At the Intersection of Interests and Objectives in Cybersecurity

Mircea Constantin ȘCHEAU[1], Mihai Daniel LEU[2], Cătălin UDROIU[3]
[1] Phd, Constanta Maritime University, University of Craiova, Romania
mircea.scheau@cmu-edu.eu, mircea.scheau@edu.ucv.ro
[2] Threat Researcher, Farscope Information Consulting, Romania
daniel.leu2810@gmail.com
[3] Hybrid Cloud Specialist, Stefanini EMEA, Romania
udroiu_catalin@yahoo.com

Abstract

The exponential increase in the advancements registered across all sectors of the information technology field gave a new, ever-expanding dimension to the idea of protesting against national governments by introducing political activism into cyberspace. Despite the apparent noble objectives, there is a thin line between hacking as a form of protest against the established order and cyber-criminal activity that can cause financial or material prejudice against organizations. This aspect outlines several dimensions of hacktivism which will be brought into discussion. Another interesting characteristic in hacktivist psychology is the pursuit of "digital clout" as a way to measure success: the more notorious a group becomes, the more attention it will get from the press alas the more successful it is. Even though it is a clear distinction between financially motivated threat actors and hacktivists, some shifts were observed in the cyber threat spectrum in the very politically charged context of war, with different groups which had a history of financially motivated cybercrime, joining the cyber conflict and engaging in hacktivist campaigns either on the one side or the other.

Index terms: cyber security, involvement, threat landscape

1. Introduction

The term "hacktivism" was introduced in the vocabulary back in 1990 by the group "Cult of the Dead Cow" and broadly encompasses hacking as a political act in the alleged fight for free speech and human rights. Even though hacktivism is not a definitive product of the recent years, with hacktivist campaigns being observed since as back as 1989, the exponential rate at which the technological expertise in the information and technology sector expanded arguably expanded the scope of protest movements by introducing the act of civil disobedience in the cyberspace.

The ever-expanding cyber threat landscape that we faced in recent years combined with the scenario in which threat actors can rapidly change the motives behind their campaigns increases the complexity of analysis and thus, a more solidified approach must be brought forward when discussing concepts such as hacktivism.

This paper aims to provide an overview on hacktivism by highlighting several dimensions of the concept as well as by presenting it through the example of one of the most popular hacker collectives in recent years. We will also tackle the issue of financing and bring into the discussion some key points on the problematic operational financing of hacktivist groups.

2. Research Method

Francis, J. R. D. [1] identified several ways in which one can be shown original research, and according with those, some of the strongest points outlined by the authors in this paper are:

- Setting down a major piece of new information in writing for the first time.
- Giving a good exposition of another's idea.
- Continuing a previously original piece of work.
- Showing originality in testing somebody else's idea.
- Providing a single original technique, observation, or result in an otherwise unoriginal but competent piece of research.

In this study, the authors brought into the discussion conceptual issues on the multiple facets of hacktivism and presented the complexity of the threat actors that operate in this space through previously documented hacktivist campaigns. This research is a literature review on relevant hacktivism and cyberterrorism literature.

3. Concept analysis

Given that we can broadly define hacktivism as the act of using technology as a form of protest in a clash between two opposed views, we could see a strong parallel with the concept of hacking as it was defined in the work of Tim Jordan and Paul Taylor 2004 as “the imaginative re-appropriation of technology’s potential within countercultural and oppositional communities”. [2]

While the goals of financially motivated threat actors are more than often straightforward, having financial gains as the ultimate objective, a more substantiated analysis has to be conducted when trying to fit cyber activity into the specter of hacktivism as it being a broadly defined concept, can encompass several methods and objectives.

FirstLinePractitioners present in an article [3] some interesting dimensions of hacktivism that we think are worth bringing into the discussion. The first dimension is cyberterrorism: How significant should the damage caused by a hacktivist campaign be in order for the national and international authorities to classify it as cyber terrorism? To answer that we need to take note of how national and international bodies define cyberterrorism.

The North Atlantic Treaty Organization (NATO) defines cyberterrorism in Responses to Cyber Terrorism 2008 [4] as "a cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal".

The United States Federal Bureau of Investigation (FBI) defines cyberterrorism [4] as "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by subnational groups or clandestine agents".

