5 rules to mitigate Office Macro risks

Thomas Kurth

About Thomas Kurth

Focus

M365 Defender

Microsoft Sentinel

Intune

Working at

baseVISION
SECURE & MODERN WORKPLACE

My Blog

https://wpninjas.ch

Certifications

MVP Microsoft® Most Valuable Professional

Microsoft 365 CERTIFIED
ENTERPRISE ADMINISTRATOR
EXPERT

Hobbies

Rollhockey

Contact

Twitter: @ThomasKurth_ch
Mail: thomas.kurth@basevision.ch

Agenda

01 Introduction

02 Defense in depth

03 Questions and Discussion

Macros are everywhere

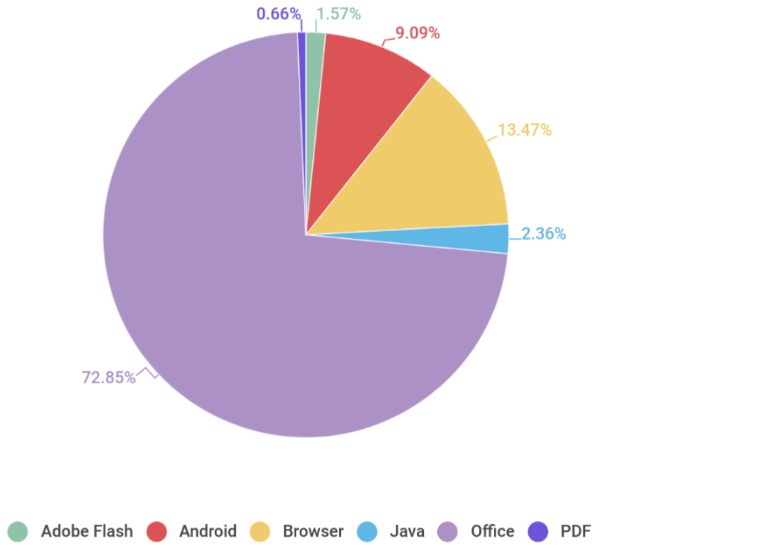
- Automation for endusers
- Simple to implement by endusers

- Still used by many products and companies
  - Templates
  - Finance calculations

- Coding Language
  - Visual Basic for Applications (VBA)

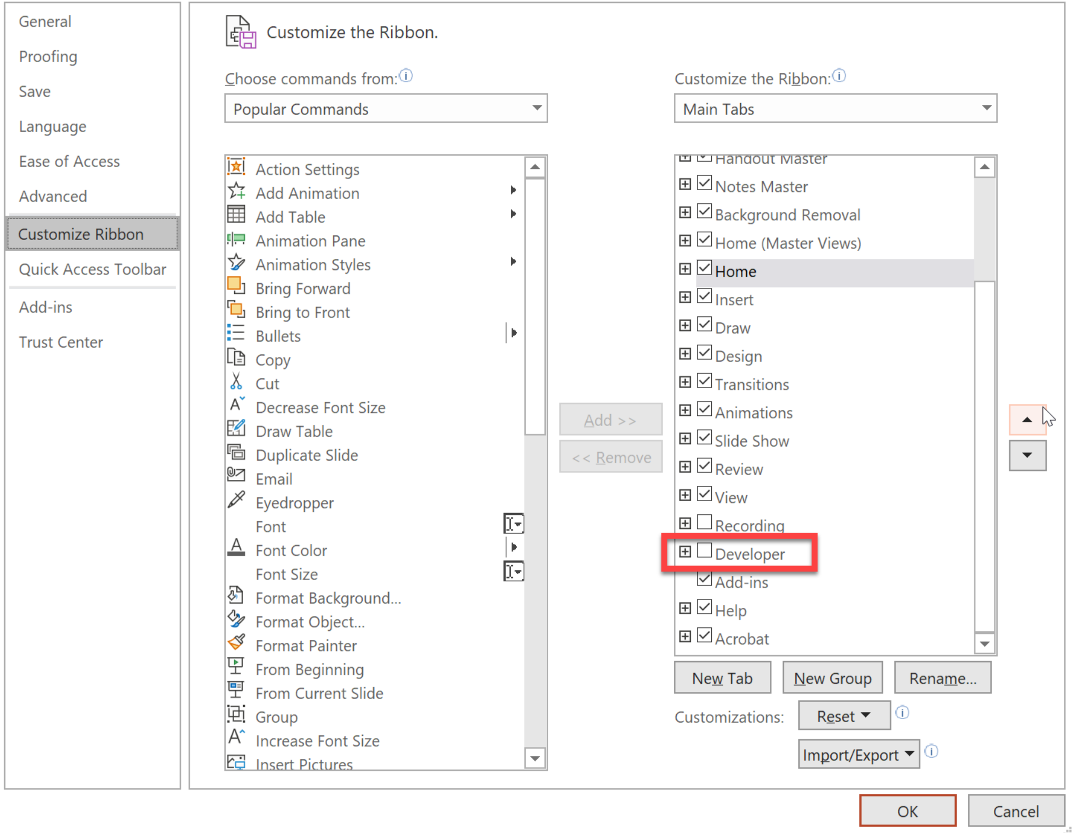
Root cause of most attacks

- Attack vector since 1990s
- Is able to deliver many different payloads
- Successors?
  - Power Automate and App can’t help like for Access DB’s!
  - Office Scripts on the Web https://techcommunity.microsoft.com/t5/excel-blog/announcing-office-scripts-preview/ba-p/1093559



kaspersky

How to show the Developer Tools



Customize the Ribbon.

Choose commands from: Popular Commands

Customize the Ribbon: Main Tabs

- ☑ Handout Master
- ☑ Notes Master
- ☑ Background Removal
- ☑ Home (Master Views)
- ☑ Home
- ☑ Insert
- ☑ Draw
- ☑ Design
- ☑ Transitions
- ☑ Animations
- ☑ Slide Show
- ☑ Review
- ☑ View
- ☐ Recording
- ☐ Developer
- ☑ Add-ins
- ☑ Help
- ☑ Acrobat

How can a malicious macro look like?

