allot
See. Control. Secure.

H2 2023 Cyber Threat Report

Cybercrime Against Telco Customers

The Methods and the Motives

Lucrative Cyber Threats Targeting Telco Subscribers

The rise in cybercrime is an undeniable reality. However, the threat is underestimated, particularly when it comes to individuals, small businesses, and small offices / home offices (SOHOs). The prevailing notion is that regular internet users have little to offer to cybercriminals because of the misconception that they are low-value targets.

But what exactly constitutes target value?

What motivates cybercriminals to target the everyday internet users within a Telco's customer base?

For providers of cybersecurity solutions for the everyday user, understanding the motivations for cybercriminals in targeting your customer base is crucial. This report aims to provide a fresh perspective on the questions of "Why do Telco customers need protection?" and "Why is cybersecurity essential, even for small internet users?" To begin to answer these questions, we will "follow the money," which is a common approach in deciphering complex issues.

In the subsequent pages, we analyze prevalent cyber threats effectively thwarted by Allot Secure on subscribers from over 20 international telecommunication service providers, shedding light on the underlying business motivations driving cybercriminal activities.

> Cyber attacks on regular individuals are considerably more lucrative than commonly perceived.

Neglecting the need for security is a risk we can no longer afford, particularly given the escalating dependence on the digital world, which introduces an increasing number of vulnerabilities. Cybercriminals continue to refine their deceptive tactics, operating silently behind the scenes, and the potential gains are too substantial for this trend to subside anytime soon. We take pride in reaffirming that Allot Secure has proven to be a reliable ally in the ongoing battle to keep users secure online.

Table of Contents

Each of the following sections focuses on different types of cyber threats with a particular business case for cyber criminals attached to it. Together with an essential explanation, we offer examples of the most common cyber threats targeting Telco subscribers that Allot Secure blocked during 2023.

