HEIMDAL®

Heimdal®
Cyber Threat Report 2023

A 2022 Review of the Cyber-Threat Landscape
and Predictions for 2023

Table of contents:

2022 Threatscape Overview

2022 Threatscape Overview

Marked by significant geopolitical shifts and unrest, 2022 has galvanized the cybersecurity landscape as well; war-profiteering fueled by endless media disputes has allowed the threat actors not only to operate unhindered but also to find safe harbor with states that choose to turn a blind eye to cyber-criminal activity. In this portentous context, the defender is coerced to research and implement new strategies for risk minimization and early threat-signaling. Taking into account the multi-surface factor (i.e., threat actors staging multi-vector attacks), the cyber-defense industry has very swift in embracing full or partial security automatization models.

Whereas a couple of years ago heavy reliance on policy-based security was the norm, current praxis has turned towards technologies capable of detecting the early signs of an impending cyber-attack and mitigating them via low- and medium-level (security) automations; SIEM (i.e., Security Information and Event Management) along with SOAR (i.e., Security Orchestration, Automation and Response) are proven value approaches in spite of their lack of maturity compared to other time-honored cybersecurity methods such as antivirus or endpoint-based antimalware solutions.

Although the industry's having a clear-cut trajectory, automatizations, be them all-inclusive or partial, carry inherent challenges and limitations (e.g., SIEM solutions are prone to alert fatigue, while SOAR-type responses are confined to low- and medium-level security incidents). Other factors that encumber the adoption and implementation processes are licensing, medium- to long-term costs (i.e., setup, configuration, upscaling, and maintenance) and workforce, the latter being considered a deal-breaker for organizations seeking to embrace SIEM, SOAR or hybrid approaches.

2023 will most likely be just as challenging as the previous few years, but I'm confident that the cybersecurity market has the right tools to deal with the constantly shifting cybercrime landscape and new/consolidated threats, whether we're talking about supply chain attacks, ransomware, deepfakes or cyber espionage.
With significant movements all across the grid, we have compiled this threat report not only to mirror the data-backed facts, but also to serve as a guide; a handbook to better threat protection, detection, and mitigation.

Most Important Cyber-Attacks of 2022 & Dangerous Malware

Most Important Cyber-Attacks of 2022 & Dangerous Malware

1. UKRAINE-RUSSIA CYBER CONFLICT

The border conflict soon to turn into a full-scale invasion has transformed in an incubator for non-traditional weapon-testing, especially in the area of cyberwarfare. On both sides, hackers are mounting devastating attacks in order to take down strategic assets (i.e., Governmental websites, military networks, public infrastructure) or targets of opportunity. The latest intel reveals that Russia is allegedly hiring or rather harboring well-known threat groups in an attempt to turn the tide of the conflict.

A briefing elaborated by the European Parliament's Think Tank reveals a tacit cyber-conflict between Russia and Ukraine, one that stretches across a period of 8 years. Per the timeline enclosed below, the cyber-warfare between the two East European countries began in early 2014, with Russia-sponsored hackers launching multiple DDOS attacks at Ukraine-held networks and communicational infrastructure, in an attempt to divert attention from troop movements taking place in Crimean region. With the conflict ongoing, we ought to expect more cyberwarfare incidents from both sides.

March 2014 — DDoS attack aims at destabilizing Ukrainian computer networks and communications, diverting attention from Russian troop operations in Crimea.

May 2014 — Pro-Russian hacktivist group carries out a series of cyberattacks to manipulate voting in Ukraine presidential elections (malware was removed but the election count was delayed).

December 2015 — Pro-Russian hacktivist group carries out a series of cyberattacks to manipulate voting in Ukraine presidential elections (malware was removed but the election count was delayed).

January 2016 — Disruptions in Kyiv substation result in a one-hour power blackout.

June 2017 — NotPetya malware hits Chernobyl nuclear power plant and infects multiple government and financial institutions, postal services, newspapers, transport infrastructure and businesses.

July 2018 — Attempted cyberattack on Auly chlorine distillation stations, which serves 23 Ukrainian provinces.

February 2021 — Attempted cyberattack targets Ukraine's security service website.

2022

- **13.02** – Microsoft reports the existence of malware targeting the Ukrainian government and several non-profit and information technology organizations.
- **14.02** – Hackers display 'Wait for the worst' message on 70 government websites.
- **15.02** – DDoS attacks disables Ukrainian government, banks, and radio websites for several hours.
- **23.02** – Government websites targeted, and the HermeticWiper malware impacts financial, IT, and aviation sector organizations.
- **24.02** – Attacks against the KA-SAT satellite network facilitates Russian invasions.
- **25.02** – IssacWiper attack against government websites and a cyberattack aimed at a border checkpoint.
- **28.02** – Attacks on Ukraine's digital infrastructure disable access to financial and energy resources.
- **04.03** – Malware launched against non-governmental, charity and aid organizations.
- **07.03** – Phishing attacks against citizens and government services.
- **09.03** – Cyberattack on a telecommunication service provider.
- **14.03** – CaddyWiper Malware infiltrates several Ukrainian organizations' computer systems.
- **16.03** – Hacked TV stations Ukraine 24 falsely reports that President Zelenskyy has called on the population to surrender.
- **17.03** – Phishing emails target Ukrainian government and military.
- **18.03** – Phishing emails target several organizations.
- **20.03** – LoadEdge backdoor used to install surveillance software.
- **28.03** – Cyberattacks against Ukrtelecom and WordPress websites.
- **30.03** – MarsStealer plunders Ukrainian citizens' and organizations' user credentials.
- **02.04** - Hackers steal Ukrainian government officials' user credentials.
- **07.04** – Hackers steal media and government entities user credentials.
- **08.04** – Attempt to interrupt power stations.
- **14.04** - Public banking data accessed via Trojan malware.
- **19.04** – Ukrainian citizens' payment data accessed via social media page survey.
- **22.04** – Cyberattack on Ukraine's national postal service.
- **07.05** – Cyberattack against Odesa City Council in parallel to missile attack against Odesa's residential areas.
- **09.05** – DDoS attack aimed at filtering and re-routing online traffic to Russian-occupied Ukrainian territories.

