Arab Warriors Team, and Anonghosts. AnonCoders shows how hackers can also be members of various groups, and how hackers from different countries can form a group.

Other examples showing the liquidity of group membership are Pakistan's two biggest hacking groups: ZCompany Hacking Crew and Muslim Liberation Army. Both have fairly large teams; ZCompany Hacking Crew has at least 30 members, and Muslim Liberation Army has around 26. Below you can see seven hackers who are members of both groups simultaneously, as we've seen defacements made by both teams acknowledging the hackers in their defacement pages within the same time frame.

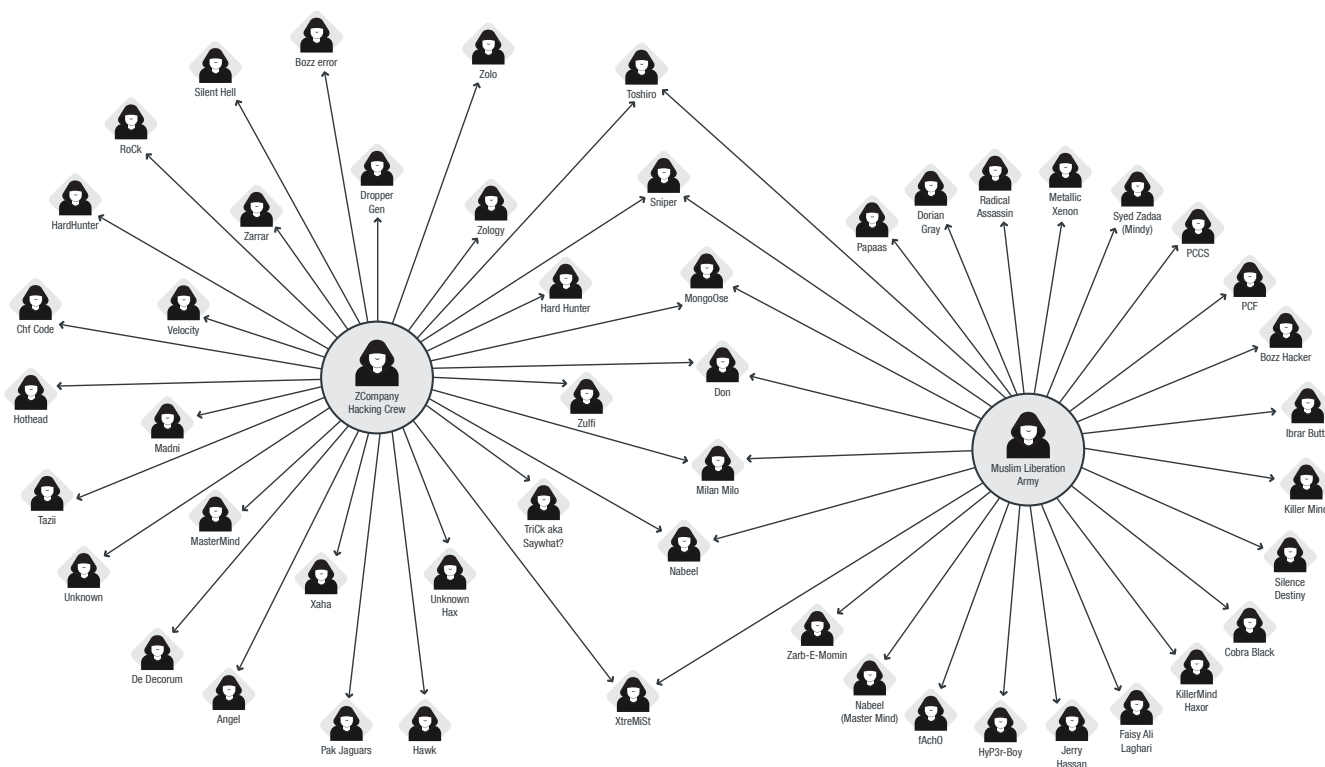


Figure 53. Members of the ZCompany Hacking Crew and the Muslim Liberation Army

Collectives

Hacking groups can also band together to form bigger groups or collectives. The well-known group Anonymous is a model for this. They can rightly be considered the biggest hacking collective in the world based on the numerous hacking groups who identify and associate themselves with the name “Anonymous”.

On a smaller scale, a collective can be formed simply to support a campaign. Take, for example, the defacements done by Bangladeshi hackers against Indian websites, triggered by the Cricket World Cup. The collective Rise of the Tigers was borne out of various Bangladeshi hacking groups working together: 3xp1r3 Cyber Army, Blacksmith Hacker's Team, Cyb3r Command0S, Bangladesh Grey Hat Hackers, Bangladesh Black HAT Hackers, Cyber Sword and Bangladesh Script Kidde Hackers.

Campaign Recruitment and Tools

Certain individuals or groups loosely organize hacktivism campaigns. They set time frames for a particular campaign, and even use social media to coordinate and launch these campaigns.

