BI01
Advanced Threat Detection and Removal with FEP 2010

Jason J. Joyce
Principal Lead Program Manager
Session Objectives and Takeaways

Session Objective(s):
- Overview of protection enhancements in FEP 2010
- Deep dive and demos on several new features

Key Takeaways:
- Understand how FEP technologies are used to protect against malware
Forefront Endpoint Protection 2010
Next Generation Of Forefront Client Security

Ease of Deployment
- Built on distribution infrastructure of Microsoft® System Center Configuration Manager software
- Supports all System Center Configuration Manager topologies and enables enterprise-wide scalability
- Facilitates easy migration
- Able to deploy across various operating systems (including Microsoft Windows® client and Microsoft Windows Server®)

Enhanced Protection
- Protection against viruses, spyware, rootkits, and network vulnerabilities
- Productivity-oriented default configuration
- Integrated management of host firewall
- Backed by Microsoft Malware Protection Center

Simplified Desktop Management
- Unified management interface for desktop administrators
- Timely and effective alerts
- Simple, operation-oriented policy administration
- Historical reporting for security administrators
We’ve been busy...

- Process/registry/network RTP watchers
- Directional scanning
- Persisted file cache
- Wildcard support for exclusions
- Scheduled scan randomization
- CPU throttling
- Command line scanner
- Signature update package chaining
- UNC signature distribution
- Signature source ordering fallback
- Dynamic translation
- Live system behavior monitoring
- Kernel inspection (Komoku)
- Dynamic signature service
- WLSP integration
- Network vulnerability shielding (NIS)
- Kernel Support Library (KSL) driver
- Reboot tracking (remediation)
- Directed scanning improvements
- Offline scan integration
- Diagnostic scan
- Service hardening/anti-tampering
- State management
- Kernel-mode boot-time removal
Known malware: blocked. Some new malware blocked by generics.

**GOAL:** Continue to provide high-quality protection & cover more attack vectors

- Real-time Protection
- Generics & Heuristics
- Browser Protection
- Network Vulnerability Shielding

Remaining new malware samples sent to MMPC for analysis. New signatures delivered to customers and active infections detected and neutralized.

**GOAL:** Shrink customer “window of vulnerability” by discovering new threats and delivering signatures faster

- Anti-rootkit
- Behavior Monitoring
- Dynamic Signature Service
- Malware Response
Forefront Protection Stack: Overview

- Putting our assets together – we have created a comprehensive protection stack

- Focus:
  - Reduce time and cost to protect
  - Increase cost to attack, decrease exploit window
  - Operationalize new protection technologies
  - Destroying malware’s value prop

- Recent investments:
  - Closing vulnerability and social engineering vectors
  - Operationalizing protection
  - Balancing protection vs. performance
  - Remediation and threat management improvements
  - Simplifying deployment
Antimalware Details

- Real-time protection provides high-quality reactive detection with optimized performance
- Key improvements:
  - Improved Monitoring: Process/Registry/Network watchers
  - Improved performance scenarios for servers
  - Performance improvements using advanced caching
  - Cached files are not rescanned
  - Cache persists across reboots
  - New exclusion features (wildcard support)
  - Scheduled scan flexibility
  - CPU throttling
  - Command line scan options
  - Signature update improvements
  - Service hardening/anti-tampering
Other Improvements

- Performance improvements
  - New exclusion features (wildcard support in exclusions)
  - Schedule scan flexibility (scan times randomized)
  - CPU throttling (configurable – mitigates impact of scheduled scan to system performance)
- Focus on server scenarios
  - Memory footprint improvements for Terminal Server
  - Directional scanning
  - Command line scan options (mpcmdrun.exe improvements)
- Hardening of the client against malware attack
- Signature update improvements
- Support for UNC distribution
- Source ordering (fallback)
- Package chaining
Signature Update Improvements

- Support for UNC distribution
- Source ordering (fallback)
- Package chaining dramatically reduces signature update size
  - 95% reduction in WSUS traffic

![Graph showing daily WSUS Bandwidth consumption with a sharp decrease in June and July.](image)
Generics and Heuristics

- Industry leading proactive detection based on our Dynamic Translation technology
- Dynamic Translation helps us deal with malware volume – many are the same threat, just obfuscated differently
  - With polymorphic malware, what the code does may be the only common aspect of two samples
- Generics/heuristics based on emulated behavior and/or decrypted binary characteristics
  - Allows a single signature to detect thousands of files
- Advanced+ Certification from AV-Comparatives.org on pro-active detection