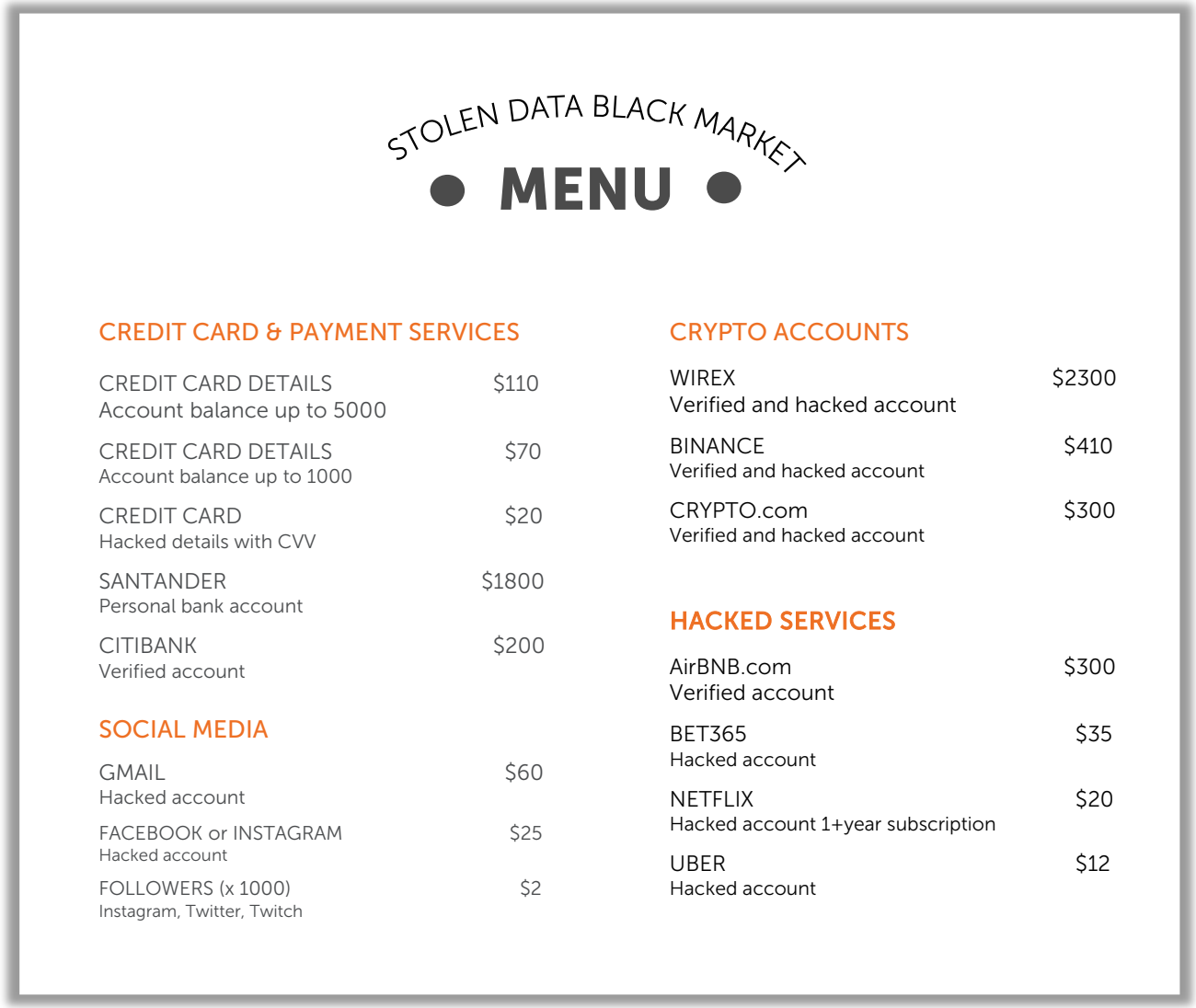
1

Follow the money

Private User Data in the Black Market

The Market Demand for Cyber Crime

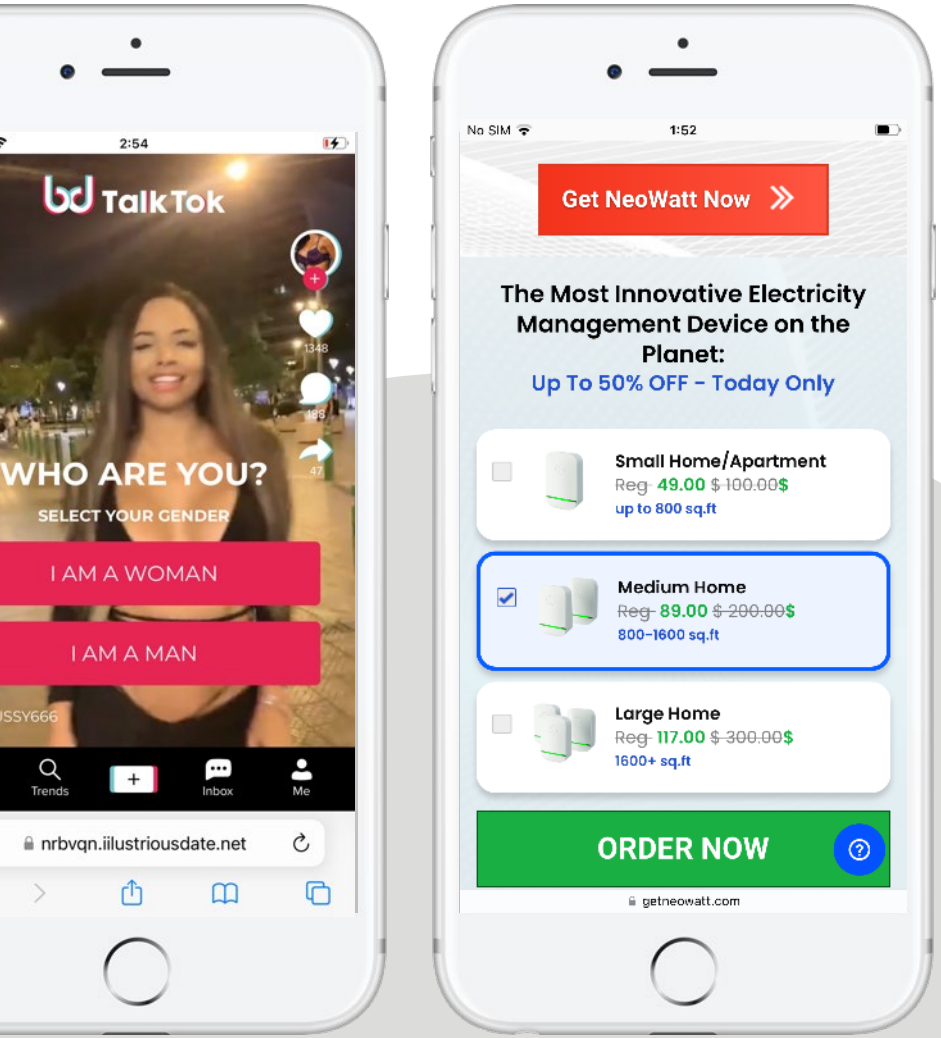
More and more individuals and small businesses handle personal, operational, and financial matters online. Everyday users may have varied levels of awareness and unknowingly fall victim to cybercriminals with access to their valuable information for identity theft, fraud, or financial exploitation. Additionally, regular internet users are an easy target due to the frequent lack of robust cybersecurity measures compared to more sophisticated institutions.
Subscribers' credentials are becoming as valuable as any other commodity. One has a perfect picture of it simply by looking at the rates regular user credentials fetch in the black market and the alarming ease of trading them.



Source: privacyaffairs.com/dark-web-price-index-2023

Beware When Shopping or Dating

Phishing, the most well-known and widespread technique behind data theft, shows no signs of fading away. Instead, it continues to demonstrate endless creativity in luring online users.
Out of the dozens of thousands of phishing sites blocked by Allot Secure in 2023, we'll focus here on two types of success stories that were particularly popular during the year's second half. Both utilize phishing sites as a nefarious means to steal sensitive information, including credit card credentials and personal profiles. These deceptive websites mimic legitimate platforms, unknowingly tricking users into divulging confidential information.



The Temptation of Gadget's Irresistible Deals

The first step in a cybercriminal's playbook is to create an irresistible offer. Promotions like "70% off on Smart Home Devices" are designed to catch the eye and trigger curiosity. Most people are naturally drawn to saving money, especially when upgrading their home technology. For a good sample of this, we have ProjektMini.com*, which offers the highest cinema resolution at home for an incredible discount in a time-limited opportunity.

