Living Off the Walled Garden: Abusing the Features of the Early Launch Antimalware Ecosystem

Hi!

Matt Graeber

Director, Threat Research @ Red Canary

Who protects the protector?

Introduction to ELAM and PPL

Previous work - Everything is derivative

Unknown Known DLLs

... and other Code Integrity Trust Violations

@aionescu
@tiraniddo

Recon Montreal
2018

Thank you James and Alex!

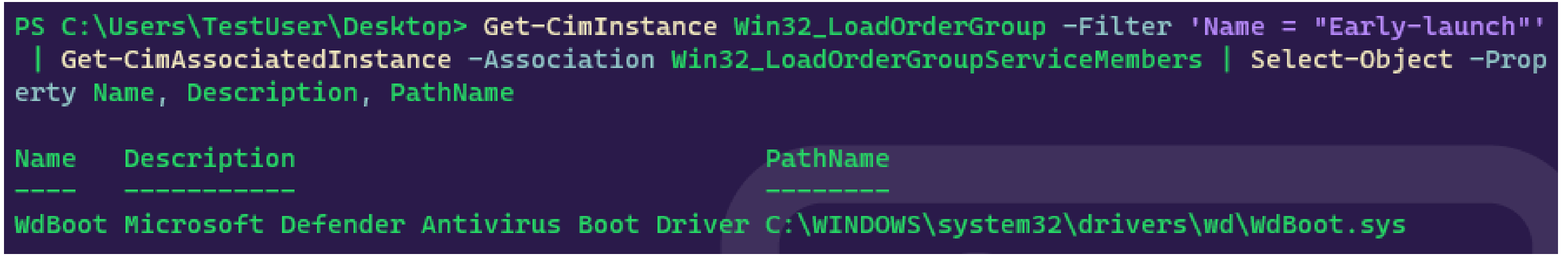
Protected Process Light Protections

- Designed to prevent tampering in user-mode, even as admin.
- Cannot start or stop protected processes
- Cannot get a handle to a protected process
- Cannot attach a debugger to a protected process
- To run protected, an executable must meet specific signing requirements.

Early Launch AntiMalware (ELAM) Drivers

- Microsoft's supported 3rd party security product anti-tampering mechanism.
- Specifies certificate hashes allowed to run at the Antimalware-Light PPL protection level
- "Microsoft requires that Early Launch Antimalware vendors be members of the Microsoft Virus Initiative (MVI)."
- Vendors must pass the WHQL driver submission.

Enumerating installed ELAM drivers



```
PS C:\Users\TestUser\Desktop> Get-CimInstance Win32_LoadOrderGroup -Filter 'Name = "Early-launch"'
 | Get-CimAssociatedInstance -Association Win32_LoadOrderGroupServiceMembers | Select-Object -Prop
erty Name, Description, PathName

Name   Description                              PathName
----   -----------                              --------
WdBoot Microsoft Defender Antivirus Boot Driver C:\WINDOWS\system32\drivers\wd\WdBoot.sys
```

Early Launch AntiMalware (ELAM) Driver Hashes

- Certificate hashes are To-Be-Signed (TBS) hashes.
- TBS hash is not the same as a Thumbprint!
- Tools to calculate TBS hash:
  - certmgr.exe (Windows SDK)
  - Get-TBSHash
- VirusTotal doesn’t understand TBS hashes…

ELAM Driver Signer Resource

```
MicrosoftElamCertificateInfo  MSElamCertInfoID
{
      3, // count of entries
      L”CertHash1\0”,
      Algorithm,
      L”EKU1\0”,
      L”CertHash2\0”,
      Algorithm,
      L”\0”, //No EKU for cert hash 2
      L”CertHash3\0”,
      Algorithm,
      L”EKU3a;EKU3b;EKU3c\0”,  //multiple EKU entries supported (max: 3)
}
```