Source: European Parliament
https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

2. NVIDIA DATA BREACH BY LAPSUS$ APT.

On March 1st, the chipmaker company confirmed that its network had been hacked in February, with threat actors getting access to login credentials of employees as well as to confidential information.

Following NVIDIA's first statement that it was investigating an incident with some impact on its systems, as the Telegraph reported, Lapsus$, a data extortion group claimed responsibility for this attack together with declaring the theft of 1TB of Nvidia's network data. During the weekend, Lapsus$ released further information regarding the hack consisting of a 20GB archive with Nvidia servers' data. What's more, this archive also included password hashes of the business personnel.

The hacking group warned Nvidia to perform hardware information leakage if the GeForce RTX 30 Series firmware's lite hash rate (LHR) constraints were not removed.
It was also reported that the threat actor group requested the chipmaker company to agree to open-sourcing its GPU drivers for Windows, macOS, and Linux devices

3. COSTA RICA ATTACK BY CONTI RANSOMWARE.

On April 11, 2022, the gang launched their final attack under the Conti name after obtaining initial access to the network of the Costa Rican government and conducting reconnaissance activity.

The steps taken by the Russia-based cybercrime group, from gaining initial access to stealing 672GB of data on April 15 and deploying the ransomware, are explained in a report published by cyber intelligence company Advanced Intelligence (AdvIntel).
The experts said that the fileshare output was then downloaded to a local device by MemberX using the Cobalt Strike backdoor channel. The hacker gained access to administrative shares, where they uploaded a Cobalt Strike DLL beacon and used the remote file execution tool PsExec to run it.

The researchers also state that Conti developers used the open-source, credential-dumping application Mimikatz to carry out a DCSync and Zerologon attack that granted them access to all the hosts on Costa Rica's interconnected networks.

In order to ensure that they wouldn't lose access in the event that security specialists find the Cobalt Strike beacons, the attacker installed the Atera remote access tool on machines with less user activity where they had administrator rights.

4. SPICEJET RANSOMWARE ATTACK.

SpiceJet is a low-cost airline that operates out of Gurgaon, which is located in the state of Haryana. As of March 2019, it has a market share of 13.6 percent, making it the nation's second-biggest airline in terms of the number of passengers transported inside the country. "Certain SpiceJet systems faced an attempted ransomware attack last night that impacted and slowed down morning flight departures today. Our IT team has contained and rectified the situation and flights are operating normally now."

5. ROMPETROL RANSOMWARE ATTACK.

Rompetrol is the operator of Petromidia Navodari, the largest oil refinery in Romania, with a processing capacity of more than five million tons annually.

It looks like a ransomware attack hit the Rompetrol gas station network, with the KMG International's subsidiary declaring that it is fighting a "complex cyberattack."
KMG International is one of the world's largest oil companies, with operations in fifteen countries across Europe, Central Asia, and North Africa. Refining, marketing, trading, production, and oil industry services such as drilling, EPCM, and transportation are among KMG's main activities.

Following the attack, the petroleum provider was forced to shut down its websites and the Fill&Go service at gas stations. Based on an anonymous tip the attackers have also gained access to the Petromidia refinery's internal IT network, but Rompetrol claims that the refinery's operations are unaffected.

6. TURLA APT

Turla APT group, also known in the information security field as Snake, Venomous Bear, Uroburos, or WhiteBear, is an advanced operation that has been operational since at least 2004.

The infamous group has a long list of high-profile victims from all over the world in its portfolio. The APT attacked various European government entities and organizations in the U.S., Ukraine, and Arabic countries.

Turla's attacking methods include covert exfiltration tactics using hijacked satellite connections, watering hole attacks, rootkits, and hidden channel backdoors.

7. MUSTANG PANDA

State-backed Chinese hackers started a spear phishing attempt to spread personalized malware stored in Google Drive to international governmental, academic, and scientific institutions.

The attacks were observed between March and October 2022, and researchers attributed the actions to the cyber espionage group Mustang Panda (Bronze President, TA416). The majority of the organizations the threat group targeted were in Australia, Japan, Taiwan, Myanmar, and the Philippines. The Chinese threat group used Google accounts to send luring emails to their targets, tricking them into downloading custom malware from Google Drive links. Researchers found that Mustang Panda used messages with geopolitical subjects, with 84% targeting governmental/legal organizations.

The embedded link directed the target to a Google Drive or Dropbox folder, two legitimate platforms perceived as less suspicious. These links direct you to download RAR, ZIP, and JAR compressed files that include ToneShell, ToneIns, and PubLoad-specific malware variants. The procedure typically involved DLL side-loading once the victim started an executable contained in the archives, despite the fact that the hackers used a variety of malware-loading routines.

8. HODUR - KORPLUG REVAMPED

The Korplug RAT (also known as PlugX) is a spyware that has previously been associated with Chinese APT organizations and has been linked to targeted assaults on significant institutions in a number of different countries.

The RAT functionality of the variation utilized in the most recent campaign is mostly consistent with the RAT feature of prior Korplug variants.

Hodur has a few more commands and properties and as a result, it may gather vast system information while also running commands and reading and writing arbitrary files, as well as launching remote cmd[.]exe sessions.

9. LOG4J

At the end of 2021 proof-of-concept exploits for a significant zero-day vulnerability discovered in the widely used Apache Log4j Java-based logging library were distributed online, exposing both home users and businesses to continuous remote code execution assaults.

The vulnerability, officially tagged as CVE-2021-44228 and called Log4Shell or LogJam, is an unauthenticated RCE vulnerability that allows total system takeover on systems running Log4j 2.0-beta9 through 2.14.1.