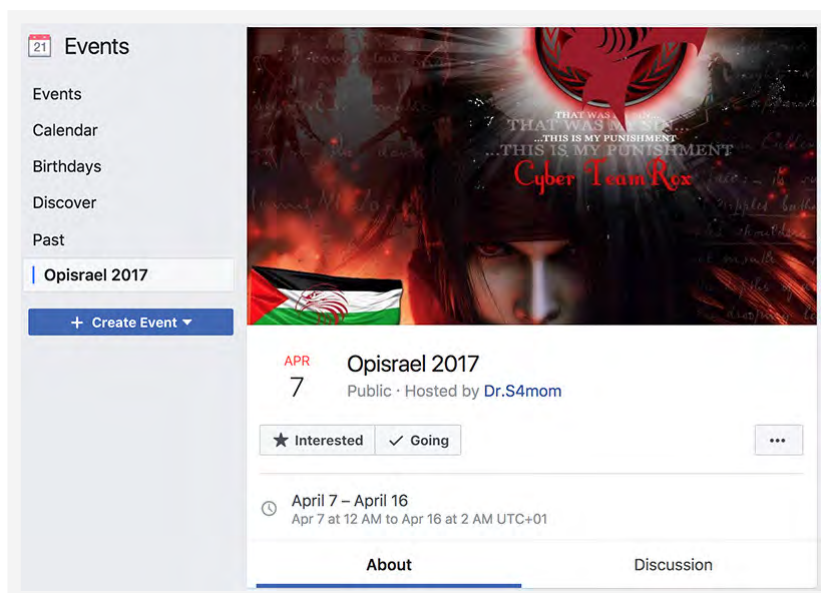


Figure 54. Facebook calendar used to schedule defacement activities

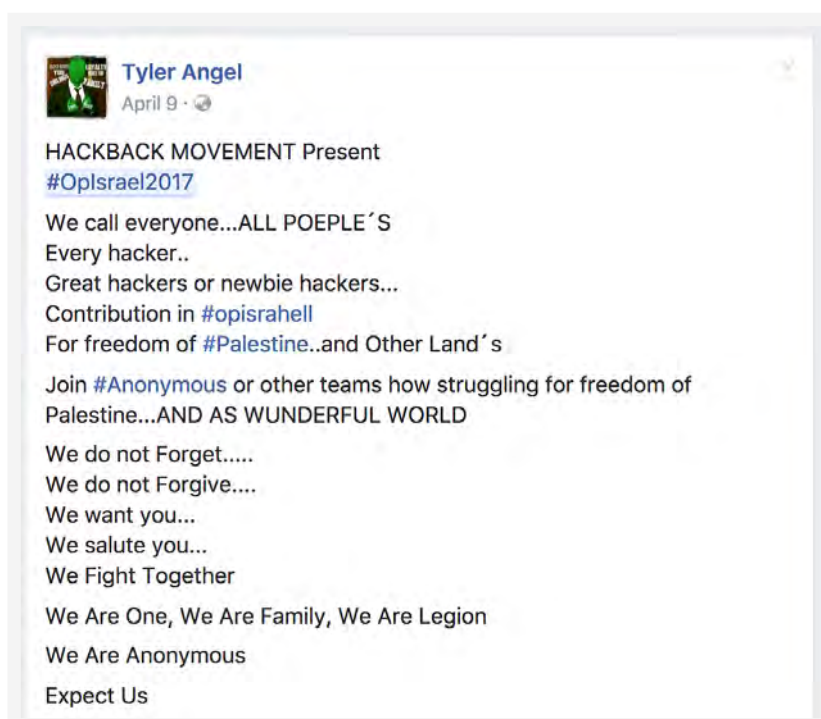


Figure 55. Social media post used to spread templates for defacement scripts

They use calendar event features like Facebook Events to organize campaigns. They also advertise campaigns on their team pages and actively recruit other hackers and hacking groups to participate.

Tools, targets, and defacement page templates are also shared openly by those participating in a campaign.

