CWL
CyberWarFare Labs

MALWARE ANALYSIS 101

- Static Edition

ABOUT CYBERWARFARE LABS :

CW Labs is a Global Infosec company specializing in cybersecurity practical learning situated across UK, US & India. The company has 2 primary divisions :

1. Niche Cyber Range Labs
2. Continuous Learning : Infinity Platform

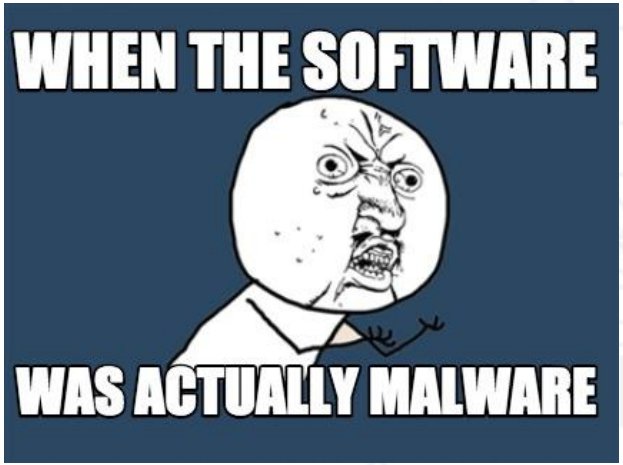
About Speaker

Abhijeet Kumar
(Security Researcher)

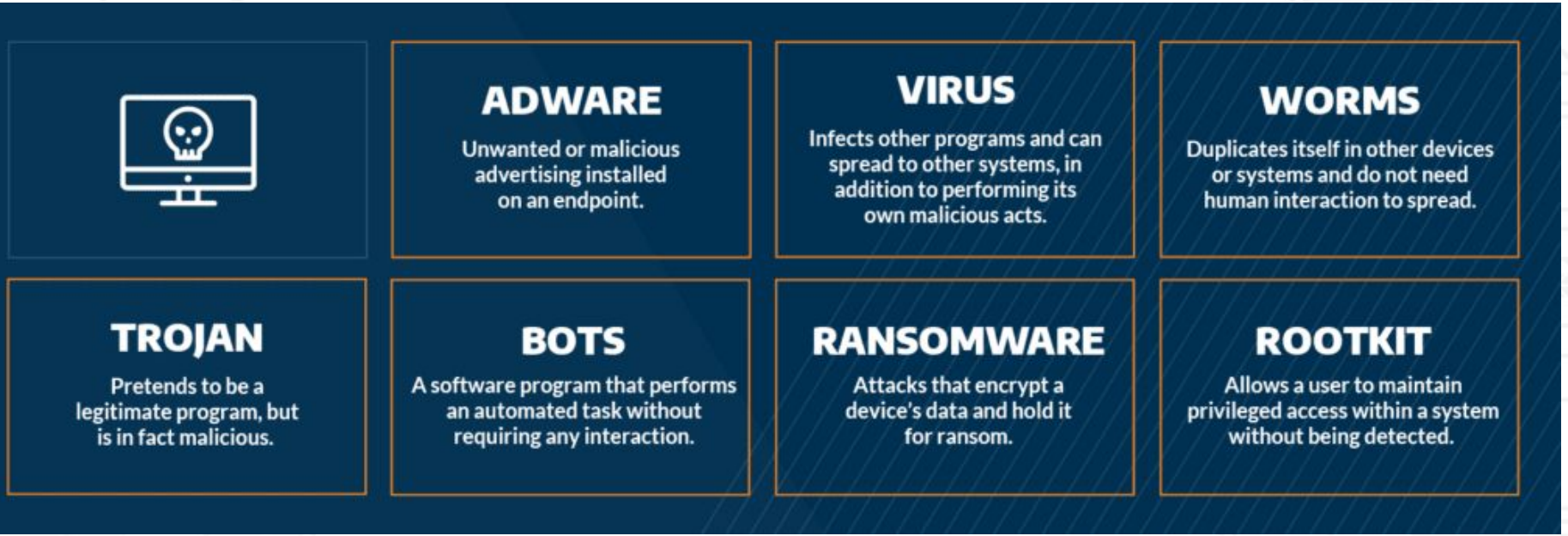
His areas of interests includes Red Team Operations, Network Security, Cloud infrastructure, and Linux Systems. Apart from this, he enjoys researching Adversarial TTPs and experimenting in his homelab during his free time.