AV-Comparatives.org August 2010 Results

<table>
<thead>
<tr>
<th></th>
<th>On-Demand</th>
<th>Pro-active</th>
<th>Performance</th>
<th>Dynamic</th>
<th>Removal</th>
<th>PUA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>Advanced</td>
<td>Advanced+</td>
<td>Advanced+</td>
<td>Advanced</td>
<td>Advanced+</td>
<td>Advanced</td>
</tr>
</tbody>
</table>
HANDLE hFile;
hFile = CreateFile(L"NewVirus.exe", GENERIC_WRITE, 0, NULL, CREATE_NEW, FILE_ATTRIBUTE_HIDDEN, NULL);

... push 40000000h
push offset string L"NewVirus.exe"
call dword ptr [__imp__CreateFileW@28]
cmp esi, esp

---

Generics and Heuristics: Dynamic Translation (DT)

Potential malware

- Translate code that accesses unsafe resources into code that accesses safe resources
- Execute translated program on the real CPU – very fast
Behavior Monitoring

- Live system behavior monitoring identifies new threats
- Tracks behavior of unknown processes and known good processes gone bad
- Provides Live OS anomaly detection
- Primary sensors
  - Process / File / Registry operations
  - Network Activity – Spam and BotNets
  - Kernel Modification – “Komoku Inc” Integration for Anti-rootkit (AR) protection
  - Web Downloads
- Behavior Monitoring “detections” driven by the engine and trigger a request to the Dynamic Signature Service
- New signature support enables AV researchers (MMPC) to rapidly respond to evolving threats
Applications call library functions
- Some of these library functions call a much smaller set of system calls
- RTP logs calls to some of these system calls
  - Queues notifications
  - Consumed by Behavior Monitoring
- RTP logs calls, BM makes sense of them.
- It takes some practice to map high-level behaviors (1) to low-level notifications (4) when designing new detections
Behavior Monitoring: Notifications

Filesystem
- FileCreate
- FileOpen
- FileModify
- FileDelete
- FileRename

Registry
- RegistryKeyCreate
- RegistrySetValue
- RegistryKeyDelete
- RegistryValueDelete
- RegistryKeyRename

Network
- IRC

Good for detecting IRC bots

Other
- ModuleLoad
- ProcessCreate
- OpenProcess
- ProcessTerminate
- DriverLoad
- BootSectorChange
- RemoteThreadInject
- RawWrite

Good for detecting droppers and file infectors

Good for ASEPS and detecting tampering with software keys and configuration.

Good for detecting process infectors and exploits

Good for detecting rootkit installers
Behavior Monitoring: Example Detection

**Upon detection:**
- Trojan Dropper: A process creates or modifies a file and a traditional signature indicates the new file is malware.
- MBR/VBR tampering: A process modifies a Master or Volume Boot Record.
- Kernel tampering: the Anti-Rootkit sensor detects tampering in kernel memory

**FILTER for EVENTS:**
- Ignore if the program the process is running has a clean file reputation
  (Or driver in the kernel tampering case.)

**Emit Event and Telemetry:**
- Program the process was running.
- Malware it dropped.
- Program the process was running.
- Driver the AR sensor found linked to the tampering, if any.
Dynamic Signature Service (DSS)

- **Firewall & Configuration Management**
- **Antimalware**
- **Generics and Heuristics**
- **Behavior Monitoring**
- **Anti-Rootkit**
- **Vulnerability Shielding**
- **Browser Protection**
- **Malware Response “MMPC”**

- Delivers protection for new threats not in signature set on endpoint.
  - Low Fidelity: New class of generics looks for suspicious characteristics as behavior is emulated with Dynamic Translation
  - Queries SpyNet telemetry service about ‘interesting’ files
- Back-end classifiers use machine learning to identify new malware
- If the file is known bad, a new signature is delivered in real-time to the client requesting it
- Balances signature distribution time/cost with need for real-time updates
- Admins must choose to opt-in to at least ‘Basic’ SpyNet to use this feature
Dynamic Signature Service