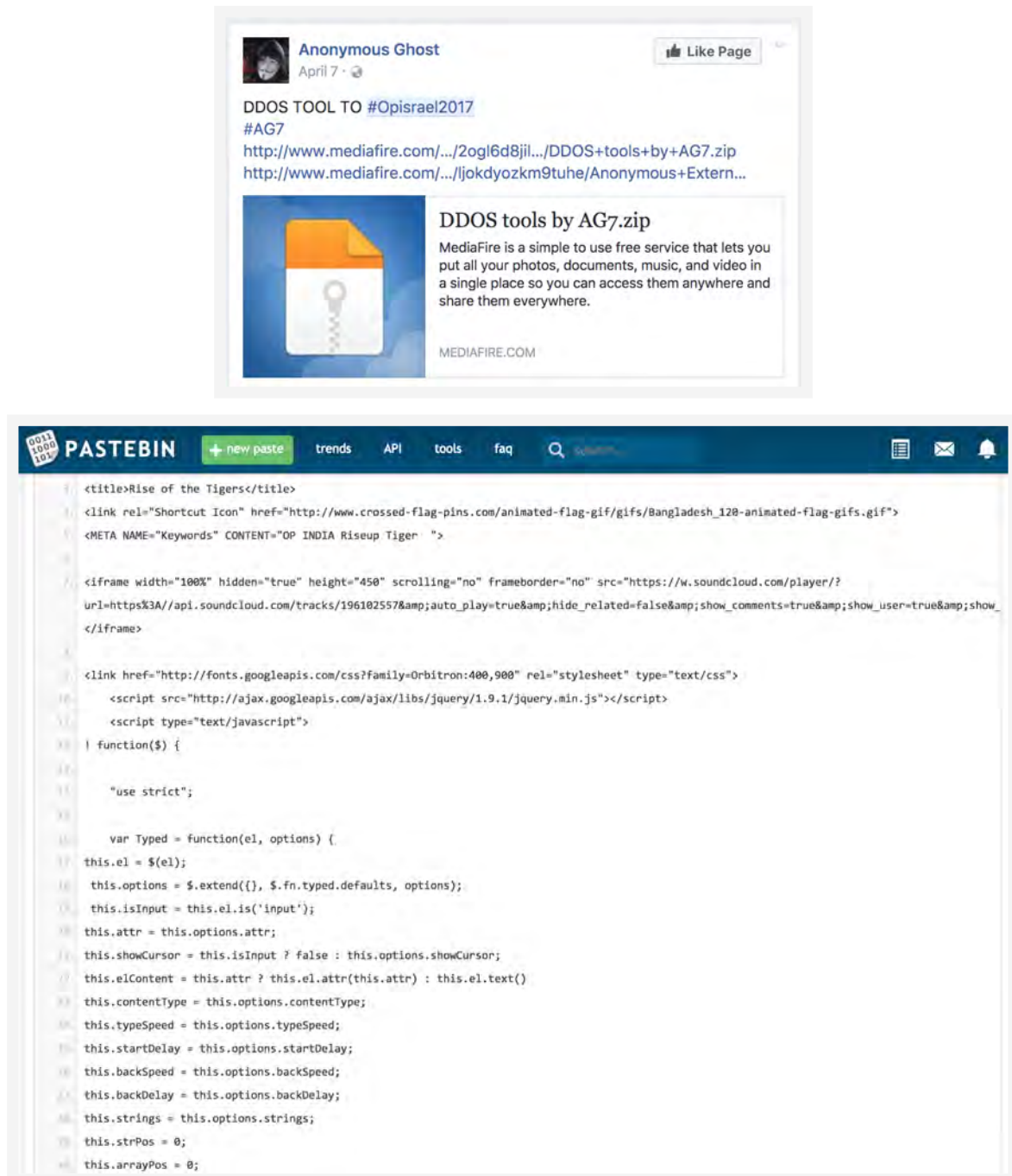


Figure 56. Tools spread through social media and sharing sites

Certain groups also set up team websites to host content, post announcements, and facilitate discussions through forums. These commonly have sections for tutorials, tools, and kits.



Figure 57. Different community sites hosting forums, downloads, news and more

Auxiliary Activities of Defacement Groups

Besides tools and defacement templates, these groups also share attack techniques. For example, groups post hacking tutorials on GitHub and upload tutorial videos to streaming sites.

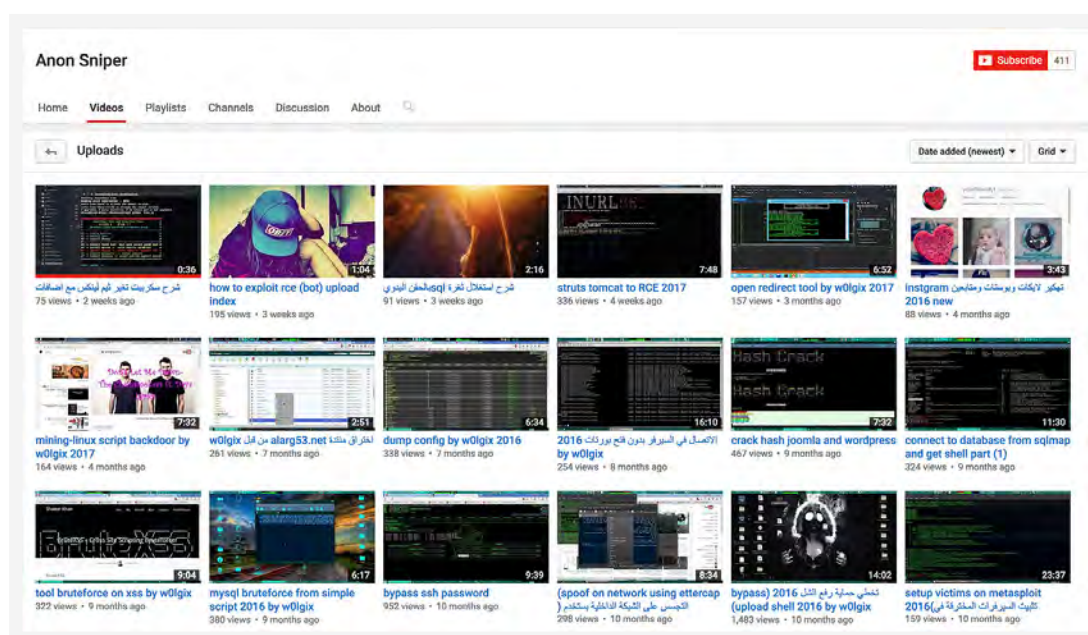
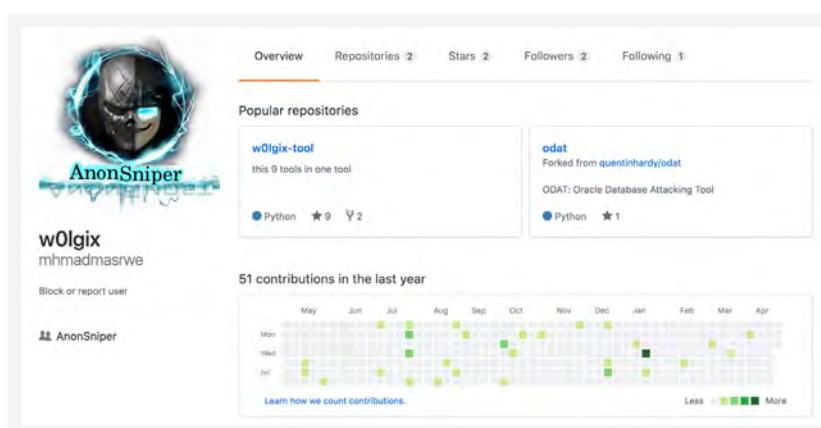


