ThreatDown™
Powered by Malwarebytes

2025
State of Malware

The year of autonomous AI and “dark horse” ransomware

Contents

1. Lessons from 2024

As a new year starts to unfold it's natural to wonder what the next 12 months will bring, and to look backwards for clues. For years, the past has been a reliable guide to the immediate future of cybersecurity because cybercrime is a mature criminal enterprise with well-established tools, techniques, and practices (TTPs).

However, the imminent emergence of autonomous, agentic artificial intelligence (AI) is a cybersecurity wild card promising transformative risks and breakthroughs in 2025. For now, ransomware remains cybercriminals' most effective way to monetize illegal access to Windows networks, and it will almost certainly be the primary concern for defenders in 2025.

The number of active ransomware groups and the total value of ransoms paid all increased in 2024, while attacks became faster, stealthier, and more numerous.

Criminals also made extensive use of remote desktop tools and old software vulnerabilities to gain entry to their targets' networks, showing that while technology marches on, many defenders continue to struggle with the basics.

Elsewhere, attacks targeting payment processing systems and medical service providers highlighted the vulnerability of supply chains and critical infrastructure once again.

On macOS, the threat landscape was disrupted by a notable shift towards sophisticated infostealer malware like Poseidon and Atomic Stealer, reflecting the platform's growing attractiveness to cybercriminals.

2024 also saw generative AI find its niche as an ever-present coding, writing, and research assistant for both attackers and defenders, but its impact on the threat landscape was muted. It seems that while generative AIs made activities like researching vulnerabilities and writing malware easier for threat actors, they did not deliver any truly novel or disruptive capabilities.

However, what AIs can do is likely to advance significantly in 2025 as companies like OpenAI deliver autonomous AI agents—AIs that can use tools and navigate the internet with little or no assistance. In other words, in 2025, AI won't just answer questions, it will be able to think and act, transforming it from an assistant that responds to prompts, into a peer, or even an expert, that can interact with the world and carry out complex tasks unaided.

In a world where cybersecurity suffers a perpetual skills gap and labor-intensive ransomware struggles to scale, the arrival of autonomous AIs could be a game-changer.

About this report

To create this report, we asked our experts what resource constrained IT teams should pay attention to in the year ahead, across Windows, Mac, and Android. Rather than create an exhaustive list of all the threats you could face, they chose the cybercrime tactics you should focus on. If you are equipped to handle these then you are well placed to deal with anything the cybercrime ecosystem can throw at you in 2025.

2. Agentic AI

AI's impact on small and medium-sized business cybersecurity has been limited so far, but that could change in 2025. The arrival of "agentic" AI could finally deliver the profound cybersecurity disruption that many expected after ChatGPT's release in 2022.

> "...One area where AI does provide a novel capability is deepfakes... which can be used for fraud."

The current state of AI threats

Cybercrime has changed little despite the rise of generative AI tools like ChatGPT, indicating that while much has been written on the topic, these tools haven't impacted the field significantly. This isn't because they cannot be used for cybercrime—jailbreaking methods that bypass AI safeguards against criminal activity are well-documented, and tools like GPT-4 can be abused to create basic ransomware even with its safeguards intact. Additionally, specialized and unfiltered AIs like WhiteRabbitNeo and FraudGPT can be used for illicit activities directly.

The limited impact of AI on malware stems from its current capabilities. Although there are notable exceptions, generative AIs tend to provide efficiency rather than brand new capabilities. Cybercrime is a very mature field that relies on a set of well-established tools, such as phishing, information stealers, and ransomware that are already feature complete.

In its October report, Influence and cyber operations: an update, OpenAI detailed attempts by three threat actors—STORM-0817, SweetSpecter, and CyberAv3ngers—to use ChatGPT to discover vulnerabilities, research targets, write and debug malware, and setup command and control infrastructure. In each case, OpenAI concluded that its models offered the threat actors "limited, incremental capabilities for malicious cybersecurity tasks beyond what is already achievable with publicly available, non-AI powered tools."

One area where AI does provide a novel capability is deepfakes—clones of peoples' voices and likenesses—which can be used for fraud. Even here though, the technology has been used to make incrementally more convincing versions of social engineering attacks like CEO fraud, rather than creating an entirely new threat.

For now, it seems that cybercriminals use ChatGPT the same way everyone else does—as an assistant that makes tasks like research, writing documents, and writing code easier.

Agents and the future of AI threats

AI is likely to advance significantly in 2025, as companies like OpenAI, Anthropic and Google DeepMind compete to deliver the first artificial general intelligence (AGI)—an AI that is equal to or better than human experts across a wide range of tasks.

AGI is expected within the next few years, but whether it arrives in two years or ten, it's widely agreed that the next step towards AGI is "agentic" AI, which is likely to arrive in 2025. AI agents are AIs that can plan, act, reason, and use tools. The step change from generative AIs to agentic AIs could have significant implications for cybersecurity.

Estimates for AGI arrival based on public statements

Anthropic CEO, Dario Amodei	1-2 years
Microsoft AI CEO, Mustafa Suleyman	3-5 years
OpenAI CEO, Sam Altman	Within 5 years
Google DeepMind CEO, Demis Hassabis	10 years

The generative AI technology we're used to, like ChatGPT and Gemini, is good at making sense of data: It can search it, summarize it, and rearrange it into new documents, code, and images. While this helps people do their work more efficiently, it has not addressed a critical cybersecurity bottleneck facing either attackers or defenders.

If agentic AIs arrive in 2025, they won't just answer questions, they will be able to think and act, transforming AI from an assistant that responds to prompts, into a peer, or even an expert that can plan out tasks, interact with the world, and solve the problems it encounters.

> "If agentic AIs arrive in 2025, they won't just answer questions, they will be able to think and act, transforming AI from an assistant that responds to prompts, into a peer, or even an expert that can plan out tasks, interact with the world, and solve the problems it encounters."

Agentic defenders

Agentic AI could be used to narrow the growing cybersecurity skills gap. As AI becomes more capable, security teams will be able to delegate an ever-increasing range of tasks to autonomous agents that get things done with minimal instructions.

It is not far-fetched to imagine agents being tasked with looking out for supply-chain vulnerabilities, keeping a running inventory of internet-facing systems and ensuring they're patched, or monitoring a network overnight and responding to suspicious EDR alerts.

Agentic attackers

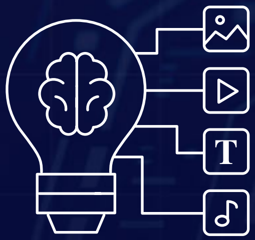
Agentic AI could be used to scale up the number and speed of attacks. Big game ransomware requires a lot of human labor. With the expected near-term advances in AI, we could soon live in a world where well-funded ransomware gangs use AI agents to attack multiple targets at the same time.

Malicious AI agents might also be tasked with searching out and compromising vulnerable targets, running and fine-tuning malvertising campaigns or determining the best method for breaching victims.

How ThreatDown uses AI

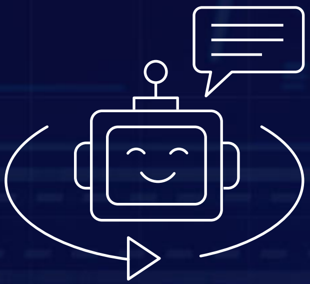
ThreatDown uses multilayered detection technologies, including machine learning, to identify malware and zero-day attacks. The malware detections are powered by an automated system with 100% autonomous learning, meaning that it does not require human interaction to correctly identify these attacks. This system is one of many techniques our engine uses for mass detection of malware, ransomware, adware, and fileless attacks.

What's the AI difference?



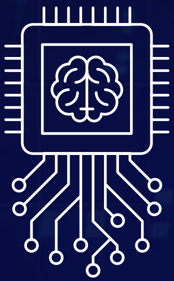
Generative AI

Creates new content like text, images, and music based on learned patterns.



Agentic AI

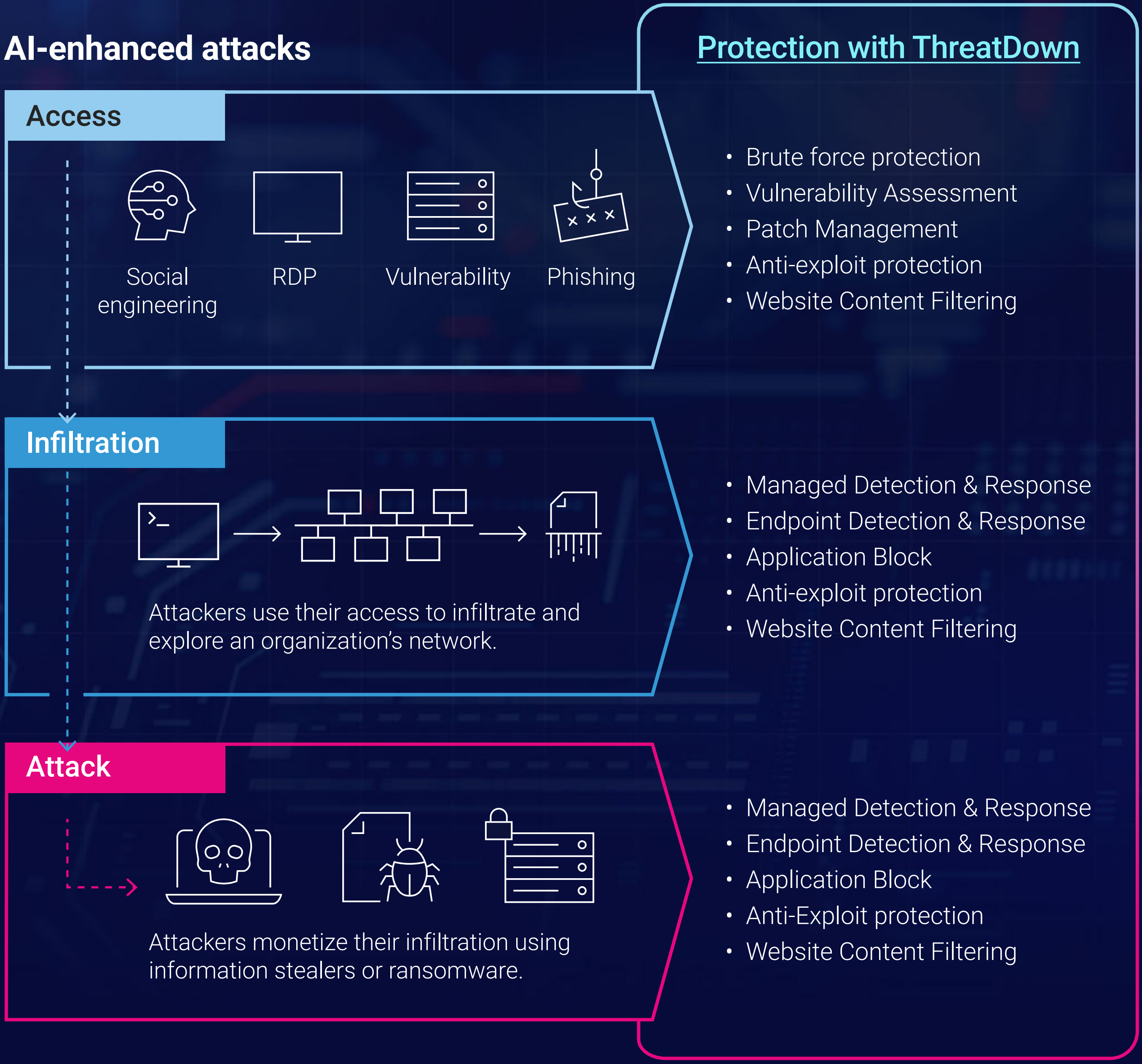
Navigates computer systems and networks, carrying out complex tasks.



