The State of Consumer Cybersecurity

2024 January

A Report by ReasonLabs

Table of Contents

01. Executive Summary
Methodology
Key Takeaways

02. Top 5 General Detections Affecting Home Users
Trojans
HackUtilities
Adware
Viruses & Worms
Ransomware

03. Web Threats
Global Landscape
U.S. Landscape
Malicious Extensions

04. Cyberwarfare
Top 20 Most Attacked Countries
State-Sponsored Hacking

05. Online Piracy
Torrent Files
Top 10 Malicious Torrent Files
Top Threats Found In Torrents

06. Emerging Threats
Malicious Web Extensions
Generative AI Attacks
Deepfake Scams

07. How Home Users Can Protect Themselves
Endpoint Protection Tools
EDR In The Home
Identity Protection
Parental Control Software
Continuing Education

08. 2024 Predictions

09. Conclusion
Contributors

01 Executive Summary

Consumers are increasingly immersed in online activities today's connected world. Whether engaging in e-commerce, gaming, remote work, virtual education, content streaming, or any other pursuit, **home users continuously confront an array of cyber threats.**

A shared reality among most individuals or home users, regardless of geographical location or socio-economic status, is **the absence of robust cybersecurity measures to safeguard their devices, home networks, and physical lives** against evolving digital threats. While some threats have persisted over decades, others are more novel developments, emerging from technologies such as cryptocurrency, virtual, or mixed reality.

Within this report, **researchers from ReasonLabs' Threat Intelligence Center** will intricately outline the prevalent threats encountered by home users throughout 2023 and offer valuable insights into the evolving nature of specific threats. ReasonLabs' researchers will also delve into the areas where these threats have exhibited notable success and assess their potential for damage, both present and future.

Complementing their research findings, members of ReasonLabs' Threat Intelligence Center will share **how home users can fortify their defenses, advocating the use of diverse endpoint security tools** and implementing safety controls for their families. Drawing on this knowledge and identified trends, ReasonLabs researchers have extrapolated predictions regarding challenges anticipated in the coming year and guide how consumers can navigate and overcome them.

Methodology

The State of Consumer Cybersecurity 2024 incorporates information compiled from intelligence meticulously gathered by **security researchers at ReasonLabs' Threat Intelligence Center.** The data spans from January 1, 2023, to December 31, 2023.

The gathered malware information originates exclusively from **ReasonLabs users dispersed across more than 180 countries globally.** The data specifically focuses on real-time detections from users holding both free-to-use and premium accounts. This approach is employed to safeguard against the inclusion of outlier data that could potentially distort trend analyses.

ReasonLabs

Key Takeaways

1

Phishing is by far the most prevalent browser-originated threat facing U.S. residents. At 56.7% of all U.S. detections made by RAV Online Security, consumers must learn to better recognize phishing and avoid falling victim to these very simple but harmful attacks.

2

Russia was one of the most highly targeted countries in 2023. Almost 20 detections were made per user in Russia and 25% of all users had either downloaded or received a malicious web extension.

3

25% of this year's top 20 'Most Attacked Countries' are in Europe - more than doubling last year's total. There was also a notable decrease in countries from Asia/Middle East, as 40% of this year's list is comprised of countries from that region compared to 50% from last year.

4

There has been a sharp increase in the use of harmful web extensions by malicious actors looking to steal sensitive data, personal information, and intellectual property.

5

Fake versions of "Grand Theft Auto V" and "World of Warcraft" were the two games most used to distribute malware by bad actors. These games were often downloaded through torrent files by users.

6

Home users are not immune from state-sponsored hacking campaigns. We saw many users in South Korea affected by North Korean-backed hackers' use of the Magniber ransomware.

7

Consumers must look to Identity Protection services to fight the dangers associated with data breaches. Even if a user doesn't download malware, they can still be affected.