Figure 58. Tools and tutorials for different hacking activities shared by defacers

Defacers are also contributing to Exploit-DB, which is an open-source database for sharing exploit codes and security papers. To find the number of defacers that are also active on Exploit-DB, we compared our list of known defacers against this list of authors³⁶ from Exploit-DB:

- Total defacer/hacker alias that are also listed as Exploit-DB authors: 790 of 7,858 (10.05%)
- PoC submitted by possible defacers: 6,380 of 36,576 (17.44%)

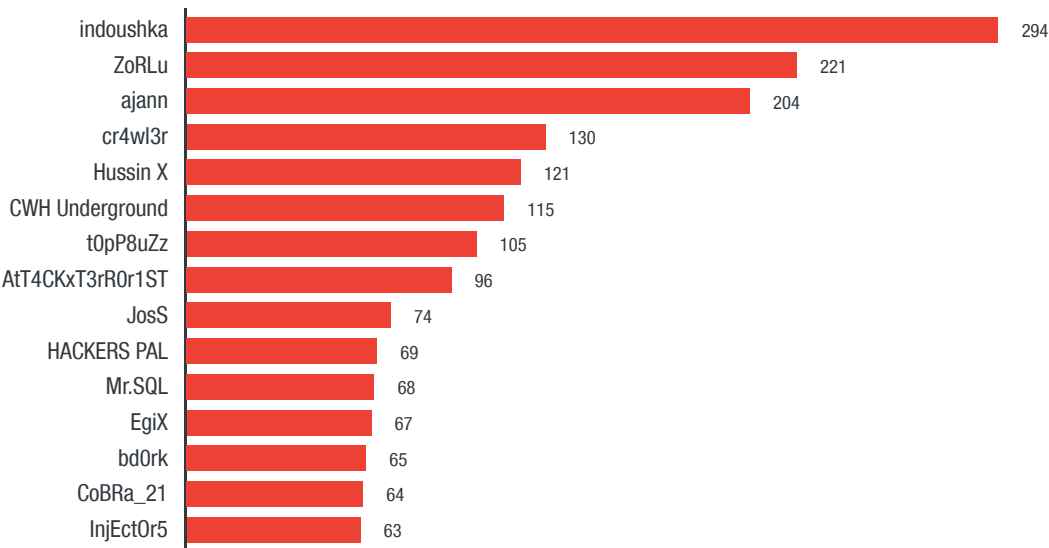


Figure 59. Top 15 defacers who shared exploit codes

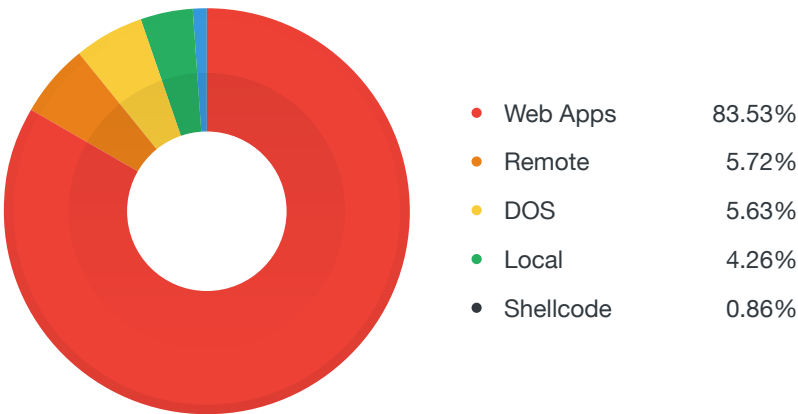


Figure 60. Breakdown of exploit types submitted by possible defacers

Escalating into Real-World Terrorism Activities

Hackers who participate in defacement and also other forms of hacking can also segue into more serious crimes, possibly also driven by real-world disputes and political agendas. An example would be the case of Team P0ison's founder Junaid Hussain (TriCk), who started notable defacements in 2010.