Artificial General Intelligence (AGI)

Matches or exceeds human abilities in a wide range of tasks.

To combat threat actors using AI to make attacks more potent, organizations need to operate their security as efficiently as possible: Minimizing their attack surface, actively monitoring EDR consoles and acting on alerts immediately, and using automation to ensure vulnerabilities are patched or mitigated in the shortest possible time.



AI-enhanced attacks

Protection with ThreatDown

Access

Social engineering

RDP

Vulnerability

Phishing

- Brute force protection
- Vulnerability Assessment
- Patch Management
- Anti-exploit protection
- Website Content Filtering

Infiltration

Attackers use their access to infiltrate and explore an organization's network.

- Managed Detection & Response
- Endpoint Detection & Response
- Application Block
- Anti-exploit protection
- Website Content Filtering

Attack

Attackers monetize their infiltration using information stealers or ransomware.

- Managed Detection & Response
- Endpoint Detection & Response
- Application Block
- Anti-Exploit protection
- Website Content Filtering

3. The ransomware landscape

“Big game” ransomware attacks were the most significant threat to organizations of all sizes in 2024 and will remain so in 2025.

Ransomware is the most lucrative and successful method devised so far for monetizing illegal access to computers. “Big game” ransomware attacks target entire organizations rather than individual computers and extort vast ransoms using encryption and the threat of damaging data leaks.

+13%

Known ransomware attacks increased 13% in 2024

2024 was the worst year ever for big game ransomware. The number of known attacks increased 13% year-over-year, the largest ever ransomware payment was made when an unknown victim paid $75 million into a crypto-wallet owned by the Dark Angels group, and November saw the highest number of known attacks ThreatDown analysts have ever recorded.

$75 million

2024 saw the largest ransomware payment ever made

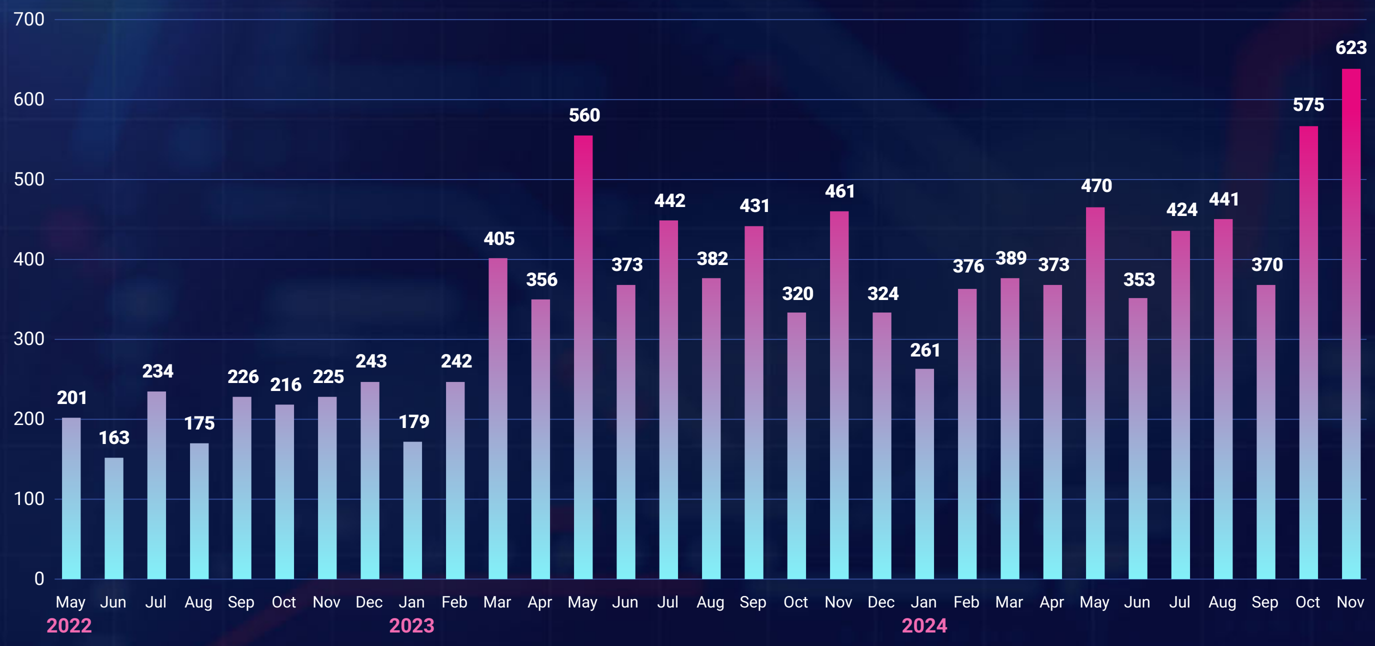
In February, a ransomware attack on Change Healthcare exposed the personal health information of 190 million people and left huge numbers of medical practices, hospitals, and pharmacies unable to submit claims or receive payments. Change Healthcare’s owner, UnitedHealth, estimates that the total direct costs associated with the attack could be as high as $1.15 billion.

$1.15 billion

Estimated direct costs of the Change Healthcare attack

The ransomware landscape

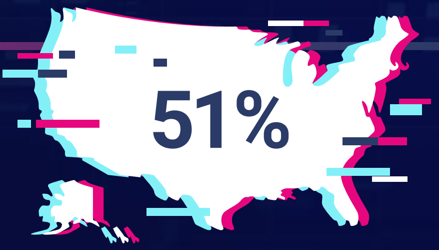
Known ransomware attacks by month



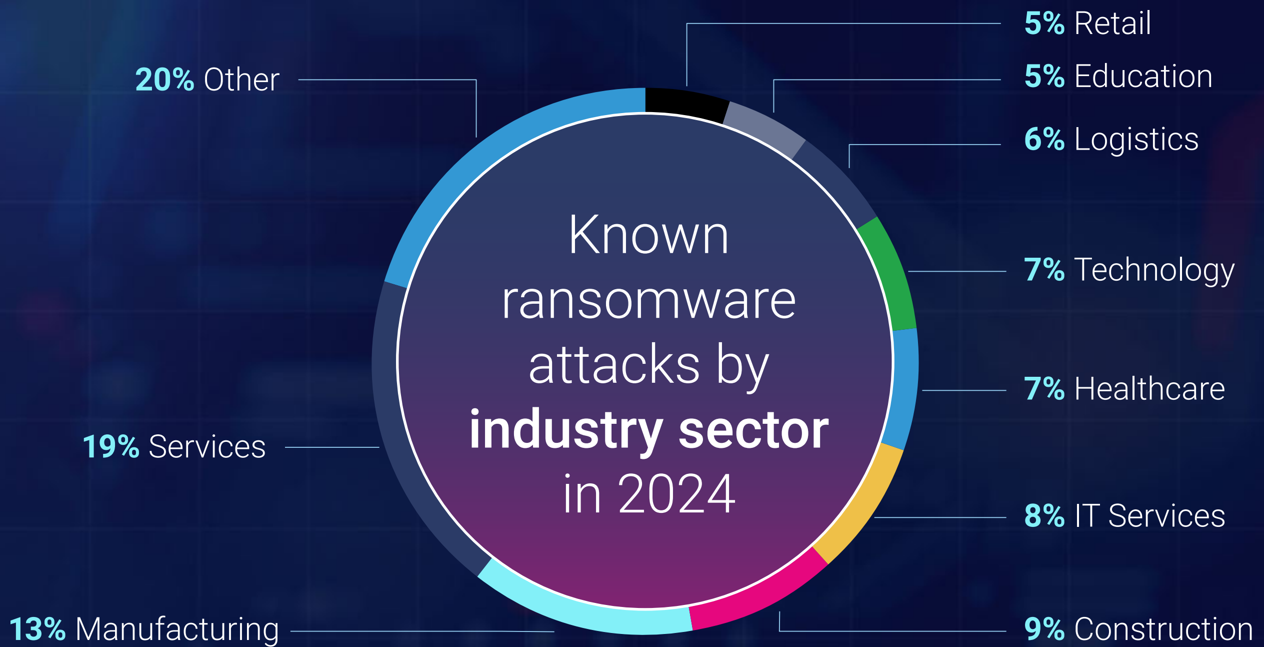
The USA has always been the primary focus of big game ransomware gangs, but in 2024 it received more attention than the rest of the world combined, accounting for 51% of known attacks. Outside of the USA, ransomware activity remained focused on English-speaking countries and major European economies.