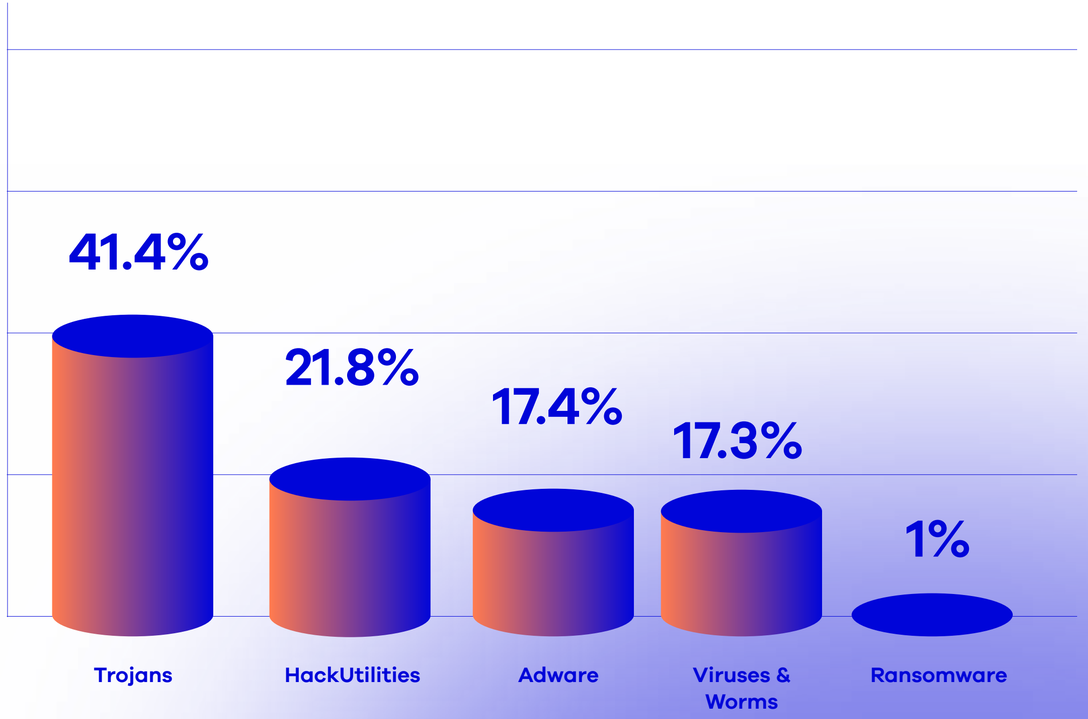
8

Social engineering and phishing attacks will continue to rise in 2024. These attacks will thrive as the gap between the sophistication of hackers and the awareness of consumers continues to grow.

02 Top 5 General Detections Affecting Home Users

Looking at data derived from RAV Endpoint Protection users, this year's investigation found that **Trojans were by far the top threat to home users, accounting for over 41% of all detections made.**

The category of HackUtilities, which is comprised of cheats, trainers, license software hacks, hacking tools, and more, accounted for more than 21% of detections made worldwide. Following HackUtilities were Adware, Viruses & Worms, and Ransomware detections respectively.



Trojans

Computer Trojans are a type of malware that disguise themselves as legitimate programs but, once executed, carry out nefarious activities, often without a user's knowledge or consent. A Trojan typically appears benign or even beneficial on the surface but conceals harmful intent.

One prevalent type of Trojan we would like to highlight is Infostealers, which are one of the top Trojans plaguing home users today.

Infostealers are a type of malware specifically designed to infiltrate computer systems and hijack sensitive information. They are usually created and deployed with the primary purpose of stealing valuable data, which can include personal information, login credentials, financial details, and other confidential items.

HackUtilities

HackUtilities comprises various items like game cheats, trainers, license software hacks, hacking tools, and more that home users worldwide often download.

One way these items make their way onto user's devices is through online piracy. Online piracy is by no means a new topic, however, it remains a major driver of the deployment of malware. The prevalence of HackUtilities detections throughout 2023 is clear evidence that home users are turning more and more to pirated or cracked software instead of purchasing software. We will discuss online piracy more later in the report.

Adware

Adware is typically divided into two categories: software that pushes ads outside of the software's scope or nefarious adware that causes harm.

The second of the two categories consists of malware that can inject unwanted ads onto a device, hijack a computer's settings, such as search behavior, and show potentially dangerous ads that can spread into other forms of malware. Some common types of this form of adware include Malicious Browser Modifiers and Extension, Ad-Injecting Trojans, Deal Finders, and more.

Viruses & Worms

Although many associate malware with viruses, the term 'virus' refers to programs designed specifically to autonomously replicate and contaminate other files on a target computer.

This occurs through the incorporation of its malicious code into unsuspecting files, including other programs. Upon execution of these programs, they proceed to undertake malicious activities outlined by the virus. Contrary to the belief that their prevalence diminishes over time, numerous legacy viruses from the past continue to remain active in the ecosystem, disseminating their payloads.

