Jukka Ruotsila

Implementing Microsoft Enhanced Mitigation Experience Toolkit in a Corporate Environment

Proof of Concept

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Thesis

April 29, 2016

Metropolia

Author	Jukka Ruotsila
Title	Implementing Microsoft Enhanced Mitigation Experience Toolkit in a corporate environment: proof of concept
Number of Pages	40 pages + 1 appendix
Date	April 29, 2016
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Computer Networks and Telecommunications
Instructor(s)	Tarmo Anttalainen, Principal Lecturer

The implementation and functionality of Microsoft Enhanced Mitigation Experience Toolkit (EMET) is studied in this bachelor's thesis. The goal in this study was to test installation and log gathering of the tookit using centralized management. Functionality tests were also done to find out if there are incompatibilities, such as crashing or slowing down of applications.

To perform the tests, EMET was installed for a week on Windows 8.1 and Windows 10 systems. Normal work routines were carried on, but the systems were monitored closely. In addition, twenty specified tests using normal office applications were done.

The settings for EMET were created using a graphical user interface of a system that was connected to domain controller, so the settings could directly be saved on the server. Initially the settings were identical for all operating system versions.

Windows Management Instrumentation scripts were used to target the settings which allows unique settings for different operating system versions. Unique settings are also allowed if the operating system is a workstation or a server. The same method was used to target the remote installation only on supported systems.

Installation and creation of settings was simple and fast. Problems regarding them did not come up with either tested Windows operating system. No problems were noticed with log gathering either.

The compatibility tests, which lasted for a week, did not indicate any larger issues with either operating system version. Not a single crash was seen. Slowness was noticed in one test out of twenty. Based on the results, EMET could be implemented more extensively.

Keywords	EMET, Security

Tekijä Otsikko Sivumäärä Aika	Jukka Ruotsila Microsoft Enhanced Mitigation Experience Toolkit -apu-ohjelman käyttöönoton konseptitestaus yritysympäristössä 40 sivua + 1 liite 29.4.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot ja tietoliikenne
Ohjaaja	Yliopettaja Tarmo Anttalainen

Insinöörityössä tutkittiin Microsoft Enhanced Mitigation Experience Toolkit -työkalun käyttöönottoa ja toimintaa yritysverkossa. Tulosten perusteella tehtäisiin päätös laajemmasta käyttöönotosta. Tavoitteena oli testata tuotteen asennus ja lokitietojen keräys keskitetyn hallinnan kautta. Lisäksi testattiin, aiheuttaako työkalu yhteensopivuusongelmia, kuten ohjelmien kaatumista tai hidastumista. Työkalu oli asennettuna viikon ajan, jolloin työskenneltiin tavanomaiseen tapaan mutta tarkkailtiin järjestelmän toimintaa. Lisäksi tehtiin 20 erikseen määritettyä, tavallista toimisto-ohjelmien toimivuutta testaavaa koetta.

Työkalun asetukset tehtiin graafisella käyttöliittymällä koneella, joka oli yhteydessä toimialueen ohjauspalvelimeen, jolloin asetukset saatiin tallennettua suoraan palvelimelle. Asetukset tehtiin aluksi samanlaisiksi kaikille käyttöjärjestelmäversioille.

Asetukset kohdennettiin Windows Management Instrumentation -skriptien avulla, jolloin saadaan yksilöityä asetukset eri käyttöjärjestelmän versioille,ja sen perusteella, onko käyttöjärjestelmä työasema vai palvelin. Samaa tekniikka käytettiin myös kohdistamaan etäasennus vain tuettuihin Windowsin versioihin.

Asennus ja asetusten luominen oli helppoa ja nopeaa. Niiden kanssa ei ilmaantunut ongelmia kummassakaan testatussa käyttöjärjestelmässä: Windows 10:ssä tai Windows 8:ssa. Lokien keräyksen kanssa ei myöskään ollut ongelmia.

Viikon kestäneessä yhteensopivuustestauksessa ei tullut esille suurempia ongelmia kummallakaan käyttöjärjestelmäversiolla. Yhtäkään ohjelman kaatumista ei esiintynyt. Hidastumista havaittiin yhdessä kokeessa kahdestakymmenestä. Testien perusteella voisi käyttöönottoa laajentaa.

Avainsanat	EMET, Tietoturva, konseptitestaus

Table of contents

Abbreviations

API	Application Programming Interface
APT	Advanced Persistent Threat
ASLR	Address Space Layout Randomization
ASR	Attack Surface Reduction
BHO	Browser Helper Objects
C&C	Command and Control
CKC	Cyber Kill Chain
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
DEP	Data Execution Prevention
DMZ	Demilitarized Zone
DOS	Denial of Service
DRM	Digital Rights Management
EAF	Export Address Filtering
EAT	Export Address Table
ELAM	Early Launch Antimalware
EMET	Enhanced Mitigation Experience Toolkit
ENISA	European Network and Information Security Agency

GPO	Group Policy Objects
HIPS	Host-based Intrusion Prevention System
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IE	Internet Explorer
IOC	Indicators of Compromise
IP	Internet Protocol
IPS	Intrusion Prevention System
LAN	Local Area Network
LM	Lan Manager
LSA	Local Security Authority
MS	Microsoft
NAP	Network Access Protection
NTLM	NT Lan Manager
OS	Operating System
OU	Organizational Unit
P2P	Peer-to-peer
PDF	Portable Document Format

PLC	Programmable Logic Controller
RAT	Remote Administrations Tool
ROP	Return-oriented Programming
SCADA	Supervisory Control and Data Acquisition
SEHOP	Structured Exception Handling Overwrite Protection
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SP	Service Pack
SRP	Software Restriction Policies
SSID	Service Set Identifier
TCP	Transmission Control Protocol
UAC	User Account Control
UEFI	Unified Extensible Firmware Interface
UNC	Uniform Naming Convention
USB	Universal Serial Bus
VBA	Visual Basic for Applications
WLAN	Wireless Local Area Networks
WMI	Windows Management Instrumentation

1 Introduction

This thesis describes how to implement Microsoft Enhanced Mitigation Experience Toolkit (EMET) with centralized management and how to log into a corporate environment. EMET 5.5 changes the way central configuration is made, making it easier to take it into use and to configure it compared to older versions of EMET. It also brings support for Windows 10. [1.]

Targeted and complex sophisticated Advanced Persistent Threats (ATP) are hard to detect and prevent but a defence and security company called Lockheed Martin has developed a seven step Cyber Kill Chain (CKC) to mitigate the risk. The fourth step of the chain is exploitation. EMET works in that step by mitigating memory corruption exploits. All phases of the CKC are covered from attacker and defender side with additional techniques taken from the European Network and Information Security Agency (ENISA) Proactive Detection of Network Security Incidents guide. [2;3.]

Studying how EMET behaves with non-malicious documents gives information on how to configure the settings so that it does not cause any loss of productivity for normal users. Most studies around EMET have concentrated on how to bypass it or how effective it is against a set of exploits. [4;5.]

Spear phishing, which is commonly executed by sending emails that usually contain Microsoft Office and PDF documents or links to websites containing malicious code, are the most common methods of delivering an exploit. EMET has proved to be effective against those types of exploits and it is free, so all companies and home users should install it. [4.]

Evolvement of Windows security features as new versions of the operating system have been released, and they are covered to give historical information on how Microsoft has tried to tackle the ever evolving threat landscape. Three well known and documented real world attacks are covered to show how the attacks were carried out and if EMET could have helped in mitigating the attack. [6;7;8.]

This study was done for ProPeople Suomi Oy. The goal was to find out if EMET 5.5 runs stable enough so that it could be added into the portfolio of security services provided by the company.

2 Emergency Experience Mitigation Toolkit

Enhanced Mitigation Enablement Toolkit is a free hardening tool by Microsoft which mitigates memory corruption exploitation by enforcing protection with several features like Data Execution Prevention (DEP), Mandatory Address Space Layout Randomization (ASLR), Structured Exception Handling Overwrite Protection (SEHOP) and Export Address Filtering (EAF). The features have been present natively in the Windows operating system since Windows Vista, but are not necessarily taken into use by applications and have required expert knowledge, such as how to modify Windows registry. EMET simplifies implementation of the protection features, enforces them and also gives a more granular view for protections per application. It does not require constant updating, because it is behavior-based unlike most anti-malware and IPS solutions, which are signature-based and require daily updates. [1.]

EMET is effective against exploits in documents. Jarno Niemelä has tested the effectiveness in his study and it had 100% success against all 927 document exploits [4].

EMET has been bypassed by security researchers like Rene Freingruber who proved in his study that EMET can be bypassed even if all protections are enabled. He used a vulnerability in Mozilla Firefox, and by bypassing DEP and ASLR, he was able to launch shellcode [5]. EMET mitigation techniques by themselves are not strong enough for targeted exploits, but the combination of them like DEP + ASLR is much harder to bypass [5;9]. A security company called FireEye found a vulnerability in EMET that allows disabling all protections, leaving EMET doing nothing useful [10].

EMET was publicly released in October 2009 with a few of the still currently used key protections available. The most recent version is 5.5, which adds support for Windows 10 and fixes some issues in the product, such as the vulnerability found by FireEye to disable all protections. EMET 1.x was a command line utility, but a graphical user interface (GUI) was introduced in 2.x and it was similar to the ones still used in the most recent version [10]. Table 1 lists the EMET versions, detailing which new functionalities are introduced in each version.

Table 1. EMET release history, protections and OS support per version.