Figure 61. Sample of defaced pages done by TriCk supporting Free Kashmir

Hussain was arrested in 2014 for hacking into Katie Kay's (special advisor to British Prime Minister Tony Blair) email account and leaking PM Blair's personal information³⁷. After six months in jail, Junaid Hussain traveled to Syria and joined ISIS. He took the name Abu Hussain al-Britani, and is believed to be the person behind the hack of U.S. Central Command's Twitter and YouTube accounts. He is also believed to have been killed in a US air strike in Syria in 2015³⁸.

Defaced Sites as Unwitting Infection Sources

Aside from actively committing criminal activities, defacement pages can unwitting carriers of malware code. In the course of our research, we saw the malware Ramnit distributed through malicious websites or packaged as fake software installers. Ramnit is an actively developed malware family whose main goal is to steal banking credentials. It also evolved to include worm propagation capabilities, as well as the ability to infect files, including HTML files. Ramnit does this by appending a VBScript code at the end of the HTML file found in the affected machine. The infected HTML file contains code to install a copy of the Ramnit malware.

Unfortunately, some defacers' machines were infected by Ramnit and had their web defacement templates infected to include the malicious VBScript. This, in turn, made their defacement pages unwitting distributors of the Ramnit malware.

Based on our records, 9,726 defacements were seen to include the Ramnit VBscript. Below are the top 30 defacers who were infected by Ramnit and had their compromised web defacement pages distribute the malware. Most of the defacers were either from Arabic-speaking countries in the Middle East and North Africa or from China. In a serendipitous turn of events, the top defacer that unwittingly spread Ramnit goes by the nickname "stupid".

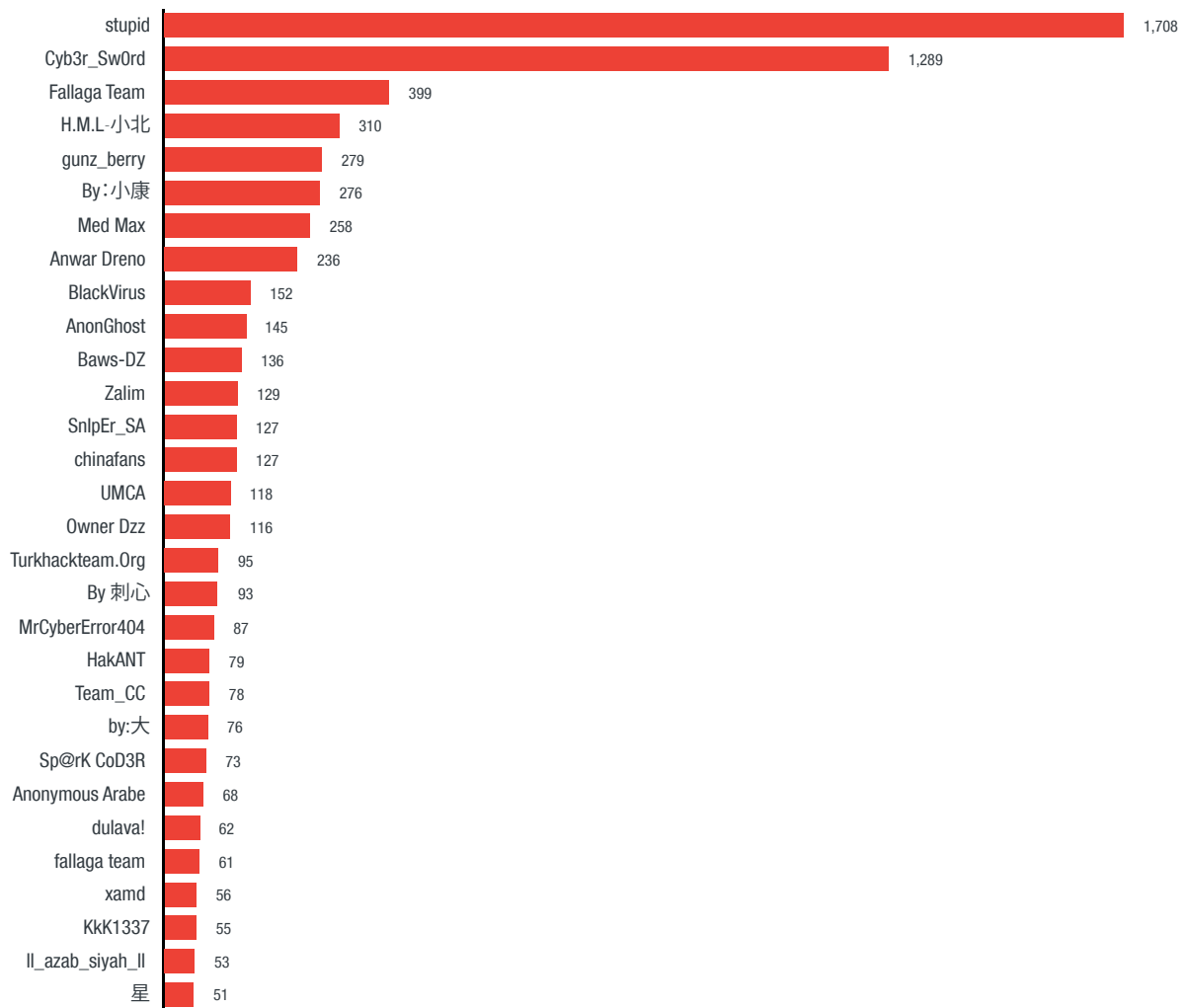


Figure 62. Defacers who were unknowingly spreading Ramnit through their defacement pages

Conclusion

As seen in the examples above, real-world conflict can trigger web defacement on a large scale. One event can lead to a campaign that brings hacking groups together, and large collectives can sustain defacement campaigns for long periods of time. Most are politically or religiously motivated, and attackers are typically keen to express fervent patriotism over specific causes. While these web defacement activities seem relatively benign, it is plausible for defacers to move on to other hacking activities and criminal behavior.