MALWARE 101

- ★ A piece of software which does malicious things.
- ★ Used for initial access and persistence, among other things.

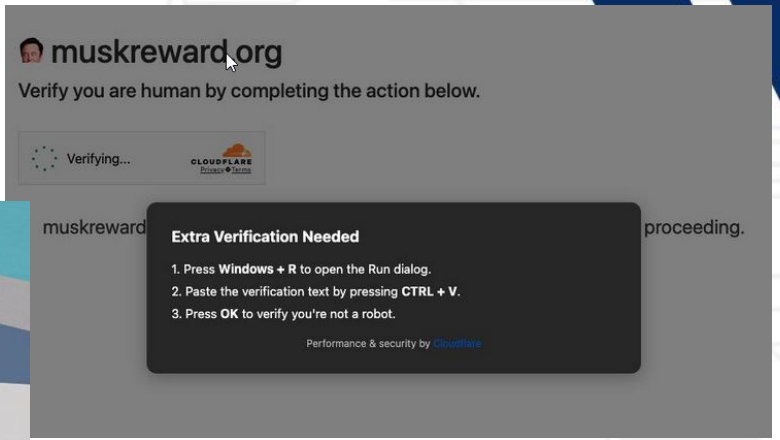


TYPES OF MALWARE



Source: [Arctic Wolf]

HOW MALWARE USUALLY INFECT THE DEVICES ???



Re: Blockchain btc confirmation

MN [redacted] <ceo@[redacted]>

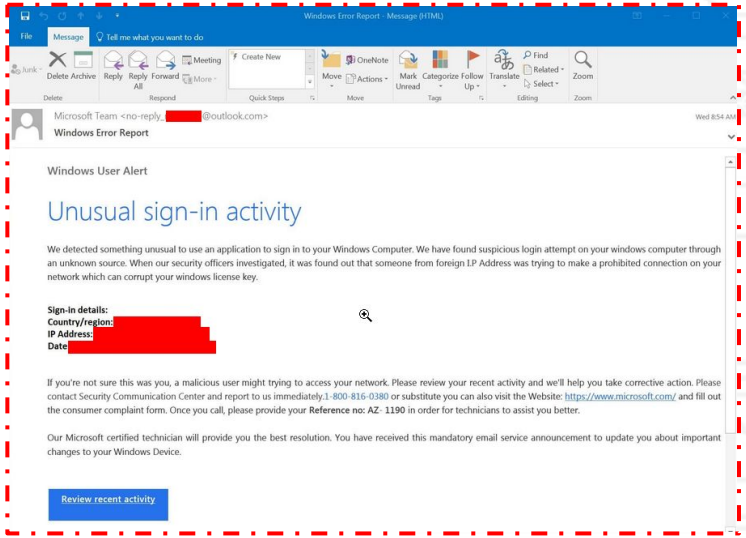
To

6:55 AM

btcconfirmation.doc
2 MB

Action Items Get more add-ins

Could you kindly acknowledge my payment? I have funded your BTC wallet address as instructed.
Enclosed is the blockchain screenshot confirmation.
Thanks
Sent from my iPhone