- Researchers
- Real-Time Signature Delivery
- Behavior Classifiers
- SpyNet
- Reputation
- Sample Request
- Sample Submit
- Properties / Behavior
- Real-time Signature
- Client
Behavior Monitoring + DSS Scenario: Running an Unknown Program

User Launches an unknown program

Program Starts

Result State

Threat Warning/Sample Request/None

Customer Experience
- RTP - Mini-filter Intercepts

Protection Technology
- Scanning - Loading Signatures
- Scanning - Dynamic Translation
- Scanning - Checking Against Local Reputation Cache
- Performance - Adding to Reputation Cache
- BM - Behavior Monitoring Telemetry

Protection Services
- SpyNet - Signatures Downloaded
- SpyNet - Low-Fidelity Detection
- SpyNet - Expensive File
- SpyNet - Reputation Check
- SpyNet - BM Detection

SpyNet Responses Include:
- Sample Submission Request
- Extended Report
- Real-time Signature

- AV Submit - Sample Submitted
- Scanning - Loading Signatures
- Dynamic Translation
- Scanning - Checking Against Local Reputation Cache
- Performance - Adding to Reputation Cache
- BM - Behavior Monitoring Telemetry

Anti-Rootkit

- Advanced rootkit scanning and remediation defends against sophisticated threats.
- New remediation features:
  - Reboot Tracking
    Provides awareness that the system is in the process of rebooting which lets us take aggressive remediation actions that would be too risky otherwise (e.g. swapping out registry hives)
  - Directed scanning improvements
  - Offline scan integration
  - Diagnostic Scan

Microsoft Anti-Rootkit Test Results
Source: AV-Test.org

<table>
<thead>
<tr>
<th>Year</th>
<th>Detect inactive</th>
<th>Detect active</th>
<th>Remove active</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>83%</td>
<td>57%</td>
<td>33%</td>
</tr>
<tr>
<td>2009</td>
<td>100%</td>
<td>72%</td>
<td>60%</td>
</tr>
<tr>
<td>2010</td>
<td>100%</td>
<td>100%</td>
<td>86%</td>
</tr>
</tbody>
</table>
Anti-Rootkit

- Monthly engine releases ensure down-level clients such as FCS and MSE v1 still get detection and removal:
  - KSL (Kernel Support Library)
    Kernel-inspection technology acquired from Komoku that lets us detect advanced rootkits such as TDSS/TDL3 Alureon
  - kBTR (Kernel-mode boot-time removal)
    Kernel-mode driver that loads early in the boot process to perform remediation actions before the malware starts
  - DFSP (Direct File System Parsing)
    Raw parsing of the disk to detect hidden rootkits and identify potential new rootkits
- However advanced detection and remediation for rootkits and other sophisticated threats may require new platform features only in FEP
  - Diagnostic Scan
  - Advanced remediation support
Anti-Rootkit: Diagnostic Scan

- In FCS quick scan is very linear:
  - Scan is static – do x, then y, then z…
  - All users pay the same ‘tax’

- FEP 2010 adds scan intelligence based on context
  - If we can determine the kernel integrity has been tampered use more aggressive scanning with features like direct file-system parsing (DFSP) or KSL (kernel rootkit detection)
  - If the computer is clearly at greater risk, the scan should be more aggressive
  - If RTP has been on the whole time, don’t rescan user-mode ASEPs during quick scan
  - Users who are “doing everything right” should have a less aggressive scan
**Anti-Rootkit: Diagnostic Scan**

- **Quick scan in FEP 2010 = Smarter, Safer Scan**
  - Quick Scan is now context-based. Users with signs of a possible infection will receive a more thorough system check-up than users whose computer appears healthy and haven’t been exposed to possible infection.

- **Benefits**
  - Default scan is faster and less obtrusive on uninfected computers
  - Default scan is thorough and more aggressive on infected computers
  - AM Engine dynamically adjusts the depth of the scan based on context information
  - Scanning behavior learns over time and adjusts
  - Telemetry from user base provides a clear picture of real-world scan behavior
  - Improved detection rates
Anti-rootkit: Advanced Remediation Support

- New remediation features:
  - Reboot Tracking
  - Provides awareness that the system is in the process of rebooting which lets us take aggressive remediation actions that would be too risky otherwise (e.g. swapping out registry hives)
  - Directed scanning improvements
  - Ensures all parts of a threat are found and removed at once