Version	Released	DEP	SEHOP	Nullpage	Heapspray	ASLR	EAF	ROP	EAF+	Certificate Trust	OS Support
1.x	10/2009	X	X	X	X						XP, Vista, W7, W8
2.x	09/2010	X	X	X	X	X	X				XP, Vista, W7, W8
3.x	05/2012	X	X	X	X	X	X	X			XP, Vista, W7, W8
4.x	04/2013	X	X	X	X	X	X	X		X	XP, Vista, W7, W8
5.x	07/2014	X	X	X	X	X	X	X	X	X	Vista, W7, W8
5.5	01/2016	X	X	X	X	X	X	X	X	X	Vista, W7, W8, W10

EMET is incompatible with several software. Microsoft maintains an official web document about incompatibilities and there is also MS forum where users can post information about problems with EMET. Programs such as anti-malware, debuggers, digital rights management (DRM) handling programs, software using anti-debugging, obfuscation or hooking and some host-based IPS are known to have issues with EMET. The website about incompatibilities has not been updated to include version 5.5, but comparing the list to the configurations in a running EMET shows that they are very similar. [11;12.]

2.1 Data Execution Prevention

Data Execution Prevention is a security feature which marks all memory locations for a process non-executable unless it is explicitly marked as executable, so that an attack which tries to write executable code in the non-executable space and then run it, fails. DEP is enforced at the hardware level so the processor marks the address spaces non-executable. DEP support was introduced in Windows XP SP2 and has been supported in every Microsoft OS since then. DEP is always enabled in 64-bit processes running on 64-bit Windows and it cannot be disabled. Virtual machines do not support DEP as it

requires support from the Central Processing Unit (CPU). It is not required to disable DEP for virtual machines, but it just does not do anything.

DEP can also be configured to run system-wide on 32-bit OSs with four separate options.

1. Opt-In. DEP is enabled if processes explicitly opt-in to DEP. This is the fefault configuration for Windows client OS.

2. Opt-Out DEP is enabled for all processes except the ones that have explicitly opt-out of DEP. This is the default configuration for Windows Server OS.

3. Always On. DEP is enabled for all processes even if the process does not support it.

4. Always Off. DEP is disabled for all processes.

There are known issues if DEP has been configured as "Always On", such as BitLocker full disk encryption can require a recovery password in the first reboot after changing the option if it was not suspended while the change took place. Google Talk and Microsoft Office Web Components also have issues with the same setting. [1;13.]

2.2 Mandatory Address Space Layout Randomization

Address Space Layout Randomization is used for randomizing the addresses which processes use to make it harder for an attacker to find which memory addresses are allocated to an application. ASLR has opt-in or disabled as the system-wide settings. "Always On" is a hidden option because it is unsafe, so it requires a change in the Windows registry and can cause the OS to crash on start-up. [1.]

2.3 Structured Exception Handler Overwrite Protection

Structure Exception Handler Overwrite Protection protects against stack overflow exploitations. An attacker can overwrite the handler pointer of an exception record on the stack. When an exception happens, the OS goes through the exception record chain calling all the handlers. The attacker controlled record will make the OS to jump to where the attacker wishes, allowing the attacker to control the execution flow. SEHOP is supported for 32-bit processes only. SEHOP has the same system-wide options as DEP. [1.]

2.4 Attack Surface Reduction

Attack Surface Reduction allows controlling which modules or plugins are used with applications such as Microsoft Office applications loading Adobe Flash. Adobe Flash vulnerability in Microsoft Office caused RSA breach, which is covered in chapter 5.2 [9]. Internet Explorer can be configured to load plugins only in certain zones. An Internet zone can be much more restrictive about which plugins can be loaded compared to Intranet zone, allowing an internal web application to work. ASR supports basically just MS applications [1]. Chrome for Work supports centralized deployment and configuration so it can be controlled the way Internet Explorer is controlled with GPO templates or EMET [14].

2.5 Heapspray

A heapspray attack means that an exploit writes its shellcode to as many addresses in the heap memory as it can, so it could get to the shellcode by guessing, because sometimes the exploit does not know where the shellcode resides. The areas of memory that EMET has pre-allocated are visible when opening EMET application settings and selecting “Show All Settings”. The attacker could then bypass the protection by selecting any area of the memory that is not allocated and is available for such an attack. [1.]

2.6 Return Oriented Programming

Return-oriented Programming exploits code that is already loaded into the memory region of the attacked application or the OS. There are several ROP mitigations in EMET and some work only in 32-bit processes [1].

- Load library checks for monitoring all calls to LoadLibrary API and blocks loading libraries from Uniform Naming Convention (UNC) paths (\\xyz\malware.dll) [1].

- Memory protections checks: Changing stack memory to be executable is prevented by EMET. A stack should just store data [5].

- Caller checks: Reaching critical function is only allowed via CALL instructions and not via RET instructions [1].

- StackPivot checks: A stack pointer should point to a value in stack memory, but an attacker could try to shift the pointer to heap memory which is controlled by the attacker [5].

2.7 Nullpage

The nullpage mitigation prevents null deference issues in user mode. EMET preallocates and takes ownership of the null page, so that the attacker cannot change the memory page [1;5].

2.8 Export Address Table Access Filtering (EAF)

EAF mitigation filters shellcode's read access to Export Address Table (EAT). EAT contains information about the memory locations of loaded modules and which API they use. Typically kernel32.dll, ntdll.dll and kernelbase.dll are the target of the attackers because they contain such an API that allows control over the entire system. [1;5.]

2.9 Export Address Table Access Filtering Plus (EAF+)

EAF+ mitigation adds a few detections to EAF. It detects if the stack register is out of the allowed boundaries, a mismatch of stack and frame pointer registers, memory read access to EAT of the typical target libraries described in chapter 2.8 from specific modules and memory read accesses to the MZ/PE header of specific modules. The modules pre-configured in EMET 5.5 are mshtml.dll, flash*.ocx, jscript*.dll, vbscript.dll and vgx.dll. [1.]

2.10 Bottom-up Randomization

Bottom-up randomization mitigation randomizes the base address of bottom-up memory allocations such as heaps and stacks, so that the attacker cannot use the default or previously used value [1].

2.11 Untrusted Font Mitigation

Untrusted font mitigation is supported only on Windows 10. It enables system-wide and application-wide blocking of font files loaded outside %windir%\Fonts directory. The font file parsing process has some known Escalation of Privilege (EOP) attacks [1].

3 Microsoft Windows

The Windows NT product family was first launched in 1992. The first version was 3.1 which is also its kernel version to the latest Windows 10 with kernel version 10. Windows versions previous to Windows XP have separate OS families for home and small business users. The Windows 9x family is for home and small businesses and the Windows NT family is for enterprises. Kernel architecture is different between the 9x and the NT families. Starting from Windows XP, Microsoft has only provided OSs based on one kernel architecture for 32-bit and one for 64-bit OSs, with the differences being in the features the OSs provided. The Home versions have less features than Enterprise versions such as disk encryption and possibility to join a Windows domain. The NT architecture is layered with separate user and kernel modes, while the Windows 9x architecture was monolithic with everything running in kernel mode. [15.]

3.1 Application and Kernel Modes

Applications and user-mode drivers run in the user mode. The OS provides a process, allocates virtual address space and private handle table for each application and user-mode driver. This allows the applications to run isolated from each other, so if the application or user-mode drivers crashes, it doesn't crash other applications or the OS. The user mode process cannot access virtual addresses of the OS in normal circumstances. [15.]

Kernel-mode code shares a virtual address space, so drivers running in kernel-mode are not isolated from each other or from the OS kernel. If a kernel mode driver crashes, then the whole operating system crashes [15]. Kernel-mode rootkits are especially harmful because they can be hiding themselves and other parts of malware from anti-malware scanners when running at the same security level as the anti-malware drivers. Full OS reinstallation is normally the only action after infection with a kernel-mode rootkit [16]. Starting from Windows Vista, all 64-bit operating systems have only accepted digitally signed drivers, making it harder to add a kernel-mode rootkit to the system. Digital signatures can be stolen though to sign malicious drivers like in the case of Stuxnet [6]. Windows 10 changed the policy so that only drivers signed by Windows Hardware Dev Center Dashboard are approved [17].

3.2 Windows Versions

Windows versions from Windows NT 4.0 to Windows 10 are discussed from security perspective in this chapter. This chapter also deals with how they have developed in each iteration of the product family.

3.2.1 Windows NT

Windows NT 4.0 released in 1996 was the first widely adapted Microsoft enterprise level operating system. It brought the shell from Windows 95 allowing a better graphical user experience and system policies for restricting actions. Even though the extended support for Windows NT 4.0 SP6a ended in 2004, there are still systems in health care sector running the OS [18]. NT 4.0 does not support USB without a third party utility, so the computers running it are at least safe from malicious pen drives [19].

3.2.2 Windows 2000

Windows 2000 was released in 2000 with NT kernel version of 5.0 for both workstations and servers.

Windows 2000 provided several security enhancements compared to NT 4.0 such as Kerberos 5.0 as the authentication protocol, IPsec support for encrypting network traffic, Encrypted File System and a more granular control of settings with Active Directory group policies. There are also pass-the-hash vulnerabilities with NT Lan Manager (NTLM) which was the previous authentication protocol along with an even older Lan Manager (LM) before Kerberos. However, NTLM is still required for backwards compatibility with older Windows versions, some devices and software and when using local credentials for authentication. Kerberos is vulnerable for pass-the-ticket attacks, but the attacks have a more limited time span because tickets expire by default in 10 hours. The password hashes change only when the password is changed. Extended support for Windows 2000 SP4 ended in July 2010. [20;21.]

3.2.3 Windows XP / Windows Server 2003

Windows XP 32-bit was released in 2001 with NT kernel version 5.1. Windows XP 64-bit and Windows Server 2003 were released in 2003 with the kernel version 5.2.

Extended support for XP 32-bit SP3 ended in April 2014, which was widely reported by the press, because at the time, and still currently, many XPs are used in production systems, health care equipment and ATMs, for example. Some of them use Windows XP embedded the support of which ended in January 2016. The support for Windows XP 64-bit, Windows 2003 Server SP2 and Windows 2003 Server R2ended in July 2015.