Ransomware

Most Ransomware gangs often target enterprises or large institutions because they can usually pull off a greater ransom from them instead from consumers. Moreover, the majority of businesses ultimately comply with ransom demands, whereas consumers are considerably less prone to do so.

Nevertheless, given the increased investment in cyber protection by larger institutions in recent years, this trend may shift.
In 2023, the most common ransomware threats that targeted consumers included some familiar faces, with a couple of new ones.

Top 5 Global Ransomware Family Detections

Fusion

25.2%

LoveRabbit

16.9%

GandCrab

11.8%

REvil

9.9%

Magniber

7.2%

03 Web Threats

As of October 2023, there were 5.3 billion internet users worldwide, amounting to over 60% of the global population. To best protect internet users, **ReasonLabs introduced a robust identity protection tool called RAV Online Security** in 2022—a web extension embraced by over 15 million users globally, compatible with Google Chrome and Microsoft Edge.

The Online Security extension safeguards users by obstructing malicious cookies and trackers, providing identity protection services, conducting threat scans, and more. **The following data sets are browser-originated threats** derived from users of the Online Security web extension.

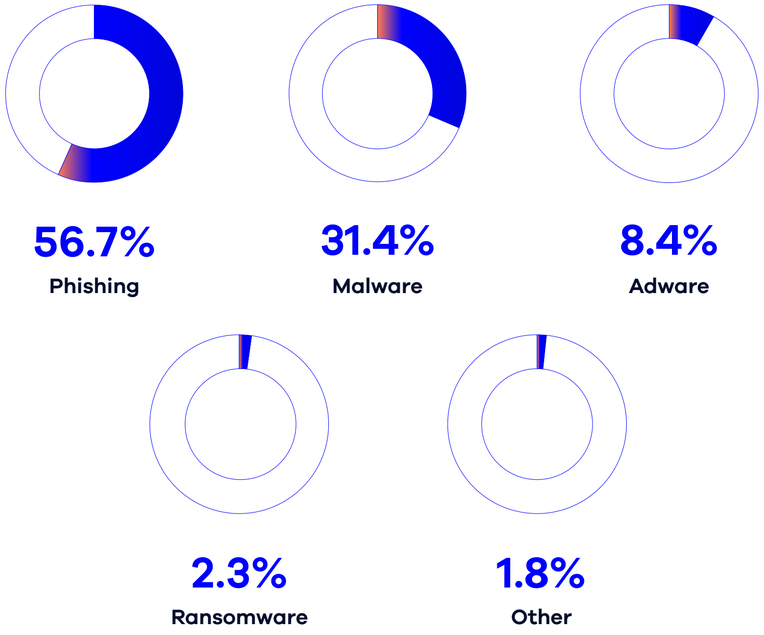
Global Landscape

Of the more than 15 million global users of the Online Security web extension, **Malware was largely the top threat they faced in 2023**. Phishing followed Malware as the second most common browser-originated detection, browser-originated detection, followed by Adware and cryptomining respectively.

Malware	Phishing	Adware	Cryptomining	Other
54.3%	26.4%	15.5%	2.1%	1.7%

U.S. Landscape

Looking at the U.S. data, however, phishing was by far the most common detection made in 2023, followed by Malware, Adware, and Ransomware respectively.



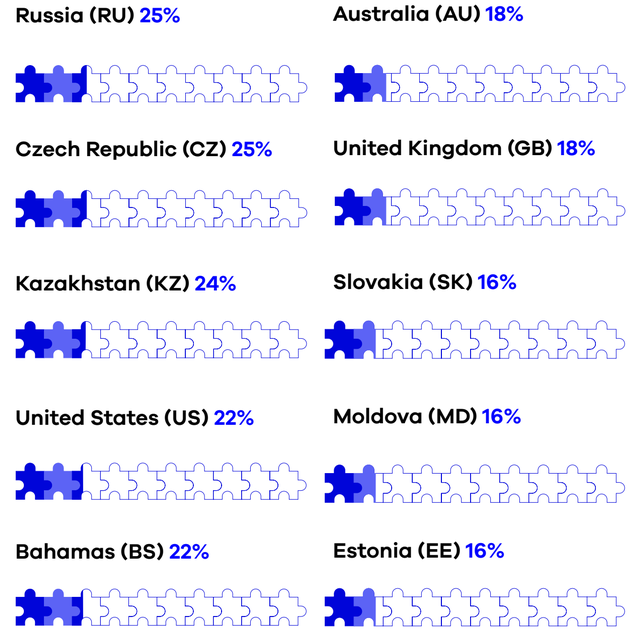
Seeing as Phishing is the number one browser-originated attack vector for U.S. residents, consumers must educate themselves on internet data hygiene and do their best to avoid falling victim to attacks.

