ThreatDown™
Powered by Malwarebytes

2024 State of Malware

From malware to threats, a comprehensive defense guide

Contents

1. Why you need a guide

From malware to threats

Cybercrime is a thriving and highly organized business—a multi-billion-dollar mirror to the legitimate economy it feeds off. Its ecosystem supports entire supply chains which are dotted about with specialized organizations like access brokers and malicious software vendors. It has brand names, PR stunts, HR departments, incentive schemes, and "employees of the month."

And like broader, law-abiding "Business" at large, cybercrime has settled on a collection of tools that work. Sit at a regular desktop computer in the US or Europe and you'll see software that would have been familiar 15 years ago such as Microsoft Windows, Office, and a web browser.

Cybercrime has info stealers, phishing, and ransomware. Like Windows and Office, they are mature and effective, and for years the latest iterations have only offered marginal improvements on their predecessors. As a result, innovation in cybercrime has increasingly shifted towards tactics—advancements that focus more on how attacks can succeed and less on what malware can do.

Malware is as dangerous as ever, but when it is used, it is just one link in an attack chain of multiple different threats. IT and security teams now face "Living Off The Land" (LOTL) attacks, active adversaries, zero-day exploits, compromised accounts, social engineering, and a range of other threats that don't meet the traditional definition of malware.

Against this backdrop, security budgets are shrinking while resource-constrained IT and security teams firefight ever more complex environments. More of the same will not work in 2024. Handling the burden of 24/7 adversaries, a dearth of deep security resources, and the proliferation of poorly integrated point security products will require a different approach to security.

Effective cyberdefense will require skilled and experienced security professionals identifying and investigating anomalous activity whenever it occurs, day or night, backed by sophisticated, tightly bundled, and easy-to-use security software equipped to take down not just malware, but cyberthreats of every stripe.

About this report

To reflect the shift from malware to threats we have evolved our State of Malware report once again. We asked our experts what resource constrained IT teams should pay attention to in the year ahead. They have chosen six threats that illustrate some of the most serious cybercrime tactics we've seen on Windows, Mac, and Android. It is not an exhaustive list, but if you are equipped to handle these then you are well placed to deal with anything the cybercrime ecosystem can throw at you.

2. Lessons learned from 2023

Key developments

As we enter 2024, ransomware remains the most significant cyberthreat facing businesses. Awash with money, the ransomware ecosystem surged in 2023 and continued to evolve its tactics.

The number of known attacks increased 68%, average ransom demands climbed precipitously, and the largest ransom demand of the year was a staggering $80 million—requested by the LockBit gang following an attack on Royal Mail.

$80M

The largest known ransomware demand in 2023 was LockBit's $80 million demand of Royal Mail.

In an alarming break from established norms, the CL0P ransomware gang harnessed two zero-day vulnerabilities to conduct a pair of devastating, automated data theft campaigns that affected thousands of unsuspecting organizations in just a few days. CL0P's approach allowed it to significantly outperform even the most practiced Ransomware-as-a-Service groups, raising as much as $100 million in the process. Its tactics seem bound to be copied by others in 2024.

Less sophisticated gangs preyed on the continuing difficulty that some organizations have with effective patch management. In February, the largest known non-Windows ransomware attack ever compromised thousands of out-of-date VMWare ESXi servers using a two-year-old vulnerability. And in May, MalasLocker appeared out of nowhere to trump every other ransomware gang with a campaign targeting Zimbra servers that had gone unpatched for six months.

Cyberthreats evolved elsewhere too

Following Microsoft's decision to block macros in documents that are downloaded from the Internet, criminals diversified their tactics, most notably with a renewed interest in malicious advertising (malvertising). Countless campaigns appeared mimicking brands like Amazon, Zoom, and WebEx to deliver both Windows and Mac malware through highly convincing ads and websites, with the ad vendors seemingly powerless to stop them.

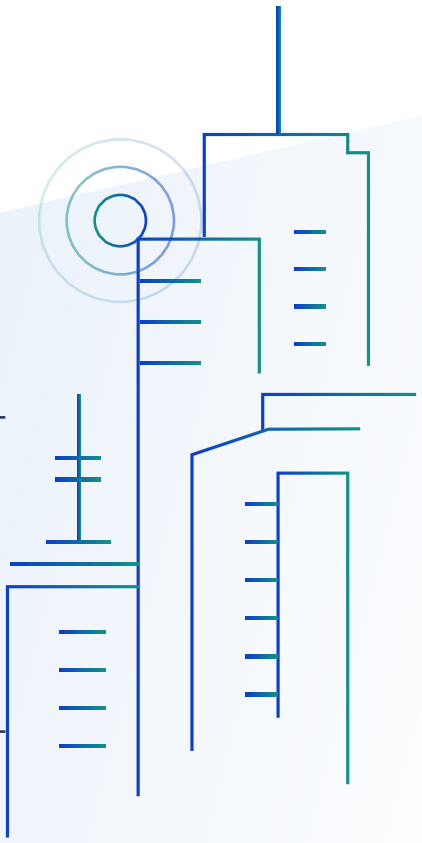
Criminals didn't have it all their own way, though. In August, the US Department of Justice announced the takedown of the notorious Qakbot malware, calling it "the largest US-led financial and technical disruption of a botnet infrastructure leveraged by cybercriminals to commit ransomware, financial fraud, and other cyber-enabled criminal activity."

2023 also saw a more tempered response to generative AI, as the breathless enthusiasm that greeted the launch of ChatGPT the previous year later gave way to a measured appreciation of the technology behind it. A year after ChatGPT's arrival, no significant security tools or cyberthreats based on it or other generative AIs have emerged. However, AI's potential to profoundly disrupt cybersecurity remains undimmed and its likely long-term impact unclear.

In a move that other countries will likely pay close attention to, the UK's Online Safety Act attempted to challenge the status quo for social media and messaging companies. The act was widely interpreted as a demand that companies scan users' messages for illegal material, which would require them to break end-to-end encryption (E2EE). In response, both WhatsApp and Signal threatened to leave the UK if the act passed into law. A political fudge saved everyone's blushes, but the controversial wording of the act was not changed, and its potential to be used as a challenge to encryption remains.

While encryption was under threat in some quarters, it was enabling significant improvements in security elsewhere. Google and Microsoft made good on their promise to back passkeys, an encryption-based alternative to passwords that can't be stolen, guessed, cracked, or phished. The companies have rolled out support for passkeys and are actively encouraging users to adopt them—an unqualified win for security, and something we're likely to see much more of in 2024.

The evolution of cyberthreats over the last year requires businesses to respond with a defensive evolution of their own. The following chapters explain what you need to know about the most consequential cyberthreats, and what advice, techniques, and technology you'll need to protect your business.



Ransomware remains the most significant criminal threat to businesses.

3. Big game ransomware

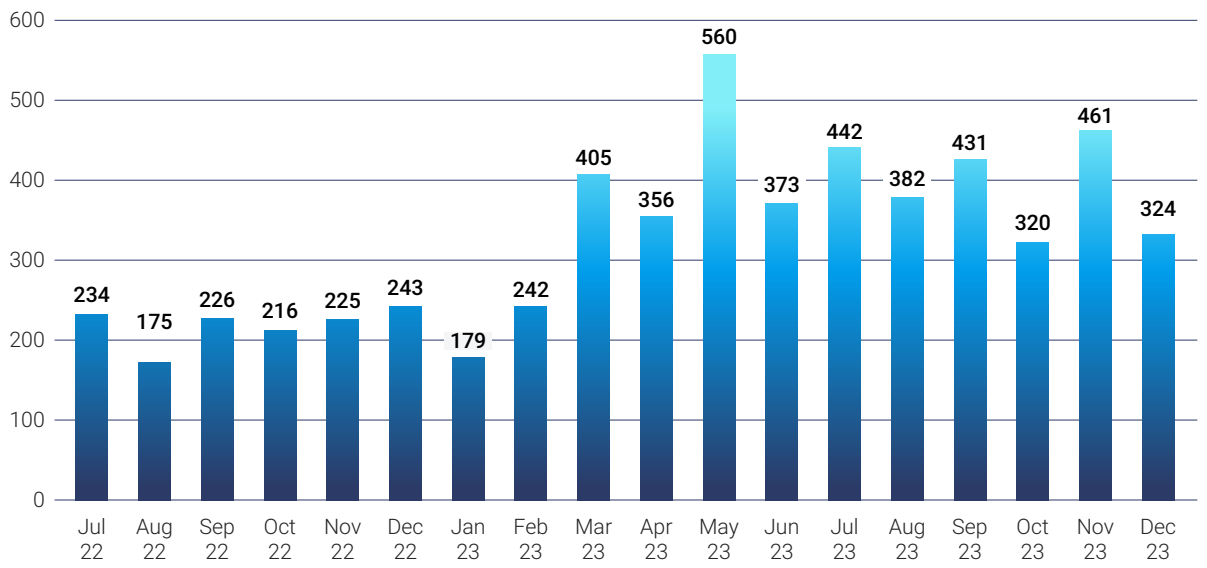
Since its emergence in 2018, "big game" ransomware has been the most serious cyberthreat to businesses all around the world. Big game attacks extort vast ransoms from organizations by holding their data hostage—either with encryption, the threat of damaging data leaks, or both.