Web Defacements and IoT

Web defacements are going to continue in the foreseeable future, and may even become more prevalent as more Internet of Things (IoT) devices are connected online.

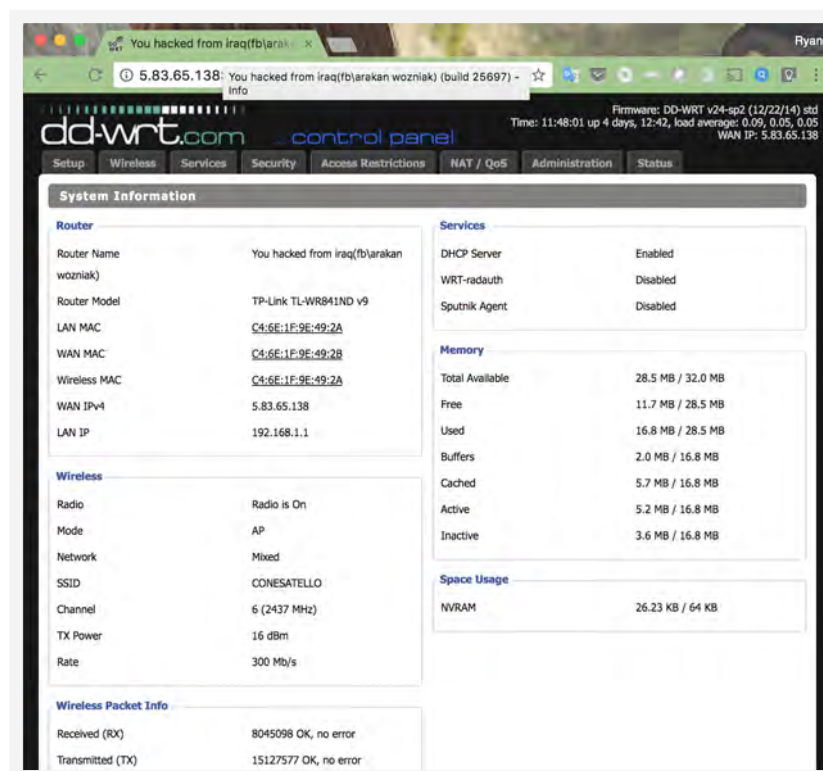


Figure 63. Router control panel replaced with a hacker's page

The above screenshot shows a defaced router control panel, changing the title of the HTML page to "You hacked from iraq(fb\arakan".

A lot of people may not realize that IoT devices have stripped down versions of web servers that host their control panels and management consoles. The setup is something that would be relatively easy for a defacer to exploit and compromise. In the case of the router defacement above, the attacker might not even have known that he was able to deface a non-traditional/IoT website.

Exploits for vulnerabilities of common web applications or server components are also applicable and effective on non-traditional/IoT websites. It would be simple for a defacer to transition into compromising connected IoT devices. With the growing number of IoT devices, it might be appealing for defacers to continue down that route.

Hacktivism in the Future

There are various vulnerabilities that attackers exploit to deface websites to push their specific agenda. But despite compromising these web sites that contain potentially sensitive data (PII, account credentials, transaction histories, etc), most defacers have yet to abuse their access further. They are seemingly content just to deface the site. However, the delineation between pure web defacement and cybercriminal or cyberespionage activity is disappearing. Hackers are now increasingly involved in developing web shells (backdoors to maintain access to compromised web servers), and also delving into doxing and leaking stolen data. After defacing websites, the next step would seem to be capitalizing on the available information on compromised sites.

Apart from individuals, defacement groups have yet to monetize their activities. According to our data, 99.9% of the web defacement pages are harmless. Pages found containing malicious code are mostly infected by VBS_RAMNIT.SMC. These pages were unknowingly infected, and not intentionally put online to spread malicious code. These defacers had their templates infected by the malware and unwittingly spread the Ramnit malware.

A troubling scenario is if these defacement groups decide to monetize their successful hacks by, for example, installing malicious redirections or exploit code in the defacement pages that would then install ransomware. As previously mentioned, so far these defacements have been benign and motivated by real-world conflicts or political agendas. However, cybercriminals could easily use hacks for profit-driven criminal activities.

We have already seen some instances of this. There were reports of Indian hackers targeting Pakistani servers and users to install ransomware for "patriotic" purposes³⁹. If this continues and escalates, then the line between defacers, hacktivists, and cybercriminals will become even more blurred.

How can enterprises protect their sites?

