Heimdal®

Leading the fight against cybercrime.

Heimdal®
Threat Report

A 2021 review of the cyberthreat landscape and our predictions for 2022.

Table of contents:

2021 in Cybersecurity

2021 in Cybersecurity

In the present pandemic scenario, the more companies continue to engage in digital transformation and IT projects, the more at risk they are, and, therefore, more protection is needed to guarantee networks stay secure.

However, cybersecurity goes beyond simply funding actions; it is critical to educate staff and ensure they understand their responsibility in securing company data. We believe that in 2022, cybersecurity will be recognized as a vital asset.

Assessing the situation from the standpoint of risk management activities, organizations will shift their focus from asset preservation and start concentrating on loss avoidance. Increasing loss prevention capabilities will probably turn out to be the new norm, as more executives and board members might become involved in their companies' cybersecurity.

Enterprises should not be shocked by interruptions or caught off guard when it comes to securing their networks and infrastructure from malicious attackers. Within this volatile climate, one big question arises: is implementing a multi-layered security system that proactively acts to prevent prospective attacks (and is reactive in the event of potential assaults) the greatest precaution?

Looking back at all the cybersecurity events that marked 2021, one thing is certain - cybersecurity is here to stay and will only grow in importance from now on. We're here to protect your company's operational integrity and prevent cyberattacks from day one.

Heimdal™ delivers unified corporate security and is ready to protect your operational integrity by stopping even the most sophisticated cyberattacks from day one.

Most Important Attacks

Most Important Attacks

2021 was another pandemic year that brought with it many security incidents, some of these representing the beginning of taking new legal actions.

The SolarWinds Incident

Was one of the largest cyberattacks that we saw in the past years, and it may be the start of new data breach notification law in the US, as following the attack, Congress became interested in enacting a federal law requiring breach notifications.

ATTACK TIMELINE - OVERVIEW

04.09.2019	Threat Actor accessed SolarWinds
12.09.2019	Threat Actor injects test code and begins trial run
04.11.2019	Test Code injections ends
20.02.2020	SUNBURST complied and deployed
26.03.2020	Hotfix 5DLL available to customer
04.06.2020	Threat Actor removes malware from build VMs
12.12.2020	SolarWinds notified of SUNBURST
14.12.2020	SWI files 8-K and notifies shareholders and customers
15.12.2020	SWI releases software fix
17.12.2020	US-CERT alert issued
11.01.2021	New findings related to SUNSPOT released
Investigation ongoing	

All events, dates, and times approximate and subject to change; pending completed investigation

Colonial Pipeline

The Colonial Pipeline assault is perhaps the year's most significant hack, both for its ability to demonstrate the destructive possibilities of cybercrime and for the strong official reaction it sparked. It also demonstrated that the US is still entirely reliant on oil and will remain so for the foreseeable future. Colonial Pipeline, one of America's major oil and gas firms, was breached by hackers linked with the ransomware group DarkSide in May.

The attack not only sparked a brief energy crisis across the Southeast, which developed into a frenzied riot at gas stations across numerous states, but it also profoundly changed how the federal government conducts cyberattacks of this sort.

TIMELINE OF EVENTS

May 7

- Colonial Pipeline becomes aware of a ransomware attack subsequently attributed to the Darkside group.
- Digital systems are taken offline to contain the threat.
- Colonial engages leading third-party cybersecurity firm and activates incident response team.
- The FBI, CISA, FERC, PHMSA, U.S. Department of Energy and Homeland Security are notified of the incident.
- Colonial releases the first of eight statements informing the public about the ransomware attack.

May 8 - May 9

- Colonial begins daily coordination meetings with the federal government led by the Department of Energy.
- Colonial begins daily on-the-ground and aerial system integrity monitoring across 5.500-mile pipeline footprint.
- Colonial begins to manually operate some smaller lateral lines between terminals and delivery points while existing inventory is available.
- Colonial's operations team begins development of a system restart plan.

May 10 - May 11

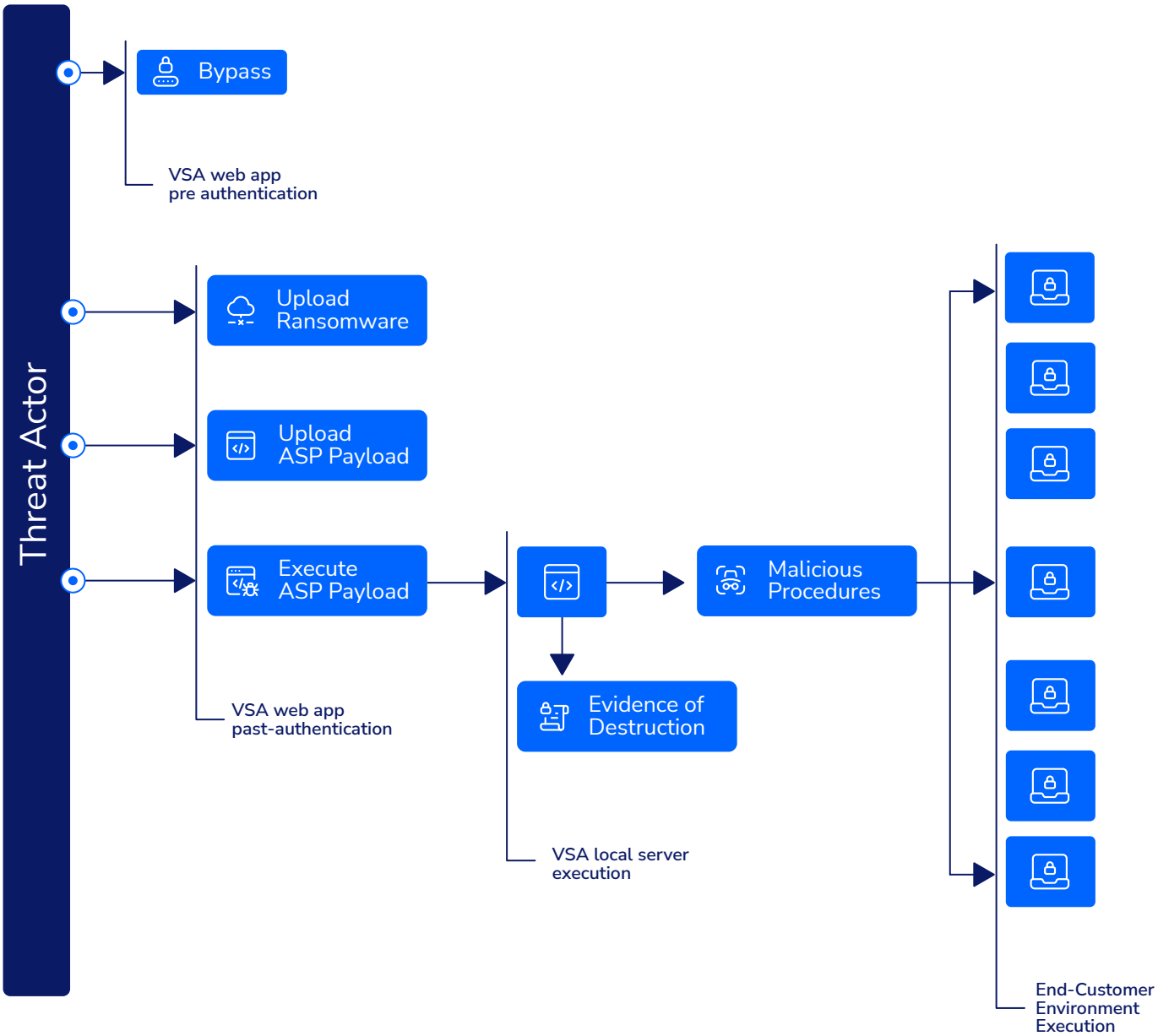
- The FBI confirms ransomware is responsible for the incident.
- Colonial continues to work with the Department of Energy and customers to identify where product shortages may exist and prioritize those locations.
- Federal and state governments take emergency actions to help alleviate disruptions to the fuel supply chain.

May 12

- Colonial restarts pipeline operations at approximately 5:00 p.m. ET.

Kaseya

The assault, which compromised a major Kaseya software product called VSA, was used to transmit malware to dozens of Kaseya clients, many of whom were managed service providers, or MSPs, companies that assist small businesses and government agencies with outsourced IT work. As a result, the virus infected the MSPs' clients as well as affecting hundreds of thousands of organizations.

