ThreatDown™
Powered by Malwarebytes

2023 STATE OF MALWARE

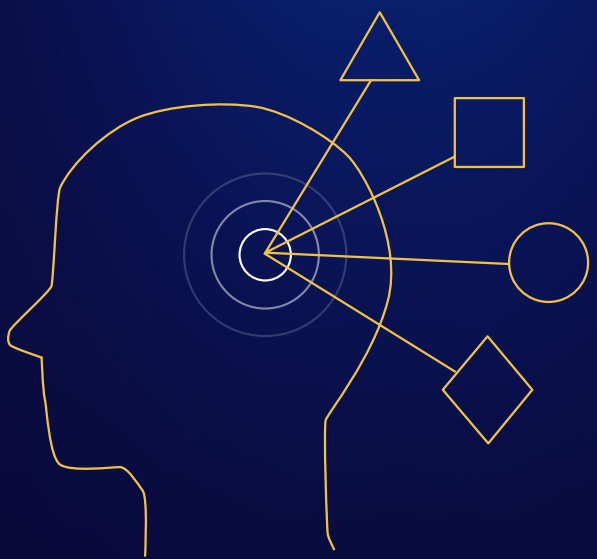
The 5 cyberthreat archetypes to stop this year

CONTENTS

1 INTRODUCTION

Adapt or die

The old rules of cybersecurity are dead. No longer can your business rely solely on the best security software to defend you from your attackers' most dangerous malware. Now, the fight is increasingly human—it's your best people against their worst.



Their worst

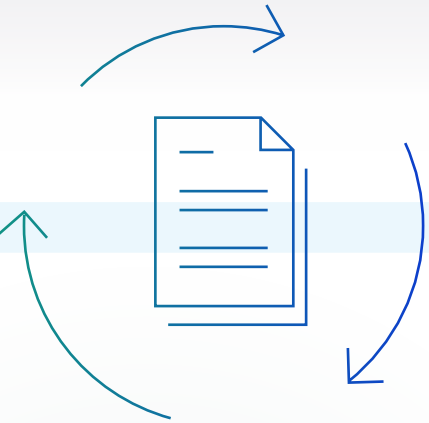
Over the last five years, the most serious cybersecurity task facing businesses has changed from defending your organization against waves of malicious software delivered by email to stopping seasoned criminals breaking into your networks and manually deploying ransomware.

And as vendors have fixed or retired reliable attack vectors like Flash, Internet Explorer, and Microsoft Office macros, criminals have increasingly turned to social engineering—psychological manipulation—as a replacement.

Your best

Endpoint protection remains singularly important for businesses—nothing else can diffuse a malware detonation when its countdown hits 00:00. However, the skills and experience of the people in the loop are now just as critical.

Increasingly, running malware is just the final act in breaches by criminal hackers who are practiced at moving through networks unnoticed. It takes experts who can aggregate and correlate data from tools like EDR, SIEM and other telemetry with global threat intelligence to find cybercriminals, trace their steps, and evict them.



About this report

To reflect the elevation of human skills and experience in cybersecurity, we've evolved our annual State of Malware report. Lists of the most detected malware are gone—they reflect what is the most common, not what is the most dangerous. It is shorter, too. What you want is to get the facts, to get security right, and to get on with running your business.

So, this year we asked our experts, our threat intelligence analysts, and the threat hunters in our Managed Detection and Response (MDR) team: What do resource-constrained organizations need to know?

Together we identified the key cybersecurity developments of 2022, and chose five threats that represent the diversity and seriousness of the dangers that organizations face at the start of 2023. Each of our five threats is a danger in its own right, and each one is an archetype for a class of similar threats. Between the five threats, they form a blueprint for understanding the likely dangers of the year ahead.

Key developments in 2022

Several events occurred in 2022 that are likely to have an impact on cybersecurity in the year ahead.

In some ways it was a break from the past few years of turmoil. There were few defining events—no high-profile attacks on the scale of 2021's Colonial Pipeline shutdown, and no upheavals that came close to 2020's shift to remote work.

And despite countless other atrocities, the outbreak of a major land war in Europe did not unleash a wave of destructive malware attacks against critical infrastructure as some predicted.

But to call the year uneventful would be to trivialize the relentless, daily assault on organizations and individuals of all

6 KEY DEVELOPMENTS

71%

of companies worldwide were affected by ransomware.

kinds, in all countries. 71 percent of companies worldwide were affected by ransomware, and by the end of November, over 22,500 new vulnerabilities had been added to the global CVE database—already 10 percent more than the previous year.

If anything, 2022 lacked the blaring klaxon of any single cyber-crisis, and was instead drowned in the din of daily cyberattacks.

Amidst all this, some progress emerged.

The imminent retirement of desktop operating systems older than Windows 10 is good news; a viable form of password-free authentication received major backing from Google, Microsoft and Apple; and there were signs that ransomware is having to adapt to pressure from defenders.

Ukraine Conflict

Speculation about whether Russia's invasion of Ukraine would include the first "cyberwar," where malware would be used to cause physical damage and destruction, proved unfounded. Although destructive attacks by wipers occurred, the cyberspace domain was largely reserved for information gathering and espionage, as it also is during peacetime.

The strategic importance of the Ukraine conflict made it a useful social engineering lure, and the ThreatDown Threat Intelligence team saw the topic of the war being used as a theme in attacks against German targets by suspected Russian state actors, and against Russian targets by suspected Chinese state actors.

Will Putin use nuclear weapons in Ukraine? Our experts answer three burning questions.

As Russian President Vladimir Putin confronts a series of humiliating battlefield setbacks since his February 24 invasion of Ukraine, and amid an increased flow of Western arms in the country, the risk of escalation reamains all too real.

So we asked some of our top experts to answer three burning questions about a scenario that has alarmed many analysts watching this war unfold: the Kremlin following through on its threats and using nuclear weapons in the conflict, they weighed in on the chances of Putin taking the fateful step, how he might do it, and how the West would likely respond.

#1: What's the likelihood that Vladimir Putin uses nuclear weapons in the course of the war in Ukraine?

Putin is more likely than not to use nuclear weapons in the war in Ukraine if he faces devastating defeat. If Putin perceives an existential threat to his regime, then he will be compelled to prevent that outcome—even if that requires taking risky

A malicious Word document from Russia's APT28 group asks "Will Putin use nuclear weapons in Ukraine?"