Threat-Hunting by Heimdal®.

The Most Powerful Statistics of 2022

Threat-Hunting by Heimdal®.

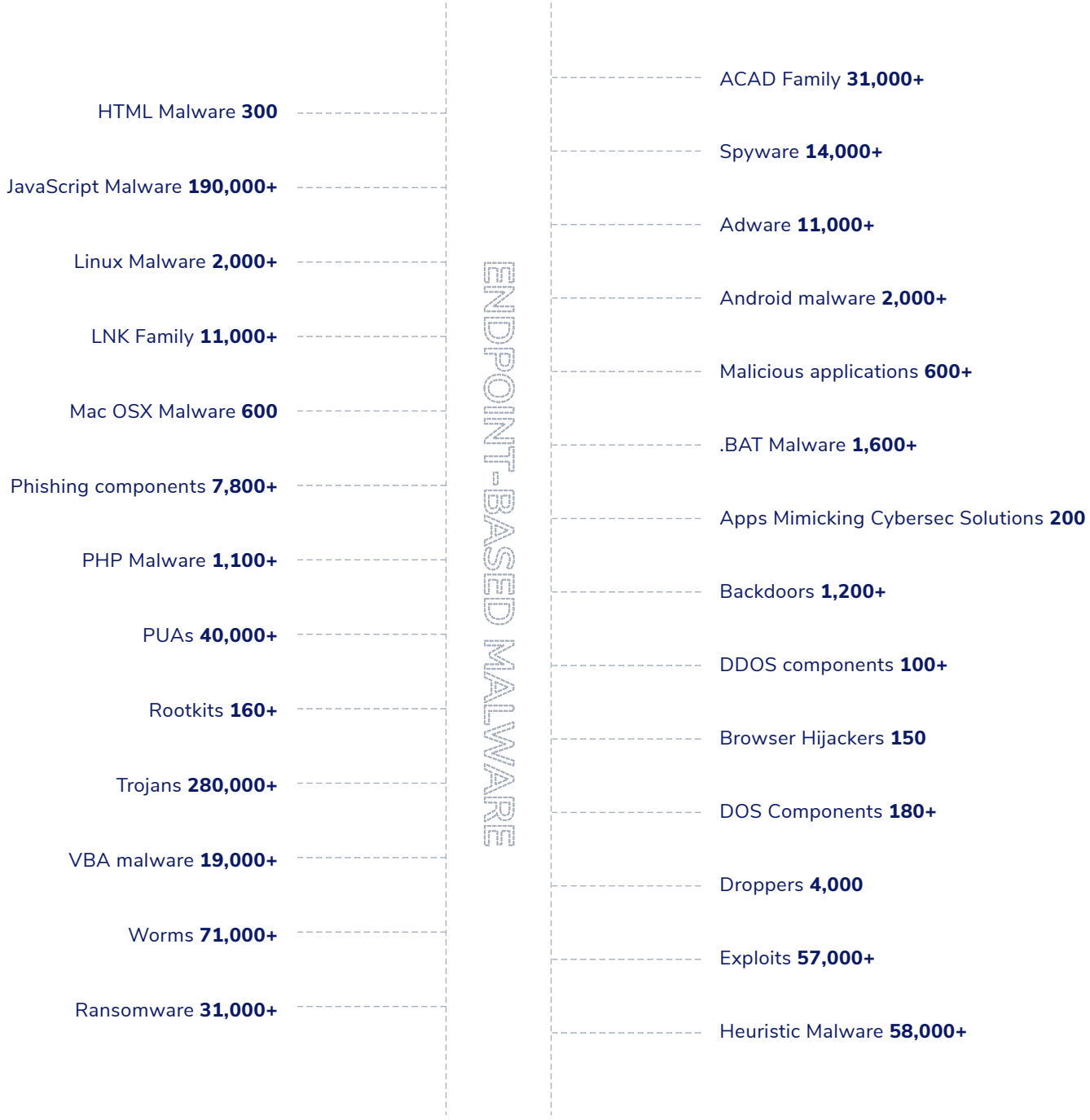
The Most Powerful Statistics of 2022

This section is exclusively dedicated to Heimdal®'s ongoing, telemetry-based, threat-hunting endeavor, covering each and all attack surfaces including, but not limited to, endpoint-based events, email, firewall, software vulnerabilities, and email.

In 2022, Heimdal® has processed, addressed, and resolved over 25 million cybersecurity events.