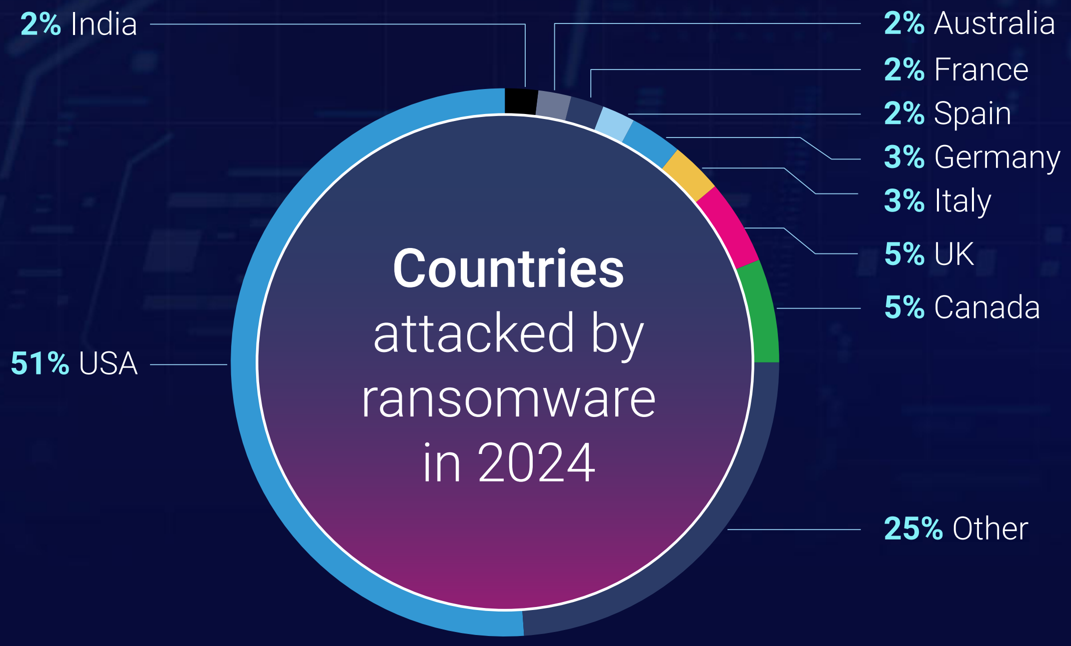
2024 saw attacks on the manufacturing sector increase by almost two thirds, and smaller increases in attacks on construction companies, and the technology and healthcare sectors.

It appears that by necessity or design, ransomware gangs are finding more targets outside of the service sector, in areas of the economy that are less obviously dependent on computers.



More than half of known ransomware attacks happened in the USA

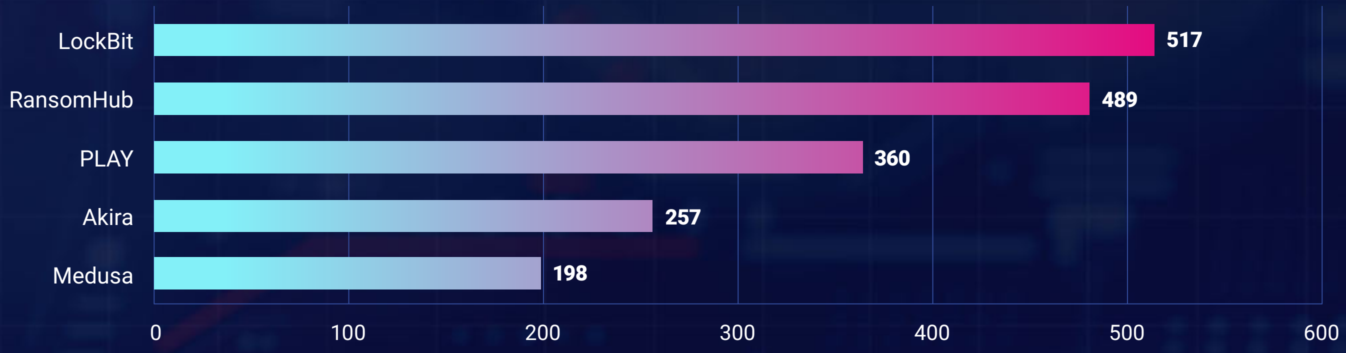

5% Retail
5% Education
6% Logistics
7% Technology
7% Healthcare
8% IT Services
9% Construction
13% Manufacturing
19% Services
20% Other
Known ransomware attacks by **industry sector** in 2024


2% India
2% Australia
2% France
2% Spain
3% Germany
3% Italy
5% UK
5% Canada
25% Other
51% USA
Countries attacked by ransomware in 2024

The demise of LockBit

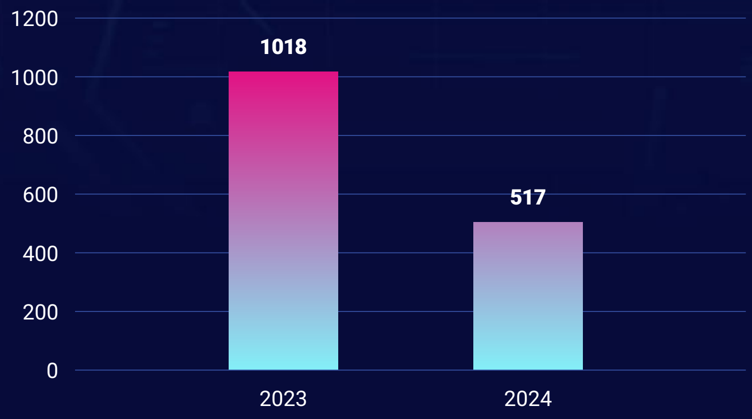
For the last few years, the most dangerous ransomware group has been LockBit, a ransomware-as-a-service vendor that once boasted of having 100 affiliates using its software to attack targets. LockBit's perennial bridesmaid was ALPHV, an equally unpleasant group, responsible for hundreds of attacks, including the devastating assault on Change Healthcare. That picture changed significantly at the start of 2024.

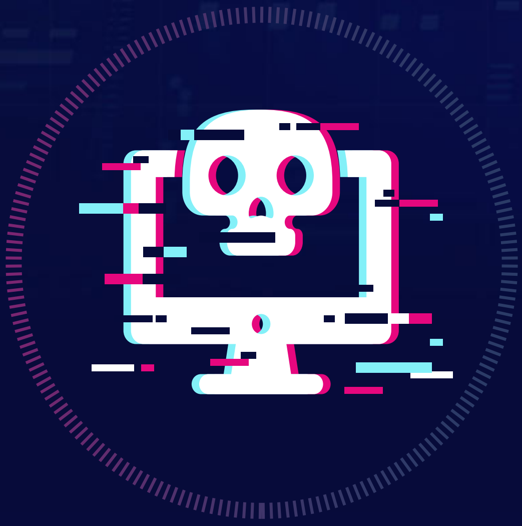
Top 5 ransomware groups by known attacks in 2024



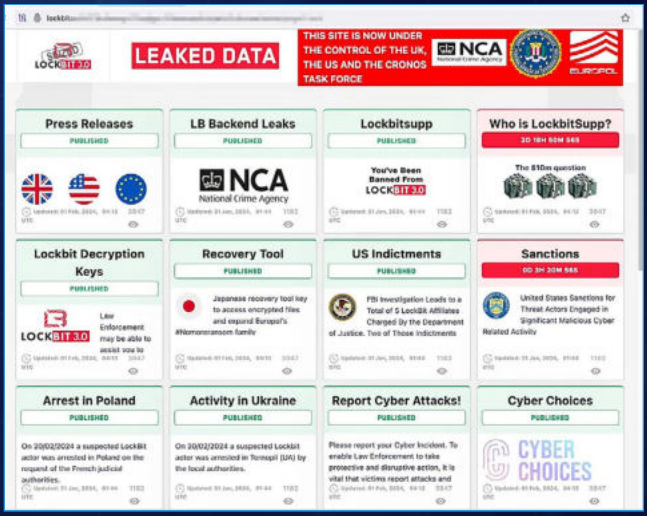
Operation Cronos, a multi-pronged law enforcement action against LockBit, brought down the ransomware gang's dark web site and placed it under the control of the UK National Crime Agency (NCA) in February, with the NCA using the site to troll the cybercriminal group and its affiliates with a series of damaging announcements. Although, by the numbers, LockBit was still the most dangerous ransomware group in 2024, its influence has declined massively in the wake of Cronos.

Known LockBit attacks in 2023 and 2024





Law enforcement trolls LockBit using its own dark web site



LOCKBIT 3.0

LEAKED DATA

THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE

NCA National Crime Agency

EUROPOL

Press Releases
PUBLISHED
Updated: 01 Feb, 2024, 04:13 UTC 3347

LB Backend Leaks
PUBLISHED
NCA National Crime Agency
Updated: 31 Jan, 2024, 01:44 UTC 1182

Lockbitsupp
PUBLISHED
You've Been Banned From LOCKBIT 3.0
Updated: 31 Jan, 2024, 01:44 UTC 1182

Who is LockbitSupp?
3D 18H 50M 58S
The $10m question
Updated: 01 Feb, 2024, 04:12 UTC 3347

Lockbit Decryption Keys
PUBLISHED
LOCKBIT 3.0
Law Enforcement may be able to assist you to
Updated: 01 Feb, 2024, 04:13 UTC 3347

Recovery Tool
PUBLISHED
Japanese recovery tool key to access encrypted files and expand Europol's #Nomoreransom family
Updated: 01 Feb, 2024, 04:13 UTC 3347

US Indictments
PUBLISHED
FBI Investigation Leads to a Total of 5 LockBit Affiliates Charged By the Department of Justice. Two of Those Indictments
Updated: 31 Jan, 2024, 01:44 UTC 1182

Sanctions
0D 3H 20M 58S
United States Sanctions for Threat Actors Engaged in Significant Malicious Cyber Related Activity
Updated: 31 Jan, 2024, 01:44 UTC 1182

Arrest in Poland
PUBLISHED
On 20/02/2024 a suspected LockBit actor was arrested in Poland on the request of the French judicial authorities.
Updated: 31 Jan, 2024, 01:44 UTC 1182

Activity in Ukraine
PUBLISHED
On 20/02/2024 a suspected Lockbit actor was arrested in Ternopil (UA) by the local authorities.
Updated: 31 Jan, 2024, 01:44 UTC 1182