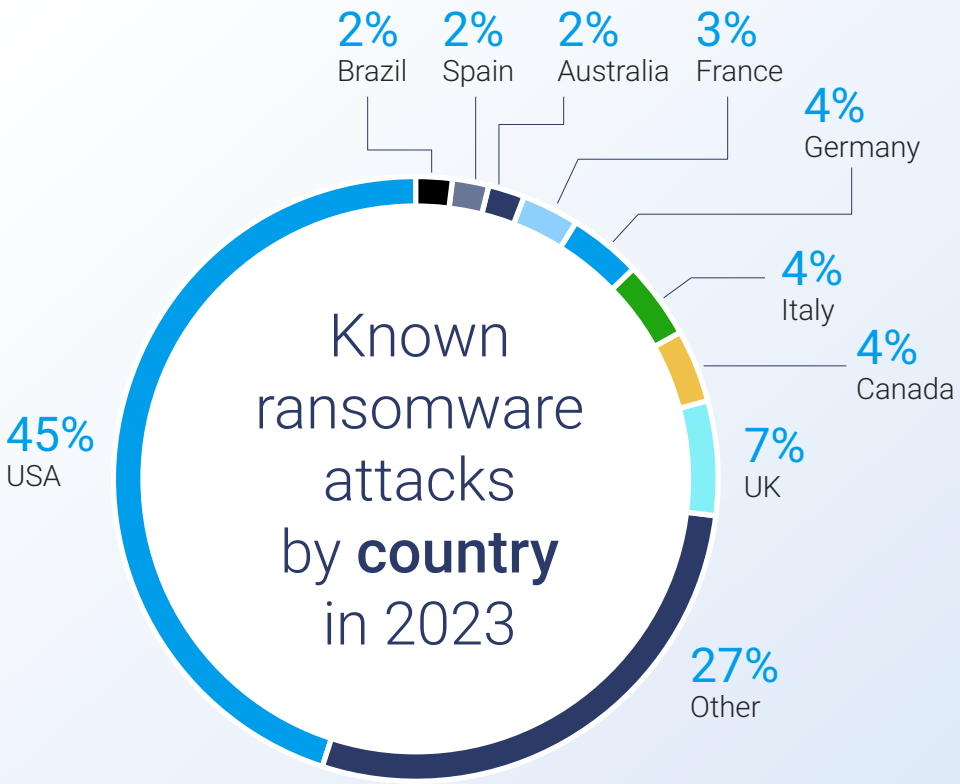
Sadly, the big game ransomware problem significantly worsened in 2023 with the number of known attacks increasing by 68%. The average ransom payment soared to $740,000 in the first quarter of the year according to Coveware, a ransomware incident response firm that also claims that total ransom payments in 2023 will approach a billion dollars.

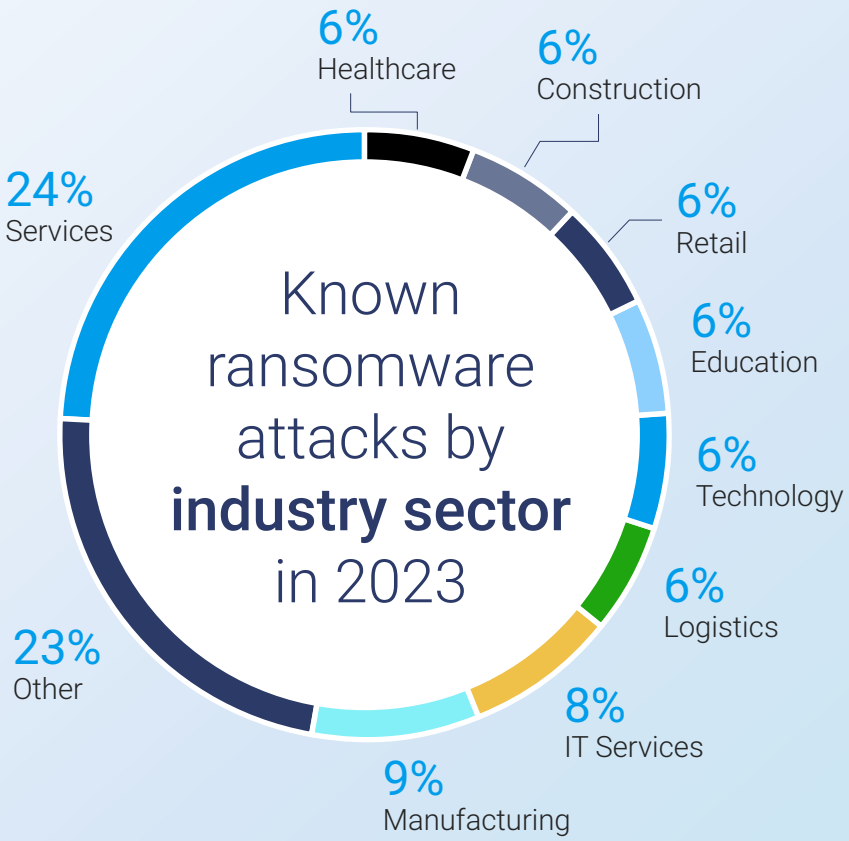
68% The number of known ransomware attacks increased 68% in 2023.

45% The US accounted for almost half of all ransomware attacks in 2023.

Known ransomware attacks by month




Known ransomware attacks by country in 2023
2% Brazil
2% Spain
2% Australia
3% France
4% Germany
4% Italy
4% Canada
7% UK
27% Other
45% USA


Known ransomware attacks by industry sector in 2023
6% Healthcare
6% Construction
6% Retail
6% Education
6% Technology
6% Logistics
8% IT Services
9% Manufacturing
23% Other
24% Services

Ransomware attacks can take weeks to prepare as criminal hackers breach a target, make themselves administrators, explore their environment, steal data, and then spread their ransomware to every corner of the network. When the attack is finally triggered it happens when the victim is least able to respond: Overnight, at the weekend, or during a holiday. Representatives from the target and the ransomware gang then negotiate in a dark web chat for days or even weeks.

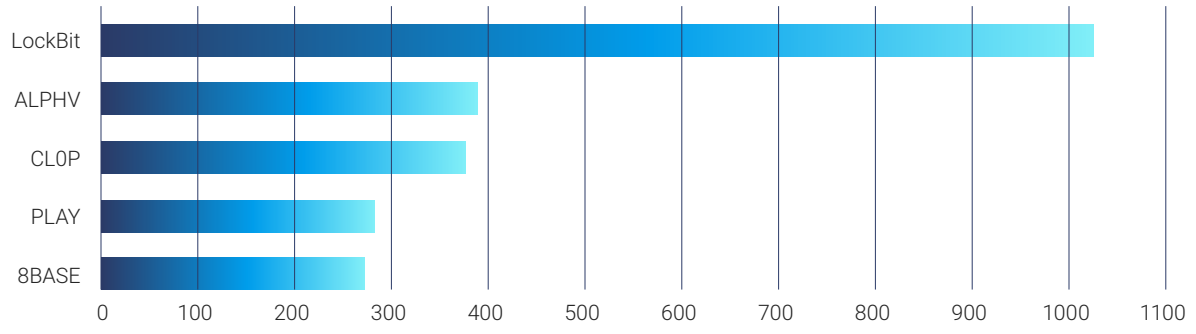
Big game attacks can be enormously lucrative, but they are labor intensive. The criminal underground's answer to big game ransomware's inherent scalability problem is Ransomware-as-a-Service (RaaS), a type of ransomware that often sees three different types of criminal organizations coordinating for a single attack.

First, criminal gangs that specialize in gaining a foothold inside company networks will breach a business. These malicious groups, called Initial Access Brokers (IABs), rely on a variety of tactics to break into companies, such as phishing, trojan horses, password spraying, and exploiting vulnerabilities in internet-facing infrastructure. Moving into the next phase of an attack, IABs then sell the access they gain to ransomware "affiliates."

Affiliates are criminal gangs that carry out ransomware attacks. Instead of writing their own ransomware, affiliates purchase it from a Ransomware-as-a-Service (RaaS) vendor like LockBit, ALPHV, or Play.

RaaS vendors sell everything you need to carry out a ransomware attack: The encrypting ransomware itself, access to a dark web leak site to hold and leak stolen data, and a means to negotiate with the victim. Affiliates pay for these services with a share of the ransoms they extort. Leaks from inside the Conti ransomware gang show that these groups can grow quite large, and have many of the trappings of a regular company. Conti had 60 employees, an HR department, performance reviews, and even an "employee of the month."