Another one is NeoWatt -getneowatt.com*- which offers revolutionary home gadgets for clean and efficient energy that can reduce the electricity bill by up to 90%! Sounds good. Well, only in the last two months of 2023 has Allot stopped thousands of subscribers from falling for these phishing scams.

Date to Lose

Online dating and adult-oriented platforms, another prime target for cybercriminals, are vulnerable to attacks due to the wealth of personal information users willingly share. Social engineering plays a crucial role in these attacks, as hackers exploit human psychology to manipulate users into revealing sensitive details.

Once more, Allot played a significant role in keeping subscriber credit card and profile information secure and protected from bad actors.

Red Alert for Online Credentials

A “stealer” on the rise

RedLine is a Trojan Stealer with a significant presence in the market during H2 2023.

The virus specializes in stealing from personal and enterprise devices, causing financial losses and data leaks. It goes after sensitive information like passwords, credit card details, and usernames found in browsers, messaging systems, and file transfer clients. In addition, it collects data such as location, autofill details, cookies, software settings, and hardware configurations, including keyboard layout and User Account Control (UAC) settings. Notably, RedLine can even pilfer cryptocurrency and may be utilized to distribute further attacks like ransomware, Remote Access Trojans (RATs), and crypto-miners.

Easily accessible on underground forums and command-and-control (C&C) panels, RedLine provides a range of options, including malware-as-a-service versions or subscriptions, with prices between $100 and $200. To propagate the Trojan, attackers employ social engineering tactics in email campaigns, including business email compromise, spam, fake updates, and Google ads, ultimately leading to the dissemination of malicious attachments or links.

Credential Stealer Trojan

What is it?

It’s a virus designed to secretly gather login credentials and sensitive information from a user's device. It operates in the background, often without the user's knowledge.

How does it act?

Through deceitful methods, the Trojan gains access to the device, monitors user activity, captures keystrokes, screenshots, and scans files to extract valuable login credentials, and then sends the stolen data to the cybercriminal’s C&C server.

How does it impact internet users?

Stealer trojans can lead to financial loss, unauthorized transactions, and identity theft.

Noon Trojan targeted European bank customers

Meet Noon, a version of Trojan spyware gaining notoriety in the digital world. As the most sophisticated in its category, this Trojan slips through anti-virus defenses and installs itself without manual intervention.

The Noon Trojan operates under the radar, utilizing spam emails as its primary distribution vehicle. These deceptive emails disguise themselves as product quote inquiries, shipping details, fake invoices, or product orders. Once an unwitting recipient opens the attachment, Noon springs into action, silently embedding itself in the victim's system.

This Trojan is not the average cyber intruder; it goes beyond merely residing on the device.

It goes on a mission to gather as much information as possible. From stealthily recording keystrokes to snatching stored email credentials across various mail clients, this Trojan aims to leave no digital stone unturned. Noon has a voracious appetite for browser-stored data, extracting usernames, passwords, and hostnames.

Stolen data becomes a payload, which is sent back to the cyber-criminal.

Trojan Spyware

What is it?

Trojan spyware is a type of malicious software that disguises itself as a legitimate program but includes hidden malicious functionalities

How does it act?

It tricks users into installing it, often through deceptive methods. Once installed, it can secretly collect sensitive information, monitor user activities, and transmit the data to remote servers without the user's knowledge.

How does it impact internet users?

The impact on internet users includes potential identity theft, financial loss, privacy breaches, and compromised system security.

Coper / Octo Banking Trojans

Full access to everything on your Android device

When it comes to Android Trojans, we find more and more cases where one specific click makes the victim completely vulnerable; that is the enablement of accessibility services. The concept covers a set of features available in most Google Play applications designed to help users with disabilities to interact with mobile apps. The features range from audible feedback and a screen reader for visually impaired or blind users, to a switch access service that can press "yes" or "no" for users with mobility limitations. All sounds great, right? It is, until cyber criminals use them to steal user data.

The problem usually starts with the infiltration of the trojan while downloading some appealing app that prompts the option to "trust" the app in the installation process.

An excellent example of the practice was a PDF viewer with 10,000+ downloads in the Play Store by Q1 2023.

After being installed, the app downloads the Coper malware that, in a later stage, interacts with the user by disguising itself as a "Play Market" app. As it's not uncommon for this app to bring up the Accessibility Service setting option, many users eventually click OK, and that's it -- the bad guys are in control.

