Handling Internet Activism During the Russian Invasion of Ukraine: A Campus Network Perspective

MARTIN HUSÁK, MARTIN LAŠTOVIČKA, and TOMÁŠ PLESNÍK,
Masaryk University, Czech Republic

The Russian invasion of Ukraine in 2022 raised an enormous wave of Internet activism and distributed denial-of-service (DDoS) attacks launched with the help of common users across the world. In this article, we describe the events of the first days after the invasion from the perspective of the cybersecurity incident response team of Masaryk University in the Czech Republic. We observed hundreds of users intentionally participating in DDoS attacks against Russia from the university's network. The campus network faced only minor issues in terms of service unavailability, but alerts flooded the cybersecurity team. Two dimensions of the events are highlighted. First, the large-scale attacks in an unexpected direction were highly unusual and brought technical challenges in network monitoring and intrusion detection. Second, hacktivism still violates the campus network's terms of use and requires the cybersecurity team to communicate the issues very carefully with the community.

CCS Concepts: • **Networks** → **Network security**; • **Security and privacy** → **Denial-of-service attacks**; **Human and societal aspects of security and privacy;**

Additional Key Words and Phrases: Internet activism, DDoS, incident handling, campus network

ACM Reference format:
Martin Husák, Martin Laštovička, and Tomáš Plesník. 2022. Handling Internet Activism During the Russian Invasion of Ukraine: A Campus Network Perspective. *Digit. Threat.: Res. Pract.* 3, 3, Article 17 (September 2022), 5 pages.
https://doi.org/10.1145/3534566

1 INTRODUCTION

The Russian invasion of Ukraine in 2022 was a major event in the physical world and cyberspace. Numerous examples of cyber attacks attributed to Russia were discussed in the past, including the disruptive attacks on Ukrainian power grids [10] or widely discussed attacks on Estonia [9]. Such events could be considered acts of cyberwar between countries. The invasion opened another front by raising an enormous wave of Internet activism [7]. Probably the most publicized was the declaration of war on Russia by Anonymous [2] and the subsequent cyber-attacks by the hacking group. However, Internet activism also appeared in the form of community-driven **distributed denial-of-service (DDoS)** attacks in which everyone could participate. Simple websites facilitating participation in DDoS attacks appeared shortly after the invasion and were used by many common

This research was supported by ERDF "CyberSecurity, CyberCrime, and Critical Information Infrastructures Center of Excellence" (Grant No. CZ.02.1.01/0.0/0.0/16_019/0000822).
Authors' address: M. Husák, M. Laštovička, and T. Plesník, Institute of Computer Science, Masaryk University, umavská 416/15, 602 00, Brno Czech Republic; emails: husakm@ics.muni.cz, lastovicka@ics.muni.cz, plesnik@ics.muni.cz.

2576-5337/2022/09-ART17 $15.00
https://doi.org/10.1145/3534566

users worldwide. Similar community-driven DDoS attacks were seen in the past; an example is Operation Payback by Anonymous [12].

In this article, we describe the events of the first days after the invasion from the perspective of CSIRT-MU,[1] the cybersecurity incident response team of Masaryk University in the Czech Republic. Masaryk University[2] is one of the largest in the Czech Republic, with over 30,000 students, 6,000 employees, and 30,000 actively communicating IP addresses observed daily. CSIRT-MU operates network monitoring and intrusion detection infrastructure and provides the services of incident handling and incident response with the capabilities to mitigate cyberattacks on the network level. Moreover, the cybersecurity team enforces cybersecurity directives and raises cybersecurity awareness among users. As we show later in this article, the "soft" part of the team played a significant role in handling the situation in the campus network after its users joined the community-driven DDoS attacks. While there were not many technical challenges in handling the events, the actions of users, albeit well-intentioned, posed a violation of the campus network's terms of use and had to be communicated very carefully to the users with respect to the statements by the university's top management.

This article is composed of four sections. After the Introduction, in Section 2, we present a timeline of events in the first days after the invasion from the perspective of the campus network's cybersecurity team. Subsequently, in Section 3, we discuss various aspects of the events, including the effects on the network, risks to the users, and activities of the cybersecurity team. Section 4 concludes the events and lessons learned.