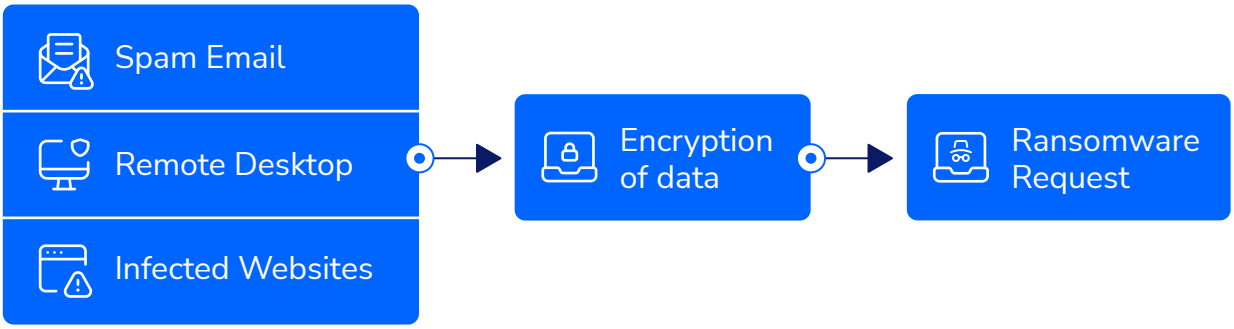


Most Dangerous Threats

Most Dangerous Threats

Clop Ransomware

Ransomware has grown dramatically, and it currently ranks first among the world's most hazardous new cyberthreats. Clop ransomware is one of today's most dangerous ransomware threats. Clop ransomware is a form of the well-known CryptoMix malware, which frequently targets Windows users. It disables many Windows apps, including Microsoft Security Essentials and Windows Defender, and inhibits numerous Windows processes before encrypting your PC.



Gameover Zeus

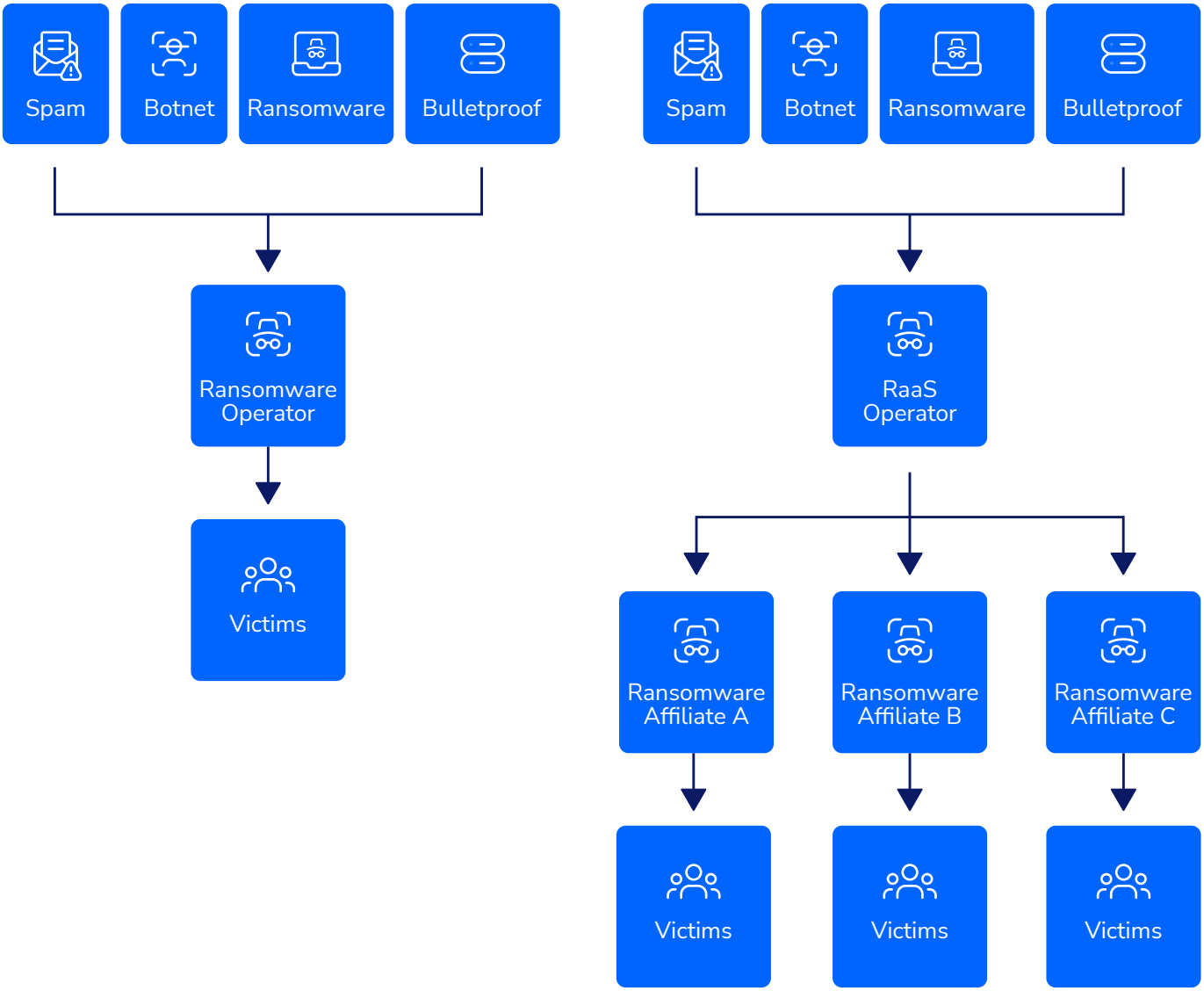
Gameover Zeus is a harmful spyware that targets your financial information and is part of the "Zeus" malware family. It's a trojan that targets your personal financial information and utilizes it to steal all of your money. Furthermore, Gameover Zeus may exfiltrate sensitive data without using centralized servers by creating its own independent servers.

Social Engineering

Aside from technological proficiency, hackers tend to veer towards social psychology. Humans have been recognized as the weakest link in cybersecurity by hackers. "Hackers who abuse human psychology to get access to a user's personal information" are leveraging social engineering. Hackers employ a variety of methods, including social media and phone calls. They persuade victims to hand up sensitive information, which they subsequently exploit to defraud the victim.

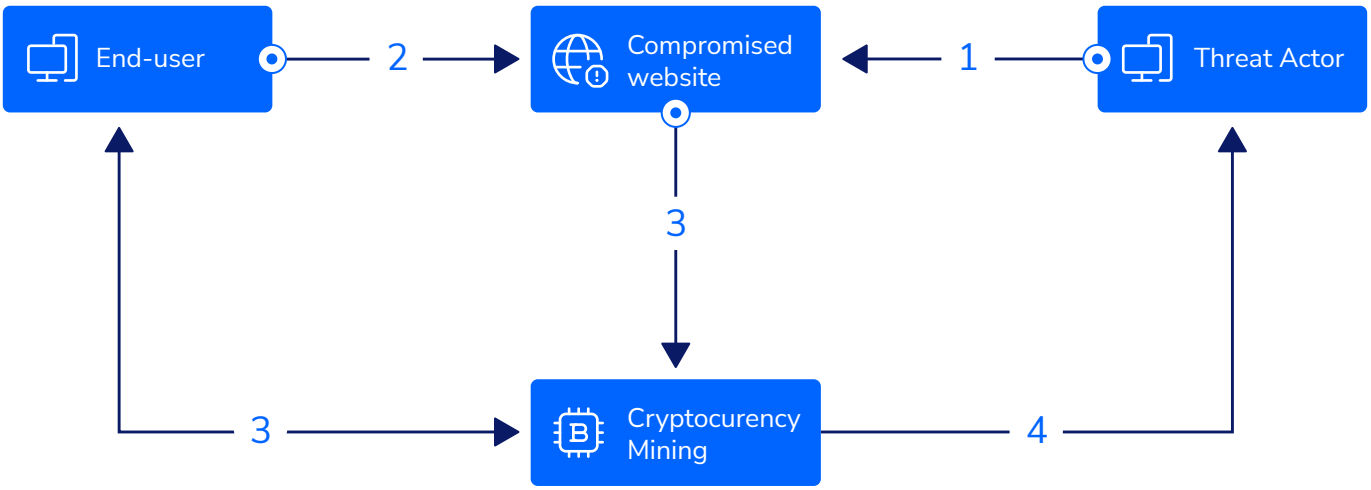
Ransomware as a Service (RaaS)

In the hacking and cybercrime arena, RaaS is a small, but growing industry. Those who are still unfamiliar with RaaS might employ a "professional hacker" or team to conduct an assault on their behalf. With a "high success rate" as ransomware, RaaS has grown in prominence, attracting more actors to take advantage of its user-friendliness. It's attracting even individuals who have no prior experience with malware coding. Netwalker, Stampado, RaaSberry, Satan and Frozr Locker are just a few threat actors that operate under this “business” model.



