CS 501
Introduction to Malware, Threat Hunting and Offensive Capabilities Development

Course Developers
Kai Bernardini Winnona DeSombre

Instructors
Kai Bernardini (kaidb@bu.edu)

Course Description
The class introduces students to the wild world of offensive capabilities development and cyber threat hunting by taking on the role of both attacker and defender to better understand various stages of cyber attacks. Focusing on the Windows operating system, students will create and analyze malware in the context of combating a simulated threat actor APT-ChonkyBear in addition to creating their own tools to emulate their capabilities.

PreReqs:
Required: CS 210, 237, 391 (computer systems, probability in computing, intro to cybersecurity,)
Recommended: CS 558 or EC 521
Relevant Skills: Python, x86 (32/64) Assembly C/C++, bash comfort with Linux + Windows.

Grading:
Subject to change:
Class Participation: 5%
Scribe: 5%
Written/Coding Assignments: 20%
Reverse Engineering Assignments: 20%
Capstone Project: 50%

Assignments
Assignments in this class are divided into one of three primary categories:

Malware Reverse Engineering
Each assignment consists of a new epoch of malware sent to students highlighting a new technique to analyze. It will be their job to reverse engineer the new implant, detail its functionality, and identify attacker infrastructure.

Threat Intelligence
The primary goal of the defenders is to perform attribution and protect against future attacks.Students will use their technical findings to produce an intelligence report on the new sample. Emphasis is placed on how the students describe the technical details of the implant, possible tactical objectives of the adversary, and any opsec failures that can be leveraged for

attribution. From there students will make recommendations for defensive countermeasures using various techniques introduced in the course.

Malware Development

On the offensive side, students will work to recreate capabilities observed within new epochs of malware that can be integrated into their own Command and Control (C2) framework. For more on this, see Capstone

Capstone

This class will guide students through the creation of their own production ready Remote Administration Tool (RAT) and Command and Control (C2) team server. Each component of the capstone will be introduced as an offensive homework assignment, and will be integrated into the framework over the course of the semester. Ambitious students are encouraged to get involved with Porchetta Industries to release their tool as sponsorware.

Tentative Course Schedule

Lecture #	Date	Topic (tentative)
0	09/02/2021	Introduction To the Course
1	09/07/2021	Threat Hunting 101
2	09/09/2021	C++, Win32 (1)
3	09/14/2021	C++, Win32 (2)/ x86-64
4	09/16/2021	Malware Basics, Static/Dynamic Analysis
5	09/21/2021	Initial Access Payloads
6	09/23/2021	YARA, hunting and all that
7	09/28/2021	Introduction to C2, RPC, Flask
8	09/30/2021	C2 Engineering, Databases, Messaging, Clients
9	10/05/2021	Cryptography 1
10	10/07/2021	Cryptography 2
11	10/12/2021	Windows Internals 1
12	10/14/2021	Windows internals 2
13	10/19/2021	Windows internals 3
14	10/21/2021	Windows internals 4
15	10/26/2021	Persistence, looting, spreading
16	10/28/2021	Reflective DLL injection
17	11/02/2021	Packers, code obfuscation, Process Injection
18	11/04/2021	Injection (1)

19	11/09/2021	Injection (2)
20	11/11/2021	Userland Hooking (1)
21	11/16/2021	Userland Hooking (2)
22	11/18/2021	Selected topics: Pivots
23	11/23/2021	Selected topics: Defense Evasion (1)
24	11/30/2021	Selected Topics: Defense Evasion (2)
25	12/03/2021	Selected topics: C2 Channels
26	12/07/2021	Selected topics: AMSI, hooking userland hooks
27	12/09/2021	Selected topics: COFF, general loaders
28	TBD	Capstone Presentations and Poster Session (instead of a final)

References:

There are no mandatory textbooks for this course. Required readings will consist of blog posts, or source code. Below are several references that will be relevant to various homework assignments

- Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software 1st Edition
- Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation 1st Edition
- Operator Handbook: Red Team + OSINT + Blue Team Reference
- Rtfm: Red Team Field Manual 1.0 Edition
- Blue Team Field Manual (BTFM)
- http://www.harmj0y.net/blog/empyre/building-an-empyre-with-python/
- https://vx-underground.org
- https://github.com/yeyintminthuhtut/Awesome-Red-Teaming