Eleven Paths

Trend Report: Hacktivist CyberThreats Report 2019

Telefónica CYBER SECURITY UNIT

elevenpaths.com

Contents

1. Introduction

The Hacktivist Cyber Threat Report is an analytical report that includes the periodic scanning of the hacktivist threat's behavior in five observation rings: Europe and the United Kingdom, North America, Latin America, MENA / Asia and Africa, where it is made a description of the most significant hacktivist operations and cyberattacks, a selective portray of hacktivist identities the authorship of actions is attributed to, and a focused analysis of the structures, infrastructures, intentions and capacities of hacktivist identities.

The report is intended to be a generalist and depthless document to be completed by a specialized analysis that could be requested from Telefónica's CyberThreats service on a case-by-case basis.

2. Europe

Hacktivist cyberthreat in Europe during 2019 has remained, as in the rest of the world, focused on **web defacement attacks on websites provided with vulnerable content managers or outdated software.** It can be said that this is globally the prevailing trend with regard to hacktivist cyberthreat in all countries.

In some countries in Europe, specific attackers have developed more ideologically-motivated cyberattacks in the militant nature of hacktivism, assigning those cyberattacks to specific narrative frameworks developed to ideologically justify the actions. In this line of more targeted offensive cyberactions it may be highlighted specific narrative frameworks in Italy and Spain.

In Italy, **'LulzSecITA' continued to reactivate narratives of the old 'Anonymous Italia'**, developing attacks for several months of 2019 with a continuity pattern in the framework of the **#OpNoTAV** and **#OpGreenRights**. The actions have mainly consisted of SQL injections on vulnerable websites of small businesses, trade associations or local and regional governments.

As regards Spain, for their part, it may be highlighted the **#OpCataluña** or **#OpCatalonia**, a narrative framework reactive to the social and political conflict in Catalonia mainly due to the judicial prosecution of political and social leaders of the region for sedition. In this context, in March there were some low-profile exfiltrations and a wave of **specific denial of service attacks against websites of the Spanish Ministry of Justice**. In June, an identity that usually performs hacktivist propaganda and misinformation activities claimed to have had **access to the Microsoft Outlook corporate email web service of the Judiciary in Spain**, disclosing part of the content from the mailbox of the Supreme Court judge Manuel Marchena. No evidence was obtained that it was a cyberattack action of the same identity that disclosed the information, but that the disclosure channel could have been instrumented by a different attacker who never claimed it and may have accessed the emails by applying some kind of technique for compromising user credentials.

In September 2019 and in the context of the **pre-campaign for the call for general elections in Spain**, an identity involved in the #OpCatalunya disclosed private information from the mobile phone of the **former leader of the political party *Ciudadanos***. Such information, according to the police complaint filed by the victim, was illegally obtained through a **phishing attack**. There is no evidence that the hacktivist identity that disclosed information had been the direct author of the phishing attack. Rather, and according to the known history of that identity, the hypothesis is that **this identity ('Anonymous Catalonia') may have been used as a channel for disseminating information obtained by another attacker that has not been revealed**.

In the first half of October 2019, **#OpCatalonia was tentatively relaunched** as a reaction to the judgement pronounced upon Catalan independence leaders charged with sedition. However, as it happened in the recent protests in Hong Kong (with the #OpHongKong), the hacktivist protest dimension is negligible compared to the intensity of street protests: the hacktivism focused on the #OpCatalonia in 2019 failed to achieve collectivization or attract hacktivist identities from other countries. It relies on identities with zero or low technical skills to carry out cyberattacks that, according to such skills, are being occasional, of poor execution, pointing to irrelevant websites for the narrative context concerned. In general, #OpCatalonia has shown very **low danger and trivial volume of participation** during 2019.

On the other hand, and more in Europe, in March 2019 the **#OpCopyWrong** was convened, a hacktivist framework to protest against the voting at the European Parliament on copyright protection legislation, which developed **some denial of service attacks** against websites of European organizations and German political parties. The narrative framework did not reach collectivization or scope.

Additionally, in July, August and October 2019, it may be highlighted the **infringement of access to several Twitter profiles corresponding to five city councils in Spain, correlating with the same type of actions on government institutions in Ecuador and the Dominican Republic**: during this temporary hijacking, all profiles on Twitter posted messages in Spanish about 'political corruption' and in some cases threats against government officials or people, sometimes replacing the bio of the profiles with sentences about corruption. The author of the wave of cyberattacks has not signed any specific claim or disseminated a militant narrative other than the messages themselves attributing corruption to councils and government bodies. The **cyberattack vector in these actions was phishing**, and the execution was based on the dissemination of offensive and threatening messages through the compromised profile while remaining hijacked.

