Ransomware & Trojan Horse Malware - Krish

▼ Ransomware

▼ About ransomware

- Malware that attacker injects in the victim’s system, which makes the system to not able to access any kind of media.
- System remains freezed until and unless the attacker receives its demanded money or wish grants
- According to **Veeam’s Ransomware Report 2023** 85% of the organizations suffered at least 1 ransomware attack in 12 months.

- Statistics:
  - Ransomware and distributed denial-of-service (DDoS) attacks were the next most common event types, each affecting about 46% of organizations.
  - Ransomware attacks continued to rise in 2023, with estimates ranging from **300,000 to 600,000** attacks globally. This represents a significant increase compared to 2022.
  - 93% of ransomware incidents did not result in any loss of data
  - In order to pay the ransom the organizations had to pay using their insurance which was able to cover it up by 19% .
  - 21% of organizations found that ransom is specifically excluded from security insurance
  - On average organizations say that 45% of production data was affected due to the attack i.e out of 5, only 2 companies had a loss in data(email, database, confidential information)
- **Current Trends** in ransom attacks is target the victims or the organizations who have a backup of their data. Now over 93% of the ransomware attacks have been targeted to systems having data backups. Recovery from the attack around 3.4 weeks. Ransomware-as-a-service (RaaS) and double extortion attacks continued to be major trends in 2023. RaaS makes it easier for less-skilled actors to launch ransomware

attacks, while double extortion involves stealing data and threatening to release it if the ransom is not paid.

Working

Ransomware malware has 6 stages:

▼ Malware Distribution & infection:

The attacker first exploits the vulnerabilities of the system by using the remote desktop protocol, tool, phishing, credential misuse, and software vulnerabilities.

- Phishing: it is the most common type of attack where the attacker sends an email to the victim containing various kinds of links which when clicked then immediately the system gets infected with the virus.
- Remote Desktop Protocol: it involves buying the credentials of the victim via dark web or performing a brute force attack to stuff the victim’s credentials and then later remotely accessing the systems virtually.
- Software vulnerability: it refers to the gap in the system of the victim. the attacker thus get benefited and use these gaps to infiltrate into the systems and get access to the system without letting the user know that the system has been compromised.

▼ Controlling Malware

The attacker sends the encryption keys to the victim’s system and install more amount of malware to infect.

▼ Discovery of malware

it is a 2 staged process where the attackers gain the information about the victim’s network and plan ahead about performing attacks to the system and the devices connected to the system and the network.

▼ Malicious theft from database & Encryption

It is the stage where the attackers take over the information stolen from the victim’s system and network later the transferring the data into the C&C server(Command & Control Server). After transferring it in the server the data then gets encrypted and is used for getting the ransom from the victim.

▼ Extortion

▼ Release of System

The attacker when demanding uses various techniques to extort money from the user. Techniques such as informing the victim that the system has malware and to remove that malware he forces to buy the software. Next method is blackmailing the victim saying that of the money is not received then the data will be published to public in open dark markets.

The common targets or potential targets of the attackers are:

1. Educational Institutes
2. Construction sites
3. Government(State & Central)
4. Media
5. Large scaled businesses
6. Financial services
7. Healthcare institutes
8. Manufacturers and telecom
9. Logistics

References:

1. https://www.Techtarget.com
2. https://www.statistica.com
3. homeland security report 2023-24
4. Veeam report 2023
5. https://www. CISA.gov
6. https://www.ibm.com

▼ Trojan Horse Malware

▼ About Trojan Horse Malware

- Trojan Horse malware: is a malware which gets downloaded in the disguised form of a software.

