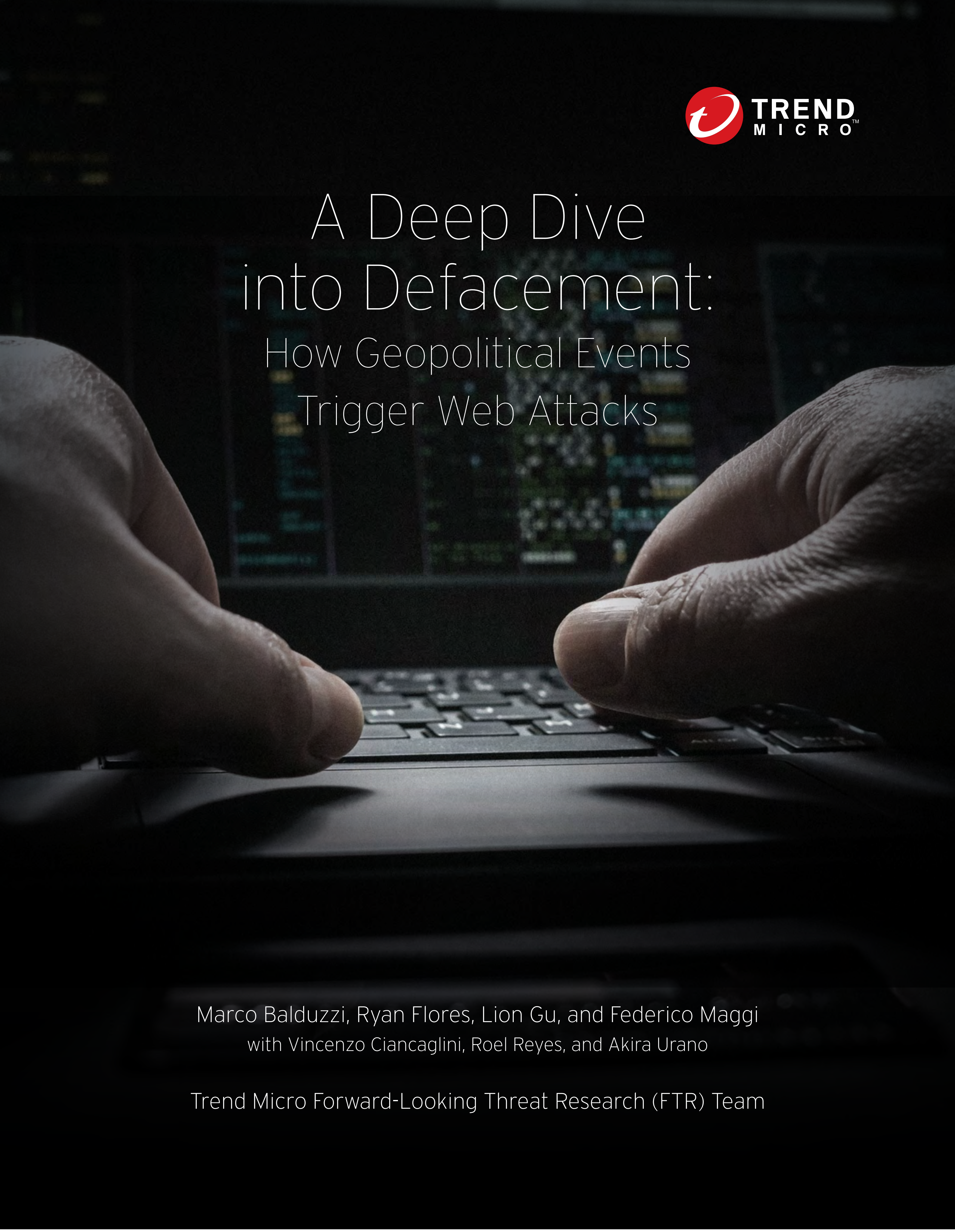


A Deep Dive into Defacement:

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

A **TrendLabs** Research Paper

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.

for Raimund Genes (1963-2017)

Contents

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.

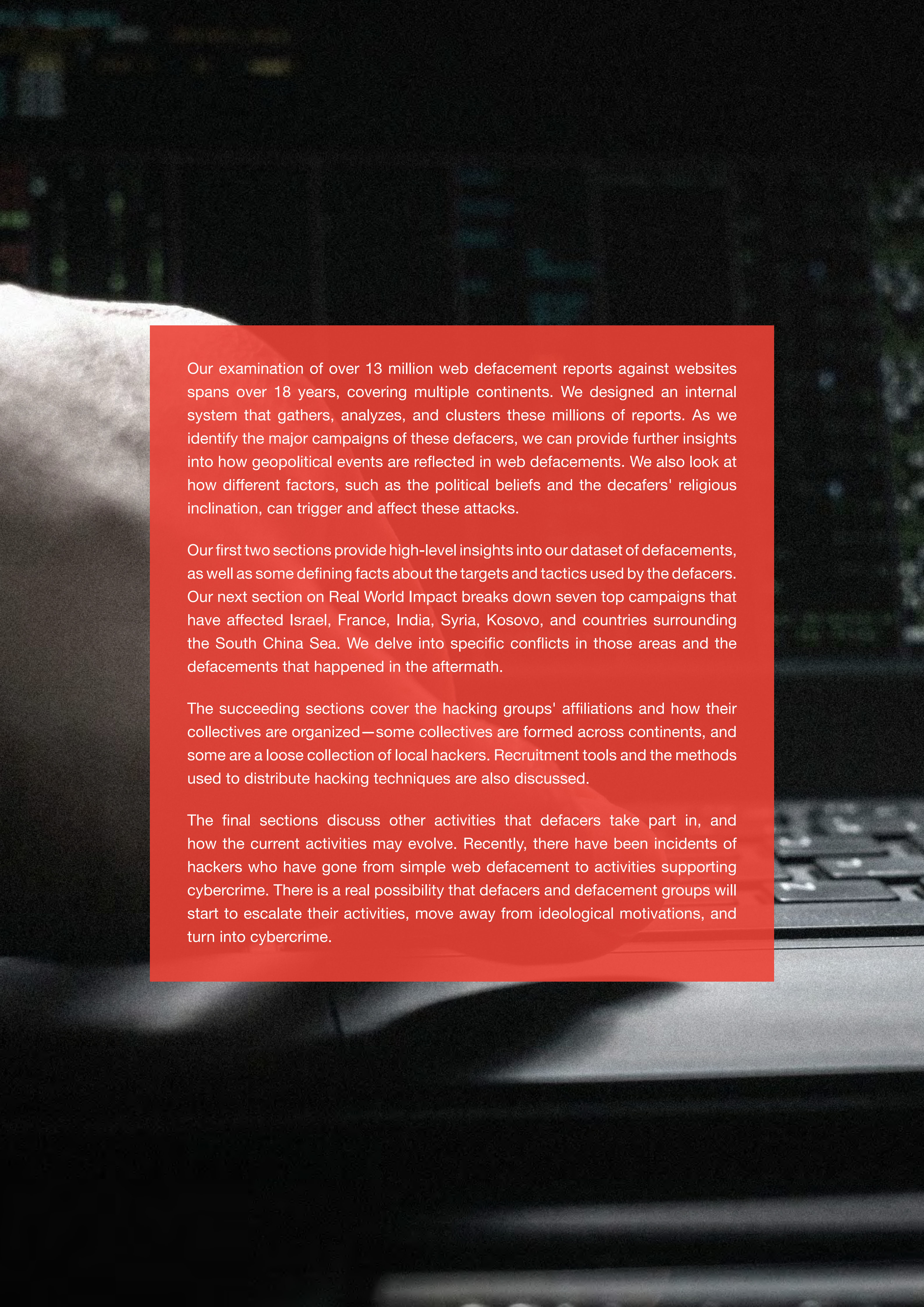
Of course, the typical cybercriminal's goal is to profit. They might compromise websites to push ransomware, or they could try and steal data—recent breaches show that information is an increasingly valuable commodity. But, as this paper discusses, more emotional motivations, such as patriotism, specific 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-H[1] 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.



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 decafers' 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-H[2]: 12,303,240 defacement incidents
- Hack-CN[3]: 386,705 defacement incidents
- Mirror Zone[4] (now offline): 195,398 defacement incidents
- Hack Mirror[5]: 68,980 defacement incidents
- MyDeface[6] (now offline): 37,843 defacement incidents

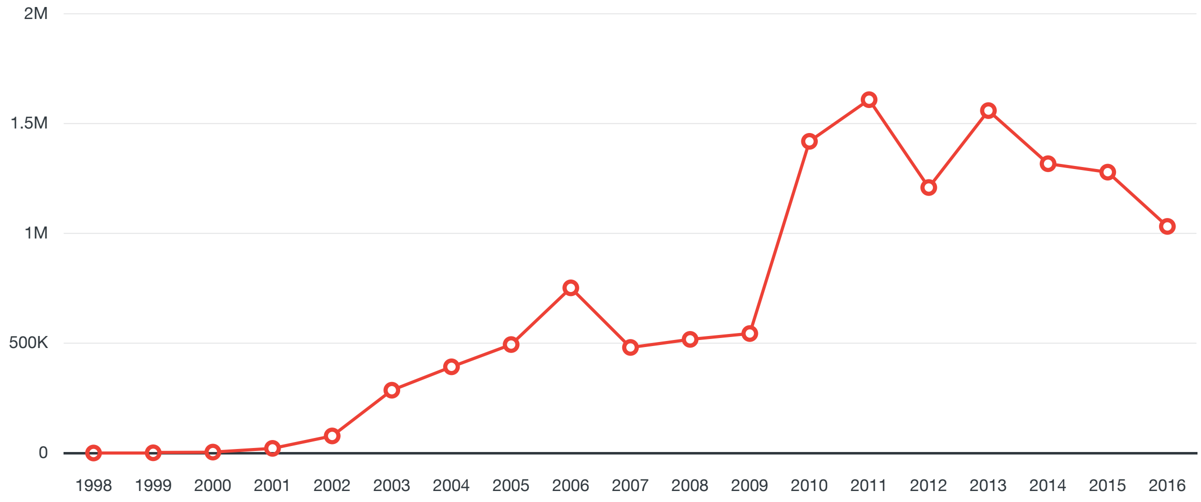


Figure 1. The rate of web defacement records per year

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.

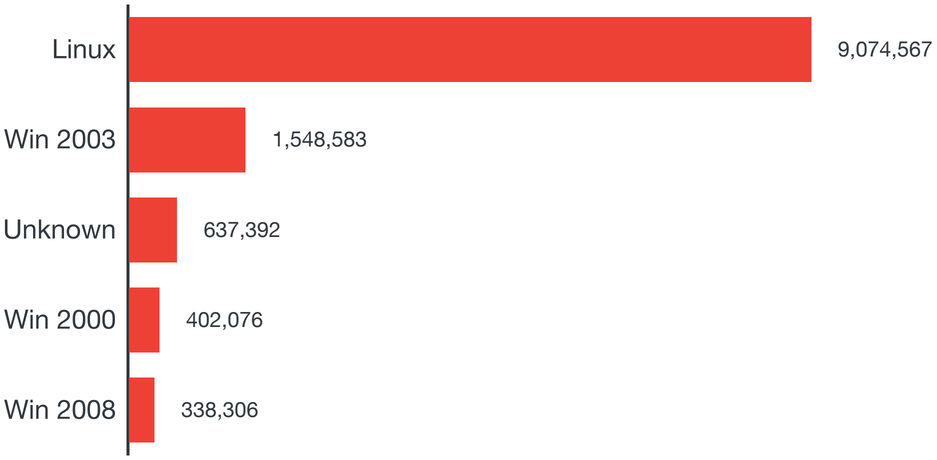


Figure 2. Operating systems of defaced web sites

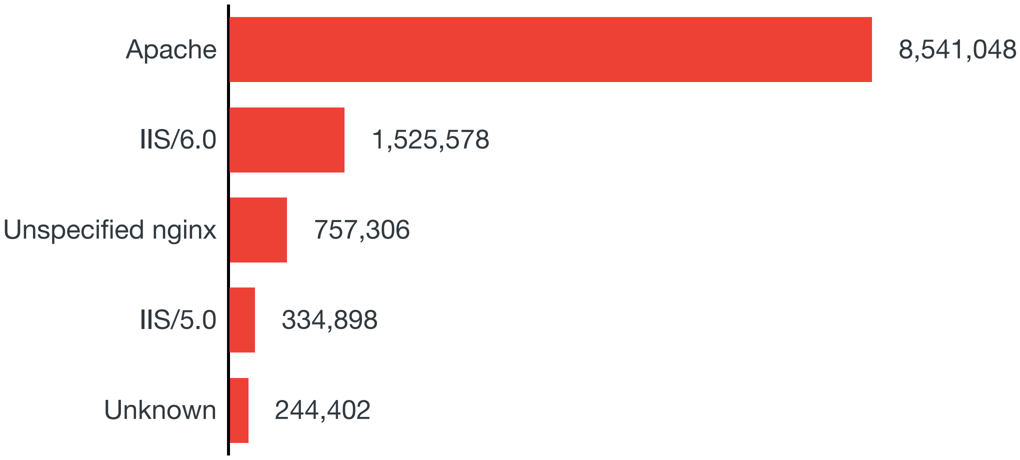


Figure 3. Web servers of defaced websites

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:

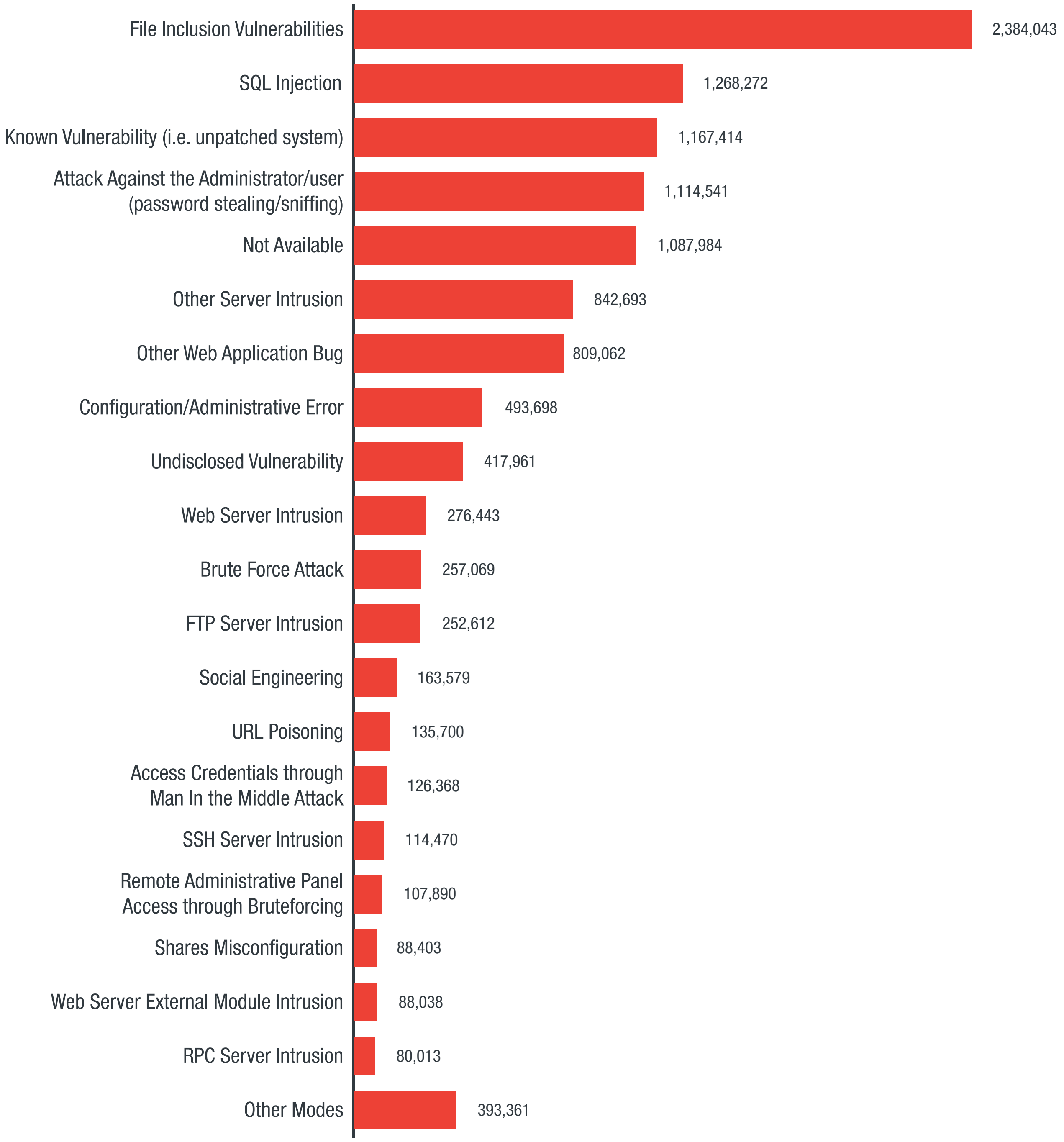


Figure 4. The methods of hacking as reported by defacers, based on defacement ID Information

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.

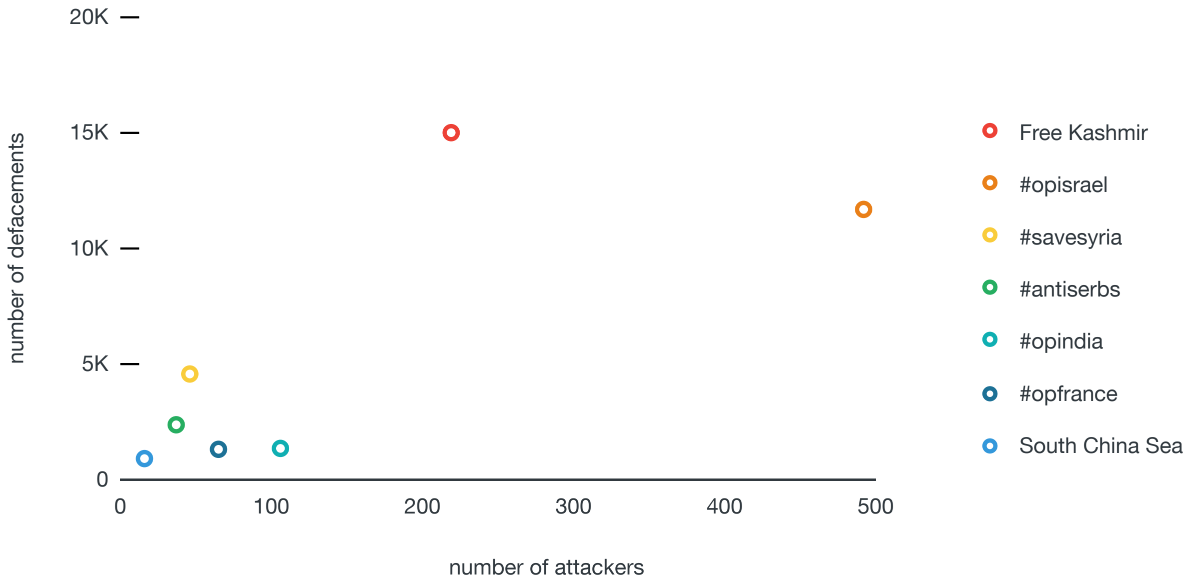


Figure 5. Overview of the top seven defacement campaigns from collected data

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.

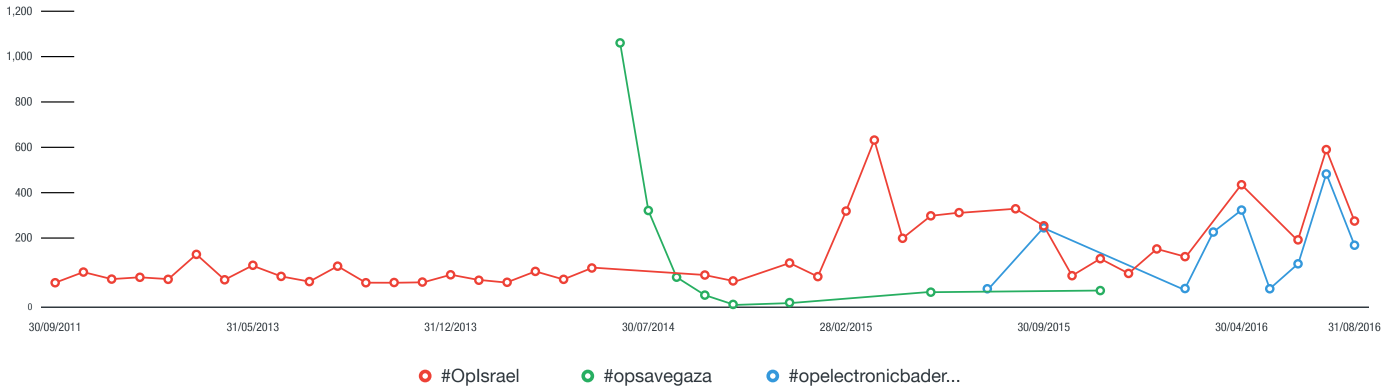


Figure 6. #OpIsrael, #opsavegaza and #opbader / #electronicbader / #baderoperation timelines

The struggle between Israel and Palestine is one of the longest modern-day conflicts, starting in 1948 and continuing to this day[7]. 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.