Top 5 "big game" ransomware groups in 2023

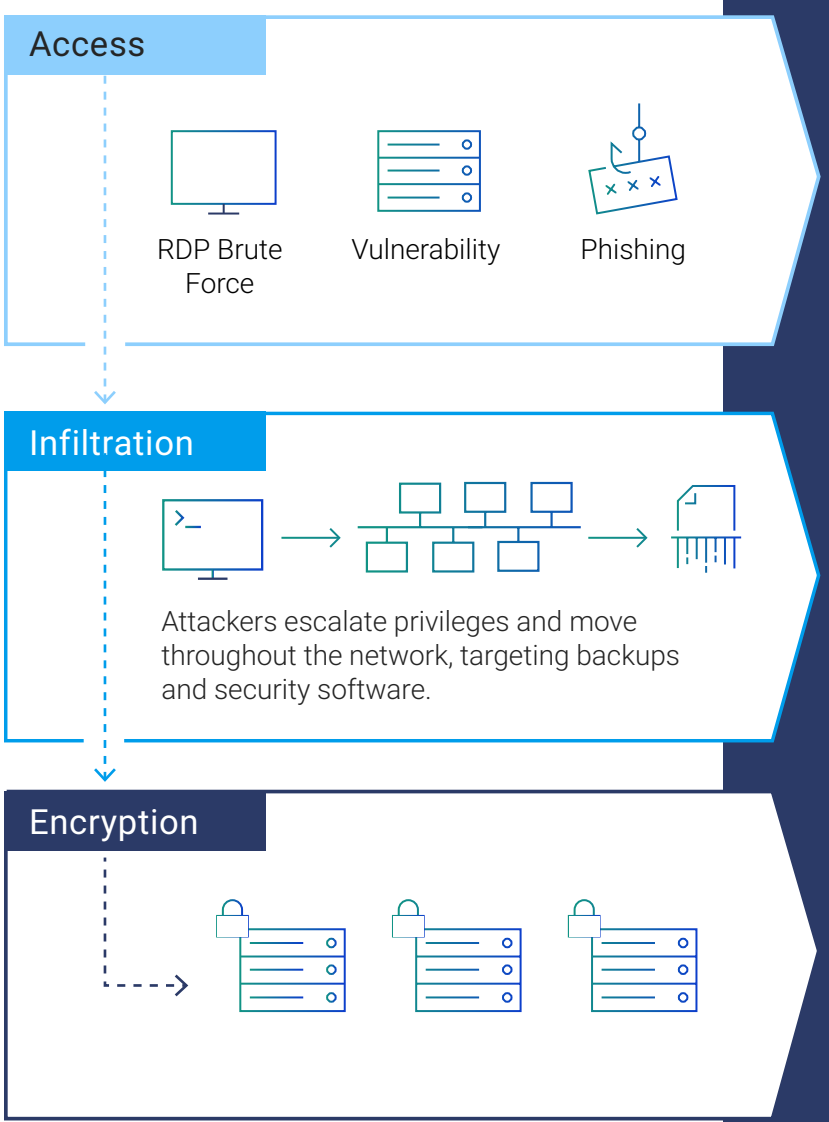


LockBit remains the most widely used RaaS, but its competitors are closing the gap.

The most widely used RaaS is LockBit, which accounted for more than twice as many attacks as its nearest competitor in 2023. However, while the total number of LockBit attacks increased year-on-year, its share of attacks decreased from 31% in 2022 to 23% in 2023, as its competitors closed the gap up—another worrying sign of ransomware's resurgence.

The big game ransomware threat is getting worse, and the gangs who do it are determined, experienced, and well resourced. Defending against big game ransomware requires an integrated approach to security that includes a best-in-class security stack allied with skilled threat hunters and incident responders.

Big game ransomware attack phases



Protection with ThreatDown

Brute Force Protection, Vulnerability Assessment, Patch Management, Anti-Exploit Protection and Website Content Filtering stop different forms of access.

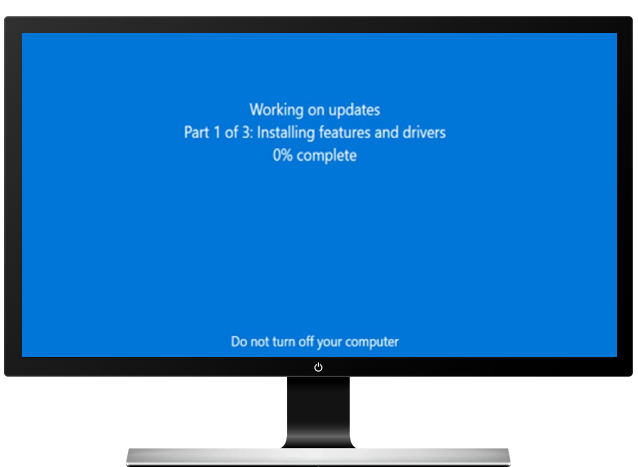
Managed Detection & Response (MDR) identifies attackers hidden inside your network before they launch ransomware; Next-gen AV, App Block, and Anti-Exploit Protection deny attackers access to their tools; Website Content Filtering blocks attackers' access to command-and-control servers.

Endpoint Detection & Response (EDR) stops ransomware; Ransomware Rollback recovers encrypted files; Incident Response gives you peace of mind after an attack.

4. Malvertising

The use of malicious advertising (malvertising) to spread malware isn't new, but in 2023 it underwent a resurgence that threatened both businesses and home users. The surge likely came because of a late (but needed) effort by Microsoft to block macros in documents downloaded from the Internet—one of cybercrime's most bankable malware delivery techniques. With this malware pathway now removed, cybercriminals innovated elsewhere.

Malvertising often uses social engineering techniques to install malware. Cybercriminals create Google Search ads mimicking popular brands, which lead to highly realistic, replica web pages where users are scammed or tricked into downloading malware.



A malvertising site masquerades as a Windows system update.

Although Google and other ad vendors battled with malvertisers all through 2023, the threat actors remained one step ahead, able to consistently bypass ad verification checks all year.

Malvertising that targets home users may mimic popular brands like Amazon, software utilities like PDF converters, or popular subjects such as cryptocurrency investments. Businesses are often targeted with ads for software downloads like Slack, Webex, Zoom, and 1Password. In 2023, criminals also targeted IT staff with fake versions of tools like Advanced IP Scanner.

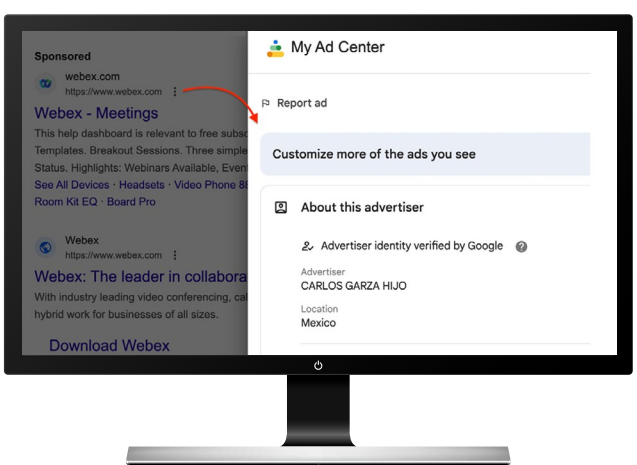
Amazon was the most impersonated brand in 2023.

The ads and the websites are highly realistic, and generally far harder to spot than malicious emails. Malvertising also uses sophisticated fingerprinting code that tries to determine if a visitor is a bot, such as the Google Search crawler, or a security researcher, ensuring that only potential victims see the fake pages—which allows them to go undetected for longer.

Top five most impersonated brands	
1	Amazon
2	Rufus
3	Weebly
4	NotePad++
5	TradingView

But while malicious pages are rapidly identified and taken down, they are easily replaced, and it is rare for the underlying infrastructure to be disrupted. With their malware delivery chain unaffected, malicious actors were free to focus on increasing the sophistication of their decoy pages and malware payloads in 2023.

Malware payloads vary with each campaign but infostealer malware such as IcedID, Aurora Stealer, and BatLoader is common. These programs steal credentials from users' browsers or computers, sowing the seeds for ransomware attacks.



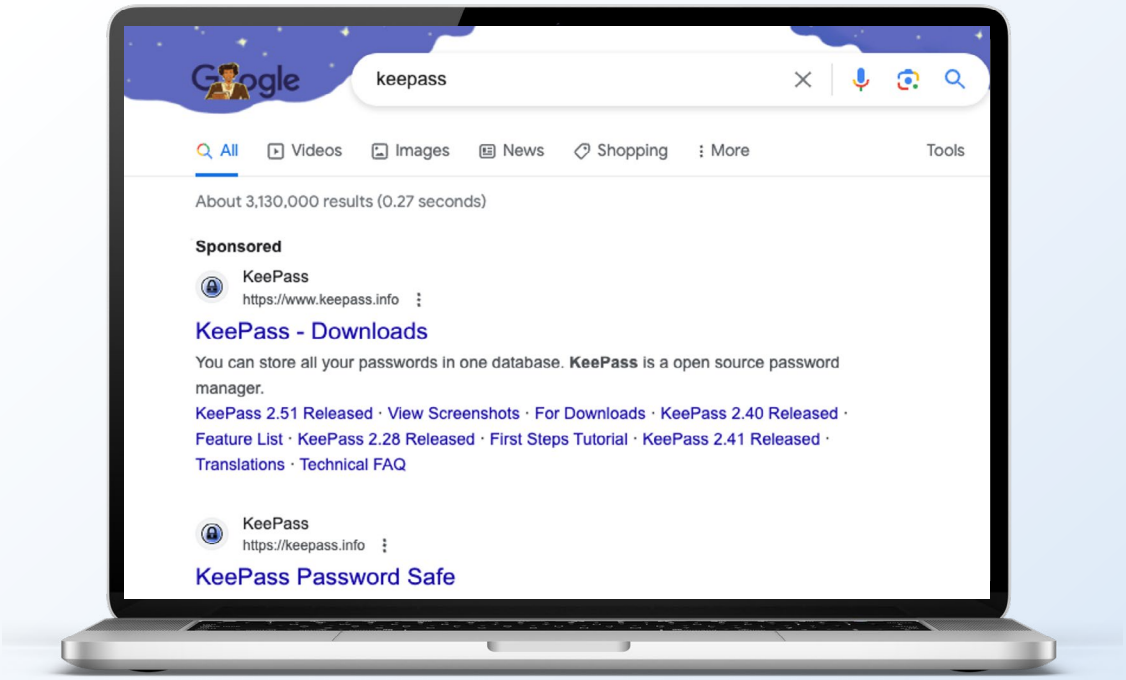
The only clue this Webex ad is fake lies in the information about the advertiser.