Based on the major vulnerabilities used by defacers, there are simple steps that can secure servers against these threats. If practiced and deployed consistently, these tips can help enterprises have long-term security:

- Ensure that basic security policies are employed and maintained long-term: strong passwords, proper administration security policies, and correct configuration.
- Use web application firewalls to filter, monitor, and block malicious traffic. Security is necessary at the web application level.
- Practice secure coding. Organizations must implement secure coding standards on all their sites.
- Regularly use testing tools to ensure deployed codes are secure.
- Make patching systems and networks a part of standard policy. This prevents cybercriminals from exploiting vulnerabilities in unpatched/ outdated software.
- Regularly scan web applications for vulnerabilities: Organizations need to check their web apps for vulnerabilities as these can lead to SQL injection and cross-site scripting attacks.
- Use multi-layered protection that secures vulnerable websites from the common attacks used by defacers. Solutions like Trend Micro™ Deep Security™ and Vulnerability Protection provides virtual patching that protects servers and endpoints from threats that may abuse vulnerabilities.

References

1. Zone-H archives. (n.d.) Zone-H Unrestricted Information. Last accessed on 11 November 2017 at <http://www.zone-h.org/>
2. Ibid
3. Hack CN. (n.d.). 全球被黑站点统计|黑客技术检测|黑客入侵攻击. Last accessed on 17 November 2017 at <http://www.hack-cn.com/>.
4. <http://www.mirror-zone.org> (offline)
5. H4ck Mirror. (n.d.) *Hack Mirror*. Last accessed on 16 November 2017 at <http://www.hack-mirror.com/>.
6. <http://www.mydeface.com> (offline)
7. BBC Newsround. (20 February 2015). *BBC Newsround*. "Guide: Why are Israel and the Palestinians fighting over Gaza?" Last accessed 16 November 2017 at <http://www.bbc.co.uk/newsround/20436092>.
8. Al-Islam. (n.d.) Al-Islam.org. "The Battle of Badr". Last accessed 14 Nov 2017 at <https://www.al-islam.org/articles/battle-badr>.
9. Yifa Yaakov. (5 August 2014). *The Times of Israel*. "After 29 days, Operation Protective Edge by the numbers". Last accessed 17 November 2017 at <https://www.timesofisrael.com/after-29-days-operation-protective-edge-by-the-numbers/>.
10. ABC. (8 January 2015). *ABC News*. "Charlie Hebdo shooting: 12 people killed, 11 injured, in attack on Paris offices of satirical newspaper". Last accessed 14 November 2017 at <http://www.abc.net.au/news/2015-01-07/charlie-hebdo-satirical-newspaper-shooting-paris-12-killed/6005524>.
11. AFP/Reuters. (16 July 2017). *Deutsche Welle*. "'Cyber Army' hacker arrested, says Bulgaria". Last accessed 17 November 2017 at <http://www.dw.com/en/cyber-army-hacker-arrested-says-bulgaria/a-18586433>.
12. Rifat Fareed. (27 October 2017) *Al Jazeera*. "'Black day' in Kashmir marks 1947 Indian army arrival". Last accessed 17 November 2017 at <http://www.aljazeera.com/news/2017/10/day-kashmir-marks-1947-indian-army-arrival-171027122649223.html>.
13. Maps of India. (n.d.) *Maps of India*. "26th October 1947: Maharaja Hari Singh agrees to the accession of Jammu and Kashmir to India" Last accessed 16 November 2017 at <https://www.mapsofindia.com/on-this-day/26th-october-1947-maharaja-hari-singh-agrees-to-the-accession-of-jammu-and-kashmir-to-india>.
14. Aijaz Hussain. (10 December 2013). *The San Diego Union Tribune*. "Activists, families protest Kashmir disappearances". Last accessed 13 November 2017 at <http://www.sandiegouniontribune.com/sdut-activists-families-protest-kashmir-disappearances-2013dec10-story.html>.
15. Rupam Jain. (19 December 2016) *Reuters*. "India indicts Pakistan-based militants over Pathankot air base attack" Last accessed 17 November 2017 at <http://in.reuters.com/article/india-pakistan-attack/india-indicts-pakistan-based-militants-over-pathankot-air-base-attack-idINKBN1480QO>.
16. Hari Kumar and Geeta Anand. (18 September 2016). *The New York Times*. "17 Indian Soldiers Killed by Militants in Kashmir" Last accessed 17 November 2017 at <https://www.nytimes.com/2016/09/19/world/asia/17-indian-soldiers-killed-by-militants-in-kashmir.html>.
17. Shubhajit Roy. (24 September 2015). *The Indian Express*. "Make seven changes to your Constitution: India tells Nepal". Last accessed 2 November 2017 at <http://indianexpress.com/article/world/neighbours/make-seven-changes-to-your-constitution-address-madhesi-concerns-india-to-nepal/>.
18. Medecins Sans Frontieres. (26 April 2016). *MSF.org*. "Syria: Update on airstrike at Al Quds hospital". Last accessed 17 November 2017 at <http://www.msf.org/en/article/syria-update-airstrike-al-quds-hospital>.