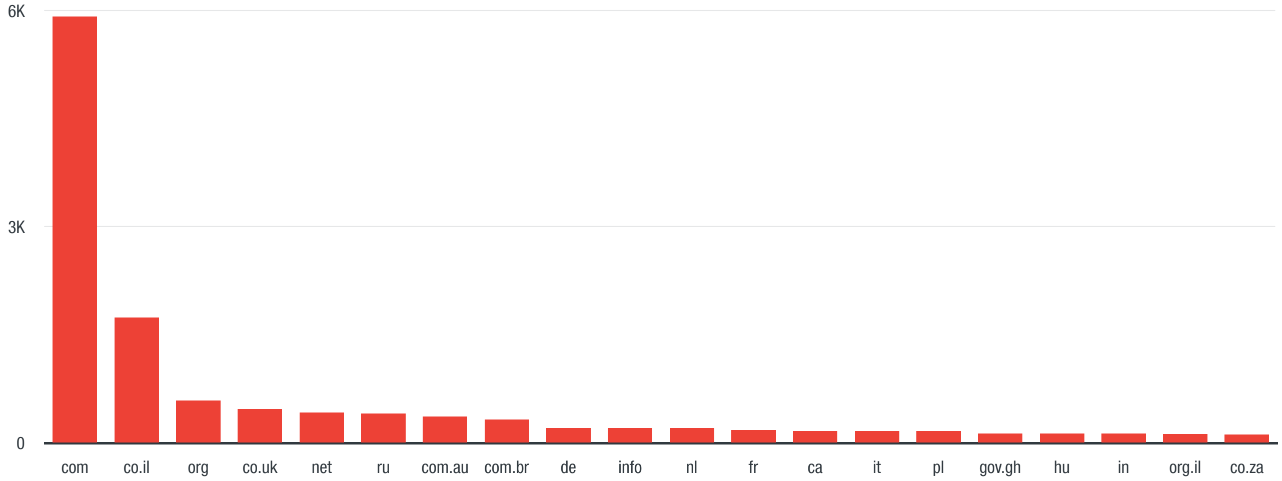
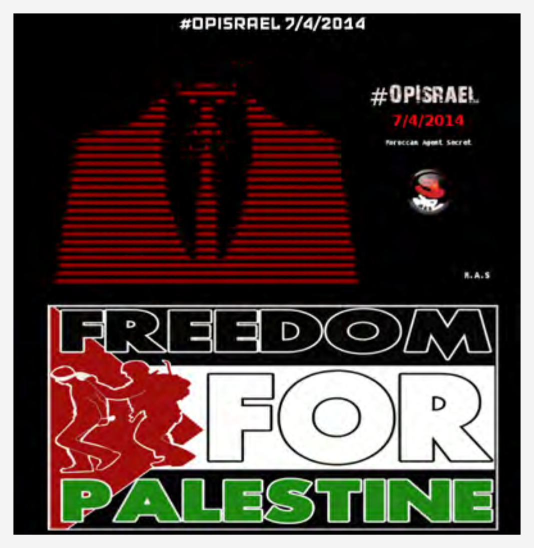
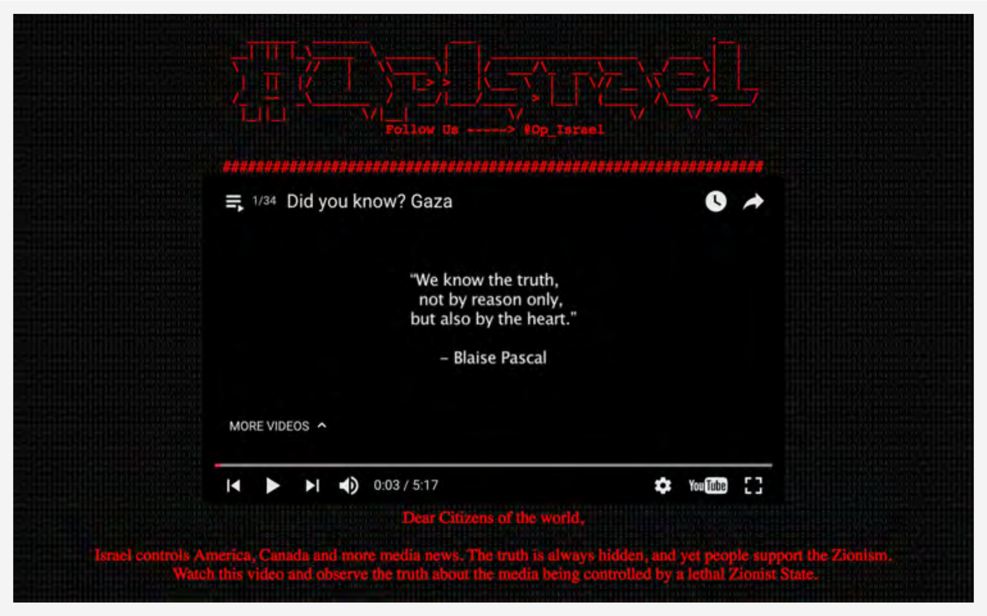


Figure 7. Target sites for #OpIsrael

#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.





Follow Us -----> @Op_Israel

Did you know? Gaza

"We know the truth,
not by reason only,
but also by the heart."

– Blaise Pascal

Dear Citizens of the world,

Israel controls America, Canada and more media news. The truth is always hidden, and yet people support the Zionism.
Watch this video and observe the truth about the media being controlled by a lethal Zionist State.

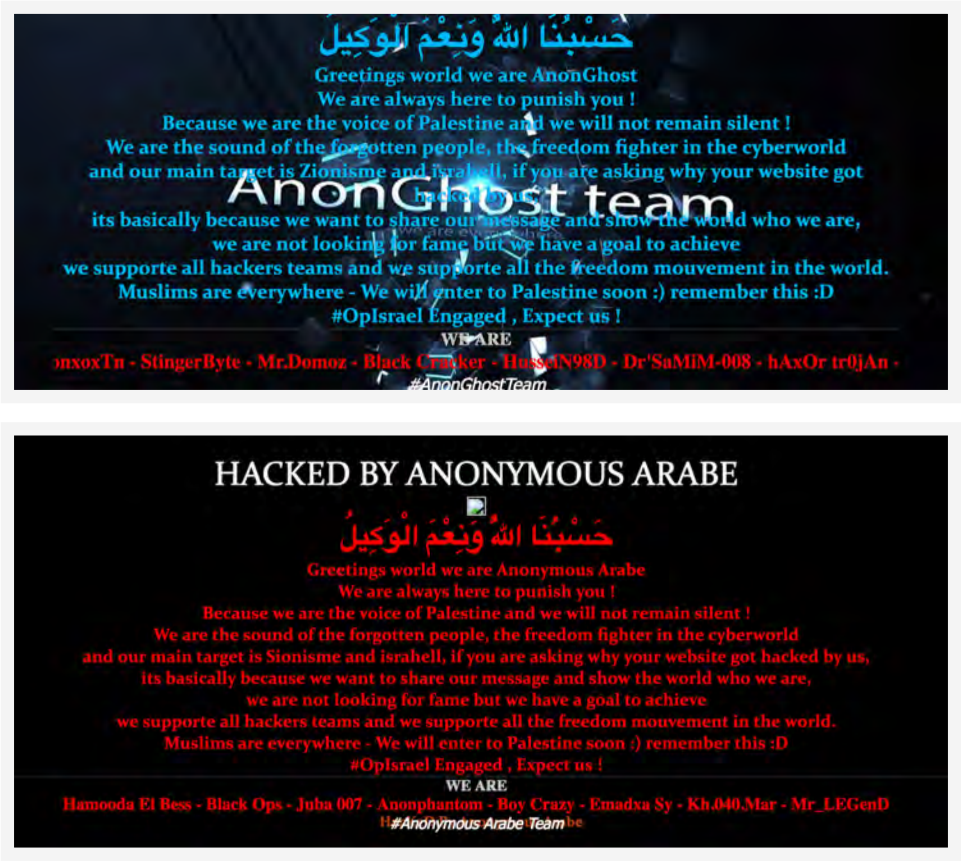
Figure 8. The first #OpIsrael defacement made by imLulzPirate

#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.



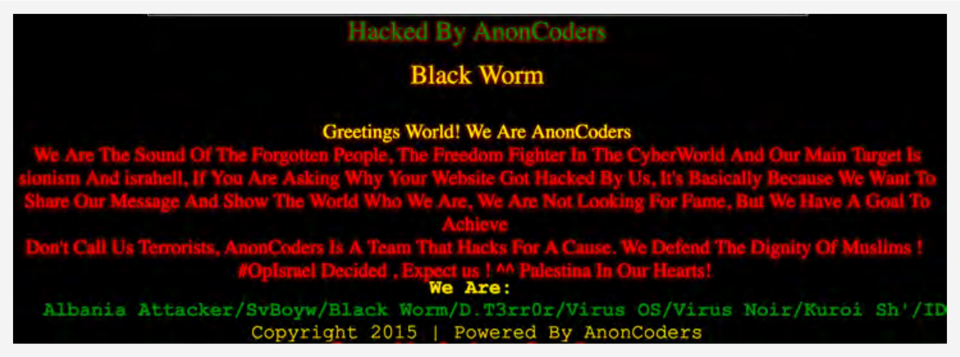
حَسْبُنَا اللهُ وَنِعْمَ الْوَكِيل
Greetings world we are AnonGhost
We are always here to punish you !
Because we are the voice of Palestine and we will not remain silent !
We are the sound of the forgotten people, the freedom fighter in the cyberworld
and our main target is Zionisme and israhell, if you are asking why your website got
hacked by us,
its basically because we want to share our message and show the world who we are,
we are not looking for fame but we have a goal to achieve
we supporte all hackers teams and we supporte all the freedom mouvement in the world.
Muslims are everywhere - We will enter to Palestine soon :) remember this :D
#OpIsrael Engaged , Expect us !
WE ARE
ınxoxTn - StingerByte - Mr.Domoz - Black Cracker - HusseIN98D - Dr'SaMiM-008 - hAxOr tr0jAn -

HACKED BY ANONYMOUS ARABE
حَسْبُنَا اللهُ وَنِعْمَ الْوَكِيل
Greetings world we are Anonymous Arabe
We are always here to punish you !
Because we are the voice of Palestine and we will not remain silent !
We are the sound of the forgotten people, the freedom fighter in the cyberworld
and our main target is Sionisme and israhell, if you are asking why your website got hacked by us,
its basically because we want to share our message and show the world who we are,
we are not looking for fame but we have a goal to achieve
we supporte all hackers teams and we supporte all the freedom mouvement in the world.
Muslims are everywhere - We will enter to Palestine soon :) remember this :D
#OpIsrael Engaged , Expect us !
WE ARE
Hamooda El Bess - Black Ops - Juba 007 - Anonphantom - Boy Crazy - Emadxa Sy - Kh.040.Mar - Mr_LEGenD

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.



Hacked By AnonCoders

Black Worm

Greetings World! We Are AnonCoders

We Are The Sound Of The Forgotten People, The Freedom Fighter In The CyberWorld And Our Main Target Is sionism And israhell, If You Are Asking Why Your Website Got Hacked By Us, It's Basically Because We Want To Share Our Message And Show The World Who We Are, We Are Not Looking For Fame, But We Have A Goal To Achieve

Don't Call Us Terrorists, AnonCoders Is A Team That Hacks For A Cause. We Defend The Dignity Of Muslims !

#OpIsrael Decided , Expect us ! ^^ Palestina In Our Hearts!

We Are:

Albania Attacker/SvBoyw/Black Worm/D.T3rr0r/Virus OS/Virus Noir/Kuroi Sh'/ID

Copyright 2015 | Powered By AnonCoders

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:

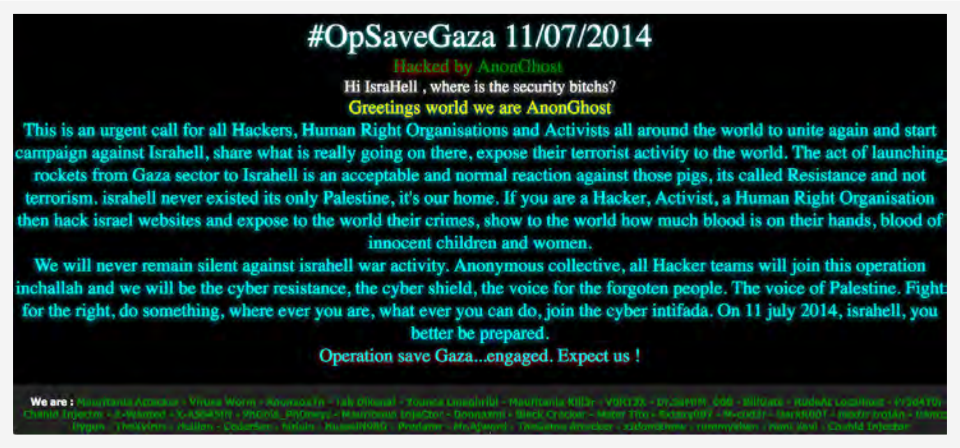
#opisrael #alfallagaTeam #fallaga #fallagateam #tunisianfallagateam #opbader #electronicBader #baderoperation #hackers #fallagahackers

"Bader" is a reference to the Battle of Badr, a significant battle won by the Prophet Muhammad in the early years of Islam[8]. 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 Israel[9]. 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.



#OpSaveGaza 11/07/2014

Hacked by AnonGhost

Hi IsraHell , where is the security bitchs?

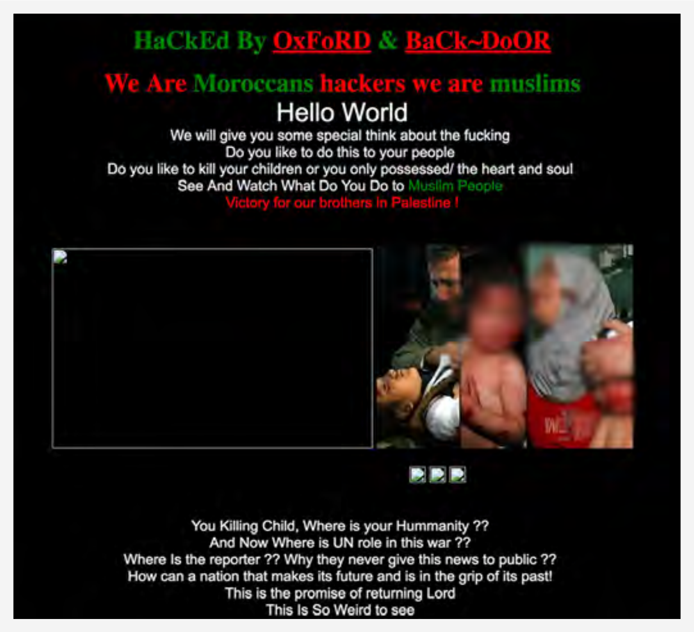
Greetings world we are AnonGhost

This is an urgent call for all Hackers, Human Right Organisations and Activists all around the world to unite again and start campaign against Israhell, share what is really going on there, expose their terrorist activity to the world. The act of launching rockets from Gaza sector to Israhell is an acceptable and normal reaction against those pigs, its called Resistance and not terrorism. israhell never existed its only Palestine, it's our home. If you are a Hacker, Activist, a Human Right Organisation then hack israel websites and expose to the world their crimes, show to the world how much blood is on their hands, blood of innocent children and women.

We will never remain silent against israhell war activity. Anonymous collective, all Hacker teams will join this operation inchallah and we will be the cyber resistance, the cyber shield, the voice for the forgoten people. The voice of Palestine. Fight for the right, do something, where ever you are, what ever you can do, join the cyber intifada. On 11 july 2014, israhell, you better be prepared.

Operation save Gaza...engaged. Expect us !

We are : Mauritania Attacker - Virus Worm - AnonsoXfn - Tak Dikenal - Younes Unaghribi - Mauritania Kill3r - V0RT3X - Dr.SaMiM_000 - BillGate - RudeAt LocalHost - Pr5d4T0r - Chahid Injector - X-Wanted - X-ASS4SSIN - PhOOl4_PhOmeyz - Mauritanie InjeCtor - Doonaxmi - Black Cracker - Mister Tito - Extazy007 - M-cod3r - DarkR00T - mOstr trojAn - [illegible]
Hygun - TheKvinn - Hullion - CoderSec - Ninja - HusseIN98D - Prodamr - Mr.Afword - TheGame Attacker - [illegible] - rummyelian - Nani Xavi - Chahid Injector



HaCkEd By OxFoRD & BaCk~DoOR

We Are Moroccans hackers we are muslims

Hello World

We will give you some special think about the fucking
Do you like to do this to your people
Do you like to kill your children or you only possessed/ the heart and soul
See And Watch What Do You Do to Muslim People
Victory for our brothers in Palestine !

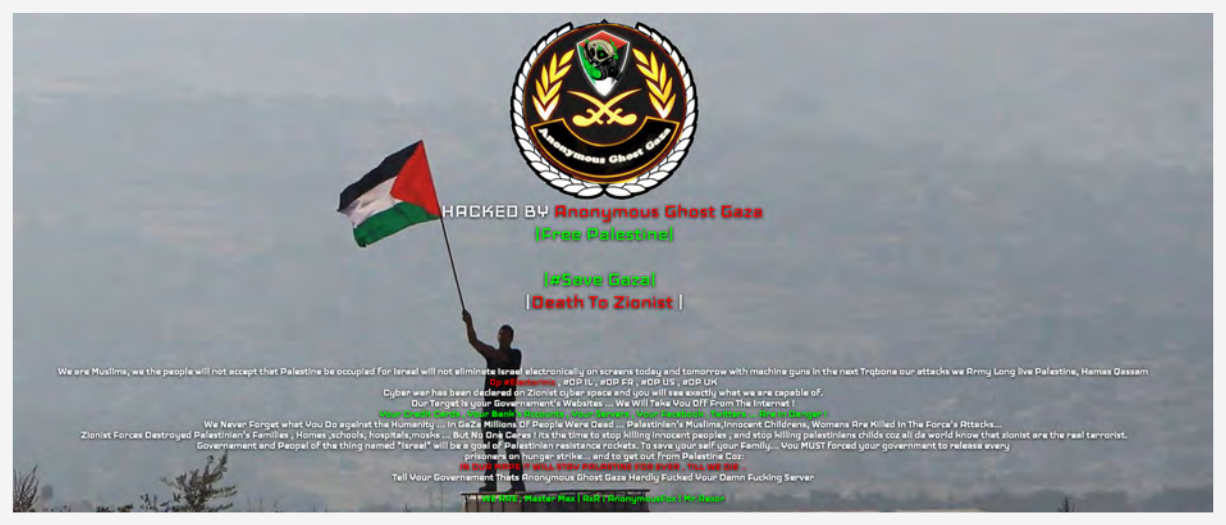
You Killing Child, Where is your Hummanity ??
And Now Where is UN role in this war ??
Where Is the reporter ?? Why they never give this news to public ??
How can a nation that makes its future and is in the grip of its past!
This is the promise of returning Lord
This Is So Weird to see

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.



HACKED BY Anonymous Ghost Gaza
|Free Palestine|

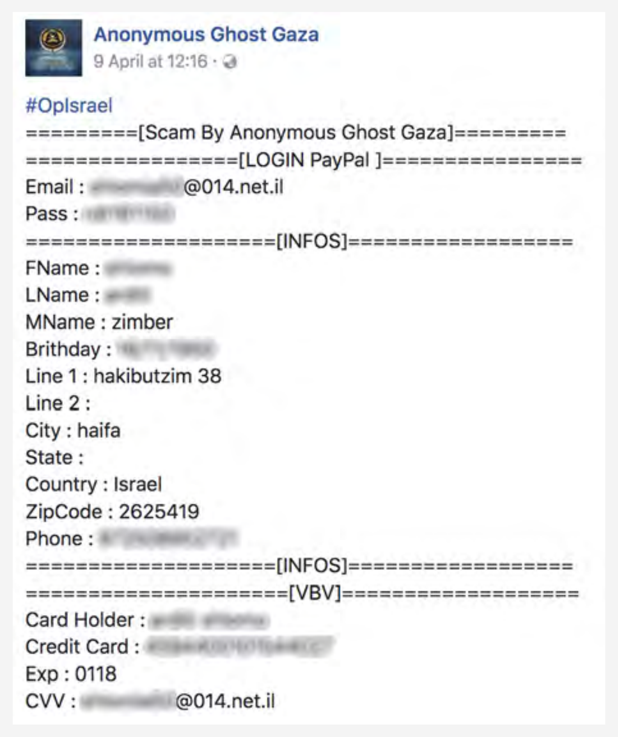
|#Save Gaza|
|Death To Zionist |

We are Muslims, we the people will not accept that Palestine be occupied for Israel will not eliminate Israel electronically on screens today and tomorrow with machine guns in the next Trqbone our attacks we Army Long live Palestine, Hamas Qassam
Op #Electorinic , #OP IL , #OP FR , #OP US , #OP UK
Cyber war has been declared on Zionist cyber space and you will see exactly what we are capable of.
Our Target is your Government's Websites ... We Will Take You Off From The Internet !
Your Credit Cards , Your Bank's Accounts , Your Servers , Your Facebook , Twitters ... Are In Danger !
We Never Forget what You Do against the Humanity ... In GaZa Millions Of People Were Dead ... Palestinian's Muslims,Innocent Childrens, Womens Are Killed In The Force's Attacks...
Zionist Forces Destroyed Palestinian's Families , Homes ,schools, hospitals,mosks ... But No One Cares ! its the time to stop killing innocent peoples , and stop killing palestinians childs coz all da world know that zionist are the real terrorist.
Governement and Peopel of the thing named "Israel" will be a goal of Palestinian resistance rockets. To save your self your Family... You MUST forced your government to release every
prisoners on hunger strike... and to get out from Palestine Coz:
IN OUR MAPE IT WILL STAY PALASTINE FOR EVER , TILL WE DIE ..
Tell Your Governement Thats Anonymous Ghost Gaza Hardly Fucked Your Damn Fucking Server

WE ARE : Master Max | RxR | AnonymousFox | Mr.Rexor

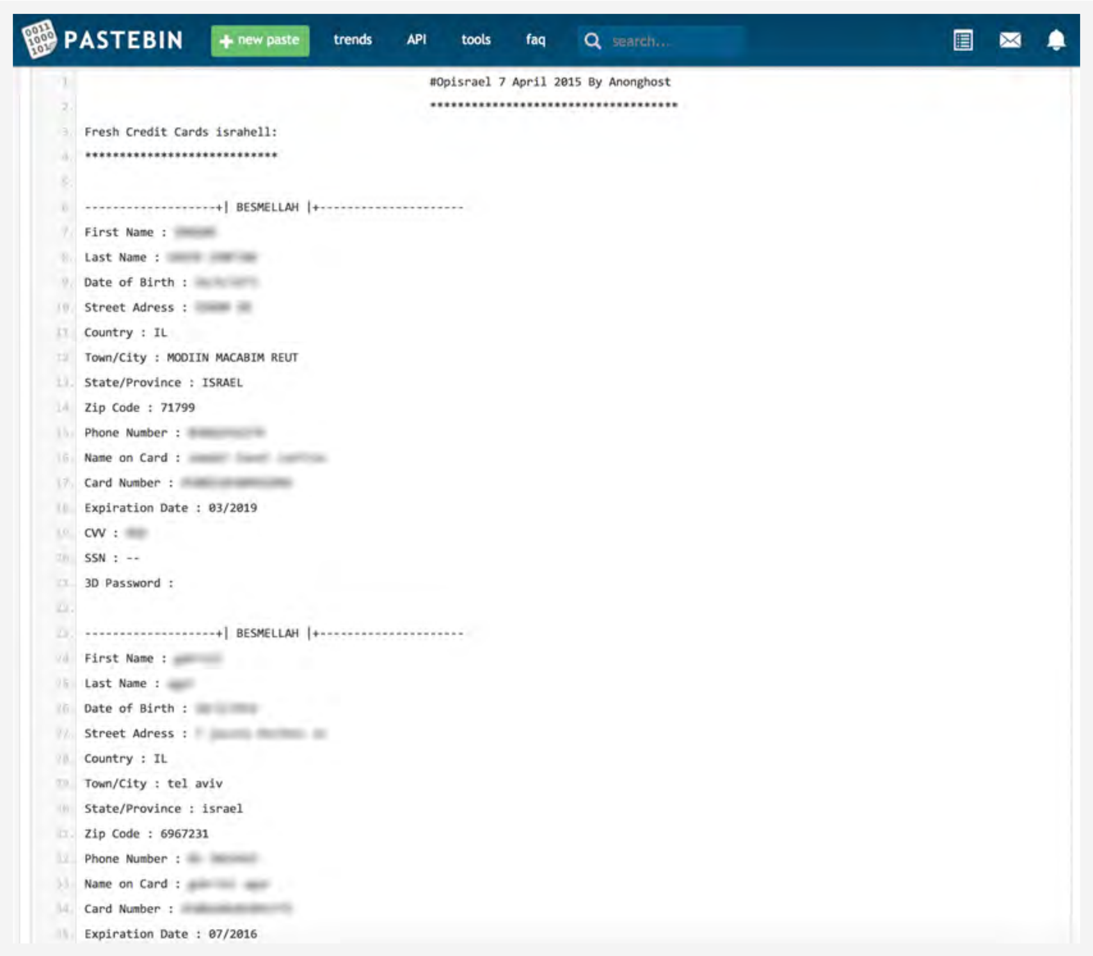
Figure 12. Forceful language in the defacement campaign #Save Gaza

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.



