BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Hafnium and the zero-day dilemma. Public-private cyber threat intelligence cooperation

Mihai OLTEANU*

*Doctoral Studies, "Carol I" National Defense University, Bucharest, Romania
e-mail: mihaiolteanu48@yahoo.com

Abstract

Cyber threat intelligence (CTI) plays a crucial role in limiting cybersecurity risks, with a particular focus on identifying and mitigating zero-day vulnerabilities. While academic literature, specialized reports, and normative documents widely argue in favor of cooperation between public and private entities to develop cybersecurity, significant systemic challenges hinder effective intelligence sharing when discussing real-time threats, such as zero-day vulnerabilities.

This article critically examines the dynamics of public-private collaboration in CTI, focusing on the obstacles preventing further development of the level of cooperation, such as trust deficits, legal constraints, financial and reputational risks, and diverging strategic interests. By performing a qualitative analysis on the existing literature and using the Hafnium cyberattack as a case study, the research highlights the complexities surrounding the zero-day vulnerability disclosures and the limitations of existing cooperative frameworks. The findings indicate that while structured CTI-sharing mechanisms exist, real-time collaboration on zero-day vulnerabilities remains constrained by competing incentives that are unlikely to be properly addressed.

Keywords:

Cyber Threat Intelligence; Hafnium; Zero-day Vulnerabilities; Public-private Cooperation.

Article info

Received: 23 June 2025; Revised: 29 July 2025; Accepted: 26 August 2025; Available online: 6 October 2025

Citation: Olteanu, M. 2025. "Hafnium and the zero-day dilemma. Public-private cyber threat intelligence cooperation." *Bulletin of "Carol I" National Defence University*, 14(3): 328-346. https://doi.org/10.53477/2284-9378-25-52

1. Introduction

Multiple types of cyber threat intelligence reports and studies consistently highlight the increased number of cyber-attacks, which excel both in diversity and technical complexity, that require extensive security measures and force authorities to develop cooperation on any given level, be it state-private, international, internal, inter-institutional, state-academia, and so on. There is a common view that is promoted both in the academic and professional areas, and it states that the ever-evolving cyberthreats require adaptive measures and more cooperation of any kind. This perspective has been around for many years. A study published in 2007 argued the need to develop international cooperation between countries and law enforcement agencies to combat and investigate cybercrime (Cerezo, Lopez and Patel 2007). Further away, in 2002, over two decades ago, Lewis argued in favor of a new normative framework that required international cooperation in cybersecurity, considering the continuously growing interdependence between different systems (Lewis 2002). Back in 1995, there were authors who anticipated that the development of the cyber world would seek new ways for cooperation among people (Rheingold 1994). Today, cybersecurity cooperation is inherent to any strategic or pragmatic document, a very high number of formats being created and operationalized, such as the NATO Cooperative Cyber Defence Centre Of Excellence, a hub focused on research and training (Smeets 2022), or Malware Information Sharing Platform (MISP), a platform focused on sharing cyber threat intelligence reports across multiple actors (Wang, et al. 2024).

Therefore, this emphasis on cooperation is not merely theoretical. In practice, the last two decades have sought to bridge the gap between sectors, nations, and actors, though various initiatives with different levels of commitment. Nonetheless, the outcomes of these efforts—whether successful or unsuccessful—require further analysis. Also, it is unclear if the cooperation mechanisms could be further developed.

The ongoing push towards improving the cyber-related cooperation mechanisms highlights a critical point: the main actors in the cyber sphere (namely, states and firms) have not managed to find a satisfactory approach to this matter. There may be multiple reasons, such as different interests or constraints generated by legal and regulatory hurdles (GDPR on one side, and national security on the other), and concerns over intellectual property (Bechara and Schuch 2020). The whole process of cyber threat intelligence sharing gains a higher urgency when it is narrowed down to exchanging data related to zero-day vulnerabilities, flaws in software or hardware that are exploited before developers have managed to find them and, inherently, release a patch (Singh, Joshi and Kanellopoulos 2019). The impact of exploiting this type of vulnerability is profound, both technically and economically, reducing the trust between the parties at the lowest level, considering that core interests such as the reputation of the company and the security of the states are at stake.

This article examines the fundamental challenges surrounding public-private cooperation in cyber threat intelligence sharing, with a focus on the structural incentives driving both sides—why each chooses to share or withhold data. The analysis will specifically address zero-day vulnerabilities, exploring how these unique threats shape the approach to information sharing and the strategies for mitigating the risks they pose.

2. Methodology

The primary objective of this research is to identify the obstacles to sharing cyber threat intelligence in a public-private context and examine how these barriers affect cooperation on zero-day vulnerabilities. To address this, the research adopts a qualitative approach, analyzing existing literature through technical lenses. Additionally, a case study on the Hafnium zero-day campaign will be presented. This case study: (1) illustrates the need for analyzing the success or failure of actual cooperation mechanisms and (2) provides critical insights into the challenges of the strategies for enhancing cooperation on zero-day vulnerabilities.

3. Cyber threat intelligence and zero-day vulnerabilities

Cyber threat intelligence (CTI) is a component of the larger concept of intelligence, with similar features and final goals (Sülü and Daş 2022). CTI has been defined as a field of activity in which data is collected, compared, analyzed, and, finally, disseminated, aiming to better understand the threats, as well as the threat actors that intend to produce damage to different components of the cyber ecosystem (Sun, et al. 2023). It is also considered to be a process that allows organizations or countries to better understand their vulnerabilities (Shackleford 2015).