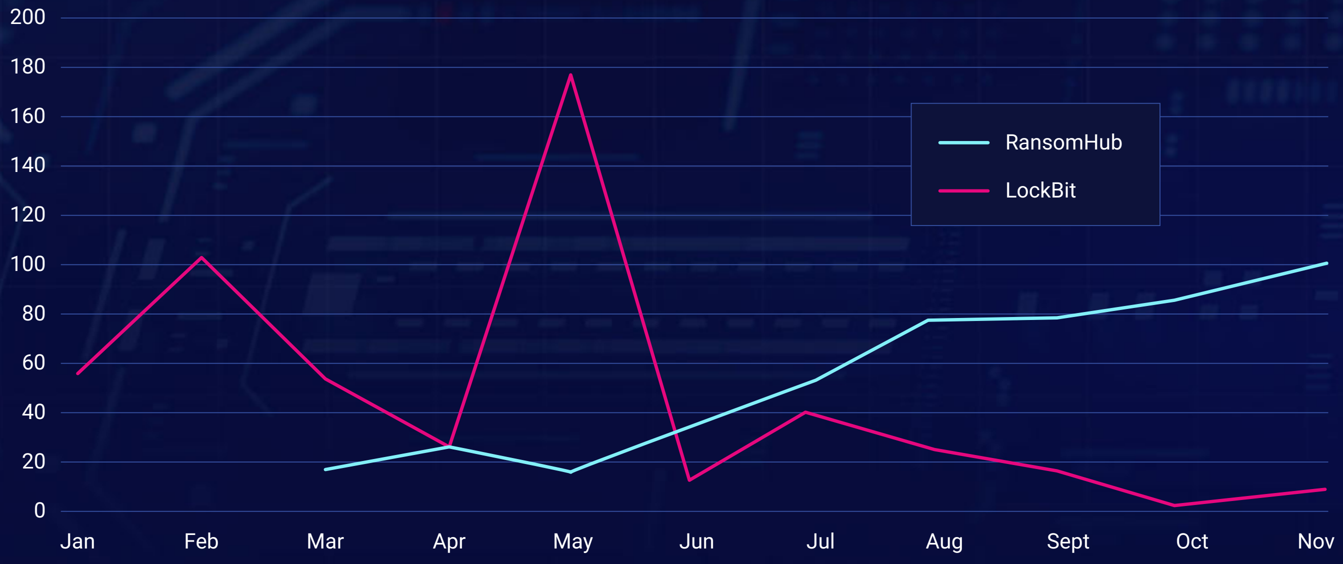
Report Cyber Attacks!
PUBLISHED
Please report your Cyber Incident. To enable Law Enforcement to take protective and disruptive action, it is vital that victims report attacks and
Updated: 01 Feb, 2024, 04:13 UTC 3347

Cyber Choices
PUBLISHED
CYBER CHOICES
Updated: 01 Feb, 2024, 04:13 UTC 3347

Shortly after the action against LockBit, the ALPHV group shut itself down in a poorly executed exit scam, after stealing the $22 million Change Healthcare ransom from the affiliate that carried out the attack.

In the wake of ALPHV's disappearance and LockBit's diminishment, the RansomHub group (which some believe is linked to ALPHV) emerged as the new dominant force in ransomware.

Known monthly attacks by LockBit and RansomHub in 2024



The rise of “dark horse” ransomware groups

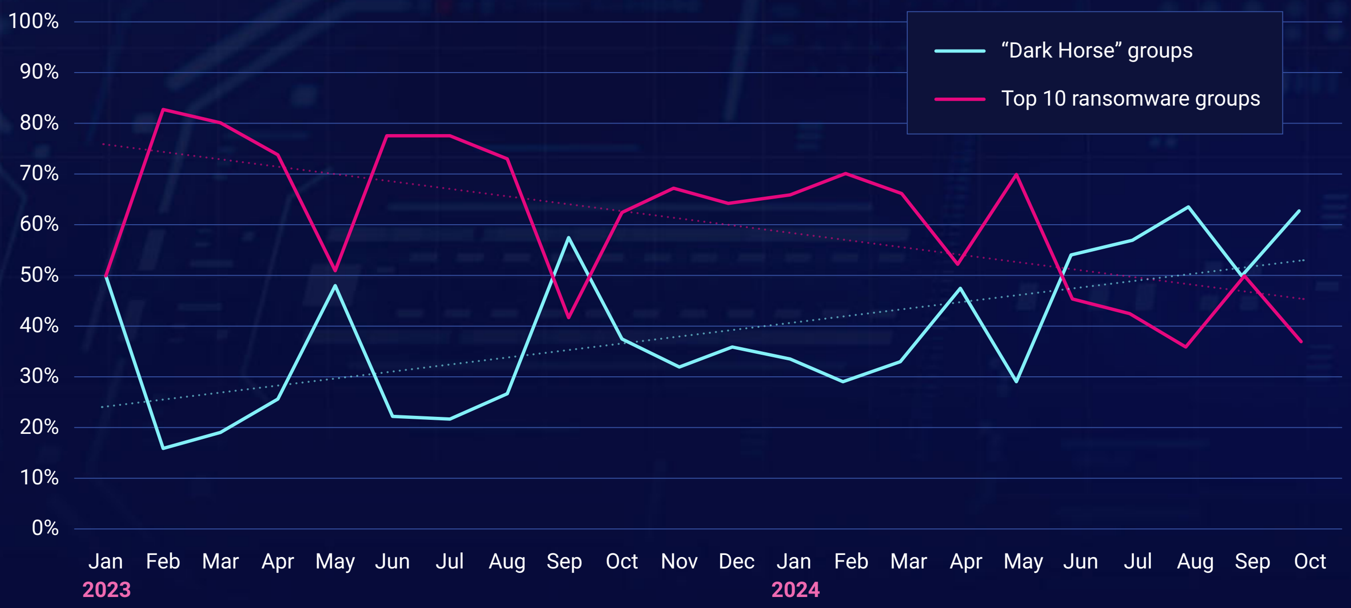
The most meaningful change in the big game ransomware landscape in 2024 was the diminished influence of large ransomware groups and the rise of little known “dark horse” gangs.

Historically, big game ransomware has been dominated by a few large criminal gangs, with a handful of groups playing a dominant role in the ecosystem. For example, in February 2023, 83% of known ransomware attacks were carried out by the ten most active groups.

Typically, the top ransomware gangs like Conti, LockBit, and RansomHub, sold ransomware-as-a-service (RaaS) to smaller affiliate gangs. The affiliates attacked on behalf of the RaaS groups and relied on them for software, infrastructure, and negotiations, and the profits were shared.

In the last year, the hobbling of LockBit and the demise of ALPHV seem to have accelerated an existing trend towards smaller groups. By October 2024, the top ten gangs accounted for just 37% of known attacks, with the bulk attributable to smaller, less well known “dark horse” gangs.

Share of known attacks by the 10 most active ransomware groups over 2 years



It appears that over time the tools and tactics for carrying out ransomware attacks have become more widely known and the barrier to entry for smaller groups has been lowered.

This "democratization" of ransomware is unwelcome news. Intelligence suggests that there are many more potential targets for ransomware than attacks. A lower barrier to entry makes ransomware an option for more criminal gangs, will fuel an increase in attacks, and could spur innovation and experimentation in the tactics that are used.

Evolving ransomware tactics

Ransomware tactics have evolved over the past year, too. In what looks like a response to improving cybersecurity defenses and a decreasing willingness to pay ransoms, attackers have improved the speed and stealthiness of their attacks with three tactics.

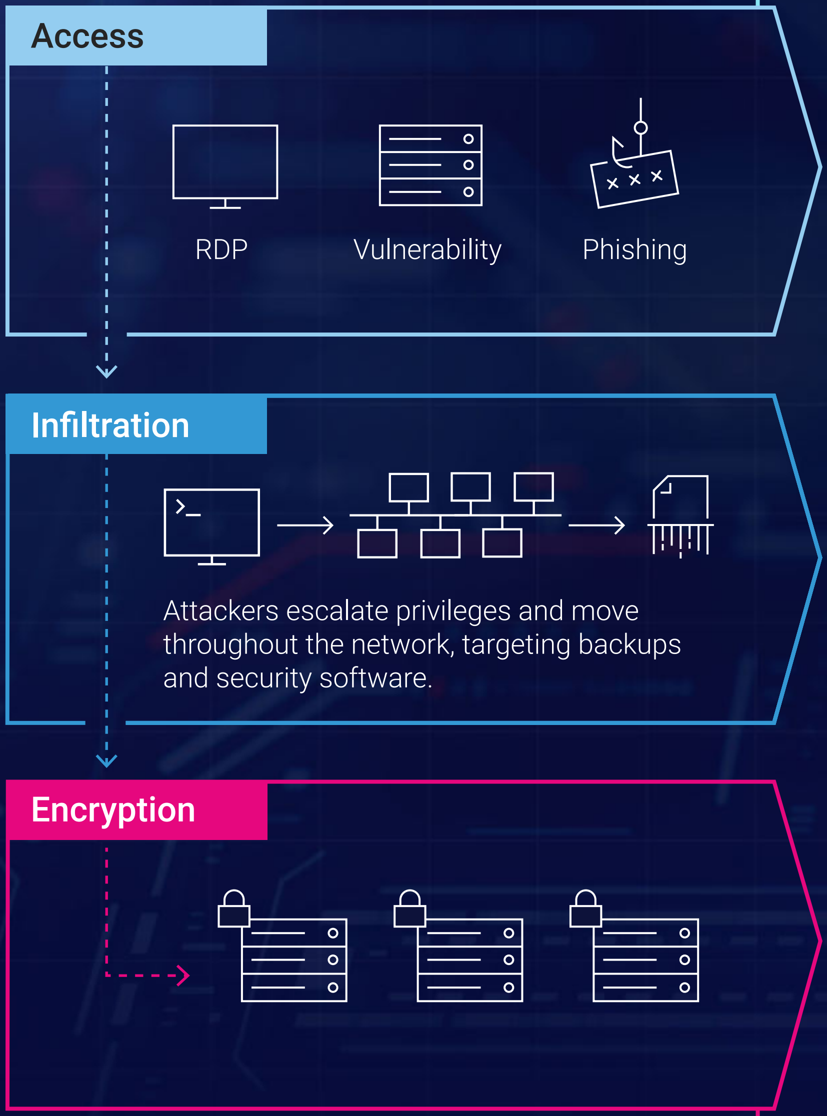
Ransomware gangs frequently attack in the early hours of the morning—when they know IT staff will not be around. The majority of ransomware attacks the ThreatDown Malware Removal Specialist (MRS) team handled in the last 12 months occurred between 1 am and 5 am.