Both of these definitions broadly explain cyberterrorism as a cyberattack ultimately motivated by an ideological goal that has the power to profoundly impact society. One can observe the general similarities between the concept of hacktivism and cyberterrorism as both basically revolve around computer hacking fueled sometimes by ideological objectives. The main and most distinctive difference is that hacktivism is generally conducted through non-violent means.

The second dimension of hacktivism that is worth bringing into discussion is cyberwarfare conducted by nation state actors. These threat actors are nation state affiliated and usually conduct their operations with the purpose of either intelligence gathering or disruption, depending on the national interests of the state that is sponsoring them. One good example, in which hacktivist objectives coincidentally (or not) aligned with the interests of a nation state, was the massive cyber-attack carried against Estonian infrastructure in 2007. The attack, which was also referenced by

FirstLinePractitioners in their report [3], was allegedly triggered by Estonia's decision to reallocate the Bronze Soldier of Tallinn monument, and consisted of a massive Distributed Denial of Service (DDoS) attack against the digital infrastructure of Estonia. It is very interesting to mention that a state affiliated youth group called "Nashi" claimed responsibility for this particular motivated cyber-attack.

In order to correctly outline the scope of hacktivism in the cyber threat activity spectrum we have to take into account several key points such as the motivation of the attack, the technical capabilities of the actor executing the attack, the type of goals and objectives set at the beginning of a campaign and, probably one of the most interesting, financing. We propose to discuss the aforementioned aspects in the context of one of the most well-known groups since the emergence of hacktivism as a concept.

4. The paradox of decentralization

Hacktivism, according to the general consent at a conceptual level, is viewed as a generally decentralized effort. But is this true entirely? In order to answer this question, we have to take a look at probably the most discussed / analyzed hacktivist movement in recent history.

Anonymous made their first appearance around the year 2003 on the popular image board 4chan. In the following years, the allegedly decentralized group continued to engage in cyber-attacks against several government agencies, government institutions as well as private sector organizations, campaigns through which Anonymous consolidated their identity as an international, leaderless, hacktivist collective. The Japanese cyber security company Trend Micro outlined in a report [5] some of the most notable cyber-attacks claimed by Anonymous affiliated groups in the timeframe 2011-2013 such as the 2011 Operation Tunisia in which Anonymous recruited Tunisian hackers to execute Distributed Denial of Service (DDoS) attacks against government digital infrastructure as part of the Arab Spring protest movement or the 2012 Distributed Denial of Service (DDoS) attack against payment services like Amazon, PayPal, Visa, and Mastercard in connection to the WikiLeaks scandal. Another notable incident recorded in the aforementioned timeframe was the 2011 arguably more sophisticated attack against the American geopolitics company Stratfor in which the attackers allegedly managed to exfiltrate 200 gigabytes worth of data.

Despite the apparent minimal funding and lack of a central command structure, the Anonymous idea was able to unite different hacker groups under a centralized, objective-based framework through which they executed various campaigns. Heather Suzanne Woods, M.A. argued [6] that "Anonymous rhetorically creates a hacktivist identity in order to constitute its audience as a collective, unified social movement". Arguably, the Anonymous collective, even though lacking central leadership, could easily rally multiple hacker groups under a centralized, objective-based, campaign against specific targets.

The aforementioned capability was again demonstrated in the most recent operations, which were initiated in 2022 and incorporated a number of cyberattacks executed by several Anonymous affiliated groups against targets from both private and public sectors. In Anonymous characteristic fashion, these cyber-attacks ranged in terms of their technical sophistication from massive Distributed Denial of Service (DDoS) campaigns aimed at causing disruption of service to the targets such as the attacks against websites considered well defensed, some ministries, state-controlled television networks, to more sophisticated attacks such as the alleged exfiltration of about 28 GB of sensitive documents from a central bank.

While the hacker groups that joined the cyber theater conflict were thoroughly documented by security researchers, perhaps the most interesting aspect was the involvement of high-profile threat actors, previously known for being financially motivated, into hacktivist campaigns, potentially

rallied by the media attention received by the call to cyber retaliation against one state, made by the Anonymous collective.