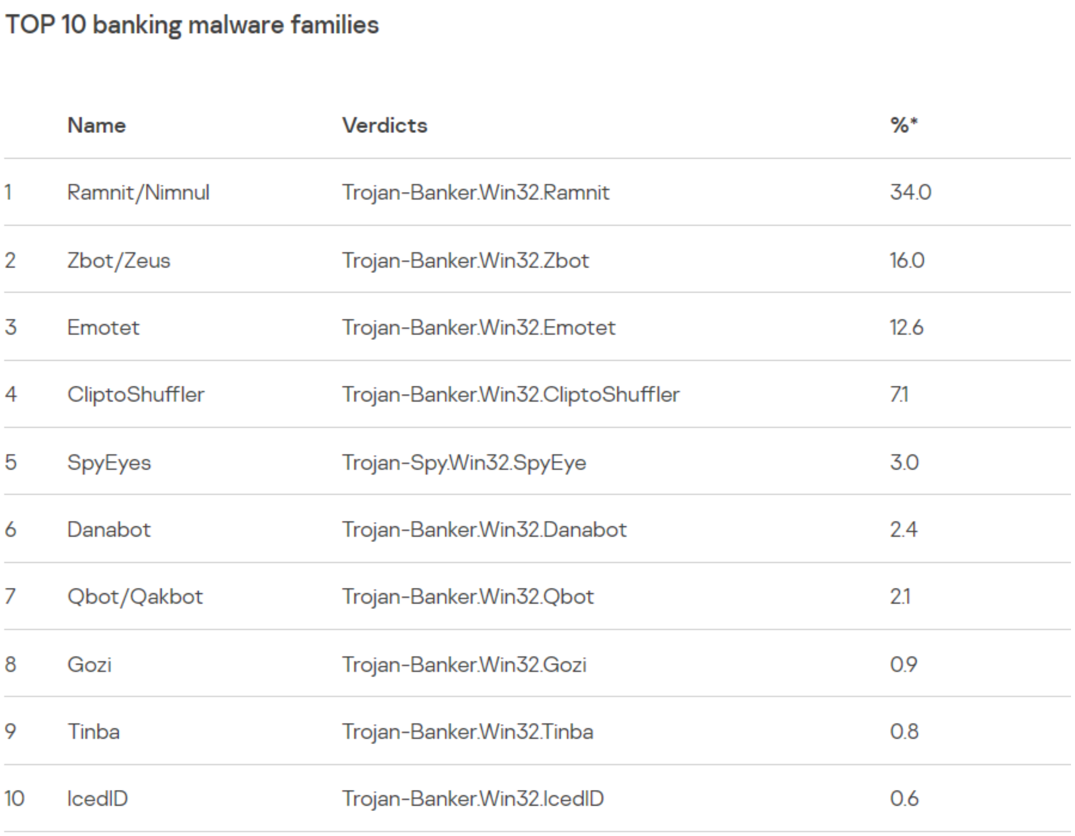
- The malware gets activated once the executable files(.exe) files have been executed. After execution it gives access such as backdoor access to transfer the confidential files of the user.
- This kind of malware is mainly used to spy on the victims without even knowing them that they are being spied.
- There are multiple types of trojan such as:
    - Backdoor trojan
    - Bank trojan
    - Distributed Denial of Service (DDoS) trojan
    - Downloader trojan
    - Fake Antivirus Trojan

▼ Working

- Trojan Horses and any normal computer virus are different. Virus can manifest into the computer without asking you. But in Trojan, the malware gets executed in a way that you may not know and in order to hide its execution it displays a layer of a legitimate software.
- This kind of malware is delivered in the forms of e-mail with attachments in order to spam people at large scale. As soon as the email is clicked to view and attachments are downloaded the trojan servers get activated and every time when the specific device is turned on the trojan gets activated and spy on the user.
- The trojan can also be shared in a computer network and spreads to multiple systems. This is known as botnet.