Ransomware

An unexpected effect of the war in Ukraine was the dissolution of Conti, which, according to the FBI, was the "the costliest strain of ransomware ever documented." When the Conti ransomware group released a statement in support of Russia's invasion of Ukraine, it inadvertently made ransom payments a potential sanctions violation. Victims stopped paying and Conti was forced to disband.

Conti's conclusion meant little to the broader ransomware ecosystem, though, which proved as robust as ever. Other cybercriminals were quick to take Conti's place, and LockBit emerged as the most active ransomware group in 2022 by a wide margin.

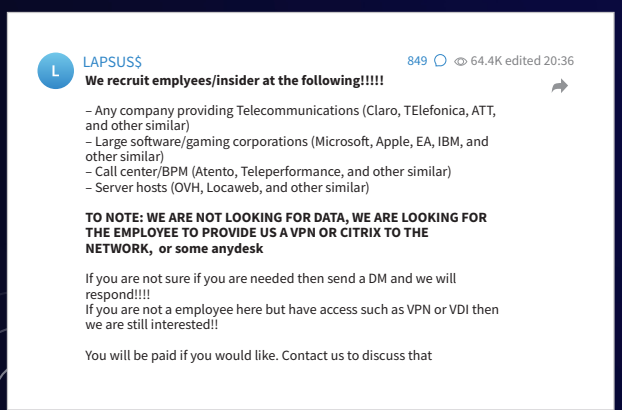
Ransomware remains the most significant criminal threat to businesses, but there were signs that the cybercriminals behind it are having to adapt. Leaking data began displacing data encryption as the primary form of extortion. This was likely a response to encrypting malware's vulnerability to both endpoint security software and effective backup and recovery strategies.

Data theft is harder to combat because it can be performed using administration tools already present on a victim's network. In 2023, organizations will need experienced staff capable of spotting stealthy intruders who don't run malware.

Ransomware groups experimented with new tactics throughout 2022, although few of those tactics caught on. One tactic that may see more success in 2023 is buying access to companies via disgruntled employees.

Ransomware remains the most significant criminal threat to businesses.

In March, the LAPSUS$ gang made headlines after posting a message on its Telegram channel saying it was looking to recruit tech company "employees/insiders" who were prepared to provide remote access, such as VPN, RDP, or Citrix access.



A message on a LAPSUS$ Telegram channel saying it was looking to recruit tech company "employees/insiders."

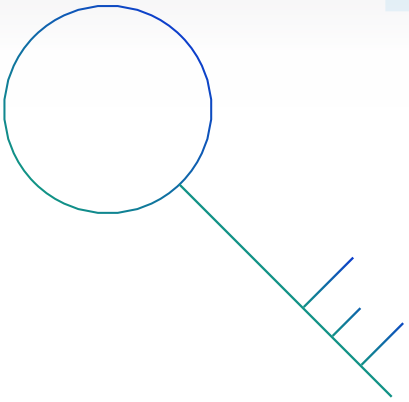
With the world indicating an economic downturn and layoffs set to continue, this is a tactic to watch closely.

Macros

In 2022, Microsoft announced that it would block macros in Office documents downloaded from the Internet, finally putting the brakes on one of the most productive malware delivery systems ever invented.

The macro block took a while to get right, and its rollout is not quite finished, but criminals have already started exploring alternative techniques.

In the absence of one obvious replacement for malicious macros, we are now entering an era of increased experimentation from threat actors. Defenders and threat hunters will need to be vigilant for novel approaches.



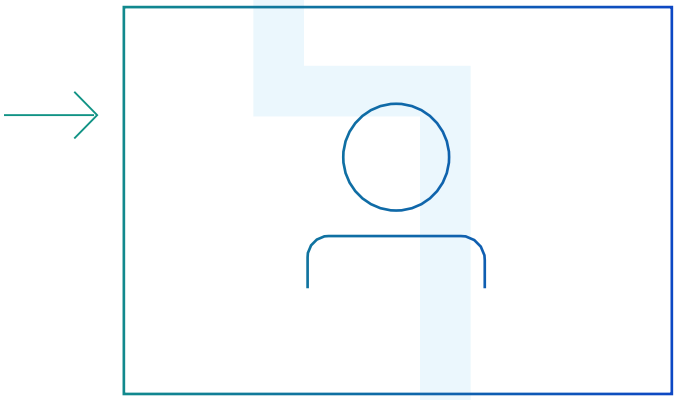
Authentication

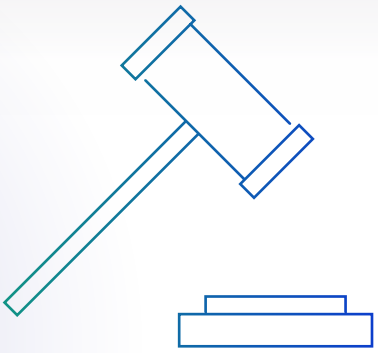
Passwords have been an Achilles heel in cybersecurity for a long time, and password attacks—like phishing, brute force guessing, credential stuffing, and password spraying—are mainstays of cybercriminal activity, enabling everything from ransomware attacks to stolen Instagram accounts.

It has taken a long time to settle on a genuinely viable alternative, but in May, Google, Apple, and Microsoft pledged substantial support for FIDO2, a mature, extant, and globally recognized standard for password-free authentication. History is littered with password replacements that never caught on because they were too costly, too poorly supported, or too difficult to implement. FIDO2 was designed to overcome those problems and the backing it received in 2022 is the result of that work. It now looks set to become an important authentication technology in 2023.

Passwords have been an Achilles heel in cybersecurity for a long time.

In the meantime, as multi-factor authentication became more common, criminals adapted their attacks. In September, Uber was gripped by a security incident after its notification-based multi-factor authentication was defeated by simply frustrating an employee into submission. After bombarding them with push notifications, the attacker messaged the victim, posing as technical support. The attacker advised the employee to accept one of the notifications to make them stop.

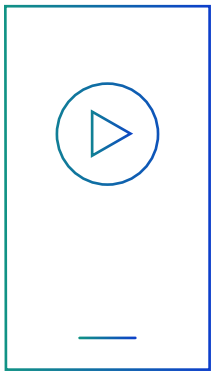




Roe v. Wade

The most consequential change to data privacy in 2022 occurred in June, when the US Supreme Court overturned Roe v. Wade. Overnight, concerns about digital privacy broke into the mainstream as previously benign data points—such as locations, shopping habits, search histories, and menstrual cycles—acquired a potentially life-changing significance. Women were left asking whether they should delete apps and data, and where it was safe to ask about abortions online, or to organize and provide support to those seeking them.