2 TIMELINE OF EVENTS

Thursday, February 24

- The Russian invasion of Ukraine starts early in the morning.
- At 11:55, a massive DDoS against one IP address in the campus network is detected and mitigated. The event is confirmed as a cybersecurity incident, but no link to the events in Ukraine is found. The cybersecurity team of the campus network is on alert.
- At 12:07, tens of alerts announce network scanning on several ports. The investigation concluded it was caused by a misconfiguration in a teaching room. Coincidentally, it was the first class in that room in the new semester. Although this was a non-security issue, the cybersecurity team is on high alert.
- In the afternoon, the university activates crisis management and intensively monitors the situation.

Friday, February 25

- The cybersecurity situation in the campus network is calm.

Saturday, February 26

- The users join activist, community-based DDoS attacks against Russia. Typically, a user connects to the network (via VPN from home or Wi-Fi at dormitories) and joins social networks, namely, Facebook, where other users share links to web pages allowing the DDoS attacks. While the user has the web page opened in a browser, the script on the web page generates requests on the web pages of Russian institutions, news websites, banks, or energy infrastructure.

Sunday, February 27

- The total number of cybersecurity incidents over the weekend is 169. The cybersecurity team commences a deeper analysis.
- The DDoS attacks against Russia seem to no longer be effective due to mitigations by the Russian side. Still, the users continue in the activity.

[1] https://csirt.muni.cz/?lang=en.
[2] https://www.muni.cz/en.

Table 1. Duration of Individual Involvements in DDoS Attacks

	Duration (ms)	Duration	# of targets
Average	6,407,303	1:46:47	47.2
Maximal	86,620,532	24:03:41	603
Minimal	11,503	0:00:12	1
Median	1,520,107	0:25:20	39

Monday, February 28

- The DDoS attacks are observed to originate also from teaching rooms at multiple faculties and departments.
- The cybersecurity team informs the university management and awaits an official statement.
- It is decided that the users will only be warned about the risks, not persecuted.
- An automated system to report specifically participation in DDoS attacks against Russian targets is deployed.

Wednesday, March 2

- The cybersecurity team releases a warning and distributes it within the university. The warning [5] explains the actions of users, pinpoints the risks, appeals to users to not use the campus network, and draws attention to the directive on using the campus network [11].
- In total, more than 400 incidents caused by around 130 unique users were detected during the first week. See Table 1 for a detailed breakdown of the duration of individual involvement in the attacks.

3 DISCUSSION

In this section, we discuss the events from several viewpoints. First, it is worth mentioning the motivation of the users to participate in such attacks. People worldwide were shocked by the invasion, and many soon started finding ways to help Ukraine, making public statements, organizing and contributing to charity, and many others. The anti-Russian sentiment and willingness to help Ukraine were, in this case, multiplied by two factors. First, the academic community is very receptive and active in such situations. University's top officials condemned the invasion right on February 24 [3]. Second, there is a long-standing strong anti-Russian sentiment in the Czech Republic given by historical events (e.g., the Warsaw Pact invasion of Czechoslovakia in 1968) or the recent discovery of Russian involvement in the explosion of ammunition warehouse in the Czech republic [6]. Under such circumstances, it is no surprise that the people were actively seeking any form of retaliation, including community-driven DDoS.

The attacks were executed via simple websites containing a simple JavaScript code. After a user accessed the website, the script started sending requests to several Russian targets. All the users had to do was have the website opened in their browsers, which makes it even simpler to use than well-known tools like **low-orbit ion cannon (LOIC)** [12]. Some of the websites also displayed information on the availability of the targets to inform the users if the attack was successful. However, at the same time, two risks to users emerged in the form of illegitimate attack websites and applications. Illegitimate websites claimed they conduct DDoS attacks but instead mined cryptocurrency on the host computer. The illegitimate applications were a more serious threat, because they started collecting information (e.g., credentials) on the host system and its users. For an unskilled user, it was very difficult to distinguish between a genuine and forged application. We may assume that the number of users willing to participate in the attacks was even higher, but some used illegitimate attack websites and applications.