Top five most frequently discovered malware	
1	Aurora Stealer
2	Vidar
3	Redline Stealer
4	BatLoader
5	IcedID

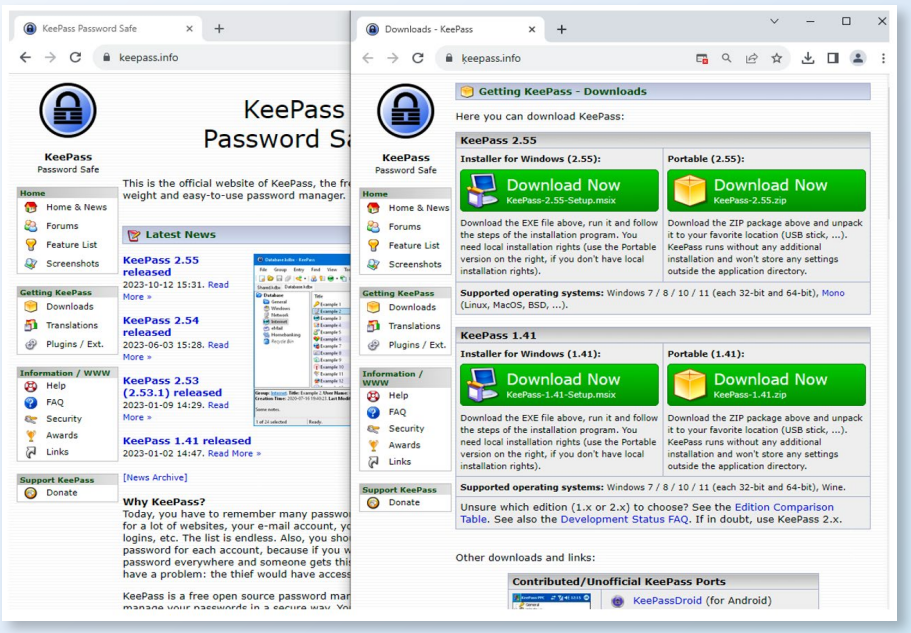
For example, the Royal ransomware group has used TeamViewer as a malvertising lure for BatLoader, which was used to drop a Cobalt Strike Beacon as a precursor to a ransomware attack.

For criminals, malvertising has several advantages over malicious email attachments. Users are much less aware of it and are rarely trained to spot it. And even if they are, the strictly controlled format of search ads gives users very little to scrutinize. Search ads can also be targeted at specific search terms, geographies, and demographics, ensuring that targets only see campaigns that are likely to appeal to them.

Top five most abused hosts	
1	Dropbox
2	Discord
3	4sync
4	GitLab
5	Google



A malicious ad for the KeePass password manager appears as a legitimate ad.



The real KeePass website (left) side-by-side with a malvertising site (right)

Malvertising is surging as criminals look for alternatives to macros for delivering malware like trojan horses, info stealers, and ransomware. Defending against malvertising requires effective website content filtering to stop the websites that distribute the malware, and a best-in-class security stack as a backstop to prevent attacks from escalating.

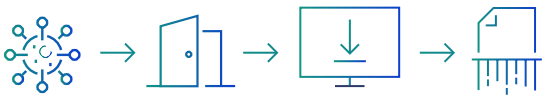
Malvertising attack phases

Malicious Ad

Malicious Website

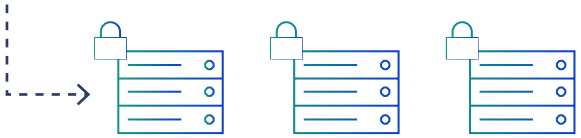
Malware disguised as legitimate software downloaded.

Malware



Malware steals data, downloads other malware, or creates access for a ransomware attack.

Ransomware



Protection with ThreatDown

Website Content Filtering blocks malvertising sites, Next-gen AV stops malware.

Managed Detection & Response (MDR) identifies and investigates suspicious behavior on your network; Website Content Filtering blocks attackers' access to command-and-control servers.

Endpoint Detection & Response (EDR) stops ransomware; Ransomware Rollback recovers encrypted files; Incident Response gives you peace of mind after an attack.

5. Zero-day ransomware

Big game ransomware is the most serious cyberthreat facing businesses today because of its destabilizing potential and devastating severity. Coupled with this existential threat, however, is a seemingly benign attack count that reveals big game ransomware's scaling problem. Limited because it is so reliant on human labor, attacks and negotiations can take weeks to conclude, and more attacks require more people. As a result, many potential targets are passed over.

But in 2023, the CL0P ransomware gang broke the scalability barrier and shook the security world with a series of short, automated campaigns, hitting hundreds of unsuspecting targets simultaneously with attacks based on zero-day exploits.

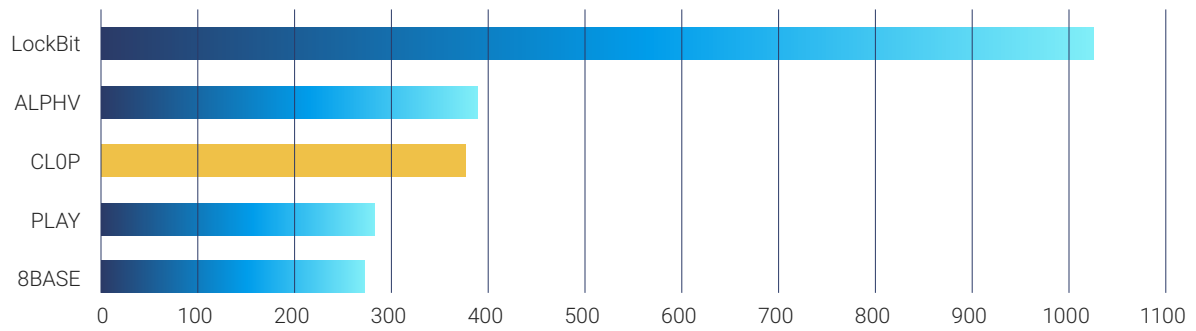
The repeated use of zero-days signaled a new level of sophistication for a ransomware gang, and within just a few weeks of activity, CL0P made itself the third most active "big game" ransomware of 2023, outstripping rivals that were active in every month of the year.

The use of zero-day vulnerabilities left organizations unable to protect themselves with security patches and traditional malware detection techniques.

Significantly, the attacks did not rely on encryption. In both campaigns, the CL0P gang stole victims' data and threatened to leak it if a ransom wasn't forthcoming—no ransomware deployment necessary.

Between January 18 – 31, CL0P launched an automated attack on businesses running Fortra's GoAnywhere MFT secure file transfer tool. The gang used a zero-day vulnerability

Top 5 ransomware groups in 2023 by known attacks



CL0P was the third most active gang despite being dormant for most of the year.

to create unauthorized accounts in victims' environments, which were used to steal files and install malicious tools. Details of 100 or so victims that didn't pay a ransom began appearing on the CL0P data leak site in March.

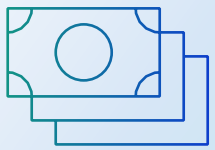
Not long after, the gang returned with an even bigger campaign based on a zero-day in Progress MOVEit Transfer software. The vulnerability was used to install a web shell, which in turn was used to steal files from the software's database.

Exploitation began on May 27, and Progress Software alerted its customers to the existence of the vulnerability on May 31. A week later, CL0P claimed responsibility for the attacks.

The smash and grab nature of the attacks meant the stolen data was not as carefully selected or sensitive as it might have been in a manual attack, leading to many victims refusing to pay a ransom. However, ransomware incident response firm Coveware believes the group managed to compensate by demanding much higher than average ransoms, earning itself as much as $100 million from this one campaign.

$100M

It's estimated that CL0P extorted between $75M – $100M with its MOVEit Transfer zero-day campaign.



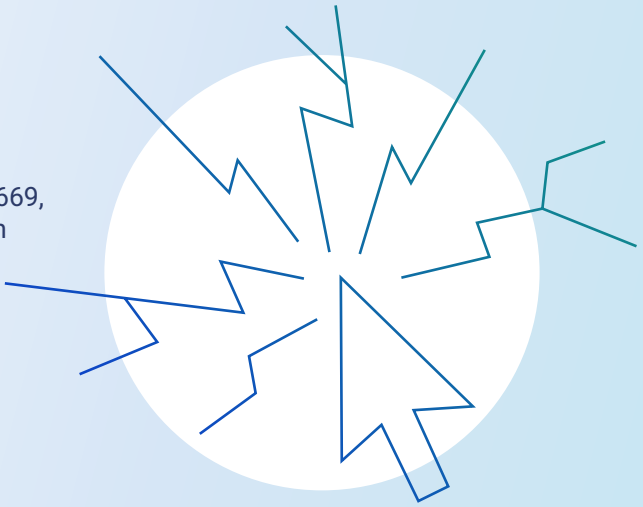
The result is that, going into 2024, CL0P has a fortune to reinvest in buying or discovering new zero-days, and it has shown that ransomware can scale beyond its established boundaries. It is hard to imagine that other ransomware groups won't try to replicate these tactics in 2024.

