

MALWARE AND RANSOMWARE ATTACKS

AARUSHI CHOPRA
ASSOCIATE AT SETH ASSOCIATES



STATISTICS



- A ransomware attack occurs every 2 secs.
- Every day 1.7 million, and every second 19 ransomware attacks occur.
- The average cost of a ransomware attack was \$1.85 million in 2022.
- The first half of 2022 saw nearly 236.7 million ransomware attacks worldwide.
- There is 51% increase in ransomware incidents reported in 2022 compared to 2021.

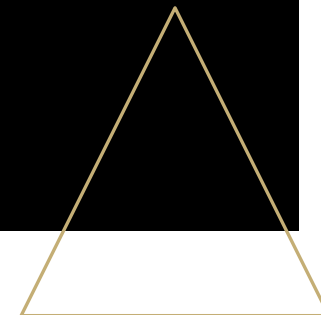


MALWARE ATTACKS



What is a malware?

- Malware is one of the most common cyber threats.
- It is an umbrella term for any type of malicious software designed to **steal data and or destroy data on a computer or network.** .
- It is used to represent a variety of cyber threats like spyware, ransomware, viruses, bots, trojans, and worms.
- It is commonly introduced via email attachments, downloads or network vulnerabilities.





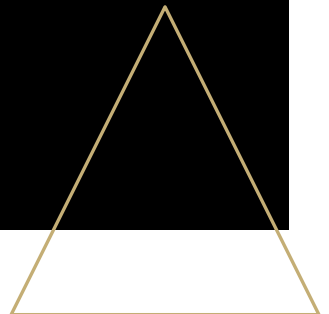
Main aspects of a malware attack

- **Objective:** What the malware is designed to achieve.
- **Delivery:** How the malware is delivered to the target.
- **Concealment:** How the malware avoids detection.



Common Objectives

- Stealing data, credentials, payment information, etc.
- Destroys computer systems. Here the level of destruction can vary depending on the intention of the attacker.
- Locking up networks and PCs, making them unusable to further extort money from the target either by scareware or ransomware.
- Uses your computing power to send spam emails.





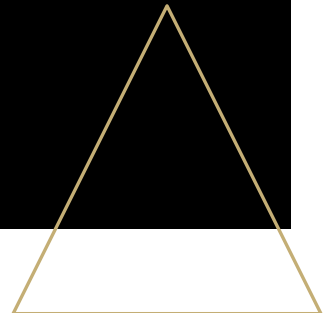
TYPES OF MALWARE PACKS

- Virus
- Worm
- Trojan
- Hybrid malware
- Adware
- Malvertising
- Spyware
- Ransomware
- Fileless malware
- Scareware
- Rootkit
- Bot
- Keyloggers
- Backdoors
- RAT
- Downloaders
- POS

- **Adware**: It shows ads and popups that link to unsafe sites. It redirects users to similar lookalike sites promoting advertised products that can be potentially malicious.



<https://www.techtarget.com/searchsecurity/definition/adware>



- **Spyware**: It monitors users' online activities and browsing habits without their consent, to collect financial details and login credentials.

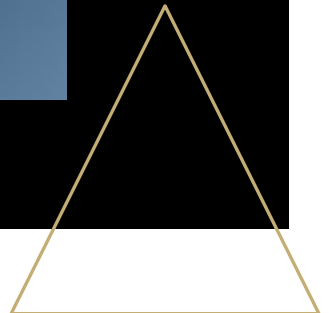


<https://www.techtarget.com/searchsecurity/answer/The-effects-of-spyware>

- **Viruses:** They can delete important files or corrupt data by shutting down the device in the middle of use.



<https://cyware.com/news/luzerne-county-in-pennsylvania-hit-with-virus-attack-09a9058b>



- **Trojans**: They are hidden in online games or software and take control of the device. It is used to install further malware, delete or steal important data, monitor online activities, or modify files.