Protecting anti-malware services

An Example Parsed ELAM Ruleset - WdBoot.sys

- Allow Rule #1

SignerHash: `f6f717a43ad9abddc8cefdde1c505462535e7d1307e630f9544a2d14fe8bf26e`

SignerHashAlgorithm: `SHA256`

SignerEKUs: `1.3.6.1.4.1.311.76.8.1;1.3.6.1.4.1.311.76.11.1`

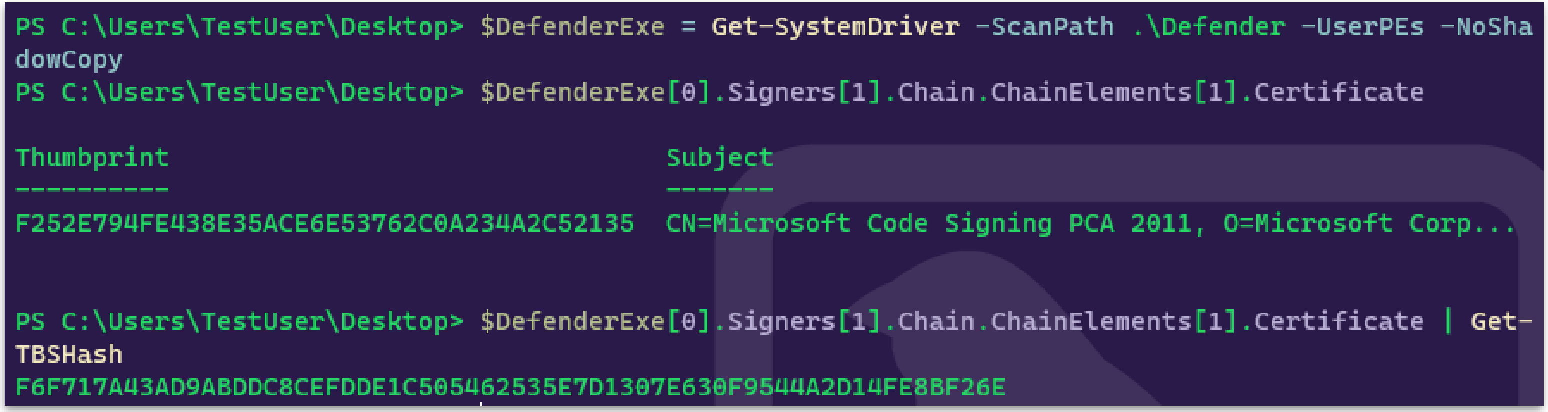
- Allow Rule #2

SignerHash: `4e80be107c860de896384b3eff50504dc2d76ac7151df3102a4450637a032146`

SignerHashAlgorithm: `SHA256`

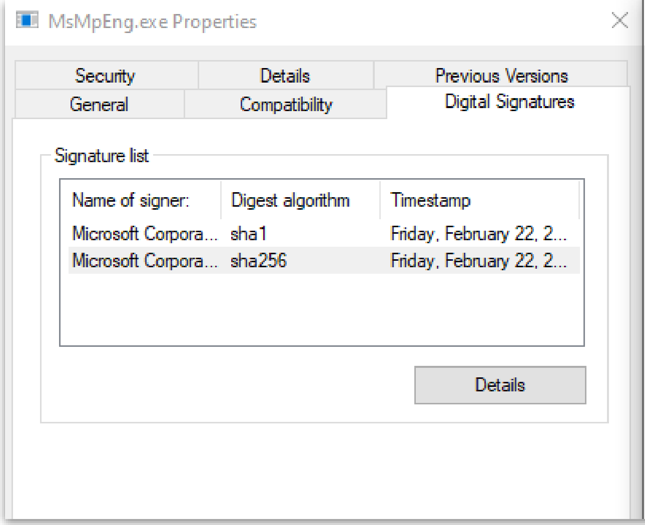
SignerEKUs: `1.3.6.1.4.1.311.76.8.1;1.3.6.1.4.1.311.76.11.1`