CVE-2023-0669

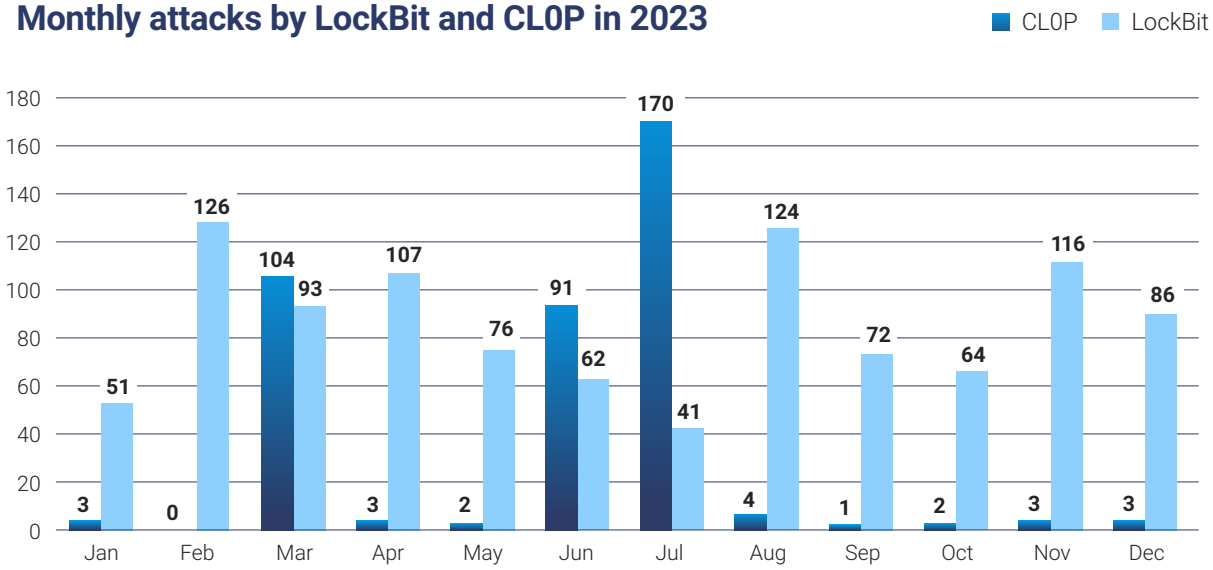
CL0P's first campaign exploited CVE-2023-0669, a previously unknown remote code execution vulnerability in GoAnywhere MFT.

CVE-2023-34362

CL0P's most successful campaign exploited CVE-2023-34362, a previously unknown SQL injection vulnerability in MOVEit Transfer.



Monthly attacks by LockBit and CL0P in 2023



LockBit was active in every month of the year, but CL0P became one of its main rivals with just a few weeks of attacks.

Statement on CL0P Website

CL0P hit so many companies it had to issue this statement on its website to streamline negotiations with hundreds of victims.

> WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE
>
> ***STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE***
> ***STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU***
> ***STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE***
> ***STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING***
> ***STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED***
> ***STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION***
> ***STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH***

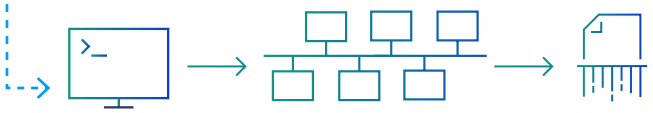
Zero-day ransomware is an emerging threat that poses a serious danger to your business. It relies on unknown vulnerabilities, making it difficult to detect. Defending against zero-day ransomware requires an integrated approach to security that includes a best-in-class security stack allied with skilled threat hunters who can find and investigate suspicious activity on your network.

Zero-day ransomware attack phases

Access

Zero-day vulnerability

Infiltration



Attackers deploy tools and steal data

Protection with ThreatDown

Vulnerability Assessment and Patch Management, ensure systems are protected quickly once a patch is available.

Managed Detection & Response (MDR) identifies and investigates suspicious behavior on your network; Website Content Filtering blocks attackers' access to command-and-control servers; Next-gen AV stops malicious backdoors.

6. Living Off The Land

Living Off The Land (LOTL) is a covert cyberattack technique in which criminals carry out malicious activities using legitimate IT administration tools like Powershell, PsExec, or Windows Management Instrumentation (WMI).

Because even the malicious use of these tools can resemble normal network activity to the untrained eye, LOTL attacks are extremely difficult for IT teams to detect.

Ransomware gangs like LockBit, ALPHV, and Royal use LOTL techniques to work unnoticed as they set up attacks inside corporate networks, elevating privileges, executing commands, downloading scripts, moving laterally, stealing data, and deploying ransomware.

For example, LockBit ransomware affiliates have used PowerShell to download malicious code from Google Sheets, and the Windows Task Scheduler to run malicious VBScripts. ALPHV affiliates have used the Windows Task Scheduler as well, to configure malicious Group Policy Objects (GPOs). The Royal ransomware group has used the Windows Volume Shadow Copy service to delete Windows snapshot backups and hinder recovery efforts.

The appeal of LOTL attacks spreads far within cybercrime. Data theft gangs and Advanced Persistent Threat (APT) groups may never run any malware at all and can use LOTL techniques to stay undetected for years, while cybercriminals of all kinds are happy to use remote access tools like RDP, AnyDesk, and TeamViewer because they provide enormous amounts of control without looking out of place.

To defend against LOTL attacks, IT and security teams need a detailed understanding of their environment so they can spot anomalies, such as unfamiliar administration tools (or familiar tools in unfamiliar hands), strange data usage patterns, or uncharacteristic working hours.

> "For effective detection of LOTL attacks, understanding the environment is paramount. Armed with this baseline, security analysts can identify anomalies or outliers which might not be inherently malicious but are uncommon for the environment."

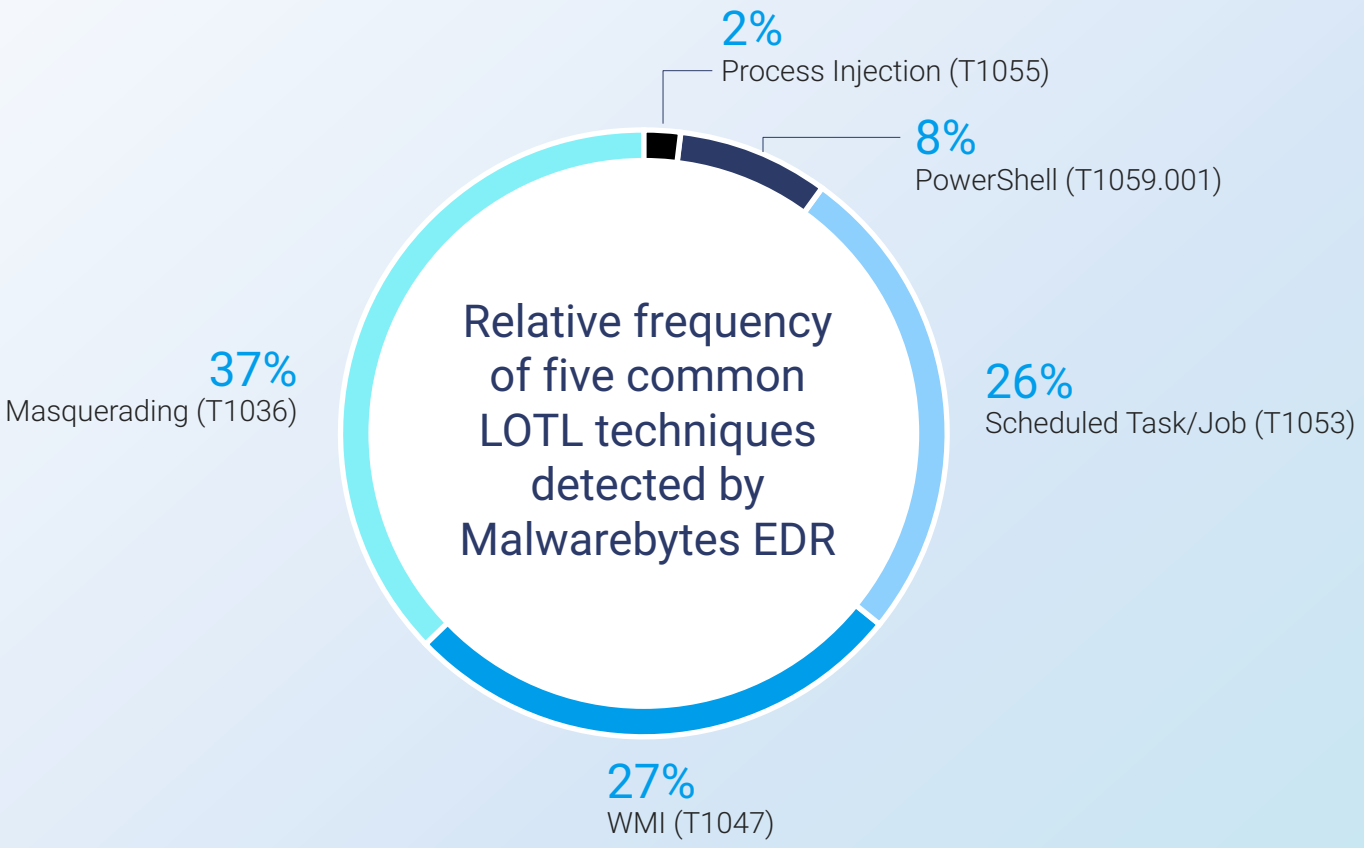
Hiep Hinh
Principal MDR Analyst, Malwarebytes

Defending against LOTL attacks

- **Use MDR** so that expert human analysts are monitoring your endpoints 24/7 for unusual patterns, signs of compromise, or connections.
- **Use threat intelligence feeds** to fine tune monitoring to spot the latest attack techniques and indicators of compromise.
- **Implement advanced monitoring tools** that focus on detecting unusual user or system behavior.
- **Limit access to commonly abused tools** to just the users who need them, monitor their usage, and use security policies to restrict potentially harmful actions.