Cryptojacking

Cryptojacking is a type of cybercrime that targets cryptocurrency. It's a piece of software that uses a victim's computer to "mine" cryptocurrencies like Ethereum and Bitcoin. They use a device's computational resource making the machine unresponsive or hard to work with. This ransomware poses a significant security risk to cryptocurrency dealers.

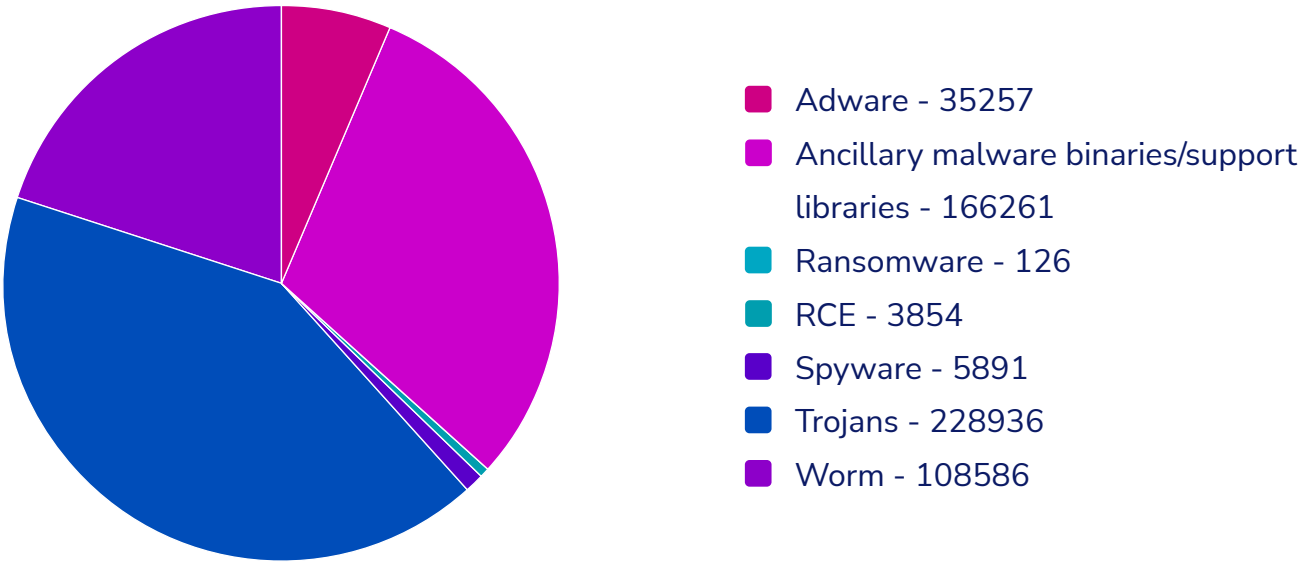


1. The threat actor compromises a website;
2. Users connect to the compromised website and the cryptocurrency script executes;
3. Users unknowingly start mining cryptocurrency on behalf of the threat actor;
4. Upon successfully adding a new block to the blockchain, the threat actor receives a reward in cryptocurrency coins.

IoT Device Attacks

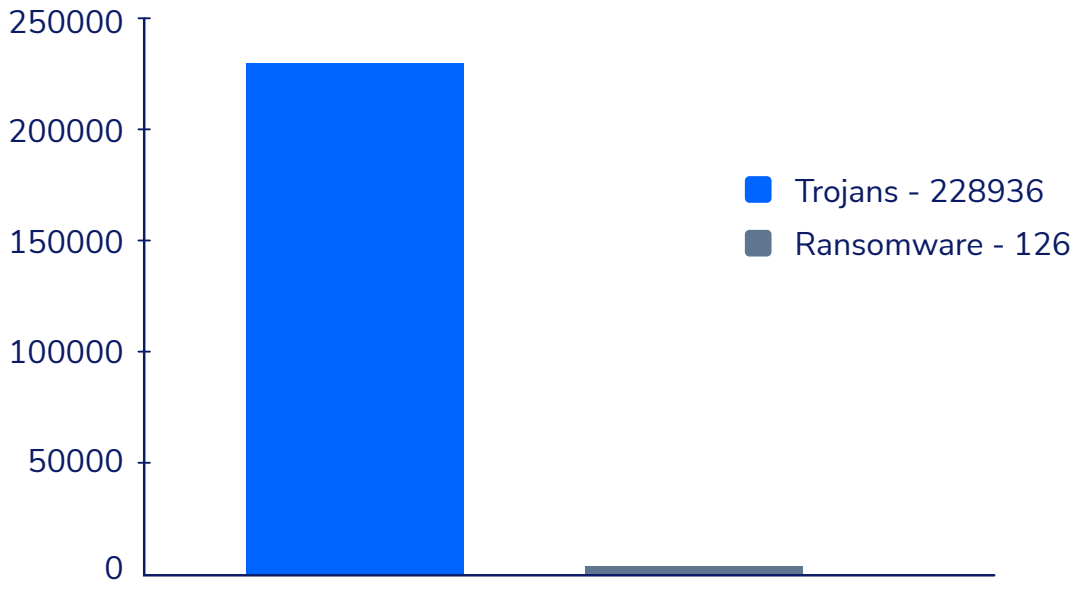
In 2021, we noticed a significant increase in the use of IoT devices in both homes and enterprises. The majority of these IoT gadgets, however, lack robust security capabilities. Because of native security weaknesses, IoT devices are easy to hack. Hackers have noticed the security holes and are attempting to hijack and exploit these devices by smuggling malware entities in to assist them acquire vital data.

Heimdal™ SOC Team for Incident Response Engagements 2020-2021



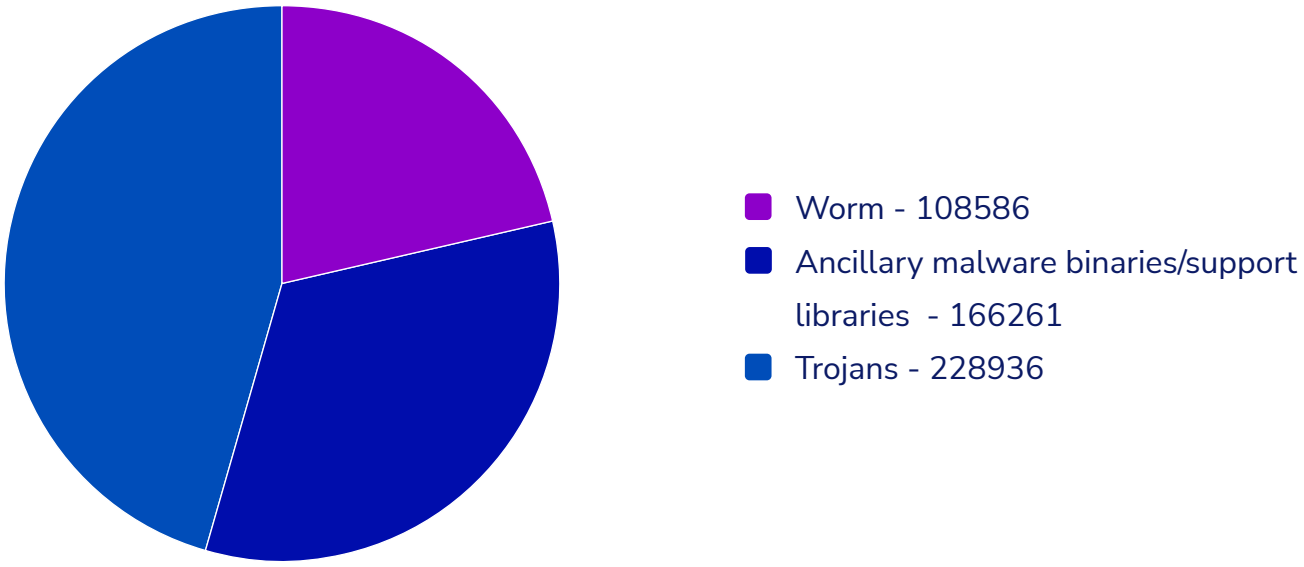
In 2021 our SOC team detected and analyzed over 500.000 cybersecurity related events. We were able to conclude the fact that most of the detections consisted of Trojan malware, leaving the ransomware strains behind.