XP Security enhancement includes disallowing use of blank password for user account, forcing use of Guest account when connected over the network and Software Restriction Policies. An Internet connection firewall with inbound traffic filtering was added in SP2. SRP is a tool for blacklisting, which means preventing unwanted software SRP can also do whitelisting, which means that only allowed software can run. [20;22.]

3.2.4 Windows Vista / Windows Server 2008

Windows Vista was released in 2007 with NT kernel version 6.0 and Windows Server 2008 was released in 2008 with the same kernel version.

User Account Control (UAC) was introduced in Vista. The UAC enforces the users to work most of the time as a standard user and they are prompted if elevated privileges are needed, for example, if new software or devices are installed to the system. Users that are part of the local administrators' group get a prompt to allow or disallow actions, and standard users need to provide administrator level credentials for UAC and allow or disallow the actions. This mitigates drive-by-downloads or unknown malware installations. It also virtualizes some parts of the file system and the registry to allow running legacy software that might otherwise crash if the legacy software could not reach operating system files or registry keys. [30.]

Automatic Windows updates can be enforced with GPO, so that the user cannot interfere with updating. Windows Update was separated from Internet Explorer to its own process, so the updating worked even if Internet Explorer was broken.

Network Access Protection (NAP), which is a health check for the clients, checks whether the computers running NAP have the latest security updated or a running and up-to-date anti-malware, for example. Network access can then be restricted so that clients which are not compliant can only connect to servers which allow fixing the issues. [30.]

The Windows firewall in Vista supports also outbound filtering while the Windows firewall in XP could only filter inbound traffic. This can be useful for blocking unwanted peer-to-peer (P2P) applications, for example.

BitLocker full disk encryption is included in the Ultimate and Enterprise versions of Vista. If a laptop is lost or stolen, all the data remains secure if it is encrypted and a strong enough algorithm and passphrase are used. [30.]

3.2.5 Windows 7 / Windows 2008 Server R2

Windows 7 was released in 2009 with kernel version 6.1 and Windows 2008 R2 was released at the same time with the same kernel version.

UAC user experience was improved in Windows 7 so that the prompting for elevated user rights was reduced by a great number. Excessive prompts caused unhappy users Therefore many administrators were forced to disable UAC completely with Windows Vista. [31.]

BitLocker full disk encryption implementation became simpler with Windows 7 because Vista required drive partitions for BitLocker to be made before installing the OS. Windows 7 can create partitions for BitLocker when it is enabled and without having to reinstall the whole OS. BitLocker To Go allows encrypting USB pen drives and USB disks as they can easily be lost or stolen.

AppLocker lets administrators select which applications, scripts or libraries are allowed to run with the possibility to add exceptions to its rules. It has an audit-only mode for testing the configuration before switching to enforcement mode. AppLocker replaces SRP introduced in Windows XP. [32.]

3.2.6 Windows 8 / 8.1 / Windows Server 2012 / 2012 R2

Windows 8 was released in 2012 with kernel version 6.2. Windows Server 2012 was released at the same time with the same kernel version. Windows 8.1 was released in 2013 with kernel version 6.2.Windows Server 2012 R2 was released at the same time with the same kernel version.

Windows Defender anti-malware program is shipped with the OS so there is protection against malware from the moment of the OS installation and without having to install a third-party anti-malware. Automatic updates are enabled by default, which removes the need for a user to start the update process.

Secure Boot utilizes Unified Extensible Firmware Interface (UEFI) to prevent bootkits, which are malware that load before Windows starts and are therefore unrecognized by the OS. UEFI verifies the integrity of Windows bootloader before it is loaded.

Trusted Boot checks for the integrity of Windows Startup files. Early Launch Antimalware (ELAM) allows antimalware to be loaded before any software that Microsoft has not written.

SmartScreen, which comes with Internet Explorer (IE) 8, controls how applications downloaded from websites, which are not classified as safe by reputation services, are allowed to be executed. [33]

3.2.7 Windows 10

Windows 10 was released in 2015 with the kernel version 10.

Credential Guard isolates and virtualizes Windows Local Security Authority (LSA). That allows domain credentials to be isolated from the running OS and by doing that mitigating Pass-the-Hash and Pass-the-Ticket attacks [34].

Microsoft Edge web browser does not support ActiveX or Browser Helper Objects (BHO), which could both be used for malicious actions. IE is still installed on Windows 10 for backwards compatibility [34].

Device guard utilizes virtual isolation for Code Integrity service and it protects the system core and the processes and the drivers running in kernel mode. All kernel mode drivers must be signed by Microsoft as explained in chapter 3.1. All running code must be signed by trusted signers which is configurable in Code Integrity policy. Basically this can only be used in a very static environment [34].

5 Typical Cyber Kill Chain for a Targeted Attack

There is typically an order in which a targeted attack is performed and CKC gives information on how a typical attack chain is constructed. The chain consists of seven steps following each other to allow the next step in the chain to work. Different parts of the chain require different approaches for proactive detection and incident response as shown in figure 1. The steps are explained in more detail in following chapters. [2;3.]

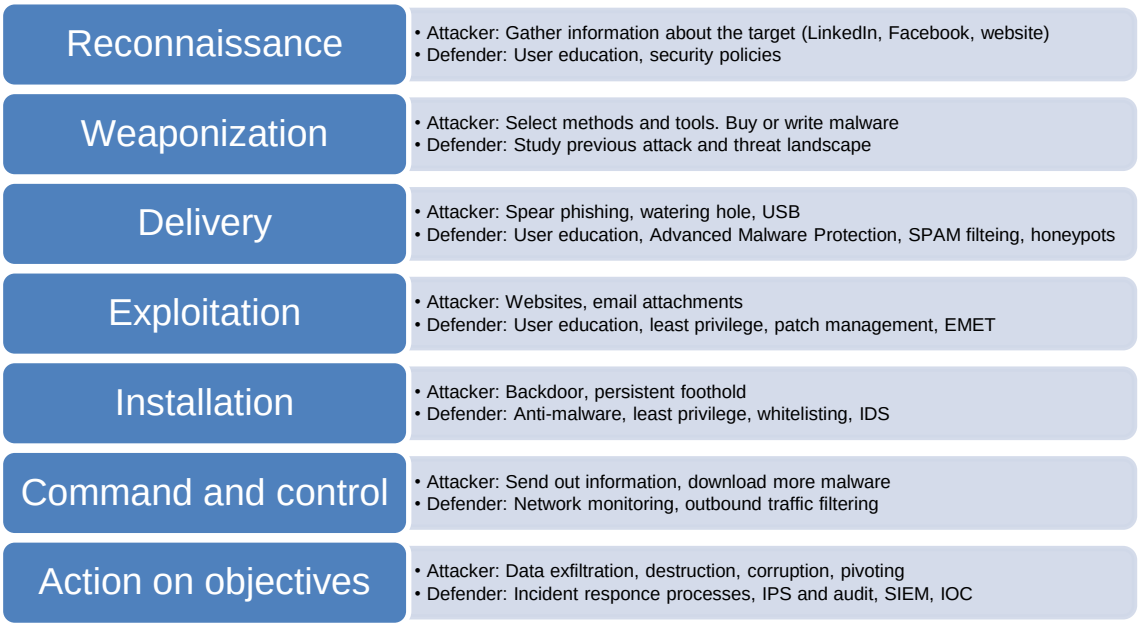

Figure 1. Lockheed Martin Cyber Kill Chain. Data gathered from Lockheed Martin and ENISA [2;3].

5.1 Reconnaissance

Attacker

Gathering data about the company and its people and systems is the key in information gathering. Names of interesting key personnel can be gathered from the company website, LinkedIn and other social media. These people can consist of CxO level directors and system administrators, who have access to several different IT systems. Social engineering like pretending to be from IT support and asking for a password over the phone can be used to fool people to provide information that the attacker can use.

Laptops, USB drives or confidential documents can be wrongly disposed or stolen. Internet facing servers and network equipment can be scanned to map the used software and version to see if there are possible vulnerabilities in them. Wireless Local Area Networks (WLAN) can be scanned by getting close enough for radio access. [2;3.]

Defender

Educating people on a regular basis on what information to give out on the Internet or over the phone is the best way to tackle social engineering. Equipment and document handling also needs to be covered regularly and always when a new employee starts in the company. There should be inventory of all the systems and what their patch level is with regular vulnerability and discovery scans to the network. WLAN SSID hiding does not really help so they should use strong security and rogue WLANs scanned or blocked with network technology. [2;3.]

5.2 Weaponization

Attacker

After finding out enough information about the target, the next stage is preparing ammunition, i.e. the methods and tools of attack. They can include malware specifically created for the victim, web pages hosting the malware and the exploit code and creating convincing looking emails. With enough resources the components of an attack can be custom made for the victim. Normally some generic exploits are used against vulnerabilities like buffer overflow to deploy a dropper, which is a malware component that loads itself into memory and then installs other parts of the malware. Exploit kits, which can attack several different products like Adobe and Java, are readily available. They do not require very deep understanding like coding skills. Different types of malware and attacks are also sold in the Dark Web, which is a separate network within the Internet, but can only be reached in a special way like using TOR, which is software for anonymizing traffic. [2;3.]

There can also be a component that connects to outside for downloading more parts of the malware and sending out information about the system, establishing Command and

Control (C&C). Malware can be obfuscated by changing the data to make it unreadable or hard to understand, by creating multiple permutations which all look a bit different to a anti-malware and testing against malware engines. These methods make it hard for anti-malware programs to find the malware using signatures, but a heuristic engine, which means a behavior based engine, could pick them up. [2;3.]

Defender

This part is hard for the defender, because there can only be guessing about what the actual weapons of attack will be, but by reviewing previous attacks and learning from them increases the readiness for future attacks. The timeline of malware creation and when it was used could provide information on whether it was custom made or readily available malware. Evolvement of the threat landscape should be studied to understand new techniques which malware use to avoid detection. [2;3.]