Overnight, concerns about digital privacy broke into the mainstream.



TikTok & Privacy

In June, US Federal Communications Commission commissioner Brendan Carr delivered the most outspoken criticism so far of the social media app TikTok, calling it "an unacceptable national security risk" because of its extensive data gathering, as well as "Beijing's apparently unchecked access to that sensitive data." Several US states banned the app from state-owned devices, and on December 14 the US Senate passed a bill barring federal employees from using it on government-owned devices.

2 LOCKBIT
The most dominant ransomware

LockBit rose to dominion in 2022 and accounted for about one-third of all known ransomware-as-a-service attacks. If you can understand and address LockBit, you'll greatly reduce the risk of any ransomware attack on your organization.

An army of affiliate attackers

LockBit is a type of ransomware-as-a-service (RaaS) which is deployed in cyberattacks by "affiliates"—criminal gangs that do not develop the ransomware itself, but who carry out attacks with it. If successful, they pay a share of their ill-gotten gains back to the ransomware's creators. In a RaaS attack, criminal hackers break into a business network, steal data, and encrypt files, grinding the organization to a halt. The attackers demand huge ransoms in return for decrypting the files, and for destroying stolen data instead of leaking it.

Lower volume. Higher severity.

The most widely used RaaS in 2022 was LockBit, with hundreds of known victims. It accounted for almost a third of all known RaaS attacks, and more than three times as many as its closest competitor. Because RaaS attacks are carried out manually, the total number of attacks is much lower than some other malware, but those attacks are extraordinarily high in severity.

Patient, meticulous attacks. Devastating effects.

An affiliate can spend days or even weeks inside a victim's network before launching a LockBit attack. Once an attack hits, ransom negotiations between affiliates and their victims can take weeks to conclude, and ransom demands can reach tens of millions of dollars.

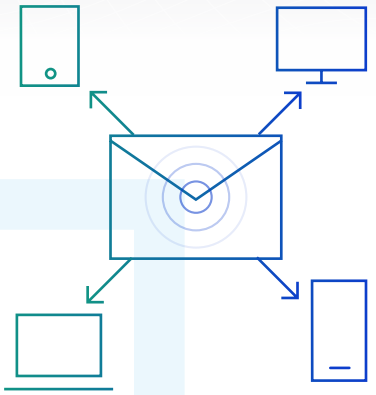
LockBit's victims included businesses of all sizes, from local law firms with a handful of employees to multi-national enterprises.

With an attractive, modern site on the dark web and sophisticated marketing, LockBit has embraced many of the practices and conventions of legitimate commercial software.

A more polished, professional approach to criminal ransomware

LockBit is a small, professional, and highly resilient operation that has evaded law enforcement since 2019. It puts a lot of effort into marketing itself to affiliates, maintains a slick dark web website, conducts PR stunts, and pays bug bounties for finding flaws in its software. It claims to have one hundred affiliates, so if one is caught, the LockBit operation is not disrupted.

LockBit's largest known ransom demand in 2022 was $50 million, although multiple sources report even higher demands were made. LockBit's victims included businesses of all sizes, from local law firms with a handful of employees to multi-national enterprises like Thales Group and Continental.



LockBit by the numbers

3.5x

LockBit is responsible for more than three times as many known attacks as the next most active ransomware, ALPHV

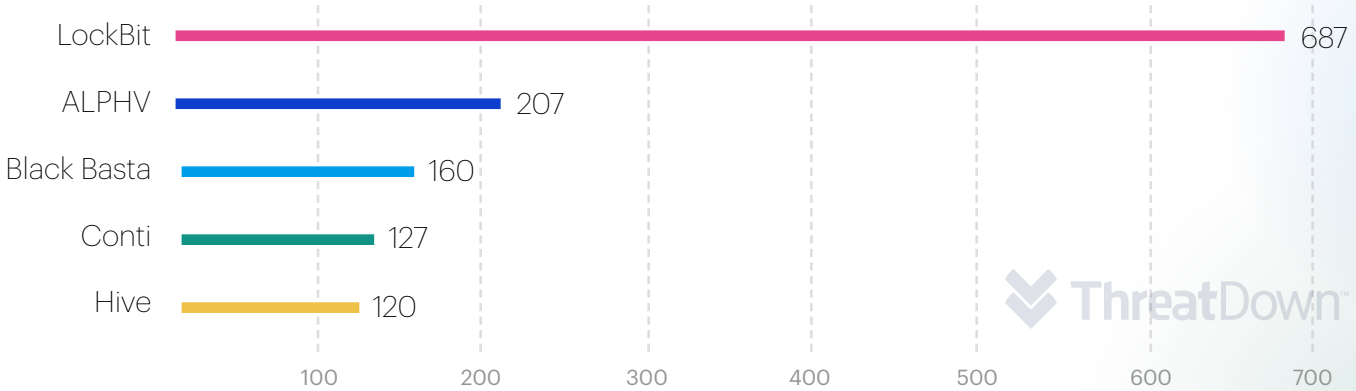
31%

Since April 2022, one in three known ransomware attacks has involved LockBit

$50M

The largest known LockBit ransom demand in 2022 was $50 million

Known attacks by top five RaaS groups in 2022*



* ThreatDown builds a picture of ransomware activity by monitoring the information published by ransomware gangs on the dark web. This information represents victims who were successfully attacked but opted not to pay a ransom.

Protecting your business from LockBit attacks

Minimizing the risks and impacts of LockBit and other RaaS attacks requires a coordinated, multi-layered approach.

Ransomware Phases	Protection
ACCESS RDP Brute Force Vulnerability Phishing	Brute Force Protection, Patch Management, and Malicious Website Protection target different forms of access.
INFILTRATION Attackers escalate privileges and move throughout the network, targeting backups and security software.	MDR can identify attackers as they operate inside your network, before they launch ransomware.
ENCRYPTION	EDR can detect ransomware, identify surreptitious encryption, and roll back affected files to an unencrypted state.

Recovery

Recovering from a ransomware attack means isolating the infected endpoints, eradicating the malware and its remnants from your network, and restoring encrypted systems from backups. The attacker's steps will need to be retraced, and their method of access closed.

3 EMOTET

Persistent, prolific, and difficult to eradicate

Our second threat archetype is Emotet, shapeshifting malware that is persistent, prolific, hard to detect, and hard to eradicate. Stop it and you will close the faucet on a potential torrent of other malware.