Trojans vs. Ransomware Detections Discovered by Heimdal™ SOC Team



This is happening as our anti-ransomware encryption solution, the Ransomware Encryption Protection module, stopped the ransomware related threats before they could do any damage to the protected systems.

Top 3 Most Encountered Detections



Worms, Trojans and Ancillary malware binaries/support libraries malware were the ones our SOC Team encountered most often. These types of malware usually look legitimate but can take control over a computer as they are designed to damage, disrupt or steal data.

2021 Malware to Watch Out for

2021 Malware to Watch Out for

2021 was a very active year in cybersecurity with old and new malicious actors making the headlines on a daily basis. Out of all these nefarious attackers, some stood out from the crowd.

Conti

Conti ransomware is an extremely damaging malicious actor due to the speed with which it encrypts data and spreads to other systems. The cyber-crime action is thought to be led by a Russia-based group that goes under the Wizard Spider pseudonym. The group is using phishing attacks in order to install the TrickBot and BazarLoader Trojans in order to obtain remote access to the infected machines.

The email used claims to come from a sender the victim trusts and uses a link to point the user to a maliciously loaded document. The document on Google Drive has a malicious payload, and once the document is downloaded a Bazaar backdoor malware connecting the victim's device to Conti's command-and-control server will be downloaded as well.

Now that it exists on the compromised machine, Conti encrypts data and then employs a two-step extortion scheme.

Double extortion, also known as pay-now-or-get-breached, refers to a growing ransomware strategy and the way it works is that the attackers initially exfiltrate large quantities of private information, then encrypt the victim's files. Once the encryption process is complete the attackers will threaten to make the data publicly available unless they get paid.

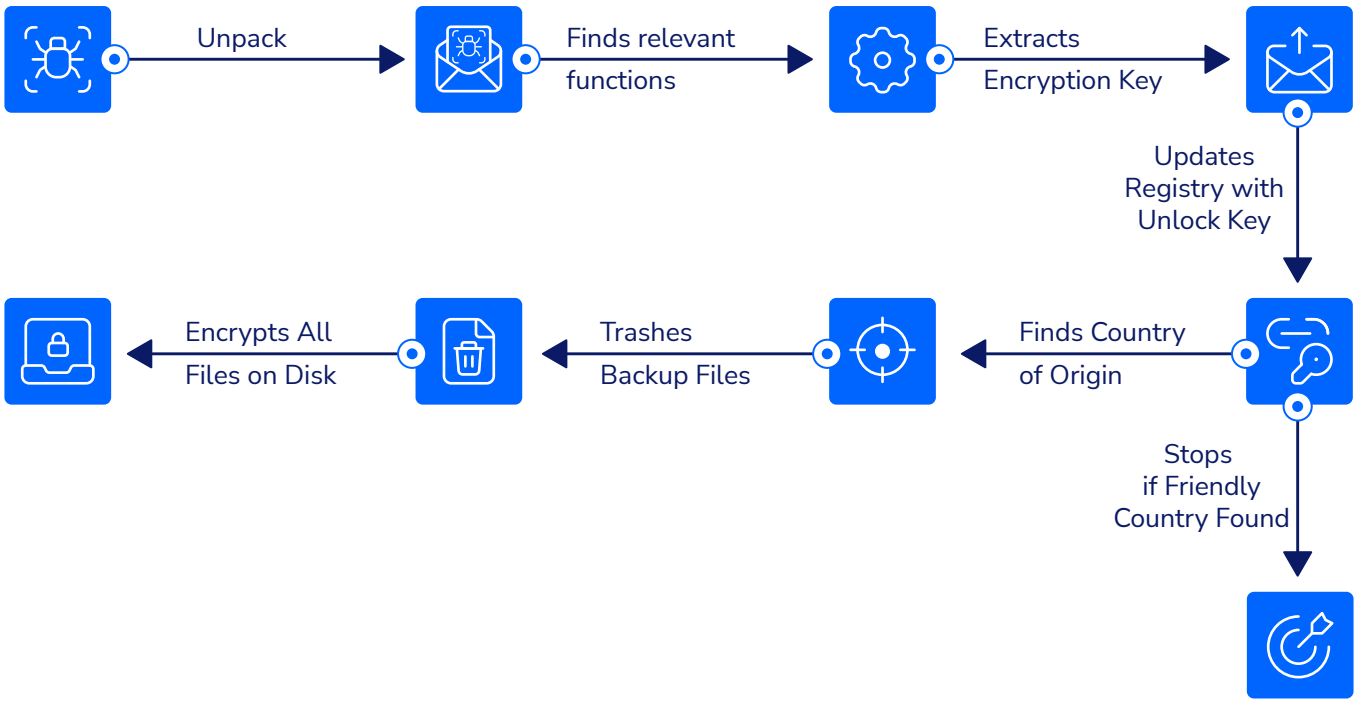
The scheme starts with a ransom demand in return for the decryption key and follows up with an extortion mechanism. In this stage, the malicious actor will reveal a small amount of the encrypted data, with the threat of releasing additional material if the ransom is not paid.

REvil

REvil/Sodinokibi ransomware (AKA Sodin) is a perfect example of Ransomware-as-a-Service, a cybercrime that involves two groups teaming up for the hack: the code authors who develop the ransomware and the affiliates who spread it and collect the ransom.

As reported by Security Boulevard, REvil/Sodinokibi is "the apparent heir to a strain known as GandCrab. The security community believes GandCrab is responsible for 40 percent of all ransomware infections globally. It has taken in around $2 billion in ransom. Then, earlier this year, the creators of GandCrab announced the malware's retirement."

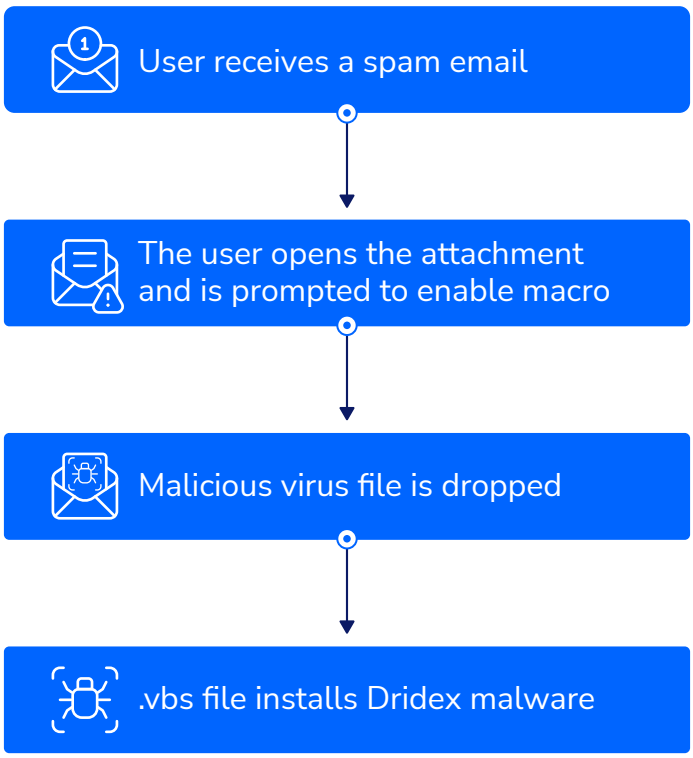
Discovered in April 2019, REvil/Sodinokibi is a highly evasive and upgraded ransomware, which uses a special social engineering move – the ones who spread it threaten to double the ransom if not paid within a certain number of days. This aspect makes Sodinokibi ransomware dangerous for companies of all sizes. Also known as Sodin or REvil, Sodinokibi shortly became the 4th most distributed ransomware in the world, targeting mostly American and European companies.



Dridex

The Dridex virus, in its different versions, has the capacity to compromise customer data confidentiality as well as the availability of data and systems for business activities. According to industry reports, the initial version of Dridex originally debuted in 2012 and had become one of the most common financial Trojans by 2015. We anticipate that attackers employing Dridex malware, and its variants will continue to target the financial services industry, including both financial institutions and clients.