ELAM Ruleset - WdBoot.sys



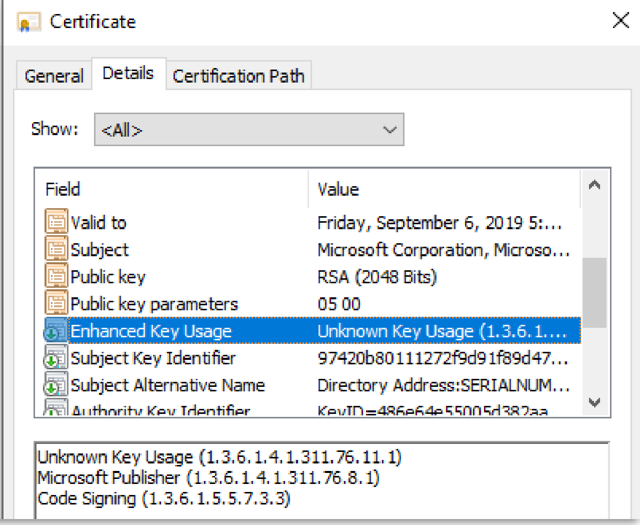
```
PS C:\Users\TestUser\Desktop> $DefenderExe = Get-SystemDriver -ScanPath .\Defender -UserPEs -NoSha
dowCopy
PS C:\Users\TestUser\Desktop> $DefenderExe[0].Signers[1].Chain.ChainElements[1].Certificate

Thumbprint                                Subject
----------                                -------
F252E794FE438E35ACE6E53762C0A234A2C52135  CN=Microsoft Code Signing PCA 2011, O=Microsoft Corp...


PS C:\Users\TestUser\Desktop> $DefenderExe[0].Signers[1].Chain.ChainElements[1].Certificate | Get-
TBSHash
F6F717A43AD9ABDDC8CEFDDE1C505462535E7D1307E630F9544A2D14FE8BF26E
```

ELAM Ruleset - WdBoot.sys



Signature list

Name of signer:	Digest algorithm	Timestamp
Microsoft Corpora...	sha1	Friday, February 22, 2...
Microsoft Corpora...	sha256	Friday, February 22, 2...

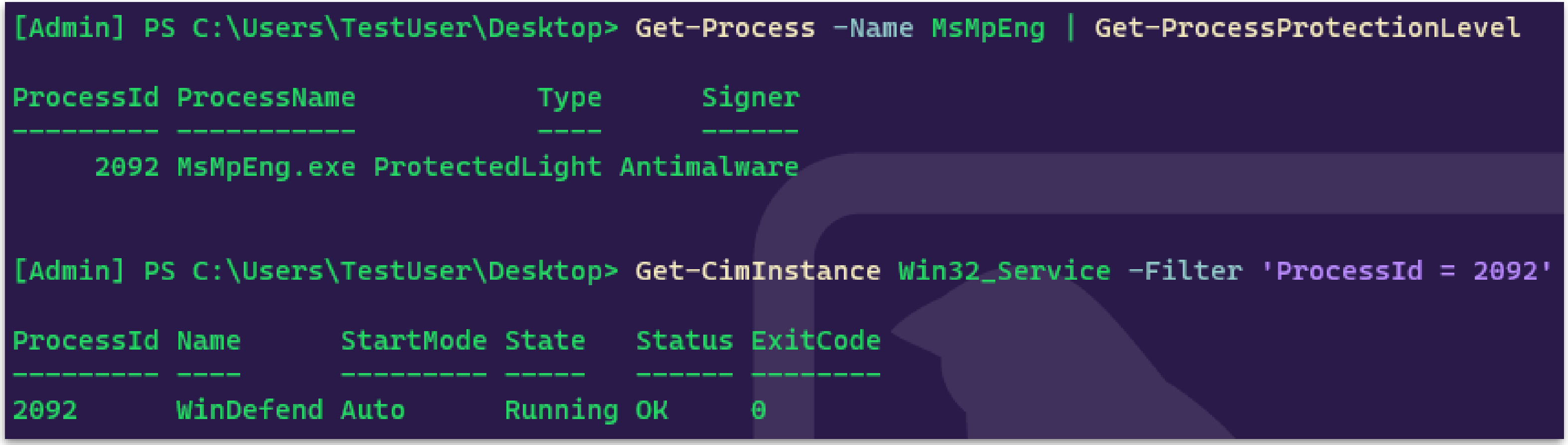


Show: <All>

Field	Value
Valid to	Friday, September 6, 2019 5:...
Subject	Microsoft Corporation, Microso...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Enhanced Key Usage	Unknown Key Usage (1.3.6.1....
Subject Key Identifier	97420b80111272f9d91f89d47...
Subject Alternative Name	Directory Address:SERIALNUM...
Authority Key Identifier	KeyID=486e64e55005d382aa