Cybersecurity Incidents by Event Type

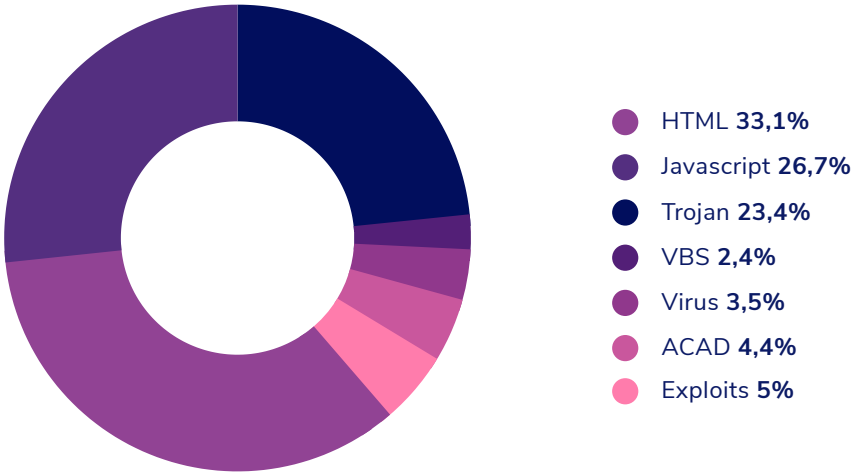
ENDPOINT-BASED MALWARE



TOP 20 ENDPOINT-BASED MALWARE DETECTIONS

Malware	No. of positive detections
HTML/Infected.WebPage.Gen2	200,000+
JS/Redir.G13	170,000+
ACAD/Bursted.AN	28,000+
TR/Worm.Gen	24,000+
TR/AD.GoCloudnet.kabtg	20,000
TR/Dropper.tfflr	19,000+
EXP/CVE-2010-2568.A	17,000+
TR/Rozena.jrrvz	16,000+
EXP/PyShellCode.G	15,000+
VBS/Ramnit.abcd	15,000+
TR/CoinMiner.uwtyu	14,000+
W32/Run.Ramnit.C	13,000+
TR/Patched.Ren.Gen4	13,000+
TR/Patched.Gen	12,000+
TR/Trash.Gen	12,000+
TR/Rozena.rfuus	11,000+
HTML/ExpKit.Gen2	11,000+
HEUR/APC	10,000+
W32/Sality.AB.2	9,000+
TR/Swrort.fkiqj	8,000+

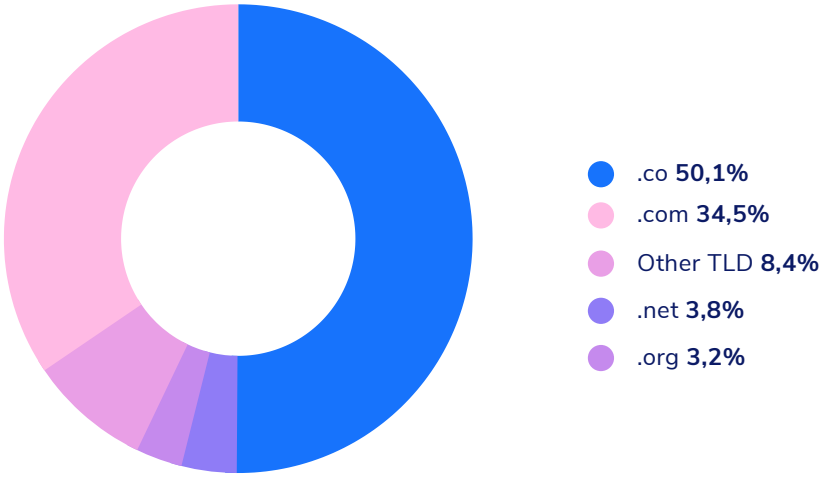
Distribution of detected (and resolved) endpoint-based malware by classification



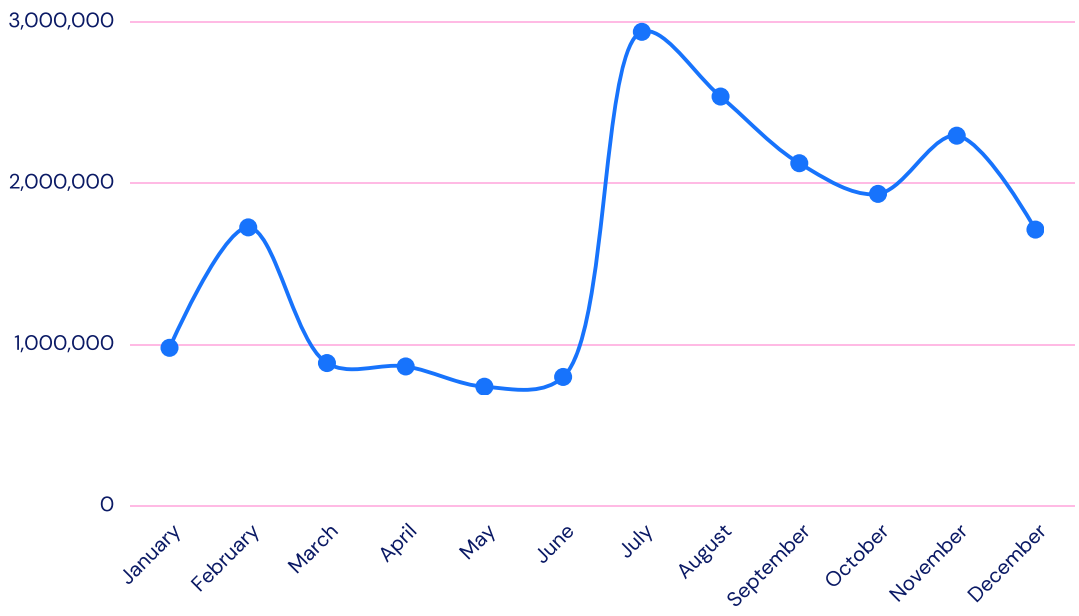
NETWORK-BASED ATTACKS

In 2022, Heimdal® has blocked over 17,000,000 network-based (i.e., DNS, HTTP, and HTTPS) cyber-attacks.

Network-based attacks by TLDs (i.e. Top-Level Domains)