Finally, in November 2019 **'The 9th Company'** penetrated the website of the **EFE News Agency**, without triggering this time any content exfiltration into the public domain.

2.1. The United Kingdom

In the United Kingdom, the pattern of **defacement** already described for Europe **has been followed mainly on private websites, probably exploiting common software vulnerabilities** (mostly on commercial content managers).

Apart from how usual this specific pattern is, in April 2019 hacktivist identities mainly from outside the country responded to the police arrest of the activist Julian Assange with the **#OpUK, a variant of the #OpAssange narrative framework** that called for attacks against websites in that country and in Ecuador. In the United Kingdom, **denial of service attacks** were performed against national government websites as well as **SQL injections** against local government websites. In general, the #OpUK had very low impact and, apart from some occasional defacement attacks on private websites, **the #OpUK variant of the #OpAssange caused low-intensity actions:** some denial of service attacks on websites of government institutions and some defacement affecting mainly university subdomains and private websites (on which Julian Assange-related content was injected).

3. North America

During 2019, hacktivist offensives in North America were also distinguished by defacements on websites endowed with outdated and vulnerable software, in a volume generally smaller than in other regions.

Among the actions performed to illustrate this pattern may be mentioned the one carried out in January when **'zHypnogaja'** defaced two subdomains[1] from the Massachusetts Institute of Technology, which were programmed with the outdated Wordpress content manager. In July, the defacement by **'G4mm4'** with a file nervo.html and its nickname on the web of the government of the city of Wappingers Falls[2] in the State of New York, which was developed with a vulnerable version of Drupal. Moreover, the injection by '**M3sicth**' of the file relaz.html with its nickname on websites of three other US cities[3], which are endowed with a vulnerable DotNetNuke content manager. In November **'unbid'** used its nickname on two subdomains[4] hosted at Yale University, which were programmed with Drupal content manager.

Aside from this typical pattern, it may be highlighted the emergence in April of an identity (**'PokemonGo Team'**) that infringed the website of an association of US police officers. After examining its features, it may be hypothesized that it is probably a **cyberthreat with cybercriminal or even disinformative intentions** that used hacktivist tactics to gain notoriety in the media, but actually being a hacker cyberthreat rather than an hacktivist one. No further attacks claimed were performed.

On the other hand, in August there was a **infringement of the Twitter profile of its CEO and founder Jack Dorsey** using a tactic not previously seen for hacktivist actions by attackers (it is likely that the attacker is not a hacktivist identity, but another type of cyberthreat): the infringement of a service associated with Twitter through the application of **SIM Card Swap**, a fraud procedure through which the attacker would obtain a duplicate of the SIM card of a victim to attack. This action on Twitter is not related to those reported about Spain and seen in Latin America as well.

4. Latin America

During 2019 in Latin America, cyberattacks have been focused mainly on violating websites of local and regional government institutions in several countries equipped with outdated and vulnerable software, mainly commercial content managers. Apart from this general pattern, two narrative frameworks of different pace have been succeeded by cyberattacks focused briefly in Ecuador and to a greater extent in Chile, as a hacktivist reaction to social protest climates in both countries and in an attempt to bringing back attacks from Nicaragua that did not materialize in any scenario.

In March 2019, a **call was made to resume #OpNicaragua**, which did not end up triggering effective cyberattacks.

---

[1] ling-phil.mit.edu, haiti.mit.edu

[2] wappingersfallsny.gov

[3] wyomingmi.gov, ride.ri.gov, nconemap.gov

[4] cbey.research.yale.edu, envirocenter.research.yale.edu

In Ecuador, in April 2019 the **#OpEcuador variant of the mentioned #OpAssange** began with the same physiognomy as in the United Kingdom: denial of service attacks were launched, carried out iSQL on local government and university websites, and probably access to the website of the Ministry of Environment was compromised. At the end of April cyberattacks declined in this narrative framework, so during the last half of the month there were several denial of service attacks against government websites. The most relevant attack of the period was the **infringement of the website of the Constitutional Court of Ecuador**, defaced with an image of Assange -probably exploiting some vulnerability on Joomla content manager.

As regards Chile, the context of social instability has had a hacktivist correlate in the **#OpChile**, a narrative framework that called for cyberattacks against government websites in the country. Although the #OpChile has generally had a low collectivization and the identities that have joined it showed low technical skills in terms of cyberthreats, **a cyberattack action on the Chilean Police Force**, with subsequent exfiltration of sensitive information in the public domain resulted in a **considerable visibility of the #OpChile**. In that cyberattack action with exfiltration, called by its attackers **#PacoLeaks**, it is likely that a hacktivist operational sequence may be involved, composed of: 1) an attacking identity that remains anonymous; 2) an instrumental identity under the 'Anonymous' typology that claims the attack on social networks; 3) another or other different identities that provide an exfiltration infrastructure through a web domain.