Malicious Extensions

The surge in the adoption of browser extensions has been accompanied by an increase in the creation of harmful extensions by malicious actors who have identified and exploited this relatively novel attack pathway. Bad actors are getting considerably better at manipulating the open architecture of web browsers and the naïveté of users. There were numerous big reports of malicious extensions plaguing home users in 2023:

- Google removed a phony Chrome browser extension in March that was masquerading as OpenAI's ChatGPT. The extension harvested Facebook session cookies and hijacked over 9,000 accounts.
- In June, Google removed 32 malicious extensions with over 75 million downloads, altering search results and pushing spam or unwanted ads to users.
- In December, ReasonLabs researchers uncovered a scam where hackers targeted users' cashback activity to hijack sensitive information via fake VPN extensions for Chrome and Edge.

Top 10 countries with the most malicious extension detections made per user in 2023.



(Country/ Percentage of users with detections)

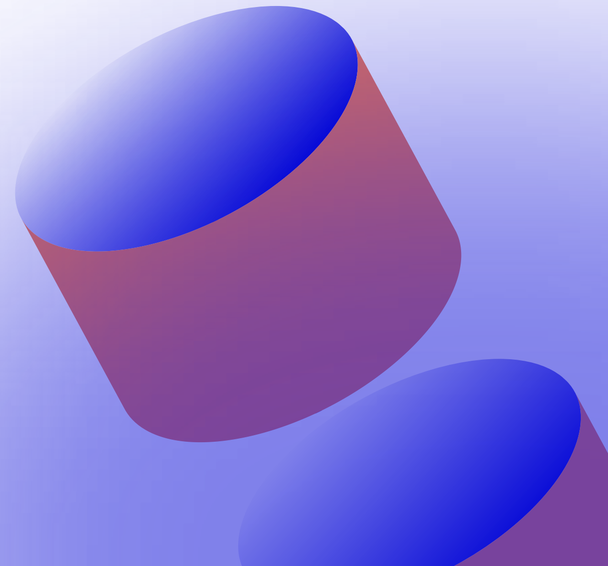
04 Cyberwarfare

Cyberwarfare encompasses the use of connected devices and networks in warfare. It entails activities conducted by decentralized entities or nations seeking to infiltrate the computer systems or networks of another country with the intent of causing harm or disruptions.

These threats fall into three main categories: Cyber Attacks, Cyber Espionage, and Cyber Terrorism. Cyber Attacks involve harmful actions that manipulate, alter, or steal crucial information from external systems, targeting not only military objectives but also various sectors and consumers. Conversely, Cyber Espionage refers to the covert use of digital methods to gather intelligence. Lastly, Cyber Terrorism employs IT-based assaults in terrorist operations to destroy networks, computer systems, and the internet itself.

Top 20 Most Attacked Countries

Geography **significantly influences the nature, quantity, and prevalence** of diverse cybersecurity attack versions. In this segment, we'll look at detection rates with data derived from RAV Endpoint Protection users.



The leading five countries with the highest number of detections per user in 2023 are **Kazakhstan, Russia, the Czech Republic, Egypt, and Belarus respectively.** Notably, the Czech Republic and Belarus made huge jumps from last year - both did not register in 2022's top 20 list, while this year they cracked the top five.

Interestingly enough, **25% of this year's top 20 are in Europe, more than doubling last year's total of 10%.** There was also a notable decrease in countries from Asia/Middle East as 40% of this year's list comprised countries from that region, compared to 50% from last year.

Country/ Average number of detections per user							
Belarus (BY) 12.06	Bolivia (BO) 10.83	Ukraine (UA) 9.75	Algeria (DZ) 9.54				
Kazakhstan (KZ) 26.73	Czech Republic (CZ) 18.36	Azerbaijan (AZ) 11.33	Moldova (MD) 10.52	Venezuela (VZ) 9.65	Myanmar (MM) 9.06	Uzbekistan (UZ) 8.72	Côte d'Ivoire (CI) 8.47
Russia (RU) 19.74	Egypt (EG) 13.44	Cameroon (CM) 11.26	China (CN) 9.82	Iran (IR) 9.56	Indonesia (ID) 8.94	Tunisia (TN) 8.57	Syria (SY) 8.40

ReasonLabs

State-Sponsored Hacking

State-sponsored hacking, also known as nation-state cyberattacks, refers to cyberattacks carried out by or with the support of governments against other countries, organizations, or individuals. State-sponsored attacks are a key component of cyberwarfare and are often motivated by a range of goals like espionage, political influence, or financial gain.