Dridex malware is often distributed by actors through phishing e-mail spam campaigns. To encourage victims to accept attachments, phishing communications use a combination of authentic corporate names and domains, professional vocabulary, and wording conveying urgency. Individuals (name@domain.com), administrative (admin@domain.com, support@domain.com), or common "do not reply" local sections (noreply@domain.com) can be used as sender e-mail addresses. Subject and attachment names can include common phrases like "invoice," "order," "scan," "receipt," "debit note," "itinerary," and so on.

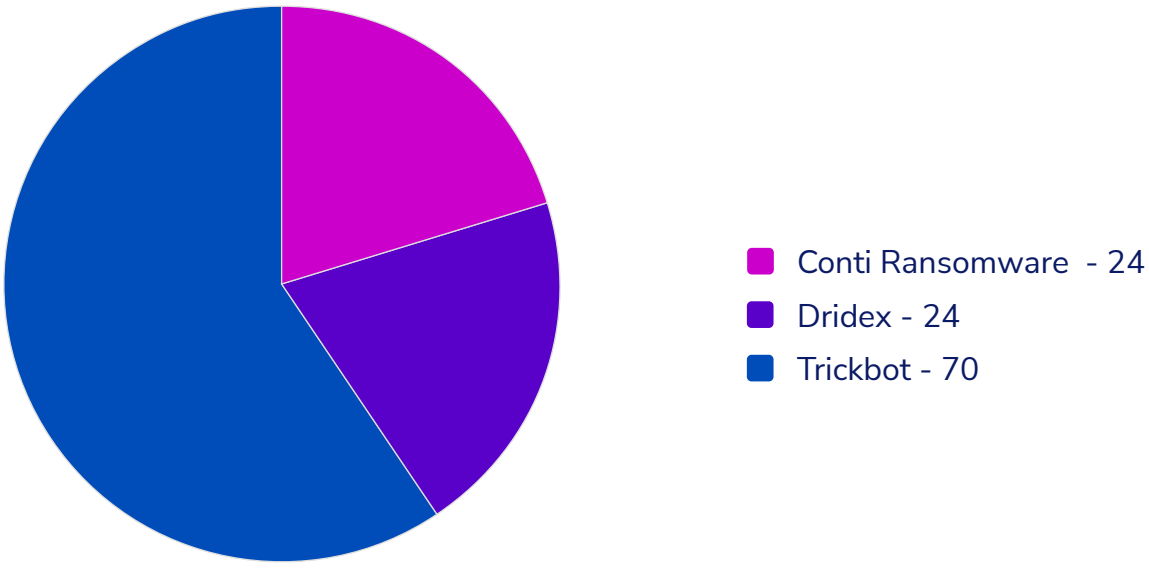


Trickbot

TrickBot began as a banking credential theft Trojan but has evolved into a modular malware enterprise with advanced system reconnaissance, persistence capabilities, and a link to subsequent ransomware attacks. The MS-ISAC is still keeping an eye on TrickBot's capabilities and the dangers it presents to MS-ISAC members.

TrickBot is a distant descendent of the ZeuS banking Trojan, which first appeared in 2005, although it is most commonly associated with Dyre or Dyreza, which went down in 2015. TrickBot appeared in 2016, replicating parts of Dyre malware while preserving its banking credential harvesting and web inject architecture. TrickBot has evolved into a malware empire with a plethora of plugin modules, crypto mining and persistence capabilities, and a growing relationship with subsequent ransomware infestations. Beginning in June 2019, the MS-ISAC noticed a growing link between initial TrickBot infections and subsequent Ryuk ransomware assaults.

Most Prevalent Ransomware Strains Discovered by Heimdal® SOC Team



By analyzing our internal data, we saw that Conti Ransomware, Dridex and Trickbot were the most prevalent ransomware strains that our customers faced in 2021. As previously stated, the number of detections was low as by employing the Ransomware Encryption Protection module these threats were stopped before they could do any damage to the protected systems.

Heimdal® and the Power of Resilience

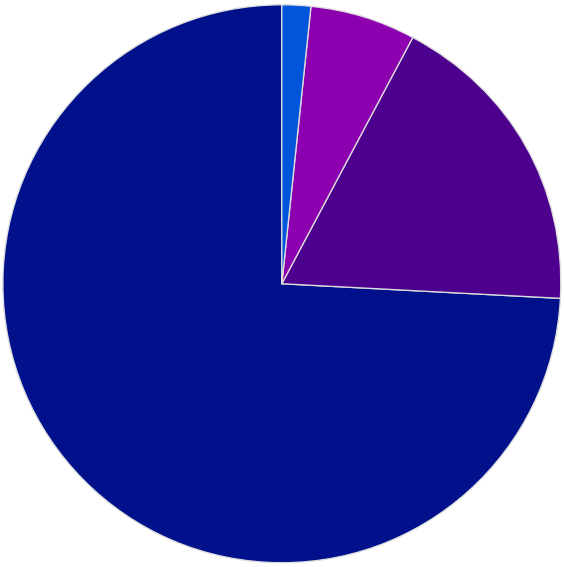
Heimdal® and the Power of Resilience

Risk of Successful Cyberattacks Apparently Drops Amidst Volumetric Attacks Increase

During the course of a larger cybercrime investigation regarding attack & exfiltration methodologies, Heimdal™ Security's SOC team has discovered that although cyberattacks have increased in volume, the odds of success have dramatically decreased. In analyzing the trendlines pertaining to successful vs. unsuccessful cyber-aggressions in the context of volumetric inflation, Heimdal™ has aggregated data from all available detection grids (i.e., anti-ransomware encryption protection, antivirus, brute-force guardrails, DNS traffic analyzer, and email protection).

Heimdal™ has pooled six months-worth of detection data from five modules: Ransomware Encryption Protection, Next-Gen Antivirus, Brute-Force Analyzer, Threat Prevention – Endpoint + Network, and Email Security. Throughout the aforementioned six-months timeframe, 10,618,665 detections have been registered by Heimdal™ Security.

A subsequent breakdown of the attack by surface reveals that a staggering 71.8% (5,004,686) of the registered aggression has been carried out by email (i.e. phishing, spearphishing, Business Email Compromise, Vendor Email Compromise, CEO fraud, etc.).



The values related to the remaining attack surfaces are as follows:

- Malicious Encryption Attempts – 4,200;
- Antivirus-related Infections – 346,955;
- Brute-Force (Attempts) – 1,090,561;
- DNS-delivered Infections – 4,172,263.

From a statistical point of view, given the surge in volume, we ought to have more cases of data breaches, illegal data exfiltration, and ransomware-type activity. However, Heimdal™'s assessment proves the exact opposite – fewer odds of impact, despite visible volumetric growth.

The data we have analyzed suggests that this development could have been caused by:

- EDR-type countermeasures that must have atenuated the efficiency of the average attack.
- The existing threat-hunting methodology based on seek-and-destroy techniques has rendered most of these attacks useless.
- The attackers' attempt to probe defenses with attacks that have fewer chances of success.

GLS SPAM Campaign, and the IP Source

Back in November, our CEO, Morten Kjærsgaard, received an email posing as a legitimate email from GLS Denmark.

After taking a look into the email, we discovered that the malicious IP was 209.85.220.41. It seems that this was an IP address from North America, United States, so it was definitely not sent by GLS Denmark.

The threat actors used a public IPv4 – Version 4 from the C class range.

Outlining the incident, Heimdal™ has unearthed a new GLS Spam sophisticated campaign. Unlike akin campaigns, the newly dubbed GLS credit card credential phishing campaign leveraged NLP obfuscation techniques that rendered the message illegible when attempting to inspect or duplicate the contents. Its modus operandi closely resembled past parcel-delivery phishing scams, whereupon e-mail that informed the victim about some details that need to be filled out for a certain shipment. The victim had to click on the provided link in order to perform a set of instructions, a link that, as its name said, was leading to a page with “delivery options”.

On closer inspection of the link’s origin, we have discovered that the user would have been redirected to a forged GLS parcel tracking and payment notification page. Another interesting aspect about the email delivery system was that the attackers employed alphanumerical permutations and/or additions in an attempt to circumvent spam filters. Additional means of obfuscations were not uncovered during the course of the investigation. The duplicitous nature of the forged GLS page wouldn’t have attracted suspicion as to its contents closely resembling the original Danish page.