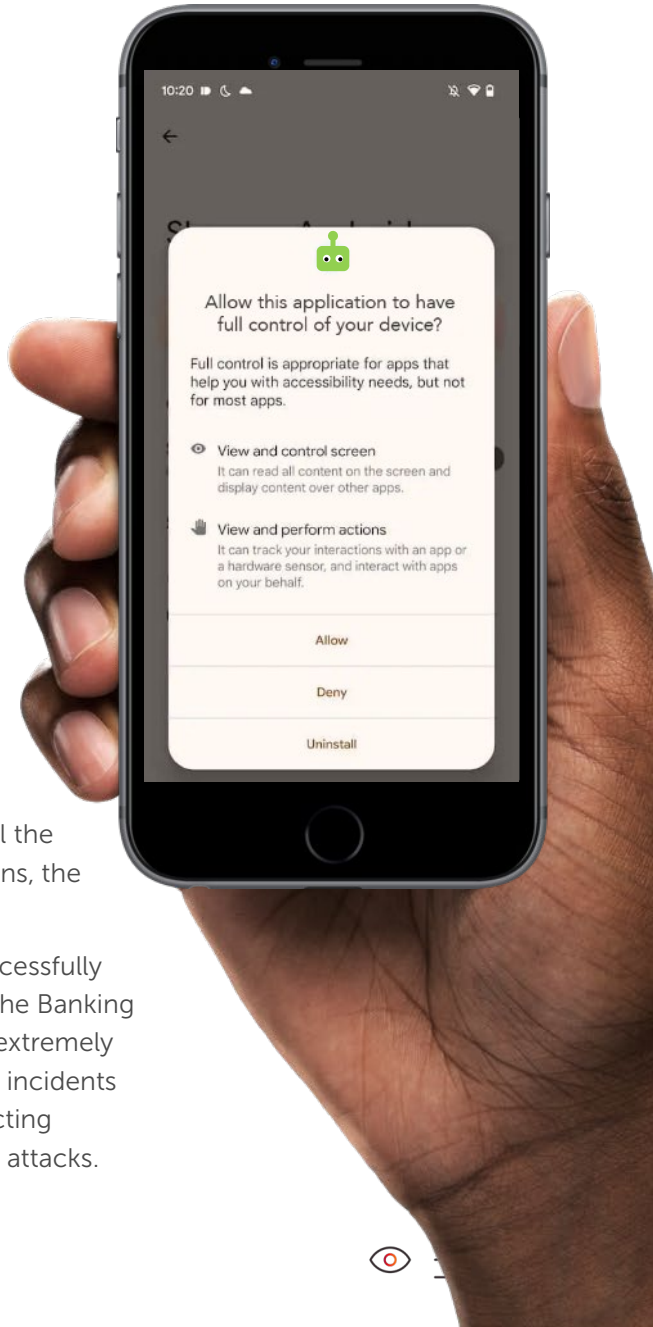
The Trojan can read the device's screen and may use it to target banking apps, crypto wallets, or any other sensitive action on the phone.

It will wait until it detects that the targeted apps are being displayed on screen to impersonate the application by injecting a fake login form through a screen overlay.

Once it acquires credentials and other confidential data, it might use additional accessibility capacities to simulate clicking on the buttons to enable it to perform actual operations, such as money transfers.

The latest versions of Android (13+) made it harder to enable Accessibility Service for an app while downloading it. However, as not all the devices are updated or allow the latest versions, the risk of being a target is still high.

Luckily for Telco customers, Allot Secure successfully stopped the internet connections related to the Banking Trojan Coper and Octo (the two Trojans are extremely similar). During 2023, hundreds of millions of incidents related to these Trojans were blocked, protecting thousands of customers from these high-risk attacks.



2

Follow the money

Crypto-mining

Cryptojacking

The Digital Heist for Easy Crypto Cash!

Cryptojacking is a crafty cybercrime involving the takeover of your devices (e.g., computers, smartphones, tablets, or even servers) without your knowledge. The goal? To mine cryptocurrency, all in the pursuit of profit.

But first, let's do a quick Crypto 101

Digital currency, or cryptocurrency, is comprised of tokens or "coins." While Bitcoin is the most well-known, roughly 3000 other virtual currencies exist. These currencies operate on a distributed database known as the 'blockchain,' which is constantly updated with transaction information. The magic happens when recent transactions are bundled into a 'block' through a complex mathematical process. Cryptocurrencies need computing power to create new blocks, which is where the miners come in. Miners are individuals who provide the necessary computing power and, in return are rewarded with cryptocurrency. Many cryptocurrencies employ teams of miners running dedicated computer rigs to tackle the mathematical calculations required. The catch? This activity consumes electricity and, in the case of Bitcoin, a shocking 127TWh per year - 2.5 times more than New Your City's demand for the same period.

And this is when cryptojackers enter the scene

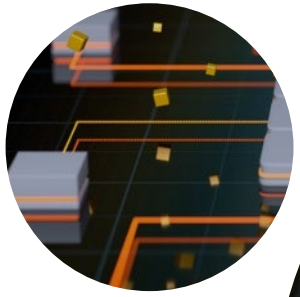
Cryptojackers are essentially resource thieves, hijacking your devices to mine cryptocurrencies without bothering to invest in expensive equipment or foot the electricity bill. It's their way of savoring crypto profits without breaking the bank.

But before you start picturing a quick cash grab from your home computer or mobile phone, think again. Mining from personal devices is often not profitable. Sure, you might rake in $10 a month with a regular computer, up to $300 with a gaming rig (featuring the proper GPU), or $10 to $15 with a decent mobile phone. But here's the kicker—the energy costs to support these operations can quickly overshadow any potential earnings.

However, for cryptojackers, the equation is different. They persist in their activities, regardless of whether the device resources are not entirely dedicated to crypto or the potential data session interruptions, because, at the end of the day, their equation always points to profit.

Allot Secure protection

Most of the protection activity in relation to crypto mining in 2023 was through the blocking of C&C, with CoinMiner one of the predominant Trojans. Web browsing was still in the picture with more than a 50% increment compared to the previous year.