- The Democratic People's Republic of Korea (DPRK), also known as North Korea, has a growing track record of executing cyberwarfare and ransomware attacks on organizations and individuals across the world. In 2023 specifically, we saw some of our users in South Korea affected by DPRK-backed hackers' use of Magniber ransomware.
- The National Intelligence's 2023 Annual Threat Assessment stated that "China probably currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks."
- The National Intelligence's 2023 Annual Threat Assessment also states that Iran remains a major cyber threat - Iran's methods of cyber attacks make critical infrastructure in the U.S. especially susceptible to being targeted. Recent Iranian state-sponsored activity has included destructive malware and ransomware operations.
- Russian state-backed cyberattacks are some of the most publicly well-known, especially since the war in Ukraine began in 2022. The notorious gang labeled APT29, also known as Cozy Bear or Blue Bravo, targeted embassies and international organizations in a recent cyber-espionage campaign, researchers found in November, 2023.

The implications of state-sponsored hacking on home users are immense. In particular, the increased risk to critical infrastructure has measurable consequences, like power outages or financial disruptions.

The attacks also erode trust in connected systems and discourage people from using online services. Finally, state-sponsored hacking can escalate tensions between countries and lead to further conflict.

05 Online Piracy

The ongoing issue of online piracy poses a continuous threat to businesses, artists, creators, and **unsuspecting users who unwittingly become targets of cyber attackers exploiting piracy to disseminate malware.** Although online piracy is not a new phenomenon, recent research from the European Union Intellectual Property Office (EUIPO) found that after a multi-year decline, online piracy is on the rise again.

ReasonLabs researchers have covered piracy-related research topics extensively in the past, including The Spider-Miner, Big Brother: the Attack Vector Affecting Metaverse Security, Pirates at the 95th Academy Awards, The Super Mario Bros. Pirate and more, as it is a major threat to home users.

The Spider-Miner

Big Brother: the Attack Vector Affecting Metav...

Pirates At The 95th Academy Awards

The Super Mario Bros. Pirate

The Cashback Extension Killer

ReasonLabs

Torrent Files

Torrents are distributed through a peer-to-peer (P2P) file-sharing service and are so prevalent that it's estimated that **over 50% of all internet traffic worldwide is done through torrents.** Torrent-based file-sharing offers several advantages over traditional file-sharing methods and is not illegal or intrinsically dangerous.

However, **torrent files play a key role in online piracy as it's almost effortless for cyber attackers to use them** to distribute malware. Below we will look at the top threats home users faced in 2023 from malicious torrent files.

Top Malicious Torrent Files

The top torrent files detected as malicious were made up of **different types of Software-as-a-Service products**, such as Microsoft Office, the Abode suite, and others. This list also includes **popular video games** such as Grand Theft Auto V and World of Warcraft. All of them were used to distribute malware such as Trojans, Remote Access Tools (RATs), malicious web extensions, coin miners, keyloggers, and more.