5.3 Delivery

Attacker

Targeted attacks can use several approaches for delivering the malware or exploit. Spear phishing means sending correct looking emails with sender impersonation to targeted individuals with the attention to lure them to a malicious website or opening a malicious attachment such as a PDF document using vulnerabilities in Adobe Reader. A case example is the RSA attack in 2011 which used an Excel spreadsheet sent to four individuals, using vulnerability in Adobe Flash. [2;3.]

A watering hole attack means inserting an exploit to a website usually used by the industry of the target or some website found out to be used frequently by the target in the reconnaissance phase. USB sticks can be dropped to a parking lot or some other place where personnel of the target company can find them, and because of the curious mindset of humans, there is a good chance that one individual will want to see what is on the removable storage. The individual might then plug it into a computer, which was likely the way the Stuxnet attack started. USB Rubber Ducky is a device that can emulate other devices, so while being inserted into a USB port, it can emulate the keyboard

and write malicious code to the computer. Not many companies block USB keyboards. [2;3;23.]

Defender

A network sandbox can be used to open up an attachment and running it in a contained environment to see if it has malicious functions. Some new malware can verify if they are running in a sandbox or in a real system, or just pause for some time doing nothing to avoid being captured. Web browsing can be secured more by user education, utilizing browser protection and hardening on host and implementing network IPS for scanning traffic. Monitoring of email and web logs can allow doing forensics in how the attack proceeded to understand and develop the security in the future. Honeypots, which are systems that look like real systems but exist only to fool attackers to attack on them and learn from the attack instead of real systems, can reveal how to prevent a real attack. [2;3.]

5.4 Exploitation

Attacker

After an exploit has been successfully delivered or the victim has been lead to a website which has the exploit, the exploit can take use of a vulnerability which can be known but which has not yet been patched or mitigated using other methods such as IPS or anti-malware signature.The exploit can also be a zero-day exploit, which means that there is a way to exploit a vulnerability but there is no patch to the vulberability yet. [2;3.]

Defender

User education is important to ensure caution with all emails. Because the emails can look correct and seem to come from a correct sender, it can be hard to distinguish spear phishing emails from normal ones. Removal of local administrative privileges could mitigate 85% of the 251 critical and 63% of all vulnerabilities in MS products in the year 2015 according to a research done by Avecto, which is a company offering solutions for removing administrator privileges [24]. The United States National Securi-

ty Agency (NSA) also recommends strict privilege management [26]. Patch management and vulnerability scanning for all software on all systems should be implemented on a monthly basis or more often [2;3].

Microsoft EMET works protecting the system at this step of the CKC by mitigating many of the memory corruption techniques used by the exploits [1].

5.5 Installation

Attacker

At the installation stage, the attacker usually installs a backdoor to the computer which allows monitoring the system or downloading more malware for other purposes. Windows processes which are started every time when the operating system starts or the registry locations which start applications at start-up are commonly used for keeping the malware loaded also after reboot, gaining a persistent foothold. File dates can be changed so that the files look to be old and installed with the OS, hiding the presence of the attacker. [2;3]

Defender

Anti-malware with modern heuristic engines might be able to pick up the malware if the malware touches some common locations or processes used by malware. Some could be picked up by signature based engines if the malware developer has not obfuscated or encrypted the malware, making it easier to recognize. Removal of administrator privileges prevents creating new processes or writing to any operating system keys in the registry or OS file locations on the file system. Host IDS, which monitors the system for new executable or configuration files, can trigger an alarm, especially if changes to Windows folders or registry is noticed. OSSEC is an open source host IDS which can be used for such a task. Whitelisting can prevent unknown, unsigned applications or applications signed by non-trusted authority from running. It is tricky to configure unless the systems are very static and there is only one way to update the systems. Several updaters lead to security issues with whitelisting as shown by Rene Freingruber. [2;3;5.]

5.6 Command and Control

Attacker

Command and control (C&C) is used to remotely do malicious activities to a victim such as sending out classified data or acting as a work horse for a botnet which do Denial of Service (DOS) attacks or mine Bitcoins. C&C network traffic commonly uses ports that are already open outbound like TCP 80 or TCP 443, which are used for normal web traffic. There are cases in which the traffic is encapsulated into Internet Control Message Protocol (ICMP) Ping traffic, which is normally used to check if some system is available in the network. An attacker can also download new malware through the channel. [2;3.]

Defender

Network monitoring with IPS systems might reveal C&C data, especially if the attacker is using known C&C servers. If C&C traffic is encrypted, it might be very hard to catch it, but as a best practise all outbound traffic should go through a proxy, which can be configured to filter the traffic going through it and which will also provide logging for forensics. NetFlow, which is a protocol for collecting, monitoring and analysing network traffic, could be used to see if there are anomalies in the network. SMTP traffic using port TCP 25, which is the default port that email servers use, should be blocked from all IP addresses except the email servers. [2;3.]

5.7 Action on Objectives

Attacker

The final stage of the chain depends on what the goal of the attack is. It might be stealing confidential data like with the RSA attack or several credit card number thefts. Pivoting, i.e. gaining more access in the network to more systems and getting higher privileges, is a common goal for attackers. Destroying the systems, which happened with Saudi Aramco and Ukraine Power Grid attacks, is another common goal. Modifying data, and by doing that destroying the system, which happened with Stuxnet, is yet

another common goal. The attacker can continue to run the attack until it gets noticed or he/she can try to remove any traces that the attack ever happened. [2;3.]

Defender

If the attack proceeds to the last stage of CKC, the amount of time it takes to detect the attack can define how wide the impact on the systems is. Incident response procedures should be available and developed to a good maturity level. IPS and auditing used together with a Security Information and Event Management (SIEM) system with correlation in place could reveal if something suspicious is going on, i.e. pointing out indicators of compromise (IOC). Low-and-slow attacks, when the attacker does something only every two weeks, can be very hard to detect and it might require very expensive and powerful systems. Forensics should be done as soon as possible after the attack is revealed so that all evidence can be gathered before it is wiped. [2;3.]

6 Attack Examples

Three well-known and documented attacks are analysed in this chapter to see if EMET could have helped in mitigating the attacks. All of them might have been stopped earlier if CKC was utilized. The disclosed information from the RSA attack was very likely used to attack Lockheed Martin, so CKC played a part in detecting the spin-off attack. [2;7;37.]

6.1 Stuxnet

Stuxnet is one of the most known malware documented. It targeted industrial control systems (ICS,) which are systems used in electric networks and production environments in Iran and possibly other countries. The goal of the malware was to reprogram programmable logic controllers (PLC) so that they would do what the attacker wished and to hide what was going on. [6.]

The most famous victim was the Natanz nuclear facility. Stuxnet had reprogrammed the PLCs so that they slowly broke the centrifuges and, by doing that, slowed down Iran's uranium enrichment. This created speculations that the attackers were from Israel and the United States, because they had interest in destroying Iran's ability to produce nuclear weapons. [36.]

It is believed that the infections started with a USB stick of an employee or a USB stick placed so that someone working at the facility picked it up, allowing the malware to enter an air gapped network, which means that it is completely isolated from other networks. It then infected Windows machines in the closed network and started looking for a machine which ran Siemens Step 7 ICS software. Stuxnet used a zero-day vulnerability in Windows and a vulnerability in Step 7. It also used drivers which had valid signatures by Realtek and JMicron, so they looked trustworthy to the OS. It remains unknown if the attackers had physically broken into the facilities of Taiwanese companies or remotely hacked and gained access to a private signing key. [6.]

The first versions of Stuxnet used Autorun, which is a feature in Windows that automatically starts content from removable media or network shares when connected, by actions defined in the file Autorun.inf. This is a feature that should be disabled according

to most system hardening guidelines. Later versions used a zero-day vulnerability in how Windows handles .lnk files. [6;35.]

When Stuxnet got a foothold on a system, it tried to spread to all Windows systems in the same Local Area Network (LAN) which makes it a worm. It used two remote code execution vulnerabilities for doing that - vulnerabilities in the Windows Print Spooler and in the Windows Server Service Remote Procedure Call. [6.]

It also contacted the C&C server for downloading additional code and updating itself. It most probably also sent information about the infected network to the attacker. Because the ICS network was air gapped, the updates were probably also done via USB which required an employee to use the same USB stick on a computer which had Internet connectivity. It then updated the other systems in the LAN via a peer-to-peer mechanism. [6.]

After reaching the goal, i.e. the Siemens S7 system, Stuxnet started silently modifying the sequence in how the centrifuges were operated and also hided that something was changed in the sequence so everything seemed to be running normally. It also ran very seldom and may remain silent for 90 days before running its malicious activities, which then eventually caused the damage. [6.]

No studies combining EMET and Stuxnet were found in the Internet, which could have shown if EMET could have mitigated the attack. By looking at the mechanisms of Stuxnet, EMET most likely could not have mitigated the malware because of how the exploit worked and which processes were targeted. The Common Vulnerabilities and Exposers (CVE) codes related to Stuxnet were not found on the web page containing information of the CVE codes that EMET protects against. [11.]

6.2 RSA

RSA is a well-known information security company, so the attack against it was covered in the news worldwide. The attack followed the CKC as the attackers selected two small groups of employees to whom the spear phishing emails were sent. The subject of the email was “2011 Recruitment Plan” and it was written to look convincing enough,

so one employee opened it, even though it had been automatically moved to a junk mail folder. [7.]

The email contained a spreadsheet with a zero-day exploit using Adobe Flash vulnerability. Then a remote administration tool (RAT) Poison Ivy was installed, allowing remote access to the system. After the connection to C&C server was established, the attacker started pivoting, i.e. moving laterally in the network, and trying to gain access to more systems and more credentials with administrator privileges. [7.]

When the attacker had reached the systems which were the goal, data from the systems was moved out from RSA in compressed RAR-files which were encrypted so that the content could not be recognized. Among the data stolen there was information on RSA's SecurID, which is a mechanism providing two-factor authentication using one-time passwords. [7.]