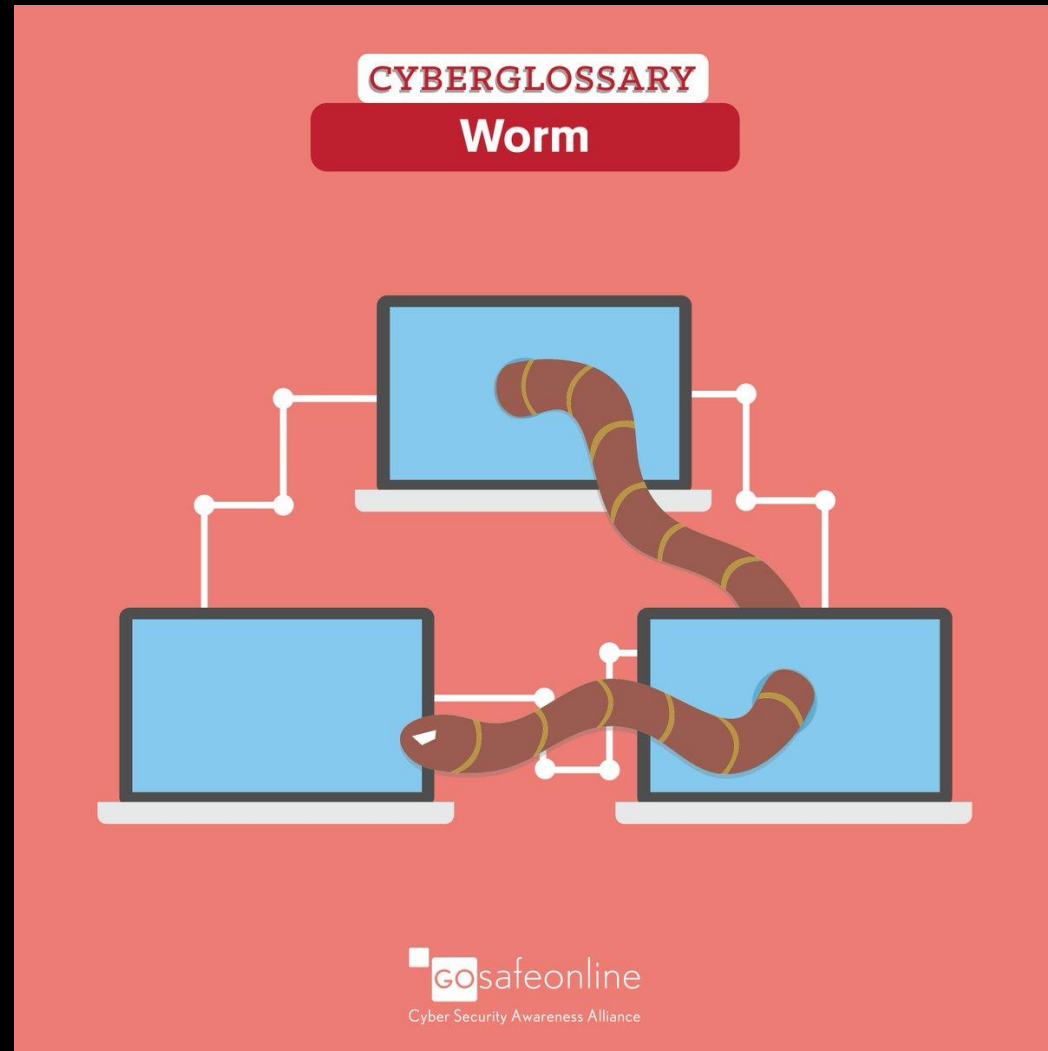


A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software.



Worms: They are a self-replicating type of malware that can spread to other computers. Worms can spread through –

- computer networks,
- e-mails,
- instant-messaging services,
- social networks,
- removable media and
- other channels.



<https://twitter.com/gosafeonline/status/997673392823140352>

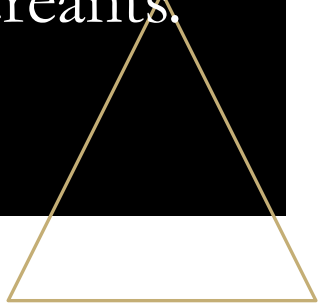
- **Scareware**: Cybercriminals scare us into thinking that our computers or smartphones have become infected to convince victims to purchase a fake application.



<https://www.wallarm.com/what/what-is-scareware-malware-removal-and-protection>



Recent Cases

- In April 2022, Oil India was hit by a malware attack in its field headquarters in eastern Assam's Duliajan, wherein the hacker demanding \$75,00,000.
 - After receipt of the report of malware threat, precautionary measures were taken by the company.
 - Network management service providers and the Anti-Virus Team were immediately informed & the incident was also reported to the Indian Computer Emergency Response Team (CERT-In).
 - The company did not attempt to establish any contacts with the miscreants.
- 

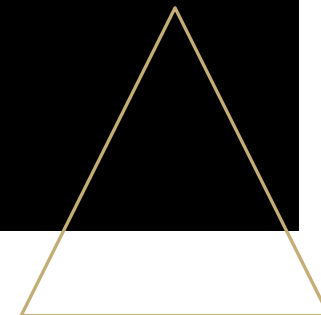


RANSOMWARE ATTACKS



What is a ransomware attack?