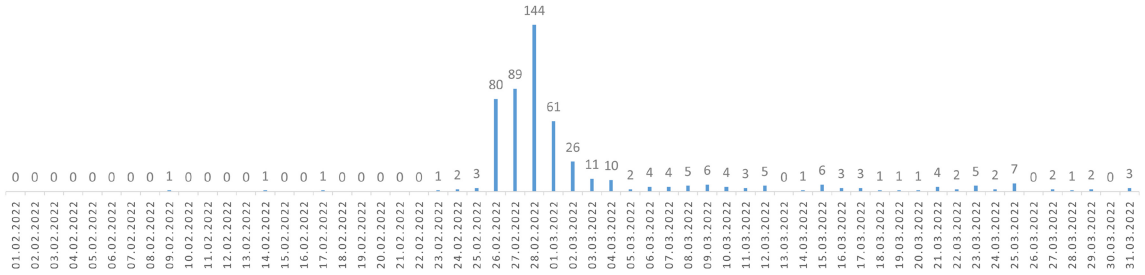

Fig. 1. Numbers of all confirmed incidents originating from the university network during February and March 2022.

The impact of the attacks on the campus network was low. Despite the number of actors and incidents observed, the total volume of network traffic from the campus network to the Russian Federation did not exceed tens of MB/s, so no link saturation or other disruptions were observed. Nevertheless, users connected to the network via Wi-Fi or VPN could decrease the quality of service of Wi-Fi access points and VPN concentrators. A more serious threat was the possibility of revenge actions by hacking groups publicly supporting Russia, such as The Conti Team (operators of the Conti ransomware) [4].

The challenges for the cybersecurity team were primarily non-technical. One of the technical issues was that the attacks were executed in the opposite direction than expected, i.e., from the campus network. Attacks from this direction are caused mainly by an infected device or a compromised account leading to cyber defenses, and intrusion detection is more likely tuned to detect threats from the outside. However, they were caused by hundreds of malicious insiders in this case. As users intentionally participating in cyber attacks are extremely rare, the processes for handling such situations are insufficient, and the security personnel has no experience with it. Apart from that, there was a need to promptly create a category of cybersecurity incidents and design specific (semi-)automated incident response.

To put the volume of attacks into a context, we provide an overview of the number of security incidents originating from the university network in Figure 1 where the distinction between before and after the invasion is evident in the two months period. Even after the initial wave of attacks calmed, the number of incidents remains highly elevated compared to the pre-war era, and the security team needs to stay on high alert.

A major legal consideration was that deliberate participation in a DDoS attack might violate the law. However, this is complicated under the Czech jurisdiction. For example, the § 230 Act No. 40/2009 mentions the denial of service only after an intrusion, not as a stand-alone event. Nevertheless, participation in the attacks is definitely a violation of the Masaryk University Directive No. 10/2017 on the use of information technology [11].

There were numerous challenges for the cybersecurity team. First, the nervousness and uncertainty in the first days were significant, and any unusual incidents were examined as related to the situation. Thus, many incidents were investigated more carefully but possibly in the wrong direction. The situation further escalated during the weekend when there were no handlers on duty (the team operates 8/5), and there was a need to gather incident handlers and decision-makers who would respond 24/7. When the incident escalated, the head of the cybersecurity team reported the events to the university's top management. Such direct communication is rare and a sign of well-executed crisis management. The top management decided not to charge anyone with violating the law or internal directive but instead to raise awareness of the risks of participating in the attacks. While the technical means were deployed on the same day as the decision was made, it took the PR specialists of the team several days to write an article about the situation. The article in Reference [5] was published on university websites and social media after a week; it explained the risks and appealed to users not to use the campus network for such actions. Nevertheless, the actively participating users were already being notified via email since Monday, February 28, and the number of incidents dropped after that day (see Figure 1).