The whole CTI process enables organizations to think and act proactively in their attempts to understand the risks and threats, as well as take advantage of the opportunities that occur in cyberspace. Therefore, the *raison d'être* of the CTI is to support the decision of stakeholders on different levels, from cyber commanders of cyber operation units to leaders of the countries and CEOs of private organizations (Lanzendorfer 2015). In doing so, CTI uses all sorts of technical data (e.g., IPs, geolocation, traffic, and so on) to understand the kind of attack that occurred, the mitigation measures required, the capabilities of the threat actor, and the existing vulnerabilities (Barnum 2014). CTI is an activity conducted in an attempt to predict threats by anticipating the attacker's next step and their main objectives, as well as the techniques used to fulfill them in the long run. In that sense, a vital component of the CTI relies on finding the existing vulnerabilities before the attacker does, to prevent their exploitation (Schlette, et al. 2021).

In this context, a particular critical and high-risk category of threats is posed by the zero-day vulnerabilities, which are unknown to the producer and, therefore, silently exploited by threat actors until patches are published (Roumani 2021). The challenge

with zero-days is that these are, by definition, known only by the specialist who found them, meaning that traditional defense mechanisms—such as signature-based detection systems—tend to be ineffective (Ahmad, et al. 2023).

The proactive nature of CTI is particularly important when it comes to zero-day vulnerabilities. Identifying and mitigating these vulnerabilities requires a deep understanding of both the threat landscape and the behavior of threat actors. However, the complexity and lack of knowledge introduce significant challenges for CTI (Albanese, et al. 2013). Unlike other threats, zero-days often require an immediate, coordinated response from both private and public sector organizations, making their timely identification and disclosure essential for minimizing damage.

Given their high value both for the offensive and the defensive sides, the zero-day vulnerabilities have become a source of income for researchers who choose to work on identifying and further commercializing them in white, grey, or black markets. The financial value of a zero-day vulnerability is given by multiple factors, the most important of them being, naturally, its secrecy. For instance, researchers may gain up to $3 million if they choose to sell the zero-day vulnerability on the grey market (Meakins 2018) to customers who are aiming to exploit it in their best interest. Over the last two decades, multiple zero-day vulnerabilities were exploited, some of them producing significant damage, such as Shellshock (on Unix and Linux systems), Heartbleed (Internet disruption), and F5 BIG-IP (HTTP requests that allowed code execution) (Teodorescu 2022). A report published by Google and Mandiant revealed that there were 97 zero-day vulnerabilities identified in 2023, 36 of which targeted enterprise-focused technologies (Google, Mandiant 2024).

4. Cyber threat intelligence cooperation

As stated in the introductory part, the nature of the CTI activity (particularly in relation to zero-day vulnerabilities) constantly underscores the need to create cooperative formats and improve the existing ones, so that cybersecurity threats are adequately prevented and mitigated.

Naturally, the need for cooperation has been argued in numerous academic papers that reflect both quantitative and qualitative benefits that might be achieved through such approaches (Pala and Zhuang 2019). In the case of zero-day vulnerabilities, the challenges could be even more pressing. Since these vulnerabilities are unknown to both vendors and defenders until they are exploited, it is unlikely for a singular organization to possess all the necessary information to respond effectively (Homburger 2019). In the absence of a cooperative public-private format, the ability to swiftly respond to and neutralize these threats is likely to be severely compromised.

The most accessible mechanism of cooperation is exchanging cyber threat intelligence reports, as this directly supports information sharing. Exchanging

technical data such as indicators of compromise, attack vectors, or tactics involved has been acknowledged to be a well-established mechanism for building a collective knowledge related to the cyber threat landscape, allowing for a faster identification of the incident and for adequate measures to be implemented in the aftermath (Wagner, et al. 2019). Similarly, in the case of zero-day vulnerabilities, sharing cyber threat intelligence reports is highly probable to support the efforts of each one of the partners in identifying the flaw and providing a timely patch.

The development of early detection capabilities is a direct result of active cooperation among different actors, as this allows different types of organizations to pool their expertise and resources, hence creating a comprehensive monitoring system. Theoretically, both private and public organizations can provide valuable knowledge that is likely to be complementary in multiple areas. While governments may develop more advanced capabilities in understanding state-sponsored cyberattacks, private companies possess much more real-time data regarding the activity of different categories of threat actors (Purohit, et al. 2023). Therefore, combining these two approaches into cooperative formats should provide the necessary links to better detect and prevent cyberattacks. This goes further in the case of zero-day vulnerabilities, as both actors possess the capabilities to identify this kind of flaw through research and bug bounty programs conducted by their technical experts (Arshad, et al. 2024).

Effective sharing data mechanisms can develop the relationship between states and private companies, further allowing them to build trust and, possibly, develop cooperative formats that create the required context for resource-sharing, allowing them to leverage each other's tools, platforms, and expertise. At least from a defensive standpoint, that approach is entirely desirable, as each of the two parties works towards finding suitable mechanisms to better protect their networks (Rajamäki 2017). That is also completely valid in the case of zero-day vulnerabilities, as public-private bug bounty programs are likely to prove themselves more effective and faster in finding hardware or software vulnerabilities.

Moreover, multiple private-public formats have been established, approaching different configurations and various types of actors, aiming to implement security measures and develop resource-sharing efforts. Each of these collaborative formats provides some added value in the fight against cyber threat actors and cyber vulnerabilities, but it is unknown whether or not the maximum level of cooperation has been reached. Considering that academic literature continues to argue in favor of developing cooperative mechanisms, it is likely that there is more room for cooperation, or at least different entities are advocating so.