3

Follow the money

Digital Footprint as a Commodity

Spyware Web Tracking

Profits in the shadow of a growing market

In 2023, the eCommerce market was estimated to be worth $3 trillion, with an expected annual growth rate of 10% over the next five years, serving 2.5 billion users. As businesses increasingly rely on digital channels to engage with customers, and with more advanced analytics tools available, user information has become the most valuable asset, raising new cybersecurity issues. Even though we often hear about major digital players facing data breaches, the reality is that spyware tracking and fingerprint collection happen every day without making headlines.

Let's talk about Tracking Services

Tracking services are like the silent heroes of the internet, making our online experience smoother. For instance, e-commerce platforms use tracking tools to remember the items in your shopping cart, making your online shopping spree a breeze. Similarly, analytics services help website owners understand user behavior, giving them the insight they need to enhance content and design.

Tracking services are created equal; some cross the line into spyware territory, collecting data about your online activities without your say-so.

Default Cookies and Privacy Concerns

Now, let's chat about default cookies. These little bits of data are stored on your device Not all the web-trackers are Spyware. Today, most websites include third-party cookies as part of the default options, allowing your digital footprint to be used extensively for advertising and retargeting across the web and social media. That might sound like a privacy concern, but it's legal. The issue can be minimized with the right browsing settings or by using a specific browsing extension for that purpose.

Why Privacy Matters to Us

What Allot Secure stops for protected subscribers is tracking with a malicious intent. Spyware web trackers will use private information without asking for a click on "accept all" cookies. Data collected by Spyware trackers is used for targeted advertising and profiling, which are sold to third parties without your knowledge.

> The impact of this spyware goes beyond mere data collection, affecting users on personal, financial, and emotional levels.

Having the most accurate and fresh user data allows cybercriminals to target their victims individually. A common and deceiving use case is getting a phishing email impersonating an online store that was used just minutes ago, talking about some issue or asking for confirmation of a purchase. Stolen information can lead to identity theft and financial loss.

4

Follow the money

Pay Per View Malvertising

Browser Hijackers and Adware

How Cyber Crooks Turn Annoyance into Profit

In the world of cyber threats, two troublemakers—Adware and Browser Hijackers—have a niche for themselves, serving as money-making tools for cyber criminals.

Let's dive into the world of their profit-driven operations and uncover the risks they pose to internet users.

Adware

The sneakiest of the duo, it tiptoes into your devices with one mission in mind: to flood your screen with irritating ads. It often disguises itself within seemingly harmless downloads or bundles itself with legitimate applications. It collects user data for ad targeting and, even worse, it can expose links associated with major cyber attacks.

Adware Cashflow: Behind the scenes, adware operates on the principle of pay-per-click (PPC) and pay-per-view (PPV). Each time you click on or even glance at those intrusive ads, cyber criminals cash in. Advertisers unknowingly foot the bill for these interactions, creating a revenue stream for the bad actors.

Browser Hijackers

Now, onto the more assertive troublemaker. Browser hijackers tweak your browser settings without your approval, redirecting you to unwanted sites and tampering with your search results. With hijackers at the wheel, you lose control over your browsing freedom. They decide where you go and what you see in your search results. This makes your navigation a highly risky open door for cybercrime. Browser hijackers may guide you straight to clicks leading to virus downloads or phishing sites, opening the door to identity theft as you unknowingly share your personal info on shady pages.

Profit Mechanism: it is mainly rooted in affiliate marketing. Cyber criminals cozy up to third-party websites, earning a commission every time you're redirected to these sites.

Additionally, the hijacked browser settings might lead you to click on sponsored links, further padding their pockets.

5

Follow the money

Ransomware

Ransomware for Individuals and SMBs

Small but Significant

While attacks on large enterprises and government organizations have been making headlines in 2023, many researchers warn that smaller-scale attacks on individuals and small businesses are also causing significant harm.

Many ransomware gangs intentionally steer clear of larger targets, choosing victims who may lack the technical knowledge to navigate such incidents. These attacks often involve ransomware-as-a-service strains deployed in spray-and-pray assaults against smaller targets facilitated by relatively unsophisticated actors. These incidents frequently zero in on individual users or small businesses that lack the resources for robust security measures.

Perpetrators often disguise these attacks as popular software downloads or deliver them through mass phishing campaigns. When targeting large organizations, the motivation for a ransomware attack may vary from the disruption of operations caused by downtime and reputation to pure financial gain. However, attacks on individuals and small businesses are less targeted and only aim at paybacks.

According to Statista, the average amount of ransomware payments in H2 2023 was over $740,000. As expected, those numbers do not correspond to attacks on regular individuals. Based on our investigation, ransomware attacks targeting small businesses and regular people typically demand payments below $1,700.

In the picture, there's an example of the actual ransomware messages from the Adhubllka-OBZ family used in 2023. Fortunately for subscribers protected by Allot Secure, this type of experience was blocked.