Attacks are also taking less time to complete than ever before. The entire ransomware attack chain—from initial access and lateral movement to data exfiltration and then encryption—has decreased from weeks to hours, according to ThreatDown Incident Response (IR) data.

Data from the ThreatDown Managed Detection and Response (MDR) team show more ransomware gangs using Living Off the Land techniques, leveraging legitimate software and administration tools for malicious purposes. Recent customer incidents from top gangs such as LockBit, Akira, and Medusa reveal that most of the modern ransomware attack chain is now composed of LOTL techniques.

Most ransomware attacks happen at night, between the hours of 1 am and 5 am, while IT staff are asleep

Big game ransomware attack phases



Access

Infiltration

Attackers escalate privileges and move throughout the network, targeting backups and security software.

Encryption

Protection with ThreatDown

- Brute force protection
- Vulnerability Assessment
- Patch Management
- Anti-exploit protection
- DNS (Website Content) Filtering

- Managed Detection & Response
- Endpoint Detection & Response
- Application Block
- Anti-exploit protection
- DNS (Website Content) Filtering

- Managed Detection & Response
- Endpoint Detection & Response
- Next-gen AV
- Ransomware Rollback
- Incident Response

4. Living Off the Land (LOTL) tactics

In the last few years, cybersecurity detection tactics have changed. Threat actors—and ransomware gangs in particular—are increasingly relying on legitimate software instead of malware, a technique known as Living Off the Land (LOTL).

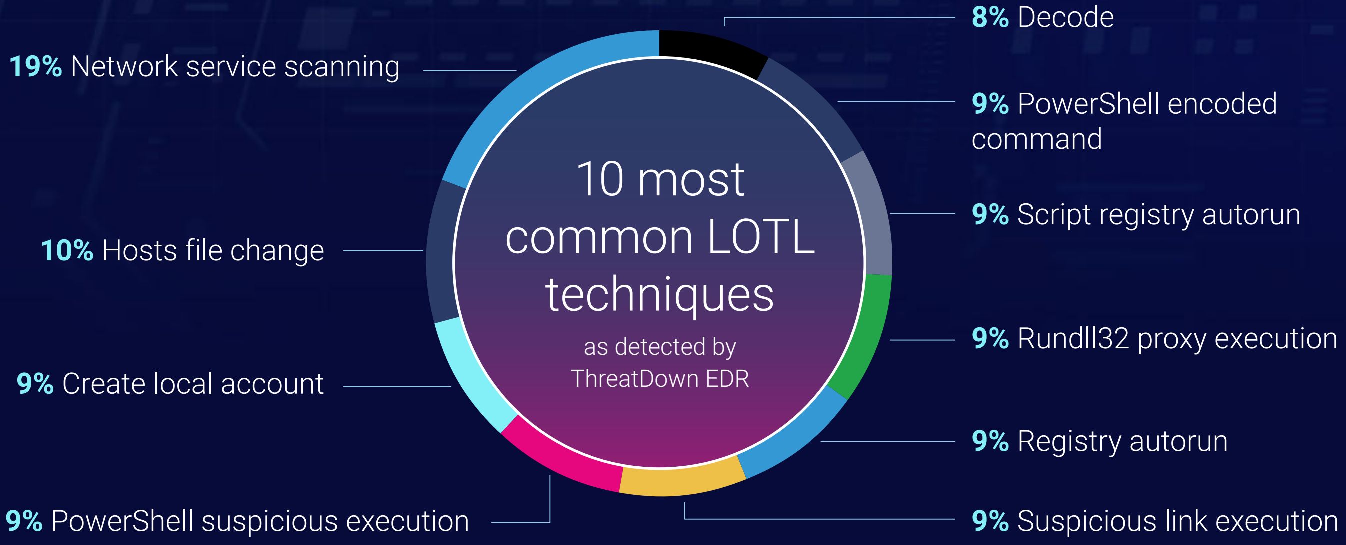
While malware remains a major problem, and multi-layered malware detection is still a vital part of the security stack, the most pressing security challenge has shifted from stopping malicious software to stopping malicious people using legitimate software.

Top EDR detections

Threat actors who gain access to your systems will try to disguise themselves as legitimate users and use commercial tools that don't look out of place on your network. Defenders can use Endpoint Detection & Response (EDR) to detect these attacks by looking for suspicious behavior and anomalies, such as software being used in unexpected ways, files being modified, activity at strange times, or accounts that shouldn't be there.

The top 5 most popular LOTL techniques detected by ThreatDown EDR in 2024 were:

1. **Network service scanning** (T1046)
   Network service scanning happens when an attacker inside a victim's network tries to discover more about it using techniques like port scans.
2. **Hosts file change** (T1565)
   An endpoint uses the hosts file for IP to hostname resolution before DNS, so attackers modify it to change the way traffic is routed.
3. **Create local account** (T1136.001)
   An attacker is creating an account for themselves on a single machine.
4. **PowerShell suspicious execution** (T1059.001)
   PowerShell is a favorite with threat actors and is used for a wide number of purposes.
5. **Suspicious link execution** (T1204.001)
   A user has clicked on a suspicious link.

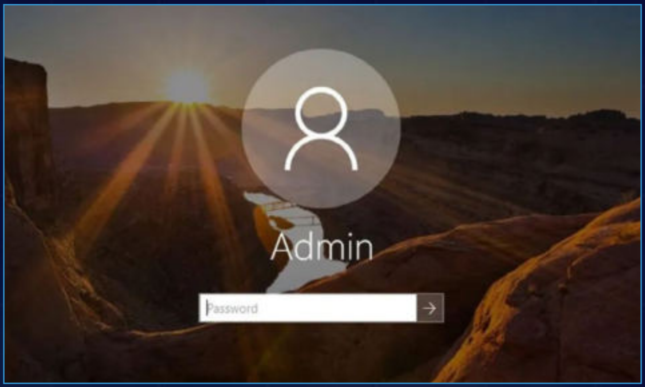


Remote access

Remote access tools are one of the most popular choices for threat actors trying to live off the land. Among ransomware gangs, the Windows Remote Desktop Protocol (RDP) remains extremely popular as a method of entry. In ransomware cases dealt with by ThreatDown's Malware Removal Specialists (MRS), RDP was by far the most common form of entry, being used in 58% of cases.

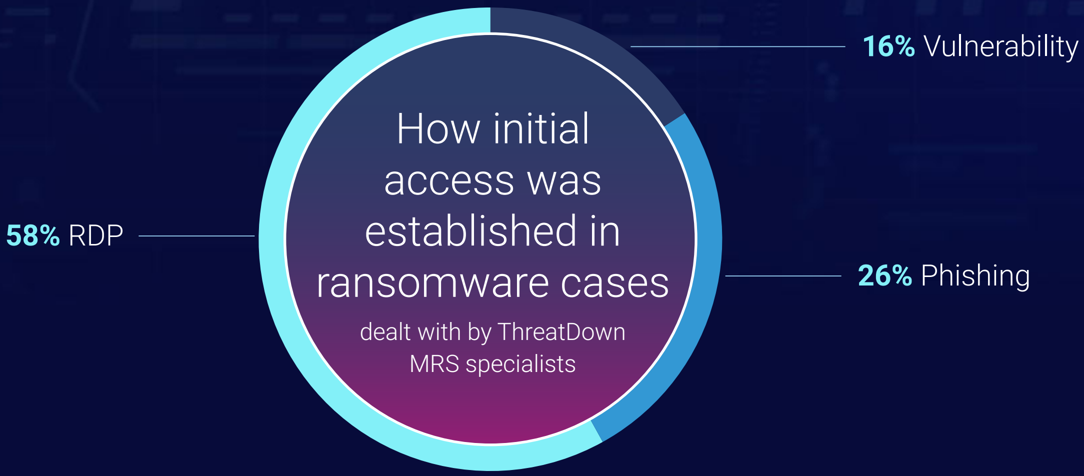
RDP exposes a login screen for a Windows computer to the Internet. There are millions of computers connected to the Internet via RDP, and each one is a gateway into a company network that gives a criminal the same access as sitting at a computer inside the company's office.

After accessing a victim's system, threat actors often try to establish persistence (long term access), and remote desktops are very popular for this task too. 21% of ransomware attacks observed by the MRS team in 2024 set up remote management and monitoring (RMM) software for persistence, and 80% of those attacks used AnyDesk or ConnectWise software—commercial software that is commonplace on business networks.



A Windows remote desktop accessible from the Internet

To make LOTL attacks more difficult, disable RDP or harden it with brute force protection, and block any remote desktop tools your company does not normally use, such as AnyDesk, ConnectWise, and TeamViewer.



Five tools to block LOTL tactics

Across the ransomware incidents we observe, certain tools show up consistently in attackers' arsenals. To disrupt LOTL attacks, you should block these tools, unless you have a good reason not to.

1. RMM tools

RMM tools like AnyDesk, NinjaRMM, and TeamViewer are used by attackers to provide remote access to environments they've compromised. Attackers can use these tools to exfiltrate data, escalate privileges, or deploy ransomware. Block as many as you can.

2. PDQ Deploy

PDQ Deploy is a legitimate tool used by administrators to install and update software across a network. ThreatDown has observed ransomware gangs like Medusa using it to deploy malware quickly to every connected machine in an organization.

3. Advanced IP Scanner

Advanced IP Scanner scans local area networks (LAN) to identify connected devices. Attackers like the Akira ransomware gang use it to perform network mapping—identifying all IP addresses, device types, and operating systems on the network.