Up until now, some of the most common formats of sharing CTI are the Information Sharing and Analysis Centers (ISAC), which have been developed across various industries and encourage sharing data related to cyber threats, Computer Security

Incident Response Teams (CSIRT), as well as different organizational structures and online sharing platforms (Wallis and Leszczyna 2022).

An ISAC is a format designed to facilitate the exchange of information related to cyber threats and threat actors, primarily through voluntary communication between different entities. Typically, an ISAC does not require the sharing of real-time technical data, such as traffic logs or malware samples. Instead, its focus is on raising awareness among its members. ISACs are common in organizations that may not yet have established high levels of trust or are not ready to share critical data (Steffensen and Gnanasekaran 2024).

A more advanced format that has been developed is the CSIRT, a mechanism that commonly uses different types of resources in order to prevent, identify, investigate, and mitigate different types of cyber threats. The entities that join a CSIRT, be they public or private, acknowledge the need to commonly share their resources to prevent cyberattacks from damaging their networks (Bada, et al. 2014). Currently, CSIRT is the most common resource-sharing format, encouraged by multiple bodies, with a special focus coming from the European Union, through the legislative mechanisms among its member states, shaped through the Directive (EU) 2022/2555 (NIS 2 Directive), that highlights the need to create a CSIRT for each of the addressed sectors, coordinated by a chosen authority (not necessarily a public one), with sufficient resources to be able to prevent specific cyber threats (European Parliament, Council of the European Union 2022).

Other agencies, such as the European Union Agency for Cybersecurity (ENISA), were established to provide guidance in handling cyber threats and preventing cyberattacks from occurring (Sklyar and Kharchenko 2019). Although it has been the subject of multiple changes over time (both in terms of structure and objectives) and does not currently hold any technical responsibilities, ENISA still manages to collaborate with private and public entities to create reports that highlight good practices and pieces of advice in the field of cybersecurity (Cavelty and Smeets 2023). ENISA stands out as a useful landmark in public-private cooperation, considering that it is an initiative of the public side. In the private area, multiple platforms have been established, and MISP stands out as being one of the most popular among them. MISP allows its members and volunteers to constantly share technical indicators related to cyber threats, such as indicators of compromise, vulnerabilities, and counter-measures (Wagner, et al. 2016).

While these formats provide various cyber threat intelligence sharing mechanisms and a wide range of options for an actor that is willing to cooperate in mitigating and preventing identified cyberattacks, the existing literature highlights that some impediments are still in place and unlikely to disappear. How these affect the chances of cooperation on multiple threats (and, particularly, on zero-day vulnerabilities) is to be addressed in the following chapters, which aim to highlight some systemic

difficulties in developing a more advanced format of cooperation, or, at least, the one that has been constantly pursued in the last decades. The impact of these matters on handling this type of vulnerability is, naturally, the focus point of this analysis and the role of the study itself.

5. Systemic setbacks in expanding the cooperative formats

While the development of cooperation is theoretically expected (as presented in the previous chapter) and sought by both public and private sector actors (at least on a certain level), and its defensive outcomes and benefits cannot be overlooked, the ideal cooperation format cannot be realized in practice. Numerous financial, social, reputational, and legislative barriers are challenging to overcome and will be addressed in this part of the paper.

A study conducted (Lanzendorfer 2015) on the American perspective regarding the CTI industry and the interaction between public and private entities addressed a set of questions to a group of American officials, and the following conclusions were reached:

- 58.82% of the participants agreed that the expertise of cybersecurity organizations surpasses the US Government's knowledge in the field;
- 70.59% trusted the private contractors to deliver effective products for the US Government in the cyber field;
- 58.82% considered that the private industry possesses more knowledge than the US Government concerning cybersecurity.

While this study does not provide a comprehensive analysis regarding the interaction between public and private organizations, it does raise certain perspectives related to the perception of public entities of the private industry. In this sense, it would be obvious that sharing the result of the CTI activity among as many actors as possible would be the right solution in handling cyberattacks (Fischer, et al. 2023). However, there are numerous reasons observed over the last decades against sharing CTI between different types of entities.

5.1. Lack of trust

One of the most important elements that prevents the day-to-day sharing of CTI is the lack of trust among multiple entities in the spectrum of cyber intelligence.

Firstly, the low level of trust in data exchange between public entities is primarily driven by the operational risks associated with sharing intelligence related to ongoing campaigns. Unlike fields such as counterintelligence or counterterrorism, CTI data is most valuable in real-time, as the real risk lies in the potential expansion of a cyber campaign to additional national entities. When exchanging real-time data between public entities, one must take into account the risk that such sharing could jeopardize ongoing CTI investigations. If another authority starts its own investigation, it could alert the attacker to the exposure. To support this, a study published by CCDCoE

pointed out that there are numerous situations in which even written agreements for information sharing among public organizations are not honored by both parties (Tolga 2019). In this scenario, public entities are more likely to share the relevant data only with a limited number of highly trusted partners or at the point at which their investigations are at least partially completed, and sharing would not produce any additional operational risks or threats.

Secondly, the lack of trust is also a problem in sharing data among private organizations, as there are problems related to open market competition and the risk of losing clients. Private organizations are often reluctant to share their data with competitors operating within the same industry, even when there is potential to enhance client services and prevent cyberattacks from compromising networks. While sharing CTI could help prevent the spread of cyberattacks across various sectors and countries, long-term trust between these organizations is unlikely to develop. This is because their primary focus remains on financial interests, which take precedence over collaborative efforts (Hausken 2007). When private companies operate in different sectors, they are more likely to share real-time data, provided that there is a prior agreement in place and a common financial interest. However, this arrangement does little to advance CTI cooperation, as one party will not operate in the field of cybersecurity and, subsequently, would not own any valuable CTI to share, preventing meaningful exchange.