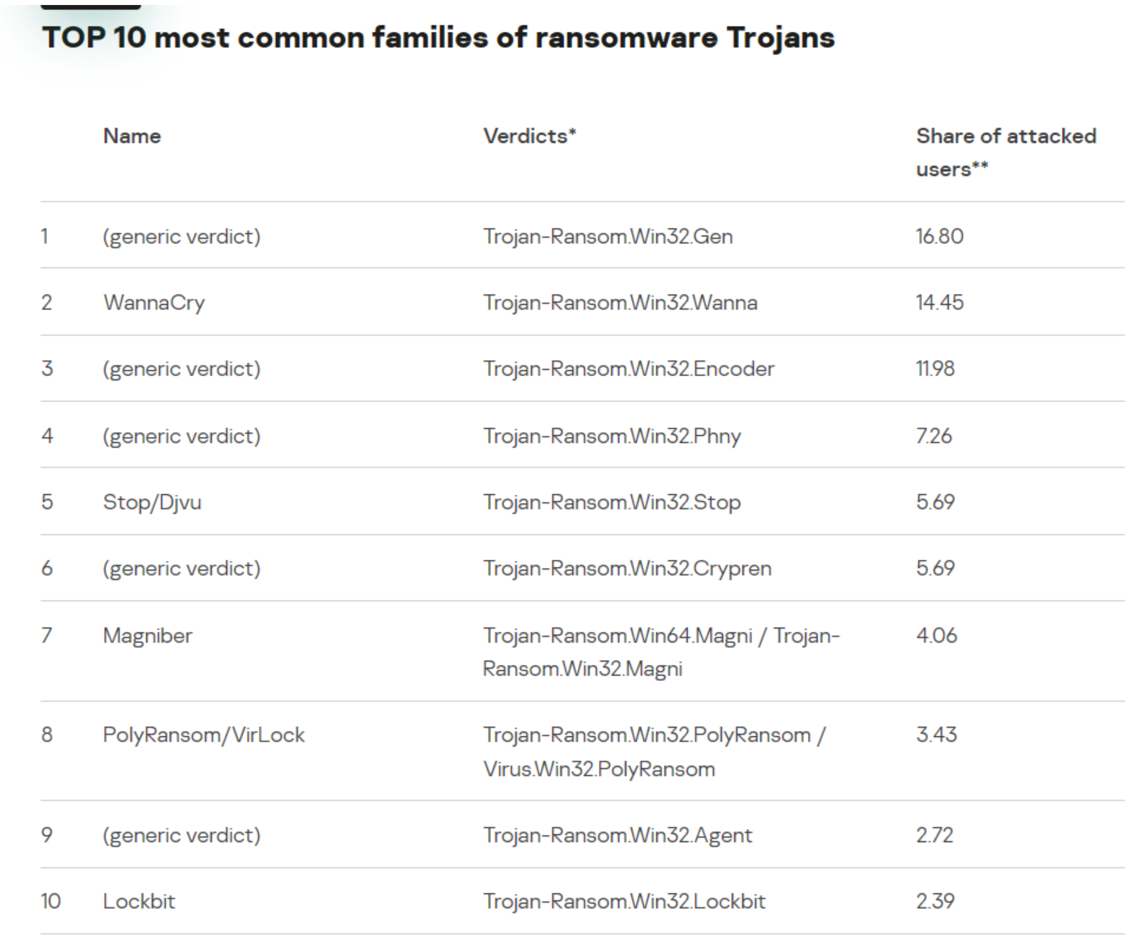
▼ Statistics

1. More than 300,000 Android users have downloaded banking trojan apps via the Google Play Store. (Threat Fabric)
2. Every minute, four companies fall victim to ransomware attacks, with Trojans accounting for 58% of all computer malware. These attacks can result in the loss of sensitive data, financial loss, and a damaged reputation.