The attack had consequences because SecurID-system was widely used by many companies and replacing the tokens was expensive, but the reputational damage was even greater. One company using SecurID was Lockheed Martin, the company that had created CKC. The company was attacked and SecurID was used as part of the attack. [37.]

According to MS web documents, EMET could have mitigated the exploit using Flash vulnerability in Excel. Stricter rules about running ActiveX in MS Office applications could also have worked. [38;39.]

6.3 Ukraine Power Grid Hack

On 23 December 2015 a regional electricity company had service outages because attackers had broken into the computer network, ruining Christmas for many people. The target was Supervisory Control and Data Acquisition (SCADA), which is an ICS used for controlling and monitoring PLCs. The attack affected 225,000 customers who lost power for different periods of time. [8.]

The malware BlackEnergy3 was delivered in Microsoft Word and Excel files via email to people who were in administrative or IT network positions. Reconnaissance was

clearly made to find out the targets. The MS Office files contained macros, which are bits of code written in Visual Basic for Applications (VBA) that allow tasks to be automated. Macros have been used for malicious purposes since 1995 when the first macro virus was found. Macros have been disabled by default since Office 2000, so users have to enable them by hand and that is what happened in this case also. [8;40.]

The malware then connected to C&C allowing remote connection to the infected systems. It seems that the attackers had a foothold on the systems for more than six months before taking down the power grid. They did the normal actions of acquiring credentials, privilege escalation and pivoting with the goal of getting access to the ICS network. [8.]

When the actual attack on the power converters started, the attackers had malware across the environment including a modified KillDisk which is used for wiping hard disks. Then they took over the control on the SCADA computer and locked out the operator who could only watch how the attackers opened the breakers, causing power outage. At the same time they uploaded malicious firmware to the serial-to-Ethernet devices, which made sure that the power network could not be taken back online remotely, so it had to be done by hand at each sub-station. Uninterruptable Power Supplies (UPS) were targeted so that the computer networks connected to UPS were brought down when the attack was done. They also created a Denial of Service (DoS) attack against the call center, so that the customers complaining about the power outage could not get through. The purpose of the DoS remains unclear. Perhaps it blocked the visibility to how wide the damage was or was just intended to annoy people who could not get through. [8.]

EMET could not have helped against this attack as no exploit was used and the personnel enabled the macros, allowing the malware to start. Anti-malware could have detected BlackEnergy3 malware and enforcing centralized rules so that macros cannot be enabled, but the most important would have been user awareness training about handling documents sent via email. [8.]

7 Installing and Configuring EMET

7.1 EMET Installation

EMET installer can be downloaded from the MS website. It can then be distributed to clients via Group Policy Objects (GPO) or with system management software such as Microsoft System Center Configuration Manager (SCCM), Microsoft Windows Server Update Services (WSUS), Symantec Altiris or similar. This chapter concentrates on using GPO for distribution. Home users or small businesses without any centralized management can just install EMET by hand. Testing installation via GPO was done in a lab environment which was separated from the normal production environment. [26.]

MS .NET framework 4.5 is required before installing EMET 5.5 on all systems. Windows 8 and Windows Server 2012 also require a compatibility update described in the knowledge base article KB2790907. Windows XP is not supported by EMET 5.5, but EMET 4.1 supports it. However, all mitigations are not available on XP though. [1.]

Users that have an earlier version of EMET than 5.5 installed need to migrate the settings by running a PowerShell script that dumps the settings from the Windows registry to a file before uninstalling old version. Then the new version has to be installed before restoring the registry settings. That brings additional complexity and it is strange why MS did not include the functionality in the installer. [1.]

WMI filters for targeting Vista or a newer client OS need to be used if there are XP or Windows Servers scattered in the same Organizational Units (OU) as newer client operating systems. The WMI filter presented in listing 1 fulfills the requirements.

```
SELECT Version, ProductType FROM Win32_OperatingSystem
WHERE Version >= '6.0' AND ProductType = '1'
```

Listing 1. WMI query for selecting targets for EMET 5.5.

A version greater than or equal to 6.0 means the Vista kernel version and above. ProductType = '1' means client operating system. [27;28.]

Assigning the policies to correct OUs is done from Group Policy Management console as shown in figure 2.

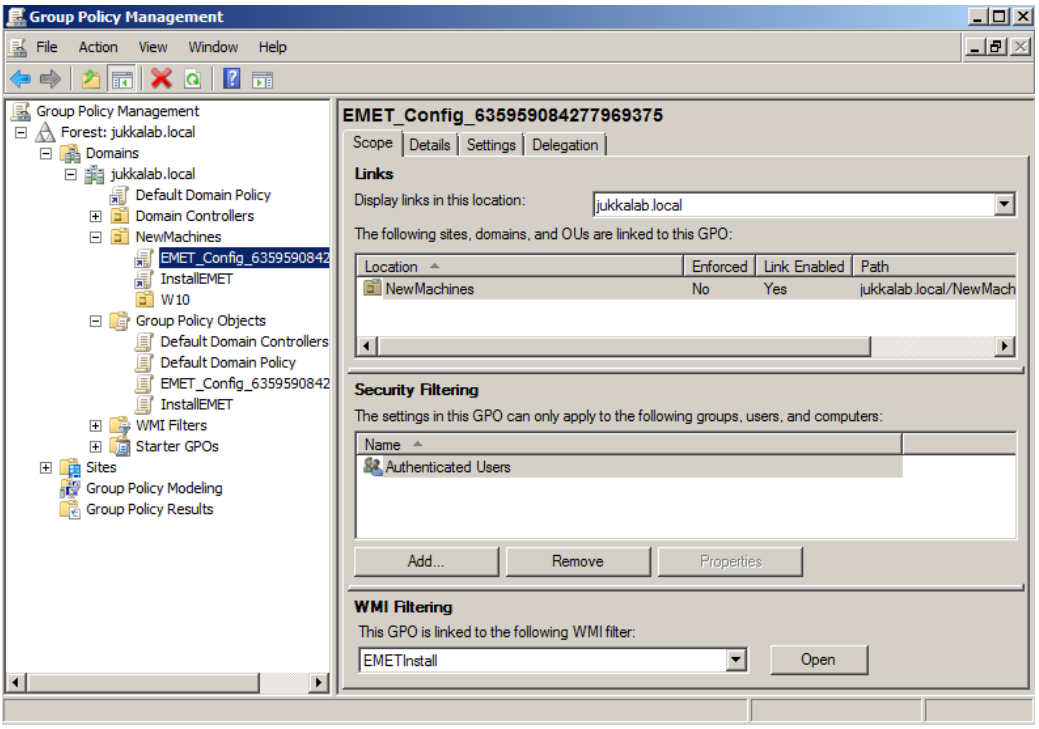

Figure 2. Assigning EMET policies.

7.2 Configuration

EMET 5.5 supports creating policies with the normal user GUI and then distributing them via GPO.

MS provides three configuration sets which have known good configurations pre-configured. The configurations are xml files, so they can be modified if necessary. The configuration sets are described below.

- Recommended Software, which includes Internet Explorer, Office, Adobe Reader, Java and WordPad.

- Popular Software, which includes everything that is included in the Recommended Software and a lot of different software from several vendors such as web browsers Firefox and Chrome.

- Cert Trust, which includes everything that is included in Popular Software and verifies certificates to mitigate man-in-the-middle attacks. Some popular web-site's certificates are included by default but this feature requires a lot of manual configuration. [1.]

The settings for the local computer and for the GPO are done from the same view which can be seen in figure 3. The Group Policy option is visible in the upper left corner.