Thirdly, sharing CTI between private and public entities is challenging from several perspectives. First of all, the process of sharing requires each of them to build a high level of trust, as the government will provide sensitive data to the company, and the private organization will share the investigations conducted at its expense. Additionally, sharing valuable CTI could mean that the government has to provide data about its citizens to a private entity, which might be seen as unacceptable by the general society, given that the company's primary motivation is financial. On the other side, the company might be subject to some regulations that prevent it from sharing its clients' data with third parties that have not been initially agreed upon (Sullivan and Burger 2017).

5.2. Lack of quality

A permanent mechanism of CTI sharing is difficult to establish, as no guarantees of reciprocity may ever be implemented. Some authors underlined that one of the problems related to sharing CTI is that a lot of information is outdated and cannot provide true, valuable insights into ongoing investigations, especially considering that there is a lot of public data and reports, while the analyzing tools and resources require time and effort to provide accurate interpretations (Schlette, Böhm, et al. 2020).

Both public and private actors lack assurance that the information shared will lead to a response that genuinely advances investigative efforts, making the burden of overcoming trust and legislative obstacles seem unjustified in some cases.

Moreover, a standardization mechanism, quality-wise, is difficult and unlikely to be implemented between multiple parties, as each entity holds specific resources and tools when conducting cyber investigations. While this obstacle could potentially be addressed between two parties, cooperative mechanisms involving multiple actors are unlikely to succeed, as no homogenous format could be agreed upon.

5.3. Reputational damage

When sharing CTI, both public entities and private organizations risk exposing themselves to either public criticism or the risk of damaging their reputation. Many organizations that faced a major cyberattack that managed to produce substantial damage to their infrastructure are likely to avoid making their investigation public soon, as there are multiple risks involved: (1) their clients may consider that there was a lack of cybersecurity measures which allowed their data to be endangered and could decide to end the collaboration with the company (Perera, et al. 2022); (2) the private organization may face competitive disadvantages if the information about a cyber campaign goes public, as their rivals will try to prove that they have a higher level of cybersecurity (Lanzendorfer 2015); (3) both private and public organizations may face the risk of being heavily targeted in the near future, as they acknowledge the lack of proper security measures (Kamiya, et al. 2018). Essentially, governments could face similar challenges, as real-time disclosure can fuel public panic and erode trust in their ability to protect critical infrastructure.

These risks, while not inherent to collaboration, underscore why entities often avoid sharing real-time data during a cyberattack. Post-factum threat reports remain a safer alternative, though their value and consistency may still be influenced by the same underlying concerns. Balancing transparency with these risks is a persistent challenge in the evolving landscape of cybersecurity.

5.4. Lack of standardization

Both public and private entities tend to avoid sharing CTI as there is no standardization framework for building the CTI reports, making them difficult to use in the case of a real-time cyber campaign. Different authors argued that the lack of standardization in the CTI industry is making the whole process of sharing data highly ineffective (Silva, et al. 2020), while many of them provide new or innovative formats for standardizing the information sharing (Tounsi and Rais 2017), which, however, were not adopted widely across the industry.

The whole problem related to the lack of standardization is that the efforts of sharing CTI among different public and private organizations and the risks that derive from this process are not worthwhile if there is no guarantee that the outcome will be useful in conducting the cyber investigation and protecting the network (Serrano, Dandurand and Brown 2014). Therefore, as no clear gains are guaranteed, it is burdensome to argue in favor of sharing critical data that is time sensitive and highly valuable, when lacking any incentive related to solving the cybersecurity crisis or limiting the damages.

5.5. Legislative problems

The entire process of sharing CTI is quite difficult, considering that some legislative measures prevent this activity, especially in the case of private organizations sharing their clients' technical data. The General Data Protection Regulation (GDPR) governs activities within the EU and specifically outlines the limitations and conditions for sharing citizens' personal data, which may include cyber-related indicators, such as users' IP addresses (Albakri, Boiten and Lemos 2018). GDPR defines personal data as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data,* ***an online identifier*** *or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*" (European Commission 2016). While GDPR works on safeguarding the data of European citizens, it clearly limits the possibility of sharing with third parties any information that may be labeled as personal data, hence reducing the real-time CTI sharing capabilities.

An extensive investigation on the impact of GDPR on CTI sharing was conducted by Albakri, Boiten, and Lemos, who concluded that companies can exchange personal data related to cyberattacks only with certain public authorities, using encryption mechanisms (Albakri, Boiten and Lemos 2019).

5.6. Different interests

As both public and private entities pursue different endeavors and describe their objectives significantly differently, the real-time CTI cooperation is affected too; some core limitations negatively impact any cooperation format. Typically, private companies prioritize their profits, hence choose to support initiatives that promise returns at least proportionate to their initial investments. Their focus is often on addressing major, high-profile threats that could lead to significant financial losses or reputational damage, such as destructive attacks, espionage or massive cyber-criminal campaigns (Maschmeyer, Deibert and Lindsay 2020). This focus can lead to reluctance in sharing CTI with public entities, as the information related to the "big fish" is highly valuable.

In contrast, governments would choose to prioritize any investigation that could provide real-life added value in society by protecting the majority of the population, as well as organizations and firms of any size. For instance, a "small fish" such as a phishing campaign may seem unattractive to private actors but essential to state authorities, as they may prove to affect a wider part of the population. In that sense, governments are willing to fund investigations that do not seem to be profitable from a financial point of view (Tropina 2015).