19. Die Morina. (2 March 2017) *Balkan Transitional Justice*. "Mitrovica's Flashpoint Bridge Symbolises Kosovo's Divisions". Last accessed 17 November 2017 at <http://www.balkaninsight.com/en/article/mitrovica-s-flashpoint-bridge-symbolises-kosovo-s-divisions-03-01-2017>.
20. Tarra Quismundo. (16 April 2016). *Inquirer*. "PCG men ordered to pay Taiwan family". Last accessed 17 November 2017 at <http://globalnation.inquirer.net/138653/pcg-men-ordered-to-pay-taiwan-family>.
21. Sofia Wu. (13 May 2013) *Focus Taiwan*. "Shooting ignites Taiwan-Philippines cyber war ", Last accessed 16 November 2017 at <http://focustaiwan.tw/news/atod/201305130041.aspx>.
22. Clifford Trigo. (11 May 2013). *Pinoy Hack News*. "Pinoy Vendetta sends warning message to Taiwan, defaces 5 websites". Last accessed 17 November 2017 at <https://www.pinoyhacknews.com/pinoy-vendetta-sends-warning-message-to-taiwan-defaces-5-websites>.
23. Petro Vietnam. (1 June 2011) *PetroVietnam*. "Chinese ships destroy Vietnam sea cable". Last accessed 17 November 2017 at <https://www.youtube.com/watch?v=w1H6zcuXjJ8>.
24. ChinaAZ. (8 June 2011). *Cheng Cold Blog*. "Many websites in the South China Sea were attacked by Vietnamese hackers and Chinese hijackers counterattacked". Last accessed 17 November 2017 at http://www.bj3gweb.com/Link201106_WebAttack_ChinaAndVietnam.html.
25. Ibid
26. Kafan. (5 June 2011) *Kafan.cn*. "Many domestic websites were attacked by Vietnamese hackers". Last accessed on 16 November 2017 at <http://bbs.kafan.cn/thread-999960-1-1.html>.
27. Xiao Bian. (6 May 2012). *Freebuf*. "My Filipino Maid is a Hackers - China and the Philippines network war". Last accessed 16 November 2017 at <http://www.freebuf.com/news/913.html>.
28. Edwin Lacierda. (23 April 2012). *Official Gazette*. "Statement of Presidential Spokesperson Edwin Lacierda". Last accessed on 16 November 2017 at <http://www.officialgazette.gov.ph/2012/04/23/statement-of-the-presidential-spokesperson-on-the-denial-of-service-attack-on-pcdspo-maintained-websites-april-23-2012/>.
29. Rappler. (25 April 2012) *Rappler*. "DBM website hacked". Last accessed on 24 November 2017 at <https://www.rappler.com/nation/4341-dbm-website-hacked>.
30. Reuters. (9 April 2015) *CNBC*. "China mounts detailed defence of South China Sea reclamation". Last accessed on 223 November 2017 at <http://www.cnbc.com/2015/04/09/china-mounts-detailed-defence-of-south-china-sea-reclamation.html>.
31. Pastebin. (28 May 2015) *#OpChina Official Index*. Last accessed 15 November 2017 at <https://pastebin.com/xii97KNy>.
32. Anni Piiparinen. (22 July 2016). *The Diplomat*. "China's Secret Weapon in the South China Sea: Cyber Attacks". Last accessed 18 November 2017 at <https://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/>.
33. Vietnam News (29 July 2016). *Vietnam News*. "Chinese hackers attack VN's airports and Vietnam Airlines' website". Last accessed 16 November 2017 at <http://vietnamnews.vn/society/300416/chinese-hackers-attack-vns-airports-and-vietnam-airlines-website.html#vecZdAWfcqd8iKGz.97>.
34. Tara Seals. (29 July 2016). *Info-Security Magazine*. "Chinese Hackers Attack Airports Across Vietnam". Last accessed 15 November 2017 at <https://www.infosecurity-magazine.com/news/chinese-hackers-attack-airports/>.
35. Vietnam News (29 July 2016). *Vietnam News*. "Chinese hackers attack VN's airports and Vietnam Airlines' website". Last accessed 16 November 2017 at <http://vietnamnews.vn/society/300416/chinese-hackers-attack-vns-airports-and-vietnam-airlines-website.html#vecZdAWfcqd8iKGz.97>.

36. GitHub. *The Official Exploit Database Repository*. Last accessed on 16 November 2017 at <https://github.com/offensive-security/exploit-database>.
37. Gianluca Mezzofiore. (2 July 2014). *International Business Times*. "Team Poison's Junaid Hussain Jailed for Tony Blair Hack and Phone Bombing Anti-Terror Hotline". Last accessed on 20 November 2017 at <http://www.ibtimes.co.uk/team-poison-phone-bomb-hacker-anti-terror-367660>.
38. Spencer Ackerman, Ewan MacAskillin and Alice Ross. (27 August 2015). *The Guardian*. "Junaid Hussain: British hacker for Isis believed killed in US air strike". Last accessed 16 November 2017 at <https://www.theguardian.com/world/2015/aug/27/junaid-hussain-british-hacker-for-isis-believed-killed-in-us-airstrike>.
39. India Defense News. (7 October 2016). *India Defense News*. "'Patriotic' Indian Hackers Lock Pakistani Websites and Refuse to Give Back the Key". Last accessed on November 17 at <http://www.indiandefensenews.in/2016/10/patriotic-indian-hackers-lock-pakistani.html>.

Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.



Securing Your Journey
to the Cloud

www.trendmicro.com