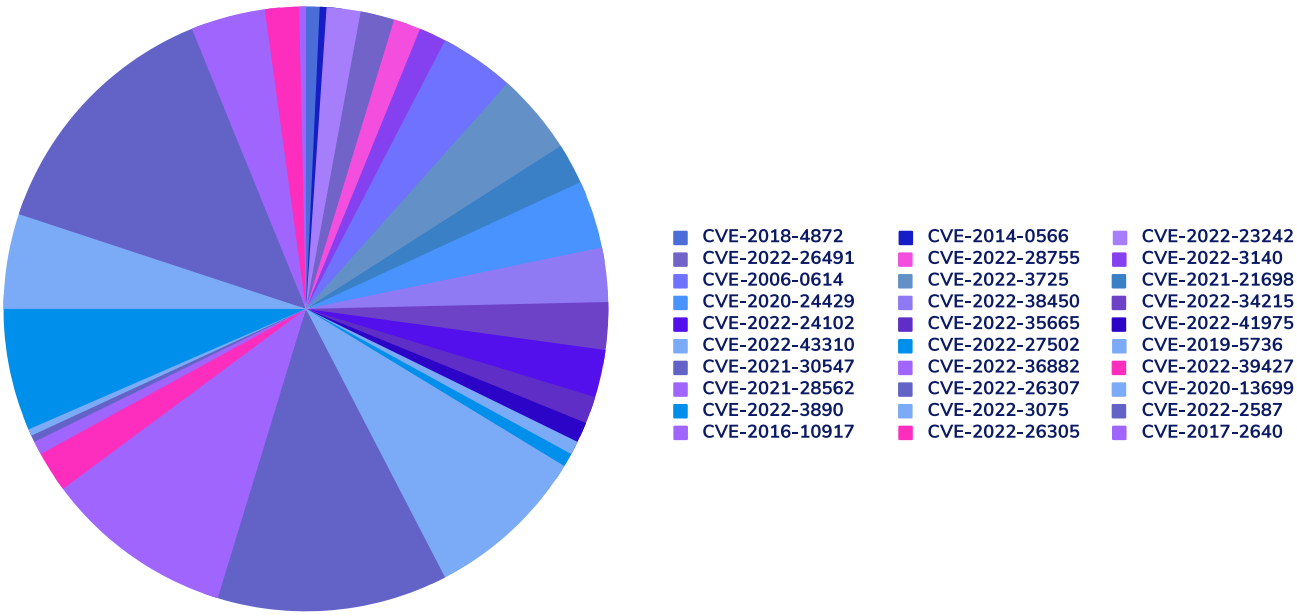


DNS-BASED ATTACKS – ANNUAL TRENDLINE



PATCHING AND VULNERABILITY MANAGEMENT

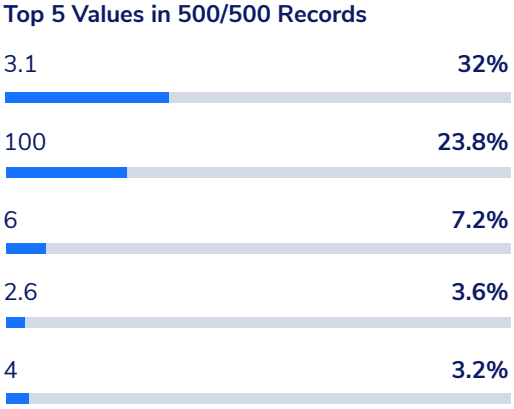
CVE coverage handled by Heimdal® by CVSS severity



EMAIL SECURITY

In 2022, Heimdal® has scanned over 50 million emails. 10% of them harbored harmful content.

Average spam score classification (500/500 records)



Heimdal® End-of-the-Year Statistics

- 100% of organizations that reported brute-force attempts were conducting fewer third-party patches (less than 100 improvement-carrying packages in the last 90 days) or had more legacy OS software.

- Government, Health, and Transportation are 16.3% more likely to be targeted compared to other industries. (Based on Heimdal® data 2022).

- 23% of connections to networks are malicious. Therefore, security awareness training and endpoint protection are needed to reduce cyber risk. (Based on Heimdal® data 2022).

- Organizations using automatic patching can apply five times more OS-based patches compared to those relying on manual patching. (Based on Heimdal® data 2022)

- Organizations using automatic patching can apply two times more third-party-based patches compared to those relying on manual patching. (Based on Heimdal® data 2022)

Heimdal® and the Power of Resilience

ANAF Spearphishing campaign

A new spearphishing campaign has been detected in the wild, specifically targeting Romanian businesses under the guise of ANAF, the Romanian counterpart of the IRS. Business owners are being informed via email that they have outstanding taxes and, therefore, are solicited to make the payment as soon as possible. Local Romanian authorities are advising business owners against responding to unprompted fiscal solicitations and to check with their zonal ANAF branch for any discrepancies in taxes. So far, no one has reported losses in the ANAF spearphishing campaign.

For the past couple of days, business owners from across Romania have received emails from ANAF informing them that they have outstanding fiscal debt. Enclosed in the email are several attachments, including a .xls document that, allegedly contains debt-related details. The spearphishing campaign comes only weeks after Lucian Heius, ANAF's chairman, announced that the institution will be engaging in country-wide fiscal investigations in an attempt to counter tax evasion in natural persons and SMBs.

Given the statement's online virality and the backlash it received from public opinion, it was only a matter of time before becoming turned into a phishing tool by threat actors.
As to the case at hand, many business owners have been met with these emails, being urged to pay their taxes as soon as possible. The email itself doesn't have any elements that could potentially draw suspicion: no grammatical issues, out-of-place annotations, or any of the other distinguishing marks associated with phishing. In this user's eyes, this would simply pass as an official notice from ANAF which would subsequently prompt him to open the .xls document. Some variations were discovered – pdf documents replacing .xls documents, tone changes, logos added or subtracted.

Heimdal® Launches Broad Investigation into Russian Cybercrime Trend

Heimdal® has recently launched an ample investigation into the Russia-linked cybercrime wave. Based on the data gathered from internal and external sources, Heimdal® has discovered that the phenomenon is expanding, both in magnitude and frequency. This article will showcase our SOC team's discoveries, delineate methodology, and propose actionable strategies that will aid organizations to counter this rising trend.

Between January 2021 and late October 2022, over 8,000 cyberattacks have been carried out from the domains, at an average of circa 6.35 attacks per day. IP-based domain tracking returned no results as the threat actor has gone to great lengths to minimize the online footprint.

Upon reviewing the final numbers and factoring in variables such as temporal spread, intent, and the number of times a specific domain was used to stage an attack, we can only conclude that Russian-based attack domains are increasing exponentially.

Our computations show a 167% year-over-year increase in .ru TLDs, a statement corroborated by the data obtained from clear web sources.