4. IObit Unlocker

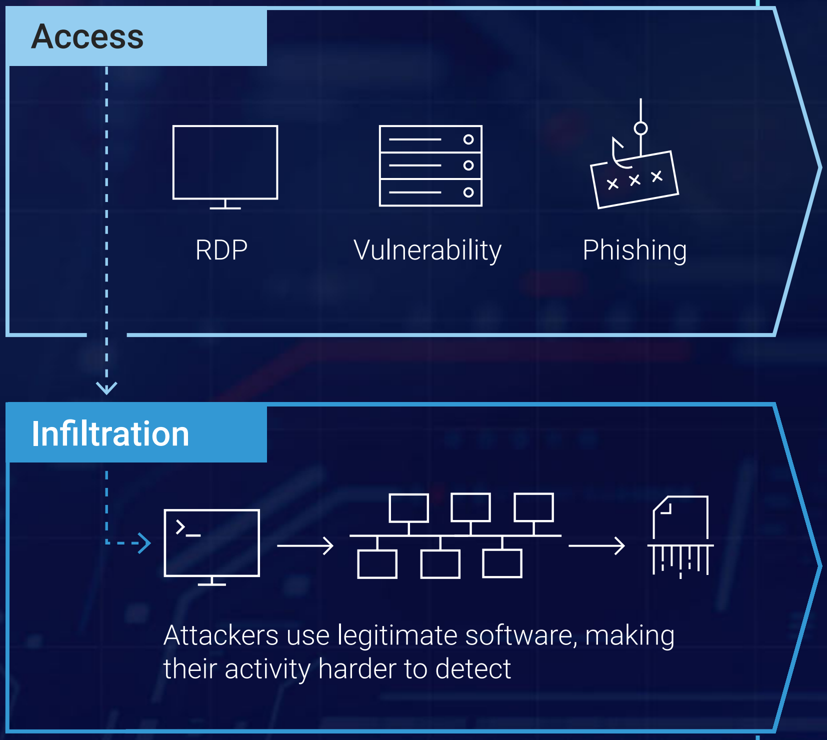
IObit Unlocker is designed to force unlock files that have been locked by another process. Ransomware gangs use it to unlock files tied to security programs, allowing them to disable or delete protective measures.

5. Process Hacker

Process Hacker is an open-source task manager used to manage processes and system services that uses elevated privileges and kernel-mode drivers. Ransomware attackers use it to disable security software.

Cybercriminals increasingly use legitimate IT administration tools instead of malware, making them extremely difficult to detect. Defending against these attacks requires skilled threat hunters using best-in-class EDR to find and investigate suspicious activity.

Living Off the Land attack phases



Access

RDP

Vulnerability

Phishing

Infiltration

Attackers use legitimate software, making their activity harder to detect

Protection with ThreatDown

- Brute force protection
- Vulnerability Assessment
- Patch Management
- Anti-exploit protection
- DNS (Website Content) Filtering

- Managed Detection & Response
- Endpoint Detection & Response
- Application Block
- DNS (Website Content) Filtering

5. macOS stealers

Mac malware is undergoing a revolution as an old guard of threats gives way to a dangerous new breed of information stealers that use the same feature set and distribution channels as Windows malware.

For many years, the most prevalent threats on macOS have been VSearch adware, or the browser hijacker Genieo. In 2024, a new generation of information stealers emerged to challenge the status quo and give Mac-using businesses a much more serious problem to worry about.

Stealers make money for criminals by finding and stealing valuable information on the computers they infect, such as credit card details, authentication cookies, passwords and cryptocurrency. Although they do not discriminate between computers on home or corporate networks, stealers' appetite for passwords and authentication cookies should be a serious concern to organizations using Macs.

The current sea change in Mac malware started in mid-2023 with the emergence of Atomic Stealer (AMOS), an information stealer with features that looked more like Windows malware than a traditional Mac threat. Since it emerged, AMOS has seen regular updates as its developers add features, and it has been used in numerous different malware distribution campaigns. Cybercriminals can control the information stealer via a web-based administration console that is sold "as-a-service" (similar to legitimate cloud applications) for $1,000 per month.

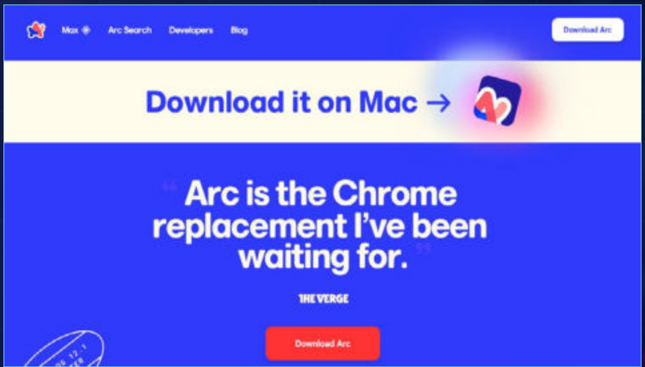
AMOS arrived at a time when demand for Macs was growing—despite declining PC sales—and malicious advertising (malvertising) was undergoing a resurgence as a malware distribution tactic. In malvertising attacks, cybercriminals make Google or Bing search ads for popular software products, and link to replica websites where unwitting users download malware instead of the software they were searching for.

Between the ad platforms' targeting features and their own fingerprinting code, malvertisers can deliver targeted ads and downloads based on a potential victim's location, operating system, software, and search terms. With this capability at hand, and modern malware like AMOS available, the stage was set for a change in Mac malware tactics.

The success of AMOS has promoted malware authors to create several copies or forks of the project. On June 23, 2024, the threat actor Rodrigo4 took to the XSS underground forum to announce that it was launching the latest version of its AMOS-based malware, RodStealer, under the name Poseidon.

The Poseidon console login screen

Poseidon boasts that it can steal cryptocurrency from over 160 different wallets, and passwords from web browsers, the Bitwarden and KeePassXC password managers, the FileZilla file transfer app, and VPN configurations including Fortinet and OpenVPN.

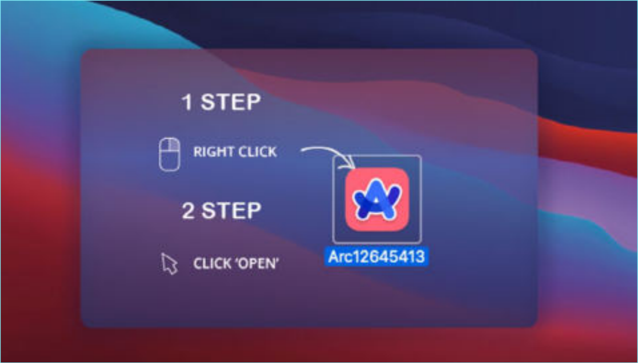


Download it on Mac →

"Arc is the Chrome replacement I've been waiting for."

THE VERGE

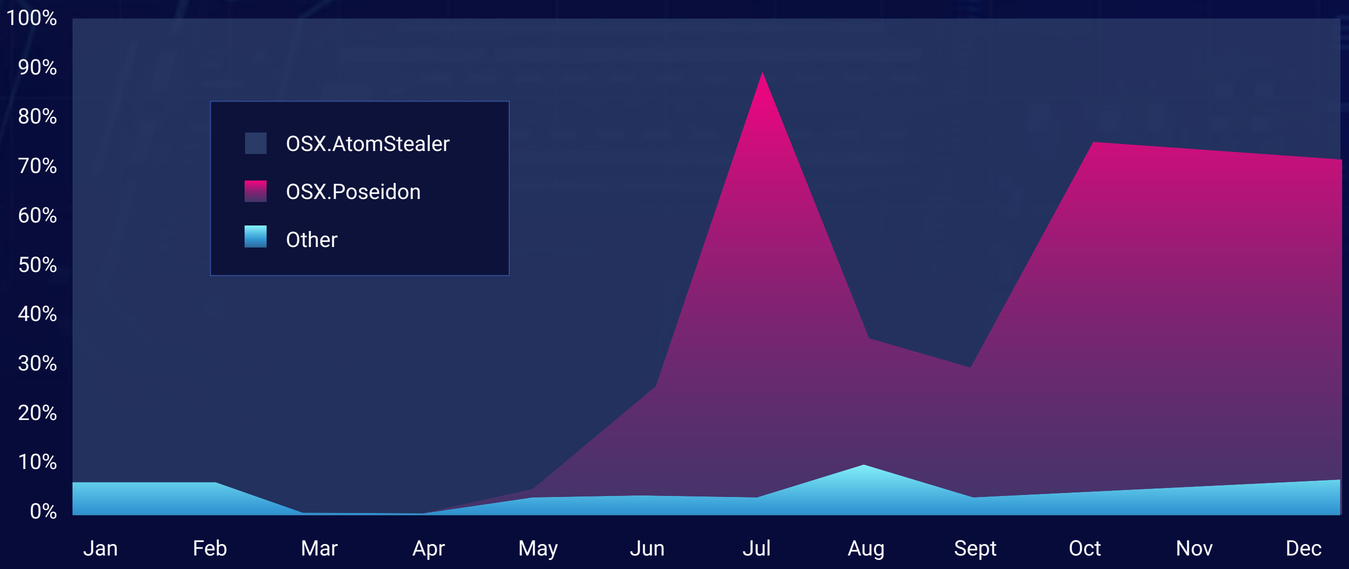
Poseidon installer disguised as the Arc browser