Simple Script

5 Rules to master Office Macros

- Disabling / Restrict Macro’s whenever possible
- Enable Attack Surface Reduction Rules
- Manage Trusted Locations / Publishers
- Microsoft Defender for Endpoints and Office 365
- Leverage Application Guard when available

Defense in depth

Defender for Office

Safe Attachments

Trust Center

Office Macro Settings

AMSI

Antimalware
Scan Interface

ASR & MDE

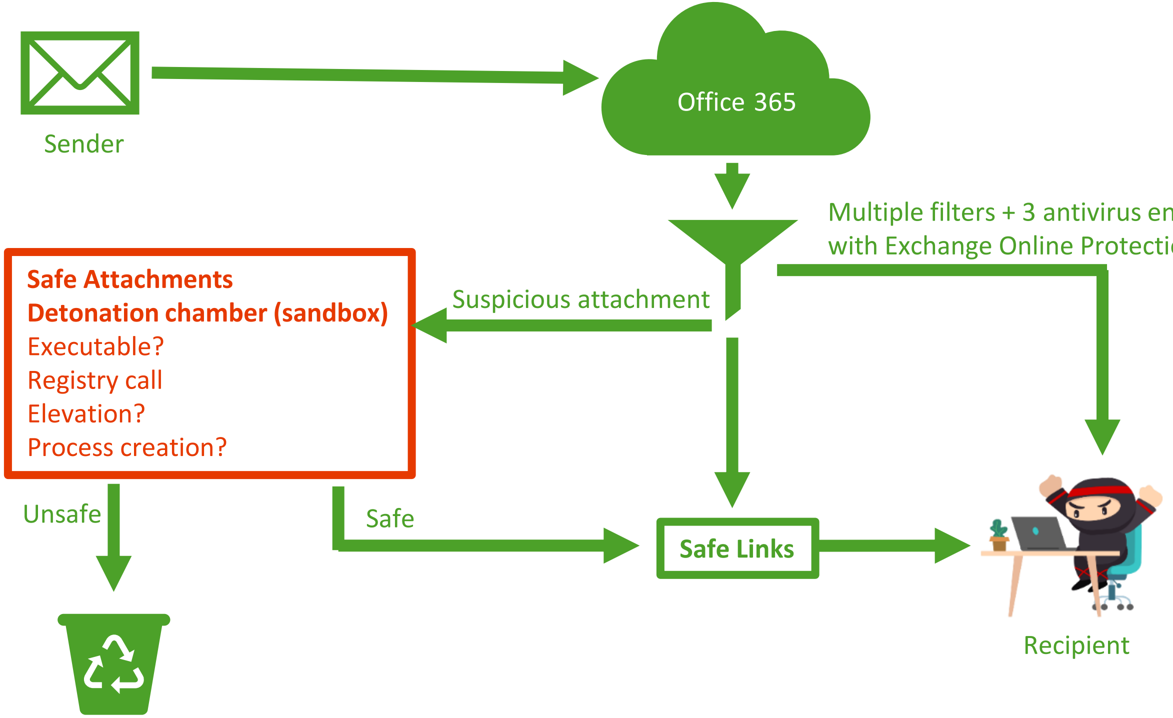
Windows Defender Exploit Guard
- Attack Surface Reduction

Application Guard

Application Guard for ProPlus

Defender for Office 365

Safe Attachment



Sender
Office 365
Multiple filters + 3 antivirus engines
with Exchange Online Protections
Suspicious attachment
Safe Links
Safe
Unsafe
Recipient

Safe Attachments
Detonation chamber (sandbox)
Executable?
Registry call
Elevation?
Process creation?

Defender for Office 365

- Policy needs to be defined
  - License Assignment is not enough

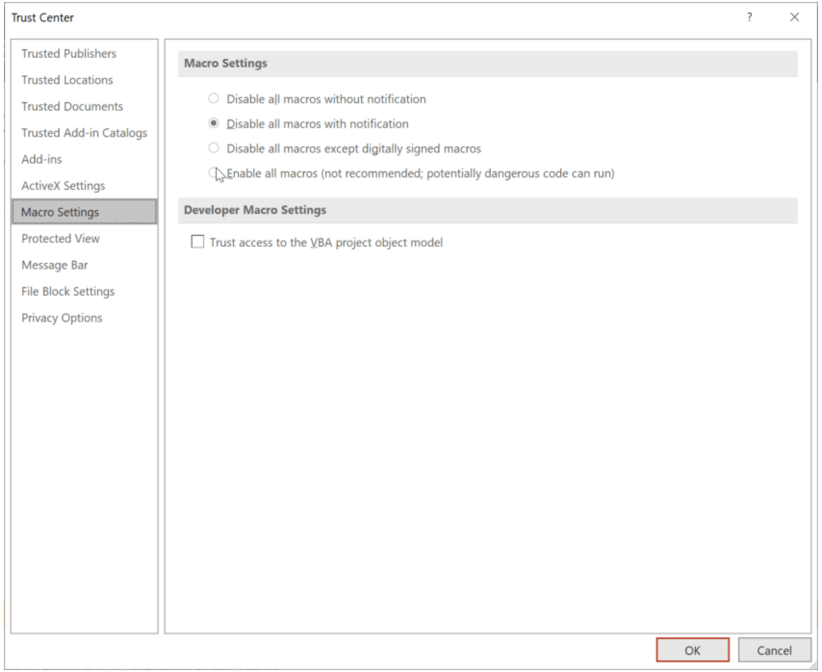
- Detonation chamber detection by Attackers
  - Windows 10 Hyper-V VM
  - 1Gb RAM (was), 1 core
  - Fake user and decoy content
  - Office apps + Adobe Reader + 3rd party browsers

- More information:
  - Microsoft Docs
  - Bypass SafeAttachment for specific senders

Trust Center

Trust Center

- Focus on Macro Settings and Trusted Location



Macro Settings

○ Disable all macros without notification

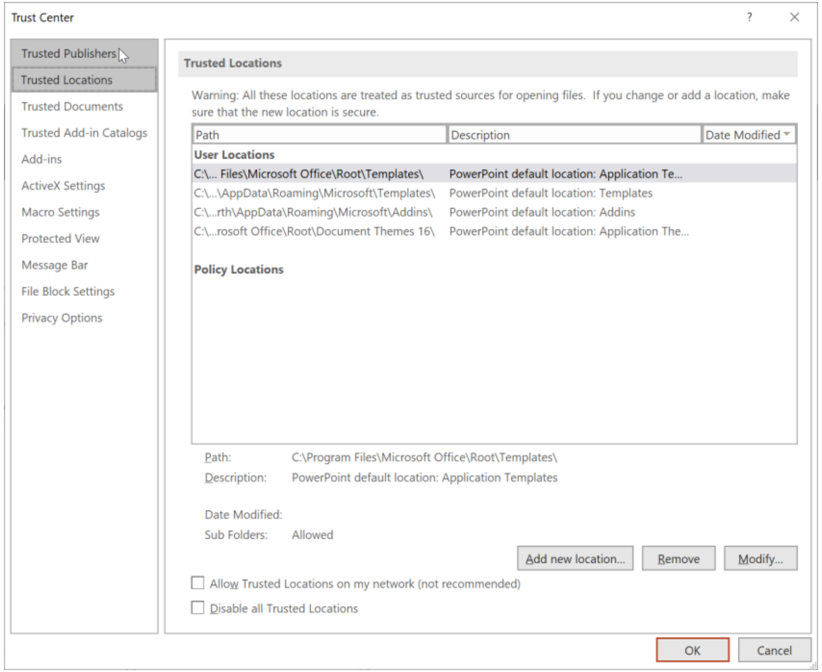
● Disable all macros with notification

○ Disable all macros except digitally signed macros

○ Enable all macros (not recommended; potentially dangerous code can run)

Developer Macro Settings

□ Trust access to the VBA project object model



Trusted Locations

Warning: All these locations are treated as trusted sources for opening files. If you change or add a location, make sure that the new location is secure.