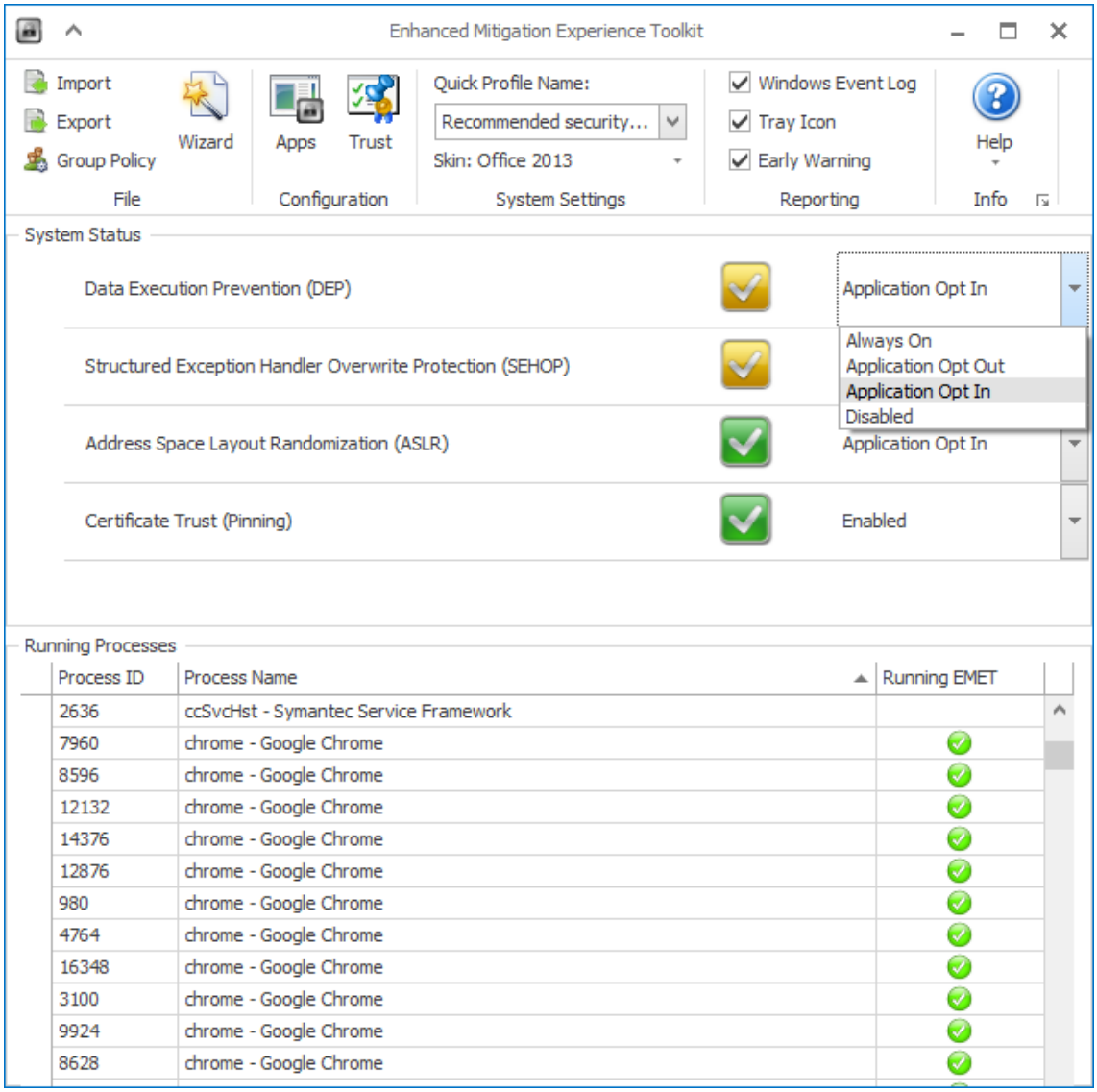

Figure 3. EMET GUI with system wide settings.

By clicking Group Policy, a new window opens up, asking whether to create a policy for the local computer, to select an existing GPO or to create a new GPO as shown in figure 4.

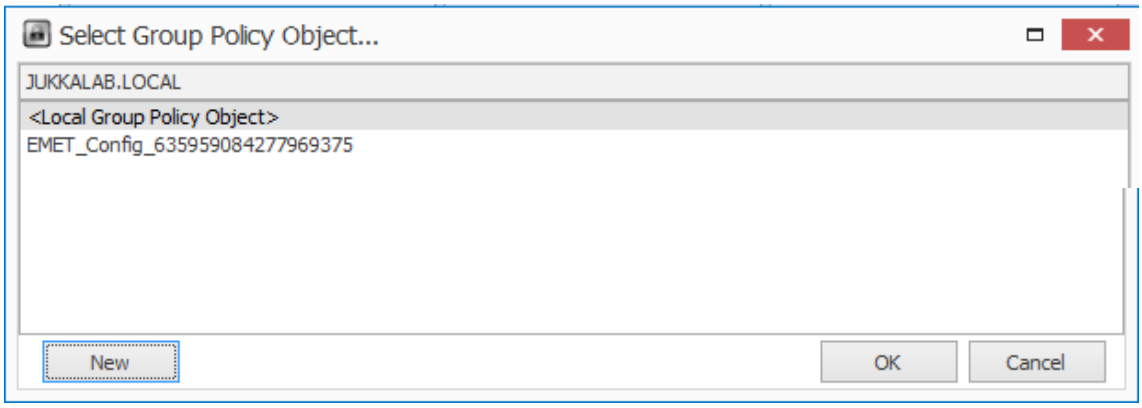

Figure 4. New EMET GPO creation.

Then a view similar to figure 3 opens up, with the exception that the System Status selection boxes have a “User Configured” option added. Different pre-configuration templates can be imported by selecting Import. Application level settings can be accessed by clicking Apps. If Popular Software was imported, there are many software already included with recommended settings as shown in figure 5. If there are issues with an application, then the problematic protection causing issues can just be disabled.

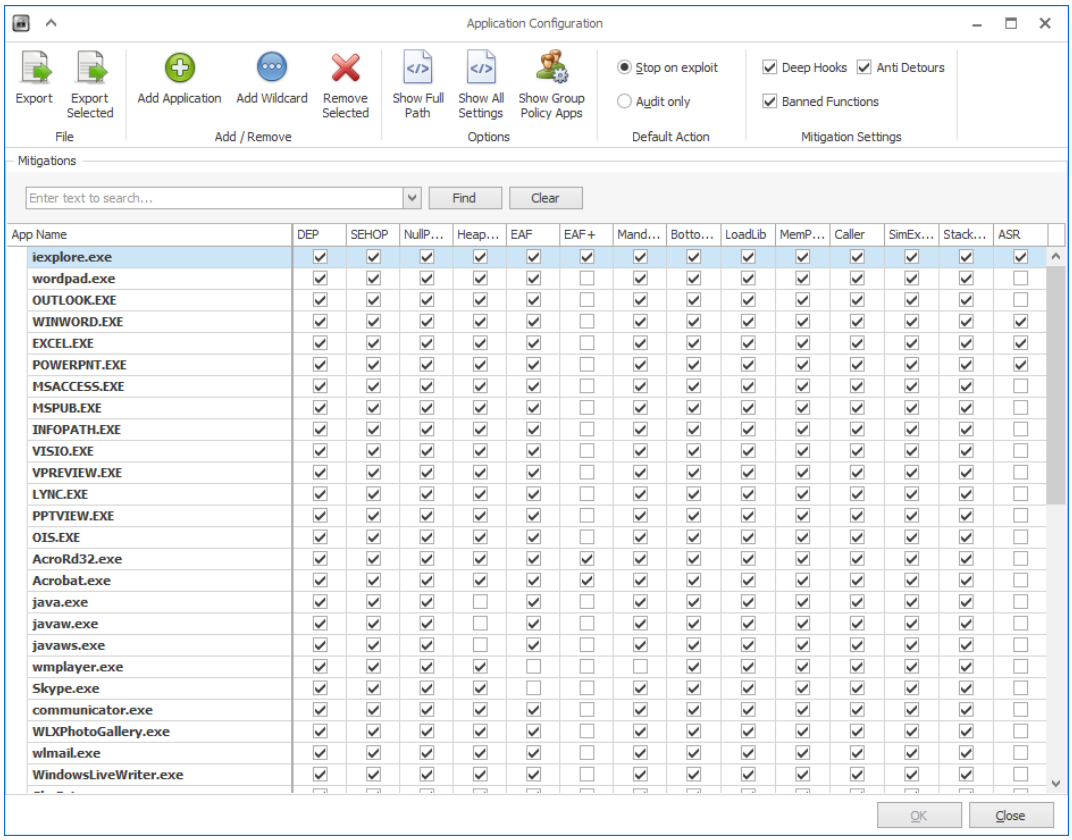

Figure 5. EMET application, default action and extra mitigation settings.

Show All Settings in figure 5 brings additional configurations available like which memory areas Heap Spray Protection pre-allocates and which modules are included in EAF+ settings. The protections which support 64-bit processes are also shown in this view, as visible in figure 6.

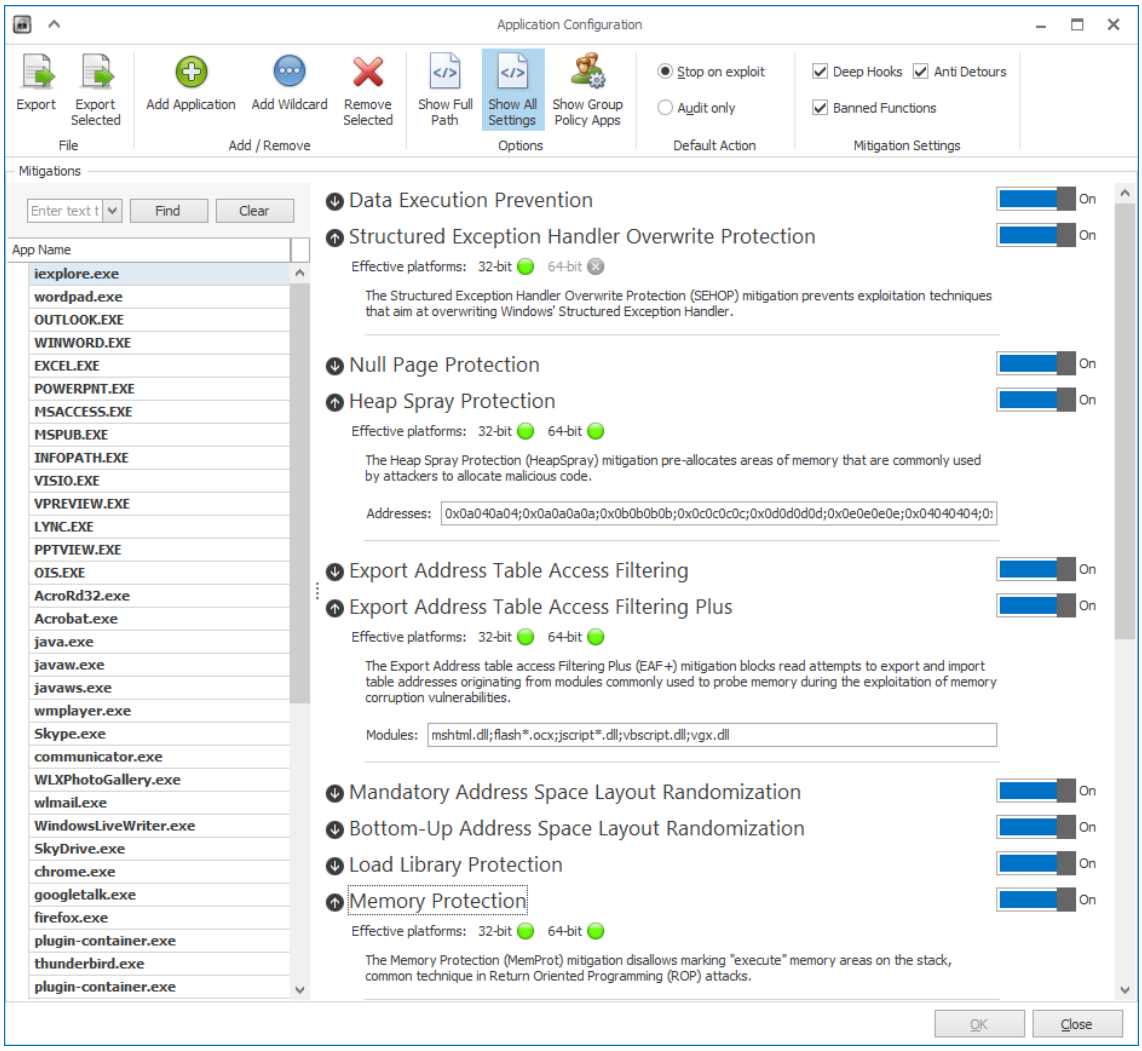

Figure 6. EMET advanced application settings.