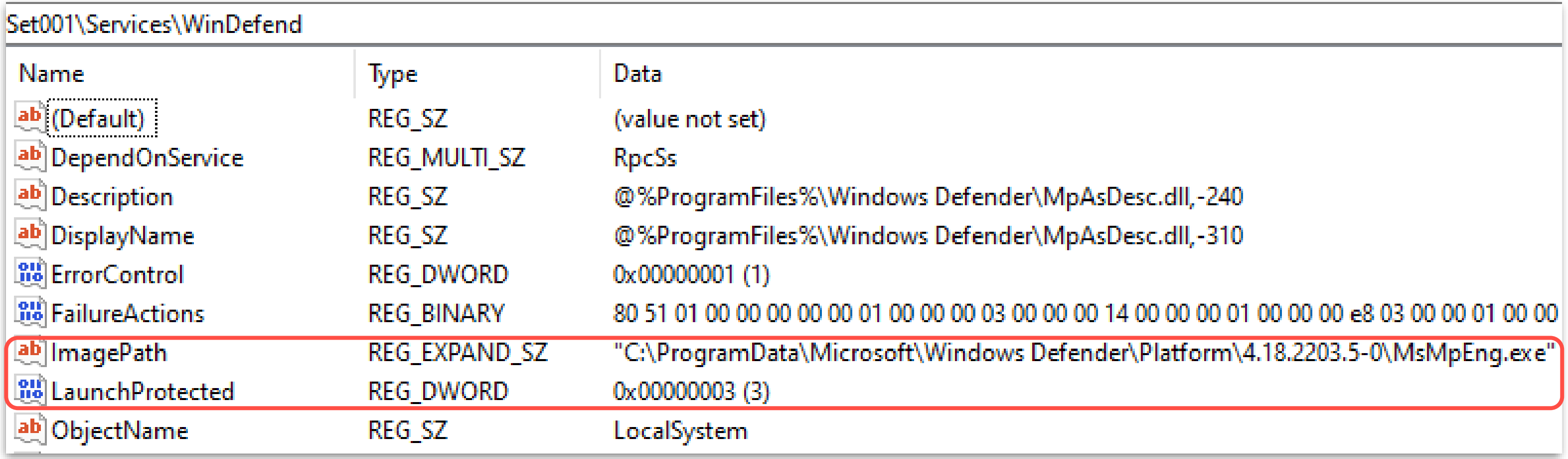
Unknown Key Usage (1.3.6.1.4.1.311.76.11.1)
Microsoft Publisher (1.3.6.1.4.1.311.76.8.1)
Code Signing (1.3.6.1.5.5.7.3.3)

ELAM Ruleset - WdBoot.sys



```
[Admin] PS C:\Users\TestUser\Desktop> Get-Process -Name MsMpEng | Get-ProcessProtectionLevel

ProcessId ProcessName           Type      Signer
--------- -----------           ----      ------
     2092 MsMpEng.exe ProtectedLight Antimalware


[Admin] PS C:\Users\TestUser\Desktop> Get-CimInstance Win32_Service -Filter 'ProcessId = 2092'

ProcessId Name      StartMode State   Status ExitCode
--------- ----      --------- -----   ------ --------
2092      WinDefend Auto      Running OK     0
```