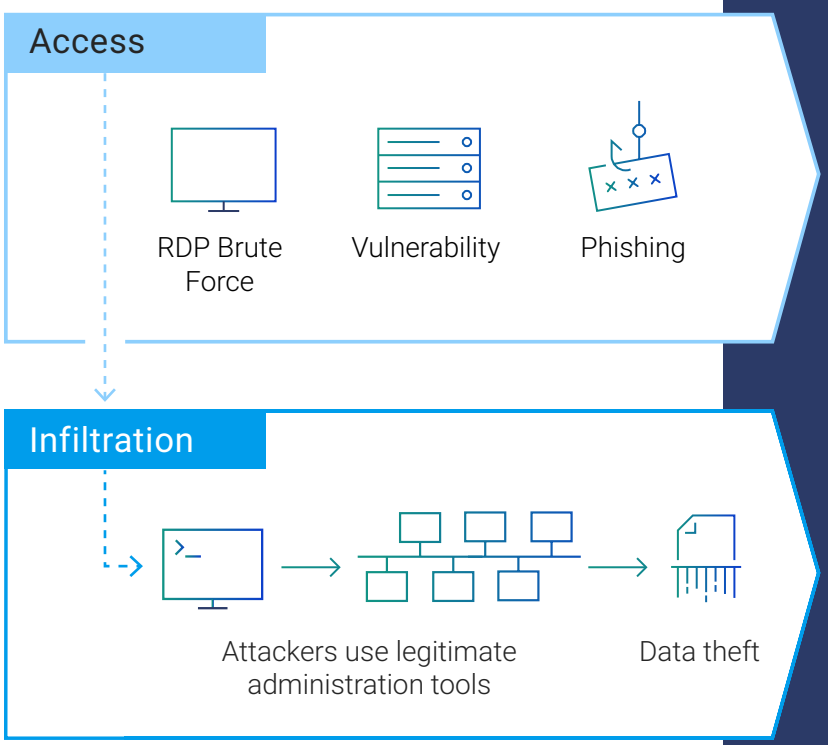
Attackers love remote desktop software. To make LOTL attacks more difficult, disable RDP and block any remote desktop tools your company does not normally use, such as Anydesk, Dameware Mini remote, TeamViewer, and Splashtop.

In one example of a LOTL attack stopped by the Malwarebytes MDR team, cybercriminals used a chain of legitimate tools in an attempt to avoid detection. They used wscript to execute a Windows Script File (WSF), which ran a PowerShell script, which downloaded malicious files that were finally executed via rundll32.



Cybercriminals who live off the land use legitimate IT administration tools instead of malware, making them extremely difficult to detect. Defending against Living Off The Land attacks relies on skilled threat hunters using best-in-class EDR to find and investigate suspicious activity on your network.

Living Off The Land attack phases



Protection with ThreatDown

Brute Force Protection, Vulnerability Assessment, Patch Management, Anti-Exploit Protection and Website Content Filtering stop different forms of access.

Managed Detection & Response (MDR) identifies and investigates suspicious behavior on your network; App Block denies attackers access to their tools; Website Content Filtering blocks attackers' access to command-and-control servers.

7. Android banking trojans

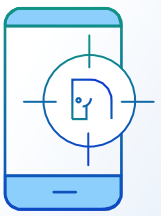
Banking trojans are one of the most serious threats facing Android devices. Sophisticated and stealthy, they combine clever technical and social engineering tactics to fool users and evade Google Play's protections so they can steal money straight out of your bank accounts.

Banking trojans come disguised as regular apps like QR code scanners, fitness trackers, or even copies of popular applications like Instagram. Once installed, the apps may test their environment to ensure they're on a genuine device and not in a researcher's lab. Tests can include looking for a SIM card, or making sure they're not running on a rooted device or in an emulator. If the banking trojan's conditions are met, it deploys a second, malicious app.

The malware may check if they are running on a rooted device or in an emulated environment, if there is a SIM card, and make other environmental checks in order to avoid reverse engineering. Or the malware may sleep for a while and then download malicious code with an update trying to avoid Google Play Protect's security checks.

72%

of smartphones run Android, and no operating system is more widely used, not even Windows.



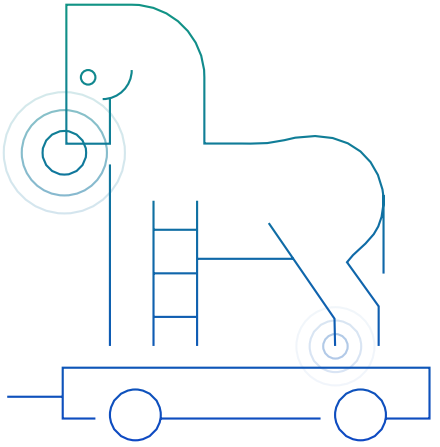
88,500

Malwarebytes detected Android banking trojans 88,500 times in 2023.

Some do this by downloading the app from an external server. To circumvent network-based detection systems, they may use a legitimate hosting platform such as Discord's Content Delivery Network (CDN).

Others trojans are "droppers" that already have the second app inside them. Third-party services like Zombinder use a sophisticated binding mechanism to hide a malicious payload inside a benign host application.

The malicious app is surreptitiously installed on the target device, typically hiding itself with a blank icon and a blank entry when a user tries to read through the app's info.

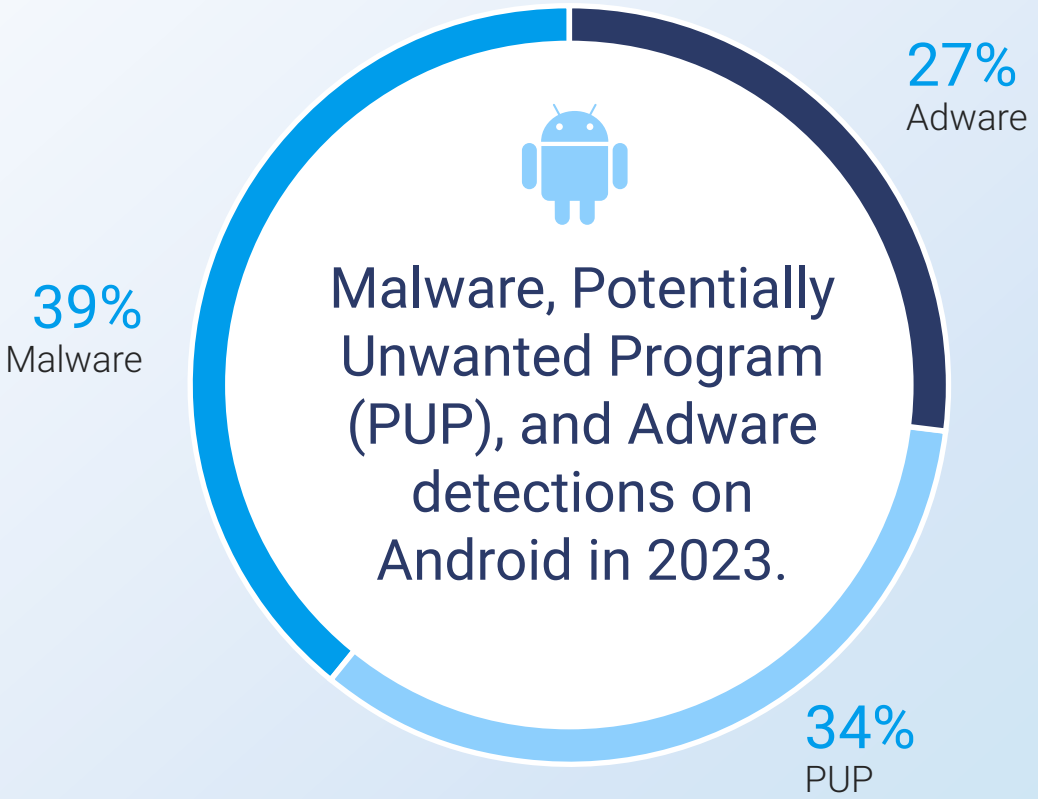


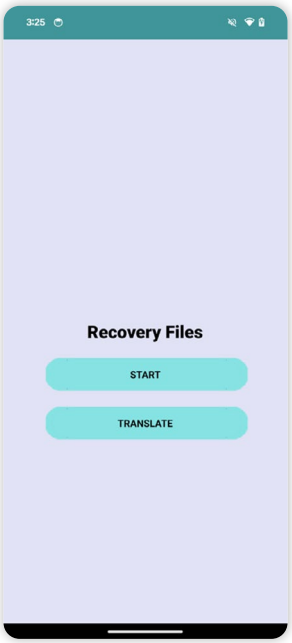
Once installed, the malicious app prompts the user to grant accessibility services under the guise of enhancing application functionality. This allows it to monitor other apps and overlay them with fraudulent interface layers. The overlays capture personally identifiable information (PII), such as passwords.

The app also implements a stealthy interception mechanism to capture Multi-Factor Authentication (MFA) tokens from SMS messages, without alerting the user.

