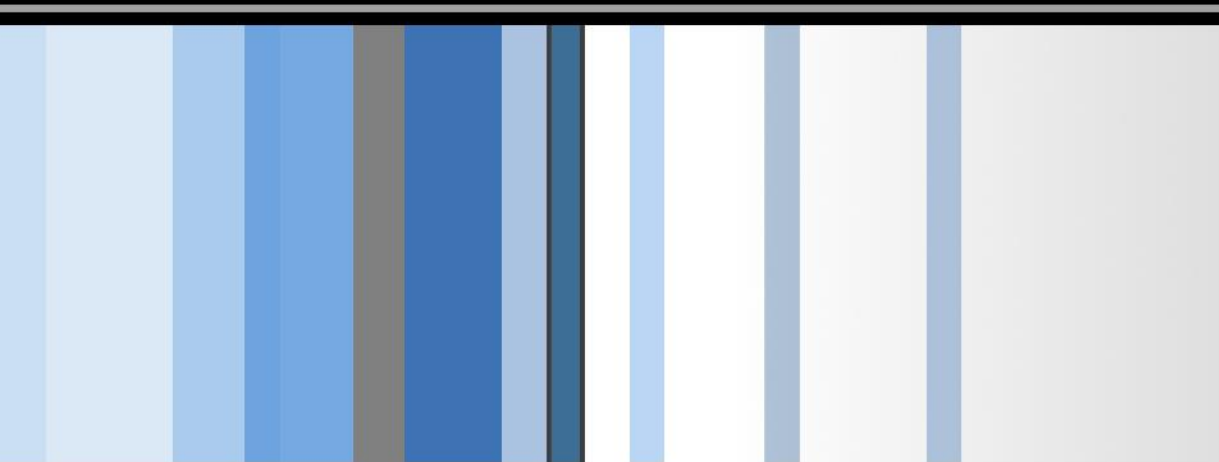


CSC 471: Modern Malware Analysis Introduction

Si Chen (schen@wcupa.edu)



What is malware?

- What is malware? Here are some common types:
 - Trojans
 - Viruses
 - Worms
 - Remote Access Trojans (RATs)
 - Rootkits
- Malware is software designed to perform unauthorized actions on a device. Examples of malicious behavior include:
 - Displaying ads
 - Stealing data
 - Consuming resources



Course Roadmap

- Basic Analysis
 - Debugging
 - Reverse Engineering
 - Malware Behavior
- Modern malware threats
 - Advanced Persistent Threats (APTs)
 - Mobile Malware
 - Web Browser Malware
 - IoT Malware
 - Blockchain and Smart Contract Malware...

