No.

Date :

Androx gh0st	Botnet	Steals credentials, exploits vulnerabilities	Regularly update software & web server
Lumma Stealer	Info Stealer	Steals credentials, crypto currency wallets	Use hardware wallets, avoid suspicious downloads
Cl0p Ransomware	Ransom were	Encrypts data, demands ransom	Use offline backups, apply patches
LOTL (Living Off the Land)	Fileless Malware	Uses built-in system tools for attacks	Restrict PowerShell, disable WMI
Malvertising	Ad-based Malware	Infects systems via malicious ads	Use ad-blockers, avoid pop-ups
BIG-Game Ransomware	Ransomware	Targets large organization for ransom	Implement zero-trust security policies
Emotet	Banking Trojan	Steals banking credentials	~~Enable MF for online banking~~ Do not open unknown attach.
GootLoader	Malware Loader	Distributes ransomware, trojans via fake websites	Be cautious of search engine results.
Dridex	Banking Trojan	Injects malicious code into browsers	Enable MFA for online banking
AZO Rult	Info stealer	Steal passwords, crypto currency wallets	Regularly update software, use antivirus.
Iced ID	Banking Trojan	Injects malicious code into browsers	Do not store passwords in browsers.
Redline Stealer	Info stealer	Steals credentials, crypto wallet	Use two-factor authentication
Trick Bot	Modular Trojan	Downloads additional malware, steal credentials	Block known malicious IPs, use security tools
Raspbery Robin	Worm	Spreads via USB drives	Disable AutoRun for USB Devices

No.

Date :

Josef Hualende Virducio BSIT III-B INFOSEC

CHAPTER 2

MALWARE APPLICATIONS

Name of Malware	Type	Type of Attack	Prevention & Protection
Fake Updates (SocGholish)	Downloader, Trojan	Installs malware via fake update prompts	Avoid clicking pop-ups use anti-virus
Q bot (Qakbot)	Banking Trojan	Steals credentials, logs, keystrokes	Avoid spam emails,
Form book	Info stealer	Steals credentials, screenshots, logs, keystroke	Use password manager, avoid unknown downloads
Nano core	Remote Access Trojan	Enables remote control webcam access	Disable Office macros, use firewalls
Async RAT	Remote Access Trojan	Monitors Activity, downloads & executes malware	Block malicious emails, keep software updated
REMCOS	Remote Access Trojan	Gains high-level priviliges vial Offree files	Avoid enabling macros in documents,
Phorpiex	Botnet	Sends spam emails, spreads malware	Scan USB devices, use email ~~security filters~~.
Ramnit	Banking Trojan	Steals banking credentials & personal data	Use security banking tools,
NJRat	Remote Access Trojan	Captures keystrokes accesse webcams	Segment networks, block suspicious traffice.
Agent Tesla	Keylogger / Infostealer	Steals credentials, monitors keystroke	Keep security software updated, use strong passwords
Necro	Mobile Malware	Infects apps, displays hidden ads	Download apps from trusted stores, enable Play Protect

No.

Date :

I. Identify Malware Types

1. MitMo
2. Ransom Ware
3. Root kit
4. Spy ware
5. Virus
6. Trojan Horse
7. Adware
8. Bot
9. Scareware
10. Worm

II. Identify the type of Attack

1. DoS
2. DDoS
3. DDoS
4. DoS
5. SEO Poisoning
6. SEO Poisoning
7. DDoS
8. DoS, DDoS

III Identify Vulnerability Terminology

1. Non-Validated Input -
2. Weakness in Security Practices -
3. Race Conditions -
4. Buffer Overflow
5. Access Control Problems