- Cybercriminals utilize ransomware as a sort of malware.
- When ransomware infects a computer or network, it either (i) locks the system's screen or (ii) locks the users' files.
- In exchange for releasing the data, cybercriminals seek ransom money from their victims.
- The Remote Desktop Protocol, phishing emails, and software flaws are commonly used as attack vectors.



TYPES OF RANSOMWARE ATTACKS

LOCKER RANSOMWARE

This malware prevents basic computer processes from functioning. For example, you may be denied access to the desktop, while the mouse and keyboard are partially disabled. This permits you to continue interacting with the ransom demand window in order to make the payment. Aside from that, the PC is unusable.

CRYPTO RANSOMWARE

Here the goal is to encrypt your vital data, such as documents, photos, and videos, while not interfering with basic computer functionality. Crypto developers frequently include a countdown to their ransom demand. The encrypted files ensures that victims are forced to pay the ransom even if the malware itself was deleted.

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through

To pay the fine, you should enter the digits resulting code, which is located on the back of your in the payment form and press OK (if you have several codes, enter them one after the other and press OK).



OK



Private key will be destroyed on
27/01/2014 16:18:45

Time left

4 d. 23 : 58 : 48

Your personal files are encrypted!

Your important files encryption produced on this computer: photos, video, documents, etc. **HERE** is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key which will allow you to decrypt the files is on a secret server on the internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** similar amount in another currency.

Click Next>> to select the method of payment and the currency.

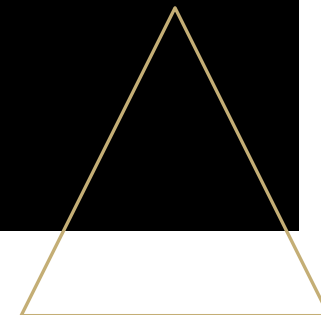
Any attempt to remove or damage this software will lead to immediate destruction of the private key by server.

Next >>




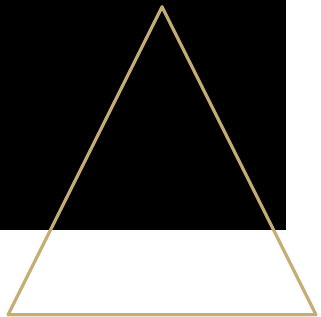
Recent Cases


- Recently, the All India Institute of Medical Sciences (AIIMS), the country's foremost healthcare institution, reported a large cyber hacking as the result of a ransomware attack.
- The cyber-attack caused a server outage, which disrupted daily hospital operations like appointments, patient registration, discharge, and more.





How to Mitigate
an Active
ransomware
Infection

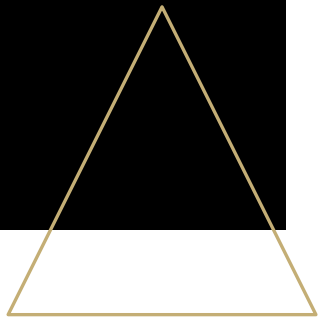
- 
1. **Quarantine the Machine:** You must isolate systems so that they cannot affect the rest of the environment.
 2. **Leave the Computer On:** Encryption of files may make a computer unstable and powering off a computer can result in loss of memory. Keep the computer on to maximize the probability of recovery.
 3. **Create a Backup:** Decryption of files is sometimes possible without paying the ransom. Make a copy of encrypted files on a removable media in case a solution becomes available in the future.
- 



4. **Check for Decryptors:** Check if a free decryptor is available. If so, run it on a copy of the encrypted data to see if it can restore the files.

5. **Ask For Help:** A digital forensics expert may be able to recover the backup copies stored on a computer if they haven't been deleted by the malware.

6. **Wipe and Restore:** Restore the machine from a clean backup. This ensures that the malware is completely removed from the device.





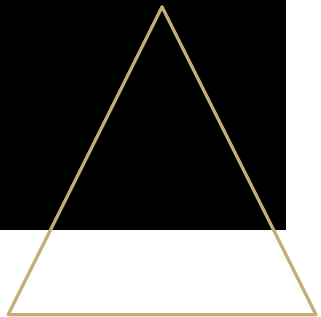
CYBER SAFETY
FOR PARENTS &
CHILDREN



DO's

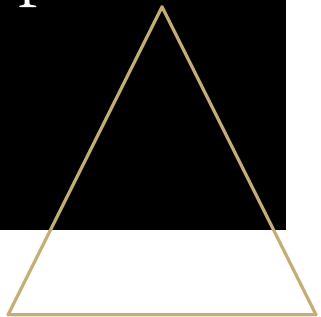
- Learn how to identify potential malware (i.e. phishing emails, unknown applications running on a system).
- If a child uses email, talk to them to ensure they know their peers and teachers' email addresses.
- Keep their social media accounts set to private and explore other settings that can keep them safe.