6

Follow the money

Plain and Simple Online Scams

allot

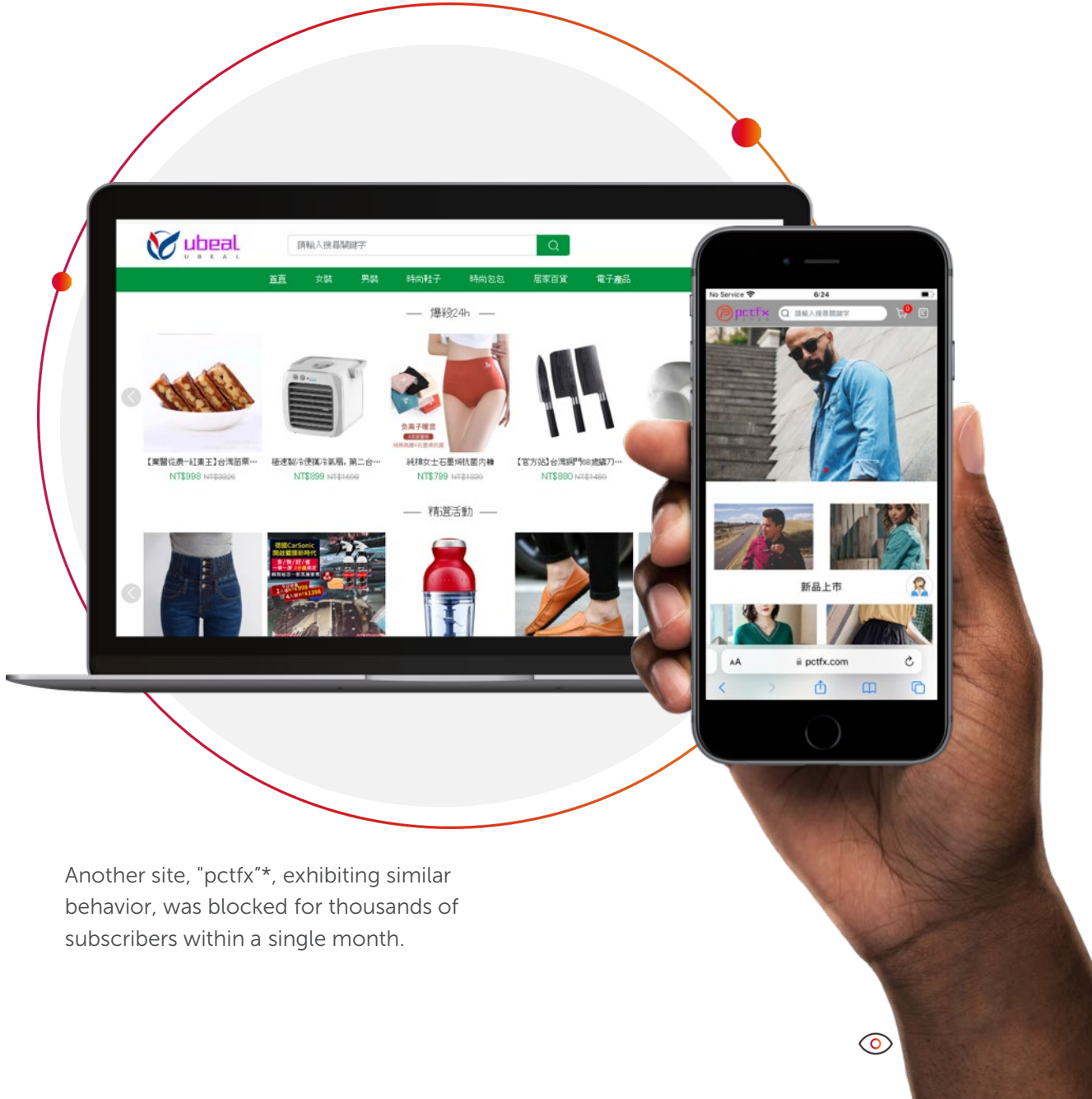
Plain and Simple Online Scams

Sometimes, there's no need for sophisticated command and control methodologies or a dark web black market. Our solution often prevents connectivity to sites built to perform plain and straightforward online scams.