Path	Description	Date Modified
User Locations		
C:\... Files\Microsoft Office\Root\Templates\	PowerPoint default location: Application Te...	
C:\...\AppData\Roaming\Microsoft\Templates\	PowerPoint default location: Templates	
C:\...rth\AppData\Roaming\Microsoft\Addins\	PowerPoint default location: Addins	
C:\...rosoft Office\Root\Document Themes 16\	PowerPoint default location: Application The...	
Policy Locations		

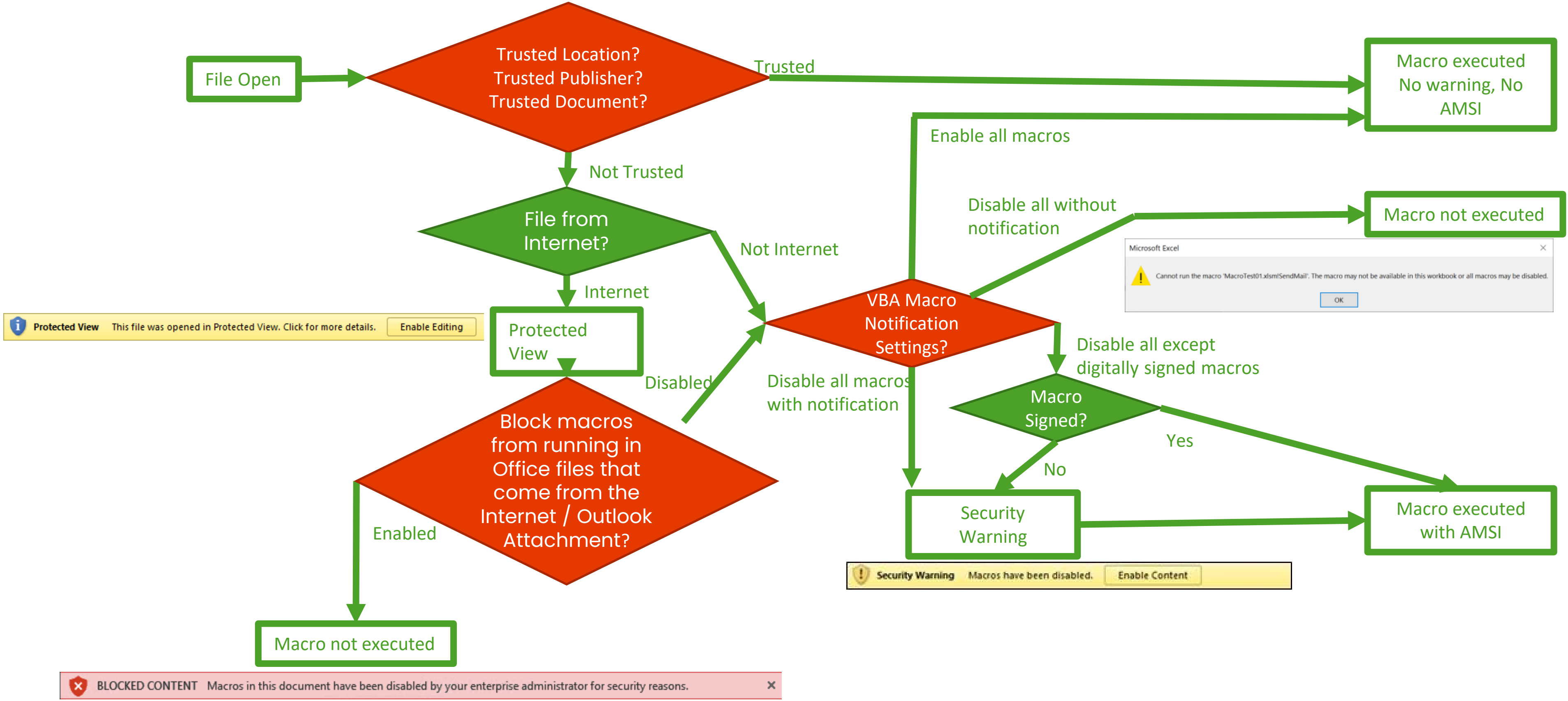
Path: C:\Program Files\Microsoft Office\Root\Templates\
Description: PowerPoint default location: Application Templates

Date Modified:
Sub Folders: Allowed

□ Allow Trusted Locations on my network (not recommended)

□ Disable all Trusted Locations

Trust Center



Protected View This file was opened in Protected View. Click for more details.

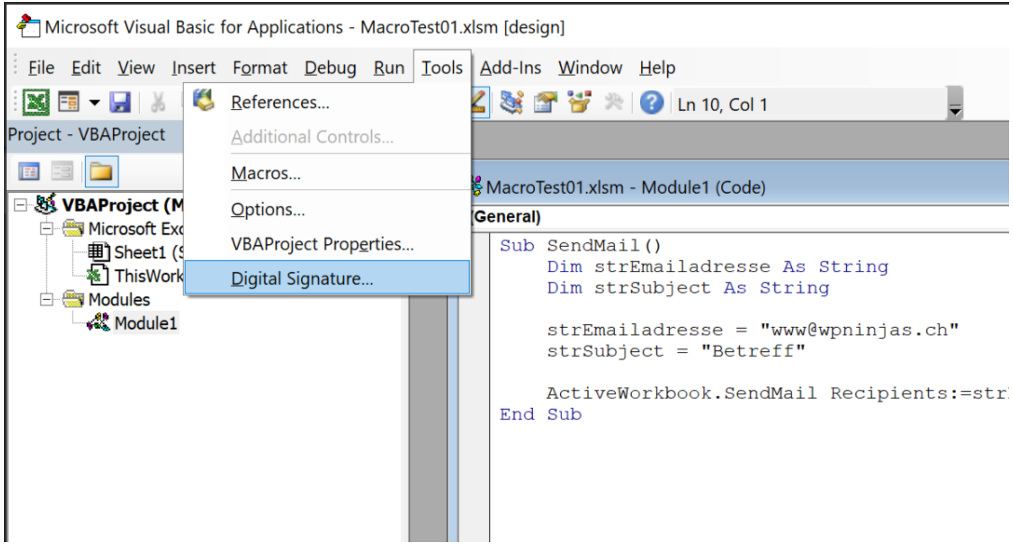
Microsoft Excel

Cannot run the macro 'MacroTest01.xlsm!SendMail'. The macro may not be available in this workbook or all macros may be disabled.