Emotet began life in 2014 as a banking trojan used to steal sensitive information. It now acts as a global-scale delivery network for malware, providing cybercriminal gangs with backdoor access to more than a million compromised computers.

The world's most dangerous malware

Described by Europol as the "world's most dangerous malware," Emotet is capable of evading traditional, signature-based detection, and it has proven enormously resilient to disruption by global law enforcement actions, even surviving a takedown of its entire global infrastructure in 2021.

What's important to know is that an Emotet infection is hardly ever just an Emotet infection. Over the last eight years, Emotet has been used to spread a laundry list of the most damaging cyberthreats, including: Ryuk and Conti ransomware, QakBot, TrickBot, and IcedID banking trojans.

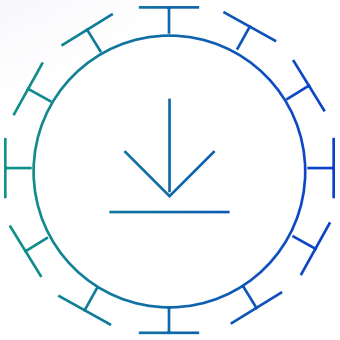
Easy to spread. Difficult (and expensive) to remove.

Emotet does not discriminate and will attack any target, no matter how big or small. It is delivered by email in the form of a malicious script, macro-enabled document, or malicious link. It can arrive out of the blue or insert itself into existing email conversations, posing as one of the correspondents.

Once it has infected a computer it uses a range of techniques to find and infect other targets. These include:

Stealing contacts from Outlook to create new spam emails.

Cracking the passwords of nearby network shares.



The software's modular architecture also allows it to be tailored to different tasks, and to update itself with new capabilities.

Because it infects and reinfects other machines so ferociously, removing Emotet from an organization can be an extremely complex and costly task. In the city of Allentown, Pennsylvania, a single errant click caused an outbreak that cost a reported $1 million to remediate. A similar incident in Frankfurt, Germany, triggered a temporary shutdown of all the city's computer systems.

$1M

According to CISA, Emotet infections "have cost state, local, tribal, and territorial governments up to $1 million per incident to remediate."

In early 2021, law enforcement agencies seized control of the Emotet botnet and used it to order Emotet infections to delete themselves. Its "death" only lasted seven months.

Protecting your business from Emotet attacks

Attack Flow	Protection
LURE Phishing, Malicious emails, or Spam	Email filtering can block some malicious emails.
INFECTION Malicious attachment downloads Emotet.	Malicious Website Protection can block downloads and EDR can block malicious scripts, exploits, and Emotet malware.
INSTRUCTION Emotet contacts command and control, joins the botnet and receives instructions.	Malicious Website Protection can block access to command and control.
OUTBREAK Emotet spreads itself inside and outside the network. It can now be used to steal data or deliver other malware.	MDR can detect suspicious network activity, EDR can block malware downloads.

Recovery

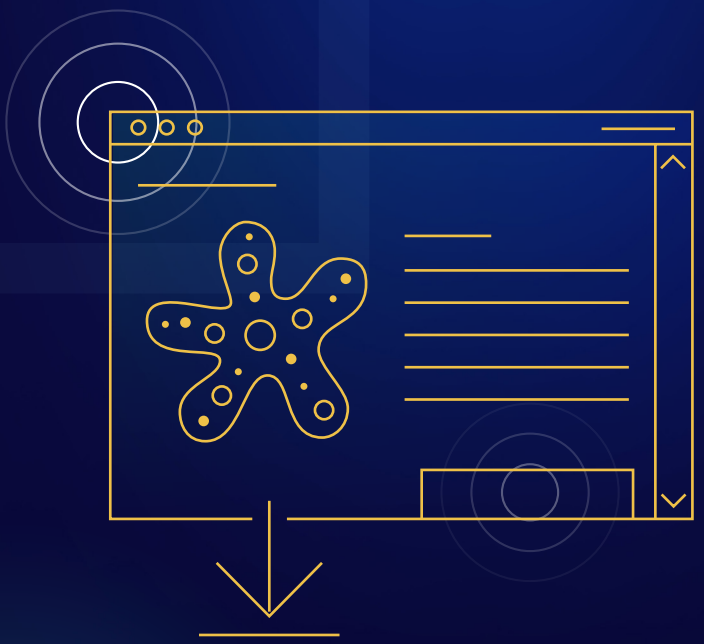
Remediating an Emotet outbreak can be a complex task. Due to the way Emotet spreads, any one infected machine can reinfect an entire network. Every affected machine should be isolated, cleaned thoroughly, and patched before re-joining your network.

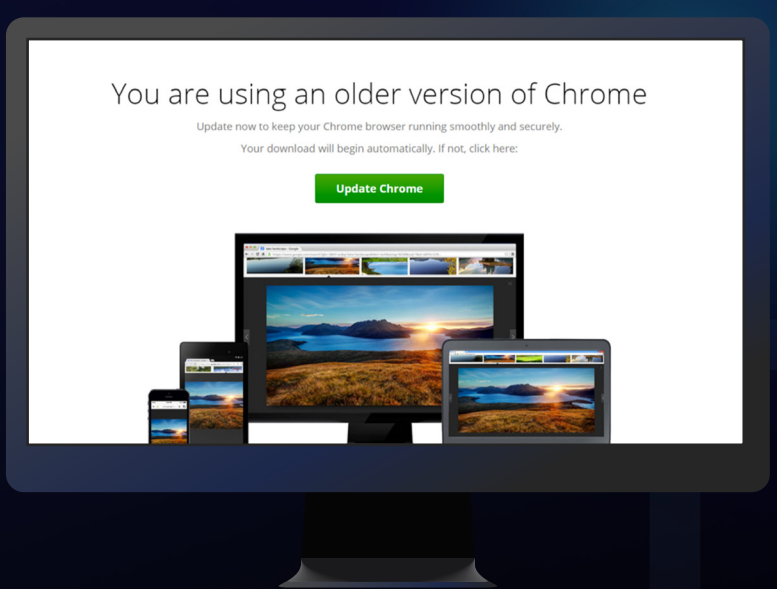
4 SOCGHOLISH

Corrupting users' security awareness

This malware archetype uses websites to spread, rather than attachments, software vulnerabilities, or brute force attacks. Stop it and you close off another important vector for delivering the most dangerous cyberattacks.