Anonymous Ghost Gaza
9 April at 12:16 ·

```
#OpIsrael
=========[Scam By Anonymous Ghost Gaza]=========
=================[LOGIN PayPal ]================
Email : [redacted]@014.net.il
Pass : [redacted]
====================[INFOS]==================
FName : [redacted]
LName : [redacted]
MName : zimber
Brithday : [redacted]
Line 1 : hakibutzim 38
Line 2 :
City : haifa
State :
Country : Israel
ZipCode : 2625419
Phone : [redacted]
====================[INFOS]==================
=====================[VBV]===================
Card Holder : [redacted]
Credit Card : [redacted]
Exp : 0118
CVV : [redacted]@014.net.il
```



```
                                          #Opisrael 7 April 2015 By Anonghost
                                          ************************************

Fresh Credit Cards israhell:
****************************

-------------------+| BESMELLAH |+---------------------
First Name : [redacted]
Last Name : [redacted]
Date of Birth : [redacted]
Street Adress : [redacted]
Country : IL
Town/City : MODIIN MACABIM REUT
State/Province : ISRAEL
Zip Code : 71799
Phone Number : [redacted]
Name on Card : [redacted]
Card Number : [redacted]
Expiration Date : 03/2019
CVV : [redacted]
SSN : --
3D Password :

-------------------+| BESMELLAH |+---------------------
First Name : [redacted]
Last Name : [redacted]
Date of Birth : [redacted]
Street Adress : [redacted]
Country : IL
Town/City : tel aviv
State/Province : israel
Zip Code : 6967231
Phone Number : [redacted]
Name on Card : [redacted]
Card Number : [redacted]
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.

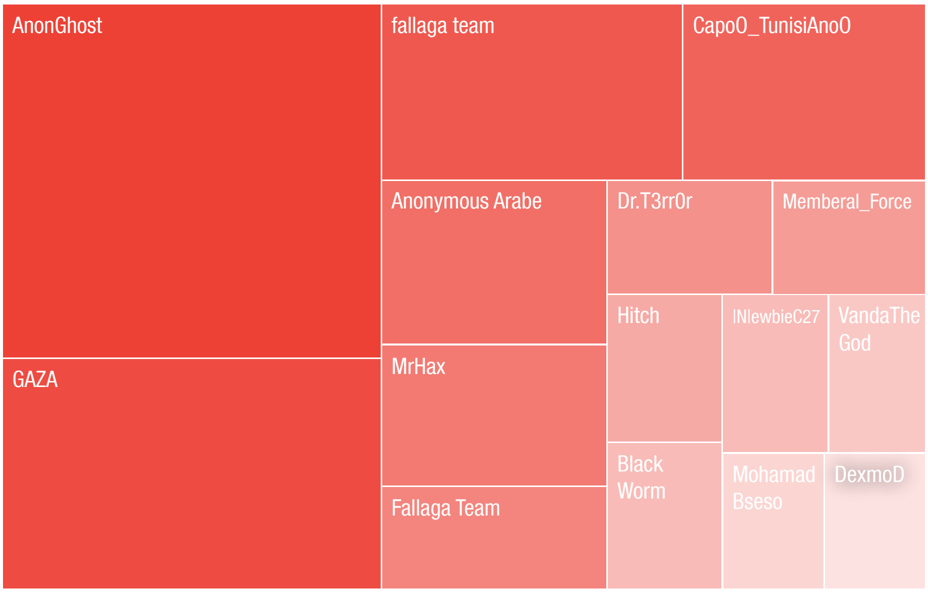


Figure 14. Top 15 participating hacking groups and hackers

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 injured[10]. In the aftermath, France was a target of other attacks, this time in cyberspace. The smaller campaigns under #OpFrance include #OpCharlie, #OPCHARLIEHEBDO, and #AntiCharlieHebdo.

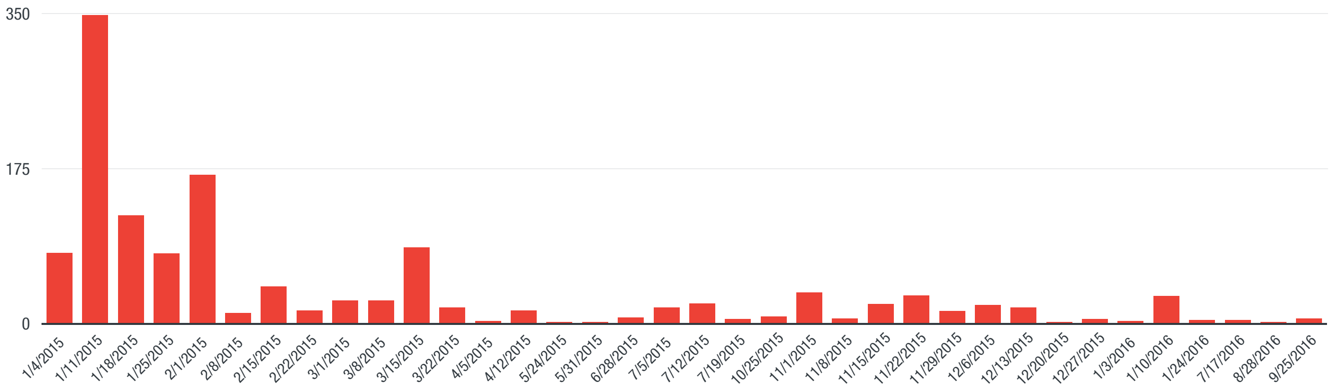


Figure 15. Timeline of #OpFrance—activity peaked January to March 2015, right after the Charlie Hebdo attacks

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.

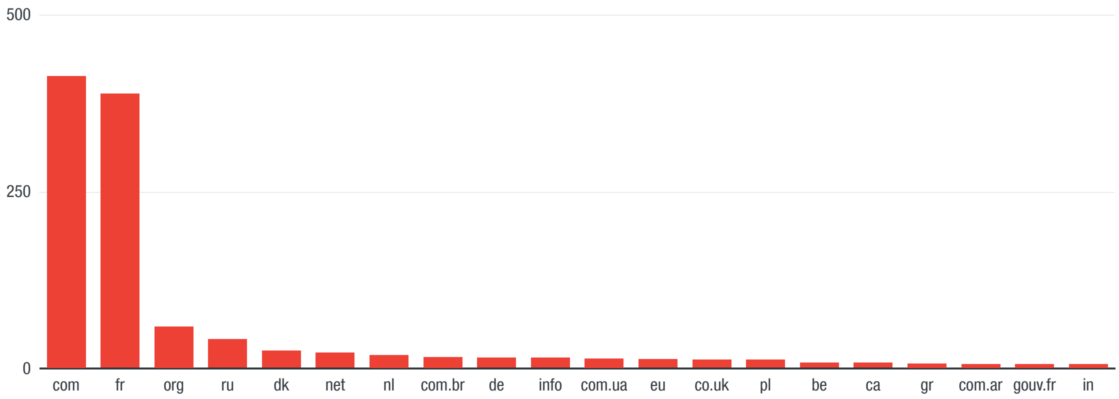
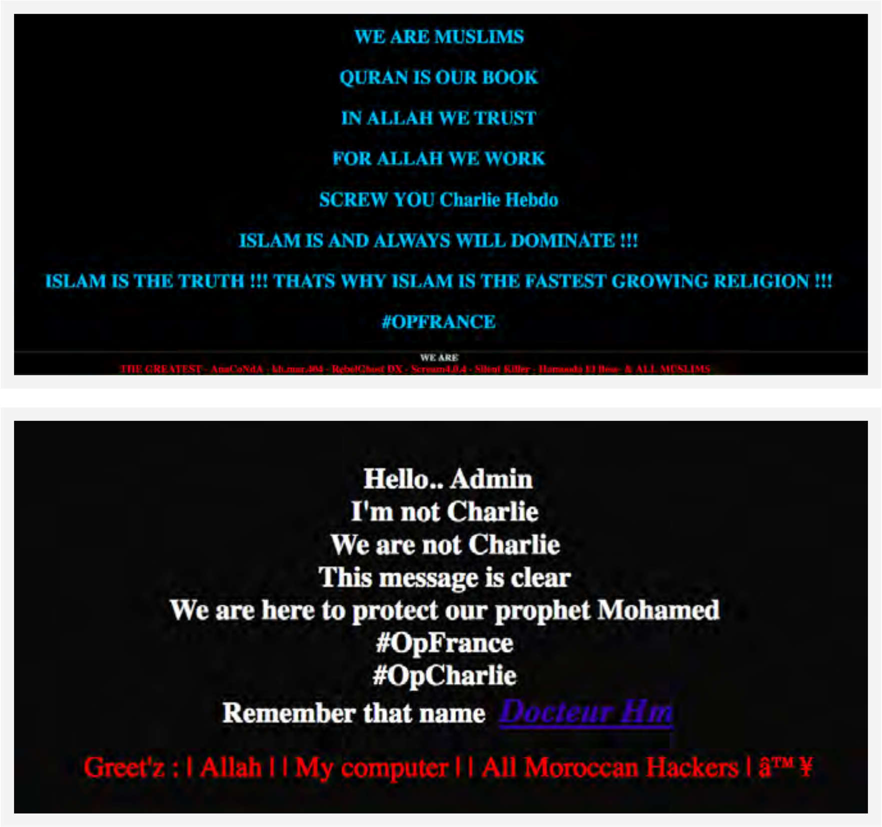


Figure 16. Target sites for #OpFrance

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.



WE ARE MUSLIMS

QURAN IS OUR BOOK

IN ALLAH WE TRUST

FOR ALLAH WE WORK

SCREW YOU Charlie Hebdo

ISLAM IS AND ALWAYS WILL DOMINATE !!!

ISLAM IS THE TRUTH !!! THATS WHY ISLAM IS THE FASTEST GROWING RELIGION !!!

#OPFRANCE

WE ARE

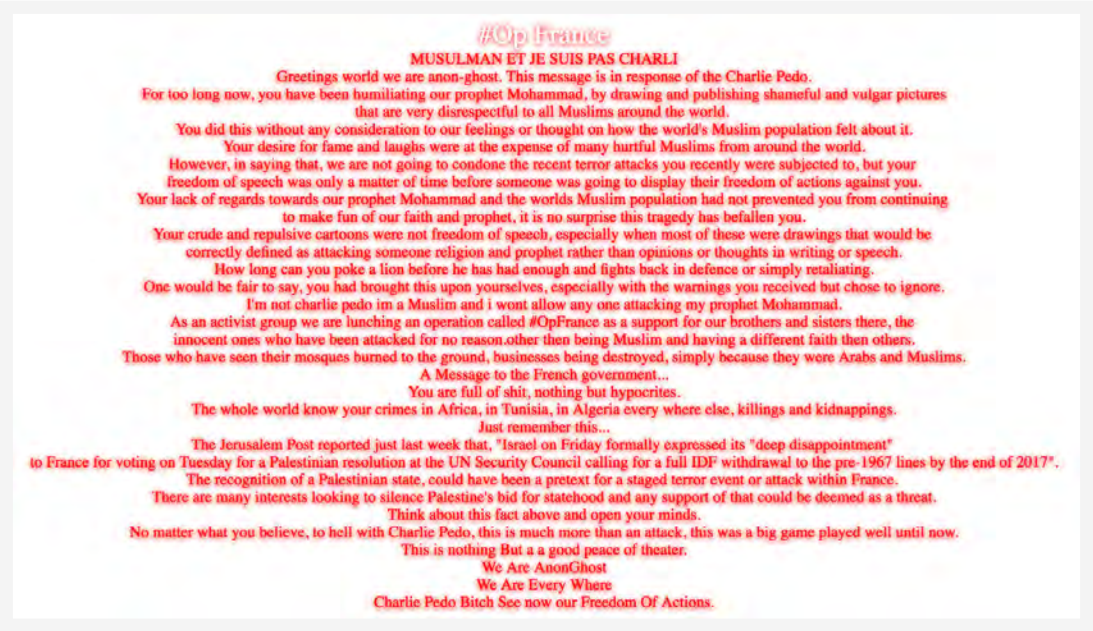
THE GREATEST - AnaCoNdA - kh.mar.404 - RebelGhost DX - Scream4.0.4 - Silent Killer - Hamouda El Bese- & ALL MUSLIMS

Hello.. Admin
I'm not Charlie
We are not Charlie
This message is clear
We are here to protect our prophet Mohamed
#OpFrance
#OpCharlie
Remember that name *Docteur Hm*

Greet'z : | Allah | | My computer | | All Moroccan Hackers | â™ ¥

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.'”



#Op France

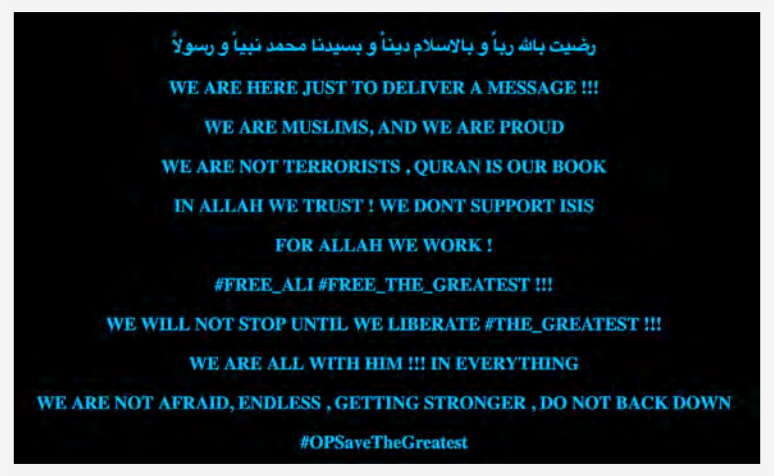
MUSULMAN ET JE SUIS PAS CHARLI

Greetings world we are anon-ghost. This message is in response of the Charlie Pedo.
For too long now, you have been humiliating our prophet Mohammad, by drawing and publishing shameful and vulgar pictures
that are very disrespectful to all Muslims around the world.
You did this without any consideration to our feelings or thought on how the world's Muslim population felt about it.
Your desire for fame and laughs were at the expense of many hurtful Muslims from around the world.
However, in saying that, we are not going to condone the recent terror attacks you recently were subjected to, but your
freedom of speech was only a matter of time before someone was going to display their freedom of actions against you.
Your lack of regards towards our prophet Mohammad and the worlds Muslim population had not prevented you from continuing
to make fun of our faith and prophet, it is no surprise this tragedy has befallen you.
Your crude and repulsive cartoons were not freedom of speech, especially when most of these were drawings that would be
correctly defined as attacking someone religion and prophet rather than opinions or thoughts in writing or speech.
How long can you poke a lion before he has had enough and fights back in defence or simply retaliating.
One would be fair to say, you had brought this upon yourselves, especially with the warnings you received but chose to ignore.
I'm not charlie pedo im a Muslim and i wont allow any one attacking my prophet Mohammad.
As an activist group we are lunching an operation called #OpFrance as a support for our brothers and sisters there, the
innocent ones who have been attacked for no reason.other then being Muslim and having a different faith then others.
Those who have seen their mosques burned to the ground, businesses being destroyed, simply because they were Arabs and Muslims.
A Message to the French government...
You are full of shit, nothing but hypocrites.
The whole world know your crimes in Africa, in Tunisia, in Algeria every where else, killings and kidnappings.
Just remember this...
The Jerusalem Post reported just last week that, "Israel on Friday formally expressed its "deep disappointment"
to France for voting on Tuesday for a Palestinian resolution at the UN Security Council calling for a full IDF withdrawal to the pre-1967 lines by the end of 2017".
The recognition of a Palestinian state, could have been a pretext for a staged terror event or attack within France.
There are many interests looking to silence Palestine's bid for statehood and any support of that could be deemed as a threat.
Think about this fact above and open your minds.
No matter what you believe, to hell with Charlie Pedo, this is much more than an attack, this was a big game played well until now.
This is nothing But a a good peace of theater.
We Are AnonGhost
We Are Every Where
Charlie Pedo Bitch See now our Freedom Of Actions.

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 group[11]. 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.



رضيت بالله رباً و بالاسلام ديناً و بسيدنا محمد نبياً و رسولاً

WE ARE HERE JUST TO DELIVER A MESSAGE !!!

WE ARE MUSLIMS, AND WE ARE PROUD

WE ARE NOT TERRORISTS , QURAN IS OUR BOOK

IN ALLAH WE TRUST ! WE DONT SUPPORT ISIS

FOR ALLAH WE WORK !

#FREE_ALI #FREE_THE_GREATEST !!!

WE WILL NOT STOP UNTIL WE LIBERATE #THE_GREATEST !!!

WE ARE ALL WITH HIM !!! IN EVERYTHING

WE ARE NOT AFRAID, ENDLESS , GETTING STRONGER , DO NOT BACK DOWN

#OPSaveTheGreatest

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.

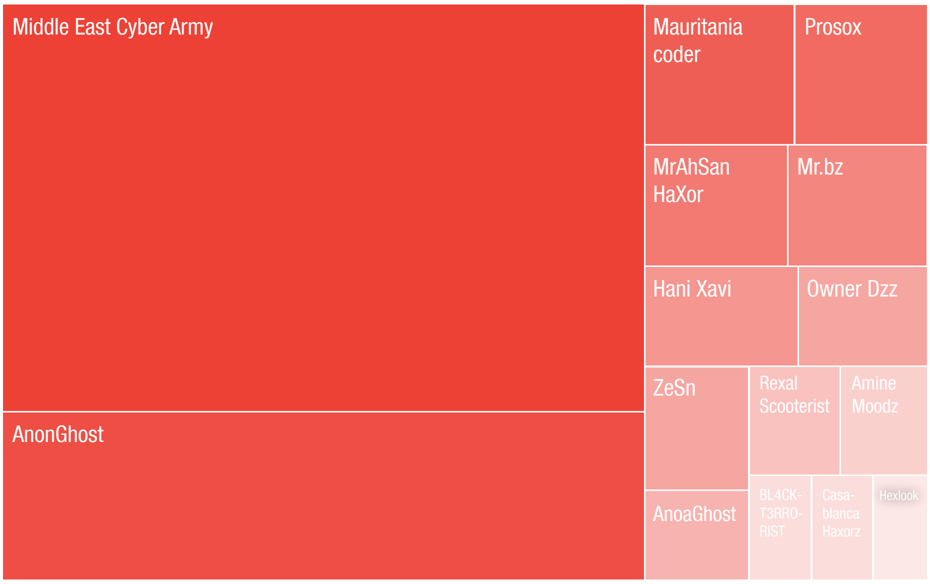


Figure 20. Top 15 participating hacking groups and hackers

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

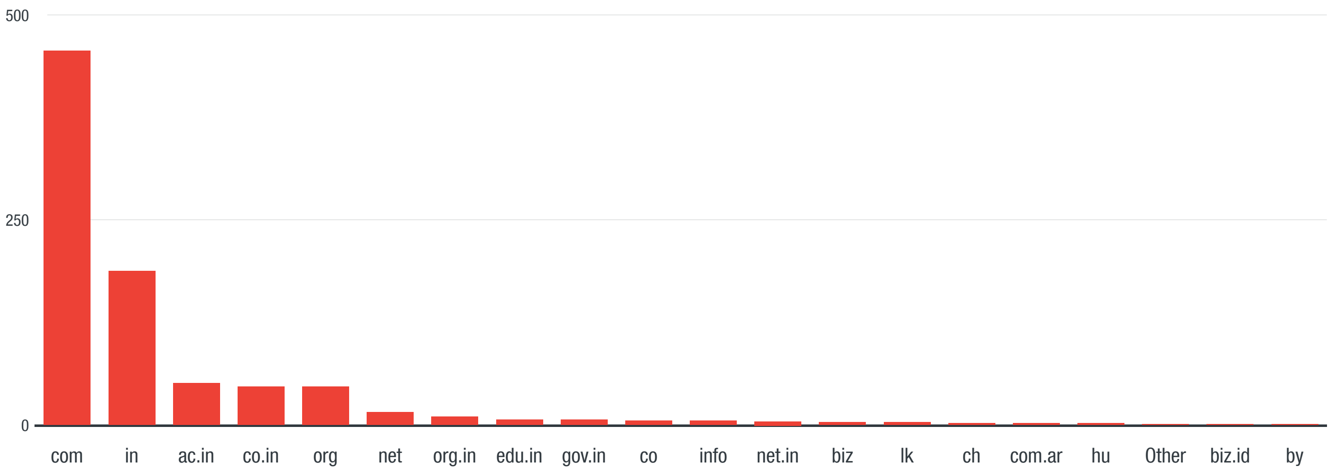


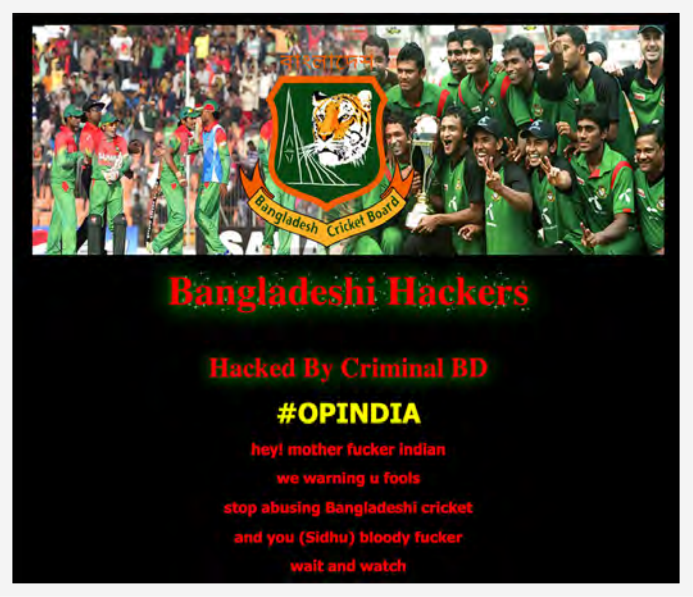
Figure 21. Target sites of #OpIndia

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.



Bangladeshi Hackers

Hacked By Criminal BD

#OPINDIA

hey! mother fucker indian

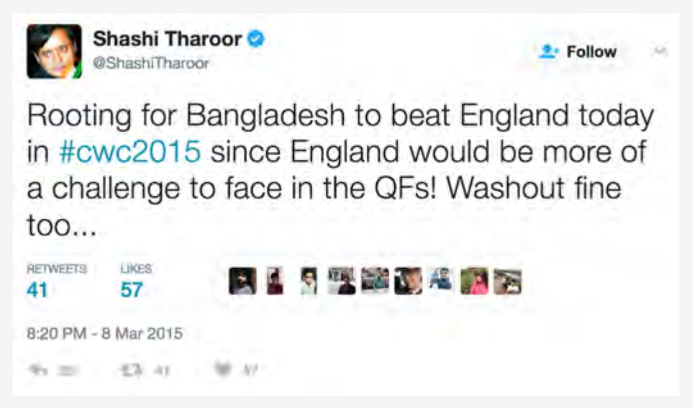
we warning u fools

stop abusing Bangladeshi cricket

and you (Sidhu) bloody fucker

wait and watch

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



Shashi Tharoor
@ShashiTharoor

Rooting for Bangladesh to beat England today in #cwc2015 since England would be more of a challenge to face in the QFs! Washout fine too...

RETWEETS 41
LIKES 57

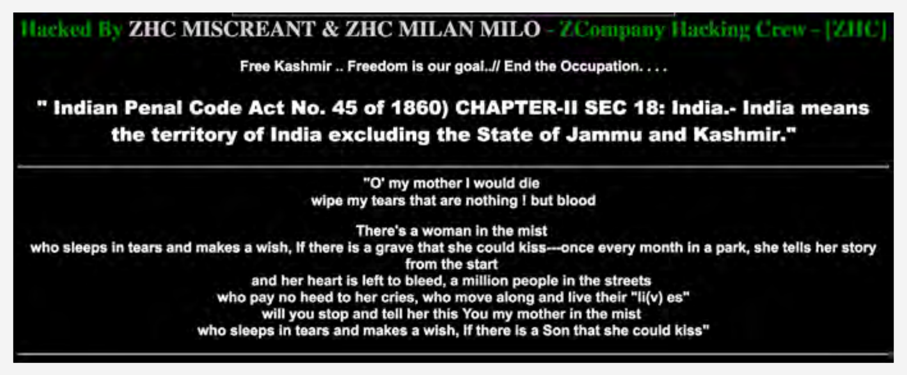
8:20 PM - 8 Mar 2015

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 Kashmiris[12]. 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 1947[13].



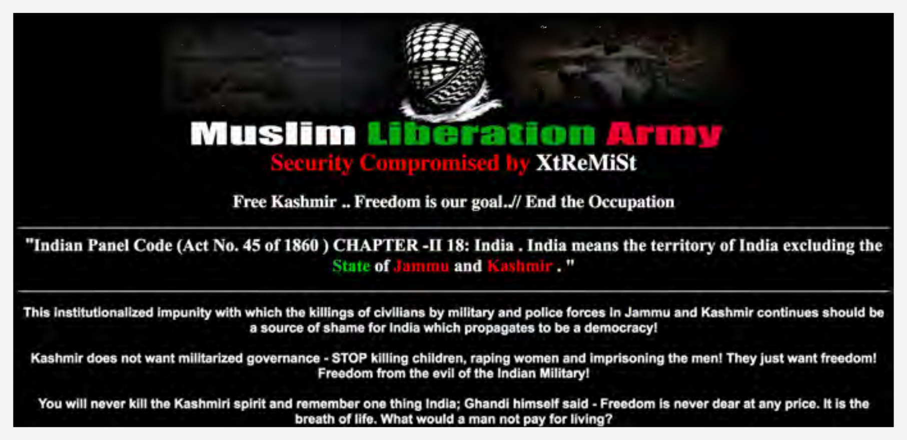
Hacked By ZHC MISCREANT & ZHC MILAN MILO - ZCompany Hacking Crew - [ZHC]

Free Kashmir .. Freedom is our goal..// End the Occupation. . . .

" Indian Penal Code Act No. 45 of 1860) CHAPTER-II SEC 18: India.- India means the territory of India excluding the State of Jammu and Kashmir."

"O' my mother I would die
wipe my tears that are nothing ! but blood

There's a woman in the mist
who sleeps in tears and makes a wish, If there is a grave that she could kiss---once every month in a park, she tells her story from the start
and her heart is left to bleed, a million people in the streets
who pay no heed to her cries, who move along and live their "li(v) es"
will you stop and tell her this You my mother in the mist
who sleeps in tears and makes a wish, If there is a Son that she could kiss"



Muslim Liberation Army
Security Compromised by XtReMiSt

Free Kashmir .. Freedom is our goal..// End the Occupation

"Indian Panel Code (Act No. 45 of 1860) CHAPTER -II 18: India . India means the territory of India excluding the State of Jammu and Kashmir . "