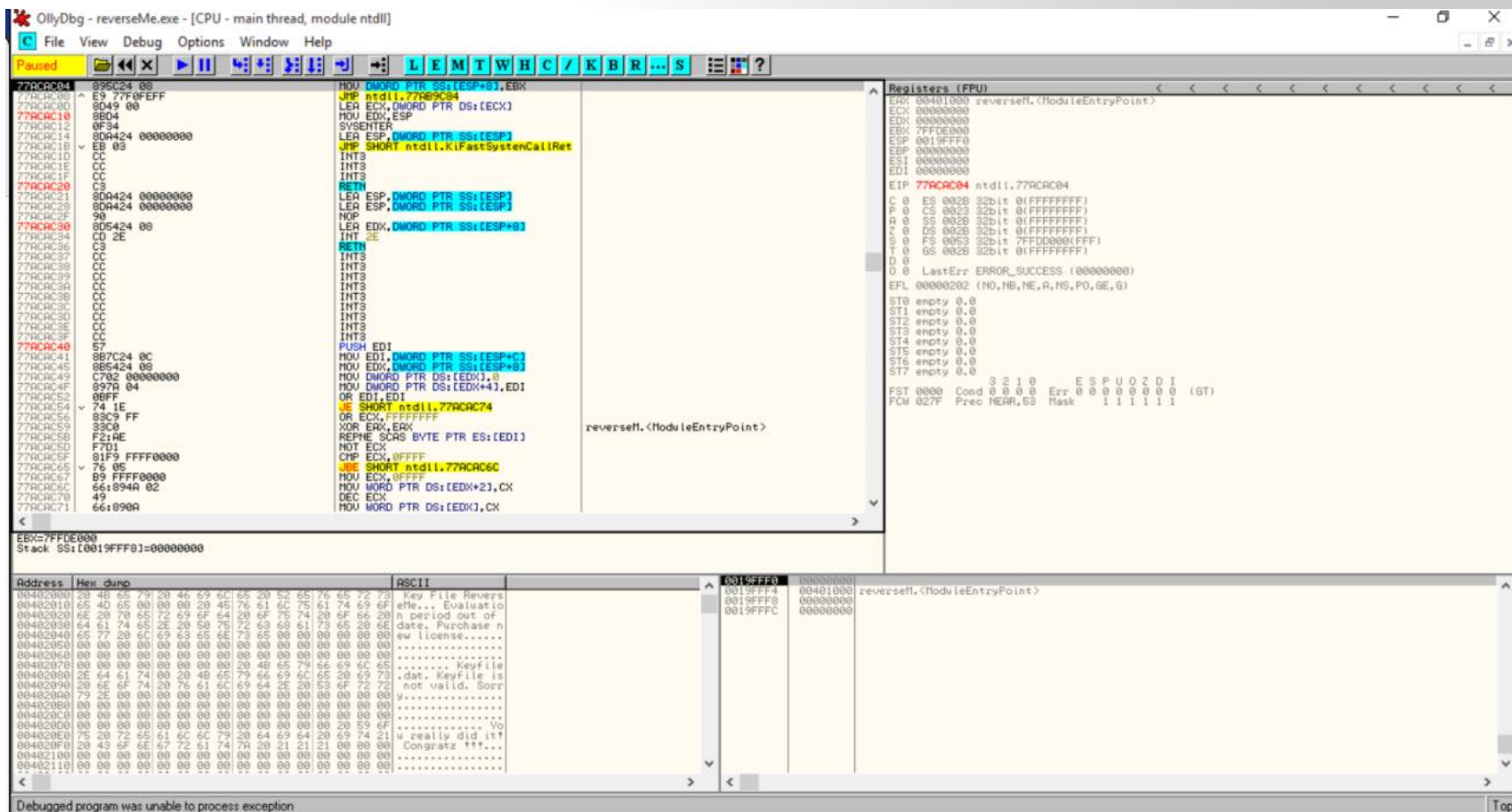
Our approach

- **The course content is divided into two sections:**
- **Section 1: Fundamentals of Malware Analysis**
 - Lectures on the subject
 - Hands-on laboratory activities
- **Section 2: Detailed Exploration of Research Topics**
 - Group presentations and discussions on research topics

Topics covered

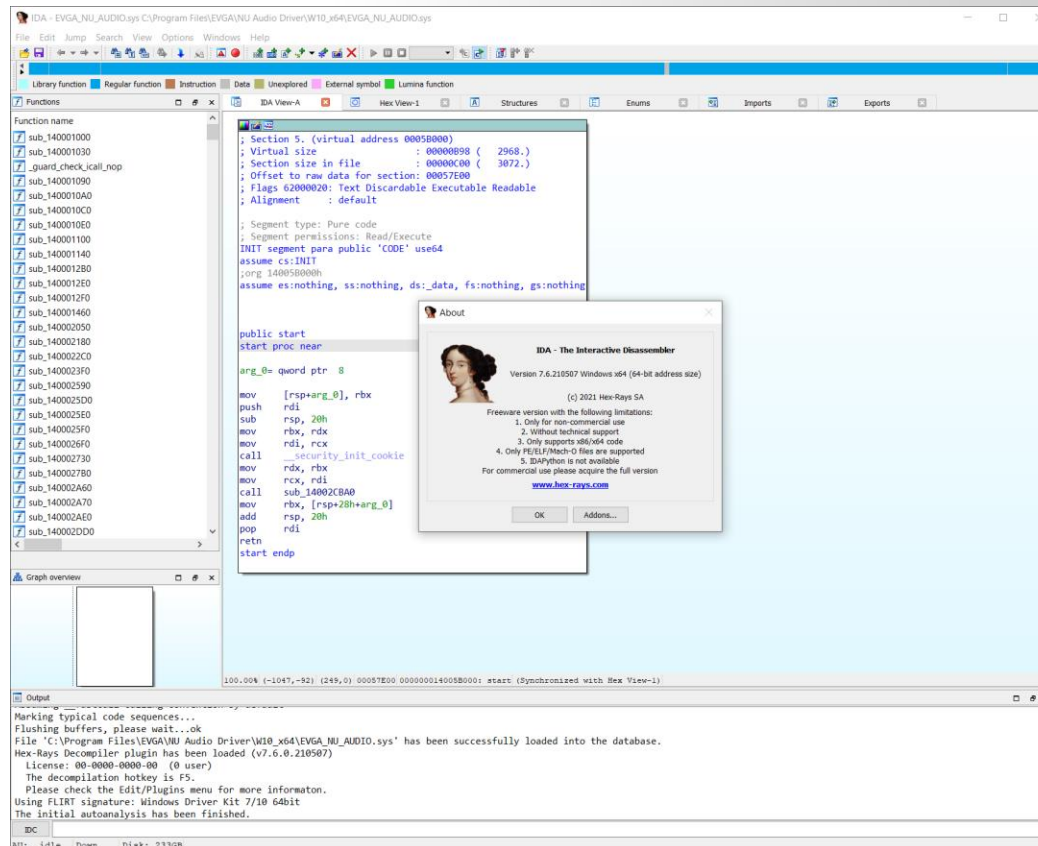
- The legal aspects of malware analysis
- DLL Injection
- Static Analysis
- IA32 Registers and Byte Ordering
- X86 ASM
- Stack and Stack Frame
- Dynamic Analysis
- Hooks
- Message Hooks and API Hooks
- Code Injection
- PE Structure
- Stealth Process (Rootkit)
- Kernel Rootkit
- Worms: CVE-2008-4250 (MS08-067), Conficker Worm
- Volatility and Stuxnet
- Anti-Debugging Techniques
- Malware Analysis: Zeus