Security Warning Macros have been disabled.

BLOCKED CONTENT Macros in this document have been disabled by your enterprise administrator for security reasons.

Codesign Macro not complicated

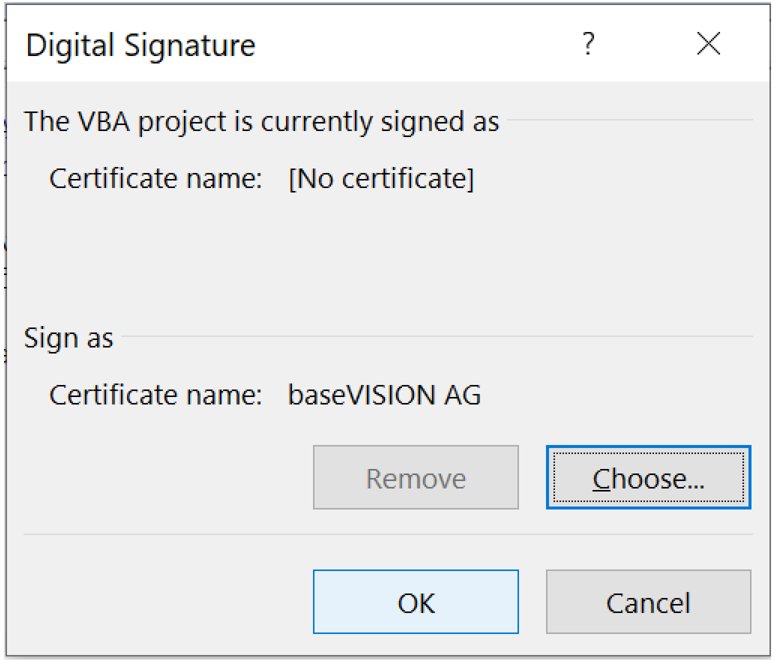


Microsoft Visual Basic for Applications - MacroTest01.xlsm [design]

```
Sub SendMail()
    Dim strEmailadresse As String
    Dim strSubject As String

    strEmailadresse = "www@wpninjas.ch"
    strSubject = "Betreff"

    ActiveWorkbook.SendMail Recipients:=str
End Sub
```



Digital Signature

The VBA project is currently signed as

Certificate name: [No certificate]

Sign as

Certificate name: baseVISION AG

Recommendation

- Block Macros from Internet
- Block Macros in Office Applications where you don’t use Macros
- Trusted Locations / Documents / Publishers
  - Use Code Signing to leverage Trusted Publisher Capability
  - Limit Locations
- Take decision from End-User

MEM Policy Experience

Virus Scan & AMSI

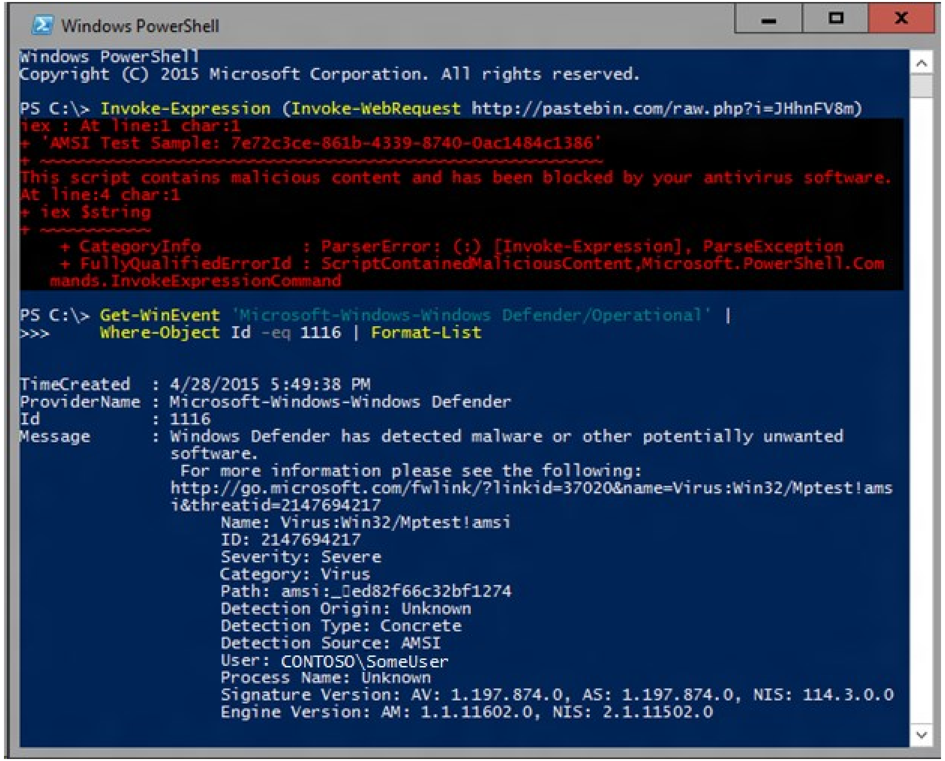
Virus Scan

- Detect known patterns and behaviors
- File based threats
- Most framework generated / Script Kiddie Attacks can be detected

AMSI – Antimalware Scan Interface

- Virus Scan must support AMSI
- The AMSI feature is integrated into these components of Windows 10.
  - User Account Control, or UAC (elevation of EXE, COM, MSI, or ActiveX installation)
  - PowerShell (scripts, interactive use, and dynamic code evaluation)
  - Windows Script Host (wscript.exe and cscript.exe)
  - JavaScript and VBScript
  - Office VBA macros

AMSI in Action

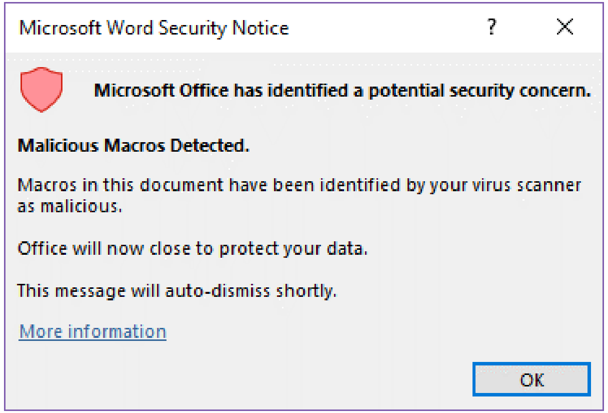


```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\> Invoke-Expression (Invoke-WebRequest http://pastebin.com/raw.php?i=JHhnFV8m)
iex : At line:1 char:1
+ 'AMSI Test Sample: 7e72c3ce-861b-4339-8740-0ac1484c1386'
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
At line:4 char:1
+ iex $string
+ ~~~~~~~~~~~
    + CategoryInfo          : ParserError: (:) [Invoke-Expression], ParseException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent,Microsoft.PowerShell.Com
   mands.InvokeExpressionCommand

