



Malware Scanning

Threat Analysis Report



Malware Scanning  
Threat Analysis Report

August 11, 2023

Prepare by ISAN Security Gizmo Box, ISAN LAB





# Table of Contents

---

- Summary
- About Malware
- VirusTotal API





## Summary



## EXECUTIVE SUMMARY

SECURITY CHECKUP

The following Security Checkup report presents the findings of a security assessment conducted in your network.

The report uncovers where your organization is exposed to security threats, and offers recommendations to address these risks.

To assess risk, network traffic was inspected by Check Point to detect a variety of security threats, including: malware infections, usage of high risk web applications, intrusion attempts, loss of sensitive data, and more.

### Malware and Attacks

**287**  
computers infected  
with bots

 **4.6K**  
communications  
with C&C\* sites

\* C&C - Command and Control.  
If proxy is deployed, there might be additional infected computers.

**8** known malware  
downloaded by

 **10** users

**21** new malware  
downloaded


New malware variant is a zero-day attack or malicious code with no known anti-virus signature.

**14**  
unique software  
vulnerabilities were  
attempted to be exploited



Indicates potential attacks on computers on your network.

### Data Loss


 **114**  
potential data  
loss incidents

 **6**  
sensitive data  
categories

Indicated information sent outside the company or to unauthorized internal users. Information that might be sensitive.

### High Risk Web Access

 **18**  
high risk web  
applications

 **96.2GB**

Potential risks: opens a backdoor to your network, hides user activity, causes data leakage or malware infections.

 **22**  
high risk web  
sites

 **409** hits

Potential risks: Exposure to web-based threats and network infection. Examples: Spam, malicious, phishing web sites.

 **15**  
cloud  
applications

 **12.5GB**

Risk of data loss and compliance violations. Examples: Dropbox, Google Drive, OneDrive.



## About Malware





## How do I get malware?

Malware is usually distributed through malicious websites, emails, and software. Malware can also be hidden in other files, such as image or document files, or even in seemingly innocuous files, such as .exe files.

Users can unintentionally install malware when they click on a link in a phishing email, or when they download and install software from a website that is not reputable. Malware can also be installed on a computer when the user plugs in an infected USB drive, or when the user visits a website that is infected with malware.

## How malware can infect your PC


There are many different ways that malware can infect your PC. One common way is through infected files that you download from the Internet. Malicious code can be hidden in all kinds of files, including videos, pictures, and software. When you open these files on your PC, the malware can infect your system and cause damage.

Another common way that malware can infect your PC is through malicious websites. If you visit a website that is infected with malware, the malware can automatically download and install itself on your PC without your knowledge.

In addition, malware can also be spread through email attachments. If you open an email attachment that is infected with malware, the malware can install itself on your PC and cause damage.

## Is malware a virus?

No, malware is not a virus. Malware is a type of software that is designed to cause harm to a computer or its users. Viruses are a specific type of malware that can spread from one computer to another.





## How to detect malware?

Malware is software that is installed on a computer without the user's consent and that performs malicious actions, such as stealing passwords or money. There are many ways to detect malware, but the most common is to scan the computer for malicious files or programs.

Malware can be installed in a variety of ways, including through email attachments, drive-by downloads, or by clicking on links in malicious websites. It can also be installed through vulnerabilities in software that the user has installed on their computer.

## How to remove malware

" There is no one-size-fits-all answer to this question, as the best way to remove malware may vary depending on the specific malware that is installed on your computer. However, some common methods for removing malware include using an antivirus program to scan your computer for malware and then delete any malware that is found, using a malware removal program to scan your computer for malware and then delete any malware that is found, or manually deleting any malware that is found on your computer.







## Types of malwares?

Unfortunately, there is a lot of malwares out there, but understanding the different types of malwares is one way to help protect your data and devices:

### **Viruses**

A virus usually comes as an attachment in an email that holds a virus payload, or the part of the malware that performs the malicious action. Once the victim opens the file, the device is infected.

### **Ransomware**


One of the most profitable, and therefore one of the most popular, types of malwares amongst cybercriminals is ransomware. This malware installs itself onto a victim's machine, encrypts their files, and then turns around and demands a ransom (usually in Bitcoin) to return that data to the user.

### **Scareware**

Cybercriminals scare us into thinking that our computers or smartphones have become infected to convince victims to purchase a fake application. In a typical scareware scam, you might see an alarming message while browsing the Web that says "Warning: Your computer is infected!" or "You have a virus!" Cybercriminals use these programs and unethical advertising practices to frighten users into purchasing rogue applications.

### **Worms**

Worms have the ability to copy themselves from machine to machine, usually by exploiting some sort of security weakness in a software or operating system and don't require user interaction to function.





## **Spyware**

Spyware is a program installed on your computer, usually without your explicit knowledge, that captures and transmits personal information or Internet browsing habits and details to its user. Spyware enables its users to monitor all forms of communications on the targeted device. Spyware is often used by law enforcement, government agencies and information security organizations to test and monitor communications in a sensitive environment or in an investigation. But spyware is also available to consumers, allowing purchasers to spy on their spouse, children and employees.

## **Trojans**

Trojans masquerade as harmless applications, tricking users into downloading and using them. Once up and running, they then can steal personal data, crash a device, spy on activities or even launch an attack.

## **Adware**

Adware programs push unwanted advertisements at users and typically display blinking advertisements or pop-up windows when you perform a certain action. Adware programs are often installed in exchange for another service, such as the right to use a program without paying for it.

## **Fileless malware**

Fileless malware is a type of malicious software that uses legitimate programs to infect a computer. Fileless malware registry attacks leave no malware files to scan and no malicious processes to detect. It does not rely on files and leaves no footprint, making it challenging to detect and remove.

Ref: <https://www.mcafee.com/en-us/antivirus/malware.html>





VirusTotal API





## VirusTotal API

The Virustotal API is a service that allows you to check files and URLs for infections by viruses, malware, or various types of malicious software automatically. Here's an explanation of how it works and how to check both URLs and files using the Virustotal API:

### How Virustotal API Works:


1.Registration and API Key Acquisition: To get started with the Virustotal API, you need to register for their service and obtain an API Key from their system. This key will be used in making API requests.

2.Sending API Requests: You can send API commands to Virustotal using HTTP requests such as GET or POST. You can send URLs or files for scanning. For URLs, you can use an API endpoint like <https://www.virustotal.com/vtapi/v2/url/report>, and for files, you can use an API endpoint like <https://www.virustotal.com/vtapi/v2/file/scan>.

### Checking URLs with the Virustotal API:

1.Send the URL to Virustotal: Send the URL you want to check to Virustotal using the API endpoint <https://www.virustotal.com/vtapi/v2/url/report>.

2.Wait for Results: Virustotal will check the URL you submitted and search for information about infections or risks from various antivirus sources. The returned results will include information such as the URL's status and scan results from different sources.





## Checking Files with the Virustotal API:

1.Upload the File: Send the file you want to check to Virustotal using the API endpoint <https://www.virustotal.com/vtapi/v2/file/scan>. The file will be sent to Virustotal for scanning.

2.Wait for Results: Virustotal will scan your file using multiple antivirus programs and malware engines. The returned results will show the scan results and any associated risks (if any) related to that file.

Using the Virustotal API is a valuable tool for checking the risk of URLs or files before downloading or running them on your system to protect against potential threats from viruses or malware that could harm your computer or data.