Upon trying to duplicate the contents of the message by clipboard exportation, the user would have been left with illegible text.

Subsequent analysis revealed that the API employed HTML span tags that would have had the aforementioned effect on this text if the user would have attempted to interact with it in an unexpected manner. NLP obfuscation to this degree proves that most spam/phishing filters function below par, allowing dangerous emails to pass.

The credit card credential phishing campaign was highly focused, as previous attempts to access the page failed. VPN-tunnelling was successful, our team being able to render the page's contents using a Denmark VPN.

The threat scenario went as follows: the user was prompted via email that a package was in waiting. After landing on the page, the user would have been instructed to supply all necessary credit card details (i.e., card number, expiration month & date, and CVV2 code) in order to receive the package in waiting. The payment information about the extra tax read "GLS Postage [taxes]". The operation would have been completed by pressing the "Pay" button. However, upon closer examination, it was discovered that the forged page was brokered by an API whose purpose was to relay the credit card information to an undisclosed Telegram account, tracked to Turkey, in the outskirts of Istanbul.

Typosquatting Domain Masquerading as Crypto-Swapping Platform

Heimdal™ Security's Security team discovered a new typosquatting domain specifically crafted to resemble Trader Joe XYZ's URL, one of the most sought-after cryptocurrency trading platforms. Tricked by a typo in the spelling of the crypto-swapping platform's URL, users would send their MetaMask wallets to an unknown party or parties that would ultimately despoil their contents.

The domain, associated with the IP address 68.65.123.18 and tracked via ARIN to US soil, contained the misspelled world "trader" (i.e. tradrjoexyz.com instead of the legitimate traderjoexyz.com). Additional metrics provided by a VirusTotal query suggest that the typosquatting domain has had numerous associations with other (potentially) harmful domains.

Trader Joe XYZ's case isn't singular. Every day, thousands of typosquatting domains are generated, some of them so flawless in design that not even an expert's eye could tell them apart.

So, as always, Heimdal™ recommends extra caution when navigating unknown websites and, of course, searching them on Google before committing your credentials.

DeepBlueMagic Ransomware

Our team of security experts was alerted to an incident that turned out to be a new ransomware strain along with a ransomware note, signed by a group dubbing themselves 'DeepBlueMagic'.

This new ransomware strain is a complex one, displaying a certain amount of innovation from the standard file-encryption approach of most others.

The affected device from which the ransomware infection originated was running Windows Server 2012 R2.

By cleverly making use of a legitimate third-party disk encryption tool, the DeepBlueMagic ransomware started the encryption process not of files on the target's endpoint, as ransomware usually does, but of the different disk drives on the server, except the system drive (the "C:\" partition).

The legit disk encryption third-party tool used is "BestCrypt Volume Encryption" from Jetico.

The "BestCrypt Volume Encryption" was still present on the accessible disk, C, alongside a file named "rescue.rsc", a rescue file habitually used by Jetico's software to recover the partition in case of damage. But unlike in the legitimate uses of the software, the rescue file itself was encrypted as well by Jetico's product, using the same mechanism, and requiring a password in order to be able to open it.

It is a very unusual modus operandi for a ransomware strain, since these infections most often focus on files.

The DeepBlueMagic ransomware used Jetico's product to start the encryption on all the drives except the system drive.

The machine was found with the “C:\” drive intact, not encrypted in any way, and with ransom information text files on the desktop. The C drive is a smaller stakes ransomware target since the more valuable files are located on the other partitions, not on the system drive which is used for running executables and performing operations.

In this case, it was the “D:\” drive that was turned into a RAW partition rather than the common NTFS, making it inaccessible. Any access attempt would have the Windows OS interface prompt the user to accept formatting the disk since the drive looks broken once encrypted.

Further analysis revealed that the encryption process was started using Jetico’s product, and stopped right after its initiation. Therefore, following this go-around process, the drive was only partially encrypted, with just the volume headers being affected. The encryption can be either continued or restored using the rescue file of Jetico’s “BestCrypt Volume Encryption”, but that file was also encrypted by the ransomware operators.

Moreover, the ransomware cleared the stage before commencing the encryption. Before using Jetico’s “BestCrypt Volume Encryption”, the malicious software stopped every third-party Windows service found on the computer, to ensure the disabling of any security software which is based on behavior analysis. Leaving any such services active would have led to its immediate detection and blocking.

Afterward, DeepBlueMagic deleted the Volume Shadow Copy of Windows to ensure restoration is not possible for the affected drives, and since it was on a Windows server OS, it tried to activate Bitlocker on all the endpoints in that active directory.

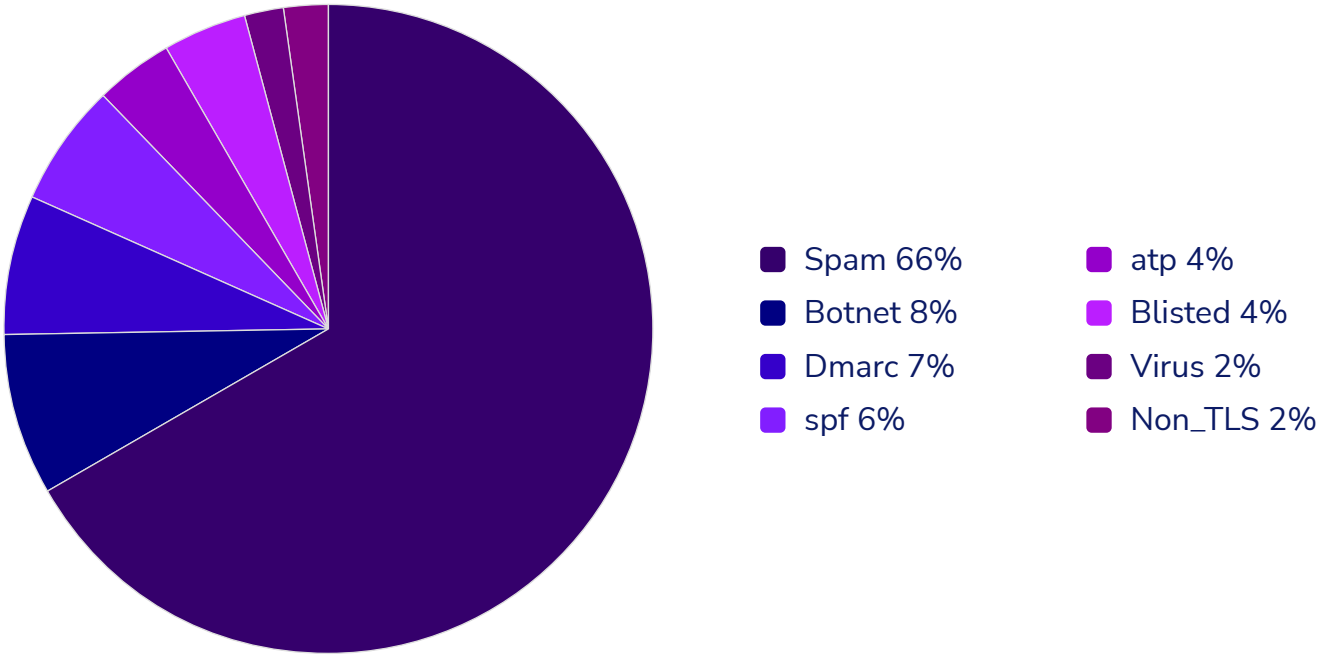
On the affected server, no failed login attempts were found in the audit logs, so the entry point was not based on any brute-force attempt. The server only had a Microsoft Dynamics AAX installed with a Microsoft SQL Server.

Over 7 Million Threats Blocked in 2021

When taking a more in-depth look at the way in which the cybersecurity landscape changed in 2021, we couldn't help but notice the fact that our clients were kept safe from major cyber events.