Debugging Software



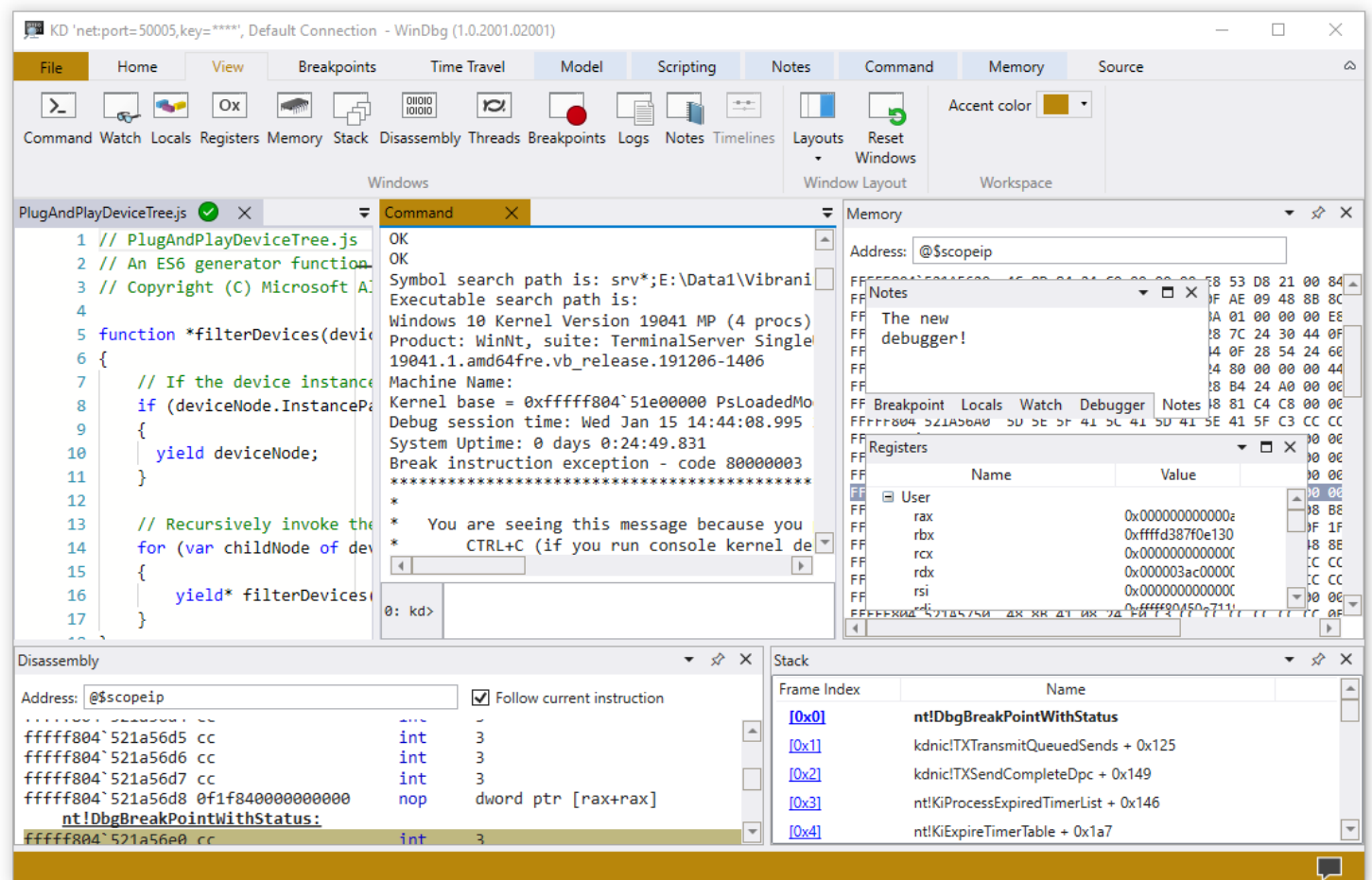
Ollydbg: OllyDbg was an x86 debugger that emphasizes binary code analysis, which is useful when source code is not available. It traces registers, recognizes procedures, API calls, switches, tables, constants and strings, as well as locates routines from object files and libraries. Wikipedia