SocGholish, also known as FakeUpdates, comes disguised as a critical browser update. It is used to gain initial access into an organization's network. The foothold it creates is then sold to other criminals who use it to download Remote Access Trojans (RATs) or conduct ransomware attacks.





A pop-up window designed to look like an alert to update your Chrome browser.

Legitimate does not equal safe

Code that spreads SocGholish is injected into legitimate but vulnerable websites.

When users visit the affected sites, they are shown pop-up windows designed to look like alerts from their browser offering "critical browser updates." This simple social engineering trick turns victims' security awareness—and their desire to improve that security—against them.

> SocGholish is simple, but its use of social engineering and target fingerprinting is effective enough to have compromised high profile companies and even critical infrastructure. Its end goal is delivering ransomware, and it's a threat to treat with respect."
>
> Jerome Segura,
> Sr. Director,
> Threat Intelligence

Other than these bogus download offers, which are only shown to users who match the malware's targeting criteria, the websites continue to function normally, showing no obvious signs of infection. It's believed that hundreds of new websites are compromised like this every month.

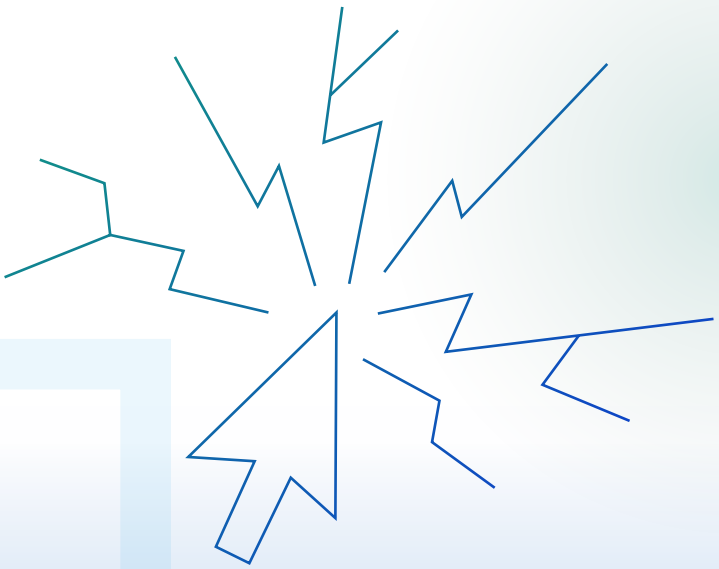
Users who fall into the trap and download the update get a ZIP file containing a small JavaScript program.

If the program is executed, it performs reconnaissance on the infected machine, which is used to determine if it's being run by a security researcher or a real victim, and what kind of network it's on.

These machinations are used to determine which payload the infected machine should download. If SocGholish determines it's running on a larger network, the payload is likely to be ransomware.

Smart, sneaky, and dangerous

SocGholish is known for the eligibility checks it performs at multiple points during infection. It attempts to ensure it is only triggered by legitimate targets, that it uses the most effective lure for that target, that it is not running in a malware analyst's testing environment, and that it downloads the form of malware most likely to make money from the victim.



Protecting your business from SocGholish attacks

Attack Flow

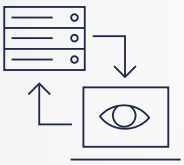
TRAP

Code for spreading SocGholish is injected into vulnerable websites.

LURE

Visitors are asked to download a bogus critical browser update.

RECONNAISSANCE



SocGholish gathers information about the system it's running on and communicates with command and control.

ATTACK

SocGholish downloads the most appropriate malware for the target.

Protection

Vulnerability and Patch Management can stop your own website from becoming a vector for SocGholish. Malicious Website Protection protects your users from infected sites.

EDR detects SocGholish. Malicious Website Protection can block access to command and control.

MDR can detect suspicious network activity, EDR can detect and mitigate malware downloads.

Recovery

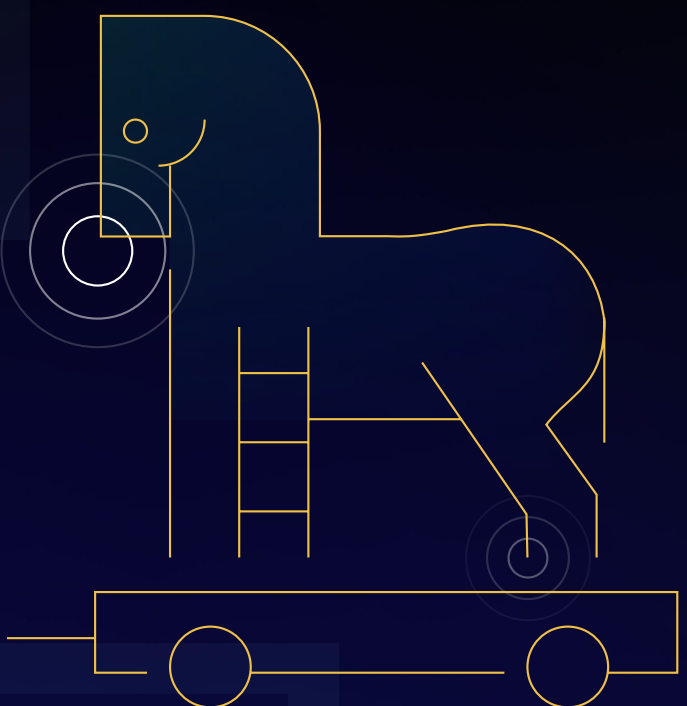
Although SocGholish is uncomplicated, it can be used to download other dangerous malware, such as ransomware. If it succeeds, the focus of the clean up effort can switch from an individual machine to an entire network.

5 ANDROID DROPPERS

The most 'Trojan' of Trojan Horses

Android droppers represent a category of malware that highlights the danger of overlooking protection for the world's most popular operating system. In the battle against malware, Android is the forgotten front line. 80 percent of people use personal smartphones for work, and 71 percent of smartphones run Android.

Android overtook Windows as the internet's most used operating system in 2017, and every type of malware that exists for Windows exists for Android, too. Because phones and desktops are used differently, different malware proliferates. For individuals, stalkerware is the most dangerous threat. For businesses, it's droppers.



Cleverly disguised dangers

Droppers are trojan horses that disguise themselves as innocent apps. They can be used to deliver:

Pernicious threats like HiddenAds that bombard users with aggressive ads.

Banking trojans like SharkBot, which can mimic touchscreen presses to perform bank transfers.