Poseidon malware DMG installer disguised as the Arc browser

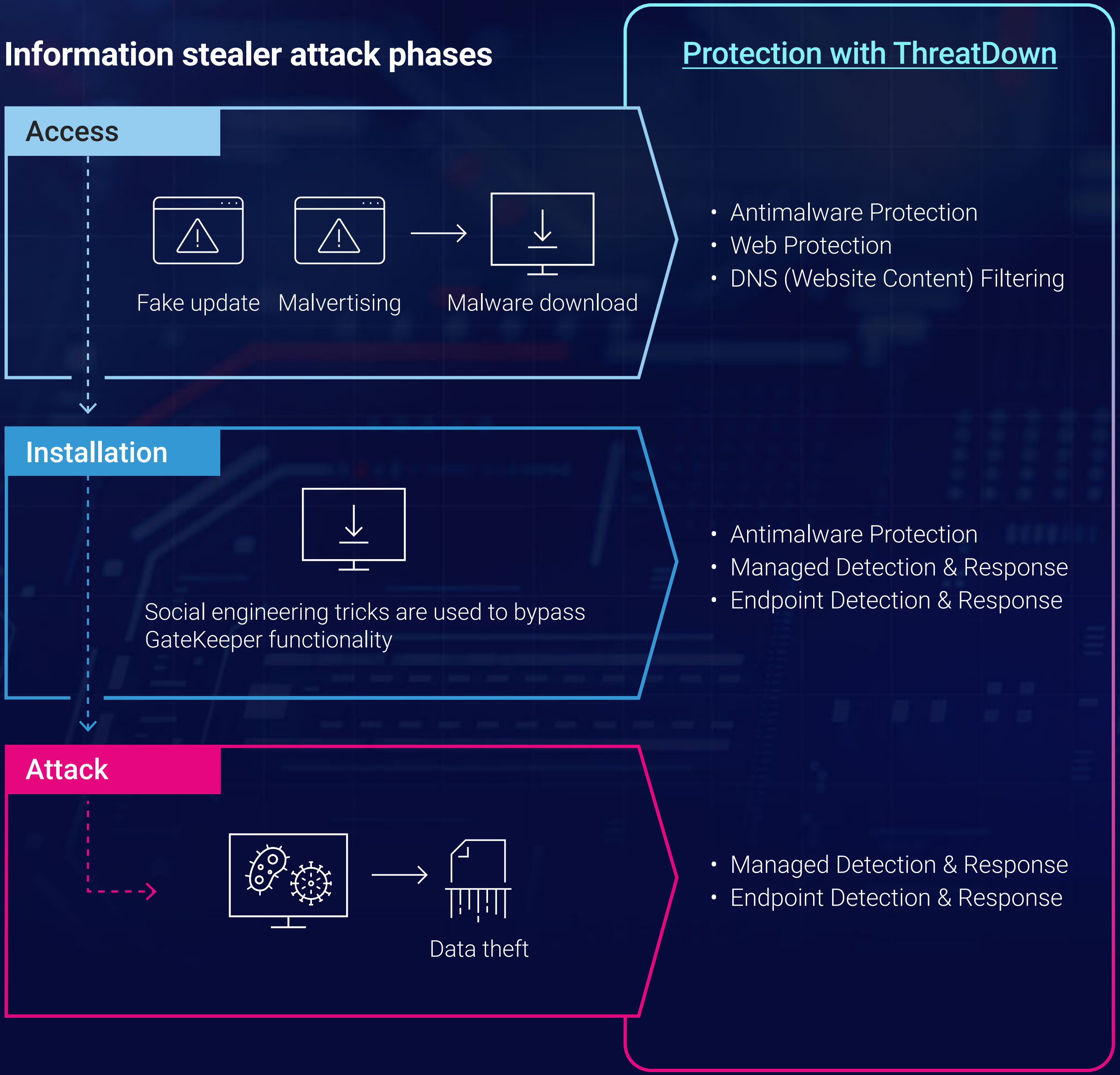
In the short time since its launch, Poseidon has overtaken AMOS as the dominant stealer and now accounts for 70% of information stealer detections on macOS. AMOS detections have remained relatively steady through the year though, so almost all Poseidon activity is net new, indicating a significant surge in stealer activity on Macs in 2024.

macOS information stealer market share in 2024



macOS stealers

Information stealers like Atomic Stealer and Poseidon are a serious and growing threat on the Mac platform. Criminals can use stolen credentials to steal information, access sensitive resources, and create convincing social engineering attacks. Defending against these stealers requires best-in-class macOS protection that can detect the malware and the malicious sites used to distribute it.



Information stealer attack phases

Protection with ThreatDown

Access

Fake update → Malvertising → Malware download

- Antimalware Protection
- Web Protection
- DNS (Website Content) Filtering

Installation

Social engineering tricks are used to bypass GateKeeper functionality

- Antimalware Protection
- Managed Detection & Response
- Endpoint Detection & Response

Attack

Data theft

- Managed Detection & Response
- Endpoint Detection & Response

6. Android phishing malware

Android phishing malware is a simple, hard-to-detect, and proven threat to organizations of all sizes. Just like phishing emails, phishing apps trick users into handing over their usernames, passwords, and two-factor authentication codes. Stolen credentials can be sold or used by cybercriminals to steal valuable information and access restricted resources.

The first phishing attacks date back to the mid-1990s, when a group of hackers posing as AOL employees used IM and email to steal users' passwords. It has since evolved into one of the most widespread and reliable cybercrime tactics.

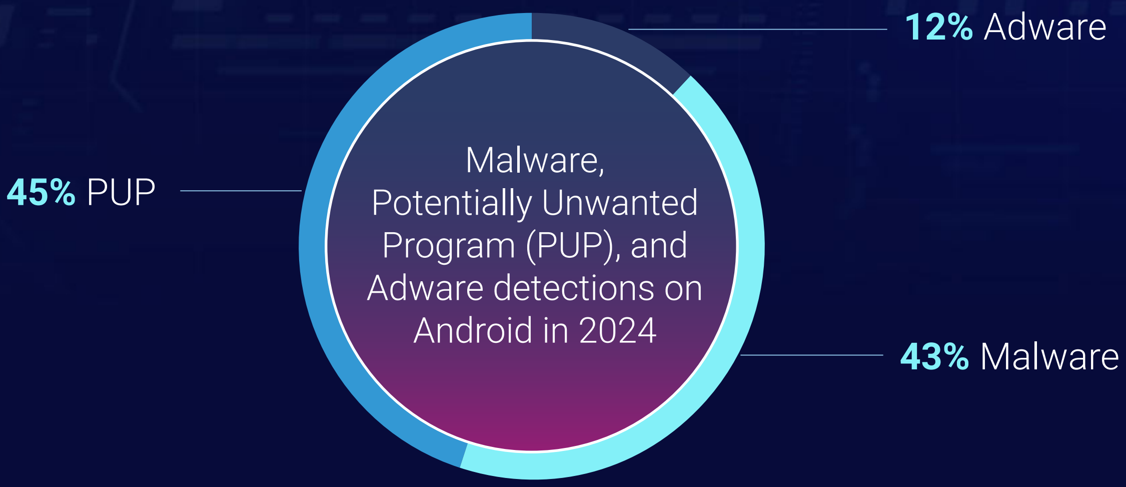
22,800

Phishing-capable apps detected in 2024

5,200

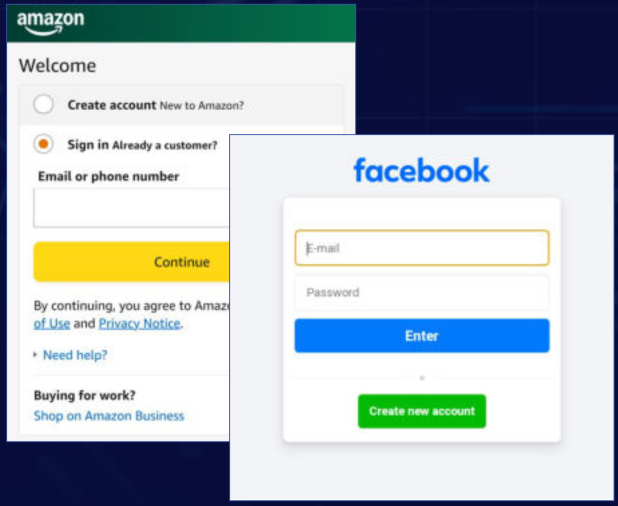
malicious apps detected containing code for reading OTPs from SMS messages

Phishing campaigns are hard to spot, scalable, low-cost, and adaptable, allowing attackers to target anyone from individuals to large organizations, and to shape their lures to fit changes in technology, fashion, and current events. Because they can be implemented with less code and simpler permissions than other types of malware, phishing apps are easier for Android malware developers to smuggle onto Android app stores.



Android phishing apps come disguised as fully functional, regular apps, such as games or utilities. On third-party app stores phishing functionality may even be bundled into illegal copies of famous apps like TikTok, WhatsApp, or Spotify. The phishing functionality may be dormant for days before it starts, to avoid drawing attention to the newly installed app.

Some malicious apps use phishing screens that are embedded in the apps themselves and relay the captured credentials to a server controlled by the threat actor. Other apps use ad functionality to open phishing websites in the phone's browser or in a WebView component inside the app. This exposes the victim to a wide variety of phishing sites and lures and ensures that the app does not contain any phishing code.



amazon

Welcome

○ Create account New to Amazon?

● Sign in Already a customer?

Email or phone number

Continue

By continuing, you agree to Amaz
of Use and Privacy Notice.

‣ Need help?

Buying for work?
Shop on Amazon Business

facebook

E-mail

Password

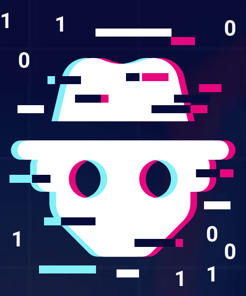
Enter

Create new account

Android phishing lures

3,900

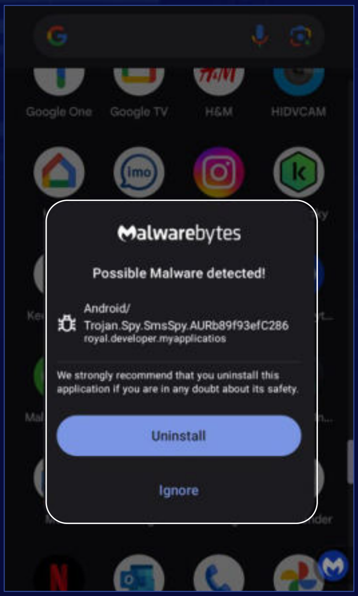
malicious apps detected containing code for reading OTPs from the notification bar



2FA theft

Organizations are increasingly using two-factor authentication (2FA) to improve the security of their login process, so Android malware developers have created techniques for compromising that too.

A lot of 2FA schemes use one-time passcodes (OTP) sent by SMS, so malicious apps monitor incoming SMS messages for OTPs, or read OTPs from the notification bar when the user is notified about an incoming SMS.