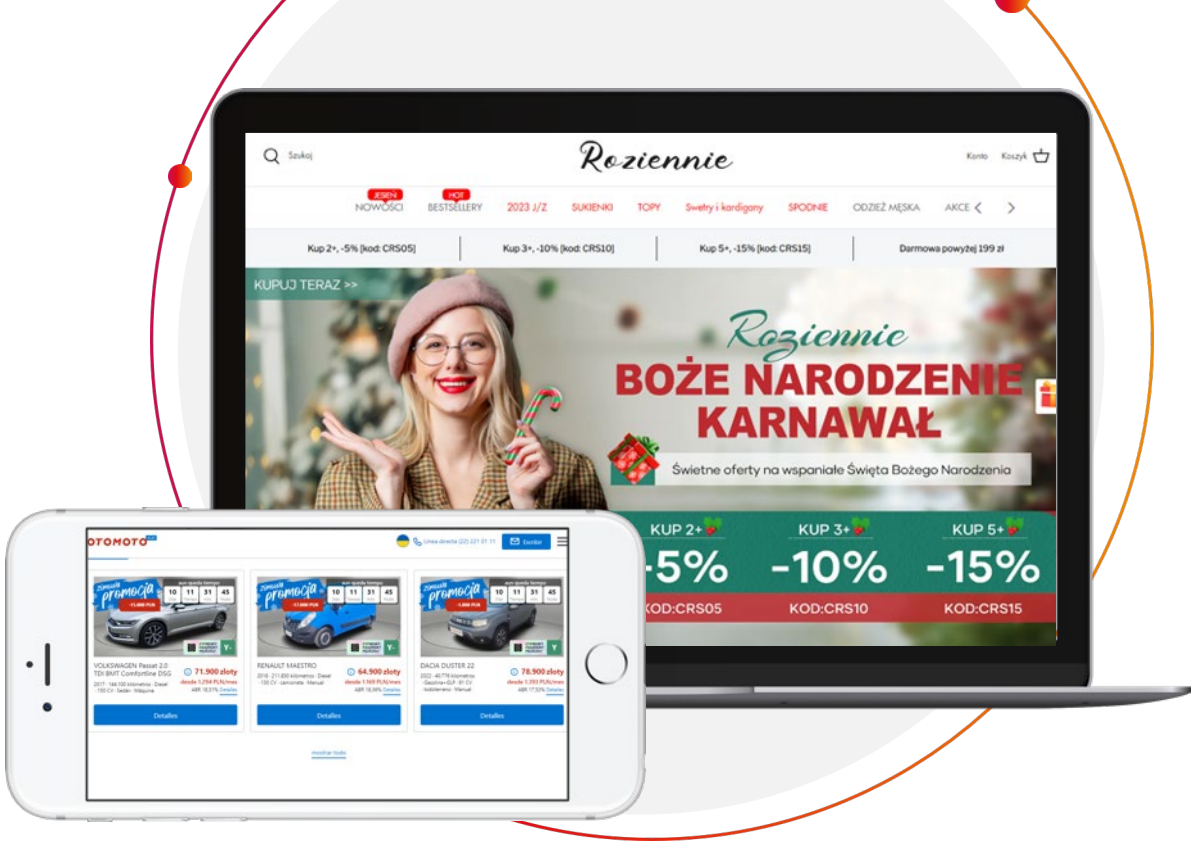
The process is almost artless: you may find an appealing item online, pay for it, and that's it! The end of the story is that after accepting the payment, you will not get the delivery of your purchased goods or enjoy the service you paid for.

Our 2023 research on the most common use cases shows examples of this modality exposed as part of Phishing attempts (where the bad guys will not steal your credit card details but will keep payments), or Malicious Download activity (where the crime is not infecting your device, but in keeping your payment for a fake service or app).

Several phishing domains linked to scams targeting online fast fashion retailers have caught our attention. One notable example is "Ubeal"*, a well-known portal that, over several months, fell victim to abuse, hosting phishing attempts connected to exceptionally aggressive offers. Blocking spared thousands of subscribers from falling victim to this online scam during the second half of the year alone. The situation was rectified in November 2023, ensuring the portal's security as of the writing of this report.



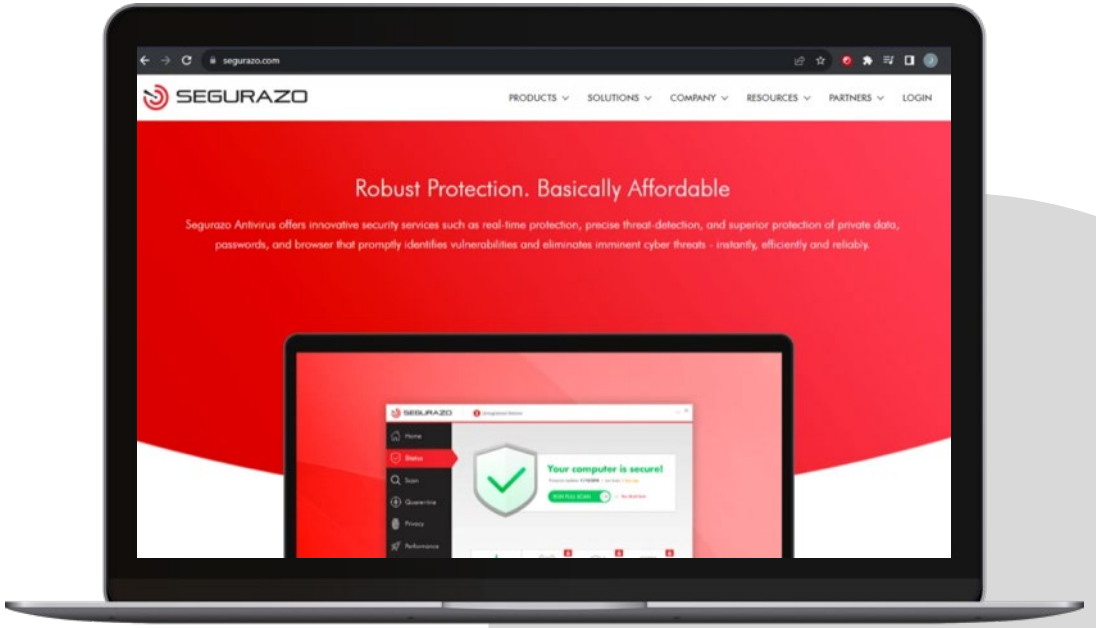
Another site, "pctfx"*, exhibiting similar behavior, was blocked for thousands of subscribers within a single month.