PS C:\> Get-WinEvent 'Microsoft-Windows-Windows Defender/Operational' |
>>>     Where-Object Id -eq 1116 | Format-List


TimeCreated  : 4/28/2015 5:49:38 PM
ProviderName : Microsoft-Windows-Windows Defender
Id           : 1116
Message      : Windows Defender has detected malware or other potentially unwanted
               software.
                For more information please see the following:
               http://go.microsoft.com/fwlink/?linkid=37020&name=Virus:Win32/Mptest!ams
               i&threatid=2147694217
                    Name: Virus:Win32/Mptest!amsi
                    ID: 2147694217
                    Severity: Severe
                    Category: Virus
                    Path: amsi:_▯ed82f66c32bf1274
                    Detection Origin: Unknown
                    Detection Type: Concrete
                    Detection Source: AMSI
                    User: CONTOSO\SomeUser
                    Process Name: Unknown
                    Signature Version: AV: 1.197.874.0, AS: 1.197.874.0, NIS: 114.3.0.0
                    Engine Version: AM: 1.1.11602.0, NIS: 2.1.11502.0
```



Microsoft Office has identified a potential security concern.

Malicious Macros Detected.

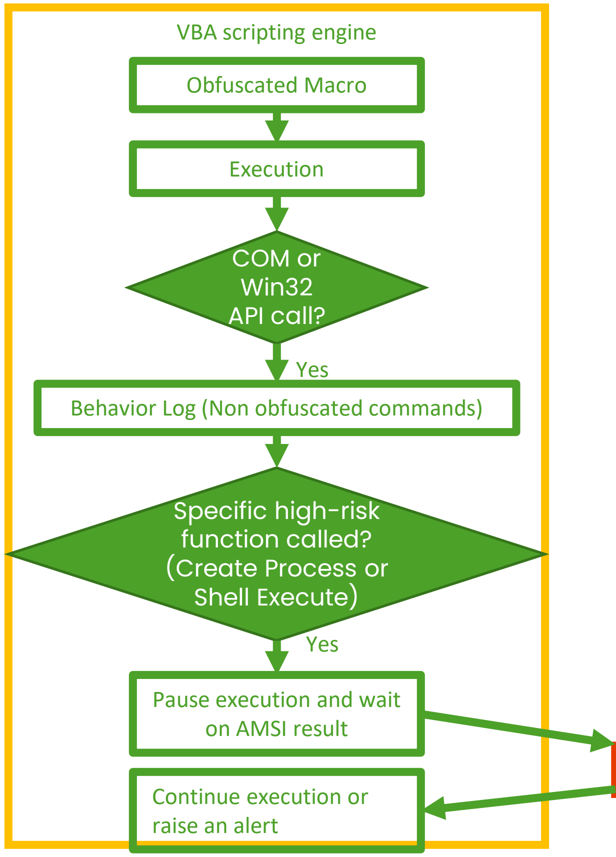
Macros in this document have been identified by your virus scanner as malicious.

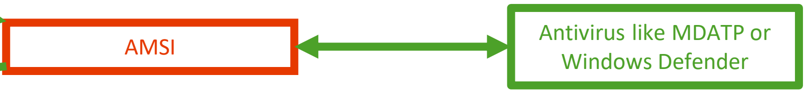
Office will now close to protect your data.

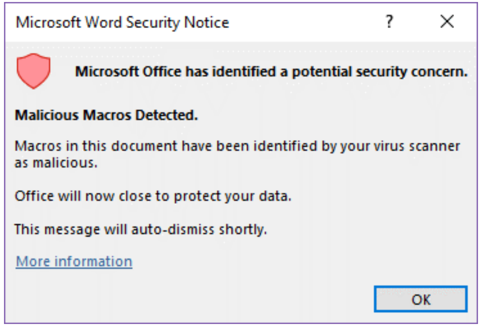
This message will auto-dismiss shortly.

More information

AMSI


VBA scripting engine
Obfuscated Macro
Execution
COM or Win32 API call?
Yes
Behavior Log (Non obfuscated commands)
Specific high-risk function called? (Create Process or Shell Execute)
Yes
Pause execution and wait on AMSI result
Continue execution or raise an alert





Microsoft Office has identified a potential security concern.

Malicious Macros Detected.

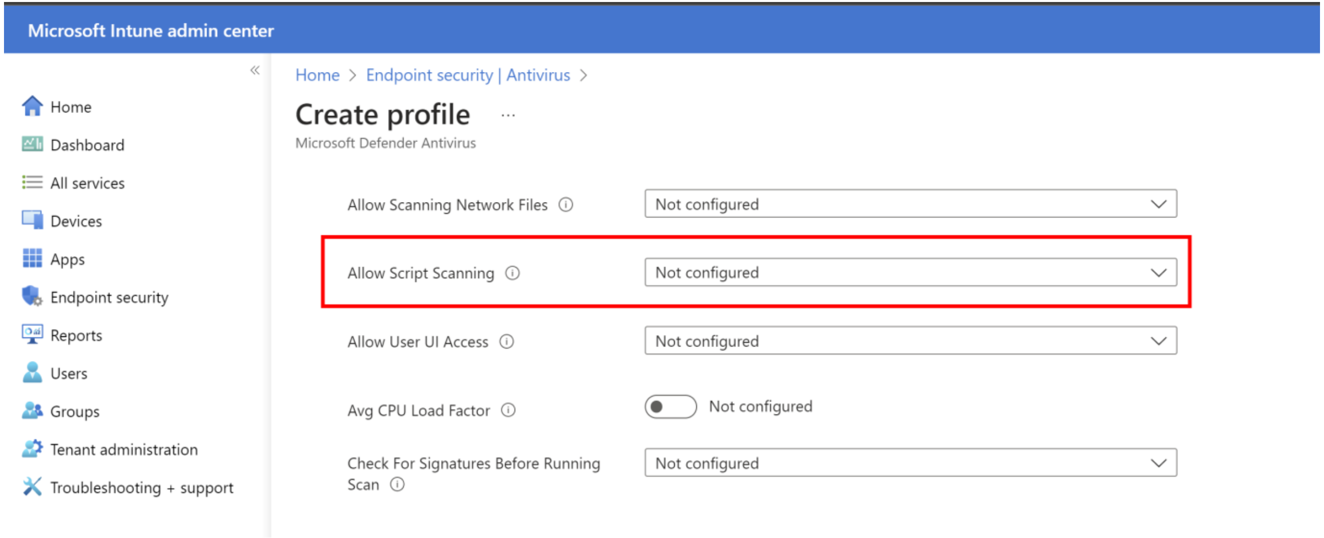
Macros in this document have been identified by your virus scanner as malicious.

Office will now close to protect your data.

This message will auto-dismiss shortly.

More information

- Microsoft Defender Antivirus



Microsoft Intune admin center

Home > Endpoint security | Antivirus >

Create profile ...

Microsoft Defender Antivirus

Allow Scanning Network Files ⓘ: Not configured

Allow Script Scanning ⓘ: Not configured

Allow User UI Access ⓘ: Not configured

Avg CPU Load Factor ⓘ: Not configured

Check For Signatures Before Running Scan ⓘ: Not configured

Attack Surface Reduction (ASR) and Defender for Endpoints

ASR Rules for Office

- Rules
  - Block all Office applications from creating child processes
  - Block execution of potentially obfuscated scripts
  - Block Win32 API calls from Office macro
  - Block Office applications from creating executable content
  - Block Office applications from injecting code into other processes
  - Block Office communication applications from creating child processes
  - Block executable content from email client and webmail
- Modes
  - Not Configured
  - Audit
  - Block

ASR - Enablement

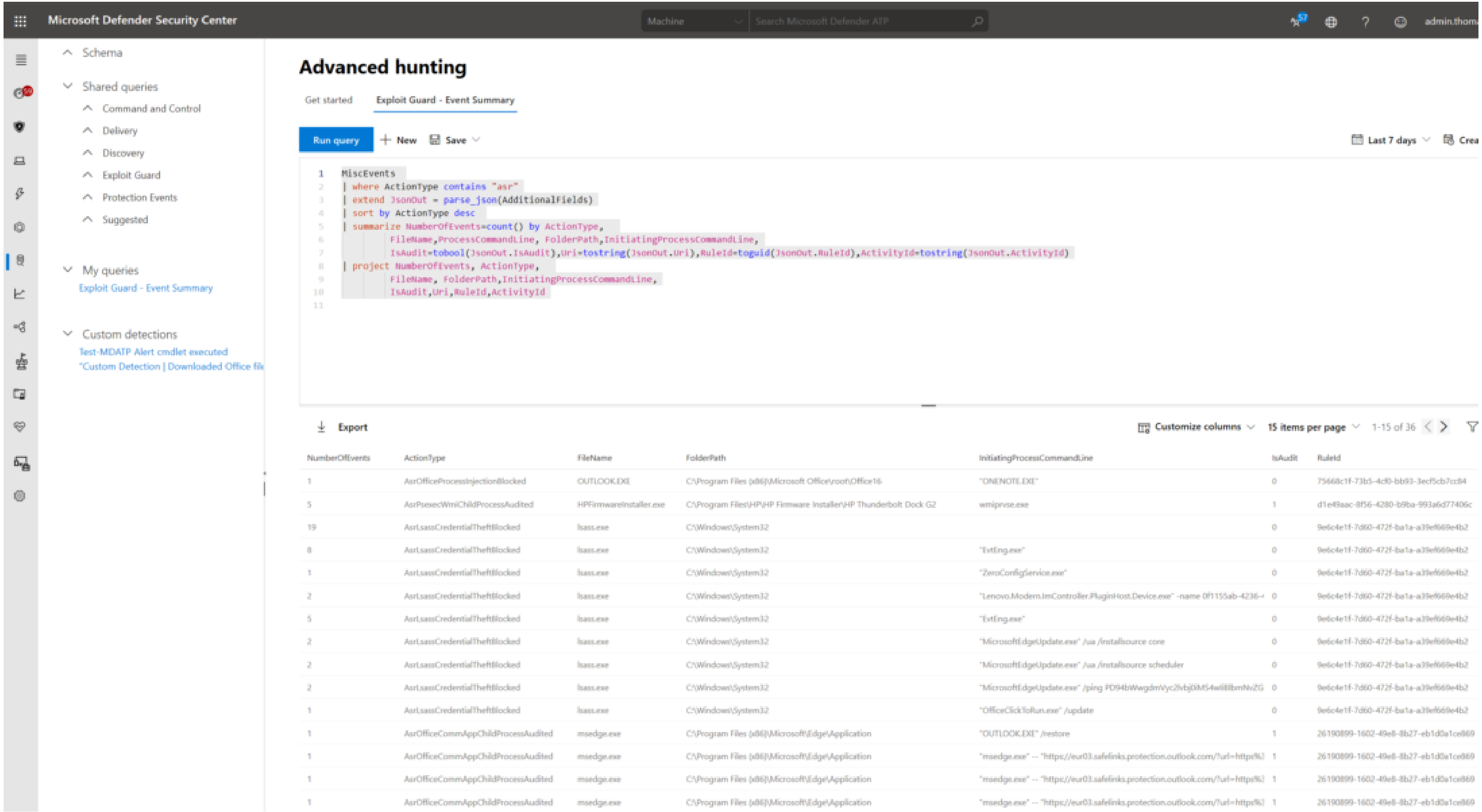
- Implementation Steps
  - Start with Audit Mode
  - Monitor
  - Enable Block Mode

- More information:
  - Microsoft Docs
  - Alex Verboon: Collect ASR logs with PowerShell
  - Microsoft Security Blog

Analyze ASR with MDATP