Audit only mode should be used when piloting the product with a larger group of machines. EMET can still cause issues even with audit only, because of the way it works. It hooks all processes which are configured to be inspected by EMET. Already that can cause slowness.

7.3 Logging

EMET writes its log entries into the Windows Application log. There are some limitations like Bottom Up ASLR and Null Page mitigations which do not generate log entries pointing the events to EMET. If system-wide mitigations are in use, ASLR, DEP and SEHOP might not be linked to EMET in the log, which needs to be considered.

There are three log levels: information, warning and error. The information level is used for normal EMET operations like when EMET process starts up. Warning is used when EMET settings change, when there is Certificate Trust detection or with ASR triggered, as can be seen in figure 7. The EMET 5.5 user guide did not mention that ASR mitigation logs are written with warning level. Other mitigations write log to the error log, so it is strange why ASR behaves differently.

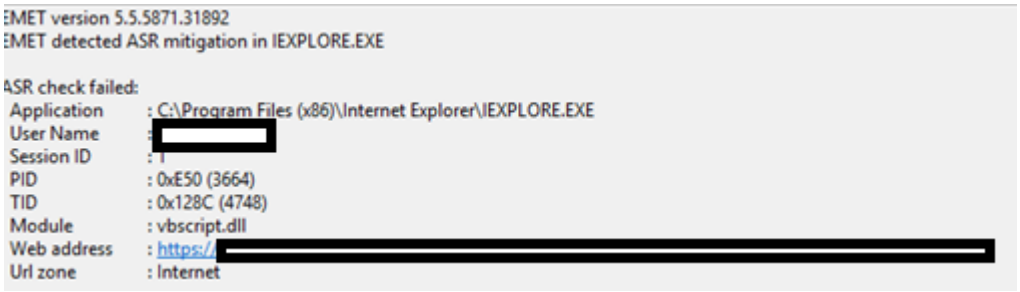

Figure 7. ASR mitigation.

An error is logged when EMET mitigates and closes an application as seen in figure 8.

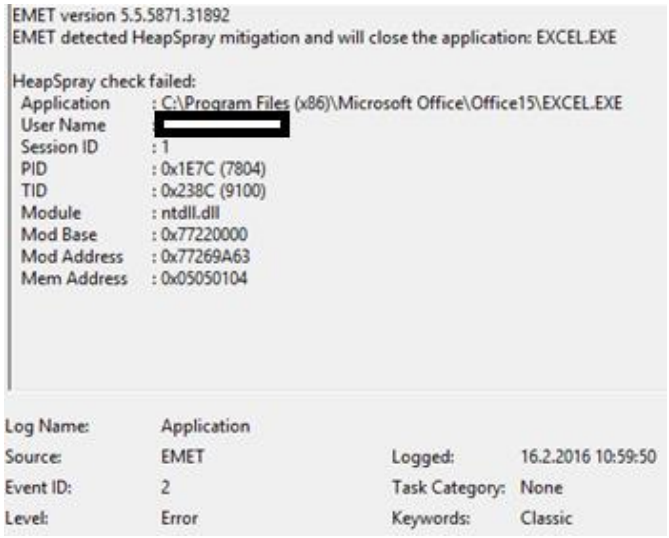

Figure 8. HeapSpray mitigation.

8 Client Compatibility Testing

8.1 Test setup

EMET 5.5 client was tested on two systems: Windows 8.1 and Windows 10. The Windows 8.1 system had Office 2010 and Windows 10 had Office 2013. Both had the latest Google Chrome and Java installed. All available security updates for the OS and Office were installed. All automatic updating was disabled for all applications so that the testing systems could not be changed during the test period. EMET 5.5 was installed manually and the Popular Software profile was selected.

8.2 Compatibility Testing

All tests were done before installing EMET 5.5 to see if there were issues even without EMET and to find out how quickly the operations, like opening files, normally took. Then EMET was installed and the tests were done again and the results were written down. The results are shown in detail in appendix 1.

Several normal day-to-day operations such as opening, creating new and modifying different files were tested. If a program crashed, the EMET protection causing the crash was documented if possible. A subjective test to measure if an application seemed to open more slowly than without EMET was also done.

All anomalies outside the pre-defined ones were also written down from one week time when EMET 5.5 was run on both systems. There was only one clear anomaly, as can be seen in table 2.

Table 2. Anomalies during EMET testing.

Time	Anomaly
5 Apr 2016	W8.1, Outlook 2013, High CPU load and lag if a new email was opened from Outlook popup. Disabling EAF fixed.

8.3 Results of Testing

All 20 tests with both OS were completed without any application crashes and the only slowness was related to presenting a PowerPoint file when having a video conference call. If Outlook was opened from a popup, there was a noticeable delay, which could be fixed by removing EAF from the program's protections.

Windows 8.1 has had EMET installed since February 2016 and since then there has been one occurrence of Excel crashing with a spreadsheet that opened up normally the second time it was opened. Also one website belonging to a collaborator had Visual Basic code in it so ASR blocked it because it was not listed as Intranet or Trusted Sites in the Internet settings of the OS.

9 Conclusions

EMET 5.5 proved to run smoothly with very few issues found on both Windows 8.1 and Windows 10. Testing at this stage was limited to only two laptops, so broader testing is required before providing EMET to customers as such. ASR requires modifications to Internet Explorer settings for the customers, because the feature could block legitimate websites belonging to partners, collaborators and service providers. Collecting the legitimate websites requires extra effort so it needs to be considered in pricing. Privacy issues may also occur, because the URL, which had the issue, included the user name in the event log entry. The audit-only mode needs to be used in the beginning to learn if there could be issues.

Installation and configuration has been made easier compared to previous versions, because the GPO settings can now be configured from the EMET GUI. The configurations that come with EMET already have the most common problematic mitigations per product disabled, so quite small modifications are required to the configuration. Outlook on Windows 8.1 slowed down very much when opening an email from a popup and if EAF was enabled.

The security of the Windows OS has improved in every iteration, so if the option to easily and cost effectively upgrade to the latest version is available, it should be done from a security perspective. Windows XP has been out of support for years already, but it is still used widely in health care, ICS and production environment, so hopefully Windows 10 will take its place when the machines running XP will be obsolete for good.

Cyber Kill Chain developed by the company Lockheed Martin could most probably have mitigated some of the stages of the attacks described in chapter 5. Like Lockheed Martin describes, “All seven steps must be successful for a cyber-attack to occur. The defender has seven opportunities to break the chain” [2]. Every time there is a new attack, it gives more information on how to build a stronger defence for the next time.

EMET is not a silver bullet that can stop every attack, but when used as a part of layered protection, it can help mitigate memory corruption exploits which have been popular in the recent years. Perhaps if EMET becomes more popular, there will be more bypasses developed for it – making it less effective.

The final assignment was done in a quite tight timeframe, so if there had been more time, testing could have included more systems including at least Windows 7, since it is still a very popular OS. Testing setting the maximum security level would be interesting, but because it causes known issues with BitLocker and other software, it could be implemented to a very limited group and have a much longer test period.

Microsoft released security updates in April 2016, which caused a lot of issues with EMET 5.5. If they had been released before making the tests described in this thesis, the results would have been very different. Disabling EAF protections in EMET restored normal functionality of the system.

In conclusion, this work offers information about memory corruption exploitation. It also gives information on how to install and configure EMET 5.5 in a corporate environment.

References

1 EMET User Guide 5.5. Microsoft [online].
URL: https://www.microsoft.com/en-us/download/details.aspx?id=50802. Accessed February 12, 2016.

2 Lockheed Martin. Cyber Kill Chain [online].
URL:http://cyber.lockheedmartin.com/hubfs/Gaining_the_Advantage_Cyber_Kill_Chain.pdf?t=1459498998121. Accessed March 21, 2016

3 ENISA. Proactive Detection of Network Security Incidents [online].
URL: https://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-report/at_download/fullReport. Accessed March 24, 2016.

4 Niemelä J. Statistical Analysis of Malware Defence Methods. Jyväskylä University of Applied Sciences; 2015.
URL: http://urn.fi/URN:NBN:fi:amk-201601071096. Accessed March 24, 2016.

5 Freingruber R. Bypassing EMET 5.1 – A case study on CVE-2011-2371. Vienna University of Technology; 2015. Accessed March 30, 2016.

6 Symantec. Stuxnet Dossier [online].
URL:https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. Accessed March 25, 2016.

7 RSA. Anatomy of an Attack [online].
URL: http://blogs.rsa.com/anatomy-of-an-attack/. Accessed March 25, 2016.

8 SANS ICS. Analysis of the Cyber Attack on the Ukrainian Power Grid [online].
URL: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf. Accessed March 26, 2016.

9 Matt Miller, MS Security and Defence Center. On the Effectiveness of DEP and ASLR [online].
URL: https://blogs.technet.microsoft.com/srd/2010/12/08/on-the-effectiveness-of-dep-and-aslr/. Accessed March 30, 2016.

10 FireEye. Using EMET to Disable EMET [online].
URL: https://www.fireeye.com/blog/threat-research/2016/02/using_emet_to_disabl.html. Accessed March 30, 2016.