This institutionalized impunity with which the killings of civilians by military and police forces in Jammu and Kashmir continues should be a source of shame for India which propagates to be a democracy!

Kashmir does not want militarized governance - STOP killing children, raping women and imprisoning the men! They just want freedom! Freedom from the evil of the Indian Military!

You will never kill the Kashmiri spirit and remember one thing India; Ghandi himself said - Freedom is never dear at any price. It is the breath of life. What would a man not pay for living?

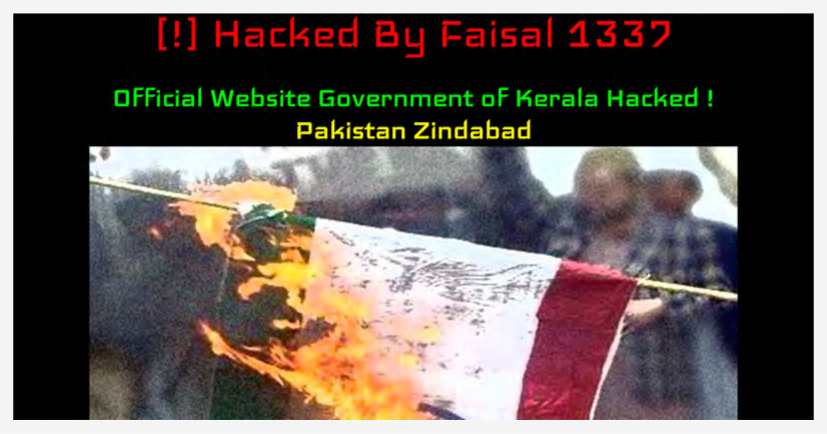
Figure 24. Free Kashmir campaign defacements

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 militants[14], 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.



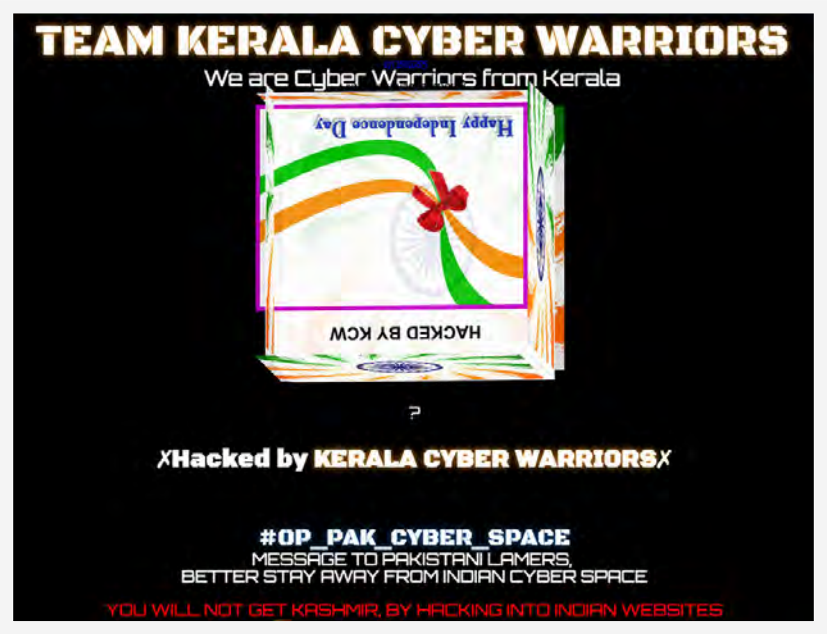
[!] Hacked By Faisal 1337

Official Website Government of Kerala Hacked !

Pakistan Zindabad

Figure 25. Indian local government websites hacked

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



TEAM KERALA CYBER WARRIORS

We are Cyber Warriors from Kerala

XHacked by KERALA CYBER WARRIORSX

#OP_PAK_CYBER_SPACE

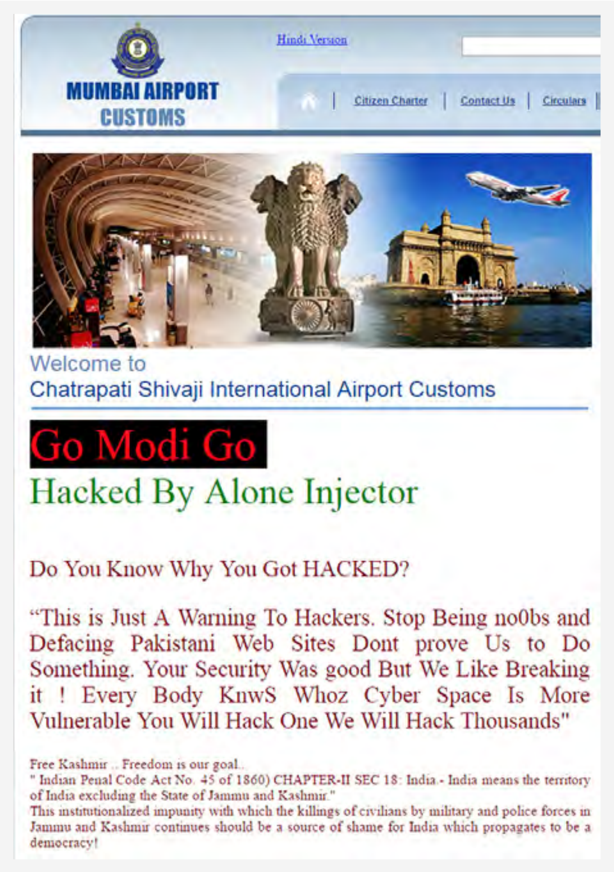
MESSAGE TO PAKISTANI LAMERS,

BETTER STAY AWAY FROM INDIAN CYBER SPACE

YOU WILL NOT GET KASHMIR, BY HACKING INTO INDIAN WEBSITES

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.



Welcome to
Chatrapati Shivaji International Airport Customs

Go Modi Go

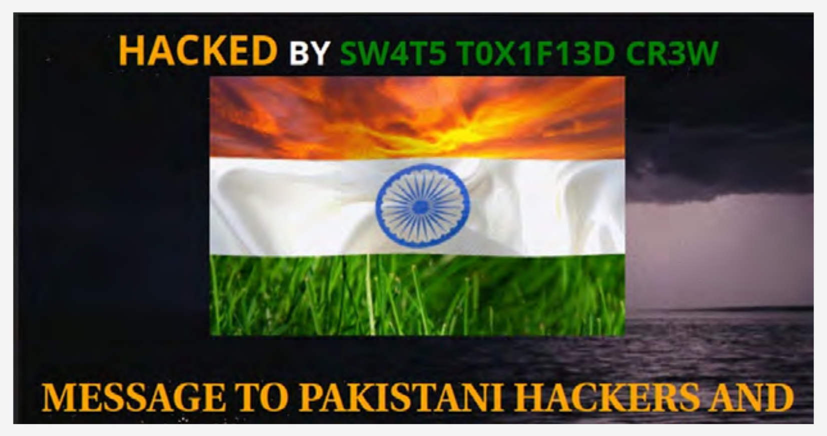
Hacked By Alone Injector

Do You Know Why You Got HACKED?

“This is Just A Warning To Hackers. Stop Being no0bs and Defacing Pakistani Web Sites Dont prove Us to Do Something. Your Security Was good But We Like Breaking it ! Every Body KnwS Whoz Cyber Space Is More Vulnerable You Will Hack One We Will Hack Thousands"

Free Kashmir .. Freedom is our goal..
" Indian Penal Code Act No. 45 of 1860) CHAPTER-II SEC 18: India.- India means the territory of India excluding the State of Jammu and Kashmir."
This institutionalized impunity with which the killings of civilians by military and police forces in Jammu and Kashmir continues should be a source of shame for India which propagates to be a democracy!

Figure 27. Mumbai Airport Customs defacement



HACKED BY SW4T5 T0X1F13D CR3W

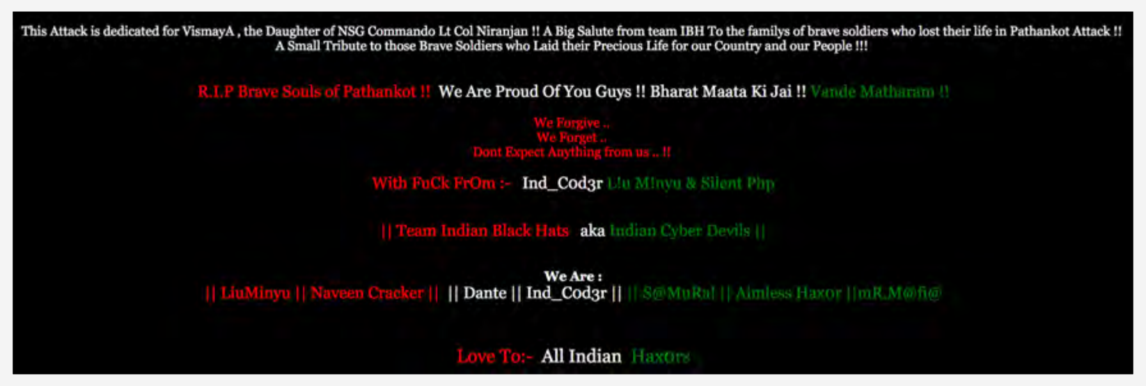
MESSAGE TO PAKISTANI HACKERS AND

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 Kashmir[15]. After the attack, Indian hacking groups retaliated by targeting Pakistani websites.



This Attack is dedicated for VismayA , the Daughter of NSG Commando Lt Col Niranjan !! A Big Salute from team IBH To the familys of brave soldiers who lost their life in Pathankot Attack !!
A Small Tribute to those Brave Soldiers who Laid their Precious Life for our Country and our People !!!

R.I.P Brave Souls of Pathankot !! We Are Proud Of You Guys !! Bharat Maata Ki Jai !! Vande Matharam !!

We Forgive ..
We Forget ..
Dont Expect Anything from us .. !!

With FuCk FrOm :- Ind_Cod3r L!u M!nyu & Silent Php

|| Team Indian Black Hats aka Indian Cyber Devils ||

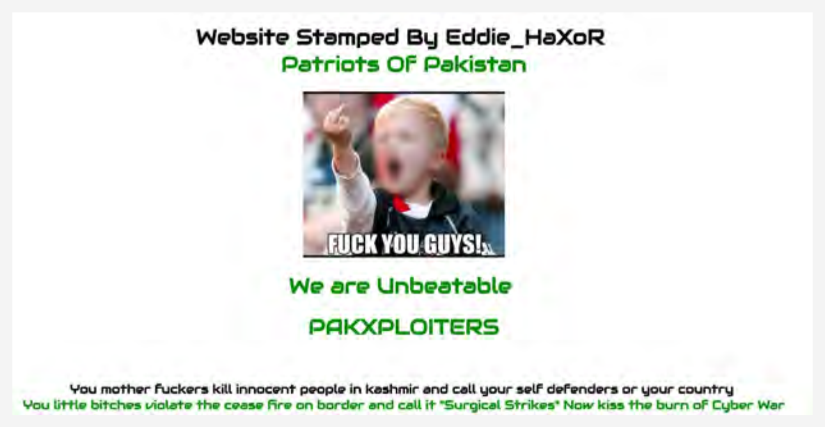
We Are :
|| LiuMinyu || Naveen Cracker || || Dante || Ind_Cod3r || || S@MuRa! || Aimless Haxor ||mR.M@fi@

Love To:- All Indian Haxors

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 attackers[16]. 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.

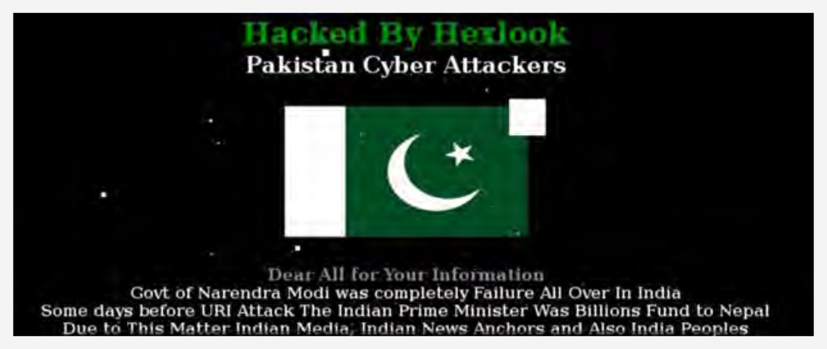


Website Stamped By Eddie_HaXoR
Patriots Of Pakistan

We are Unbeatable

PAKXPLOITERS

You mother fuckers kill innocent people in kashmir and call your self defenders or your country
You little bitches violate the cease fire on border and call it "Surgical Strikes" Now kiss the burn of Cyber War



Hacked By Hexlook

Pakistan Cyber Attackers

Dear All for Your Information

Govt of Narendra Modi was completely Failure All Over In India

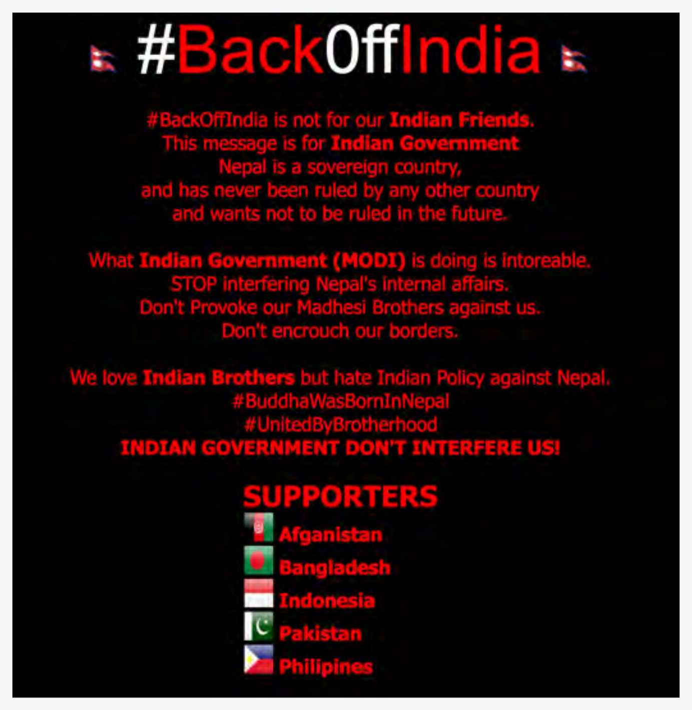
Some days before URI Attack The Indian Prime Minister Was Billions Fund to Nepal

Due to This Matter Indian Media, Indian News Anchors and Also India Peoples

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 constitution[17]. 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.



#BackOffIndia

#BackOffIndia is not for our **Indian Friends**.
This message is for **Indian Government**
Nepal is a sovereign country,
and has never been ruled by any other country
and wants not to be ruled in the future.

What **Indian Government (MODI)** is doing is intoreable.
STOP interfering Nepal's internal affairs.
Don't Provoke our Madhesi Brothers against us.
Don't encrouch our borders.

We love **Indian Brothers** but hate Indian Policy against Nepal.
#BuddhaWasBornInNepal
#UnitedByBrotherhood
INDIAN GOVERNMENT DON'T INTERFERE US!

SUPPORTERS

Afganistan
Bangladesh
Indonesia
Pakistan
Philipines

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.

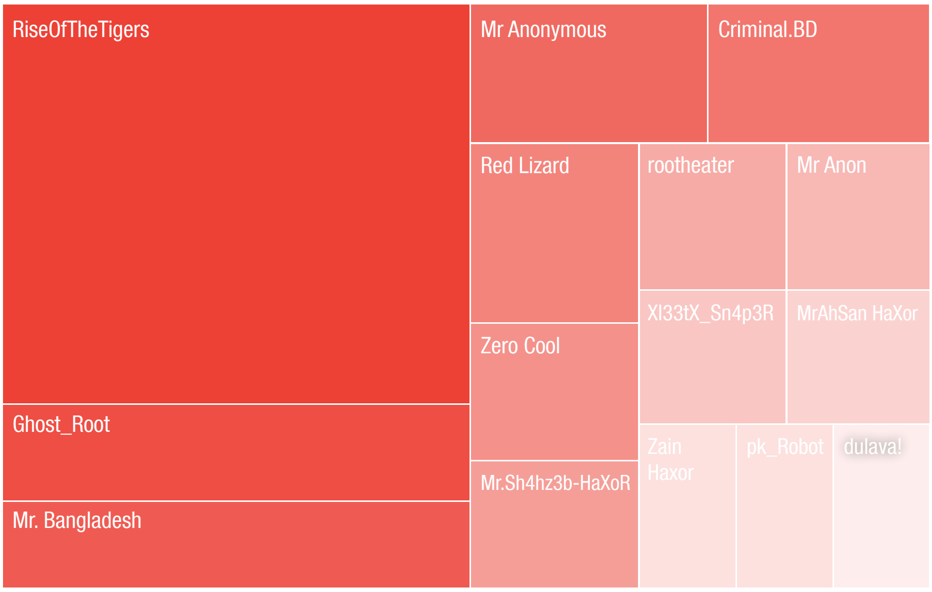


Figure 32. Top 15 participating hacking groups and hackers

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 people[18]. The incident inspired a #SaveSyria campaign that exposed graphic images of wounded civilians in Aleppo.

Target TLDs of #SaveSyria

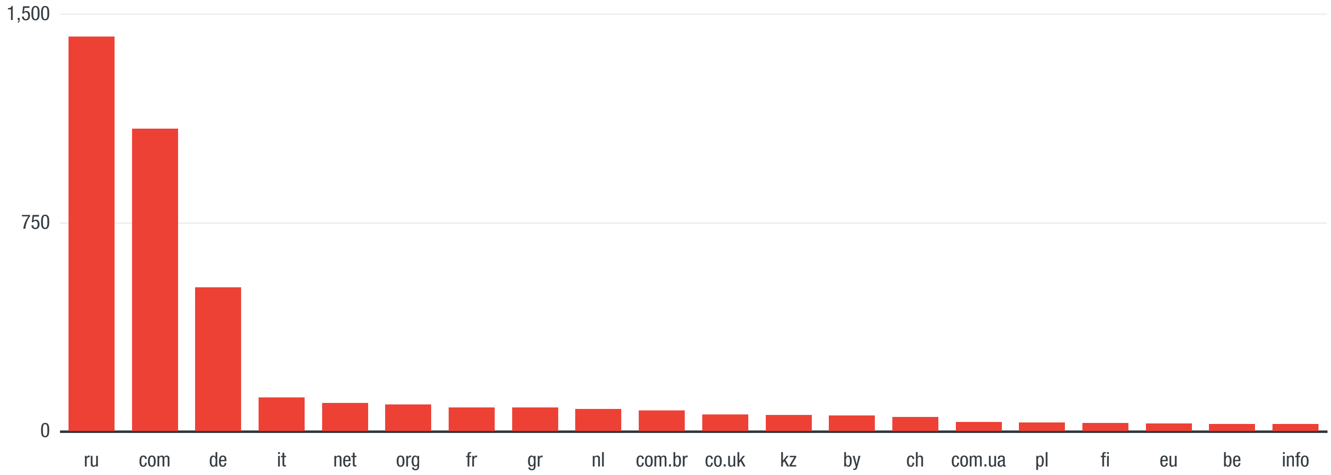
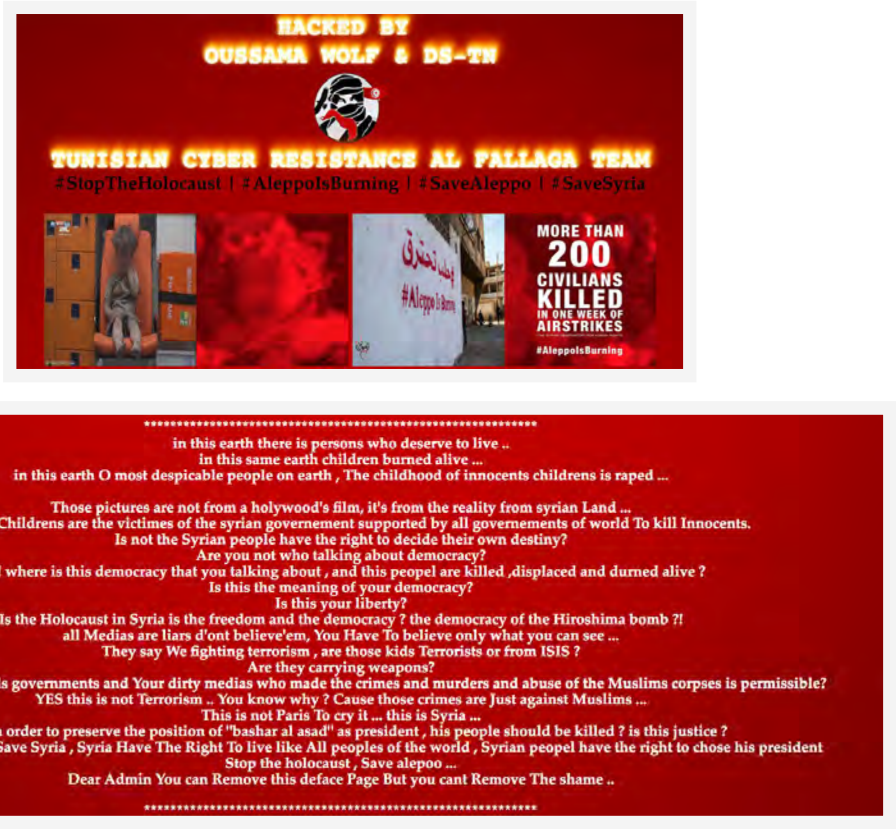


Figure 33. Targeted domains of #SaveSyria

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.



****
in this earth there is persons who deserve to live ..
in this same earth children burned alive ...
in this earth O most despicable people on earth , The childhood of innocents childrens is raped ...

Those pictures are not from a holywood's film, it's from the reality from syrian Land ...
yes those Childrens are the victimes of the syrian governement supported by all governements of world To kill Innocents.
Is not the Syrian people have the right to decide their own destiny?
Are you not who talking about democracy?
So ! where is this democracy that you talking about , and this peopel are killed ,displaced and durned alive ?
Is this the meaning of your democracy?
Is this your liberty?
Is the Holocaust in Syria is the freedom and the democracy ? the democracy of the Hiroshima bomb ?!
all Medias are liars d'ont believe'em, You Have To believe only what you can see ...
They say We fighting terrorism , are those kids Terrorists or from ISIS ?
Are they carrying weapons?
Or is it your Criminals governments and Your dirty medias who made the crimes and murders and abuse of the Muslims corpses is permissible?
YES this is not Terrorism .. You know why ? Cause those crimes are Just against Muslims ...
This is not Paris To cry it ... this is Syria ...
why In order to preserve the position of "bashar al asad" as president , his people should be killed ? is this justice ?
To Day We Have To Save Syria , Syria Have The Right To live like All peoples of the world , Syrian peopel have the right to chose his president
Stop the holocaust , Save alepoo ...
Dear Admin You can Remove this deface Page But you cant Remove The shame ..
****

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, #AleppoIsBurning, #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 control[19].

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.

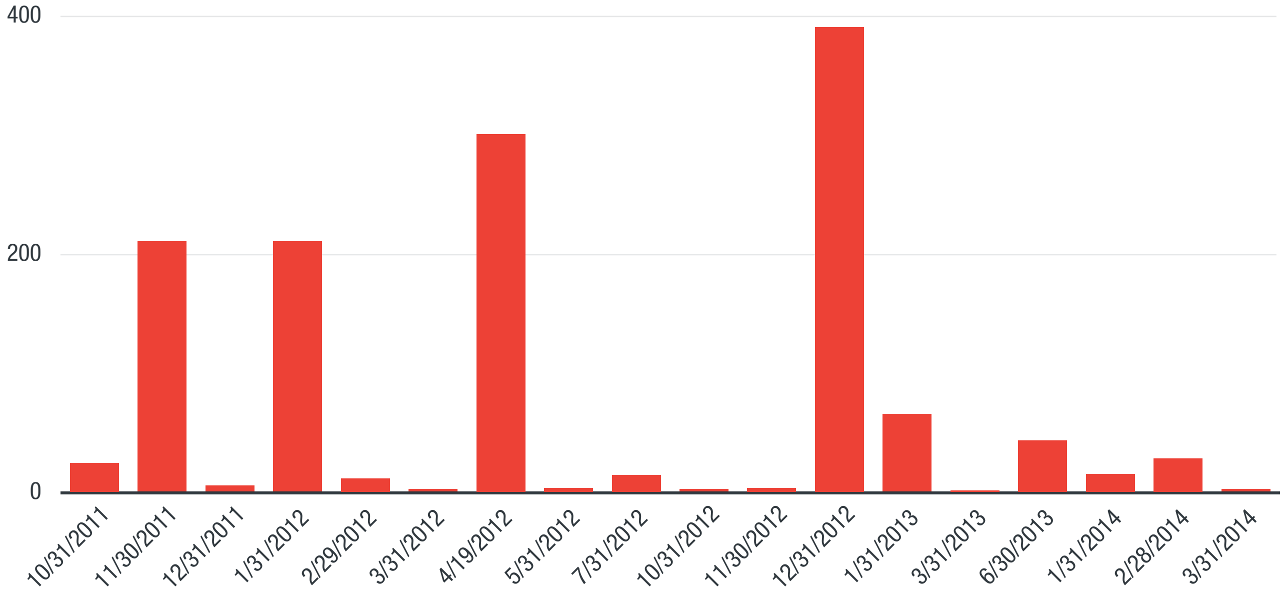
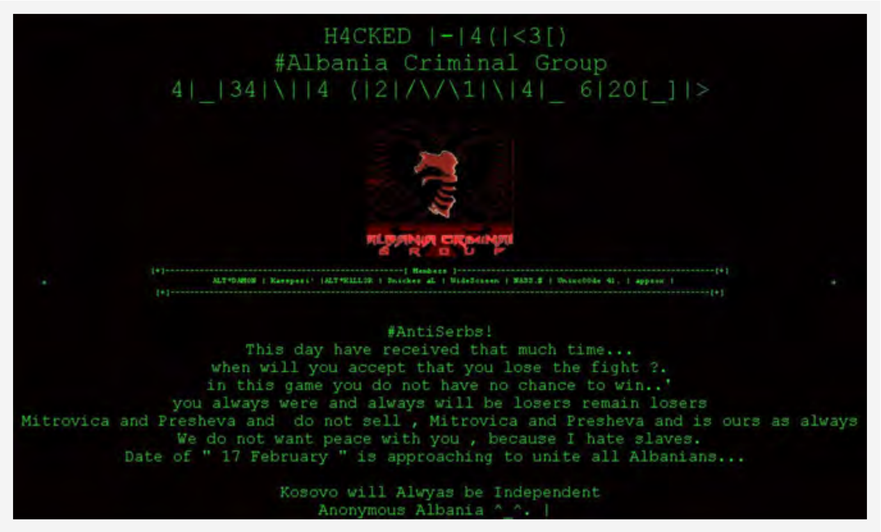


Figure 35. Timeline of anti-Serbs campaign

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.

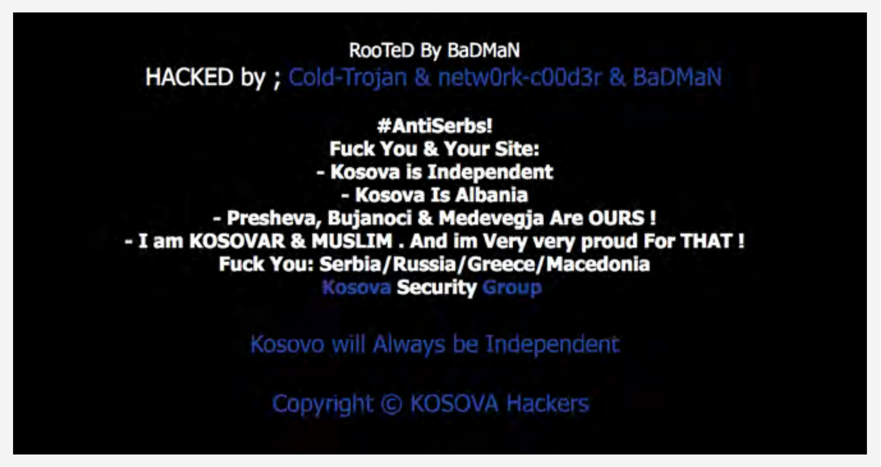


H4CKED |-|4(|<3[)
#Albania Criminal Group
4|_|34|\||4 (|2|/\/\1|\|4|_ 6|20[_]|>

[+]--[Members]--[+]
ALT*DAMON | Kaeepesi' |ALT*KILLER | Snicker aL | WideScreen | MASS.E | Unicc0de 4L. | appzo |
[+]--[+]

#AntiSerbs!
This day have received that much time...
when will you accept that you lose the fight ?.
in this game you do not have no chance to win..'
you always were and always will be losers remain losers
Mitrovica and Presheva and do not sell , Mitrovica and Presheva and is ours as always
We do not want peace with you , because I hate slaves.
Date of " 17 February " is approaching to unite all Albanians...

Kosovo will Alwyas be Independent
Anonymous Albania ^_^. |



RooTeD By BaDMaN
HACKED by ; Cold-Trojan & netw0rk-c00d3r & BaDMaN

#AntiSerbs!
Fuck You & Your Site:
- Kosova is Independent
- Kosova Is Albania
- Presheva, Bujanoci & Medevegja Are OURS !
- I am KOSOVAR & MUSLIM . And im Very very proud For THAT !
Fuck You: Serbia/Russia/Greece/Macedonia
Kosova Security Group

Kosovo will Always be Independent

Copyright © KOSOVA Hackers

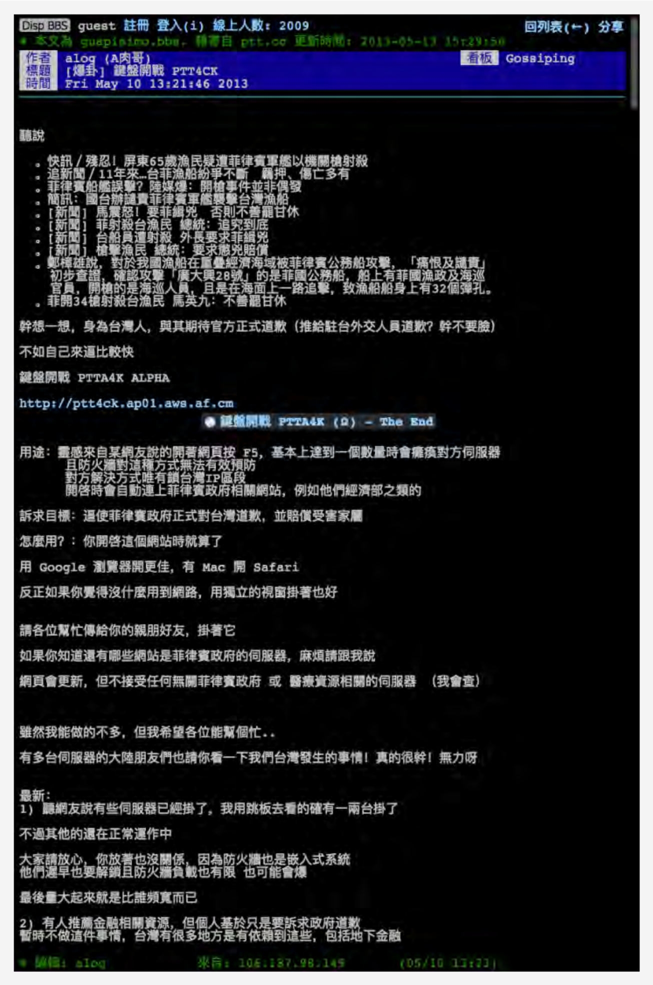
Figure 36. Web defacement pages supporting Kosovo

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 sites[21].