```
DeviceEvents
| where ActionType contains "asr"
| extend JsonOut = parse_json(AdditionalFields)
| sort by ActionType desc
| summarize NumberOfEvents=count() by ActionType,
FileName,ProcessCommandLine, FolderPath,InitiatingProcessCommandLine,
IsAudit=tobool(JsonOut.IsAudit),RuleId=toguid(JsonOut.RuleId)
| project NumberOfEvents, ActionType,
FileName, FolderPath,InitiatingProcessCommandLine,IsAudit,RuleId
```

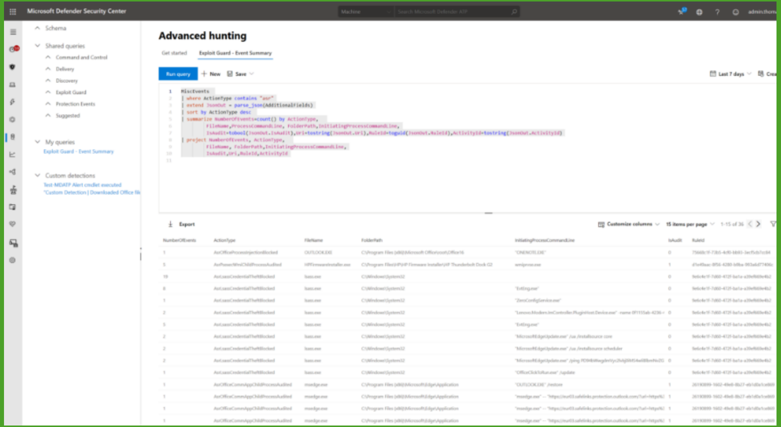
Analyze ASR with MDE