Malwarebytes

Possible Malware detected!

Android/
Trojan.Spy.SmsSpy.AURb89f93efC286
royal.developer.myapplications

We strongly recommend that you uninstall this application if you are in any doubt about its safety.

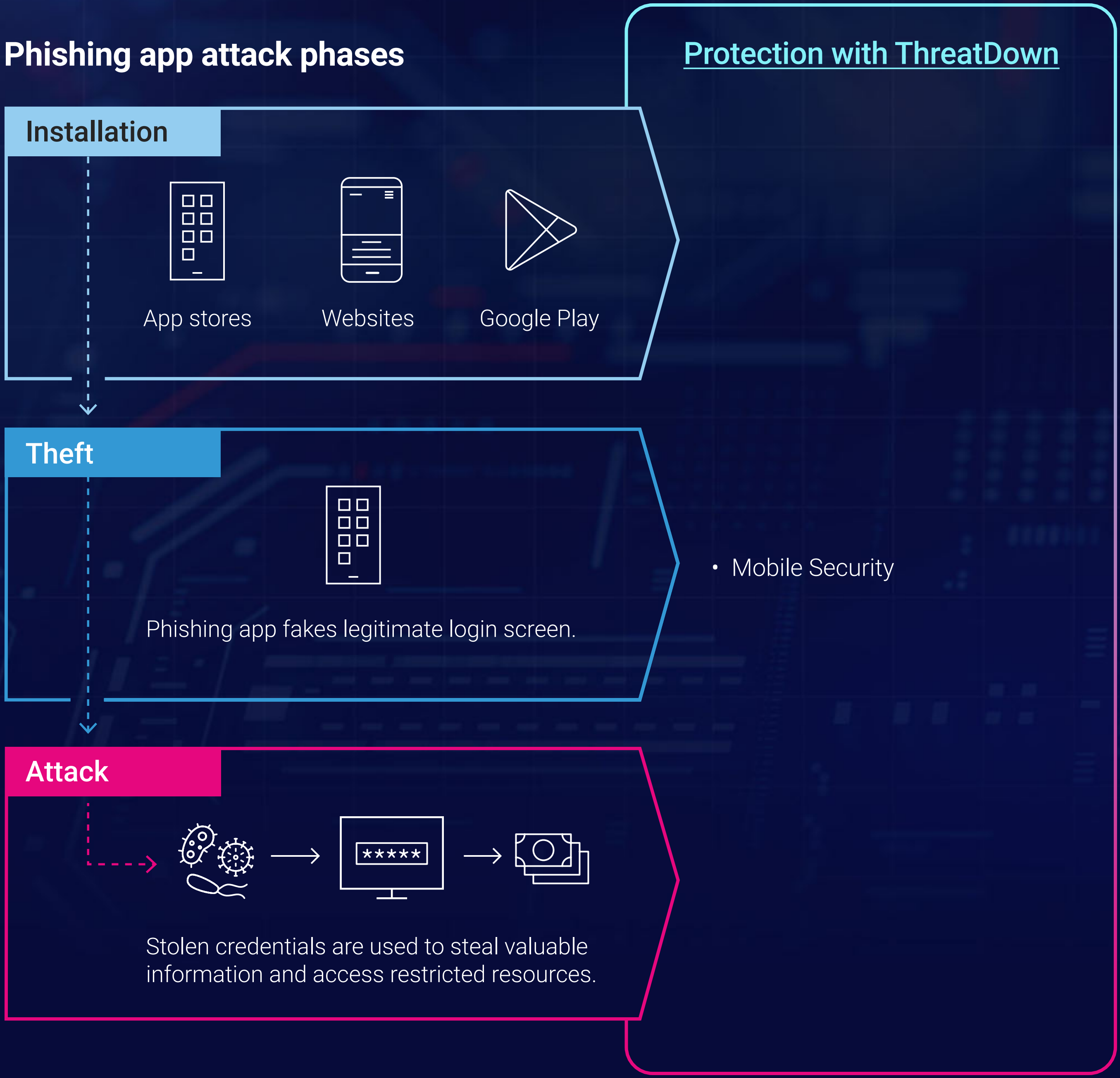
Uninstall

Ignore

ThreatDown catches malware spying on 2FA codes

Android phishing malware

Android phishing apps are a hard-to-detect danger to your organization. Criminals can use stolen credentials to steal information, access sensitive resources, and create convincing social engineering attacks. Defending against phishing apps requires best-in-class mobile protection that can detect all the different phishing tactics threat actors use in their malware.



Phishing app attack phases

Installation

App stores

Websites

Google Play

Theft

Phishing app fakes legitimate login screen.

Attack

Stolen credentials are used to steal valuable information and access restricted resources.

Protection with ThreatDown

- Mobile Security

7. Conclusion

“Big game” ransomware remains the most pressing cybersecurity challenge for organizations over the next year, as it has been for the last several years. But in 2025, IT and security teams will need to adapt to the way ransomware attacks are evolving. The two most dominant ransomware groups of the last few years, LockBit and ALPHV, have fallen away, creating a vacancy for a new leader, RansomHub, and a large group of smaller and less well known “dark horse” groups.

Attacks are getting quicker, happening at night, and becoming stealthier as ransomware groups increasingly switch from relying on malware to using Living off The Land techniques.

In 2025, an organization’s security against the most dangerous threats will rest on its ability to gather data from its endpoints, and identify anomalous behavior from benign user accounts, and applications like scripting engines and remote desktops. Armed with that data, they will need to sort the signal from the noise quickly, and act on alerts at any time of the day or night, on any day of the year.

On macOS, an invigorated criminal ecosystem is emerging based on a new generation of sophisticated infostealer malware, led by Atomic Stealer (AMOS) and Poseidon. 2024 has shown that change can happen quickly in the Mac malware landscape and organizations must ensure their Macs are as well defended against an upsurge in attacks as their Windows machines.

Although in the near term the threat landscape will likely be an evolution of what we saw in 2024, things are not as predictable as they once were. The next leap forward in AI will play out in 2025—agentic AI. Agents turn AI from a service you use into an intelligent, autonomous actor in the ecosystem. Agents will create revolutionary possibilities for defenders wrestling with a skills gap and ransomware actors looking for ways to scale their attacks. The shape of cybersecurity in 2025 could rest on who embraces the technology successfully.

8. How to protect your company

ThreatDown addresses today's evolving cybersecurity challenges with Malwarebytes award-winning technologies and services that offer protection across the entire attack cycle: from attack surface reduction; to prevention, detection, and response; and full remediation. Protect your endpoints with four powerfully simple and cost-effective bundles:

ThreatDown Core

Core offers complete next-gen AV with vulnerability assessment and application blocking. Driven from the cloud through a single pane of glass, it delivers simplified management and speed for resource-constrained organizations.

ThreatDown Advanced

Advanced offers award-winning prevention, detection and response technologies. It reduces the attack surface by patching vulnerabilities and blocking malicious and unwanted applications. Managed Threat Hunting uncovers signs of attacks, prioritizes alerts, and delivers easy step-by-step recommendations to guide remediation.

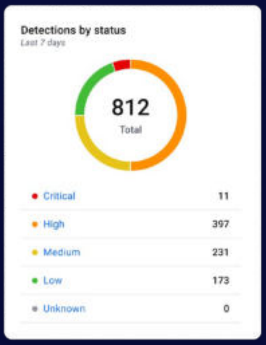
ThreatDown Elite

Elite delivers award-winning endpoint security along with 24x7x365 expert-managed monitoring and response. Elite is built on our AI/ML-driven prevention, detection, and response technologies fortified by built-in innovations that dramatically shrink the attack surface. In addition, these technologies offer unparalleled ease of use via a single pane of glass.

ThreatDown Ultimate

Ultimate is our most complete endpoint security solution. It is built on our strongest AI/ML-driven prevention, detection, and response technologies fortified by built-in innovations that dramatically shrink the attack surface. It features industry-leading technology and award-winning 24x7x365 monitoring and response by our cybersecurity experts resulting in unparalleled ease of use via a single pane of glass.

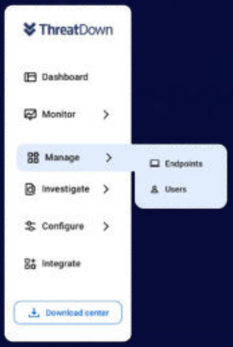
Take threats down


Detections by status
Last 7 days

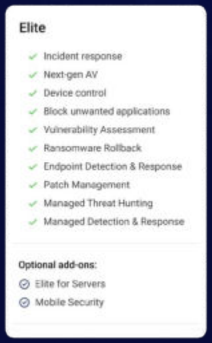
812
Total

● Critical	11
● High	397
● Medium	231
● Low	173
● Unknown	0

Take complexity down



Take costs down


Elite

- ✓ Incident response
- ✓ Next-gen AV
- ✓ Device control
- ✓ Block unwanted applications
- ✓ Vulnerability Assessment
- ✓ Ransomware Rollback
- ✓ Endpoint Detection & Response
- ✓ Patch Management
- ✓ Managed Threat Hunting
- ✓ Managed Detection & Response

Optional add-ons:

- ✓ Elite for Servers
- ✓ Mobile Security

We get it - security is hard. Security products shouldn't be.

See the capabilities in each ThreatDown Bundle.

What you get	Core	Advanced	Elite	Ultimate
Incident Response	✓	✓	✓	✓
Next-gen AV	✓	✓	✓	✓
Device Control	✓	✓	✓	✓
Application Block	✓	✓	✓	✓
Vulnerability Assessment	✓	✓	✓	✓
Ransomware Rollback		✓	✓	✓
Endpoint Detection & Response		✓	✓	✓
Patch Management		✓	✓	✓
Managed Threat Hunting		✓		
Managed Detection & Response (includes threat hunting)			✓	✓
DNS (Website Content) Filtering				✓
Add-Ons	✓	✓	✓	✓

Try ThreatDown today!

Let us take care of your endpoint security. Deploy the solution that delivers superior defense, easiest to use management, and the best value for your security investment.

Get started

ThreatDown™
Powered by Malwarebytes

threatdown.com