In November and December, the #OpChile was **called for a second phase of cyberattacks**, which resulted mainly in denials of service against government websites and political parties, as well as some minor exfiltration on the public domain. Again, there was an exfiltration of data into the public domain. Under the name of **#MilicoLeaks, email content from several corporate accounts of the Chilean Army** was disclosed. This exfiltration occurred in December with denial of service attacks on government websites in the country. Some defacements as well, and several series of SQL injections on various websites, so producing exfiltrations of users with passwords in various cases, as well as reusing data already compromised in previously-performed cyberattacks.

As regards Venezuela, in March 2019 and in parallel to the deterioration of the political situation in the country, several identities performed **cyberattacks affecting by defacements and SQL injections several second and third-level government websites**, and universities. The actions did not accumulate substantive collectivization or revitalization of the hacktivist narrative framework of **#OpVenezuela** but was limited to specific attacks.

In August 2019, the environmental situation in the Amazonia had a hacktivist response in the proposal of **#OpAmazonia**, a narrative framework that suggested attacks against government websites in Brazil, but also against countries and companies that "took advantage" of the Amazonia. The proposal was barely materialized, with just some low-risk and low-intensity actions, mainly through the execution of SQL injections (mostly failed) on public institution websites, in addition to some individual denial of service attacks on Brazilian government websites.

Also in August, the infringement of Twitter profiles of public institutions (already reported in this report for Spain) was replicated in some Latin American countries (Ecuador, Dominican Republic, Chile, Colombia or Mexico). These attacks had their **epicenter of victimization in El Salvador**, where the first attacks were carried out with the same features as the rest. In addition, on one occasion it was **claimed by an unknown identity: 'Lullz DL'** -probably an opportunity nickname.

5. MENA y Asia

During 2019, the hacktivist operation in both regions has been characterized, as in most of the countries affected in other regions, by defacement attacks on websites exposing common vulnerabilities in outdated software, generally.

No stable hacktivist narrative frameworks have been proposed in both regions, except for **#OpIsrael**, a traditional call for cyberattacks against Israel that occurs every year throughout April and that over the last five years has seen a downward course in risk, in adhesion of attacking identities, or in volume of cyberattacks. In this context, in March 2019, some preliminary attacks by defacement were observed on minor private websites in Israel. In April, and following the trend set since previous years, the #OpIsrael call resulted in a **very low collectivization and low-risk actions against minor websites**, causing a negligible impact despite some attempt to claim false actions for the purpose of gaining notoriety for hacktivist identities.

As for specific countries, in Egypt, on the **anniversary of the Egyptian revolution of 2011, defacements were achieved on top-level websites of the Public Administration and universities**, including the Cairo University, the Ministry of Health or the agency for Internet domain registration, by injecting commemorative content on them.

During the first quarter of the year in Algeria, an identity caused defacements in **several second-level government websites** without showing hostile narrative on them but probably implementing vulnerabilities in Joomla and Wordpress content managers. There were also various defacements on the web of a political party and several local governments, probably in the scenario of rejection of the presidential re-election.

In March in Lebanon the website of the **Ministry of Industry** was disrupted, which is equipped with several vulnerable software components. In April, **the website of the government agency dedicated to cybersecurity** in Libya, equipped with WordPress content manager, was compromised.

Regarding Asia, the Burmese **Ministry of Industry** was compromised, since it has a large amount of outdated and vulnerable software. Defacement was performed against the Ministry of Foreign Affairs of Laos, the Ministry of Environment of the Philippines and the Asian Parliament, since they have websites equipped with **vulnerable software**.

In October, the Turkish military offensive in Syria provoked an **unsteady hacktivist reaction resuming the #OpTurkey** to, as in #OpCatalonia in Spain, cause occasional attacks, mostly due to denial of service on low relevance websites in general.

On the other hand, in August it was observed for the first time the **intersection**, or at least the **concatenation**, between **hacktivist and cybercriminal practices** since connections between hacktivism and SEO Spam content injection (considered minor cybercriminality) have been reported for at least the last year. This time, it is a cybercriminal step beyond, injecting a **fake phishing landing web for stealing American Express credentials**, after a hacktivist defacement: it has happened against the Libyan Ministry of Planning and at least the hacktivist attacker, acting under the nickname of 'Mr. Donut's', identifies itself as an **Indonesian attacker** under the pseudonym of '**Krayzie Haxor**'.

6. Africa

In Africa, as in Latin America, the main pattern of hacktivist attacks is defacement actions on websites that expose common vulnerabilities in outdated software. However, in Africa, instead of being mainly affected local and regional government websites (such as in Latin America) are ministerial websites of the first line of government.