```
MiscEvents
| where ActionType contains "asr"
| extend JsonOut = parse_json(AdditionalFields)
| sort by ActionType desc
| summarize NumberOfEvents=count() by ActionType,
        FileName,ProcessCommandLine, FolderPath,InitiatingProcessCommandLine,
        IsAudit=tobool(JsonOut.IsAudit),Uri=tostring(JsonOut.Uri),RuleId=toguid(JsonOut.RuleId),ActivityId=tostring(JsonOut.ActivityId)
| project NumberOfEvents, ActionType,
        FileName, FolderPath,InitiatingProcessCommandLine,
        IsAudit,Uri,RuleId,ActivityId
```

NumberOfEvents	ActionType	FileName	FolderPath	InitiatingProcessCommandLine	IsAudit	RuleId
1	AsrOfficeProcessInjectionBlocked	OUTLOOK.EXE	C:\Program Files (x86)\Microsoft Office\root\Office16	"ONENOTE.EXE"	0	75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84
5	AsrPsexecWmiChildProcessAudited	HPFirmwareInstaller.exe	C:\Program Files\HP\HP Firmware Installer\HP Thunderbolt Dock G2	wmiprvse.exe	1	d1e49aac-8f56-4280-b9ba-993a6d77406c
19	AsrLsassCredentialTheftBlocked	lsass.exe	C:\Windows\System32		0	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
8	AsrLsassCredentialTheftBlocked	lsass.exe	C:\Windows\System32	"EvtEng.exe"	0	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
1	AsrLsassCredentialTheftBlocked	lsass.exe	C:\Windows\System32	"ZeroConfigService.exe"	0	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
2	AsrLsassCredentialTheftBlocked	lsass.exe	C:\Windows\System32	"Lenovo.Modern.ImController.PluginHost.Device.exe" -name 0f1155ab-4236-4	0	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
5	AsrLsassCredentialTheftBlocked	lsass.exe	C:\Windows\System32	"EvtEng.exe"	0	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
2	AsrLsassCredentialTheftBlocked	lsass.exe	C:\Windows\System32	"MicrosoftEdgeUpdate.exe" /ua /installsource core	0	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
2	AsrLsassCredentialTheftBlocked	lsass.exe	C:\Windows\System32	"MicrosoftEdgeUpdate.exe" /ua /installsource scheduler	0	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
2	AsrLsassCredentialTheftBlocked	lsass.exe	C:\Windows\System32	"MicrosoftEdgeUpdate.exe" /ping PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZG	0	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
1	AsrLsassCredentialTheftBlocked	lsass.exe	C:\Windows\System32	"OfficeClickToRun.exe" /update	0	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
1	AsrOfficeCommAppChildProcessAudited	msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application	"OUTLOOK.EXE" /restore	1	26190899-1602-49e8-8b27-eb1d0a1ce869
1	AsrOfficeCommAppChildProcessAudited	msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application	"msedge.exe" -- "https://eur03.safelinks.protection.outlook.com/?url=https%3	1	26190899-1602-49e8-8b27-eb1d0a1ce869
1	AsrOfficeCommAppChildProcessAudited	msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application	"msedge.exe" -- "https://eur03.safelinks.protection.outlook.com/?url=https%3	1	26190899-1602-49e8-8b27-eb1d0a1ce869
1	AsrOfficeCommAppChildProcessAudited	msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application	"msedge.exe" -- "https://eur03.safelinks.protection.outlook.com/?url=https%3	1	26190899-1602-49e8-8b27-eb1d0a1ce869

Defender for Endpoints Recommendation and Advanced Hunting



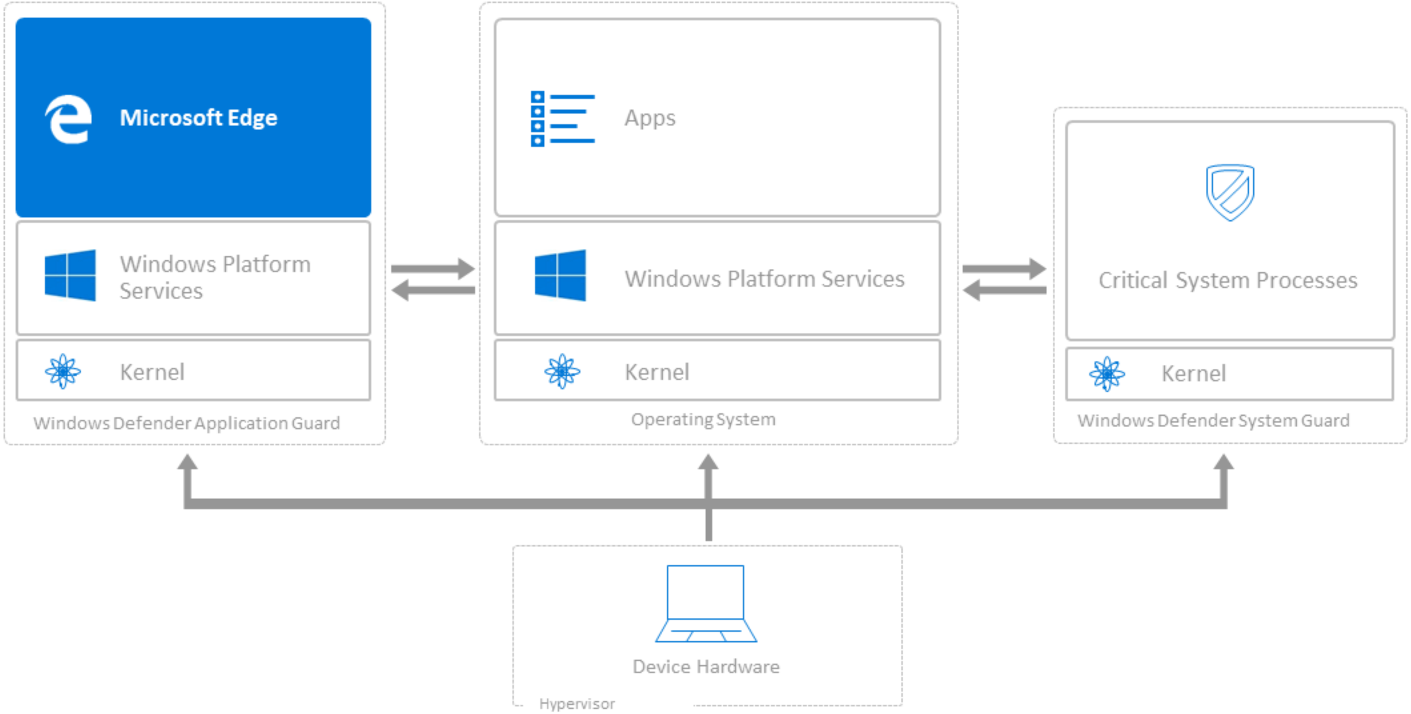
Advanced hunting