ELAM Ruleset - WdBoot.sys



Set001\Services\WinDefend

Name	Type	Data
(Default)	REG_SZ	(value not set)
DependOnService	REG_MULTI_SZ	RpcSs
Description	REG_SZ	@%ProgramFiles%\Windows Defender\MpAsDesc.dll,-240
DisplayName	REG_SZ	@%ProgramFiles%\Windows Defender\MpAsDesc.dll,-310
ErrorControl	REG_DWORD	0x00000001 (1)
FailureActions	REG_BINARY	80 51 01 00 00 00 00 00 01 00 00 00 03 00 00 00 14 00 00 00 01 00 00 00 e8 03 00 00 01 00 00
ImagePath	REG_EXPAND_SZ	"C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2203.5-0\MsMpEng.exe"
LaunchProtected	REG_DWORD	0x00000003 (3)
ObjectName	REG_SZ	LocalSystem

```
PsProtectedSignerAntimalware = 0n3
```

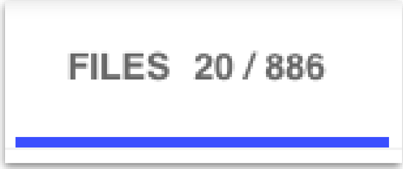
ELAM is an allowlist for Antimalware-Light PPL process execution. What if the allowlist is overly permissive?

ELAM Driver Hunting and Auditing

Hunting for ELAM drivers

VirusTotal search:

```
signature:"Microsoft Windows Early Launch
Anti-malware Publisher"

tag:native tag:signed tag:peexe

not tag:invalid-signature
```



FILES 20 / 886

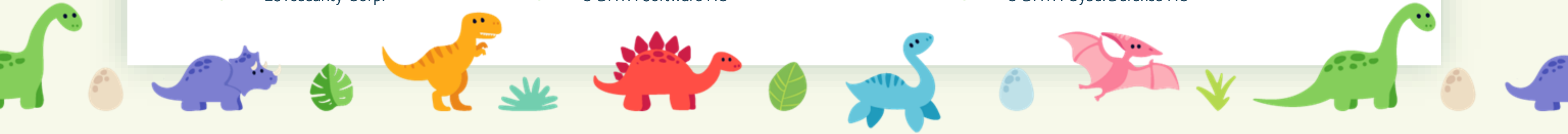
Additional ELAM driver validation

- Confirm the ELAM driver has a valid signature
- The name of the leaf certificate is "Microsoft Windows Early Launch Anti-malware Publisher"
- The driver has a MSELAMCERTINFOID resource consisting of a parsed signer allow list.
- 866⇨766 unique ELAM drivers

Identified ELAM Vendors

- Microsoft Corporation
- McAfee, LLC
- VMware, Inc.
- Total Defense, Inc.

- COMODO
- Broadcom Corporation
- CrowdStrike, Inc.
- Bitdefender
- AO Kaspersky Lab
- ESET
- AVG Technologies CZ, s.r.o.
- AVAST Software
- Cisco Systems, Inc.
- AhnLab, Inc.
- Windows (R) Win 7 DDK provider
- F-Secure Corporation
- Trend Micro Inc.
- Carbon Black, Inc.
- K7 Computing Pvt Ltd
- Sophos Limited
- ESTsecurity Corp.
- Panda Security, S.L.
- Malwarebytes
- Broadcom
- Avira Operations GmbH & Co. KG
- 360.cn
- Doctor Web, Ltd.
- Beijing Rising Network Security Technology Co., Ltd.
- Cynet Security Ltd
- TODO: <Company name>
- Fortinet Inc
- IKARUS Security Software GmbH
- Beijing Huorong Network Technology Co., Ltd.
- ThreatTrack Security, Inc.
- Acronis International GmbH
- BullGuard Ltd.
- Arcabit/mks_vir
- FireEye, Inc.
- Check Point Software Technologies
- Symantec Corporation
- Quick Heal Technologies Ltd.
- 电脑管家
- G DATA Software AG
- Webroot
- Reason CyberSecurity Inc.
- Hammock Corporation
- SentinelOne, Inc.
- Beijing Rising Information Technology Co., Ltd.
- SecureTrust
- Fidelis Cybersecurity
- Faronics Corporation
- IObit
- VIPRE Security
- Emsisoft Ltd
- SecureIT
- Rising
- TG Soft - www.tgsoft.it
- MicroWorld Technologies Inc.
- Avira Operations GmbH
- Wontok, Inc
- TeamViewer
- enSilo
- AdAware
- TeamViewer Germany GmbH
- G DATA CyberDefense AG