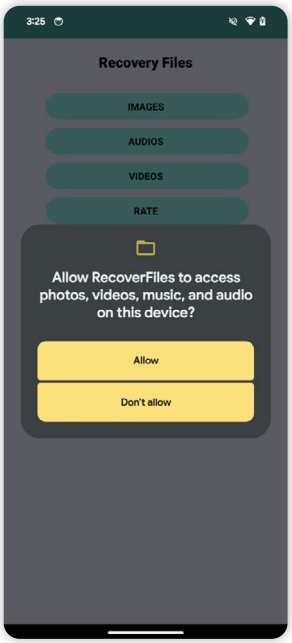
Once it has accessibility permissions, the malware initializes its Automated Transfer System (ATS) framework, a complex set of scripts and commands designed to perform automated banking transactions without user intervention.

The ATS framework uses the harvested credentials to initiate unauthorized money transfers to accounts held by the attacker. This mimics real user behavior to bypass fraud detection systems.



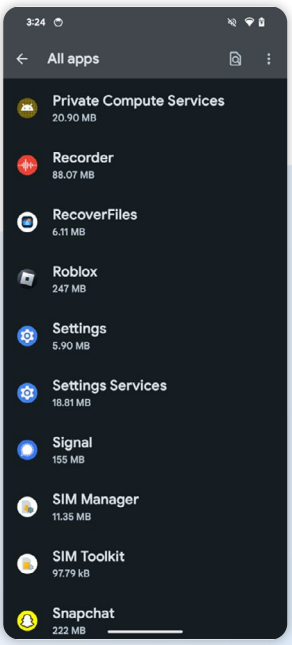


The startup screen of a banking trojan hidden inside a file recovery app.

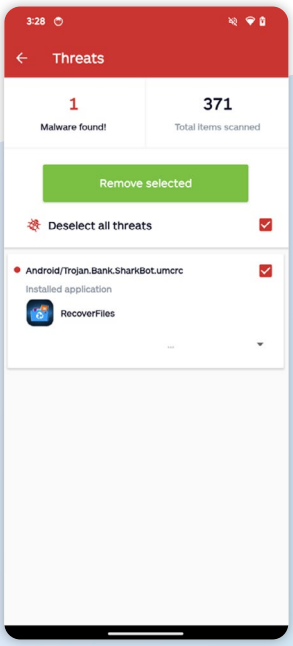


The app asks for permission to access files, to map and talk to other apps, and to send payments via Google Play.

It has no icon after installation.



However, the app can be seen in the app list.



Malwarebytes detects the app as the SharkBot banking trojan.

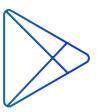
Banking Trojans are sophisticated and stealthy threats that come disguised as fully functioning regular apps. They copy your banking passwords and use them to quietly steal money straight from your accounts. Defending against Banking Trojans requires best-in-class mobile protection that can detect and remove malware from Android devices.

Banking trojan attack phases

Installation

App stores

Websites

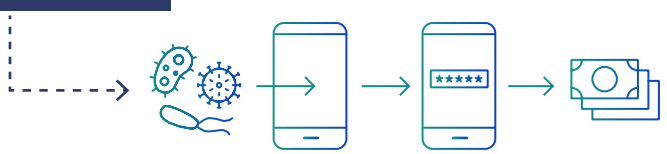


Google Play

Infection

Banking trojan comes hidden inside a regular app

Spread



Once installed it deploys a second, malicious app. The app steals banking passwords and makes fraudulent transactions.

Protection with ThreatDown

Mobile Security detects and removes banking trojans and other Android malware.

8. New Mac malware tactics

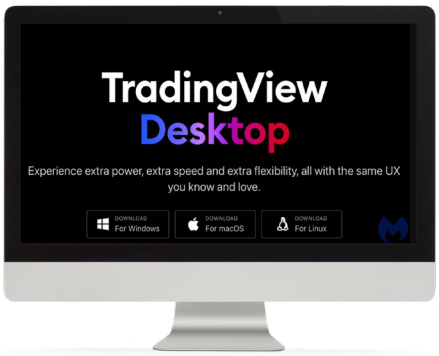
Contrary to outdated beliefs, malware has always existed for Macs. It's just that the type of detections that most frequently plague Macs are different. Instead of cybercriminals leaning most heavily on ransomware, bad actors generally favor aggressive, unwanted adware for making money on the platform. In 2023, Mac malware adopted a number of tactics that reminded us there is no intrinsic "Apple magic" that stops the malicious tools and tactics that work on Windows machines from working just as well on Macs.

Cybercrime follows the money, and Windows home computers—and networks of Windows business machines—have historically been a much bigger, more connected, and more lucrative target for cybercrime. However, there is every reason to think this is changing. Demand for Macs has grown despite declining PC sales, and Apple's macOS, in its many forms, now represents a 31% share of US desktop operating systems, while a quarter of businesses run Macs at least somewhere on their networks.

11%

Malware accounted for 11% of detections on Macs in 2023

There are signs that criminals are taking note, adapting to the platform's increasing popularity by including Mac options in their attack chains and enabling attacks to target both Windows and Mac users at the same time.



A malvertising site delivers malware downloads for Windows, Mac, and Linux.

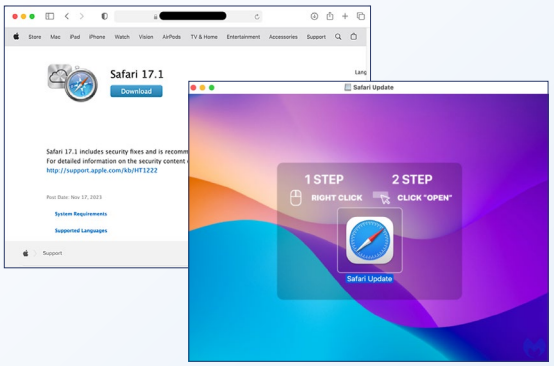
In September, Malwarebytes discovered a cybercriminal campaign spreading Atomic Stealer (AMOS) malware to Mac users through malicious ads purporting to sell the financial market tracking app TradingView.

The malicious ad directed victims to an authentic-looking, branded TradingView decoy site with separate download buttons for Windows, Mac, and Linux. Windows and Linux users got the NetSupport Remote Access Trojan, while Mac users got Atomic Stealer.

AMOS is an info stealer for Mac that can harvest passwords, browser data, cookies, files, and cryptocurrency. Cybercrime campaigns that utilize AMOS can control the info stealer via a web-based administration console that is sold "as-a-service" (similar to legitimate cloud applications) for $1,000 per month.

In November, the ClearFake fake browser update chain was also discovered distributing AMOS. ClearFake uses compromised websites to trick users into downloading malware disguised as a browser security update.

The campaign infrastructure determines what browser the victim is using to ensure they see an appropriately branded update. Fake browser updates typically target Windows users and the appearance of Safari-themed pages spreading malware for macOS is a new development.

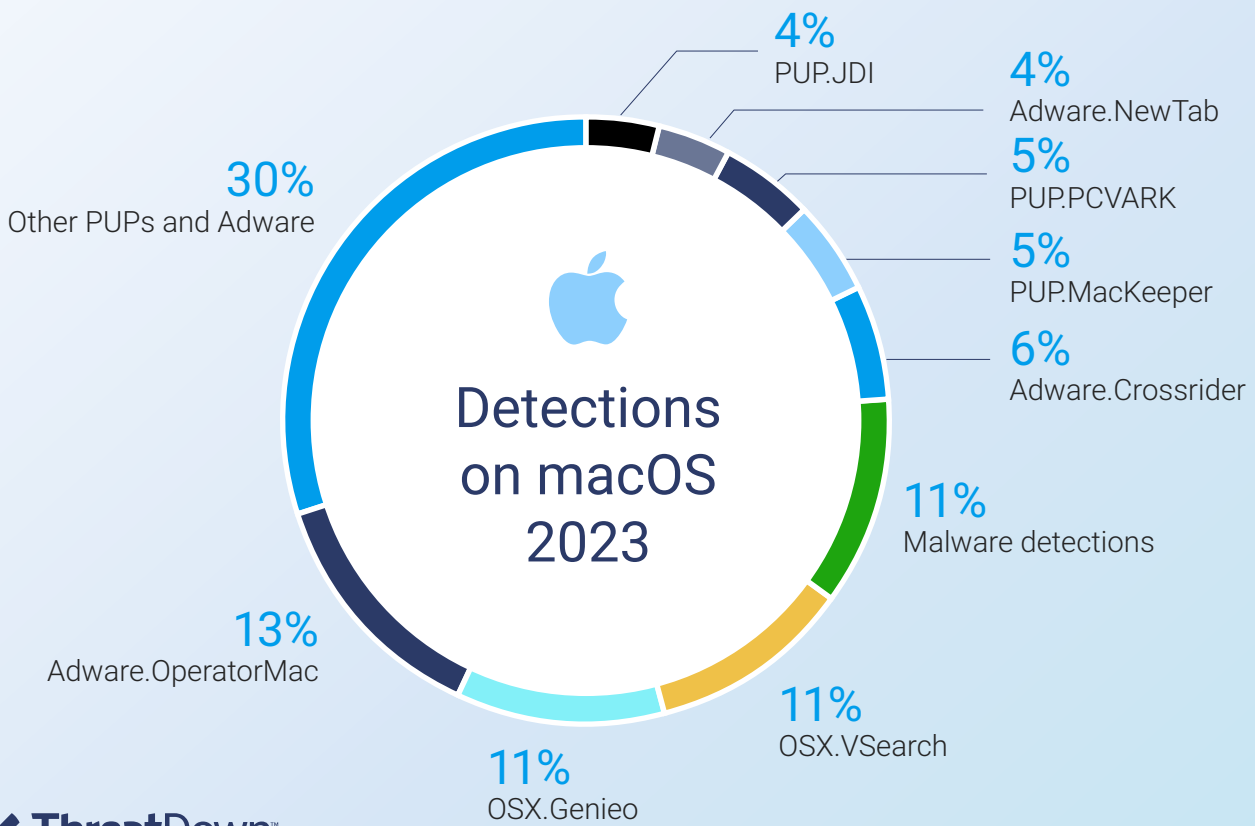


A fake Safari update mimics the official Apple website and is even available in different languages.