File	Detected file inside torrent
Grand Theft Auto V [fitgirl lolly repack]	c:\users\{user}\downloads\grand theft auto v [fitgirl lolly repack]\setup.exe, 02a227df486fea8edd6a47ab02ed97b35fa4cf8b
Nitro PDF Pro 14.7.0.17 Enterprise + Crack	c:\users\{user}\downloads\nitro pdf pro 14.7.0.17 enterprise + crack\nitro pdf pro 14.7.0.17 enterprise + crack\crack\crack\x86\nitropdf.exe, a8e3165f136d658355f7908a5c16cfdee46d8159
World of Warcraft 3.3.5a (no install)	c:\users\{user}\downloads\world of warcraft 3.3.5a (no install)\wow.exe, 0642498edffed4f5ead36fe3f3a57f6730e80b1f,
Arturia.V.Collection.9.v9.4.0-R2R	Setup V Collection 9 v9.4.0.exe, 6e355772017a2b46d537274e54f661884e61c445
Adobe Master Collection CC 2022 17.03.2022 (x64) (Selective Download) {CracksHash}	\{crackshash}\packages\setup.exe, debc2698b4eeb5cd288a7242210e31394ad9f3cd
Raft v1.09 by Pioneer	c:\users\{user}\downloads\raft v1.08 by pioneer\setup.exe, 400f25cd08a6cc1891e96af820f6b9a263d55482
Autodesk AutoCAD v2024 (x64) (Pre-Cracked)	c:\users\{user}\downloads\autodesk autocad v2024 (x64) (pre-cracked)\setup_64bit\setup_64bit_\setup.exe, 1f0a80b9a446bfdd8f25140d82dbc43fda4ddfc1
Microsoft Office	c:\users\{user}\downloads\microsoft office\setup.exe, 95a11e8091f4124ea5606441bd7b813f54e48798
Adobe Media Encoder 2021 v15.4.1.5 (x64) Multilingual	c:\users\{user}\downloads\Adobe Media Encoder 2021 v15.4.1.5 (x64) Multilingual\ win.exe, 35e2db812198f00ac9ff2c7699472b306939af7b
Eassiy Android Data Recovery 5.1.8 Multilingual	c:\users\{user}\downloads\eassiy android data recovery 5.1.8 multilingual\crack\pemoehjdticafv.exe, 5b844c929969ca079a6251a8c7d0b32d8d1afe31

Common Malware Found in Torrent Files

- The popular torrent files named World of Warcraft 3.3.5a (no install) and Grand Theft Auto V [fitgirl lolly repack], both pretend to deliver their respective games but instead infect the user's machine with the DarkComet RAT. DarkComet enables the attacker to gain complete control of the infected device and capture screenshots, keystrokes, and webcam activity.

- Malicious web extensions were highly circulated in 2023, as evident by the file named Raft v1.09 by Pioneer. It was used to widely distribute malicious web extensions posing as VPNs, but in reality, they attacked and disabled users' existing cashback and security extensions (read more about it in our recent research report, The Cashback Extension Killer).

- Among the top malware found in torrent files is a coin miner which we discovered in the file Adobe Media Encoder 2021 v15.4.1.5 (x64) Multilingual. Malicious coin mining is often referred to as "cryptojacking," and it can result in a significant drain on the affected devices' resources, leading to slower performance and increased energy consumption.

- Another widespread threat was a variant of the banking Trojan Zusy, which was found in the torrent file Microsoft Office. Once a user's device becomes infected, Zusy will inject itself into the web pages of banks, waiting for the user to enter their credentials. Once entered, Zusy will deploy Man-in-the-Browser (MitB) attacks to collect the sensitive information.

06 Emerging Threats

Malicious Web Extensions

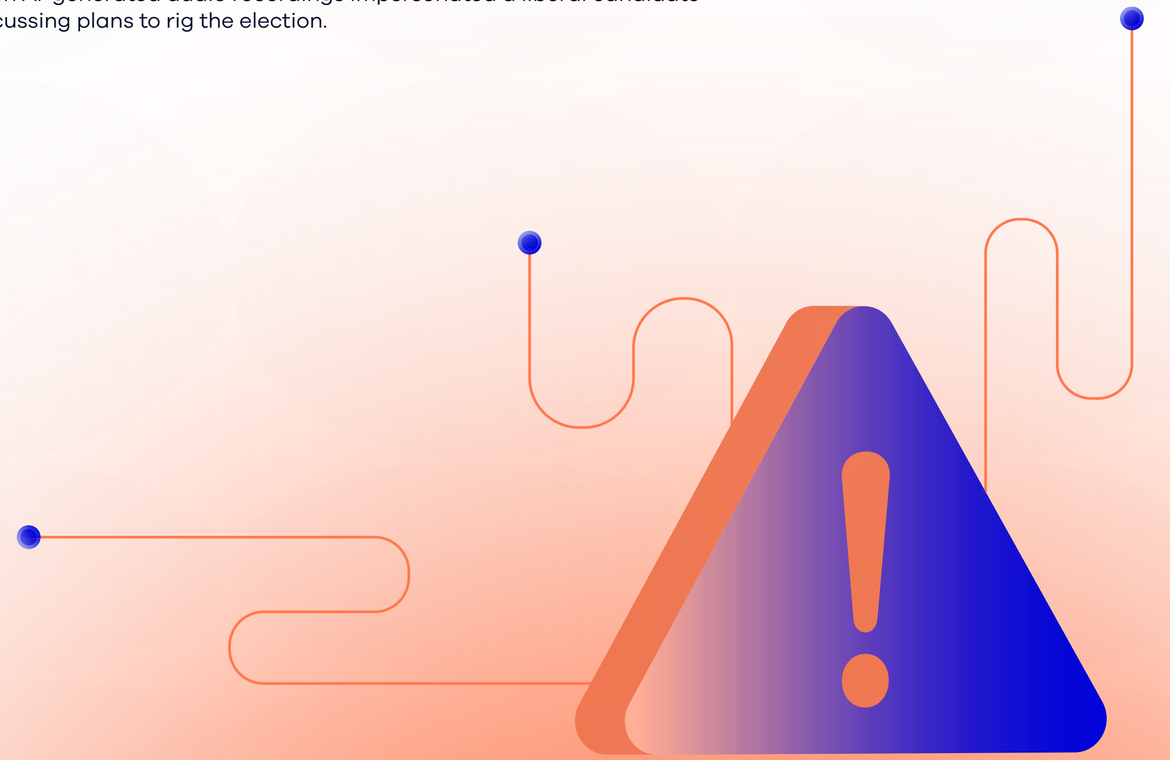
While malicious web extensions are certainly here now, new ways of delivering them are emerging daily. Their overall capabilities are also evolving as browser providers enable developers to gain growing permissions throughout larger portions of users' devices.