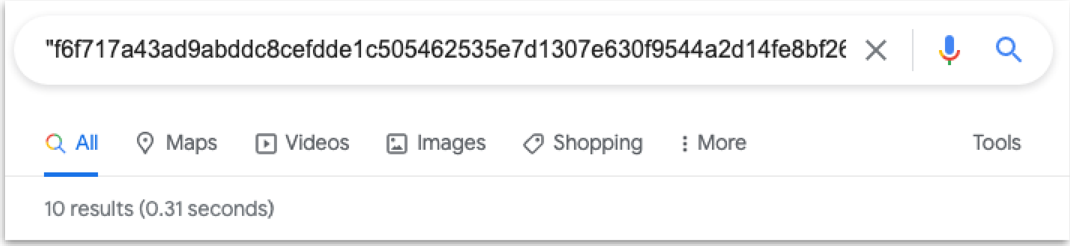


ELAM Auditing Strategy

- Identify the corresponding certificate with the TBS hash.
- Search for EXEs and DLLs signed with that certificate in the chain.
- Identify signed code that might permit code execution.
- Low-hanging fruit: LOLbins?
- Install candidate executables as a protected service.

ELAM Auditing Challenges

- VirusTotal doesn't understand TBS hashes - only Thumbprint
- You are lucky if there are any Google hits…



"f6f717a43ad9abddc8cefdde1c505462535e7d1307e630f9544a2d14fe8bf2

10 results (0.31 seconds)

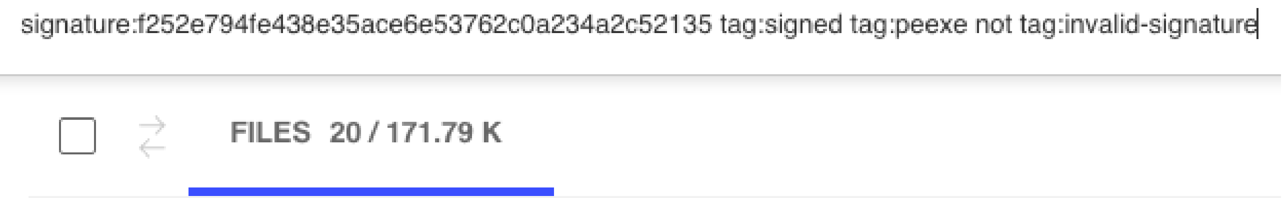
Associating TBS Hash to Thumbprint

- Sometimes you'll get lucky…

```
name: Microsoft Code Signing PCA 2011

issuer: Microsoft Root Certificate Authority 2011

thumbprint: f252e794fe438e35ace6e53762c0a234a2c52135

signature hash: f6f717a43ad9abddc8cefdde1c505462535e7d1307e630f9544a2d14fe8bf26e
```

https://famellee.wordpress.com/2016/09/08/retrieve-digital-signatures-using-wintrust/

Hunting for Potential Protected Executables



signature:f252e794fe438e35ace6e53762c0a234a2c52135 tag:signed tag:peexe not tag:invalid-signature

□ FILES 20 / 171.79 K

Note: this particular rule has an EKU restriction…

- `1.3.6.1.4.1.311.76.8.1` (Microsoft Publisher)
- `1.3.6.1.4.1.311.76.11.1` (Microsoft AntiMalware)

