

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



INFINITE LEARNING EXPERIENCE

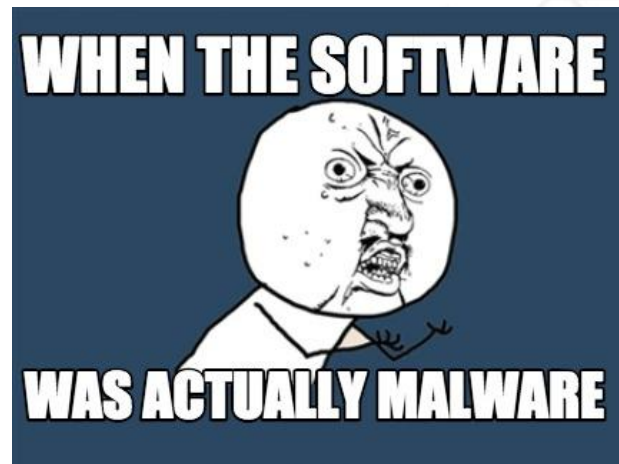
About Speaker

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



ADWARE

Unwanted or malicious advertising installed on an endpoint.

VIRUS

Infects other programs and can spread to other systems, in addition to performing its own malicious acts.

WORMS

Duplicates itself in other devices or systems and do not need human interaction to spread.

TROJAN

Pretends to be a legitimate program, but is in fact malicious.

BOTS

A software program that performs an automated task without requiring any interaction.

RANSOMWARE

Attacks that encrypt a device's data and hold it for ransom.

ROOTKIT

Allows a user to maintain privileged access within a system without being detected.

Source: [Arctic Wolf](#)

**HOW MALWARE
USUALLY INFECT THE
DEVICES ???**



Re: Blockchain btc confirmation

MN [redacted] <ceo@[redacted]>
To

btconfirmation.doc
2 MB



6:55 AM

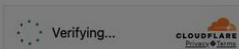
Action Items

+ 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

muskreward.org

Verify you are human by completing the action below.



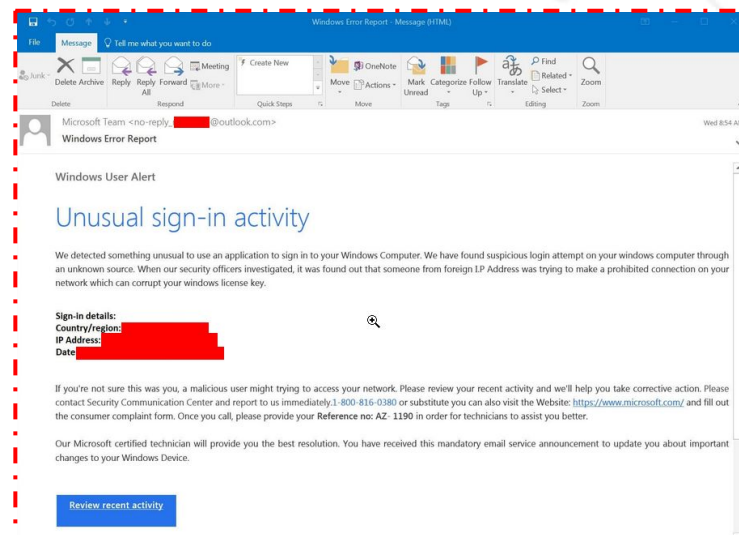
muskreward

Extra Verification Needed

1. Press **Windows + R** to open the Run dialog.
2. Paste the verification text by pressing **CTRL + V**.
3. Press **OK** to verify you're not a robot.

Performance & security by [Cloudflare](#)

proceeding.



**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

4 Stages of Malware Analysis:



Static Properties Analysis



Interactive Behavior Analysis



Fully Automated Analysis



Manual Code Reversing

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

```

140001adc 55      PUSH    RBP
140001add 48 89 e5  MOV    RBP,RSP
140001ae0 48 83 ec 20  SUB    RSP,0x20
140001ae4 e8 37 01    CALL    __main
                00 00
140001ae9 e8 f6 fa    CALL    GetSystemRAM
                ff ff
140001aee 48 8d 05    LEA     RAX,[DAT_14000a2c2]
                cd 87 00 00
140001af5 48 89 c1    MOV     _Argc=>DAT_14000a2c2,RAX
140001af8 e8 53 f9    CALL    printf
                ff ff
140001afd e8 a4 fc    CALL    GetProcessorInfo
                ff ff
140001b02 48 8d 05    LEA     RAX,[DAT_14000a2c2]
                b9 87 00 00
140001b09 48 89 c1    MOV     _Argc=>DAT_14000a2c2,RAX
140001b0c e8 3f f9    CALL    printf
                ff ff
140001b11 e8 33 fd    CALL    GetIPAddresses
                ff ff
140001b16 48 8d 05    LEA     RAX,[DAT_14000a2c2]

```

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

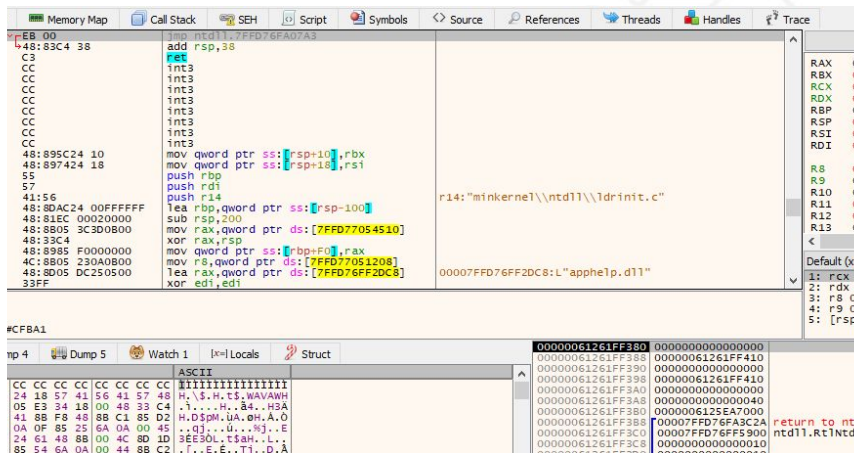
```
int __cdecl main(int _Argc,char **_Argv,char **_Env)
{
    __main();
    GetSystemRAM();
    printf("\n");
    GetProcessorInfo();
    printf("\n");
    GetIPAddresses();
    printf("\n");
    GetWinDefend();
    printf("\n");
    return 0;
}
```

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

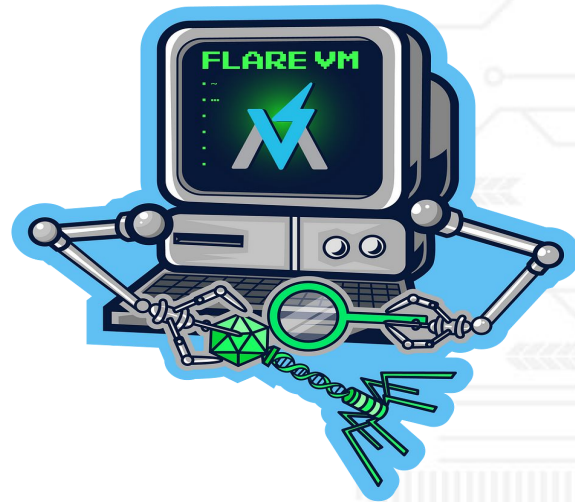
★ A hex editor is a program that lets users edit the hexadecimal code of a computer file.

★ 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

BRACE YOURSELF



MALWARE IS COMING



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>**