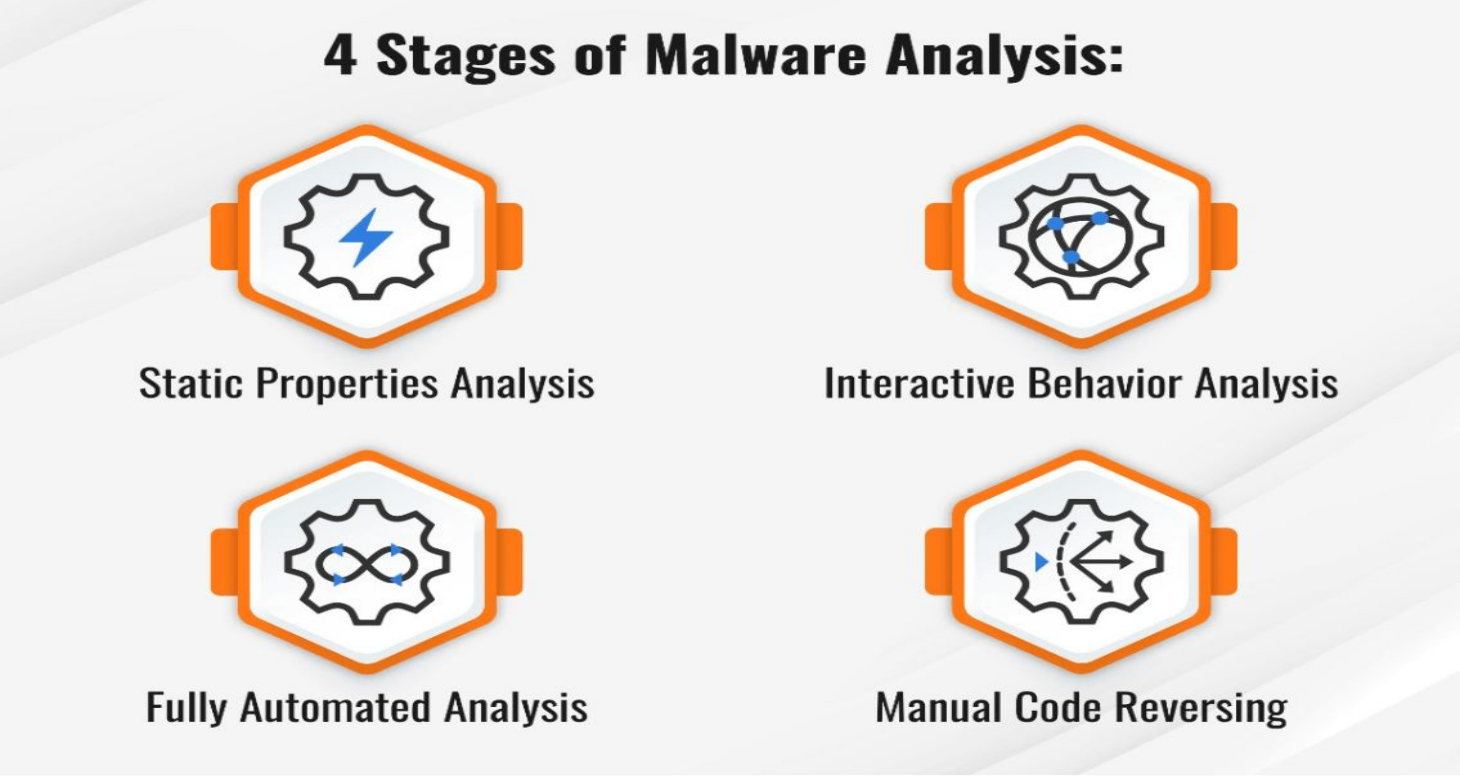
HOW DO WE KNOW IF IT'S A LEGITIMATE SOFTWARE OR A MALWARE

???

MALWARE ANALYSIS 101

Malware analysis involves examining and understanding the behavior, source, and potential effects of malicious software in order to determine its capabilities and potential harm.

MALWARE ANALYSIS STAGES



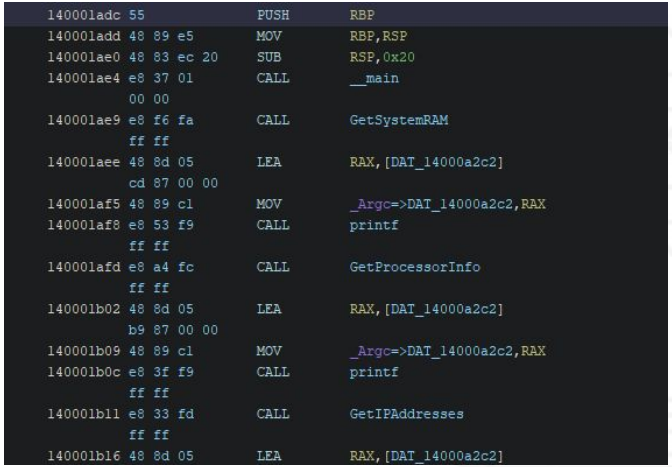
Source: ***Fortinet***

MALWARE ANALYSIS TOOLS

- ★ Disassemblers
- ★ Decompilers
- ★ Debuggers
- ★ Hex Editors
- ★ Metadata Viewers
- ★ Monitors