This discrepancy in interests – profit-driven motives versus national security objectives – shapes an important barrier in effective cooperation related to CTI.

Meaningful data sharing is less likely to occur in any situation that faces two different perspectives and a separate set of measures. Surely, in the case of a campaign that is of interest to both sides, it is more likely to see a fruitful cooperation, but that type of situation is rather isolated, considering the perspective presented above.

6. Navigating the challenges of disclosing and sharing zero-day vulnerabilities

Although the discussion related to sharing CTI seems pretty straightforward because there is a clear set of benefits as well as some strong risks or disadvantages related to public-private cooperation, that is not the case with exchanging zero-day vulnerabilities, as these tend to be seen differently, considering their value and scarcity.

The advantages of sharing CTI and improving cooperation that were presented in Chapter 4 do not entirely mirror the approach related to zero-day vulnerabilities. Most of the advantages of cooperating rely on post-factum information exchange or preventive collaborative formats in regard to cyberattacks. Therefore, from a defensive point of view, cooperation seems like an adequate recipe. Still, in the case of public-private zero-day exchanges, two main problems arise: (1) on the side of the public entity, why should the authorities freely provide such a valuable vulnerability to a private entity, sacrificing its secrecy against its own interest? (Bilge and Dumitraș 2012) and (2) on the side of the company, why should it share the zero-day and risk of having it exploited instead of patching it? The whole debate seems like a zero-sum game, in which neither of the actors has clear reasons to believe that both players will win. The entire list of advantages used by different entities to promote CTI sharing is not valid in case of a singular vulnerability, most likely unknown by any other actor that could provide significant strategic advantages. No level of trust can compensate for sharing such an important asset with an actor that, as explained previously, has different views and objectives.

Moreover, on the side of the private entity, there is another essential question, namely: with whom to share the zero-day vulnerability? While the public-private discussion seems to refer to two actors, in reality, the number is significantly higher. The great companies conduct their cybersecurity operations and commercialize their products in a large number of states, meaning that a fair cooperative initiative would require them to announce all of their partners (namely, all of the different states) that it has found such a zero-day vulnerability and expect them to act rightfully. That oversteps any financial interest and business strategy, as the value of the asset will significantly drop, while also risking its exploitation (Roumani 2021).
Besides, the reputational damage of the company is still in place, considering that sharing such an important flaw in their hardware or software product with the risk of it going publicly might significantly affect the trust of the customers and, furthermore, its financial interests in the long run (Ekong, et al. 2023).

Another problem that arises from the argument exposed in the 5.2 chapter is that of quality and reciprocity. It is difficult (if not impossible) to build the required trust mechanisms that would work in such a way that either the public authority or the private actor would have the confidence that a mirrored situation would produce a similar outcome (Schulze and Reinhold 2018) and, conclusively, decide to share a newly found zero-day vulnerability.

More progress could be made on the side of public authorities, especially states that are part of common organizations. The European Union tries to encourage the efforts towards programs of Common Vulnerability Disclosure, as this is a part of the NIS2 Directive, that regulated some mechanisms to protect the researcher that identified the vulnerability, and encourages member states to share their findings inside the EU, then with the private entity and, finally, publicly, when a patch has been developed (European Parliament, Council of the European Union 2022). Still, it is unlikely that a similar approach would be adopted on the side of private companies, which are likely to maintain the status quo, which consists of identifying zero-days and only sharing them (with partners, or publicly) when the proper security update has been created and tested.

7. Hafnium: Case Study on the Exploitation of Zero-Day Vulnerabilities

The Hafnium cyberattack, first identified at the beginning of 2021, represents one of the most significant and widespread security breaches in recent history, based on zero-day vulnerabilities. The campaign was publicly attributed to a China-based advanced persistent threat group (NATO 2021) and consisted of exploiting vulnerabilities in Microsoft Exchange Servers, managing to produce a significant impact worldwide. The cyber threat actors successfully gained unauthorized access to systems and email servers, stole sensitive data, and deployed advanced malware that could be exploited for a long period of time (Waheed, et al. 2024).

The campaign was based on the complementary exploitation of four zero-day vulnerabilities found by Chinese hackers and used for several months in a row. The zero-day vulnerabilities allowed the attacker to:

- Authenticate to the Microsoft Exchange servers that allowed stealing the content of the mailboxes through CVE-2021-26855 (Server-Side Request Forgery);
- Gain access to voice mail functionality, if administrator privileges are previously obtained, through CVE-2021-26858 (Insecure Deserialization);
- Write files (potentially malicious ones) on the compromised servers through CVE-2021-26858 and CVE-2021-27065 (Arbitrary File Write) (Narang 2021).

There are different estimations on the global damage that was produced, but several public sources claim that the Hafnium campaign managed to compromise between

10.000 and 250.000 Microsoft customers, including businesses and governmental agencies. Moreover, Microsoft inflicted severe reputational damage after this cyberattack that was based on vulnerabilities, with US-China relations also estimated to be affected (Bates 2022).

On the 2nd of March 2021, Microsoft published a communication entitled "New nation-state cyberattacks" describing the cyber threat actor dubbed Hafnium, as well as the fact that it exploited some "previously undiscovered vulnerabilities" in the products commercialized by the American company. It also stated that it briefed the U.S. government about the incident and that it was helped by other companies to address the vulnerabilities (Burt 2021). This was the first moment in which Microsoft acknowledged the existence of zero-day vulnerabilities and their exploitation. On the same day, it publicly released some patches to address these vulnerabilities, which were then updated constantly to prevent any further damages (Microsoft 365 Security 2021).