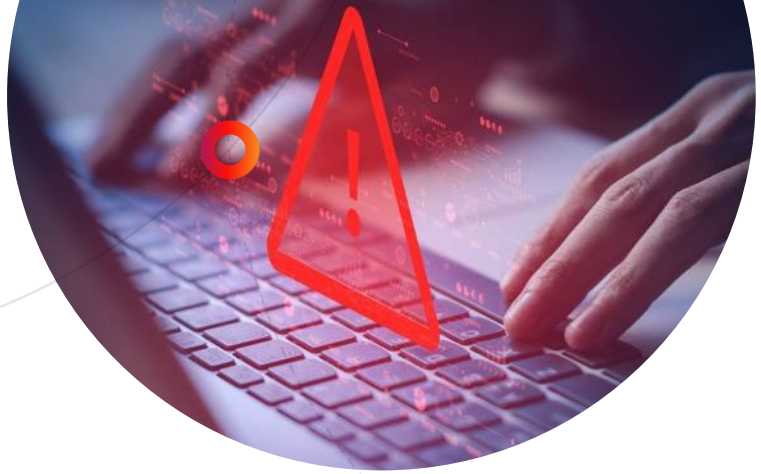
Meanwhile, the page "Roziennie"* utilizes Facebook ads to promote fashion goods, purportedly shipped from China, at remarkably low prices. Once identified as malicious, Allot promptly blocked the attempts to access those sites, keeping subscribers safe. Simultaneously, several consumer forums are rife with reviews detailing unfulfilled purchases from these sites.

Another example of a scam that came to light during 2023 was related to second-hand reselling portals. That was the case for "otomotoklik"*, a website focused on selling cars, which was found to be linked to phishing activity. This website has a dubious reputation and has been blocked thousands of times every month.

Another excellent example of this type of simple scam practice is at "segurazo"*. It's interesting to note that connections to this site were stopped more than 3M times last year. The site posed as an anti-virus service provider offering a free-of-charge basic version. After being installed, it runs the first scan on the device and notifies users about several threats detected that need to be immediately removed. But, to do so, users need to upgrade to a premium version. Everything might sound innocent; however, the scam consists of users installing fake anti-virus software; the whole app interaction is just a charade to sell premium licenses with no value.



Preventing Malware Access



Up to this point, our focus has been on addressing cyber threats with a direct economic motive targeting our consumers. However, it's crucial to recognize that subscribers face a broader range of potential threats.

Every day, Allot Secure excels at identifying and thwarting connections that pose risks related to various types of threats. Many of these threats don't necessarily seek to exploit the victims' privacy, behavior, or resources directly; instead, they serve as intermediary steps toward achieving those objectives.

One prevalent category of threats relates to malware or malicious downloads, which are often linked to online activities on suspicious domains, particularly those used for content streaming.

The plugins or video codecs required for streaming can inadvertently facilitate the download of numerous Trojans. In those cases, our solution does not stop threat activity with direct consumer impact - Spyware, Adware, Banking Trojan, or Miner Trojan - but it plays a pivotal role in preventing the vulnerability that would enable the virus to be installed.

Furthermore, Allot Secure has successfully intercepted the activities of various Trojans that were not explicitly discussed in earlier sections. These include droppers, RATs, downloaders, proxies, and backdoors, among others. Despite their diverse functionalities, these threats share a common intermediate goal: enabling unauthorized access and control (in the case of backdoors and RATs) or delivering and installing additional threats (downloaders and droppers). Once again, by thwarting the activities of these potential risks, we proactively hinder their ability to target and compromise the resources of our valued subscribers in the next step of the attack.

Summary

Insights for Enhanced Online Protection

By examining the always-evolving cyber landscape, we were able to shed some light on the real motivations behind cyber attacks on everyday users and small businesses.

Given the range of cyberthreats, from the lucrative black market for private user data, to the subtle yet impactful world of digital footprint commodification, there is a critical need to adapt cyber security measures to protect telco subscribers of all sizes.

The diverse tactics employed by cybercriminals to profit from telco customers:

- Phishing Scams
- Sophisticated credential stealers
- Cryptojacking as a digital heist
- Browser hijackers and adware
- Spyware Web Trackers
- Low-scale ransomware

Everyday users and SMBs are as much in need of online protection as any large enterprise.

Regardless of size, anyone can be a profitable target in the digital era. The diverse sources of dark profits from cyber attacks inspire a call to action for more awareness and additional resolve to bring online security to every telco subscriber.

At Allot, we will continue to be a strong ally in this commitment. We hope 2024 will bring more success stories about keeping telco subscriber customers safe and secure

The network-based solution offered by Allot Secure showed outstanding results when identifying and blocking the most diverse cyber-threat activities. We trust the real-life examples shared in the previous pages showed how subscribers were exposed to the most common attacks, as well as the positive impact of those enjoying the protection service compared to others vulnerable to the same cyberattacks. For more information about how Allot Secure can protect communication service provider's consumer and SMB customers, visit Allot Security Solutions

*Part of the malicious activity exposed in these examples correspond to the site's subdomains with bad reputations. Reputation scores might change over time. The behavior and figures shown are related to 2023 activity, while the specific examples were malicious.