From a threat research perspective, the apparent swiftness through which threat actors switched their focus from purely financially motivated campaigns towards another motivated hacking should be taken into account when one is to analyze the true motives of a cyber threat actor and the nature of the cyber incident that they caused.

The means through which the actors finance their operations represents another interesting aspect that, while clear to define for common cyber criminals and nation state sponsored hackers, needs a more thorough analysis in case of threat actors that operate in the hacktivist sphere. We will continue to bring into the discussion some key ideas on the means through which hacktivists finance their operations and attack infrastructure.

4.1. From recognition to funding

As we already know, in the past there was little or no information about how the hacktivist groups are funded to carry out certain actions.

We may say that this is the first time when on the internet appears clear information about a hacktivist organization that is now funded, indeed, through crowdfunding, for a specific reason. Even if we all know that the main scope of hacktivists it's a motivation made by a cause that can be economical, political or social: from disclosing embarrassing information's about some celebrities or political figures, by warning companies about their inside vulnerabilities, by highlighting human rights, to intercepting and tracking groups whose ideologies they do not agree. Usually, these groups' main purpose is based on an ideological and altruistic motivation, such as freedom of speech or social justice. These groups usually disrupt services as a primary goal in order to bring attention to a political or social cause.

An international war incident triggered a huge increase of crypto donations to resistance groups and has raised over $4M in cryptocurrency since one state intensified its attacks.

As we all know, cryptocurrencies have never fulfilled their main purpose when they were launched as the quotidian currency for buying daily goods, or, at least not until today, even some companies adopted this kind of payment. Moreover, this method of payment, regulation-resistant even today, offers the possibility of sending large amounts of money anywhere in the world, including to a war zone in an anonymous format.

Cryptocurrency payments made to military and hacktivist groups aimed at countering aggression against states that fell victim to outside aggression had a sudden increase, especially in the second half of 2021.

Payments number to those organizations made using crypto coins like Bitcoin, Litecoin, Ether or other types of cryptocurrencies acquired through crowdfunding reached a cumulative value of more than $500.000 last year, compared with 2020, when the value was around 5.000 $ and less still in previous years.

This kind of donations had begun to increase rapidly in the 2nd half of 2021, when many hacktivist groups like Come Back Alive [8] managed to raise around to $200,000, and another group called Ukrainian Cyber Alliance received $100,000 worth of crypto [9] all after crowdfunding campaigns were promoted. Another group known as the Myrotvorets Center raised $237,000 but started to raise again with the actual events.

Activists have utilized these funds to buy goods or products such as: medical supplies, military equipment, or advanced technologies like drone-based reconnaissance, as well as funding the development of a facial recognition application with the main scope to identify mercenaries or spies.

These crowdfunded million dollars is just a small part of the total amount of funds obtained with the scope of defending that was managed to be tracked by cyber specialists, and hacktivism groups had to raise funds through more traditional means. The sudden increase of cryptocurrency

donations around the world demonstrates how borderless, often unregulated crypto payments could fund well-intentioned or less well-intentioned organizations involved in actual or future conflicts.

For most of these kinds of fundraising campaigns, payments through cryptocurrencies can represent a small part of the funds that these type organizations receive from donors. Most of the donations were received through traditional payment methods, such as online payments services or bank wires, says Elliptic, one of the most known companies in the crypto funding investigation field.

However, for cyber specialists, cryptocurrency has made its reputation as a robust and more popular alternative against traditional payments. In some cases, blockchain owners or financial institutions had closed accounts belonging to this kind of organization with the main scope as fundraising campaigns, but similar operation may not be validated also for crypto wallet. Cryptocurrency is also particularly suited to cross-border donations, allowing donors all around the world to sponsor hacktivist or cyberterrorist groups.

4.2. Cyber Weaknesses

In a recent report [7], even one of the most powerful states known for its reputation on cyber zone faced significant challenges in cyber operations in 2022, even if it's well known for its capabilities and high operational tempo.

Many of these challenges are not unique, but raise hurdles to further growth of that state's cyber operations. Like other government agencies, security services face challenges recruiting qualified personnel.

Private sector opportunities and rival agencies compete for talent, a problem that can be found all around the world these days. As noted, this often causes security services to outsource operations to civilian and criminal hackers.