4 CONCLUSION

We described a situation in which a large number of users of a campus network deliberately participated in DDoS attacks against targets in Russia in response to the Russian invasion of Ukraine. Such a situation was unknown to the cybersecurity team that handled the situation, although this is a common sight in cybersecurity operations. Although only a negligible impact on the network was observed, the series of events illustrated how crisis management, direct communication with the organization's management, and public relations are crucial for the cybersecurity team. We may only confirm how situational awareness and mature decision-making are critical for incident response [1]. In fact, the influencing factors in incident handling vastly extended the traditionally perceived borders of so-called cyber situational awareness [8].

In conclusion, we address several issues that are, in our experience, insufficiently developed in cybersecurity teams. First, the non-technical measures, such as crisis communications and PR, are as important as technical measures. Second, detecting attacks from within the team's constituency might be neglected. Finally, certain aspects of "expecting the unexpected," such as defining new incident categories and rapidly deploying new procedures, could be trained.

REFERENCES

[1] Atif Ahmad, Sean B. Maynard, Kevin C. Desouza, James Kotsias, Monica T. Whitty, and Richard L. Baskerville. 2021. How can organizations develop situation awareness for incident response: A case study of management practice. *Comput. Secur.* 101 (2021), 102122. https://doi.org/10.1016/j.cose.2020.102122

[2] Anonymous. 2022. The Anonymous collective is officially in cyber war against the Russian government [Twitter post]. Retrieved from https://twitter.com/YourAnonOne/status/1496965776435926039.

[3] Martin Bareš. 2022. Statement of rector of Masaryk University on war in Ukraine. Retrieved from https://www.em.muni.cz/en/news/14822-statement-of-rector-of-masaryk-university-on-war-in-ukraine.

[4] Christopher Bing. 2022. Russia-based ransomware group Conti issues warning to Kremlin foes. Retrieved from https://www.reuters.com/technology/russia-based-ransomware-group-conti-issues-warning-kremlin-foes-2022-02-25/.

[5] CSIRT-MU. 2022. War and chaos in cyberspace: CSIRT-MU advises what to be careful about. Retrieved from https://csirt.muni.cz/about-us/news/valka-a-chaos-v-kyberprostoru-csirt-mu-radi-na-co-si-dat-pozor?lang=en.

[6] Mike Eckel, Ivan Bedrov, and Olha Komarova. 2021. A Czech explosion, Russian agents, a Bulgarian arms dealer: The recipe for a major spy scandal in Central Europe. Retrieved from https://www.rferl.org/a/czech-expulsions-bulgaria-gebrev-russia-gru-intelligence-explosion-spy-scandal/31209960.html.

[7] Jordana J. George and Dorothy E. Leidner. 2019. From clicktivism to hacktivism: Understanding digital activism. *Info. Organiz.* 29, 3 (2019), 100249. https://doi.org/10.1016/j.infoandorg.2019.04.001

[8] Robert Gutzwiller, Josiah Dykstra, and Bryan Payne. 2020. Gaps and opportunities in situational awareness for cybersecurity. *Digital Threats* 1, 3, Article 18 (Sep. 2020), 6 pages. https://doi.org/10.1145/3384471

[9] Stephen Herzog. 2011. Revisiting the estonian cyber attacks: Digital threats and multinational responses. *J. Strat. Secur.* 4, 2 (2011), 49–60. https://doi.org/10.5038/1944-0472.4.2.3

[10] Robert M. Lee, Michael J. Assante, and Tim Conway. 2016. Analysis of the cyber attack on the Ukrainian power grid. *Electric. Info. Shar. Anal. Center* 388 (Mar. 2016), 1–29.

[11] Masaryk University. 2020. Masaryk University Directive No. 10/2017: Use of Information Technology. Retrieved from https://is.muni.cz/do/mu/Uredni_deska/Predpisy_MU/Masarykova_univerzita/Smernice_MU/SM10-17/102278820/MU_Directive_No._10_2017_-_Use_of_Information_Technology.pdf?lang=en.

[12] Molly Sauter. 2013. "LOIC Will Tear Us Apart": The impact of tool design and media portrayals in the success of activist DDOS attacks. *Amer. Behav. Sci.* 57, 7 (2013), 983–1007. https://doi.org/10.1177/0002764213479370

Received April 2022; accepted April 2022