Generative AI Attacks

Generative AI (GenAI) has the potential to be misused in various ways to hurt consumers. This includes the development of automated customer support scams or the creation of convincing fake news articles, blog posts, or social media content. GenAI attacks are making phishing increasingly easier and large language models (LLM) have given way to a new attack surface.

Deepfake Scams

Deepfakes have been around for a few years but they are now increasingly being used to target consumers in cyberattacks. Anticipating the 2024 presidential election, there is concern that deceptive deepfake scams may emerge and could contribute to more advanced attempts at identity theft. This exact scenario recently played out in Slovakia's presidential election, when AI-generated audio recordings impersonated a liberal candidate discussing plans to rig the election.



07 How Home Users Can Protect Themselves

Numerous resources are accessible for families, individuals, and remote employees seeking to enhance their cybersecurity within the home environment. These resources encompass not only tangible and digital products but also extend to encompass general education and the promotion of cybersecurity

Endpoint Protection Tools

The most effective defense for home users against contemporary cyber threats rests in the **implementation of endpoint protection**. Hackers frequently target endpoints (such as computers, and mobile devices) as entry points, singling them out due to perceived vulnerabilities. Implementing endpoint protection systems is essential to shield these endpoints from cybersecurity threats that could potentially infiltrate and spread further across networks.

Typically thought of as an enterprise-only resource, **ReasonLabs is bringing endpoint protection into the homes of millions across the globe**. Its full suite of security products, beginning with its next-generation antivirus solution, RAV Endpoint Protection, complement each other to provide the widest array of protection possible. Other beneficial tools include a virtual private network (VPN) such as RAV VPN, and a DNS filter such as Safer Web.

EDR In The Home

Endpoint Detection and Response (EDR) represents an advanced approach employed for the monitoring, detection, and swift response to threats on individual user devices. Instead of merely flagging and overlooking potential issues, **EDR delves deeper into the problem**, aiming to fully comprehend it and deliver a comprehensive solution.

Traditionally, EDR systems have been reserved for use by the world's largest enterprises, government agencies, and educational institutions. **However malware doesn't discriminate, so why should cyber providers?** ReasonLabs is bringing its EDR solution, RAV EDR, into the homes of users worldwide so they too can benefit from this next-generation protection.

Identity Protection

Data breaches are a growing trend - the Identity Theft Resource Center (ITRC) found the total **U.S. data breach findings for just the first nine months of 2023 surpassed the total for all of 2021**, which was an all-time high. Notably, the ITRC showed a 1,620% increase in Zero-day attacks in the first three quarters of 2023 (86) compared to all of 2022 (5).

While companies, educational institutions, healthcare facilities, and government agencies are often targeted by threat actors with data breach campaigns, their users, customers, patients, or citizens are ultimately the most affected. **Even if you don't download malware, you can still be affected by a data breach**. Identity Protection instruments such as ReasonLabs' Online Security Extension and Dark Web Monitoring are great examples of tools you can use to combat the dangers of data breaches.

Parental Control Software

Kids today are growing up in a world where connected devices are as common as playgrounds. Despite this, however, **many young people underestimate existing and next-generation cyber threats**. Parental control software stands as a valuable resource for parents seeking to safeguard their children and the various endpoints scattered across their households.