DONT's

- Don't download any unknown software/App.
 - Don't open unknown attachments or links in suspicious emails.
 - Don't provide personal information to anyone through the internet.
- 



BEST PRACTICES

- Periodic, unannounced exercises, such as intentional phishing campaigns.
 - Equip the computers with a good anti-virus software.
 - Use multi-factor authentication to protect your accounts.
 - Always keep the systems updated.
 - Employ strong & complex passwords.
 - Change your passwords regularly and never save passwords electronically.
 - Back up important files using the 3-2-1 rule: Create three backup copies on two different media with one backup in a separate location.
- 



How to
identify
phishing
emails

Check Grammatical and Spelling Errors

From: MS Team, Outlook Message Center <no-reply@office365protectionservices.co.uk>
Sent: 19 September 2018 11:44
To: Bob Smith <Bob.Smith@Company.com>
Subject: Account Verification

Fake domain

This mail is from a trusted sender.



Threat

We're having trouble verifying your Office365 account: Bob.Smith@Company.com on our server, most features will be turned off.

To help prevent account malfunctions, please log into your account portal to verify your account.

Spelling mistakes

[SIGN IN TO MICROSOFT ACCOUNT PORTAL](#)

Note : Outlook will automatically fix your account after this process on the microsoft server and all account features will be turned back on

Thanks for using office365 , we hope to continue serving you.

Microsoft Corporation
One-Microsoft Way Redmond
WA, 98052

Grammatical errors

Fake email signature

All Right Reserved | Acceptable Use Policy | Privacy Notice

PayPal Services

3 February 2015 at 04:59



Reminder : Your account has ben suspended now please renew ?

To: **PayPal Services,** **Your email is not correct or not visible**

Reply-To: **Services@PayPal.cc** **Not correct domain in address fields**



Fuzzy images

Important Notice

Aggressive wording

Warning,

Impersonal greeting

Some information on your account appears to be missing or incorrect.

Please confirm your information promptly so that you can continue to enjoy all the benefits of your PayPal account.

If you don't confirm your information, **we'll limit what you can do** with your PayPal account.

Threats

Here's a link to all the legal details

[Validate your account Here](#)

Hovering over link reveals not correct domain

Thank you for being a PayPal customer.

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help Center by clicking "Help" located on any PayPal page or email.

Copyright © 2014 PayPal, Inc. All rights reserved. PayPal is located at 2211 N. First St., San Jose, CA 95131.





Reporting malware
and ransomware
attacks



CERT-In 6 Hours Reporting Timeline

- This notification is for all service provider, intermediary, data centre, body corporate and Government organisation.
- They must mandatorily report cyber incidents to CERT-In within 6 hours of noticing such incidents.
- The incidents can be reported to CERT-In via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969).

Notification No. 20(3)/2022-CERT-In,

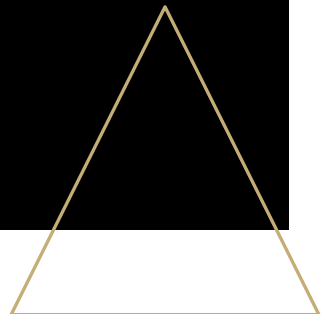
Dated: 28 April, 2022





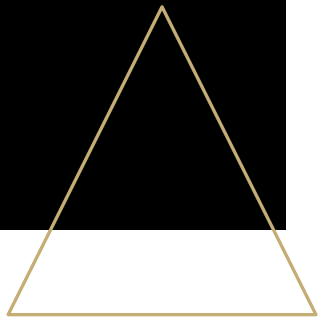
Cybercrime Reporting Portal

- <https://cybercrime.gov.in/> is the main cybercrime reporting portal in India. The offence is punishable under Section 66 of IT Act, 2000 with three years of imprisonment , fine or both.
- When you are hit by a malware or a ransomware attack, you can report the same on the portal under different heads such as “Data theft”, “Ransomware”, “Virus, Worms & Trojans”, or “Denial of Services/Distributed DOS”.





1930 Financial Fraud Helpline No.

- The singular objective of this platform is to prevent the defrauded money from exiting the financial ecosystem and ending up in the hands of the fraudsters.
 - You must report the financial fraud within 24 hours of occurrence.
 - This platform has been made operational by the Indian Cyber Coordination Centre (14C).
 - It has the active support and cooperation of Reserve Bank of India(RBI), all major banks, payment gateways and online merchants.
- 

Thank You