11 Microsoft. EMET Mitigations Guidelines [online].
URL: https://support.microsoft.com/en-us/kb/2909257. Accessed February 12, 2016.

12 Microsoft Tech Center. EMET Support Forum [online].
URL: https://social.technet.microsoft.com/Forums/security/en-US/home?forum=emet. Accessed February 12, 2016.

13 Microsoft. Understanding DEP as a Mitigation Technology Part 1 [online].
URL: https://blogs.technet.microsoft.com/srd/2009/06/12/understanding-dep-as-a-mitigation-technology-part-1/. Accessed March 30, 2016.

14 Google. Policy List for Chrome [online].
URL: http://www.chromium.org/administrators/policy-list-3. Accessed April 2, 2016.

15 Microsoft. User Mode and Kernel Mode [online].
URL: https://msdn.microsoft.com/en-us/library/windows/hardware/ff554836(v=vs.85).aspx. Accessed February 20, 2016.

16 Microsoft Malware Protection Center. Rootkits [online].
URL: https://www.microsoft.com/security/portal/mmpc/threat/rootkits.aspx. Accessed February 21, 2016.

17 Microsoft. Driver Signing Policy [online].
URL: https://msdn.microsoft.com/en-us/library/windows/hardware/ff548231(v=vs.85).aspx. Accessed February 21, 2016.

18 Pulse IT Magazine. Bug that Infected Melbourne Hospital Is a Qbot Worm [online].
URL: http://www.pulseitmagazine.com.au/news/australian-ehealth/2860-bug-that-infected-royal-melbourne-hospital-is-a-qbot-worm. Accessed February 22, 2016.

19 Microsoft. Windows NT 4.0 Does not Support Universal Serial Bus [online].
URL: https://support.microsoft.com/en-us/kb/196661. Accessed February 22, 2016.

20 Microsoft. Feature Comparison: Windows NT, Windows 2000, and the Windows 2003 Server Family [online].
URL: https://technet.microsoft.com/en-us/library/cc759589(v=ws.10).aspx. Accessed February 22, 2016.

21 Microsoft. What Is Kerberos Authentication [online].
URL: https://technet.microsoft.com/en-us/library/cc780469(v=ws.10).aspx. Accessed February 22, 2016.

22 Microsoft. What's New in Security for Windows XP Professional and Windows XP Home Edition [online].
URL: https://technet.microsoft.com/en-us/library/bb457059.aspx. Accessed February 22, 2016.

23 Hackshop. USB Rubber Ducky [online].
URL: http://hakshop.myshopify.com/products/usb-rubber-ducky-deluxe?variant=353378649. Accessed February 23, 2016.

24 Avecto. Microsoft Vulnerabitilies Report [online].
URL: http://learn.avecto.com/2015-microsoft-vulnerabilities-report. Accessed April 2, 2016.

25 NSA. Control Administrative Privileges [online].
URL:https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_ControlAdministrativePrivileges_Web.pdf. Accessed April 2, 2016.

26 Microsoft. EMET 5.5 Download [online].
URL:https://www.microsoft.com/en-us/download/details.aspx?id=50766. Accessed February 12, 2016.

27 Microsoft. Create WMI Filter for the GPO [online].
URL: https://technet.microsoft.com/en-us/library/cc947846(WS.10).aspx. Accessed April 2, 2016.

28 Microsoft. WMI Queries the Easy Way, Item-level Targeting the Much Faster and Easier Way [online].
URL: https://blogs.technet.microsoft.com/grouppolicy/2009/08/24/wmi-queries-the-easy-way-item-level-targeting-the-much-faster-and-easier-way/. Accessed April 2, 2016.

29 Microsoft. How to use Group Policy to Remotely Install Software in Windows Server 2008 and Windows Server 2003 [online].
URL: https://support.microsoft.com/en-us/kb/816102. Accessed April 2, 2016.

30 Microsoft. Windows Vista Security and Data Protection Improvements [online].
URL: https://technet.microsoft.com/en-us/library/cc507844.aspx. Accessed February 23, 2016.

31 Microsoft. Inside Windows 7 User Account Control [online].
URL: https://technet.microsoft.com/fi-fi/magazine/2009.07.uac(en-us).aspx. Accessed February 23, 2016.

32 Microsoft. Windows 7 Security Enhancements [online].
URL: https://technet.microsoft.com/en-us/library/dd560691.aspx. Accessed February 23, 2016.

33 Microsoft. What's Changed in Security Technologies in Windows 8.1 [online]. URL: https://technet.microsoft.com/en-us/library/dn344918.aspx. Accessed February 23, 2016

34 Microsoft. Windows 10 Security Overview [online]. URL: https://technet.microsoft.com/en-us/library/mt601297(v=vs.85).aspx#information. Accessed February 23, 2016.

35 CVE. CVE-2010-2568 [online]. URL: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568. Accessed April 8, 2016.

36 IEEE Spectrum. The Real Story of Stuxnet [online]. URL: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet. Accessed April 8, 2016.

37 RSA. FAQ about RSA SecurID [online]. URL: http://www.emc.com/collateral/guide/11455-customer-faq.pdf. Accessed March 25, 2016.

38 Microsoft. A Technical Analysis on the CVE-2011-0609 Adobe Flash Player Vulnerability [online]. URL: https://blogs.technet.microsoft.com/mmpc/2011/03/17/a-technicalanalysis-on-the-cve-2011-0609-adobe-flash-player-vulnerability/. Accessed March 25, 2016.

39 Microsoft. Blocking Exploit Attempts of the Recent Flash 0-Day [online]. URL: https://blogs.technet.microsoft.com/mmpc/2011/03/17/a-technical-analysis-on-the-cve-2011-0609-adobe-flash-player-vulnerability/. Accessed March 25, 2016.

40 Kaspersky. What Is a Macro Virus? – Definition [online]. URL: https://usa.kaspersky.com/internet-security-center/definitions/macro-virus. Accessed April 10, 2016.

EMET 5.5 Client Compatibility Tests

1. Open MS Excel, create a new spreadsheet and save it on local drive.

OS	Windows 8.1	Windows 10
Crash	No	No
Slowness compared to use without EMET	No	No
Addition notes		

2. Open existing MS Excel file, modify it and save it on local drive.

OS	Windows 8.1	Windows 10
Crash	No	No
Slowness compared to use without EMET	No	No
Addition notes		

3. Open MS Word, create a new document and save it on local drive.

OS	Windows 8.1	Windows 10
Crash	No	No
Slowness compared to use without EMET	No	No
Addition notes		

4. Open existing MS Word file, modify it and save it on local drive.

OS	Windows 8.1	Windows 10
Crash	No	No
Slowness compared to use without EMET	No	No
Addition notes		

5. Open MS PowerPoint, create a new presentation and save it on local drive.

OS	Windows 8.1	Windows 10
Crash	No	No

Slowness compared to use without EMET	No	No
Addition notes		

6. Open existing MS PowerPoint file, modify it and save it on local drive.

OS	Windows 8.1	Windows 10
Crash	No	No
Slowness compared to use without EMET	No	No
Addition notes		

7. Open MS Outlook, write a new email, attach an Excel sheet and send it

OS	Windows 8.1	Windows 10
Crash	No	No
Slowness compared to use without EMET	No	No
Addition notes		

8. Open MS Outlook, open existing email and reply to it

OS	Windows 8.1	Windows 10
Crash	No	No
Slowness compared to use without EMET	No	No
Addition notes		

9. Open MS Outlook, create a new calendar appointment, and invite people to it.

OS	Windows 8.1	Windows 10
Crash	No	No
Slowness compared to use without EMET	No	No
Addition notes		

10. Open Skype for Business, start a chat with someone, send a Word document over Skype.

OS	Windows 8.1	Windows 10
Crash	No	No
Slowness compared to use without EMET	No	No
Addition notes		

11. Open Skype for Business, start a call.

OS	Windows 8.1	Windows 10
Crash	No	No
Slowness compared to use without EMET	No	No
Addition notes		

12. Open Skype for Business, start a video call.

OS	Windows 8.1	Windows 10
Crash	No	No
Slowness compared to use without EMET	No	No
Addition notes		

13. Open Skype for Business, start a video call, present a PowerPoint file.

OS	Windows 8.1	Windows 10
Crash	No	No
Slowness compared to use without EMET	Yes, possible slowness, high cpu, high disk usage	Yes, possible slowness, high cpu, high disk usage
Addition notes		

14. Open company SharePoint, open an existing Excel file, and modify it in the browser.

OS	Windows 8.1	Windows 10
Crash	No	No
Slowness compared to use without EMET	No	No
Addition notes		

15. Open company SharePoint, open an existing Excel file, modify it with Excel and save the file to SharePoint

OS	Windows 8.1	Windows 10
Crash	No	No
Slowness compared to use without EMET	No	No
Addition notes		

16. Open Google Chrome, open www.metropolia.fi main page.

OS	Windows 8.1	Windows 10
Crash	No	No
Slowness compared to use without EMET	No	No
Addition notes		

17. Open Word document which has a URL to company front page, click the URL and verify that web browsers opens up and the web page is shown normally

OS	Windows 8.1	Windows 10
Crash	No	No
Slowness compared to use without EMET	No	No
Addition notes		

18. Open Appgate (Java) VPN, verify that connection through it work normally.

OS	Windows 8.1	Windows 10
Crash	No	No
Slowness compared to use without EMET	No	No
Addition notes		

19. Open up MS Excel file with macros, allow running macros and run them.

OS	Windows 8.1	Windows 10
Crash	No	No

Slowness compared to use without EMET	No	No
Addition notes		

20. Open up a PDF file with Adobe Reader in Windows 8.1 and Document Reader in Windows 10

OS	Windows 8.1	Windows 10
Crash	No	No
Slowness compared to use without EMET	No	No
Addition notes		