Debugging Software



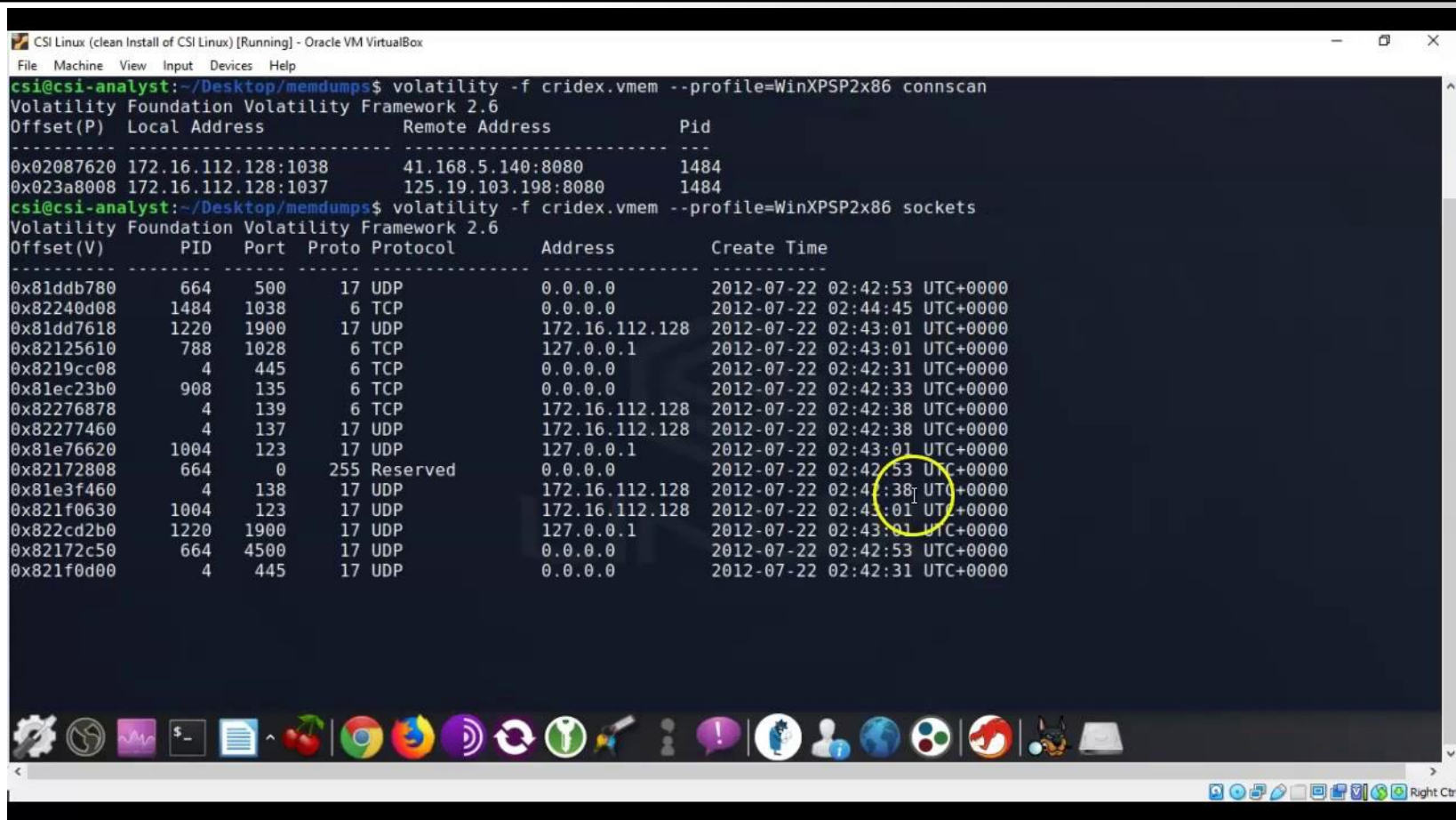
IDA free: This free version of IDA offers a privilege opportunity to see IDA in action. This light but powerful tool can quickly analyze the binary code samples and users can save and look closer at the analysis results.

Debugging Software



WinDbg: WinDbg is a multipurpose debugger for the Microsoft Windows computer operating system, distributed by Microsoft. Debugging is the process of finding and resolving errors in a system; in computing it also includes exploring the internal operation of software as a help to development. [Wikipedia](#)

Volatility



```
CSI Linux (clean Install of CSI Linux) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
csi@csi-analyst:~/Desktop/memdumps$ volatility -f cridex.vmem --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address      Remote Address      Pid
-----
0x02087620 172.16.112.128:1038    41.168.5.140:8080    1484
0x023a8008 172.16.112.128:1037    125.19.103.198:8080  1484
csi@csi-analyst:~/Desktop/memdumps$ volatility -f cridex.vmem --profile=WinXPSP2x86 sockets
Volatility Foundation Volatility Framework 2.6
Offset(V)  PID  Port  Proto Protocol  Address      Create Time
-----
0x81ddb780 664  500   17  UDP        0.0.0.0      2012-07-22 02:42:53 UTC+0000
0x82240d08 1484 1038   6  TCP        0.0.0.0      2012-07-22 02:44:45 UTC+0000
0x81dd7618 1220 1900   17  UDP        172.16.112.128 2012-07-22 02:43:01 UTC+0000
0x821125610 788  1028   6  TCP        127.0.0.1     2012-07-22 02:43:01 UTC+0000
0x8219cc08 4  445    6  TCP        0.0.0.0      2012-07-22 02:42:31 UTC+0000
0x81ec23b0 908  135    6  TCP        0.0.0.0      2012-07-22 02:42:33 UTC+0000
0x82276878 4  139    6  TCP        172.16.112.128 2012-07-22 02:42:38 UTC+0000
0x82277460 4  137    17  UDP        172.16.112.128 2012-07-22 02:42:38 UTC+0000
0x81e76620 1004 123    17  UDP        127.0.0.1     2012-07-22 02:43:01 UTC+0000
0x82172808 664  0      255 Reserved 0.0.0.0      2012-07-22 02:42:53 UTC+0000
0x81e3f460 4  138    17  UDP        172.16.112.128 2012-07-22 02:42:38 UTC+0000
0x821f0630 1004 123    17  UDP        172.16.112.128 2012-07-22 02:43:01 UTC+0000
0x822cd2b0 1220 1900   17  UDP        127.0.0.1     2012-07-22 02:43:01 UTC+0000
0x82172c50 664  4500   17  UDP        0.0.0.0      2012-07-22 02:42:53 UTC+0000
0x821f0d00 4  445    17  UDP        0.0.0.0      2012-07-22 02:42:31 UTC+0000
```

Volatility: Volatility is an open-source memory forensics framework for incident response and malware analysis. It is written in Python and supports Microsoft Windows, Mac OS X, and Linux. Volatility was created by Aaron Walters, drawing on academic research he did in memory forensics. [Wikipedia](https://en.wikipedia.org/wiki/Volatility_(memory_forensics))

Why do people write malware?