```
MiscEvents
| where ActionType contains "asr"
| extend JsonOut = parse_json(AdditionalFields)
| sort by ActionType desc
| summarize NumberOfEvents=count() by ActionType,
        FileName,ProcessCommandLine, FolderPath,InitiatingProcessCommandLine,
        IsAudit=tobool(JsonOut.IsAudit),Uri=tostring(JsonOut.Uri),RuleId=toguid(JsonOut.RuleId),ActivityId=tostring(JsonOut.ActivityId)
| project NumberOfEvents, ActionType,
        FileName, FolderPath,InitiatingProcessCommandLine,
        IsAudit,Uri,RuleId,ActivityId
```

NumberOfEvents	ActionType	FileName	FolderPath	InitiatingProcessCommandLine	IsAudit	RuleId
1	AsrOfficeProcessInjectionBlocked	OUTLOOK.EXE	C:\Program Files (x86)\Microsoft Office\root\Office16	"ONENOTE.EXE"	0	75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84
5	AsrPsexecWmiChildProcessAudited	HPFirmwareInstaller.exe	C:\Program Files\HP\HP Firmware Installer\HP Thunderbolt Dock G2	wmiprvse.exe	1	d1e49aac-8f56-4280-b9ba-993a6d77406c
19	AsrLsassCredentialTheftBlocked	lsass.exe	C:\Windows\System32		0	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
8	AsrLsassCredentialTheftBlocked	lsass.exe	C:\Windows\System32	"EvtEng.exe"	0	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
1	AsrLsassCredentialTheftBlocked	lsass.exe	C:\Windows\System32	"ZeroConfigService.exe"	0	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
2	AsrLsassCredentialTheftBlocked	lsass.exe	C:\Windows\System32	"Lenovo.Modern.ImController.PluginHost.Device.exe" -name 0f1155ab-4236-‹	0	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
5	AsrLsassCredentialTheftBlocked	lsass.exe	C:\Windows\System32	"EvtEng.exe"	0	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
2	AsrLsassCredentialTheftBlocked	lsass.exe	C:\Windows\System32	"MicrosoftEdgeUpdate.exe" /ua /installsource core	0	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
2	AsrLsassCredentialTheftBlocked	lsass.exe	C:\Windows\System32	"MicrosoftEdgeUpdate.exe" /ua /installsource scheduler	0	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
2	AsrLsassCredentialTheftBlocked	lsass.exe	C:\Windows\System32	"MicrosoftEdgeUpdate.exe" /ping PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZG	0	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
1	AsrLsassCredentialTheftBlocked	lsass.exe	C:\Windows\System32	"OfficeClickToRun.exe" /update	0	9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
1	AsrOfficeCommAppChildProcessAudited	msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application	"OUTLOOK.EXE" /restore	1	26190899-1602-49e8-8b27-eb1d0a1ce869
1	AsrOfficeCommAppChildProcessAudited	msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application	"msedge.exe" -- "https://eur03.safelinks.protection.outlook.com/?url=https%3	1	26190899-1602-49e8-8b27-eb1d0a1ce869
1	AsrOfficeCommAppChildProcessAudited	msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application	"msedge.exe" -- "https://eur03.safelinks.protection.outlook.com/?url=https%3	1	26190899-1602-49e8-8b27-eb1d0a1ce869
1	AsrOfficeCommAppChildProcessAudited	msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application	"msedge.exe" -- "https://eur03.safelinks.protection.outlook.com/?url=https%3	1	26190899-1602-49e8-8b27-eb1d0a1ce869

Application Guard for Office Apps

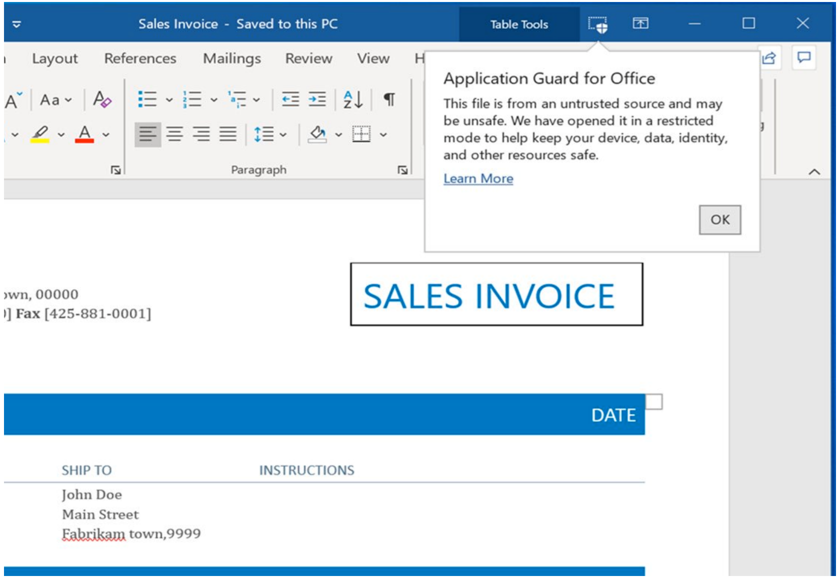
Application Guard


Microsoft Edge
Windows Platform Services
Kernel
Windows Defender Application Guard
Apps
Windows Platform Services
Kernel
Operating System
Critical System Processes
Kernel
Windows Defender System Guard
Device Hardware
Hypervisor

Application Guard for ProPlus

- Container-based isolation
- Available for Microsoft 365 E5 and E5 Security

- More information
  - [Microsoft Security Blog]



Application Guard for Office

This file is from an untrusted source and may be unsafe. We have opened it in a restricted mode to help keep your device, data, identity, and other resources safe.

Learn More

own, 00000
] Fax [425-881-0001]

SALES INVOICE

DATE

SHIP TO

INSTRUCTIONS

John Doe
Main Street
Fabrikam town,9999

Questions and Discussions

Tips

1. **Start today**
2. **Use Defense in Depth**
3. **E5 is not just expensive**

Key takeaways

- Disabling / Restrict Macro’s whenever possible
- Enable Attack Surface Reduction Rules
- Manage Trusted Locations / Publishers
- Microsoft Defender for Endpoints and Office 365
- Leverage Application Guard when required