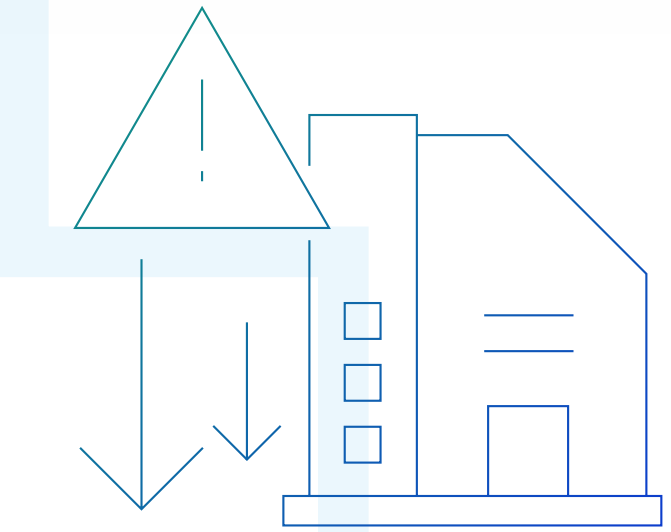
Spy malware that can harvest passwords, reveal your location, record audio, take pictures, and steal emails, contact lists, and browser histories.

Easy to pick up. Difficult to remove.

Droppers are often found on third-party app stores or websites, pretending to be free versions of popular apps. But droppers can sneak on to Google Play as well, posing as useful utilities like financial tracking apps, authenticators, document scanners, VPNs, or QR code readers.

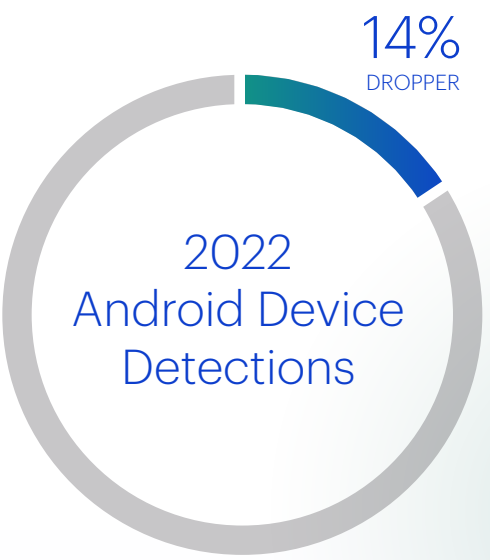
Then, after they infiltrate your organization, they can be extremely difficult to remove. Droppers can install copies of themselves, and because they can drop software that downloads other malware, they can be used to establish a permanent gateway into a smartphone, and then into a business.

Droppers are often found on third-party app stores or websites ... but droppers can sneak on to Google Play as well.



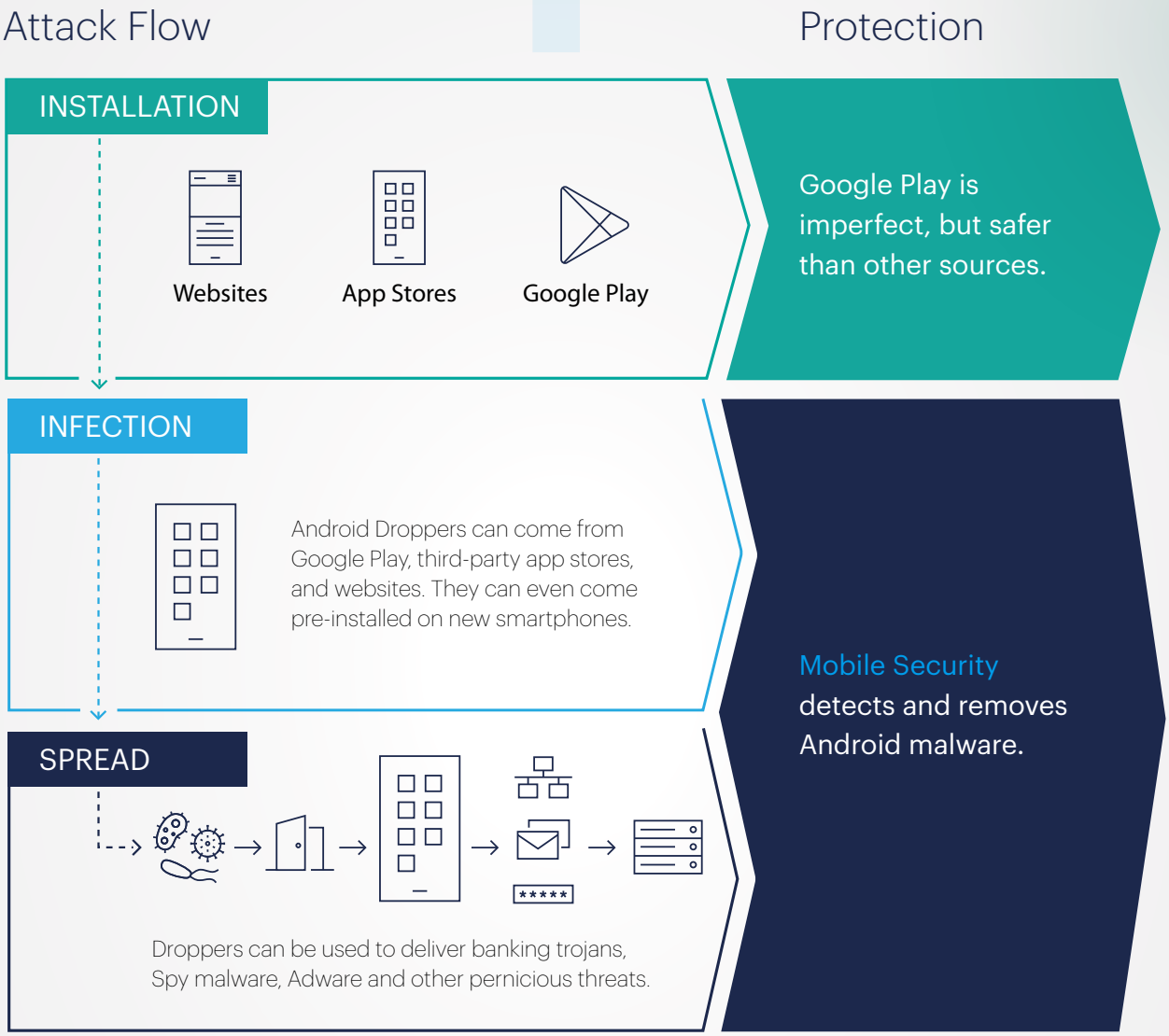
Less widespread, but more dangerous

In 2022, droppers accounted for 14 percent of detections on Android. Other malware is more widespread, but droppers pose the greatest danger to organizations.