- Morris Worm
 - Accidentally released
 - Purpose: To measure the size of the internet
 - Outcome: Created a fork bomb



Why do people write malware?

- Once upon a time... (30 Years Ago)
 - Just for fun
 - Spread to other machines & display a message

```
C:\>dir/w

Volume in drive C is MS-DOS_6
Volume Serial Number is 3B64-85C5
Directory of C:\

[DOS]          COMMAND.COM      WINA20.386      CONFIG.SYS      AUTOEXEC.BAT
[UMADD]        SPANSKA.COM
              7 file(s)          66,334 bytes
                                60,672,000 bytes free

C:\>spanska.com

C:\DOS>cd..

C:\>time
Current time is 12:33:34.11p
Enter new time: 12:30:00.00p

C:\>spa_
```

Why do people write malware?

- Today

- \$\$\$

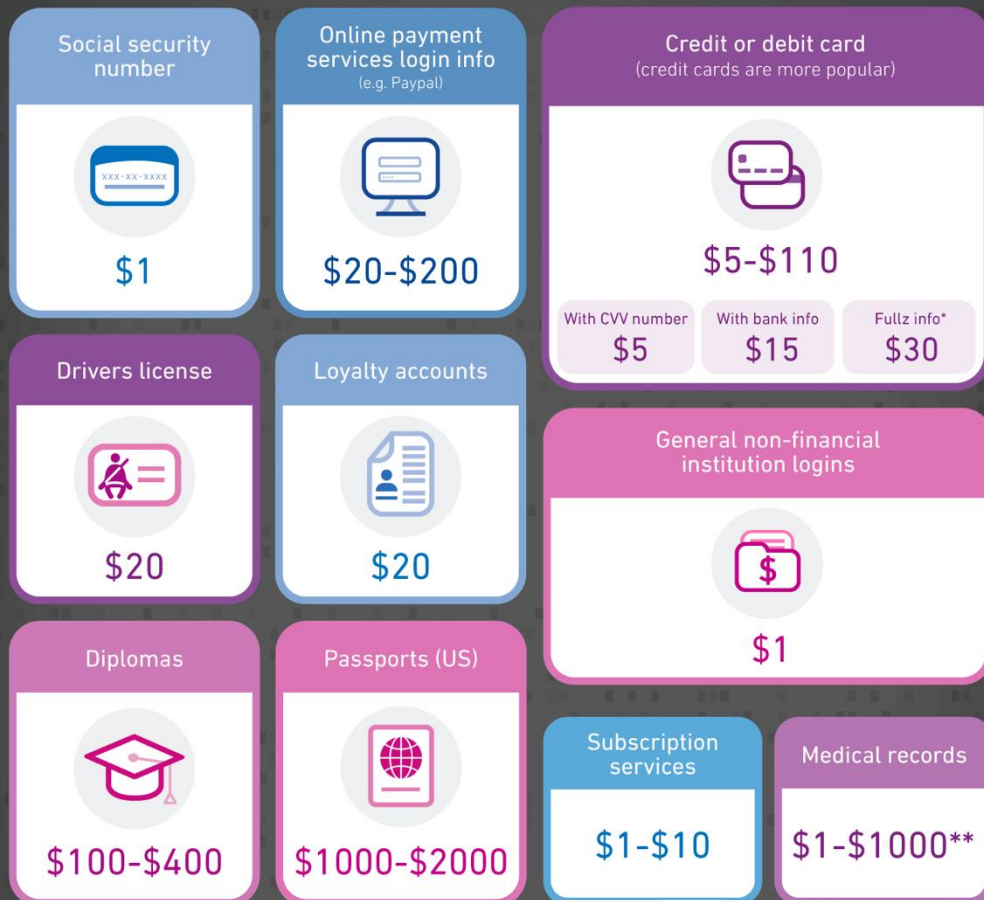
- Organizations purchase malware to

- steal passwords,
 - credit card details,
 - bank information,
 - and intellectual property,
- as well as to demand ransoms and obtain trade secrets.

They may use this information or sell it.

Your identity is a steal on the Dark Web.

Here are what the most common pieces of information sell for:



*Fullz info is a bundle of information that includes a "full" package for fraudsters: name, SSN, birth date, account numbers and other data that make them desirable since they can often do a lot of immediate damage.

**Depends on how complete they are as well as if it is a single record or an entire database.

Note: Prices can vary over time and prices listed below are an estimation and aggregation based on reference articles and hands on experience of Experian cyber analyst the last two years.

The Story Behind the CVE-2024-3094 Vulnerability

CVE Number	Description	CVSS Severity
CVE-2024-3094	Malicious code was discovered in the upstream tarballs of xz, starting with version 5.6.0. Through a series of complex obfuscations, the liblzma build process extracts a prebuilt object file from a disguised test file existing in the source code, which is then used to modify specific functions in the liblzma code. This results in a modified liblzma library that can be used by any software linked against this library, intercepting and modifying the data interaction with this library.	10.0 Critical

- In 2024, a significant vulnerability, **CVE-2024-3094**, was discovered in the **XZ Utils**, a widely used open-source data compression tool. This case became a cautionary tale about the risks of supply chain attacks in the open-source ecosystem.