```
Disp BBS guest 註冊 登入(i) 線上人數: 2009                    回列表(←) 分享
※ 本文為 guapisimo.bbs. 轉寄自 ptt.cc 更新時間: 2013-05-13 15:29:50
作者 alog (A肉哥)                                    看板 Gossiping
標題 [爆卦] 鍵盤開戰 PTT4CK
時間 Fri May 10 13:21:46 2013

聽說

  。快訊 / 殘忍! 屏東65歲漁民疑遭菲律賓軍艦以機關槍射殺
  。追新聞 / 11年來…台菲漁船紛爭不斷  羈押、傷亡多有
  。菲律賓船艦誤擊? 陸媒爆: 開槍事件並非偶發
  。簡訊: 國台辦譴責菲律賓軍艦襲擊台灣漁船
  。[新聞] 馬震怒! 要菲緝兇  否則不善罷甘休
  。[新聞] 菲射殺台漁民 總統: 追究到底
  。[新聞] 台船員遭射殺 外長要求菲緝兇
  。[新聞] 槍擊漁民 總統: 要求懲兇賠償
  。鄭樟雄說, 對於我國漁船在重疊經濟海域被菲律賓公務船攻擊, 「痛恨及譴責」
    初步查證, 確認攻擊「廣大興28號」的是菲國公務船, 船上有菲國漁政及海巡
    官員, 開槍的是海巡人員, 且是在海面上一路追擊, 致漁船船身上有32個彈孔。
  。菲開34槍射殺台漁民 馬英九: 不善罷甘休

幹想一想, 身為台灣人, 與其期待官方正式道歉 (推給駐台外交人員道歉? 幹不要臉)

不如自己來這比較快

鍵盤開戰 PTTA4K ALPHA

http://ptt4ck.ap01.aws.af.cm
                          ● 鍵盤開戰 PTTA4K (Ω) - The End

用途: 靈感來自某網友說的開著網頁按 F5, 基本上達到一個數量時會癱瘓對方伺服器
      且防火牆對這種方式無法有效預防
      對方解決方式唯有鎖台灣IP區段
      開啓時會自動連上菲律賓政府相關網站, 例如他們經濟部之類的

訴求目標: 逼使菲律賓政府正式對台灣道歉, 並賠償受害家屬

怎麼用? : 你開啓這個網站時就算了

用 Google 瀏覽器開更佳, 有 Mac 開 Safari

反正如果你覺得沒什麼用到網路, 用獨立的視窗掛著也好


請各位幫忙傳給你的親朋好友, 掛著它

如果你知道還有哪些網站是菲律賓政府的伺服器, 麻煩請跟我說

網頁會更新, 但不接受任何無關菲律賓政府 或 醫療資源相關的伺服器  (我會查)


雖然我能做的不多, 但我希望各位能幫個忙..

有多台伺服器的大陸朋友們也請你看一下我們台灣發生的事情! 真的很幹! 無力呀

最新:
1) 聽網友說有些伺服器已經掛了, 我用跳板去看的確有一兩台掛了

不過其他的還在正常運作中

大家請放心, 你放著也沒關係, 因為防火牆也是嵌入式系統
他們遲早也要解鎖且防火牆負載也有限  也可能會爆

最後量大起來就是比誰頻寬而已

2) 有人推薦金融相關資源, 但個人基於只是要訴求政府道歉
暫時不做這件事情, 台灣有很多地方是有依賴到這些, 包括地下金融
※ 編輯: alog           來自: 106.187.98.145        (05/10 13:23)
```

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.

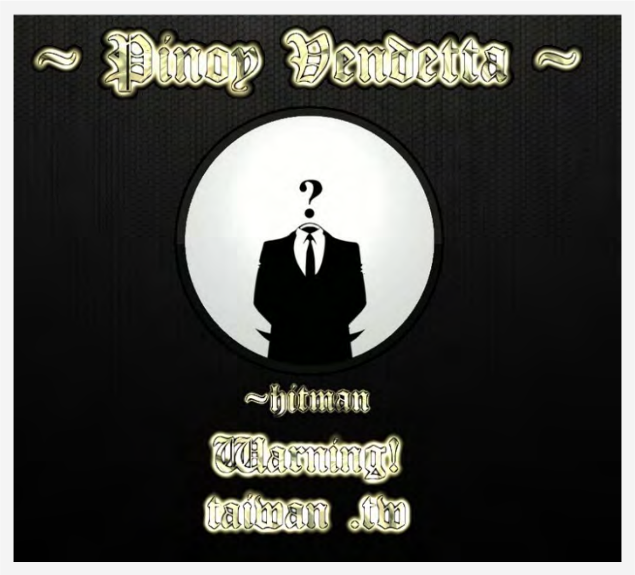
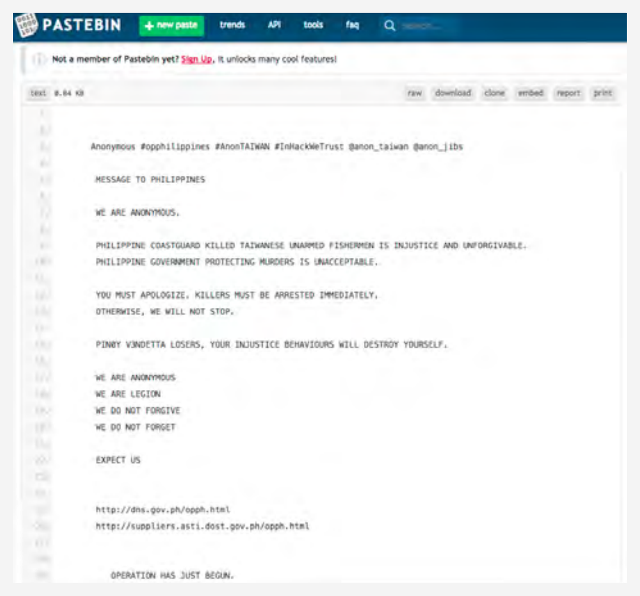
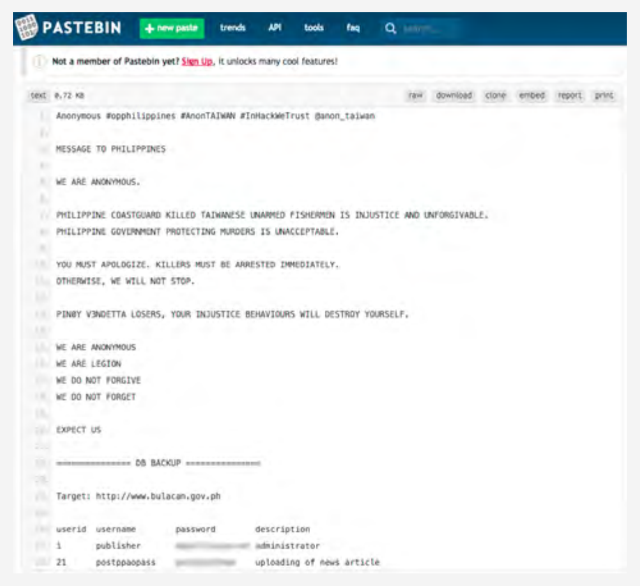


Figure 38. Web defacement page from "PinoyVendetta"

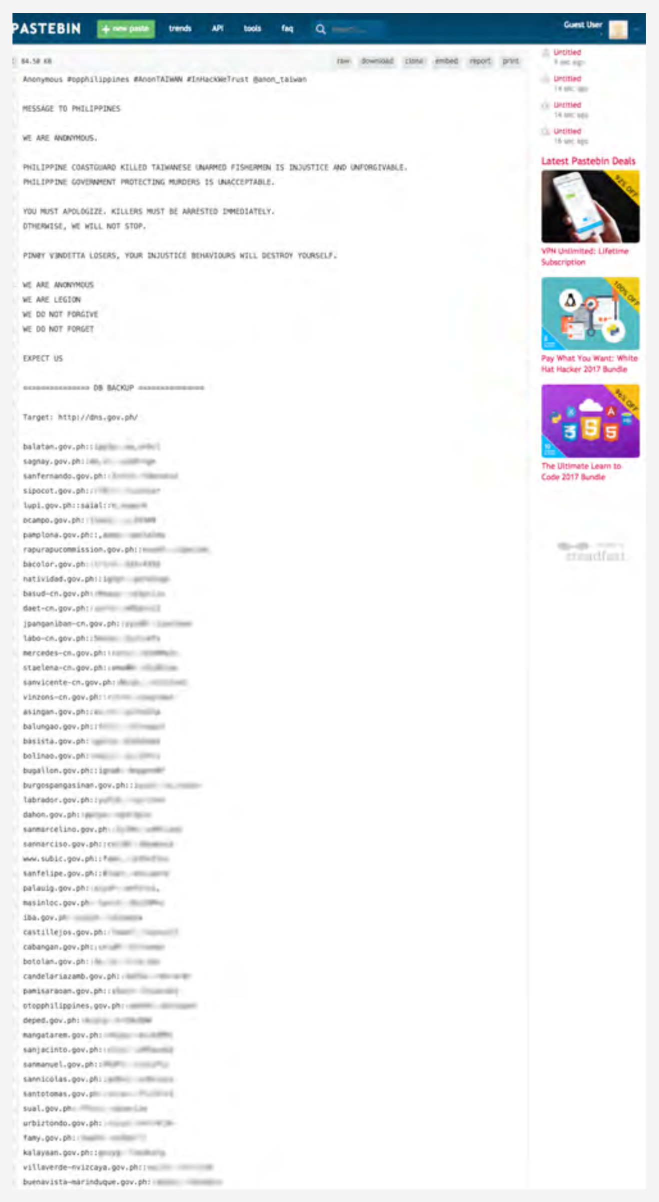
After the attack, AnonTaiwan posted leaked data from .gov.ph sites on Pastebin. One noteworthy victim was dns.gov.ph, which is the .gov.ph domain registry website. More than 2,300 accounts, which were possible admin accounts for .gov.ph domains, were leaked. These government sites faced a huge risk. 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.



```
Anonymous #opphilippines #AnonTAIWAN #InHackWeTrust @anon_taiwan @anon_jibs

 MESSAGE TO PHILIPPINES

 WE ARE ANONYMOUS.

 PHILIPPINE COASTGUARD KILLED TAIWANESE UNARMED FISHERMEN IS INJUSTICE AND UNFORGIVABLE.
 PHILIPPINE GOVERNMENT PROTECTING MURDERS IS UNACCEPTABLE.

 YOU MUST APOLOGIZE. KILLERS MUST BE ARRESTED IMMEDIATELY.
 OTHERWISE, WE WILL NOT STOP.

 PIN0Y V3NDETTA LOSERS, YOUR INJUSTICE BEHAVIOURS WILL DESTROY YOURSELF.

 WE ARE ANONYMOUS
 WE ARE LEGION
 WE DO NOT FORGIVE
 WE DO NOT FORGET

 EXPECT US


 http://dns.gov.ph/opph.html
 http://suppliers.asti.dost.gov.ph/opph.html


    OPERATION HAS JUST BEGUN.
```



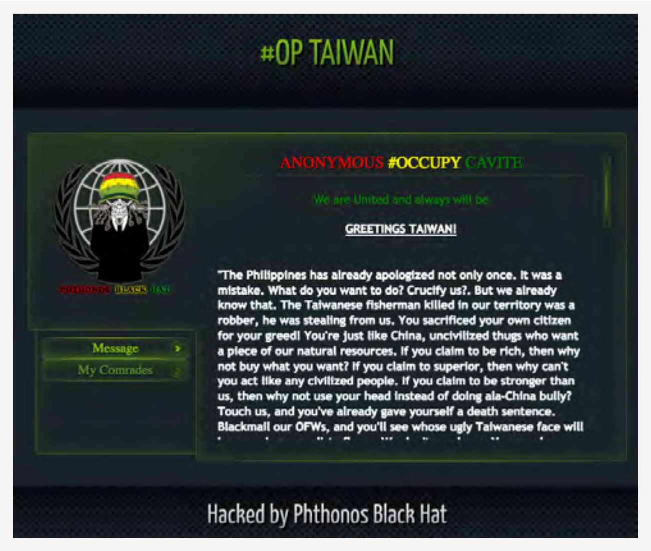
```
Anonymous #opphilippines #AnonTAIWAN #InHackWeTrust @anon_taiwan

MESSAGE TO PHILIPPINES

WE ARE ANONYMOUS.

PHILIPPINE COASTGUARD KILLED TAIWANESE UNARMED FISHERMEN IS INJUSTICE AND UNFORGIVABLE.
PHILIPPINE GOVERNMENT PROTECTING MURDERS IS UNACCEPTABLE.

YOU MUST APOLOGIZE. KILLERS MUST BE ARRESTED IMMEDIATELY.
OTHERWISE, WE WILL NOT STOP.

PIN0Y V3NDETTA LOSERS, YOUR INJUSTICE BEHAVIOURS WILL DESTROY YOURSELF.

WE ARE ANONYMOUS
WE ARE LEGION
WE DO NOT FORGIVE
WE DO NOT FORGET

EXPECT US

=============== DB BACKUP ===============

Target: http://www.bulacan.gov.ph

userid  username      password      description
1       publisher     [redacted]    administrator
21      postppaopass  [redacted]    uploading of news article
```



```
Anonymous #opphilippines #AnonTAIWAN #InHackWeTrust @anon_taiwan

MESSAGE TO PHILIPPINES

WE ARE ANONYMOUS.