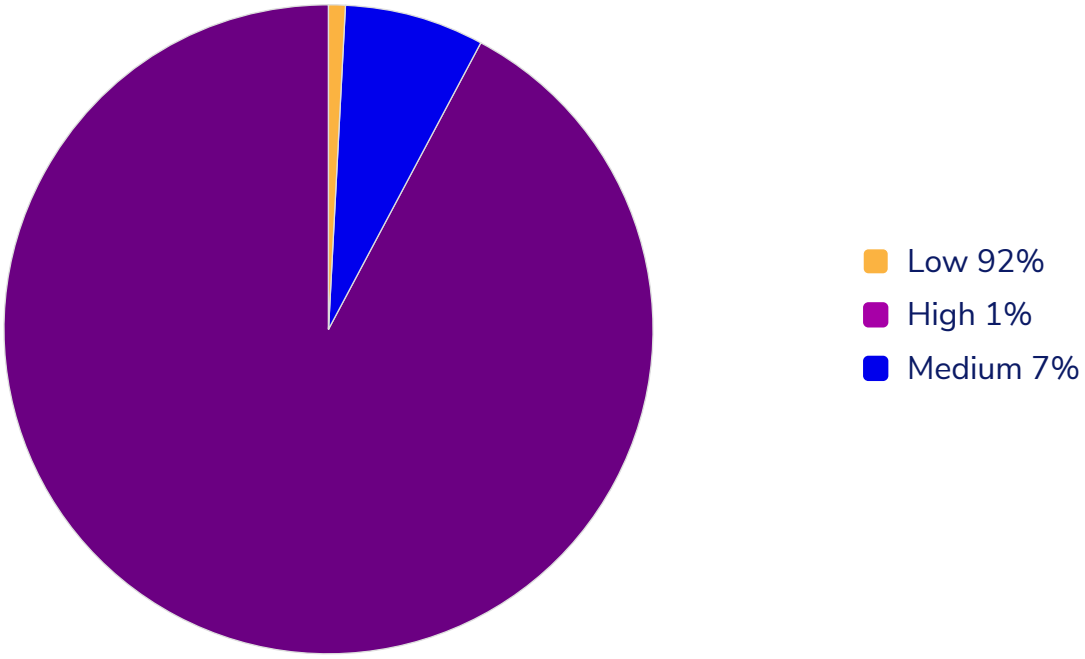
Heimdal™ Email Security is the email assurance your remote and on-premises workforce needs. Every email is scanned for impersonation, data leak risks, and more. File attachments are scanned by default and blocked if the contents are marked as suspicious.

Over the past year, our product has managed to block over 7 million threats making it the email assurance your remote and on-premises workforce needs.



By using 125 vectors of analysis coupled with live threat intelligence we were able to stop Business Email Compromise, CEO Fraud, phishing and complex malware before compromise.

In the past three months we've identified from a total of 14.9 mil mails scanned: 17 Critical, 65 High, 867 Medium, 10675 Low.



But email-originated threats were not the only ones stopped by our products, as 7,456,436 attacks were kept at bay by our Threat Prevention Module.

In 2021 our SOC team discovered and patched over 183 CVEs with an average severity score of 8.14. The vulnerabilities were encountered 1726 times.
CVE-2021-38503, a vulnerability affecting the iframe sandbox rules was one of the most prevalent vulnerabilities discovered with 123 detections. In this case the rules were not correctly applied to XSLT stylesheets, allowing an iframe to bypass restrictions such as executing scripts or navigating the top-level frame.

This vulnerability affected Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3.
The **CVE-2021-28476** and **CVE-2021-43215** were seen 53 times by the SOC team.

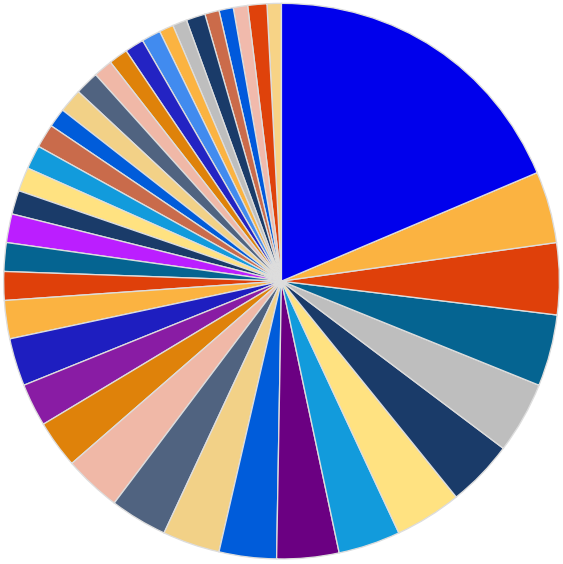
CVE-2021-28476 has a 9.9 severity score and allows a guest VM to force the Hyper-V host's kernel to read from an arbitrary, potentially invalid address.

The contents of the address read would not be returned to the guest VM. In most circumstances, this would result in a denial of service of the Hyper-V host (bugcheck) due to reading an unmapped address.

It is possible to read from a memory-mapped device register corresponding to a hardware device attached to the Hyper-V host. This may trigger additional hardware device specific side effects that could compromise the Hyper-V host's security.

CVE-2021-43215 is an iSNS Server Memory Corruption Vulnerability Can Lead to Remote Code Execution, that has a severity score of 9.8.

Most Frequently Encountered CVEs by Heimdal SOC Team



- CVE-2021-38503
- CVE-2021-28476
- CVE-2021-43215
- CVE-2021-36965
- CVE-2021-26424
- CVE-2021-1694
- CVE-2021-31962
- CVE-2021-34527
- CVE-2021-24111
- CVE-2021-26443
- CVE-2020-1472
- CVE-2021-26893
- CVE-2021-44686
- CVE-2021-43537
- CVE-2021-40461
- CVE-2021-27092
- CVE-2021-34450
- CVE-2021-30571
- CVE-2021-28449
- CVE-2021-41342
- CVE-2021-21223
- CVE-2021-28562
- CVE-2021-42275
- CVE-2021-28346
- CVE-2021-33757
- CVE-2018-16550
- CVE-2019-5736
- CVE-2018-1000182
- CVE-2020-13699
- CVE-2021-1636
- CVE-2016-10917
- CVE-2021-34446
- CVE-2020-1147
- CVE-2021-28453
- CVE-2020-0689
- CVE-2021-26855
- CVE-2021-1715
- CVE-2020-24429
- CVE-2006-0614

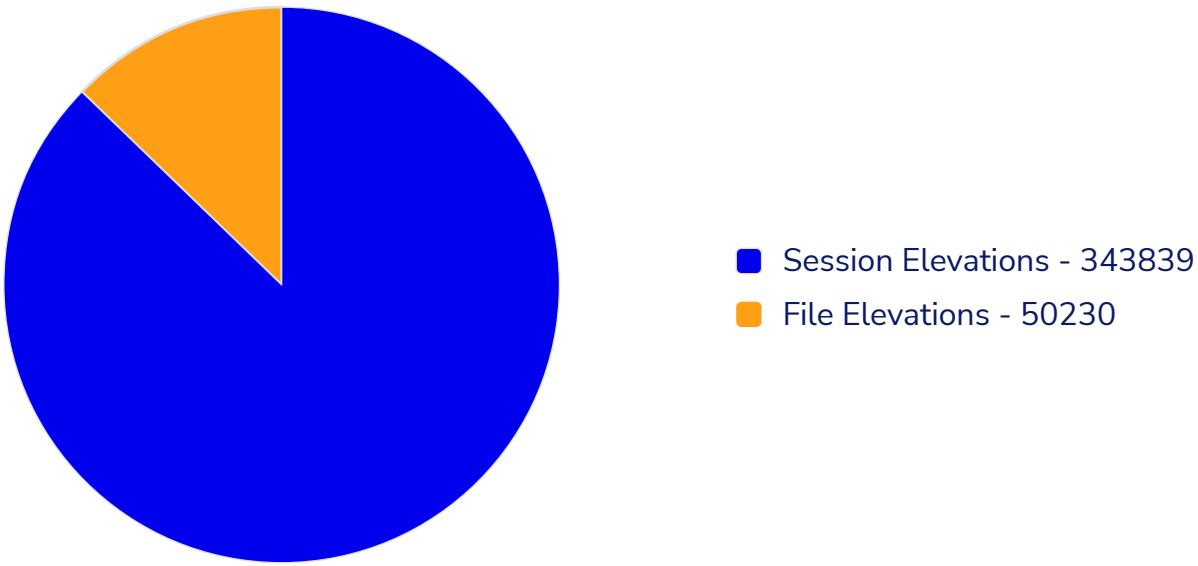
Our Privileged Access Management tool streamlines and secures the rights management flows allowing for easy and cohesive escalation efforts.