The Story Behind the CVE-2024-3094 Vulnerability

▪ How the Backdoor Was Introduced

- A developer, using the alias **Jia Tan**, had joined the XZ Utils project as a contributor back in 2021.
- Over time, Jia Tan made seemingly legitimate contributions to the project. These changes were subtle and did not raise any immediate red flags.
- Eventually, malicious code was introduced, disguised as performance optimizations or minor bug fixes. This code introduced a backdoor, allowing remote code execution on systems that used the library.

<https://jfrog.com/blog/xz-backdoor-attack-cve-2024-3094-all-you-need-to-know/>

Why do people write malware?

■ Future... Today

- Gathering more information about a person.

—

IIElevenLabs

AI AUDIO ▾ SOLUTIONS ▾ API PRICING COMPANY ▾

LOG IN

TRY FOR FREE

VOICE CLONING

Create a replica of your voice that sounds just like you

Automate video voiceovers, ad reads, podcasts, and more, in your own voice

VOICE CLONING PLANS

Swap Faces with One Click

Want to generate face swap images in batches? [Batch Swap Now](#)



History



AI-Driven Cyber Threats: Emerging Trends and Risks in 2024

The Rise of AI in Cyberattacks

- AI adoption in cyberattacks is rapidly increasing.
- New trends include AI-generated malware, phishing, and deepfake technology.
- Organizations face unprecedented challenges in defending against AI-driven threats.

Deepfake Phishing: The Dangerous New Face Of Cybercrime

AI-Powered Phishing Attacks Surge in 2024, with 96% of Organizations Impacted



Stu Sjouerman Forbes Councils Member

Forbes Technology Council COUNCIL POST | Membership (Fee-Based)



Jan 23, 2024, 09:00am EST

1. It's a fast-growing threat.

3. It's difficult to detect.

2. It's highly targeted.



Use of large language models (LLMs) to create malicious scripts.

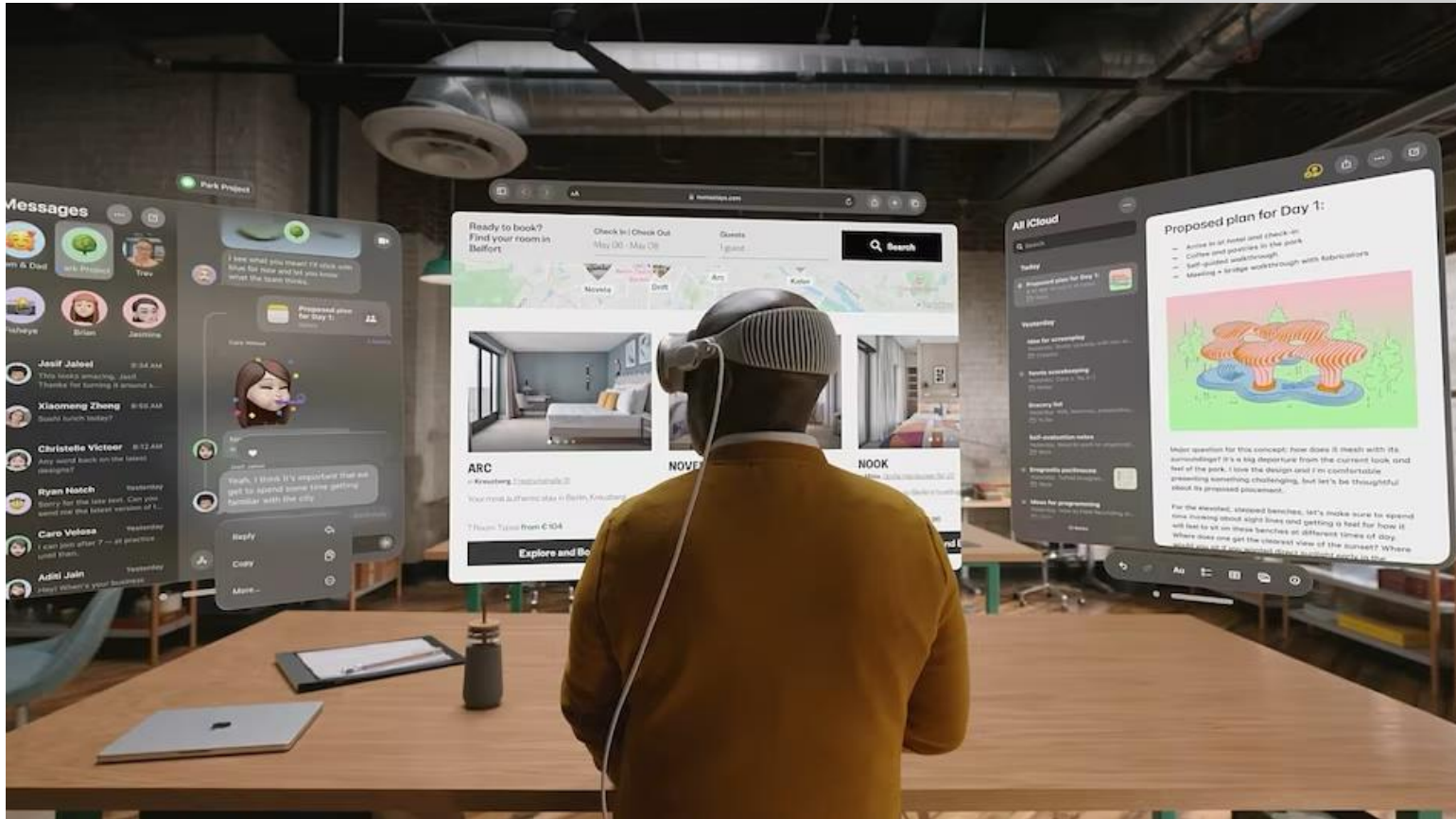
Example: AI-generated VBScript & JavaScript detected by HP researchers.