Parental control software includes mobile solutions such as FamilyKeeper and PC solutions such as the Safer Web DNS filter. **These solutions not only act as a first defense for parents to safeguard their families but also provide learning opportunities.** Parents use the apps to teach their kids right from wrong online, what types of threats exist, and how to handle situations like cyberbullying, ransomware, phishing, and more.

Continuing Education

Promoting cyber education and awareness remains crucial to mitigate the vulnerability of home users. Given that phishing continues to dominate as the primary method for distributing malware, educating individuals about this type of cyber threat is imperative. **Initiating cyber education from an early age** becomes paramount as connected devices become commonplace among younger age groups.

It is essential to cultivate awareness about cyber safety and implement protective measures to shield young users from potential harm. Prioritizing heightened awareness regarding the importance of comprehensive protection for all devices and instructing users on enabling these safeguards is equally critical. The utilization of **Endpoint Security tools such as EDR, VPN, and DNS must extend beyond large corporations**, becoming integral components of individual cybersecurity practices.

08 2024 Predictions

The onset of 2024 marks the beginning of a new year, yet the persistent trends and recurring threats observed throughout 2023 exhibit no indications of deceleration. Here are five forecasts outlining what we anticipate within the cybersecurity sector in the year 2024:

01

Social engineering and phishing attacks will continue to rise in 2024. These attacks have thrived due to a lack of awareness across the security spectrum, as the gap between the sophistication of hackers and the awareness of consumers continues to grow. We can anticipate that this gap will continue to grow if the status quo holds.

02

Parents must double down on protecting their children in 2024. Due to their lack of security knowledge and cyber hygiene, children are often the weakest link in any family's security posture. Hackers are becoming more adept at leveraging torrents, illegal streams, social media, and other common sites used by children of all ages.

03

AI-enabled social engineering techniques will drive most scams. With the emergence of generative AI, it is becoming increasingly easy for cyber criminals to deploy social engineering tactics in multiple formats to deceive consumers. From text to deep-fake audio and visuals, attackers have many tools in their arsenal to plot their deception using both publicly available information and information obtained from online security breaches.

04

Credit card scams are getting smaller but more frequent. Consumer awareness around credit card scams has grown but we are noticing a shifting dynamic. Scammers are beginning to extract a small amount from compromised credit cards in multiple executions to stay under the radar. Judging from our customer data, we expect this credit card fraud trend to rise as criminals grow more sophisticated in their efforts to mask transactions.

05

More deployment of malicious browser extensions. Malware targeting home users is strongly on the rise, with an increased use of malicious browser extensions being a perfect example. The use of malicious browser extensions is a growing trend - not just in frequency, but in sophistication as well. Bad actors are getting better at exploiting both the open architecture of web browsers and the naïveté of users.

09 Conclusion

The significance of cybersecurity protection continues to escalate with time, as observed by ongoing trends and the emergence of new technologies offering criminals additional avenues for illicit activities. In this context, **families and individuals find themselves facing unprecedented cyber risks.** While substantial resources are allocated by large corporations to fortify their network security, individual home users must receive an equivalent level of cybersecurity attention.

Creating awareness about next-generation threats and imparting education on optimal cybersecurity practices is crucial for home users.

ReasonLabs is dedicated to spotlighting the necessity for education and ensuring global protection for every home user against all cyber threats.

Contributors

Andrew Newman
Co-founder and CTO, ReasonLabs

Yaniv Dudu
VP Security, ReasonLabs

Dana Yosifovich
Security Researcher, ReasonLabs

Eric Wolkstein
Marketing Communications Manager, ReasonLabs

Abi Djanogly
Content Manager, ReasonLabs

ReasonLabs is a cybersecurity pioneer equipping tens of millions of families and individuals worldwide with the same level of cyber protection used by Fortune 500 companies. Its AI-powered, next-generation antivirus engine scans billions of files around the world to predict and prevent cyberattacks in real time, 24/7. Its full product suite—including its flagship endpoint security solution, RAV Endpoint Protection—forms a multilayered line of defense that safeguards home users against next-generation threats. Co-founded in 2016 by seasoned cybersecurity expert Andrew Newman—an architect of Microsoft's native cybersecurity program, Microsoft Defender—ReasonLabs is based in New York and Tel Aviv. For more information visit reasonlabs.com.

Contact Us

www.reasonlabs.com
support@reasonlabs.com
press@reasonlabs.com