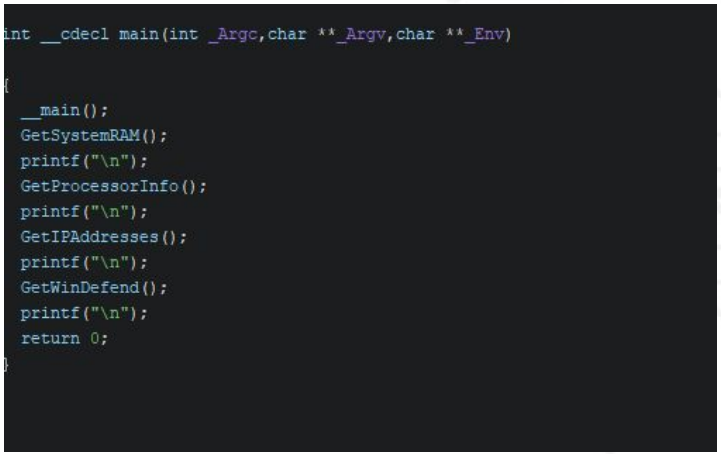
DISASSEMBLERS

- ★ Disassembler is a software tool that converts machine code into a more human-readable format called assembly language.
- ★ Tools :-
  - IDA Pro
  - Gidra
  - Binary Ninja
  - Cutter



DECOMPILERS

- ★ A decompiler is a software tool that takes a compiled program and converts it back into near-original high-level programming language.
- ★ Tools :-
  - IDA Decompiler
  - Ghidra Decompiler
  - Binary Ninja Decompiler

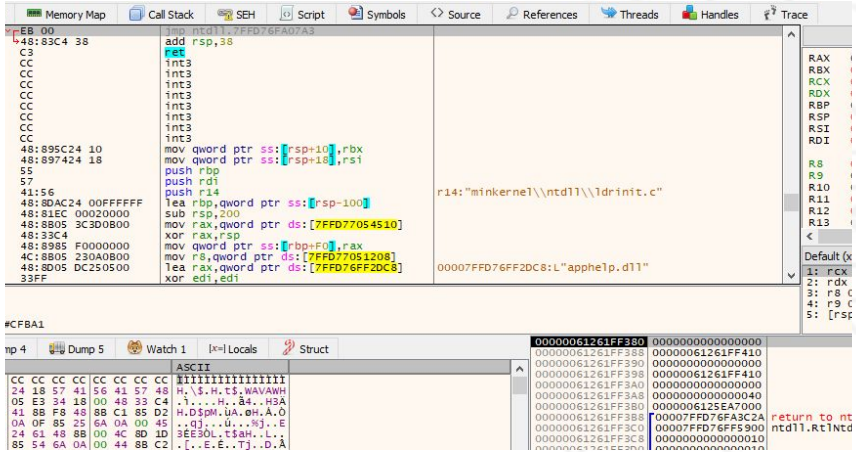


```
int __cdecl main(int _Argc,char **_Argv,char **_Env)

{
  __main();
  GetSystemRAM();
  printf("\n");
  GetProcessorInfo();
  printf("\n");
  GetIPAddresses();
  printf("\n");
  GetWinDefend();
  printf("\n");
  return 0;
}
```

DEBUGGERS

- ★ A debugger is a software tool that helps analyze the program's behavior dynamically i.e, during runtime.



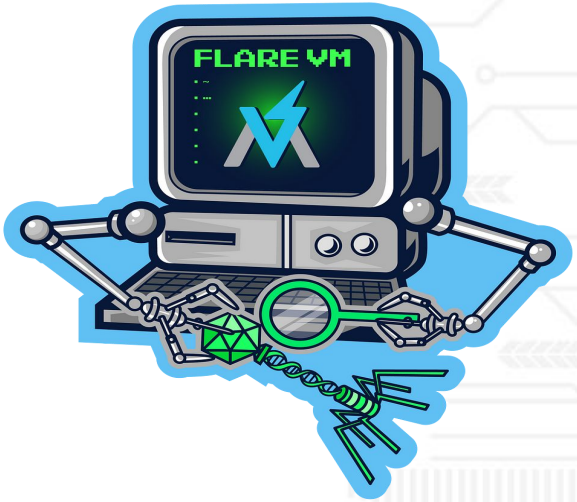
- ★ Tools :-
  - Windbg
  - x64/x32 Debugger
  - dnSpyEx

HEX EDITORS

- A hex editor is a program that lets users edit the hexadecimal code of a computer file.
- Tools :-
  - HxD
  - HexEd.it
  - WinHex

MALWARE ANALYSIS LAB

- A main VM to analyse the malicious samples.
  - E.g: Flare VM
- A secondary VM to act as DNS/Http servers.
  - E.g: Remnux



REMnux
A Linux Toolkit For Reverse-Engineering & Malware Analysis

CWL
CyberWarFare Labs

THANK YOU

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings please contact

support@cyberwarfare.live

To know more about our offerings, please visit: **https://cyberwarfare.live**