As the conflict between Russia and Ukraine trudges on, we can expect more threat groups to show up and leave their mark on the cyber world. The numbers provided by Heimdal®'s SOC team prove that the threat is real, with no indications of cessation or slowing down.

As mentioned in the section about background and methodology, only a small fraction of the detected domains was used to stage cyberattacks against undisclosed targets. Concerning the bulk, we can assume that they are either backup domains, that can be used in case the primary one is compromised or that the threat actors may be spawning them in order to create a botnet.

Heimdal® Responds to CEO Fraud Attempt Launched by Unknown Perpetrator

A Heimdal® representative of the Billing & Accounting department received an email from the company's CEO requesting aid in processing two received LinkedIn invoices. The party posing as Morten Kjaersgaard solicited the accounting department to process these payments as soon as possible. At first glance, the email communication chain between the party posing as the CEO and accounting doesn't raise any suspicions due to the fact that it does not present any of the indicators associated with email fraud attempts (i.e., typos, grammatical and/or logical inconsistencies, out-of-place graphical elements, enclosed payment links, etc.). To the naked eye, this would have passed as legitimate interdepartmental communication.

However, a closer inspection of the sender's address revealed an inconsistency. The address did not match the Outlook entry associated with Morten Kjaersgaard's identity. Furthermore, the address pointed to an unknown cloud mailing service. Acting on the suspicion, the Heimdal® employee contacted the parties involved and notified forensics.

The subsequent analysis performed on the email chain confirmed that it was a CEO fraud attempt, leading to Heimdal® blackmailing the domains. Apart from the dubious sender's address, the email chain also contained two attached PDF documents. Sandboxing and blasting efforts disclosed no information on the attacker's identity, intentions, or motivations. Both PDF documents were clean – no .vbs scripting, macros, and redirect links.

Heimdal®'s XDR Team Links Recent CEO Fraud Attempt to Notorious Turkish Threat Group

(...) Cobalt Terrapin is a rather obscure threat group; based on all of the available data, this group has presumably emerged somewhere around March 2022, banding together Turkish-speaking black-hat hackers. Its distinctiveness comes from leveraging materials belonging to reputable vendors such as ZoomInfo and LinkedIn. To increase the attack's likelihood of success, the group also employs an executive impersonation technique. This double-pronged approach adds to the legitimacy of the claim – the phrasing and information conveyed are very unlikely to pass as suspicious for the unaware company representative.

As observed by Heimdal®'s XDR team, Cobalt Terrapin uses a fine-grained social engineering-based approach consisting of vendor and executive impersonation. In the case at hand, the deception began with the threat actor impersonating Heimdal®'s CEO forwarding an email on an outstanding LinkedIn invoice. Attached to the forwarded email were two pdf documents: the LinkedIn Invoice and a W9 (i.e., Request for Taxpayer Identification Number and Certification).

Our XDR team's foray into Cobalt Terrapin's TTPs revealed that the threat group has leveraged the same attachments to stage out attacks on other HVTs (i.e., High-Value Targets). However, this does not constitute the group's distinguishing trait. As pointed out in the previously published security alert, the kill chain was interrupted soon after the targeted individual contacted the company's CEO for verification purposes.

In regards to Cobalt Terrapin's modus operandi, our analysis revealed several facts of interest that may aid our customers and other companies improve their defenses and increase awareness. In profiling the threat actor, it was remarked that the individuals employ a special enveloping technique to avoid triggering a response in the victim.

For instance, in this case, the threat actor appended the CEO's name to the email's header. From a social engineering standpoint, this technique significantly increases the stealth factor, since most email users will not be interested in reading the field that comes after the sender's name.

Email formatting, style, and tone of writing are also to be considered points of interest when investigating this particular threat actor. We have ascertained that there are discernible changes in all three email composition areas – the style appears to be more relaxed, detached, and friendly to some extent, far from the coarseness of typical spear-phishing attempts.

Second, this new approach seems to lean more on the cost-willingness trade-off implied by the "can" method (e.g. "Can you take X action?") and less on the authoritative imposition heavily leveraged by this type of infiltration attempt (e.g., "Urgent", "Act now!", "You have X minutes to get this done" etc.). A closer look at the overall writing style can also offer us additional insight into Cobalt Terrapin's social engineering strategy. The email itself contains no grammatical errors, typos, or any kind of logical inconsistencies, elements that are associated with this type of online fraud. This level of meticulosity indicates ample planning on the attacker's side.

One can venture into saying that Cobalt Terrapin might have wanted to remove all the guesswork from Business Email Compromise, by devising an attack matrix that can be customized depending on the target's characteristics (e.g., company size, annual revenue, number of employees, the security awareness level of employees in key positions, etc.). The last item on the agenda is the email's format – Cobalt Terrapin appears to have discarded any of the on-screen elements that cause suspicion (e.g., using bolded fonts or

graphical elements, adding subject lines that stress out the urgency of the request).
Our XDR's team investigation was not fruitless, managing to shed more light on the threat group's modus operandi. On that note, it is of some concern the fact that the email itself passed all the standard security checks. Email header analysis indicated that the spear-phishing email scored green in all inbound verification tests (e.g. Anti-spoofing SPF, DKIM, and DMARC).

However, most threat actors that conduct BEC attacks tend to pipe emails through legitimate servers in order to bypass security filters. In Cobalt Terrapin's case, ensuring the attack email's confidentiality and availability via enveloping is but one of the techniques used to bypass basic email security.

As our XDR experts noted, the threat actor prefers passing the financial and W9 documents after establishing contact with the company's employee, not before. This approach serves two purposes – drop below the detection threshold and increase the legitimacy of the request.