PHILIPPINE COASTGUARD KILLED TAIWANESE UNARMED FISHERMEN IS INJUSTICE AND UNFORGIVABLE.
PHILIPPINE GOVERNMENT PROTECTING MURDERS IS UNACCEPTABLE.

YOU MUST APOLOGIZE. KILLERS MUST BE ARRESTED IMMEDIATELY.
OTHERWISE, WE WILL NOT STOP.

PIN0Y V3NDETTA LOSERS, YOUR INJUSTICE BEHAVIOURS WILL DESTROY YOURSELF.

WE ARE ANONYMOUS
WE ARE LEGION
WE DO NOT FORGIVE
WE DO NOT FORGET

EXPECT US

============== DB BACKUP ==============

Target: http://dns.gov.ph/

balatan.gov.ph::[redacted]
sagnay.gov.ph::[redacted]
sanfernando.gov.ph::[redacted]
sipocot.gov.ph::[redacted]
lupi.gov.ph::saial::[redacted]
ocampo.gov.ph::[redacted]
pamplona.gov.ph::[redacted]
rapurapucommission.gov.ph::[redacted]
bacolor.gov.ph::[redacted]
natividad.gov.ph::[redacted]
basud-cn.gov.ph::[redacted]
daet-cn.gov.ph::[redacted]
jpanganiban-cn.gov.ph::[redacted]
labo-cn.gov.ph::[redacted]
mercedes-cn.gov.ph::[redacted]
staelena-cn.gov.ph::[redacted]
sanvicente-cn.gov.ph::[redacted]
vinzons-cn.gov.ph::[redacted]
asingan.gov.ph::[redacted]
balungao.gov.ph::[redacted]
basista.gov.ph::[redacted]
bolinao.gov.ph::[redacted]
bugallon.gov.ph::[redacted]
burgospangasinan.gov.ph::[redacted]
labrador.gov.ph::[redacted]
dahon.gov.ph::[redacted]
sanmarcelino.gov.ph::[redacted]
sannarciso.gov.ph::[redacted]
www.subic.gov.ph::[redacted]
sanfelipe.gov.ph::[redacted]
palauig.gov.ph::[redacted]
masinloc.gov.ph[redacted]
iba.gov.ph[redacted]
castillejos.gov.ph::[redacted]
cabangan.gov.ph::[redacted]
botolan.gov.ph::[redacted]
candelariazamb.gov.ph::[redacted]
pamisaraoan.gov.ph::[redacted]
otopphilippines.gov.ph::[redacted]
deped.gov.ph::[redacted]
mangatarem.gov.ph::[redacted]
sanjacinto.gov.ph::[redacted]
sanmanuel.gov.ph::[redacted]
sannicolas.gov.ph::[redacted]
santotomas.gov.ph[redacted]
sual.gov.ph[redacted]
urbiztondo.gov.ph::[redacted]
famy.gov.ph::[redacted]
kalayaan.gov.ph::[redacted]
villaverde-nvizcaya.gov.ph::[redacted]
buenavista-marinduque.gov.ph::[redacted]
```

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."



#OP TAIWAN

ANONYMOUS #OCCUPY CAVITE

We are United and always will be

GREETINGS TAIWAN!

"The Philippines has already apologized not only once. It was a mistake. What do you want to do? Crucify us?. But we already know that. The Taiwanese fisherman killed in our territory was a robber, he was stealing from us. You sacrificed your own citizen for your greed! You're just like China, uncivilized thugs who want a piece of our natural resources. If you claim to be rich, then why not buy what you want? If you claim to superior, then why can't you act like any civilized people. If you claim to be stronger than us, then why not use your head instead of doing ala-China bully? Touch us, and you've already gave yourself a death sentence. Blackmail our OFWs, and you'll see whose ugly Taiwanese face will

Hacked by Phthonos Black Hat

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.

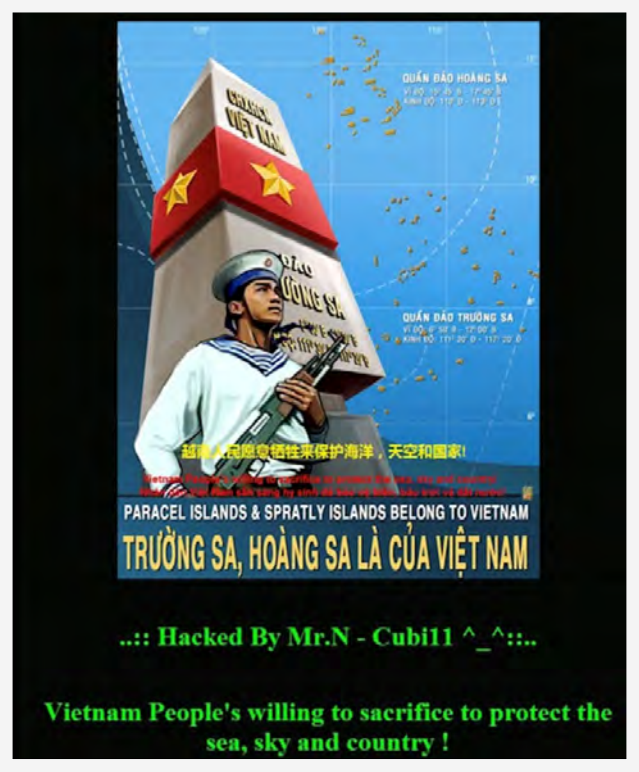
Over the last few years, the tension between China and Vietnam, and China and Philippines has increased. China has taken aggressive action, from coast guard patrols to building facilities and installations in various contested areas. This has sparked defacement activities by several groups from Philippines, 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 Sea[23]. 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 after[24].

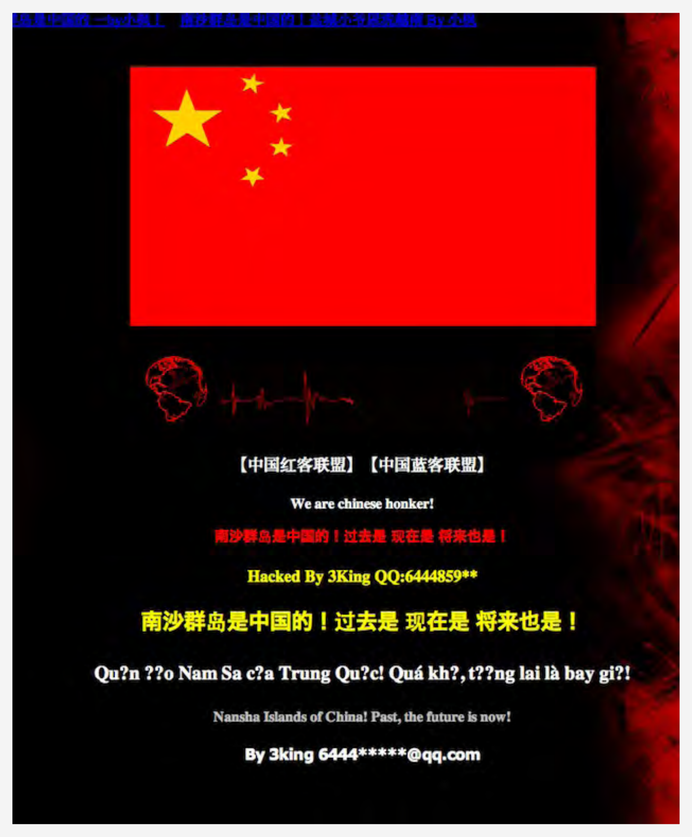

QUẦN ĐẢO HOÀNG SA
QUẦN ĐẢO TRƯỜNG SA
越南人民愿意牺牲来保护海洋，天空和国家!
PARACEL ISLANDS & SPRATLY ISLANDS BELONG TO VIETNAM
TRƯỜNG SA, HOÀNG SA LÀ CỦA VIỆT NAM

..:: Hacked By Mr.N - Cubi11 ^_^::..

Vietnam People's willing to sacrifice to protect the sea, sky and country !

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.



[illegible]

【中国红客联盟】【中国蓝客联盟】

We are chinese honker!

南沙群岛是中国的！过去是 现在是 将来也是！

Hacked By 3King QQ:6444859**

南沙群岛是中国的！过去是 现在是 将来也是！

Qu?n ??o Nam Sa c?a Trung Qu?c! Quá kh?, t??ng lai là bay gi?!

Nansha Islands of China! Past, the future is now!

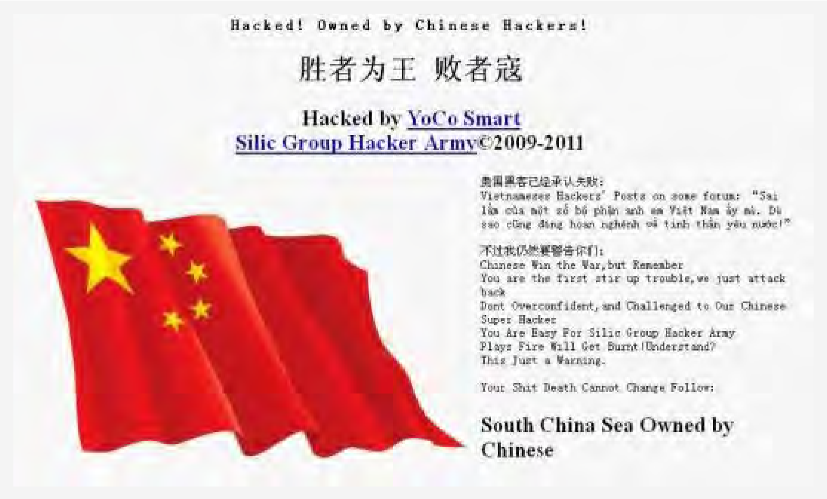
By 3king 6444*****@qq.com

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 attacks[25].

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 sites[26].



Hacked! Owned by Chinese Hackers!

胜者为王 败者寇

Hacked by YoCo Smart
Silic Group Hacker Army©2009-2011

越南黑客已经承认失败：
Vietnameses Hackers' Posts on some forum: "Sai lầm của một số bộ phận anh em Việt Nam ấy mà. Dù sao cũng đáng hoan nghênh vì tinh thần yêu nước!"

不过我仍然要警告你们：
Chinese Win the War,but Remember
You are the first stir up trouble,we just attack back
Dont Overconfident,and Challenged to Our Chinese Super Hacker
You Are Easy For Silic Group Hacker Army
Plays Fire Will Get Burnt!Understand?
This Just a Warning.

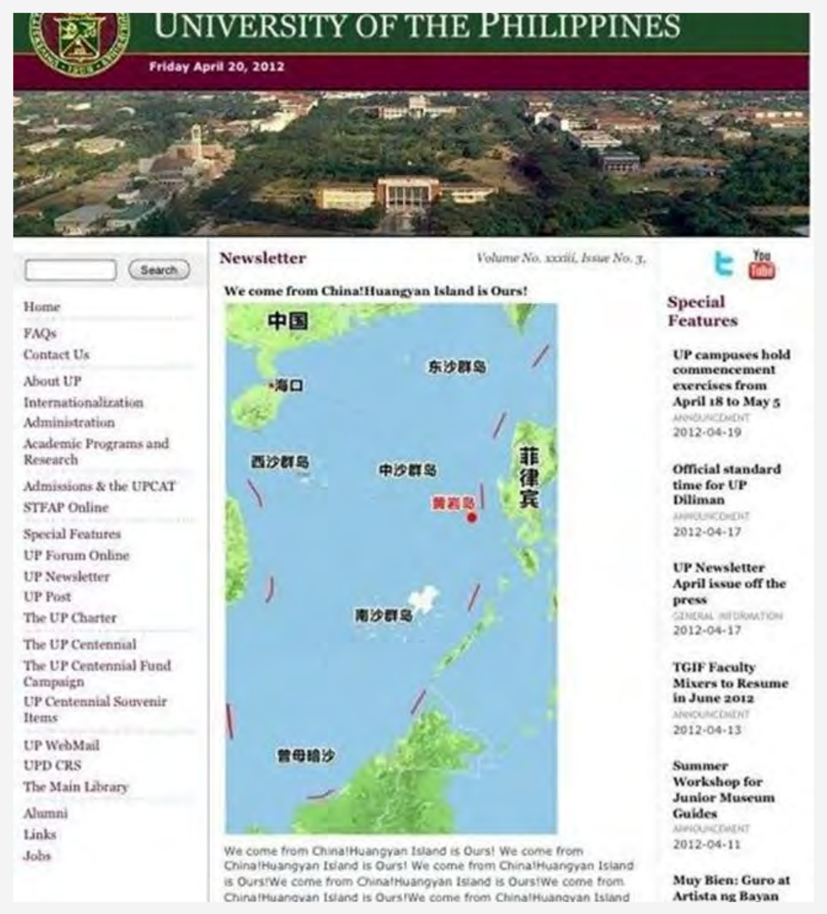
Your Shit Death Cannot Change Follow:

South China Sea Owned by Chinese

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".



UNIVERSITY OF THE PHILIPPINES

Friday April 20, 2012

Newsletter

Volume No. xxxiii, Issue No. 3.

We come from China!Huangyan Island is Ours!

We come from China!Huangyan Island is Ours! We come from China!Huangyan Island is Ours! We come from China!Huangyan Island is Ours!We come from China!Huangyan Island is Ours!We come from China!Huangyan Island is Ours!We come from China!Huangyan Island

Special Features

UP campuses hold commencement exercises from April 18 to May 5
ANNOUNCEMENT
2012-04-19

Official standard time for UP Diliman
ANNOUNCEMENT
2012-04-17

UP Newsletter April issue off the press
GENERAL INFORMATION
2012-04-17

TGIF Faculty Mixers to Resume in June 2012
ANNOUNCEMENT
2012-04-13

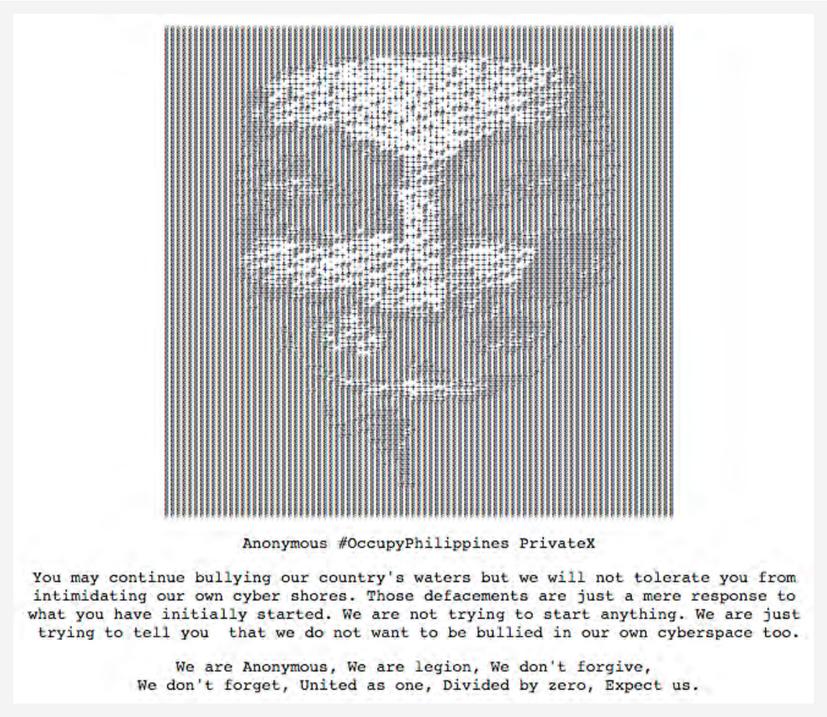
Summer Workshop for Junior Museum Guides
ANNOUNCEMENT
2012-04-11

Muy Bien: Guro at Artista ng Bayan

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 page[27].

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 attacks[28].



Anonymous #OccupyPhilippines PrivateX

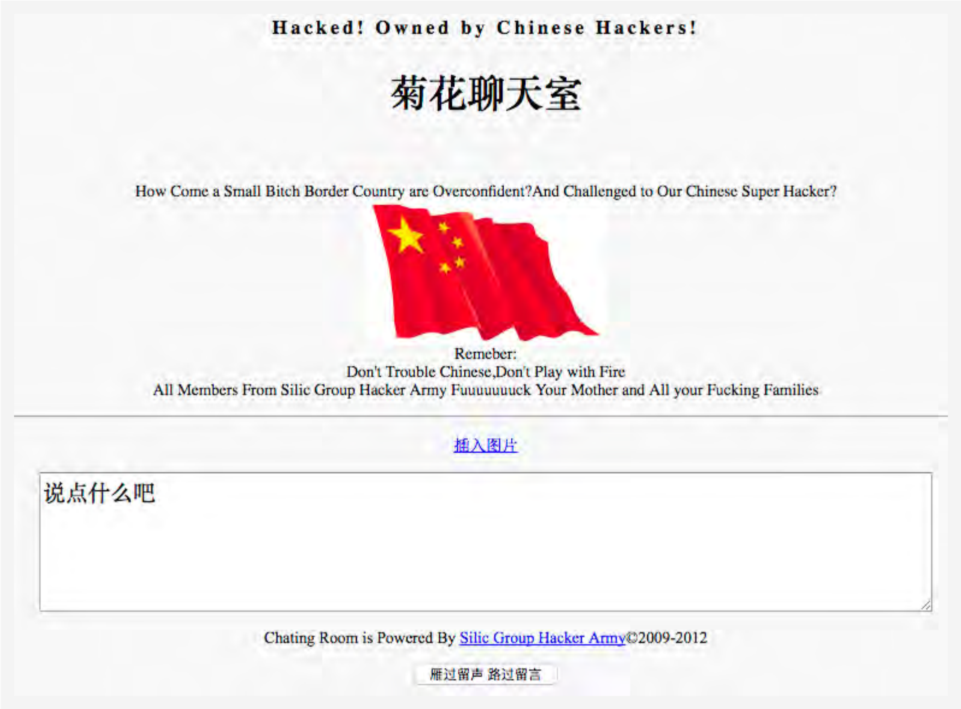
You may continue bullying our country's waters but we will not tolerate you from intimidating our own cyber shores. Those defacements are just a mere response to what you have initially started. We are not trying to start anything. We are just trying to tell you that we do not want to be bullied in our own cyberspace too.

We are Anonymous, We are legion, We don't forgive,
We don't forget, United as one, Divided by zero, Expect us.

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 pages[29].



Hacked! Owned by Chinese Hackers!

菊花聊天室

How Come a Small Bitch Border Country are Overconfident?And Challenged to Our Chinese Super Hacker?

Remeber:
Don't Trouble Chinese,Don't Play with Fire
All Members From Silic Group Hacker Army Fuuuuuuuck Your Mother and All your Fucking Families

插入图片

说点什么吧

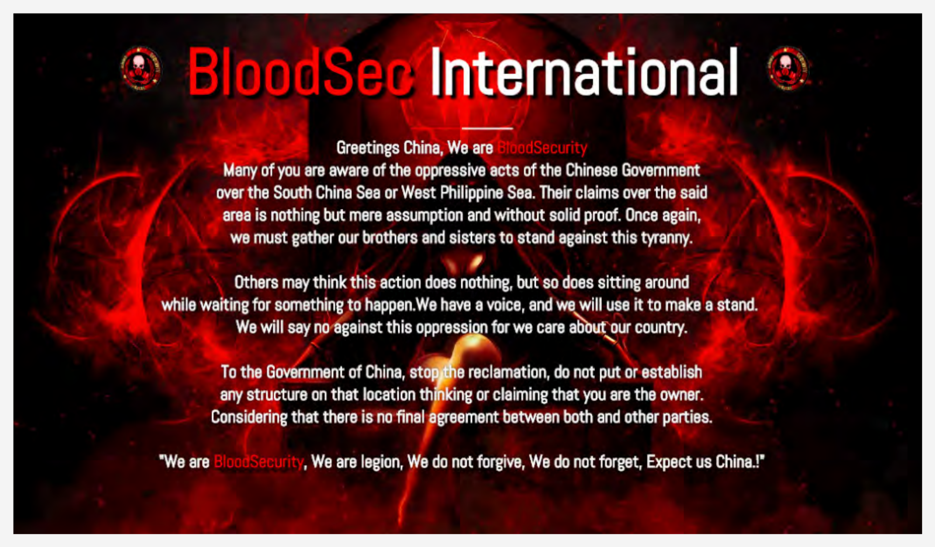
Chating Room is Powered By Silic Group Hacker Army©2009-2012

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 2015[30]. This action caused a wave of defacement attacks. BloodSec, a Philippine defacer group, launched a #StopReclamation campaign on April 26, 2015.



BloodSec International

Greetings China, We are BloodSecurity
Many of you are aware of the oppressive acts of the Chinese Government