Thus, in the first quarter of 2019 the website of the Kenyan Ministry of Defense, or ministries in Ghana, Burkina-Faso and Ethiopia, were compromised -in all cases on websites developed with vulnerable software. In April in Gambia, a website of the Ministry of Agriculture was affected, the same in Eritrea on the central bank of the country, and again in Kenya on a subdomain of the Ministry of Communications. In May in Zimbabwe, another attacker impacted another website with commercial content manager of the Ministry of Internal Affairs, while in Rwanda and Sudan regional governments' websites were compromised (also with vulnerable software).

7. Global Elements

Throughout 2019, the hacktivist pattern composed of website defacements that exposed outdated and vulnerable software has been evident, followed by these defacements due to injections of **SEO Spam content contingent on hacktivist attacks due to defacement**. This pattern has been mainly performed by **attacking identities with Turkish features**. To a lesser extent than SEO Spam content, contingent on defacements, also injected **scripts** on Javascript that led the visitors of the websites compromised to **networks distributing malicious content**.

On the other hand, in the second quarter of 2019 there was a predominance (quantitatively superior to the usual pattern of defacements on websites based on commercial content managers) of **affected websites by equipping Wordpress manager.** This is probably due to **three vulnerabilities** discovered during 2019 (CVE-2019-8942, CVE-2019-8943 and CVE-2019-9787, as well as another that has been active in Wordpress 5.0.0 for five years) and not yet patched in numerous websites.

Also, during the second half of May 2019 in several regions of the world there was an increase, above the usual, of **defacements violating websites equipped with Drupal content manager**.

Later, in July 2019, several incidents pointed out **correlations between web defacements and the use of DotNetNuke content manager and ASP.net software**, both from Microsoft. Although in the first case the last critical vulnerability is from 2017[5] and in the second case from 2011[6], they may be being exploited in non-updated websites: in fact in the second case it was verified that the defaced websites predominantly equipped the vulnerable version 4.0.30319.

In the execution of these attacks against websites equipped with ASP.net, DotNetNuke and Microsoft SharePoint in countries around the world, the **'VandaTheGod'** identity stood out during 2019, which had a **double task in terms of hacktivism and minor cybercriminality**, the latter showed in the sale of shells injected into websites. In December 2019, a 23-year-old boy from the Brazilian city of Uberlandia was arrested by the Minas Gerais State Police as alleged responsible for being behind the alias 'VandaTheGod'.

On the other hand, in March 2019, the well-known identity **'Phineas Fisher'**, which several years ago had considerable visibility for attacking cybersecurity companies, has reappeared with a message on social networks warning that it **will "hack again" in 2019**, without more data. In the second half of November 2019, they carried out their warning **by compromising the website of a bank in the Isle of Man**, penetrating some of their web servers by exploiting at least two unpatched vulnerabilities, installing a **backdoor Trojan in his network, and claiming to have made some SWIFT transfers**.

[5] https://www.cvedetails.com/vulnerability-list/vendor_id-2486/Dotnetnuke.html

[6] https://packetstormsecurity.com/files/111277/Microsoft-ASP.NET-Forms-Authentication-Bypass.html

The action of 'Phineas Fisher' was an individual cyberattack that does not presuppose the derivation from it of a specific hacktivist narrative framework in the form of cyberthreat beyond that already represented by at least five years 'Phineas Fisher' itself. On the other hand, it is the only cyberthreat of a purely hacktivist (ideological) nature on an international scale that operates technically as an advanced cyberthreat through the use of exploits, malware and penetration techniques. 'The 9th Company' in Spain would be, for example, at a lower level, with similar operational ability but without the (known) use of malware.

Finally, regarding the annual meeting of supporters of 'Anonymous' every November 5 under the name **'Million Mask March'**, continuing with a pattern of decline observed in the last years, 2019 ended **with a testimonial follow-up without incident in some cities of the world**. The only cyberattacks with the same theme of the meeting were carried out by **'LulzSecITA'** in Italy. This one, following its usual modus of behavior compromised, mainly through SQL injections, websites of several local and regional corporations in the country, in addition to the telecommunications operator Lyca Mobile, by exfiltrating personal data of their clients in the country.

About ElevenPaths

At ElevenPaths, the Telefónica's Cybersecurity Unit, we believe in the idea of challenging the current state of security, since security constitutes a feature that must be always present in technology. We are continuously redefining the relationship between security and people, with the aim of developing innovative products capable of renovating the concept of security. Thanks to this, we stay a step ahead of attackers, that are increasingly present in our digital life.

More information

elevenpaths.com

@ElevenPaths

blog.elevenpaths.com