Heimdal® Security Researchers Discover Massive Surge in DDoS Attacks

On the 16th of June 2022, Heimdal™ was solicited to investigate the anomalous timing-out of a WordPress-based stack. Having ruled out the usual suspects (e.g., coding errors, overloads, incorrect load balancing, misconfigurations), we proceeded to gather additional intel on the incident – Nginx backlogs, error logs, and crash logs which we later cross-referenced against the data retrieved from WordPress' Wordfence security addition. The data our company was commissioned to process revealed that the client's server downtime was not the result of arbitrariness, but a massive Distributed Denial-of-Service (DDoS) attack. Was it with purpose or was the client a victim of chance? Our analysis uncovered the following:

• **Unknown APT.** The threat actor's MO does not conform to any of the TTPs (i.e., Tactics, Techniques, and Procedures) associated with any known or thoroughly investigated threat actor.

• **Considering the attack's high velocity and its effectiveness, we have concluded that a botnet was employed.** Nginx backlogs revealed that 200+ dynamic IPs were used to flood the victim's WP-hosted server. The subsequent digital forensics report stated that the attacking botnet successfully harvested and used 120K endpoints to flood an unknown number of victims.

• **'Flooding' client.** The threat actor deployed a rudimentary Golang-written client to loop GET requests to the victim's server. Despite not being able to sample the actual code, our analysis revealed that the client used to stage the attack came from an open-source repo and shares many similarities with tools such as Go-http-client and Go-http-client/2.0.

• **Single URL to trigger an unexpected response.** The threat actor flooded a single URL in order to exhaust resources, thus decommissioning the WP-based server for a couple of minutes.

• **High-velocity attacks.** Nginx backlogs indicated that the GET flooding occurred within a 2-second time frame.

• **'Zombified' machines.** All IPs used in the attack have been traced to South-East Asia and Africa.

• **Brute-forcing.** Wordfence correlated data suggests that brute-forcing techniques might have been employed during the attack in order to gain access to server-hosted resources.

Heimdal® Threatscape Predictions for 2023

Morten Kjaersgaard, Heimdal®'s Chief Executive Officer (CEO), underscored the dimensionality of the threatscape. In terms of predictions, we are faced with two facets – defender and attacker.

On the defender's side the 2023 challenges and opportunities will be:

The Death of Point Solutions Is Coming – Unification is the Future

Today's CISOs and other decision-makers place a strong emphasis on centralized architectures that provide prevention, detection, and mitigation under a single roof in order to increase visibility and efficiency.

With outdated point solutions created in a time when the cyber security landscape didn't present as many threats and a talent shortage, organizations will keep turning to centralized solutions to meet the high demands of the IT threat landscape.

The Focus on Automation and Visibility Tools Will Increase

Automation is here to stay. The causes are numerous and really quite easy to grasp. Security systems generate almost infinite amounts of data, which no team could handle in real-time and react to in a timely manner. The cyber threatscape simply evolves too fast. There is a severe shortage of skilled cybersecurity professionals (and even those currently in the market are exposed to one of the most dangerous risks in the industry – human error). Moreover, hackers are using automation too!

To move from reactive to proactive security and regain control over one's environment and schedule, analytics, intelligence, and automation are essential. In the corporate IT environment, security automation can identify potential threats, assess the event to determine whether it is real or fake, and then contain and eliminate the threat. Without human assistance, automated security tools complete these actions in a matter of seconds.

Cybersecurity automation minimizes security teams' alert fatigue by examining alerts, identifying threats, and reducing the effects of attacks.

Radical Shifting Is In How We Visualize And Respond To Threats

Heimdal® is creating a new category in the cybersecurity market by providing a new approach to Security Orchestration, Automation and Response (SOAR), and Security Information and Event Management (SIEM) technology and engineering.

On the attacker's side the 2023 challenges and opportunities will be:

MSPs are the Prime Supply-Chain Target for a Multi-tiered Attack Surface

In line with last year's prediction, we also predict a heavy increase in supply chain attacks in 2023. Attacks on the software supply chain take place when a malicious actor gains access to an MSP or a software vendor's network and compromises the software before the vendor distributes it to customers. The sharp rise in software supply chain attacks is partly due to the accelerated business climate, which has resulted in less time for MSPs to react and rapid software release cycles from vendors, leaving developers with less time to identify and address security flaws.

With the rapid increase in IT outsourcing, MSPs in particular are a ripe target for cybercriminals.

This leads, naturally, to a multi-tiered attack surface, that can severely compromise customer data and IT systems. Attacks on the software supply chain increased by more than 300% in 2021 compared to 2020, and I predict that they will increase even more in 2023.

The fact that NIST has released a thorough guide on how institutions can defend themselves against supply chain attacks and compromise and the numerous 2022 news (see details about US newspapers, Oktapus, Comm100 Live Chat application) regarding supply chain attacks are clear signs of how serious this threat is.

Consumers Get Entangled in the Web of Ransomware

Cybercriminals will successfully compromise internet-based software delivery services, such as Steam, Origin, Blizzard or others, to deliver a hypercomplex ransomware attack through system rights provided by the services. Supply chain attacks will therefore no longer be just B2B-based, but expand the attack sphere into the consumer space for a mass-based exploit-to-ransomware payout attack.

Attackers Will Get Bolder and Will Spend More to Complete Their Strategical Objectives

Cybersecurity criminals have plenty of time and plenty of resources to complete their attacks and therefore they will surgically target big institutions to find a way through their defenses.

Attacks of this caliber will typically run into tens of thousands of dollars per month, as cybercriminals use resources in less developed countries, or could be state-backed from North Korea, Russia, China, Iran or similar. They will need to be numerous because even for orchestrated attacks, success is never guaranteed, but when the reward is in the tens of millions of dollars, the cost becomes insignificant.

Strategical Focus on Infrastructure across Europe and the US

Transport, energy, and other examples of critical infrastructure are becoming more complex and dependent on networks of interconnected devices. Therefore, unsurprisingly, a major concern today is the critical infrastructure's susceptibility to technical failures and cyberattacks. Recent occurrences like the war between Russia and Ukraine have only fueled these fears.