Different public sources point out that Microsoft was warned about the vulnerabilities at least two times, by different cybersecurity companies, since January 2021. Initially, Volexity saw the attackers quietly exploiting the zero-day vulnerabilities and communicated this to Microsoft. In February, before the official acknowledgment made by Microsoft, Volexity saw massive exploitation of the same vulnerabilities (Krebs 2021). Moreover, at least one more private entity told Microsoft about the active exploitation of the zero-day vulnerabilities in January 2021 (Robinson 2024).

7.1. What did Hafnium highlight?

After looking into the specifics of the Hafnium case, some ideas may be outlined in support of the points previously made regarding the cooperation on the zero-day cybersecurity vulnerabilities.

Q: Did Microsoft share the insight on the existing zero-day vulnerabilities?
A: Yes, but only after it developed a security patch. As pointed out in Chapter 6, although there were several pieces of evidence that pointed out that Microsoft was aware of the zero-day vulnerabilities before going public and sharing the insights, it chose to do so only when a patch had been developed. In doing so, it proved that its interest was, first of all, reputational (and, therefore, financial) because Microsoft chose to maintain the secrecy about the actively exploited vulnerabilities in an attempt to, most likely, avoid losing clients by admitting the problems without having a practical solution. For the general victims, it is likely that a public statement made before the 2nd of March would have been more helpful in implementing mitigation measures and, conclusively, limiting the number of compromised servers. However, Microsoft acted in its own interests, namely, protecting its financial objectives.

Q: Was there active cooperation between private actors?
A: Yes and no. On one side, multiple private entities, such as Volexity, chose to

cooperate by informing Microsoft about the zero-days, but only because they could not exploit them in their own interests; therefore, they did not compete in this matter. On the other side, Microsoft's communication from the 2nd of March did not include any form of cooperation in developing the patches with other private cybersecurity companies, although it is likely that the update would have been developed earlier. One possible reason could be that a cooperative approach would force Microsoft to admit that it was unable to single-handedly deal with the zero-days and needed to cooperate with a competitor.

Q: Was there active cooperation between public and private actors?
A: No. While Microsoft knew about the vulnerabilities, it only chose to brief the US government, while all the other states that use its technology were unaware of the zero-days. As pointed out in Chapter 6, sharing this kind of data in real-time with all the public authorities is unlikely, as it is not in the company's best interest. Therefore, governmental networks were compromised, as no state other than the US was able to implement preventive measures.

Q: Was there active cooperation between public actors?
A: It is unknown. There is no public evidence that any other state, besides the US, knew about the Hafnium campaign. Moreover, the high number of victims worldwide could underline that states were not able to implement timely defensive measures.

Conclusions

This analysis, directly supported by the Hafnium case study, highlights the obstacles in sharing zero-day vulnerabilities between all sorts of actors. While such cooperation could provide more timely measures (as the Hafnium campaign highlights), the main arguments behind this situation are systemic and unlikely to be overcome in the long run. The fundamental difference in the core interests of the states and private companies converges to a lack of extensive cooperation in dealing with real-time data, specifically focused on zero-day vulnerabilities.

Although several formats try to address this matter, their success is questionable, as well as their improvement perspectives. Volexity proves that a certain amount of cooperation is definitely possible when non-competitive interests are in place. Microsoft demonstrated that proactively cooperating with partners and promoting its financial interests are two mutually exclusive approaches. The fundamental misalignment of incentives between public and private actors indicates that a fully cooperative cybersecurity model remains difficult to achieve. While initiatives like public-private partnerships and information-sharing platforms provide some progress, they do not fully address the deeper systemic issues that have been presented in the previous chapters.

However, the active real-time cooperation between Microsoft and the US government in regard to Hafnium needs to be studied, as it creates the premises of a situation in which it seems that the company overstepped its financial interest and cooperated with an official body.

References

Ahmad, Rasheed, Izzat Alsmadi, Wasim Alhamdani, and Lo'ai Tawalbeh. 2023. "Zero-day attack detection: a systematic literature review." *Artif Intell Rev* 10733–10811. https://doi.org/10.1007/s10462-023-10437-z.

Albakri, Adham, Eerke Boiten, and Rogério De Lemos. 2018. "Risks of Sharing Cyber Incident Information." *Proceedings of the 13th International Conference on Availability, Reliability and Security* 1-10. https://doi.org/10.1145/3230833.3233284.

—. 2019. "Sharing Cyber Threat Intelligence Under the General Data Protection Regulation." *Privacy Technologies and Policy 7th Annual Privacy Forum, APF 2019.* Rome, Italy: Springer. 28-41. https://doi.org/10.1007/978-3-030-21752-5_3.

Albanese, Massimiliano, Sushil Jajodia, Anoop Singhal, and Lingyu Wang. 2013. "An efficient approach to assessing the risk of zero-day vulnerabilities." *International Conference on Security and Cryptography (SECRYPT).* Reykjavik, Iceland: IEEE. 1-12.

Arshad, Junaid, Muhammad Talha, Bilal Saleem, Zoha Shah, Huzaifa Zaman, and Zia Muhammad. 2024. "A Survey of Bug Bounty Programs in Strengthening Cybersecurity and Privacy in the Blockchain Industry." *Blockchains* 2 (3): 195-216. https://doi.org/10.3390/blockchains2030010.

Bada, Maria, Michael Goldsmith, Chris Mitchell, and Elizabeth Phillips. 2014. "Improving the Effectiveness of CSIRTs." *Global Cyber Security Capacity Centre.*

Barnum, Sean. 2014. *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™).* The MITRE Corporation.

Bates, Alicia. 2022. "Prepare and Prevent, Don't Repair and Repent." *The Cyber Defense Review* 7 (3): 17-30.