Droppers account for 14% of all detections on Android devices.

Protecting your business against Android droppers

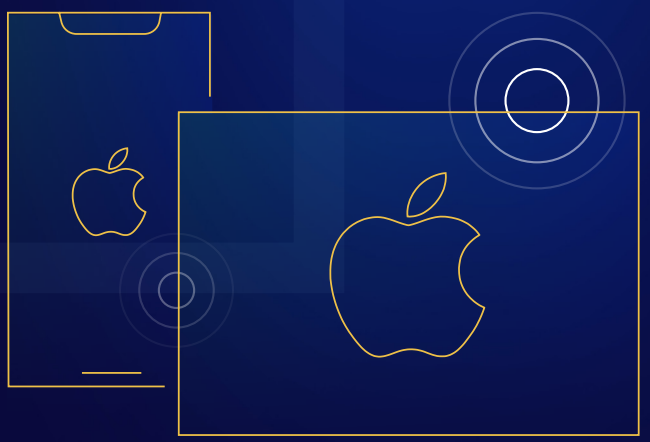


Recovery

Endpoint protection for Android can clean up most infections, but in extreme cases booting into safe mode, or even a factory reset, may be required.

6 OSX.GENIEO
The duplicitous Mac menace

Our last threat archetype shows the very different way that Macs are abused compared to Windows computers. About a quarter of businesses run Macs on their networks, and in the macOS threat landscape, deceptive, sophisticated, hard-to-remove adware is the most common type of threat. Understand OSX.Genieo and you're well placed to protect your Mac fleet.



Mac malware is rare but it does exist. In 2022, 11% of machines with detection events were affected by malware.

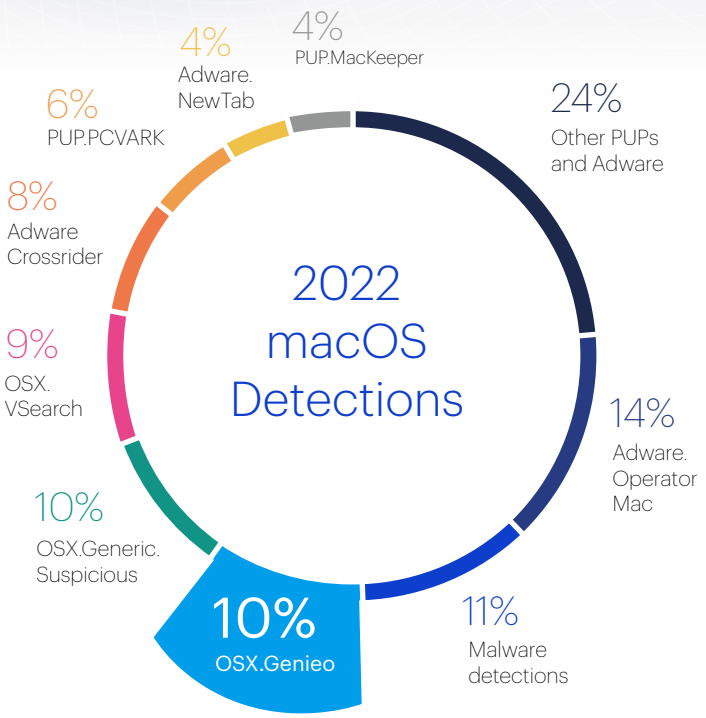
The darkest side of adware

Though classified as adware, Genieo has deployed an array of malware-like behaviors to dig further into the computers it's installed on, piercing defenses and compromising security in the name of making itself extremely difficult to remove. Its tricks have included injecting a dynamic library into all other processes, to monitor web browser activity; exploiting a system vulnerability to grant itself elevated permissions; manipulating users' keychains; and installing browser extensions without consent.

ThreatDown has spent a decade monitoring Genieo, tracking the techniques it uses to sink its claws into macOS, and dislodging every piece of it from stubborn infections.

In the Mac world, PUPs and adware are king

ThreatDown tracks tens of millions of detection events for Mac adware and potentially unwanted programs (PUPs) each year, but the worst is OSX.Genieo. It is both dangerous and abundant: In 2022, it was the second most common detection on Macs, appearing on 10 percent of all machines that triggered a detection event.



Making money with intrusive ads

Genieo is a browser hijacker that makes money by intercepting users' web searches and injecting its own intrusive ads into the results. Here's how it works:

Users get it unwittingly from software download sites, either bundled with other software or disguised as an app.

In the past, Genieo has posed as a Flash update and been bundled with video codecs. These days, it is more likely to come dressed as a PDF or video converter app.

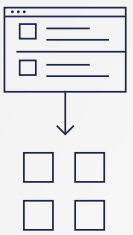
No matter what app Genieo disguises itself as, users get Genieo, and no sign of the app they thought they were getting, except perhaps a folder with its name and an empty file.

The Genieo software tries to evade detection by imitating system files, imitating files belonging to third-party software, and using a variety of techniques to obfuscate its code.

Protecting your business from Genieo attacks

Attack Flow

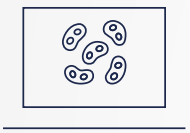
LURE



Genieo lurks on legitimate software download sites

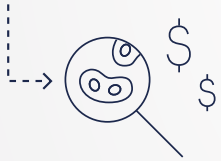
It comes deisguised as an app or bundled with other software.

INSTALLATION



Genieo uses a variety of techniques to hide itself and avoid detection and removal

SEARCH HIJACK

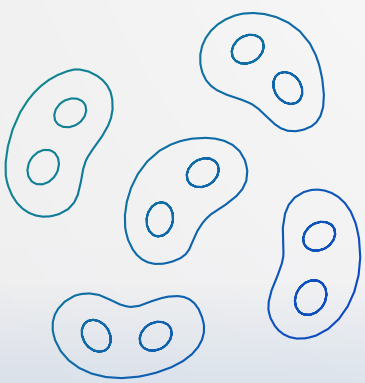


Genieo injects its own ads into search results.

Protection

Browser protection can block websites that distribute Genieo.

EDR detects and completely removes Genieo.