Most powerful nation states are implying significant resources and time to achieve strategic cyber advantage to advance their national interests, intelligence-gathering capabilities, and military strength through espionage, disruption and theft.

The security of the services and information about the citizens and partners that the government agencies have is a challenge, the security of these data being paramount and being their responsibility.

Therefore, the importance of this data and essential services is besieged by cyber-attacks on their integrity, being targeted by persevering actors who use sophisticated techniques, but also by cyber criminals who try to earn a little in an easier way and less effort as possible.

It's critical for government networks to both do the basics in terms of cybersecurity and vulnerability management. As the speed of information technology gets more advanced day after day, thread actors and their used method of attack are getting more complex and sophisticated, but, by integrating and implementing up-to-date security policies, governments can more effectively secure their assets

5. Results and Discussions

According to a recent report published by Shimon Noam Oren [10], the year 2021 registered a noticeable increase in the complexity of cyber-attacks with an observed 125% increase in all threat types combined. As the cyber threat landscape continues to expand, so does the complexity behind the motivation, capabilities and objectives of the threat actors that operate in cyberspace. Given the aforementioned fact, the analysis efforts have to take into account all these developments when working towards the successful profiling of threat actors and towards their classification as either financially motivated, state sponsored or hacktivists.

While threat actors involved in hacktivist campaigns usually prefer to communicate through popular social media platforms, these last few months brought forward an interesting shift in the behavior of some actors which were previously observed mostly in the cyber underground on

cybercriminal forums or on chat groups hosted on different instant messaging applications. Those aforementioned actors, some of which were previously known to be mostly financially motivated, registered a sudden shift in motivation, getting involved in the ongoing hacktivist campaigns ignited by the current international context.

While we presented an overview on hacktivism and on the most recent shifts in cyber threat actors' motivation, influenced by world events, there are still several key points which need to be further elaborated in separate discussions if we are to further solidify a threat analysis model, such as the collection of huge amounts of data available across several communication channels used by threat actors as well as financing models associated with each type of cyber threat actor.

6. Conclusions

Even though, in its most basic form, we can simply define hacktivism as breaking into computer systems for political and social reasons or as a form of civil disobedience against the government, we must take into account the diverse and complex facets of hacktivism when researching groups that operate in this sphere. Aspects such as technical sophistication, campaign objectives as well as financing methods are paramount to the correct profiling of hacktivist cyber threat groups.

This paper also highlights the apparent paradox of decentralization that is mostly predominant in the cyber campaigns executed by the Anonymous hacking collective, which, despite the lack in a centralized form of leadership and command structure, was proven to be able to rally several hacking groups and individuals that operated across multiple sectors of the cyber threat landscape in seemingly well-coordinated, politically motivated campaigns.

References

[1]. Francis, J. R. D. (1976) Supervision and examination of higher degree students, Bulletin of the University of London, 31: 3-6.
[2]. Hacktivism and Cyberwars: Rebels with a Cause. Tim Jordan and Paul Taylor, 2004.
[3]. "Hacktivism": about the origins, meaning and history of online Activism. FirstLinePractitioners. Available: https://www.firstlinepractitioners.com/hacktivism/.
[4]. Responses to Cyber Terrorism. Centre of Excellence Defence against Terrorism, 2008.
[5]. Hacktivism 101: A Brief History and Timeline of Notable Incidents. Trend Micro, 2015.
[6]. The Rhetorical Construction of Hacktivism: Analyzing the Anonymous Care Package. Heather Suzanne Woods, B.A., 2013.
[7]. Come Back Alive. Available: https://www.comebackalive.in.ua/.
[8]. NGOs turn to bitcoin to browdfund the Fight Against. Available: https://www.reuters.com/technology/crypto-donations-soar-groups-backing-ukraines-government-report-2022-02-08/.
[9]. CRS Report R45415, U.S. Sanctions on Russia, coordinated by Cory Welt; CRS Report R46616, Russian Military Intelligence: Background and Issues for Congress, by Andrew S. Bowen. Available: https://sgp.fas.org/crs/intel/R46616.pdf.
[10]. Cyber Threat Landscape Report 2022: Summary & Predictions. Available: https://www.deepinstinct.com/blog/2022-cyber-threat-landscape-report.