The incremental cost of adding a macOS option to an established Windows malware distribution chain is low. If Macs continue to buck the trend for declining PC sales in 2024, targeting the platform will become an increasingly easy choice for cybercriminal businesses to make.

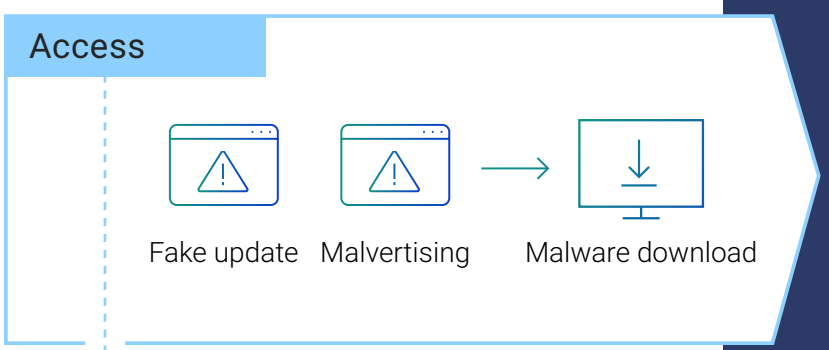
LOCKBIT 3.0

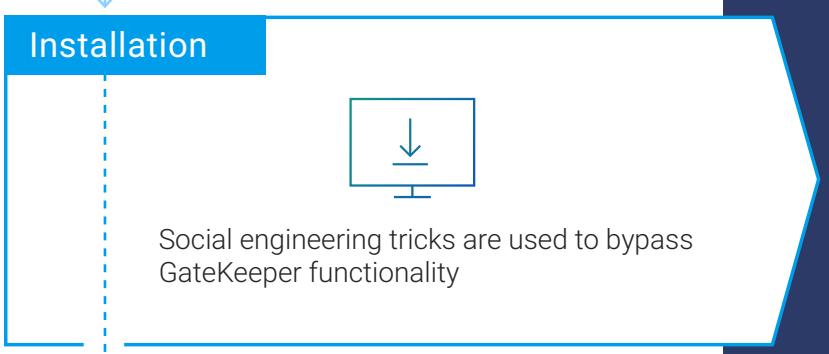
In April, researchers stumbled upon a Mac version of LockBit, the world's most dangerous ransomware. Although the tool was experimental, the LockBit ransomware group said its Mac ransomware was "actively being developed."

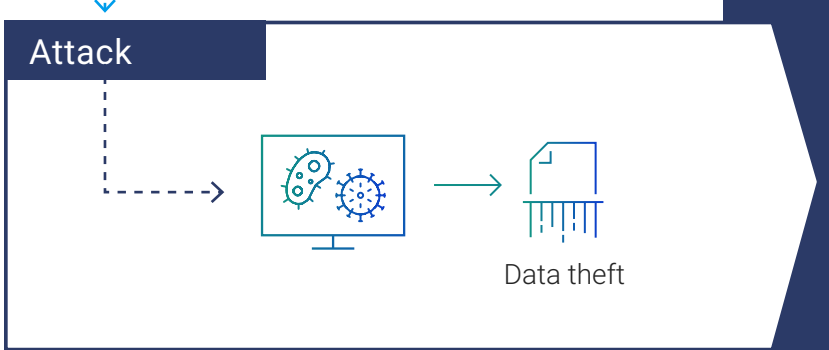


As Macs become more popular, cybercriminals are adding Mac options like Atomic Stealer to their malvertising and fake browser updates campaigns. Defending against Mac malware requires a Next-gen AV capable of detecting Mac malware.

Atomic Stealer attack phases







Protection with ThreatDown

Website Content Filtering can block sites used for malvertising and fake updates.

Next-gen AV can stop Mac malware.

9. How to prepare

Mark Twain said that history doesn't repeat itself, but it often rhymes. The persistent rhythm of cybersecurity, repeated over decades, is that threats often evolve from exploiting weakness in software to exploiting weaknesses in people.

But for just as many decades, cybersecurity has largely been addressed with efforts in the former. After all, technology and the processes that deliver it can be improved in a way that people cannot. With dedication and persistence, systems can slowly be made more secure—detection capabilities improved, attack surfaces reduced, testing expanded, and updates made more frequently, closing the window for technical exploitation.

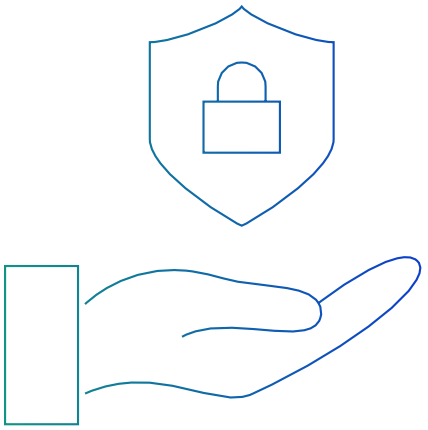
And yet, it is this exact rhythm of work that has spurred innovation in cybercrime.

Improvements in web browser security have seen the routine exploitation of browsers and plugins disappear in favor of social engineering attacks like fake updates and malvertising.

Ransomware turned into a billion-dollar industry by switching from automated email campaigns to manual "big game" attacks where criminal hackers pit themselves against IT and security staff more directly.

Improvements in backups and detection have seen an increasing number of ransomware gangs supplement their malicious encryption with threats to leak stolen data—a human predicament that no software can solve. It has also driven the adoption of Living Off The Land (LOTL) techniques that are hard for software to spot without human guidance.

This evolution has inevitably made people an increasingly vital component in the process of threat detection. No matter the size of your organization, in 2024 your success in pairing state of the art security software with skilled security staff will be a deciding factor in your ability to take down the most serious cyberthreats.



10. Introducing ThreatDown Bundles

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

ThreatDown Core

Core delivers comprehensive prevention against malware, zero-day threats, and more. **Core** includes award-winning technologies that appreciably simplify endpoint protection management

ThreatDown Advanced

Advanced delivers superior protection in a single, easy-to-use solution at a price that makes sense. Purpose-built for organizations with small security teams with limited resources, **Advanced** includes award-winning technologies that appreciably simplify endpoint protection management.

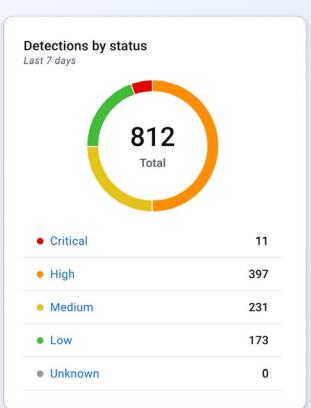
ThreatDown Elite

Elite delivers comprehensive protection in a single solution that offers unparalleled ease of use at a price that makes sense. Purpose-built for organizations with small (to non-existent) security teams that lack the resources to address all security alerts, **Elite** includes award-winning technologies and 24x7x365 expert-managed monitoring and response

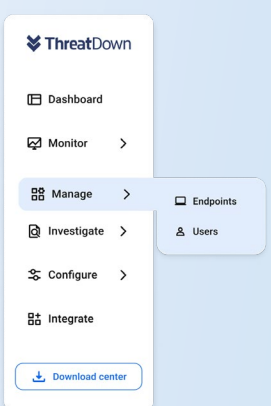
ThreatDown Ultimate

Ultimate delivers the most comprehensive protection across the attack cycle from superior attack surface reduction to fully-managed 24x7x365 prevention, detection, response, and full remediation.

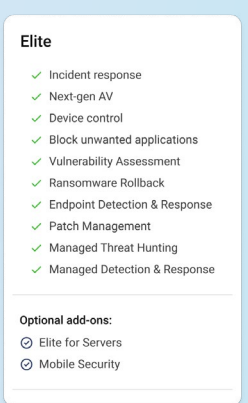
Take threats down.



Take complexity down.



Take costs down.



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

See the capabilities in each ThreatDown Bundle to address the six critical cyberthreats.

What you get	Core	Advanced	Elite	Ultimate
Incident response	✓	✓	✓	✓
Next-gen AV	✓	✓	✓	✓
Device control	✓	✓	✓	✓
Block unwarranted applications	✓	✓	✓	✓
Vulnerability Assessment	✓	✓	✓	✓
Ransomware Rollback		✓	✓	✓
Endpoint Detection & Response		✓	✓	✓
Patch Management		✓	✓	✓
Managed Threat Hunting		✓	✓	✓
Managed Detection & Response			✓	✓
Website Content Filtering				✓
Add-Ons	✓	✓	✓	✓

Try ThreatDown Bundles 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

3979 Freedom Circle, 12th Floor
Santa Clara, CA 95054 USA
+1-800-520-2796