over the South China Sea or West Philippine Sea. Their claims over the said
area is nothing but mere assumption and without solid proof. Once again,
we must gather our brothers and sisters to stand against this tyranny.

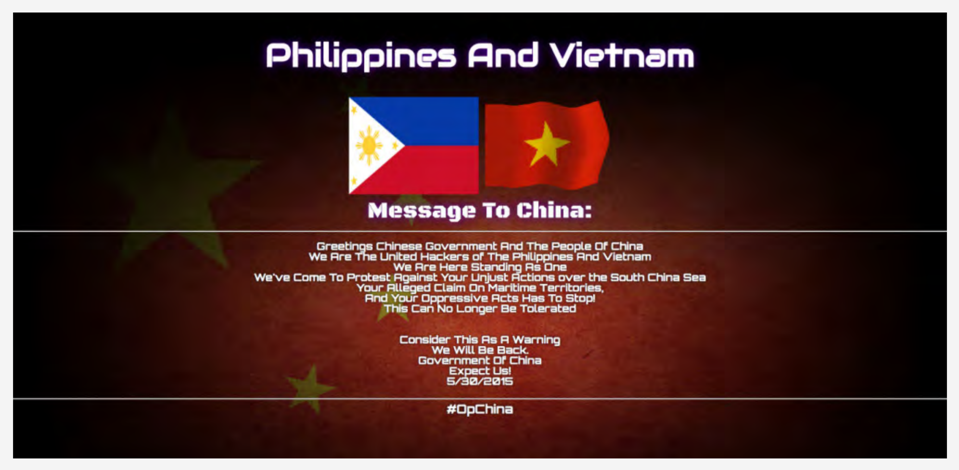
Others may think this action does nothing, but so does sitting around
while waiting for something to happen.We have a voice, and we will use it to make a stand.
We will say no against this oppression for we care about our country.

To the Government of China, stop the reclamation, do not put or establish
any structure on that location thinking or claiming that you are the owner.
Considering that there is no final agreement between both and other parties.

"We are BloodSecurity, We are legion, We do not forgive, We do not forget, Expect us China.!"

Figure 48. BloodSec defacement page

Tensions escalated a month later. Posting on Pastebin[31], 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".



Philippines And Vietnam

Message To China:

Greetings Chinese Government And The People Of China
We Are The United Hackers of The Philippines And Vietnam
We Are Here Standing As One
We've Come To Protest Against Your Unjust Actions over the South China Sea
Your Alleged Claim On Maritime Territories,
And Your Oppressive Acts Has To Stop!
This Can No Longer Be Tolerated

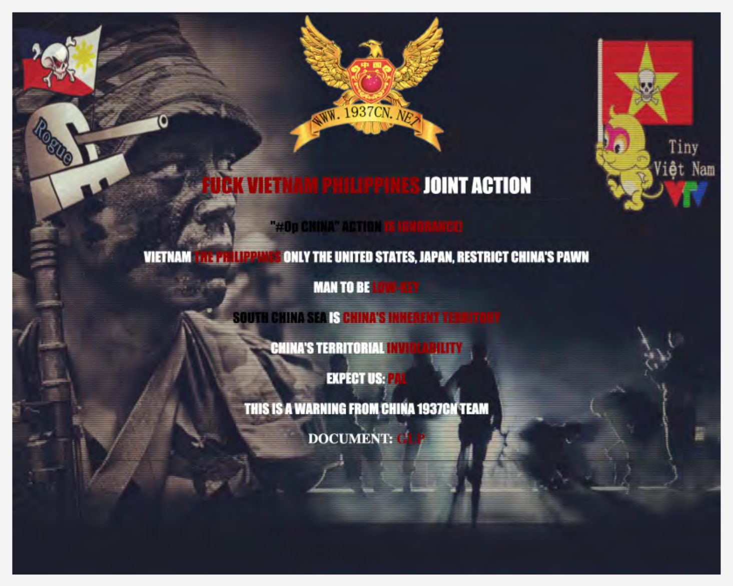
Consider This As A Warning
We Will Be Back.
Government Of China
Expect Us!
5/30/2015

#OpChina

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."



FUCK VIETNAM PHILIPPINES JOINT ACTION

"#Op CHINA" ACTION IS IGNORANCE!

VIETNAM THE PHILIPPINES ONLY THE UNITED STATES, JAPAN, RESTRICT CHINA'S PAWN

MAN TO BE LOW-KEY

SOUTH CHINA SEA IS CHINA'S INHERENT TERRITORY

CHINA'S TERRITORIAL INVIOLABILITY

EXPECT US: PAL

THIS IS A WARNING FROM CHINA 1937CN TEAM

DOCUMENT: GLP

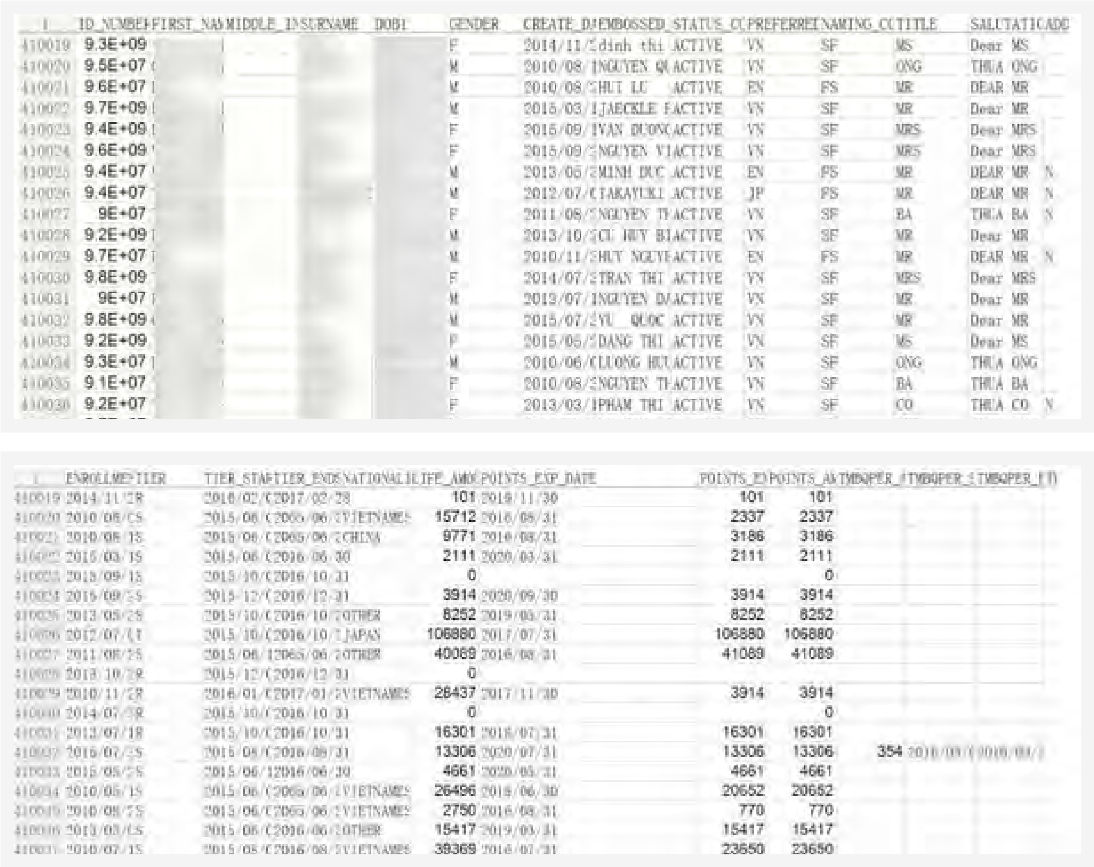
Figure 50. Retaliation from Chinese hackers

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 Vietnam[32].

On July 29, 2016, the Chinese hacker group 1937cn attacked two major airports in Vietnam and the website of Vietnam Airlines[33]. 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 Airlines[34]. This was not the first time 1937cn attacked Vietnam Airlines; the group also launched a similar attack on May 30, 2015.



I	ID_NUMBEF	FIRST_NA	MIDDLE_I	SURNAME	DOB1	GENDER	CREATE_D	EMBOSSED	STATUS_C	PREFERREI	NAMING_C	TITLE	SALUTATI	CADD
410019	9.3E+09	[redacted]		[redacted]	[redacted]	F	2014/11/	dinh thi	ACTIVE	VN	SF	MS	Dear MS	
410020	9.5E+07	[redacted]		[redacted]	[redacted]	M	2010/08/	NGUYEN Q	ACTIVE	VN	SF	ONG	THUA ONG	
410021	9.6E+07	[redacted]		[redacted]	[redacted]	M	2010/08/	HUI LU	ACTIVE	EN	FS	MR	DEAR MR	
410022	9.7E+09	[redacted]		[redacted]	[redacted]	M	2015/03/	JAECKLE F	ACTIVE	VN	SF	MR	Dear MR	
410023	9.4E+09	[redacted]		[redacted]	[redacted]	F	2015/09/	VAN DUON	ACTIVE	VN	SF	MRS	Dear MRS	
410024	9.6E+09	[redacted]		[redacted]	[redacted]	F	2015/09/	NGUYEN V	ACTIVE	VN	SF	MRS	Dear MRS	
410025	9.4E+07	[redacted]		[redacted]	[redacted]	M	2013/05/	MINH DUC	ACTIVE	EN	FS	MR	DEAR MR	N
410026	9.4E+07	[redacted]		[redacted]	[redacted]	M	2012/07/	TAKAYUKI	ACTIVE	JP	FS	MR	DEAR MR	N
410027	9E+07	[redacted]		[redacted]	[redacted]	F	2011/08/	NGUYEN T	ACTIVE	VN	SF	BA	THUA BA	N
410028	9.2E+09	[redacted]		[redacted]	[redacted]	M	2013/10/	CU HUY B	ACTIVE	VN	SF	MR	Dear MR	
410029	9.7E+07	[redacted]		[redacted]	[redacted]	M	2010/11/	HUY NGUYE	ACTIVE	EN	FS	MR	DEAR MR	N
410030	9.8E+09	[redacted]		[redacted]	[redacted]	F	2014/07/	TRAN THI	ACTIVE	VN	SF	MRS	Dear MRS	
410031	9E+07	[redacted]		[redacted]	[redacted]	M	2013/07/	NGUYEN D	ACTIVE	VN	SF	MR	Dear MR	
410032	9.8E+09	[redacted]		[redacted]	[redacted]	M	2015/07/	VU QUOC	ACTIVE	VN	SF	MR	Dear MR	
410033	9.2E+09	[redacted]		[redacted]	[redacted]	F	2015/05/	DANG THI	ACTIVE	VN	SF	MS	Dear MS	
410034	9.3E+07	[redacted]		[redacted]	[redacted]	M	2010/06/	LUONG HU	ACTIVE	VN	SF	ONG	THUA ONG	
410035	9.1E+07	[redacted]		[redacted]	[redacted]	F	2010/08/	NGUYEN T	ACTIVE	VN	SF	BA	THUA BA	
410036	9.2E+07	[redacted]		[redacted]	[redacted]	F	2013/03/	PHAM THI	ACTIVE	VN	SF	CO	THUA CO	N

I	ENROLLME	TIER	TIER_STAF	TIER_END	NATIONALI	LIFE_AMO	POINTS_EXP_DATE	POINTS_E	POINTS_AV	TMBQPER_	TMBQPER_	TMBQPER_ET
410019	2014/11/2	R	2016/02/(	2017/02/28		101	2019/11/30	101	101			
410020	2010/08/C	S	2015/06/(	2065/06/2	VIETNAMES	15712	2016/08/31	2337	2337			
410021	2010/08/1	S	2015/06/(	2065/06/2	CHINA	9771	2016/08/31	3186	3186			
410022	2015/03/1	S	2015/06/(	2016/06/30		2111	2020/03/31	2111	2111			
410023	2015/09/1	S	2015/10/(	2016/10/31		0			0			
410024	2015/09/2	S	2015/12/(	2016/12/31		3914	2020/09/30	3914	3914			
410025	2013/05/2	S	2015/10/(	2016/10/2	OTHER	8252	2019/05/31	8252	8252			
410026	2012/07/(	T	2015/10/(	2016/10/1	JAPAN	106880	2017/07/31	106880	106880			
410027	2011/08/2	S	2015/06/1	2065/06/2	OTHER	40089	2016/08/31	41089	41089			
410028	2013/10/2	R	2015/12/(	2016/12/31		0						
410029	2010/11/2	R	2016/01/(	2017/01/2	VIETNAMES	28437	2017/11/30	3914	3914			
410030	2014/07/2	R	2015/10/(	2016/10/31		0			0			
410031	2013/07/1	R	2015/10/(	2016/10/31		16301	2016/07/31	16301	16301			
410032	2016/07/2	S	2015/08/(	2016/08/31		13306	2020/07/31	13306	13306	354	2016/08/(	2016/08/
410033	2015/05/2	S	2015/06/1	2016/06/30		4661	2020/05/31	4661	4661			
410034	2010/05/1	S	2015/06/(	2065/06/1	VIETNAMES	26496	2018/06/30	20652	20652			
410035	2010/08/7	S	2015/06/(	2065/06/1	VIETNAMES	2750	2016/08/31	770	770			
410036	2013/03/C	S	2015/06/(	2016/06/2	OTHER	15417	2019/03/31	15417	15417			
410037	2010/07/1	S	2015/05/(	2016/08/5	VIETNAMES	39369	2016/07/31	23650	23650			

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 passengers[35].

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.

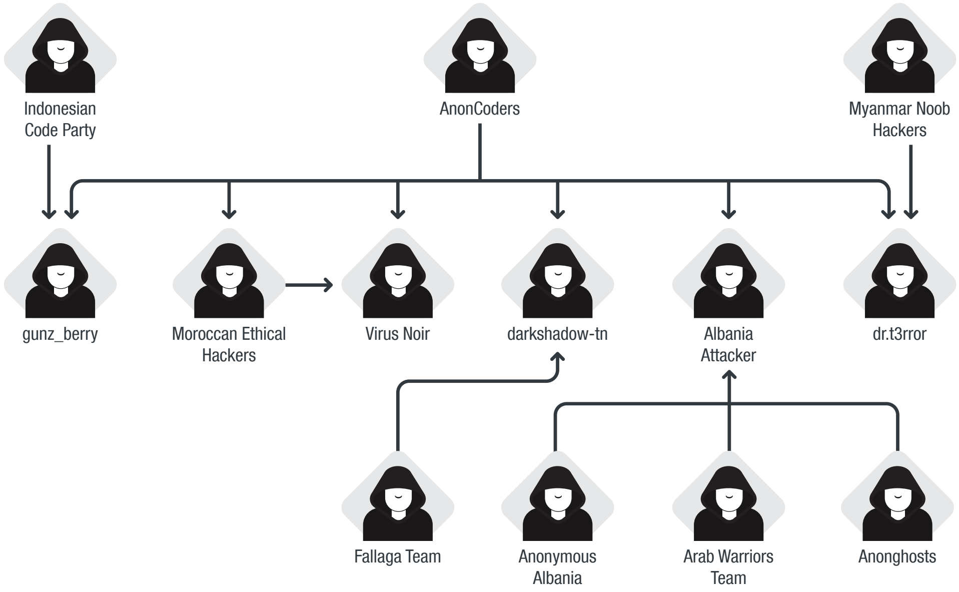


Figure 52. The hacking group AnonCoders

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.

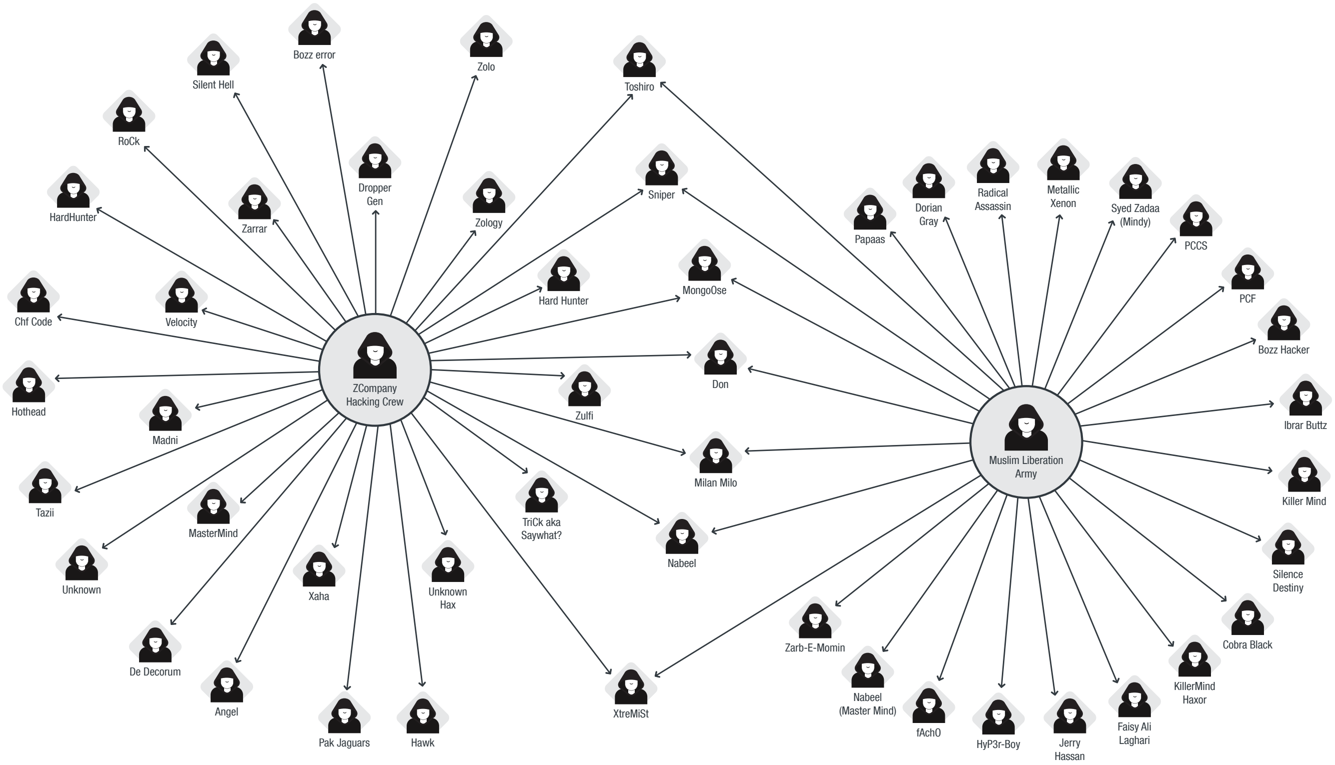


Figure 53. Members of the ZCompany Hacking Crew and the Muslim Liberation Army

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.

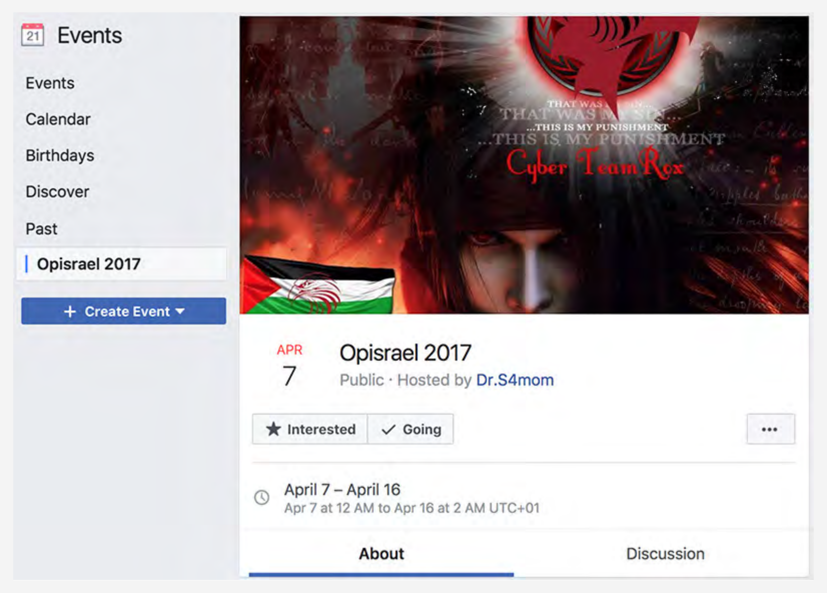
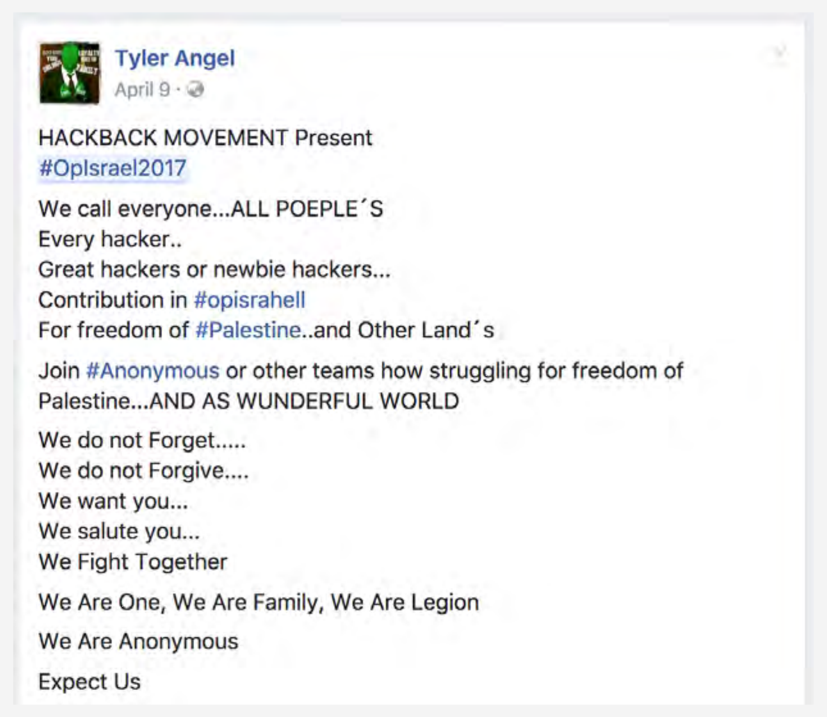


Figure 54. Facebook calendar used to schedule defacement activities


Tyler Angel
April 9 ·

HACKBACK MOVEMENT Present
#OpIsrael2017

We call everyone...ALL POEPLE´S
Every hacker..
Great hackers or newbie hackers...
Contribution in #opisrahell
For freedom of #Palestine..and Other Land´s

Join #Anonymous or other teams how struggling for freedom of
Palestine...AND AS WUNDERFUL WORLD

We do not Forget.....
We do not Forgive....
We want you...
We salute you...
We Fight Together

We Are One, We Are Family, We Are Legion

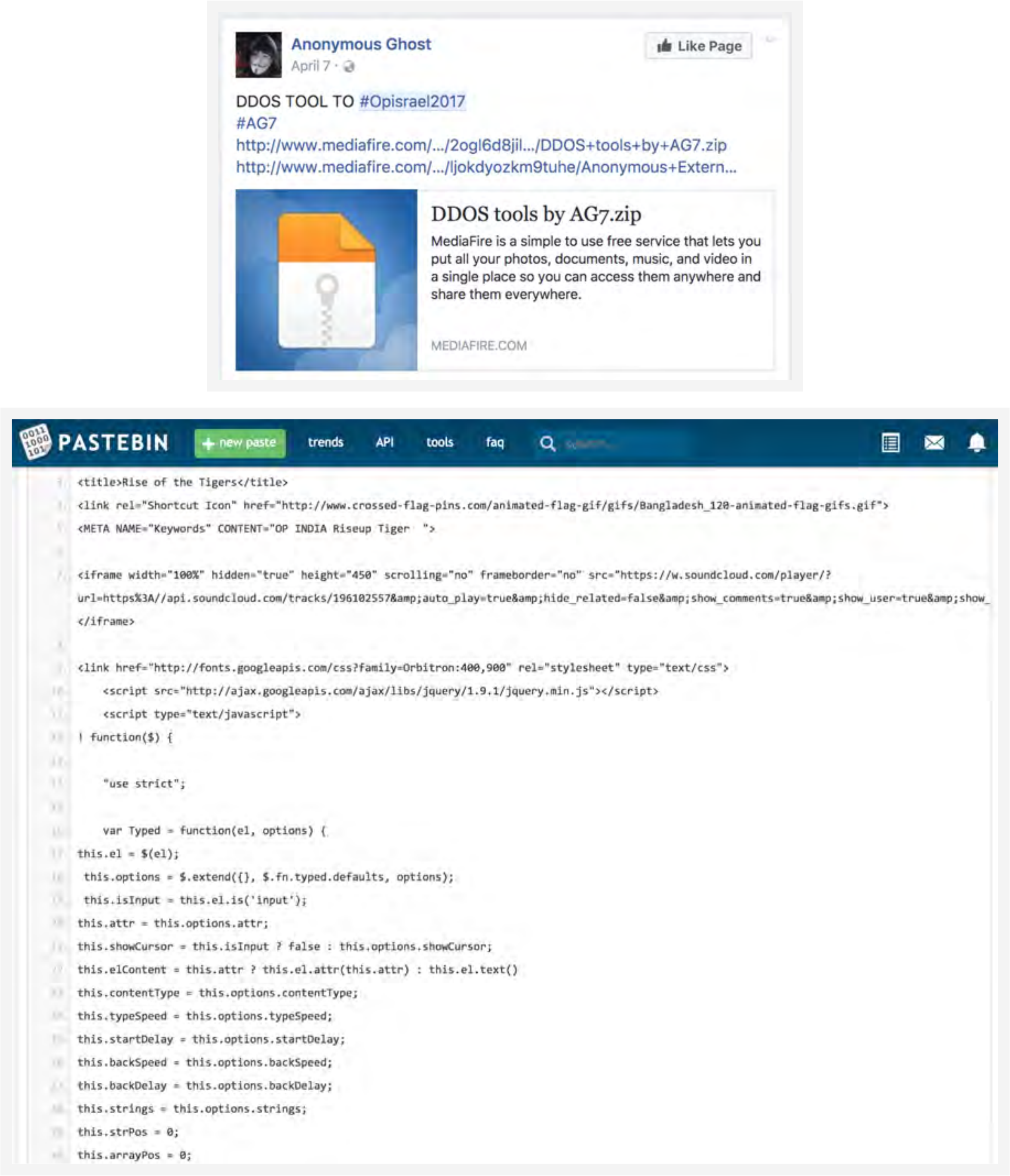
We Are Anonymous

Expect Us

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.



Anonymous Ghost
April 7 ·

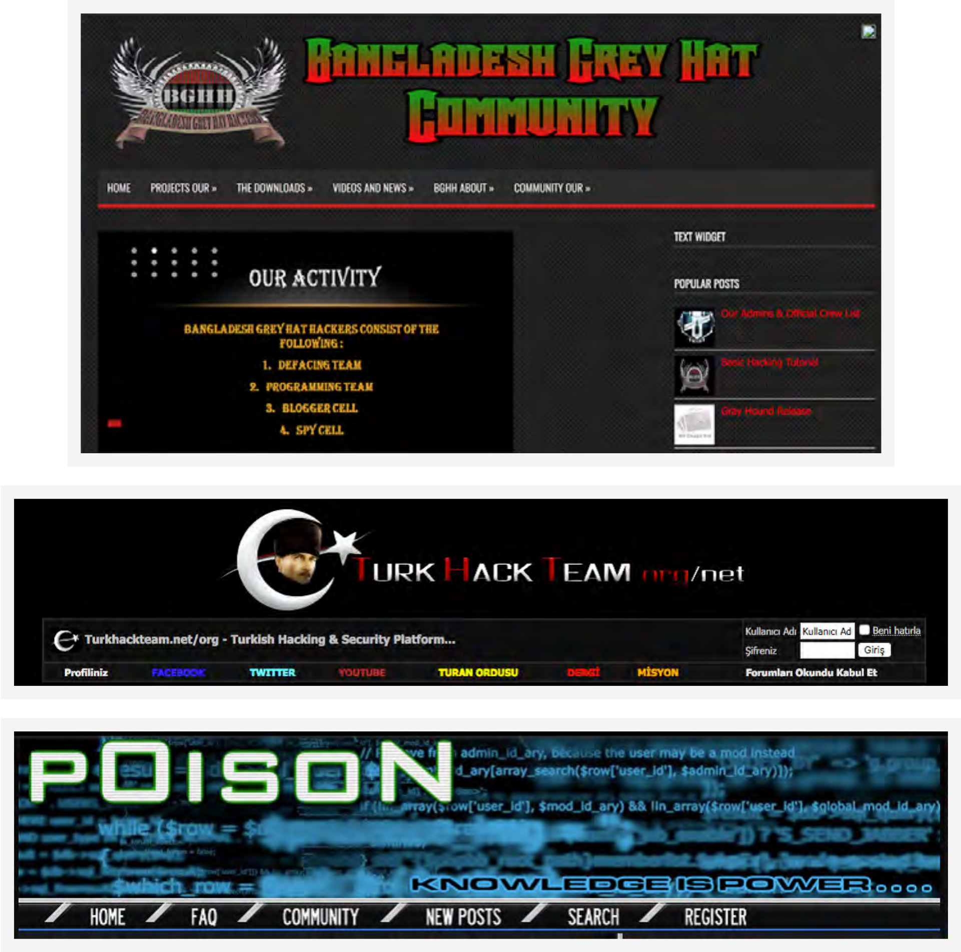
DDOS TOOL TO #Opisrael2017
#AG7
http://www.mediafire.com/.../2ogl6d8jil.../DDOS+tools+by+AG7.zip
http://www.mediafire.com/.../ljokdyozkm9tuhe/Anonymous+Extern...

DDOS tools by AG7.zip
MediaFire is a simple to use free service that lets you put all your photos, documents, music, and video in a single place so you can access them anywhere and share them everywhere.
MEDIAFIRE.COM