Identified Overly-Permissive Allowed Signers

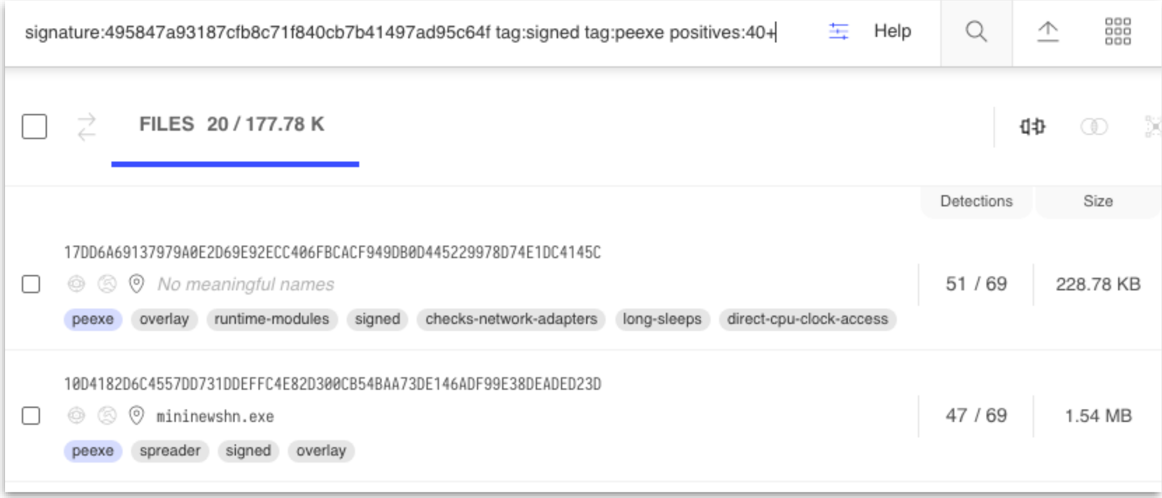
Leaf Certificates

- Microsoft Corporation (Thumbprint: B9EAA034C821C159B05D3521BCF7FEB796EBD6FF)
  - TBS: 84D8717A416C8C9E214C6E0DBD091860D8133F413BCFF35673998F27BBA084CA
- Microsoft Corporation (Thumbprint: 62009AAABDAE749FD47D19150958329BF6FF4B34)
  - TBS: E17764C39F2AFD7114F8528D2F9783D9A591F6679715EECE730A262CF5CFD3B3

Intermediate Certificates

- Symantec Class 3 SHA256 Code Signing CA (Thumbprint: 007790F6561DAD89B0BCD85585762495E358F8A5)
  - TBS: A08E79C386083D875014C409C13D144E0A24386132980DF11FF59737C8489EB1
- VeriSign Class 3 Public Primary Certification Authority - G5 (Thumbprint: 495847a93187cfb8c71f840cb7b41497ad95c64f)
  - TBS: 4843A82ED3B1F2BFBEE9671960E1940C942F688D
- DigiCert Assured ID Code Signing CA-1 (Thumbprint: 409AA4A74A0CDA7C0FEE6BD0BB8823D16B5F1875)
  - TBS: 47F4B9898631773231B32844EC0D49990AC4EB1E

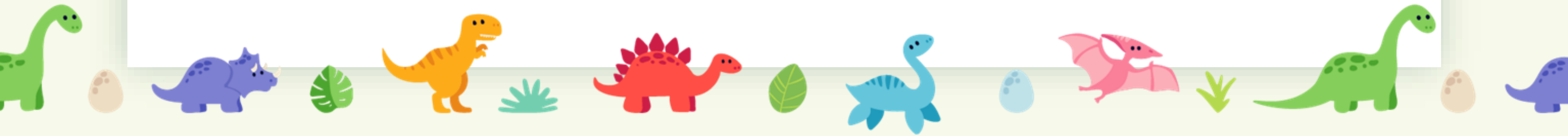
Identified Overly-Permissive Allowed Signers



signature:495847a93187cfb8c71f840cb7b41497ad95c64f tag:signed tag:peexe positives:40+