State and non-state actors now have more technical know-how, motivations, and financial resources than ever before to destabilize a nation's vital infrastructure. An attack on vital infrastructure in one region of a nation can have a significant negative impact on many others - the most recent cyberattack on DSB demonstrated exactly how an online threat on a third-party IT service provider can cause serious disruption in the real world.

Espionage and Information Operations Will Rise

Information operations and cyber espionage will likely increase. Iran, China, and Russia, the usual actors in information operations, will probably continue to promote narratives that best serve their objectives.

Additionally, they will highlight the idea that the United States failed to honor its obligations to international organizations and nations.

We can already see that the Russian invasion of Ukraine is partially supported by a cyber strategy that entails at least three separate, occasionally coordinated processes: destructive cyberattacks inside Ukraine, network penetration and espionage in other states, and cyber-influence operations aimed at people all over the world.

Deepfakes Will Become Increasingly Dangerous

Deepfake technology manipulates existing or brand-new audio and video content using artificial intelligence techniques. Although it can be used for legitimate purposes — satire and gaming, for example —, it can also, just like everything else, be misused by malicious actors for malicious purposes.

Deepfakes are used to fabricate a story that seems to come from reliable sources. The two main threats are against civil society (disseminating false information to influence public opinion in a particular direction) and against people or businesses so that malicious actors can make a profit.

The path to a dystopian future will be guaranteed if people will no longer be able to distinguish between truth and lies.

Deepfakes pose a significant cybersecurity threat to businesses because they could make phishing and BEC attacks more successful, make identity fraud much simpler, and significantly reduce share value by twisting brand reputation.

Ready to stay ahead of cyber threats?

Here's how Heimdal® can help.

Threat Prevention

Threat Prevention – Endpoint

Heimdal® Threat Prevention scans traffic in real time, blocking infected domains and preventing communication to cybercriminal infrastructures with minimal system footprint.

Threat Prevention - Network

Heimdal® Threat Prevention – Network provides you with unique threat hunting and ultimate visibility over your entire network. A to Z protection, regardless of device or operating system.

Privileges and Application Control

Privileged Access Management (PAM)

Heimdal® Threat Prevention – Network provides you with unique threat hunting and ultimate visibility over your entire network. A to Z protection, regardless of device or operating system.

Application Control

Application management solution created for whitelisting and blocking running applications. You can customize live sessions, log everything on the go, and prevent users from running malicious software.

Vulnerability Management

Patch and Asset Management

This solution lets you deploy and patch any Microsoft, 3rd party and proprietary software, on-the-fly, from anywhere in the world and according to any schedule. With complete visibility and granular control over your entire software inventory.

Endpoint Detection

Next-Gen Antivirus and MDM

One license and one console - Next-Gen Antivirus and MDM all unified for impeccable detection of sophisticated online threats such as ransomware, hidden backdoors, rootkits, brute-force attacks, and undetectable malware.

Ransomware Encryption Protection

Ransomware Encryption Protection is a revolutionary 100% signature-free solution, that protects your devices against malicious encryption attempts initiated during ransomware attacks.

Email Protection

Email Fraud Prevention

125 vectors of analysis coupled with live threat intelligence allows you to identify and stop Business Email Compromise, CEO Fraud, phishing and complex malware before compromise.

Email Security

Cloud and on-premises email protection solution, mixing Office 365 support with proprietary e-mail threat prevention to protect against mail-delivered threats and supply chain attacks.

Assistance

Remote Desktop

Cloud and on-premises email protection solution, mixing Office 365 support with proprietary e-mail threat prevention to protect against mail-delivered threats and supply chain attacks.

Services

Endpoint Prevention Detection and Response (EDR)

Endpoint Prevention Detection and Response provides unique prevention, threat-hunting, and remediation capabilities, empowering you to respond quickly and effortlessly to sophisticated malware.

eXtended Detection and Response (XDR)

Heimdal® can monitor your environment in our Extended Detection and Response team. We alert you on infection or attack, monitor your environment, validate policy checking for maximum compliance, and employ rapid and decisive responses to attacks.

To learn more about how Heimdal® can help you prevent, detect, hunt and respond to any security threat, we invite you to schedule a personalized live demo.

Threat-hunting & Action Center

The Heimdal® Threat-hunting and Action Center is a revolutionary platform that is fully integrated with the Heimdal solution suite. Designed to provide security teams with an advanced threat-centric view of their IT landscape, the solution employs granular telemetry to enable swift decision-making, using built-in hunting, remediation, and actioning capabilities – all managed from the Heimdal Unified Security Platform.

Book a demo

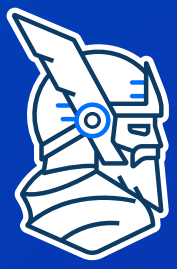
About Heimdal®

Founded in 2014 in Copenhagen, Denmark, Heimdal® is a leading European provider of cloud-based cybersecurity solutions. The company offers a multi-layered security suite that combines threat prevention, patch and asset management, endpoint rights management, and antivirus and e-mail security which together secure customers against cyberattacks and keep critical information and intellectual property safe. Heimdal has been recognized as a thought leader in the industry and has won multiple awards both for its solutions and for its educational content.

Currently, Heimdal®'s cybersecurity solutions are deployed in more than 60 countries and supported regionally from offices all over the world, by 175+ highly qualified specialists. Heimdal® is SOC 2 Type II and ISAE 3000 certified, securing more than 3 million endpoints for over 11,000 organizations. The company supports its partners without concessions on the basis of predictability and scalability, creating sustainable ecosystems and strategic partnerships

Become a Heimdal® Partner

Gartner peerinsights ★★★★★
SOURCEFORGE ★★★★★
G2 CROWD ★★★★½
Trustpilot ★★★★½



HEIMDAL®

Leading the fight against cybercrime.

www.heimdalsecurity.com

Vat No. 35802495, Vester
Farimagsgade 1, 2 Sal, 1606 København V