- Offline scan integration
  - Support for “Offline Scan Required” remediation action that lets administrators know that they need to run Standalone System Sweeper to remove the rootkit.
Firewall & Configuration Management

Antimalware

Dynamic Signature Service

Generics and Heuristics

Behavior Monitoring

Anti-Rootkit

Network Vulnerability Shielding

Browser Protection

Malware Response “MMPC”

- Network Inspection System (NIS) detects and blocks Conficker-style network vulnerability exploits
- NIS inspects inbound and outbound network traffic and blocks detected exploits
- Only on if users are vulnerable: signatures enabled individually based on specific patch level
  - Disabled once the machine is patched
- If no signatures are active, NIS turns off traffic interception
- Starting small in FEP 2010 – protection for top severity Windows vulnerabilities
  - Can be extended via engine updates over time
Vulnerability Shielding: Network Inspection System
**Browser Protection**

- Firewall & Configuration Management
- Antimalware
- Dynamic Signature Service
- Generics and Heuristics
- Behavior Monitoring
- Anti-Rootkit
- Network Vulnerability Shielding
- Browser Protection
- Malware Response “MMPC”

- FEP 2010 tightly integrates with browser download managers (IE, Firefox) to ensure deep scanning of all downloads
- Integration and data sharing with IE SmartScreen cloud services provides real-time protection from malicious web sites
- No additional performance or compatibility costs when running IE

Mean Block Rate for Socially Engineered Malware
Source: NSS Labs

![Mean Block Rate Chart]

Internet Explorer 9: 99%
Internet Explorer 8: 90%
Firefox 3.6: 19%
Safari 5: 11%
Chrome 6: 3%
Opera 10: 0%
Microsoft Malware Protection Center

- Firewall & Configuration Management
- Antimalware
- Dynamic Signature Service
- Generics and Heuristics
- Behavior Monitoring
- Anti-Rootkit
- Network Vulnerability Shielding
- Browser Protection
- Malware Response “MMPC”

- FEP customer submissions and telemetry are prioritized across the global response team
- Ability for enterprise customers to engage virus researchers and analysts 24/7 for high priority submissions
- Ability to track submission status online
- Detailed information on detections added or modified in a definition set (change log)
- RSS feeds to keep our customer base up to date on new encyclopedia write ups, definition releases, and telemetry
- Visit the portal at: www.microsoft.com/mmpc
Forefront Protection Stack: Summary

- Real-time Protection
  - Provide high-quality protection
- Generics and Heuristics
- Browser Protection
  - Cover more attack vectors
- Network Vulnerability Shielding
- Anti-Rootkit
- Behavior Monitoring
  - Discovering new threats
- Dynamic Signature Service
- Malware Response
  - Delivering signatures faster
Forefront Endpoint Protection 2012
One infrastructure for desktop management and protection

**Ease of Deployment**
- Built on top of System Center Configuration Manager
- Supports all Configuration Manager topologies and scale
- Supports various operating systems Windows® Client and Server
- Facilitates easy migration from previous versions and 3rd parties
- User- and device-based roll out of client updates, sigs, policies
- Enables migration from FEP 2010 without client roll out

**Enhanced Protection**
- Protection against all types of malware
- Proactive security against zero day threats
- Productivity-oriented default configuration
- Integrated management of host firewall
- Backed by Microsoft Malware Protection Center
- Additional server role protection: TMG, OCS
- Multi-role server protection

**Simplified Desktop Management**
- Unified experience for desktop administrators
- Simple, operation-oriented policy administration
- Historical reporting for security administrators
- Real-time security alerts
- Role-based security permissions with CM RBA
- AM signatures can be managed via CM ADR
- User- and device-view in security reports
In Review: Session Objectives and Takeaways

- **Session Objective(s):**
  - Overview of protection enhancements in FEP 2010
  - Deep dive and demos on several new features

- **Key Takeaways:**
  - Understand how FEP technologies are used to protect against malware

- **Related Talks:**
  - B102 – Forefront Endpoint Protection Overview
    - Wednesday 4:00pm – 5:15pm
  - Lagoon L
Announcing the TechNet Gallery!

- A **central place** to find community content for System Center
- **Easy to share & download**
- See ratings of download & author, Q&A, and more!

http://gallery.technet.microsoft.com/
Microsoft Management Summit 2011

March 21-25, 2011