Bechara, Fabio Ramazzini, and Samara Bueno Schuch. 2020. "Cybersecurity and global regulatory challenges." *Journal of Financial Crime* 359-374. https://doi.org/10.1108/JFC-07-2020-0149.

Bilge, Leyla, and Tudor Dumitraş. 2012. "Before we knew it: an empirical study of zero-day attacks in the real world." *CCS '12: Proceedings of the 2012 ACM conference on Computer and Communications Security.* North Carolina, Raleigh, USA. 833 - 844. https://doi.org/10.1145/2382196.2382284.

Burt, Tom. 2021. *New nation-state cyberattacks.* March 02. https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/.

Cavelty, Myriam Dunn, and Max Smeets. 2023. "Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority." *Journal of European Public Policy* 30 (7): 1330-1352. https://doi.org/10.1080/13501763.2023.2173274.

Cerezo, Ana I., Javier Lopez, and Ahmed Patel. 2007. "International Cooperation to Fight Transnational Cybercrime." *Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007).* Karlovassi, Greece: IEEE. doi:10.1109/WDFIA.2007.4299369.

Ekong, Anietie P., Aniebiet Etuk, Saviour Inyang, and Mary Ekere-obong. 2023. "Securing Against Zero-Day Attacks: A Machine Learning Approach for Classification and Organizations' Perception of Its Impact." *Journal of Information Systems and Informatics* 5 (3): 1123-1140. doi:10.51519/journalisi.v5i3.546.

European Commission. 2016. *Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.* May 04. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434.

European Parliament; Council of the European Union. 2022. "DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL." *Official Journal of the European Union.* December 14. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555.

Fischer, Daniel, Clemens Sauerwein, Martin Werchan, and Dirk Stelzer. 2023. "An Exploratory Study on the Use of Threat Intelligence Sharing Platforms in Germany, Austria, and Switzerland." *ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security.* New YorkNYUnited States: Association for Computing Machinery. 1-7. https://doi.org/10.1145/3600160.3600185.

Google; Mandiant. 2024. *We're All in this Together. A Year in Review of Zero-Days Exploited In-the-Wild in 2023.* March. https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Year_in_Review_of_ZeroDays.pdf.

Hausken, Kjell. 2007. "Information sharing among firms and cyber attacks." *Journal of Accounting and Public Policy* 26 (6): 639-688. https://doi.org/10.1016/j.jaccpubpol.2007.10.001.

Homburger, Zine. 2019. "The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace." *Global Society* 33 (2): 224-242. https://doi.org/10.1080/13600826.2019.1569502.

Kamiya, Shinichi, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and René M. Stulz. 2018. "What is the Impact of Successful Cyberattacks on Target Firms?" *National Bureau of Economic Research.* doi:10.3386/w24409.

Krebs, Brian. 2021. *At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software.* March 05. https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/.

Lanzendorfer, Quinn E. 2015. *Enabling knowledge in the paradigm of international cyber intelligence.* Robert Morris University ProQuest Dissertations Publishing.

Lewis, James A. 2002. "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats." *Center for Strategic and International Studies.*

Maschmeyer, Lennart, Ronald J. Deibert, and Jon R. Lindsay. 2020. "A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society." *Journal of Information Technology & Politics* 18 (1): 1-20. https://doi.org/10.1080/19331681.2020.1776658.

Meakins, Joss. 2018. "A zero-sum game: the zero-day market in 2018." *Journal of Cyber Policy* 60-71. doi:10.1080/23738871.2018.1546883.

Microsoft 365 Security. 2021. *HAFNIUM targeting Exchange Servers with 0-day exploits.* March 02. https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/.

Narang, Satnam. 2021. *CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065: Four Zero-Day Vulnerabilities in Microsoft Exchange Server Exploited in the Wild.* March 2. https://www.tenable.com/blog/cve-2021-26855-cve-2021-26857-cve-2021-26858-cve-2021-27065-four-microsoft-exchange-server-zero-day-vulnerabilities.

NATO. 2021. *Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise.* July 19. https://www.nato.int/cps/en/natohq/news_185863.htm.

Pala, Ali, and Jun Zhuang. 2019. "Information Sharing in Cybersecurity: A Review." *Decision Analysis* 16 (3): 172-196. https://doi.org/10.1287/deca.2018.0387.

Perera, Srinath, Xiaohua Jin, Alana Maurushat, and De-Graft Joe Opoku. 2022. "Factors Affecting Reputational Damage to Organisations Due to Cyberattacks." *Informatics* 9 (28). https://doi.org/10.3390/informatics9010028.

Purohit, Soumya, Roshan Neupane, Naga Ramya Bhamidipati, Varsha Vakkavanthula, Songjie Wang, and Matthew Rockey. 2023. "Cyber Threat Intelligence Sharing for Co-Operative Defense in Multi-Domain Entities." *IEEE Transactions on Dependable and Secure Computing* 20 (5): 4273-4290. doi:10.1109/TDSC.2022.3214423.

Rajamäki, Jyri. 2017. "Cyber Security, Trust-Building, and Trust-Management: As Tools for Multi-agency Cooperation Within the Functions Vital to Society." In *Cyber-Physical Security. Protecting Critical Infrastructure at the State and Local Level*, by Robert M. Clark and Simon Hakim, 233–249. Springer.

Rheingold, Howard. 1994. *The Virtual Community: Finding Connection in a Computerized World.* Secker & Warburg.

Robinson, Philip. 2024. *The Hafnium Breach – Microsoft Exchange Server Attack.* December 17. https://www.lepide.com/blog/the-hafnium-breach-microsoft-exchange-server-attack/.

