EMET Introduction

Craig Jacquez: cjacquez@servit.net

EMET Introduction

What is EMET?

How much does it cost?

How do I get it?

Why use it?

Mitigation Types?

EMET Introduction

What is EMET?

EMET is Microsoft's

Enhanced Mitigation Experience Toolkit (freeware)

EMET Introduction

How much does it cost?

Acquire=free -> your time & resource to download/install/configure

EMET Introduction

How do I get it?

http://microsoft.com/emet

EMET Introduction

What does EMET do?

Stops Malware: improperly formatted file/content causes computer to run code(attackers program)

EMET Introduction

Attackers use the web, email & other tricks to allow a program or user to open Word, Excel, PowerPoint, PDF & other documents

EMET Introduction

EMET provides zero-day, buffer overflow and other memory corruption attacks.

EMET protection is not the same for every version of Microsoft Windows

EMET Introduction

MITIGATIONS

----------SYSTEM WIDE----------

DEP-Data Execution Prevention

SEHOP-Structured Exception Handler Overwrite Protection

ASLR- Address Space layout Randomization

----------Application----------

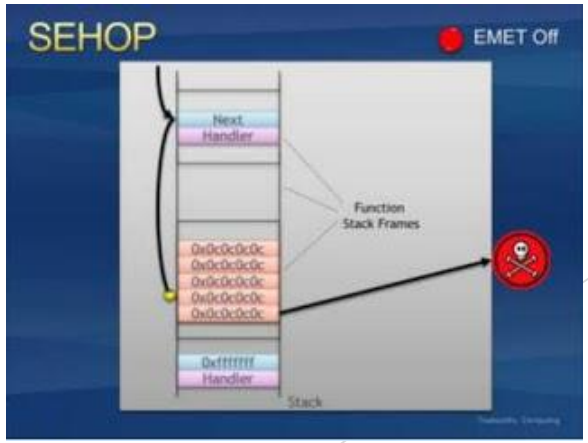
Pinning- Certificate Trust

Heapspray Allocation

EAF- Export Address Table Access Filtering

ROP – Return Oriented Programming

ASR – Attack Surface Reduction



EMET Introduction

MITIGATIONS - continued

----------Application-continued----------

EAF- existing Export Address table Filtering

EAF+

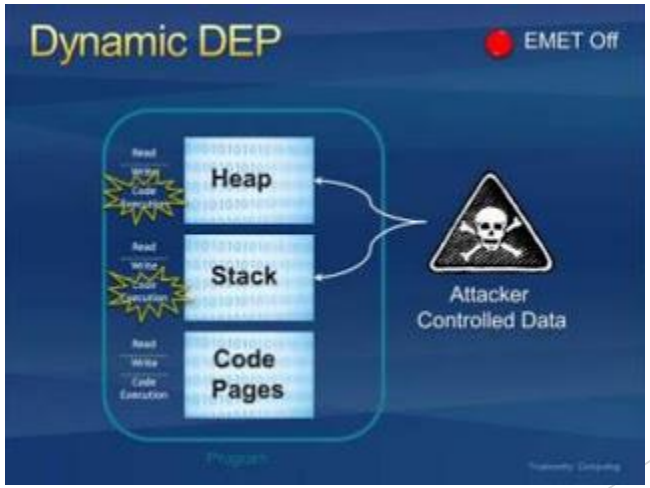
Load Library

Memory Protection

Simulate execution flow

Stack pivot

Caller checks



EMET Introduction

Thanks for your time.