Capabilities:

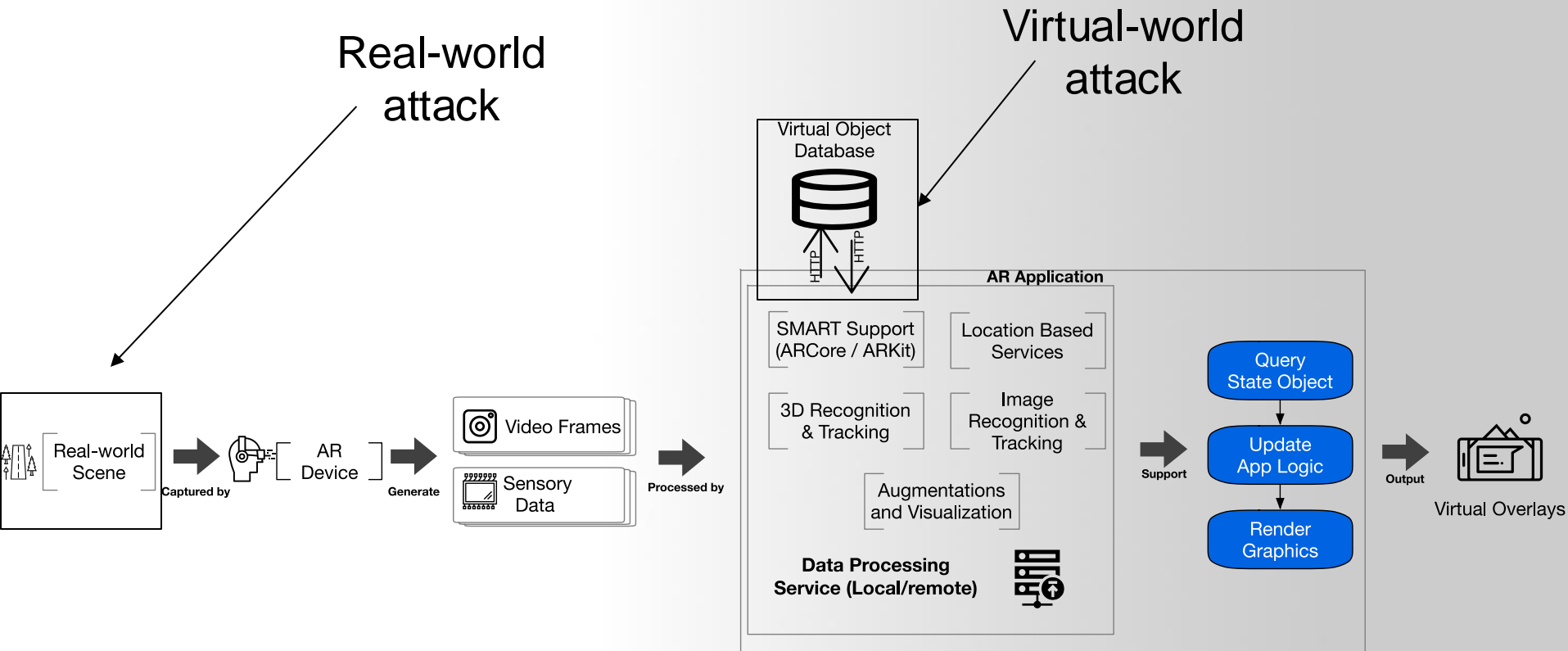
- Infect systems.
- Modify settings.
- Evade antivirus detection.

Why do people write malware?

- Future...
 - Control your Life



Our project –AR Security



Why analyze malware?

- Detect and respond to intrusions
 - Threat analysis
 - Host & Network signatures
 - What's the damage?
 - Who/What is infected?
 - Threat prevention
 - Threat removal

Top computer security conference --- The Big 4

ACM Conference on Computer and Communications Security (CCS)

About CCS

The ACM Conference on Computer and Communications Security (CCS) is the flagship annual conference of the Special Interest Group on Security, Audit and Control (SIGSAC) of the Association for Computing Machinery (ACM). The conference brings together information security researchers, practitioners, developers, and users from all over the world to explore cutting-edge ideas and results. It provides an environment to conduct intellectual discussions. From its inception, CCS has established itself as a high-standard research conference in its area.

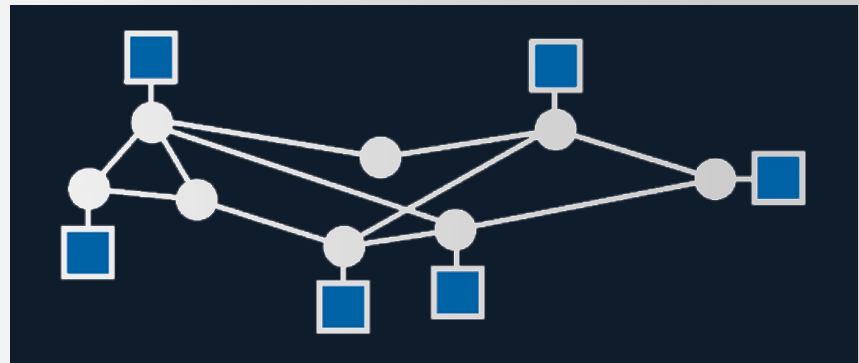
IEEE Symposium on Security and Privacy (S&P)

Since 1980, the IEEE Symposium on Security and Privacy (S&P) has been the premier forum for the presentation of developments in computer security and electronic privacy, and for bringing together researchers and practitioners in the field.