Roumani, Yaman. 2021. "Patching zero-day vulnerabilities: an empirical analysis." *Journal of Cybersecurity* 7 (1). https://doi.org/10.1093/cybsec/tyab023.

Schlette, Daniel, Fabian Böhm, Marco Caselli, and Günther Pernul. 2021. "Measuring and visualizing cyber threat intelligence quality." *International Journal of Information Security* 21–38. https://doi.org/10.1007/s10207-020-00490-y.

Schulze, Matthias, and Thomas Reinhold. 2018. "Wannacry about the tragedy of the commons? Game-theory and the failure of global vulnerability disclosure." *ECCWS 2018 17th European Conference on Cyber Warfare and Security V2.* Oslo, Norway: Academic Conferences and Publishing International Limited. 454-463.

Serrano, Oscar, Luc Dandurand, and Sarah Brown. 2014. "On the design of a cyber security data sharing system." *Proceedings of the 2014 ACM workshop on information sharing & collaborative security.* New York, United States: Association for Computing Machinery. 62-69. https://doi.org/10.1145/2663876.2663882.

Shackleford, Dave. 2015. "Who's Using Cyberthreat Intelligence and How?" February. https://cdn-cybersecurity.att.com/docs/SANS-Cyber-Threat-Intelligence-Survey-2015.pdf.

Silva, Alessandra de Melo e, João José Costa Gondim, Robson de Oliveira Albuquerque, and Luis Javier García Villalba. 2020. "A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence." *Future Internet.*

Singh, Umesh Kumar, Chanchala Joshi, and Dimitris Kanellopoulos. 2019. "A framework for zero-day vulnerabilities detection and prioritization." *Journal of Information Security and Applications* 164-172. https://doi.org/10.1016/j.jisa.2019.03.011.

Sklyar, Vladimir, and Vyacheslav Kharchenko. 2019. "ENISA Documents in Cybersecurity Assurance for Industry 4.0: IIoT Threats and Attacks Scenarios." *IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications.* Metz, France: IEEE. doi:10.1109/IDAACS.2019.8924452.

Smeets, Max. 2022. "The Role of Military Cyber Exercises: A Case Study of Locked Shields." *2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon).* Tallinn, Estonia: IEEE. doi:10.23919/CyCon55549.2022.9811018.

Steffensen, Vilja, and Vahiny Gnanasekaran. 2024. "Information Sharing between the Computer Security Incident Response Team and its Members: An Empirical Study." *NIKT* 3.

Sullivan, Clare, and Eric Burger. 2017. ""In the public interest": The privacy implications of international business-to-business sharing of cyber-threat intelligence." *Computer Law & Security Review* 33 (1): 14-29. https://doi.org/10.1016/j.clsr.2016.11.015.

Sülü, Mücahit, and Resul Daş. 2022. "Graph Visualization of Cyber Threat Intelligence Data for Analysis of Cyber Attacks." *BALKAN JOURNAL OF ELECTRICAL & COMPUTER ENGINEERING.* https://doi.org/10.17694/bajece.1090145.

Sun, Nan, Ming Ding, Jiaojiao Jiang, Weikang Xu, Xiaoxing Mo, and Yonghang Tai. 2023. "Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives." *IEEE Communications Surveys & Tutorials* 25 (3): 1748-1774. doi:10.1109/COMST.2023.3273282.

Teodorescu, Cosmin Alexandru. 2022. "Perspectives and Reviews in the Development and Evolution of the Zero-Day Attacks." *Informatica Economică* 26 (2). doi:10.24818/issn14531305/26.2.2022.05.

Tolga, İhsan Burak. 2019. *Whole-of-Government Cyber Information Sharing.* Talinn: CCDCoE.

Tounsi, Wiem, and Helmi Rais. 2017. "A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attacks." *Computers & Security* 212-233.

Tropina, Tatiana. 2015. "Public–Private Collaboration: Cybercrime, Cybersecurity and National Security. In: Self- and Co-regulation in Cybercrime, Cybersecurity and National Security." *SpringerBriefs in Cybersecurity* 1-41. https://doi.org/10.1007/978-3-319-16447-2_1.

Wagner, Cynthia, Alexandre Dulaunoy, Gérard Wagener, and Andras Iklody. 2016. "MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform." *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security.* Vienna, Austria: Association for Computing Machinery. 49-56. https://doi.org/10.1145/2994539.2994542.

Wagner, Thomas D., Khaled Mahbub, Esther Palomar, and Ali E. Abdallah. 2019. "Cyber threat intelligence sharing: Survey and research directions." *Computers & Security* 87. https://doi.org/10.1016/j.cose.2019.101589.

Waheed, Azheen, Bhavish Seegolam, Mohammad Faizaan Jowaheer, Chloe Lai Xin Sze, and Ethan Teo Feng Hua. 2024. "Zero-Day Exploits in Cybersecurity: Case Studies and Countermeasure." *Preprints.* doi: 10.20944/preprints202407.2338.v1.

Wallis, Tania, and Rafał Leszczyna. 2022. "EE-ISAC—Practical Cybersecurity Solution for the Energy Sector." *Energies* 15 (6). doi:https://doi.org/10.3390/en15062170.

Wang, Han, Alfonso Iacovazzi, Seonghyun Kim, and Shahid Raza. 2024. "CLEVER: Crafting Intelligent MISP for Cyber Threat Intelligence." *2024 IEEE 49th Conference on Local Computer Networks (LCN).* Normandy, France: IEEE. doi:10.1109/LCN60385.2024.10639749.