```
<title>Rise of the Tigers</title>
<link rel="Shortcut Icon" href="http://www.crossed-flag-pins.com/animated-flag-gif/gifs/Bangladesh_120-animated-flag-gifs.gif">
<META NAME="Keywords" CONTENT="OP INDIA Riseup Tiger  ">

<iframe width="100%" hidden="true" height="450" scrolling="no" frameborder="no" src="https://w.soundcloud.com/player/?
url=https%3A//api.soundcloud.com/tracks/196102557&amp;auto_play=true&amp;hide_related=false&amp;show_comments=true&amp;show_user=true&amp;show_
</iframe>

<link href="http://fonts.googleapis.com/css?family=Orbitron:400,900" rel="stylesheet" type="text/css">
    <script src="http://ajax.googleapis.com/ajax/libs/jquery/1.9.1/jquery.min.js"></script>
    <script type="text/javascript">
! function($) {

    "use strict";

    var Typed = function(el, options) {
this.el = $(el);
 this.options = $.extend({}, $.fn.typed.defaults, options);
 this.isInput = this.el.is('input');
this.attr = this.options.attr;
this.showCursor = this.isInput ? false : this.options.showCursor;
this.elContent = this.attr ? this.el.attr(this.attr) : this.el.text()
this.contentType = this.options.contentType;
this.typeSpeed = this.options.typeSpeed;
this.startDelay = this.options.startDelay;
this.backSpeed = this.options.backSpeed;
this.backDelay = this.options.backDelay;
this.strings = this.options.strings;
this.strPos = 0;
this.arrayPos = 0;
```

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.



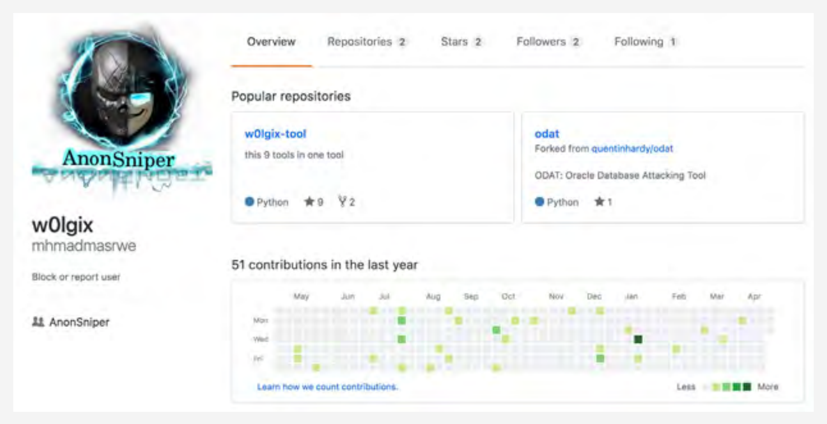
BANGLADESH GREY HAT HACKERS CONSIST OF THE FOLLOWING :

1. DEFACING TEAM
2. PROGRAMMING TEAM
3. BLOGGER CELL
4. SPY CELL

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.



w0lgix
mhmadmasrwe

Block or report user

AnonSniper

Overview | Repositories 2 | Stars 2 | Followers 2 | Following 1

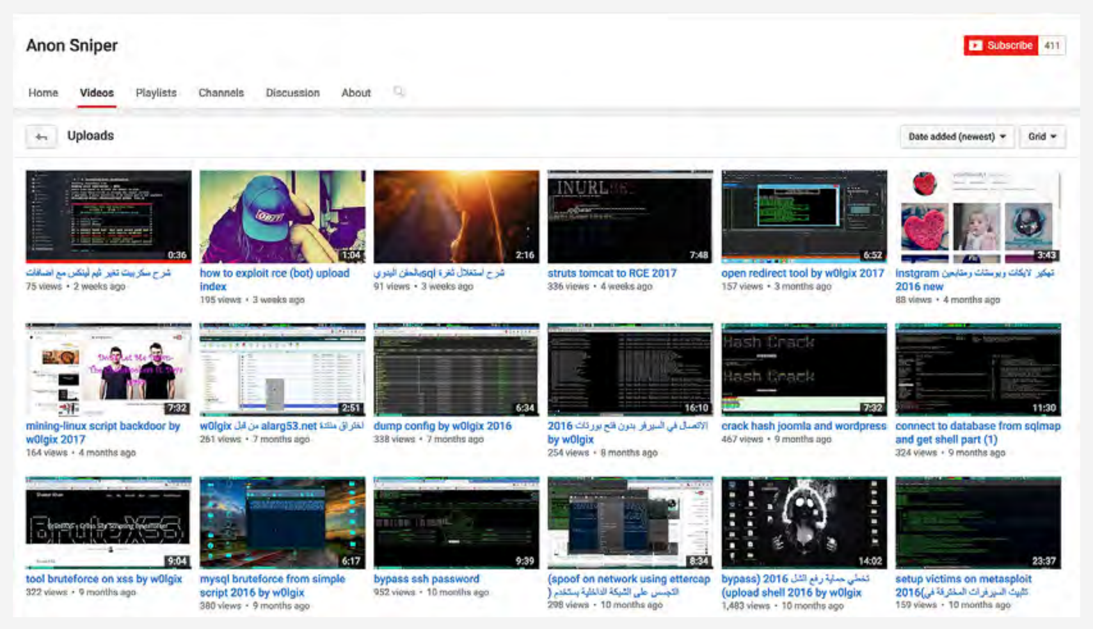
Popular repositories

w0lgix-tool
this 9 tools in one tool
Python ★ 9 Forks 2

odat
Forked from quentinhardy/odat
ODAT: Oracle Database Attacking Tool
Python ★ 1

51 contributions in the last year

Learn how we count contributions.



Anon Sniper

Uploads

شرح سكربيت تغير ثيم لينكس مع اضافات
0:36 · 75 views • 2 weeks ago

how to exploit rce (bot) upload index
1:04 · 195 views • 3 weeks ago

شرح استغلال ثغرة sqlبالحقن اليدوي
2:16 · 91 views • 3 weeks ago

struts tomcat to RCE 2017
7:48 · 336 views • 4 weeks ago

open redirect tool by w0lgix 2017
6:52 · 157 views • 3 months ago

تهكير لايكات وبوستات ومتابعين instgram 2016 new
3:43 · 88 views • 4 months ago

mining-linux script backdoor by w0lgix 2017
7:32 · 164 views • 4 months ago

اختراق ملتقة alarg53.net من قبل w0lgix
2:51 · 261 views • 7 months ago

dump config by w0lgix 2016
6:34 · 338 views • 7 months ago

الاتصال في السيرفر بدون فتح بورتات 2016 by w0lgix
16:10 · 254 views • 8 months ago

crack hash joomla and wordpress
7:32 · 467 views • 9 months ago

connect to database from sqlmap and get shell part (1)
11:30 · 324 views • 9 months ago

tool bruteforce on xss by w0lgix
9:04 · 322 views • 9 months ago

mysql bruteforce from simple script 2016 by w0lgix
6:17 · 380 views • 9 months ago

bypass ssh password
9:39 · 952 views • 10 months ago

(spoof on network using ettercap) التجسس على الشبكة الداخلية بستخدم
8:34 · 298 views • 10 months ago

bypass) 2016 تخطي حماية رفع الشل (upload shell 2016 by w0lgix
14:02 · 1,483 views • 10 months ago

setup victims on metasploit 2016(تثبيت السيرفرات المخترقة في
23:37 · 159 views • 10 months ago

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

Defacers are also contributing to Exploit-DB, which is 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 authors[36] 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%)

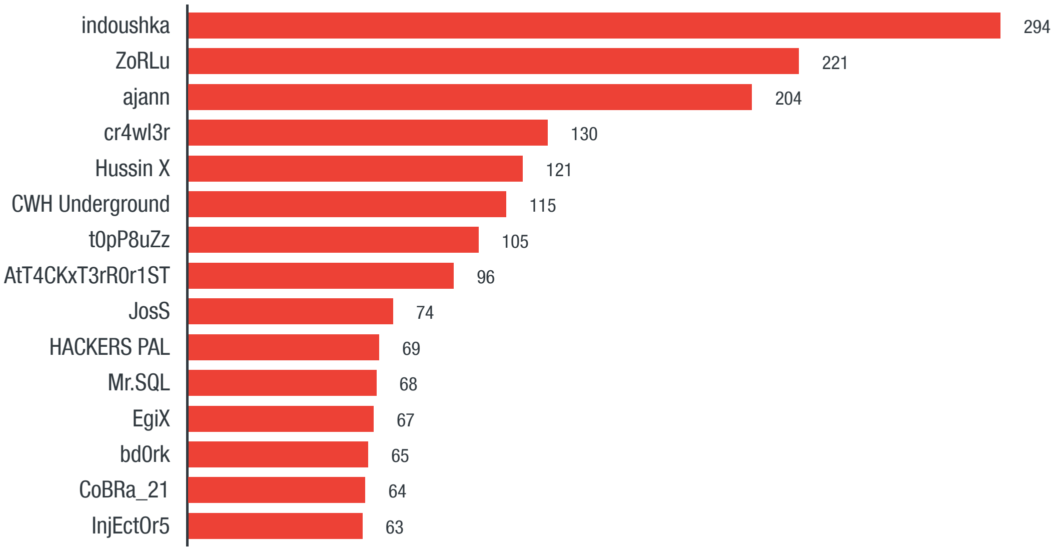


Figure 59. Top 15 defacers who shared exploit codes

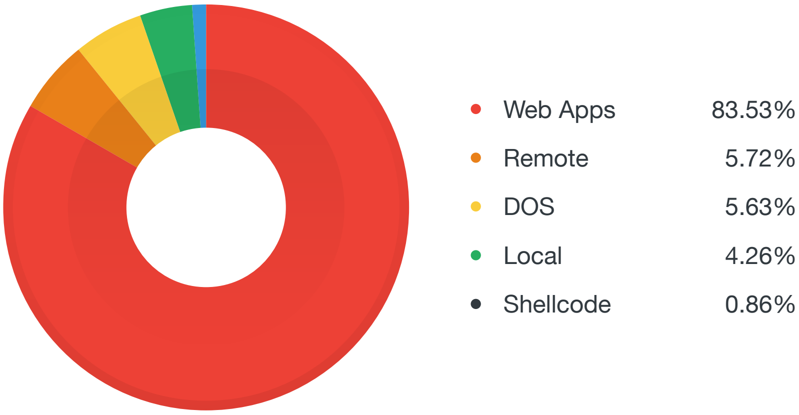
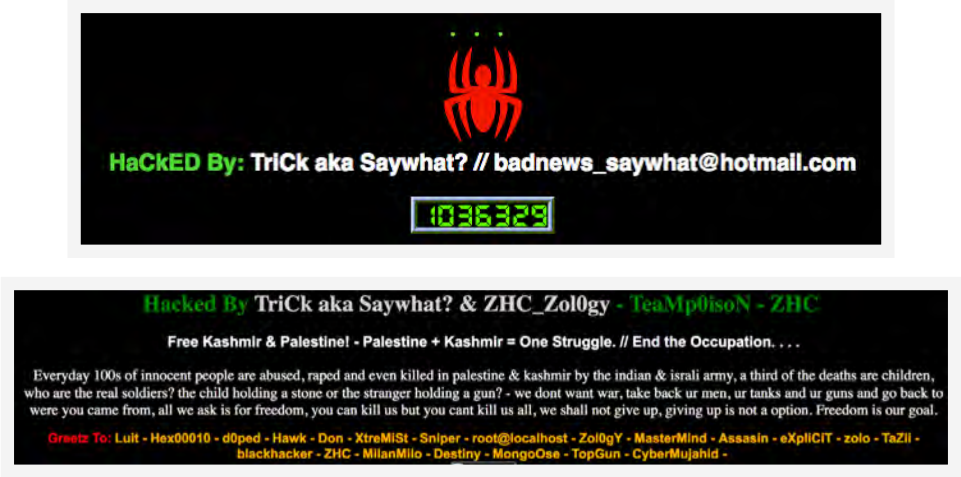


Figure 60. Breakdown of exploit types submitted by possible defacers

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.



HaCkED By: TriCk aka Saywhat? // badnews_saywhat@hotmail.com

1036329

Hacked By TriCk aka Saywhat? & ZHC_Zol0gy - TeaMp0isoN - ZHC

Free Kashmir & Palestine! - Palestine + Kashmir = One Struggle. // End the Occupation. . . .

Everyday 100s of innocent people are abused, raped and even killed in palestine & kashmir by the indian & israli army, a third of the deaths are children, who are the real soldiers? the child holding a stone or the stranger holding a gun? - we dont want war, take back ur men, ur tanks and ur guns and go back to were you came from, all we ask is for freedom, you can kill us but you cant kill us all, we shall not give up, giving up is not a option. Freedom is our goal.

Greetz To: Luit - Hex00010 - d0ped - Hawk - Don - XtreMiSt - Sniper - root@localhost - Zol0gY - MasterMind - Assasin - eXpliCiT - zolo - TaZii - blackhacker - ZHC - MilanMilo - Destiny - MongoOse - TopGun - CyberMujahid -

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 information[37]. 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 2015[38].

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".

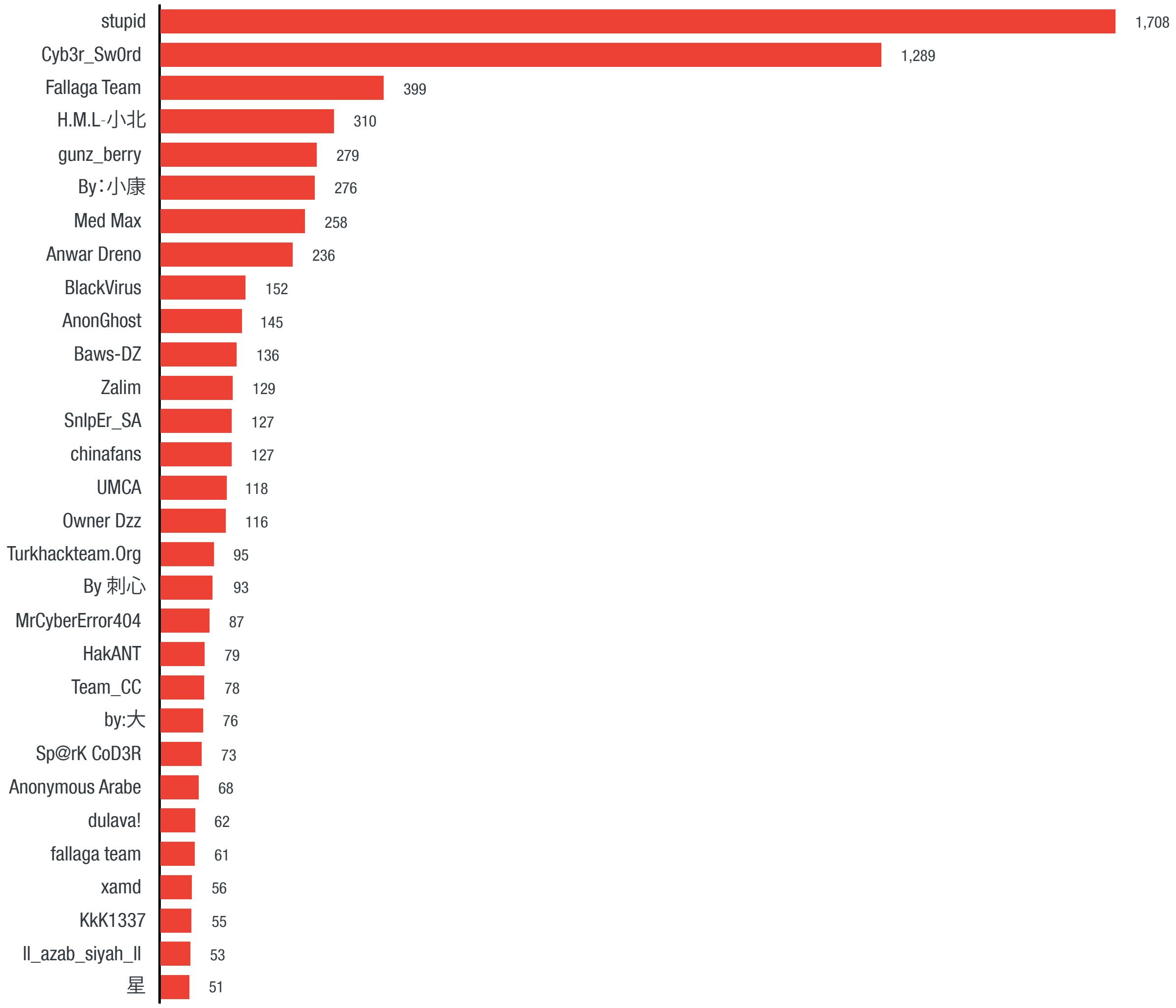


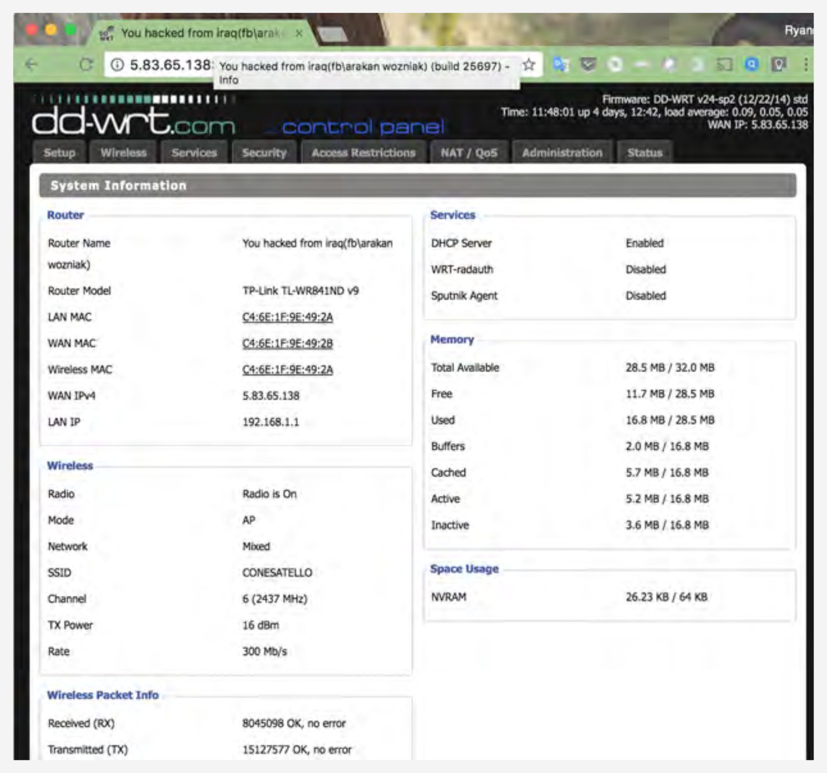
Figure 62. Defacers who were unknowingly spreading Ramnit through their defacement pages

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.



You hacked from iraq(fb\arak

5.83.65.138: You hacked from iraq(fb\arakan wozniak) (build 25697) - Info

Firmware: DD-WRT v24-sp2 (12/22/14) std
Time: 11:48:01 up 4 days, 12:42, load average: 0.09, 0.05, 0.05
WAN IP: 5.83.65.138

System Information

Router

Router Name	You hacked from iraq(fb\arakan wozniak)
Router Model	TP-Link TL-WR841ND v9
LAN MAC	C4:6E:1F:9E:49:2A
WAN MAC	C4:6E:1F:9E:49:2B
Wireless MAC	C4:6E:1F:9E:49:2A
WAN IPv4	5.83.65.138
LAN IP	192.168.1.1

Wireless

Radio	Radio is On
Mode	AP
Network	Mixed
SSID	CONESATELLO
Channel	6 (2437 MHz)
TX Power	16 dBm
Rate	300 Mb/s

Wireless Packet Info

Received (RX)	8045098 OK, no error
Transmitted (TX)	15127577 OK, no error

Services

DHCP Server	Enabled
WRT-radauth	Disabled
Sputnik Agent	Disabled

Memory

Total Available	28.5 MB / 32.0 MB
Free	11.7 MB / 28.5 MB
Used	16.8 MB / 28.5 MB
Buffers	2.0 MB / 16.8 MB
Cached	5.7 MB / 16.8 MB
Active	5.2 MB / 16.8 MB
Inactive	3.6 MB / 16.8 MB

Space Usage

NVRAM	26.23 KB / 64 KB

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" purposes[39]. 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 Ovtober 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 Match 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. Gianlucca 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**.

TREND MICRO™

Securing Your Journey
to the Cloud

www.trendmicro.com