TOP 10 banking malware families

	Name	Verdicts	%*
1	Ramnit/Nimnul	Trojan-Banker.Win32.Ramnit	34.0
2	Zbot/Zeus	Trojan-Banker.Win32.Zbot	16.0
3	Emotet	Trojan-Banker.Win32.Emotet	12.6
4	CliptoShuffler	Trojan-Banker.Win32.CliptoShuffler	7.1
5	SpyEyes	Trojan-Spy.Win32.SpyEye	3.0
6	Danabot	Trojan-Banker.Win32.Danabot	2.4
7	Qbot/Qakbot	Trojan-Banker.Win32.Qbot	2.1
8	Gozi	Trojan-Banker.Win32.Gozi	0.9
9	Tinba	Trojan-Banker.Win32.Tinba	0.8
10	IcedID	Trojan-Banker.Win32.IcedID	0.6

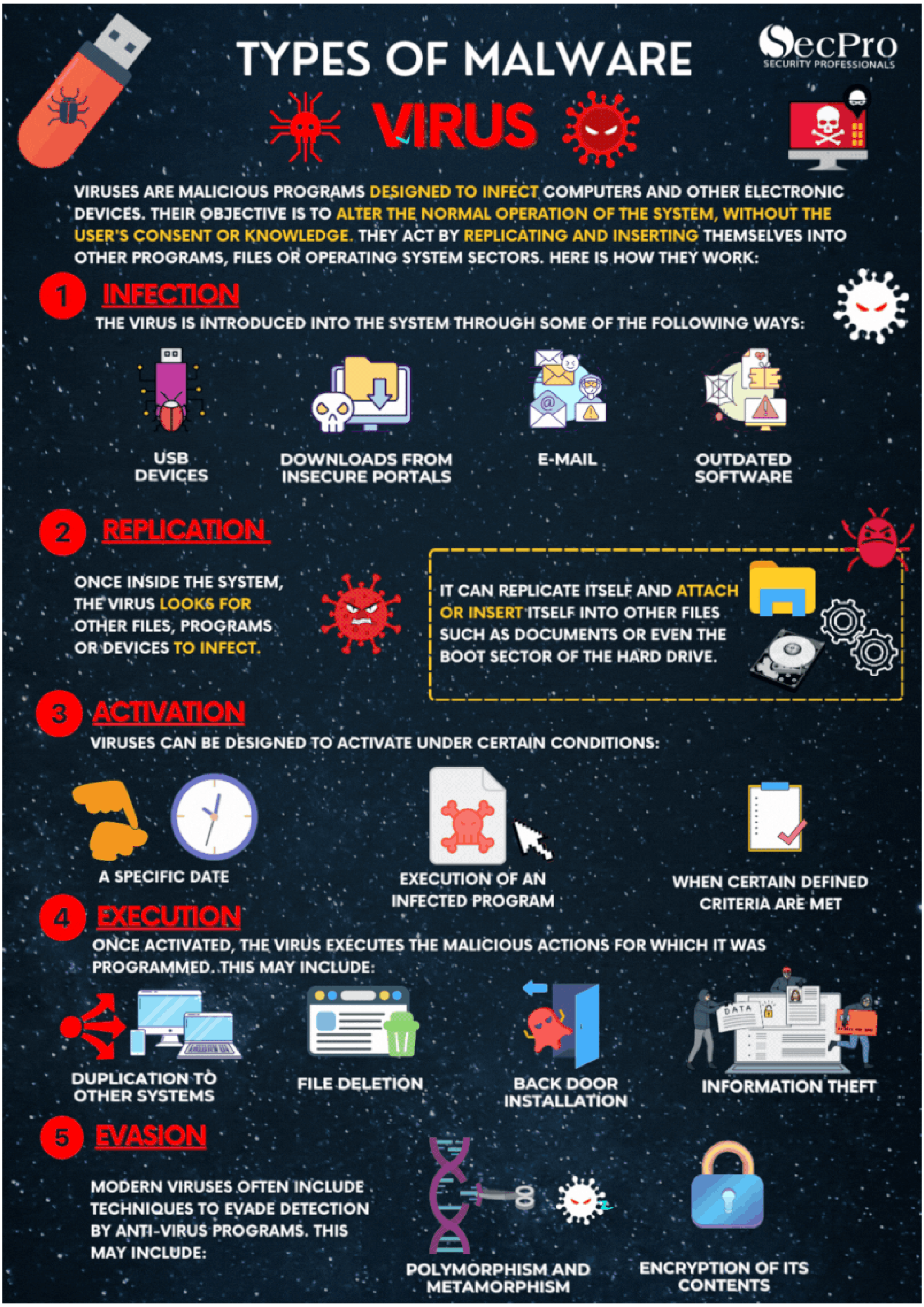


TOP 10 most common families of ransomware Trojans

	Name	Verdicts*	Share of attacked users**
1	(generic verdict)	Trojan-Ransom.Win32.Gen	16.80
2	WannaCry	Trojan-Ransom.Win32.Wanna	14.45
3	(generic verdict)	Trojan-Ransom.Win32.Encoder	11.98
4	(generic verdict)	Trojan-Ransom.Win32.Phny	7.26
5	Stop/Djvu	Trojan-Ransom.Win32.Stop	5.69
6	(generic verdict)	Trojan-Ransom.Win32.Crypren	5.69
7	Magniber	Trojan-Ransom.Win64.Magni / Trojan-Ransom.Win32.Magni	4.06
8	PolyRansom/VirLock	Trojan-Ransom.Win32.PolyRansom / Virus.Win32.PolyRansom	3.43
9	(generic verdict)	Trojan-Ransom.Win32.Agent	2.72
10	Lockbit	Trojan-Ransom.Win32.Lockbit	2.39

References

1. https://www.fortinet.com
2. PC malware statistics, Q3 2023 | Securelist



TYPES OF MALWARE

SecPro
SECURITY PROFESSIONALS