A decade of results

A browser hijacker may sound dull, but its creators don't care. Genieo exists—and has persisted for ten years—because it makes money, using your computers. The people behind Genieo are happy to deceive your employees and play fast and loose with your security to get their payday.

7 POST-MACRO MELEE

In 2022, cybercriminals began experimenting with alternative ways to deliver malware, in response to Microsoft blocking the execution of macros in documents downloaded from the Internet.

New twists on an old threat

Office macros are small computer programs that can be embedded in Microsoft Office documents. They have been a mainstay of malware delivery for almost three decades, surviving every attempt by cybersecurity experts to better inform users about the danger they pose.

In February 2022, the education campaigns got their biggest help yet, as Microsoft announced it would simply block macros in files downloaded from the Internet—which includes documents delivered as email attachments, the most common attack vector. The change began in April, but the rollout is phased and it will continue into early 2023.

DID YOU KNOW?

The beginning of an era: The first in-the-wild macro virus appeared in 1995. It was accidentally shipped on a CD-ROM by Microsoft.

Moving beyond macros

Though malicious macros have remained popular since Microsoft's announcement that it would block marcos in documents downloaded from the Internet, ThreatDown has observed cybercriminals trying several alternative techniques at malware delivery, in a likely attempt to prepare for a day when macros are less effective. These include:

- The use of malicious ISO, LNK, CHM and CAB files
- The Follina exploit (CVE-2022-30190)
- Equation Editor exploits

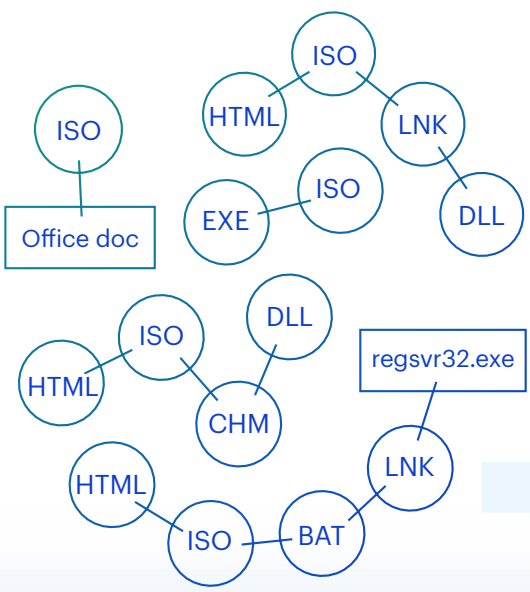
Macro alternatives in 2022

268%
Increase in LNK

365%
Increase in ISO

364%
Increase in CHM

195%
Increase in CAB



Misdirecting users and security software—and avoiding MOTW

ISO, LNK, CHM, and CAB files are used individually or in chains that are designed to misdirect users and security software, and to avoid Microsoft's Mark-of-the-Web (MOTW), a property Windows attaches to files downloaded from the Internet to indicate they came from an untrusted source.

Windows and other programs use the MOTW to trigger additional security features, such as Windows Defender SmartScreen, Microsoft Office Protected View, and macro blocking.

8 CONCLUSION

Protecting your business for the rest of 2023 requires one, critical understanding: The most dangerous cyberthreats you will face are not the strangest attacks you will see on any given week, or the most sophisticated, or the most eye-catching, they are not even the most prevalent. Instead, the most dangerous threats come from a set of known, mature tools and tactics that an entire ecosystem of cybercriminals rely upon to take in billions of dollars a year.

Criminals rely upon these attack types and their vectors because they work, and they work because they are hard to defend against and difficult to remove.

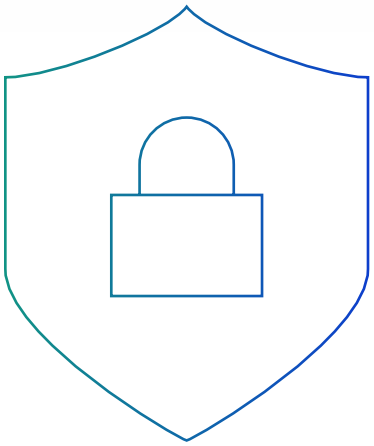
The most dangerous threats come from a set of known, mature tools and tactics that an entire ecosystem of cybercriminals rely upon.

The threats in this report are archetypes of the most dangerous malware on Windows, Mac, and Android. Like any successful software, they are actively developed and regularly updated, and their latest incarnations are set to be the most challenging threats you face in 2023.

Stopping them requires the same basic elements regardless of the size of your business: Layers of software protection overseen by skilled security staff with a range of specialist skills. Remediating these malware types to prevent reinfection means removing every trace and artifact created by them, and in the attack that delivered them.

Take the guesswork out of 2023

Whether your team is made up of security experts, or IT generalists, ThreatDown, powered by Malwarebytes, makes it easy to deploy proactive tools to prevent more threats, immediately detect and stop zero-day vulnerabilities, and thoroughly remove malware to restore business as usual.



Solutions for every step in the threat lifecycle

PREVENT

- Endpoint Protection
- Mobile Security
- DNS Filtering
- Cloud Storage Scanning

DETECT

- Endpoint Detection and Response
- Mobile Security
- Vulnerability Assessment

RESPOND

- Managed Detection and Response
- Patch Management

RECOVER

- Endpoint Detection and Response
- Managed Detection and Response
- Patch Management

SIMPLIFY

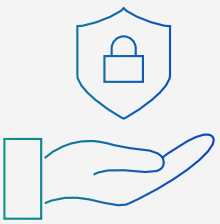
- ThreatDown Nebula

EDR

Famous around the world for catching the threats that others miss, ThreatDown Endpoint Detection and Response (EDR) provides complete protection with precise threat detection, proactive threat blocking, and thorough remediation, for both Windows and Mac.

MDR

Small and medium-sized businesses, without dedicated around-the-clock threat experts, experienced in combating the cybercriminals responsible for ransomware and other advanced attacks, can now add Malwarebytes' own experts to their staff with ThreatDown Managed Detection and Response (MDR). Our MDR service provides powerful and affordable threat detection and remediation services with 24x7 monitoring and investigation that's purpose-built for resource constrained IT teams.



We're here to help

Learn more about today's most serious malware trends and threats—and how ThreatDown, powered by Malwarebytes, can help keep your organization safe.

Request A Demo

ThreatDown™
Powered by Malwarebytes

Malwarebytes Inc.

3979 Freedom Circle, 12th Floor

Santa Clara, CA 95054

USA

+1-800-520-2796