ISOC Network and Distributed System Security Symposium (NDSS)

The Network and Distributed System Security Symposium (NDSS) fosters information exchange among researchers and practitioners of network and distributed system security. The target audience includes those interested in practical aspects of network and distributed system security, with a focus on actual system design and implementation. A major goal is to encourage and enable the Internet community to apply, deploy, and advance the state of available security technologies.



Usenix Security Symposium (USENIX)

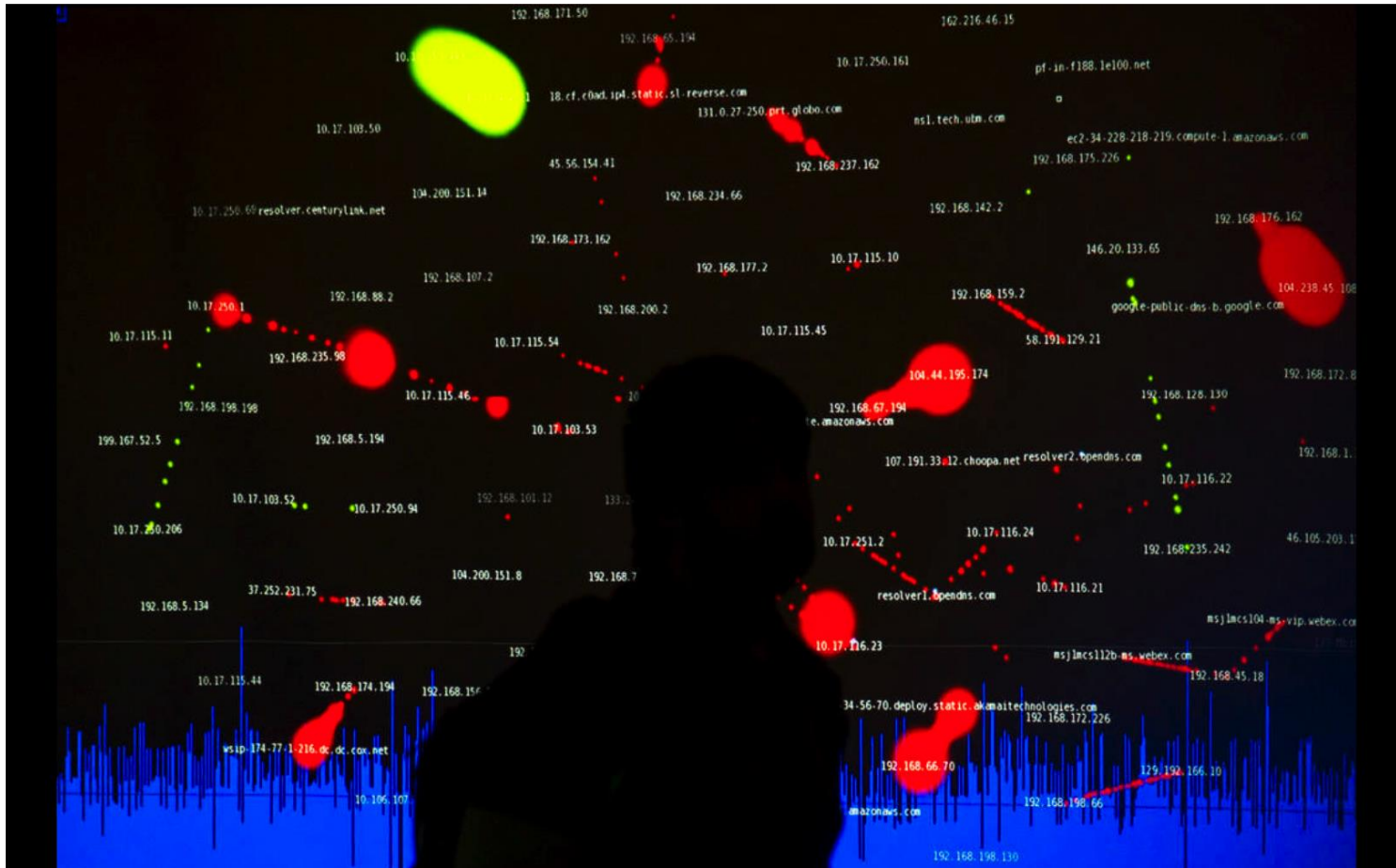
The USENIX Security Symposium brings together researchers, practitioners, system administrators, system programmers, and others interested in the latest advances in the security and privacy of computer systems and networks.

- **Top Security Conference for Hacking**

- **Black hat USA**
- **DEFCON**



DefCon, Black Hat bring extra cybersecurity concerns to Las Vegas



A Black Hat tech associate works in the network operating center (NOC) during the Black Hat information security conference at Mandalay Bay, Wednesday, July 26, 2017, In Las Vegas. Richard Brian Las Vegas Review-Journal



Q & A