VIRUS

VIRUSES ARE MALICIOUS PROGRAMS DESIGNED TO INFECT COMPUTERS AND OTHER ELECTRONIC DEVICES. THEIR OBJECTIVE IS TO ALTER THE NORMAL OPERATION OF THE SYSTEM, WITHOUT THE USER'S CONSENT OR KNOWLEDGE. THEY ACT BY REPLICATING AND INSERTING THEMSELVES INTO OTHER PROGRAMS, FILES OR OPERATING SYSTEM SECTORS. HERE IS HOW THEY WORK:

1 INFECTION

THE VIRUS IS INTRODUCED INTO THE SYSTEM THROUGH SOME OF THE FOLLOWING WAYS:

- USB DEVICES
- DOWNLOADS FROM INSECURE PORTALS
- E-MAIL
- OUTDATED SOFTWARE

2 REPLICATION

ONCE INSIDE THE SYSTEM, THE VIRUS LOOKS FOR OTHER FILES, PROGRAMS OR DEVICES TO INFECT.

IT CAN REPLICATE ITSELF AND ATTACH OR INSERT ITSELF INTO OTHER FILES SUCH AS DOCUMENTS OR EVEN THE BOOT SECTOR OF THE HARD DRIVE.

3 ACTIVATION

VIRUSES CAN BE DESIGNED TO ACTIVATE UNDER CERTAIN CONDITIONS:

- A SPECIFIC DATE
- EXECUTION OF AN INFECTED PROGRAM
- WHEN CERTAIN DEFINED CRITERIA ARE MET

4 EXECUTION

ONCE ACTIVATED, THE VIRUS EXECUTES THE MALICIOUS ACTIONS FOR WHICH IT WAS PROGRAMMED. THIS MAY INCLUDE:

- DUPLICATION TO OTHER SYSTEMS
- FILE DELETION
- BACK DOOR INSTALLATION
- INFORMATION THEFT

5 EVASION

MODERN VIRUSES OFTEN INCLUDE TECHNIQUES TO EVADE DETECTION BY ANTI-VIRUS PROGRAMS. THIS MAY INCLUDE:

- POLYMORPHISM AND METAMORPHISM
- ENCRYPTION OF ITS CONTENTS