By allowing two types of privileged elevations: per session and per single file, the Heimdal Privileged Access Management tool is vital when it comes to scalability and achieving data protection compliance. When thinking about elevation automation, PAM should come to mind as it will certainly save money on staff costs for IT ops, whilst providing as well a secure way to perform elevations.

Using Heimdal's Privileged and Access Management tool in 2021 our customers performed **343839 session elevations** and **502230 file elevations**.

The usage extent of the tool clearly points to how easy it is for organizations to rely on using a dedicated platform in order to manage user rights, as opposed to granting them to everyone, whilst making sure to maintain optimal cybersecurity standards.

PAM Elevations Discovered by Heimdal's SOC Team



Powershell, cmd and msc were the main elevated apps from our Privileged and Access Management tool.

Constantly Innovating

Constantly Innovating

Conquering New Heights in Remote Support

To further augment your flexibility in a remote support scenario, Heimdal™ Remote Desktop allows you to invite multiple users to the same session.

Furthermore, Remote Desktop allows you and your end-users to share files, media, and anything else you might need for the session in a seamless collaborative environment. Everything you need for remote support is at your fingertips when using Heimdal™, only one click away.

In addition to this, our solution will be compatible with any device and operating system in 2022, which means that you won't be limited by any prerequisites when helping your employees or customers.

New Zero-Trust Feature for Application Control, Privileged Access Management, and Next-Gen Endpoint Antivirus

Heimdal™ Security has launched this year a new and market redefining cross-module Zero-Trust Execution Protection functionality that will allow customers to seamlessly protect their organization against zero-hour threats.

The submodule is bound to work in the Heimdal™ Agent if at least one of the three main modules which encapsulate it is enabled: Privileged Access Management, Application Control or Next-Gen Antivirus, and MDM.

It will be manageable from the Endpoint Settings section across three different Heimdal™ Dashboard areas:

- Privileges & App Control -> Application Control;
- Privileges & App Control -> Privileged Access Management;
- Endpoint Detection -> Next-Gen Antivirus.

If the submodule is enabled or disabled in one of the three above-mentioned Settings areas, the change will take effect in all of the three modules.

The new Zero-Trust Execution Protection will intelligently diagnose all running processes within the customer's IT environment to detect and block malign or questionable executions. Our cutting-edge technology will appropriately mitigate the potentially harmful processes with no impact on the overall machine performance, which will definitely save a significant amount of time for system administrators.

In a cybersecurity market that keeps accelerating the focus on privileged and identity access management, this is the most advanced golden standard in cybersecurity EDR tools, empowering users to always stay one step ahead of any attacker.

Cybersecurity Predictions:

What to Expect in 2022?

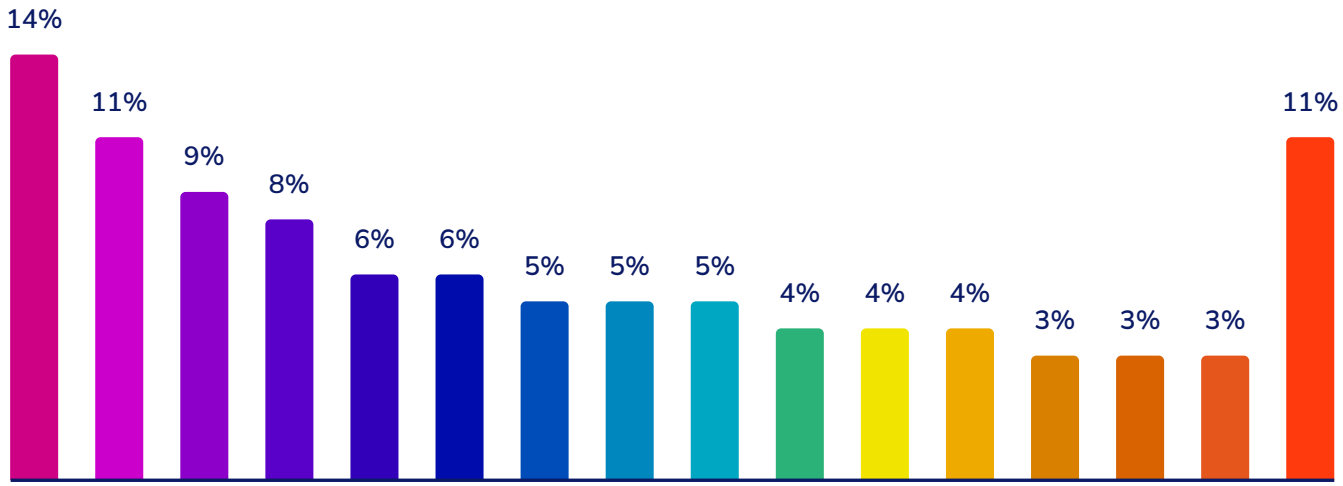
Cybersecurity Predictions:

What to Expect in 2022?

Heimdal™ Security is a rapidly growing cybersecurity company that provides easy, world-class solutions for unified, intelligent cybersecurity.

We are ready to help your company to deal with a large range of concerns, including threat volume and complexity, a rising cybersecurity skills gap, and the requirement for threat prioritization, to name a few.

Top Internal Security Pain Points



- User Behavior
- Politics/Lack of attention to Security
- Compliance Related Requirements
- Staffing Information Security
- Malicious Software (Malware)
- Security Awareness Training
- Lack of Budget
- Vulnerability Management
- Data Loss/Theft
- Endpoint Security
- Accurate Monitoring of Security Events
- Application Security
- Mobile Device Security
- Cloud Security
- Keeping Up with New Technology
- Other

Heimdal™ Security is already uniquely positioned against what we believe to be the upcoming market challenges and red-hot problems, offering our customers:

- An outstanding Ransomware Encryption Protection module, that is universally compatible with any antivirus solution, and is 100% signature-free, ensuring superior detection and remediation of any type of ransomware, whether fileless or file-based (including the most recent ones like LockFile);

- Market-leading Threat Prevention for both network and endpoint, that will discover and prevent threats at DNS, HTTP, and HTTPS level, helping you keep away much more of today's and tomorrow's cyber threats than any antivirus will do;

- A truly unique, highly automated patching solution, that allows you to deploy secure Microsoft, 3rd party and custom updates whenever you choose, anywhere in the world;

- A Privileged Access Management solution that completely simplifies the process of granting admin rights and also de-escalates privileges upon threat detection when used in conjunction with our Threat Prevention and Endpoint Detection solutions;

- Two fantastic Email Security modules, that will help you avoid email-deployed malware and ransomware, business email compromise, phishing, CEO fraud, and botnet attacks.

The most important cybersecurity trends that we expect to see in 2022 are: a massive increase in supply chain attacks (ransomware especially), potentially through globally reaching supply chains like Microsoft Update, huge remote work challenges, data protection and authentication transformations, machine learning and AI favouring the evolution towards prevention instead of mitigation, an increased necessity for real-time data visibility, extended detection and response and unified endpoint management, as well as a long-awaited increase in user awareness.

Top Cybersecurity Trends for 2022

- Supply Chain Attacks and Ransomware
- Remote Work Challenges (IOT, BYOD, Cloud Security, Phishing, PAM, Zero-Trust)
- Data Protection and Authentication Transformations
- Machine Learning and Artificial Intelligence for Prevention Instead of Mitigation
- Real-Time Data Visibility
- Extended Detection and Response & Unification
- Increased Cybersecurity Awareness

About Heimdal® Security

About Heimdal[1ZZ] Security

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 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 international awards for both its solutions and educational content creation.

Currently, Heimdal's cybersecurity solutions are deployed in more than 45 countries and supported regionally from offices in 15+ countries, by 175+ highly qualified specialists. Heimdal is ISAE 3000 certified and secures more than 2 million endpoints for over 10,000 companies. Heimdal supports its partners without concessions on the basis of predictability and scalability. The common goal is to create a sustainable ecosystem and a strategic partnership.

Become a Heimdal™ Partner

Products and Services

Products and Services

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

Privileged Access Management allows you to easily elevate user rights or file executions, gives you the ability to revoke escalations and supports zero-trust execution.

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.

Assist

Remote Desktop

Remote access and support solution compatible with Windows, Mac, and Android. Easily connect with your employees and customers across various devices. Secure, ready-to-use, compliant, with stunning visuals, and steady remote connection.

Services

Endpoint Prevention Detection and Response (EPDR)

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.

Book a demo

Heimdal®

Leading the fight against cybercrime.

www.heimdalsecurity.com

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