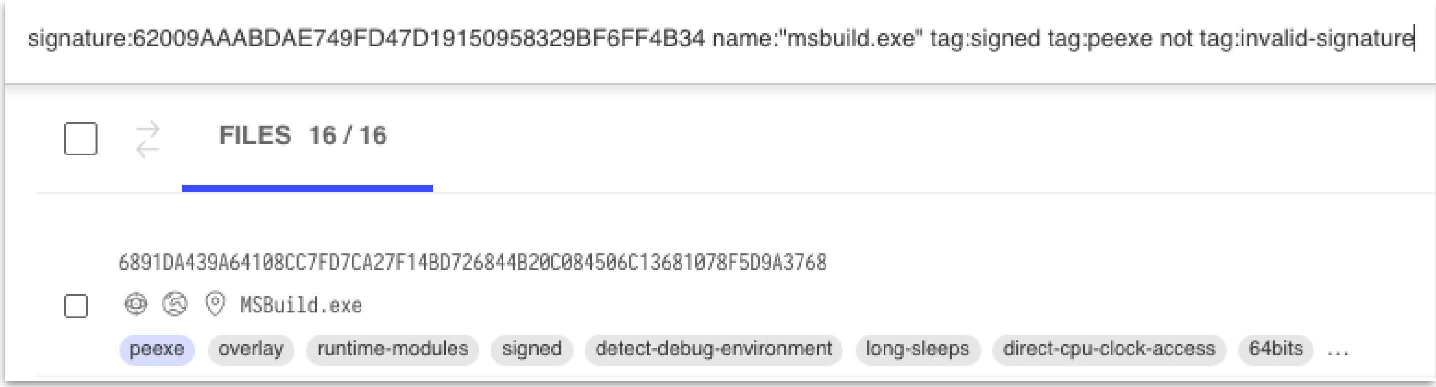
□ FILES 20 / 177.78 K

	Detections	Size
□ 17DD6A69137979A0E2D69E92ECC406FBCACF949DB0D445229978D74E1DC4145C *No meaningful names* peexe overlay runtime-modules signed checks-network-adapters long-sleeps direct-cpu-clock-access	51 / 69	228.78 KB
□ 10D4182D6C4557DD731DDEFFC4E82D300CB54BAA73DE146ADF99E38DEADED23D mininewshn.exe peexe spreader signed overlay	47 / 69	1.54 MB



Weaponization

Identifying a Candidate Abusable Executable



```
signature:62009AAABDAE749FD47D19150958329BF6FF4B34 name:"msbuild.exe" tag:signed tag:peexe not tag:invalid-signature
```

□ FILES 16 / 16

6891DA439A64108CC7FD7CA27F14BD726844B20C084506C13681078F5D9A3768

□ MSBuild.exe

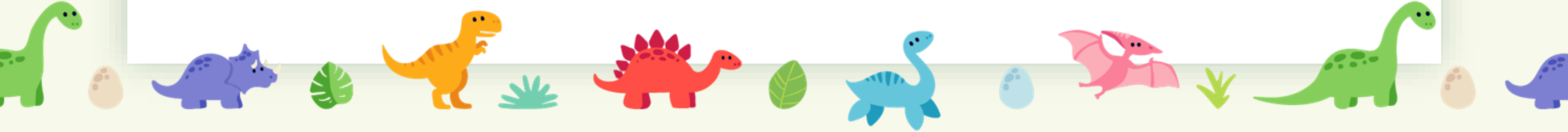
peexe · overlay · runtime-modules · signed · detect-debug-environment · long-sleeps · direct-cpu-clock-access · 64bits …

Weaponization Steps

- Register overly-permissive ELAM driver with InstallELAMCertificateInfo function in kernel32.dll.
- Create service for abusable executable (e.g. MSBuild)
- Specify service as SERVICE_LAUNCH_PROTECTED_ANTIMALWARE_LIGHT with ChangeServiceConfig2W
- Start service. Profit.

Weaponization Constraints

- Many “LOLBins” are likely not designed to run protected.
- PPL doesn’t permit spawning a child process by default.
- Must permit arbitrary unsigned code execution
- MSBuild payloads spawn a child process by default.
  - Property functions don’t spawn a child process!
  - Thank you, Casey Smith!



MSBuild Weaponization Constraints

MSBuild Property Function payload must be implemented as a one-liner using pseudo-.NET syntax

```
<Project ToolsVersion="4.0" xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
<Target Name="TestTarget">
<PropertyGroup>
<TestProperty>$([System.Activator]::CreateInstance($([System.Reflection.Assembly]::Load($([
System.Convert]::FromBase64String("REPLACEME"))).GetType("Test"))))</TestProperty>
</PropertyGroup>
</Target>
</Project>
```

Demo

Demo #1 – Running MSBuild Protected

https://youtu.be/-Pij0IoMWA4

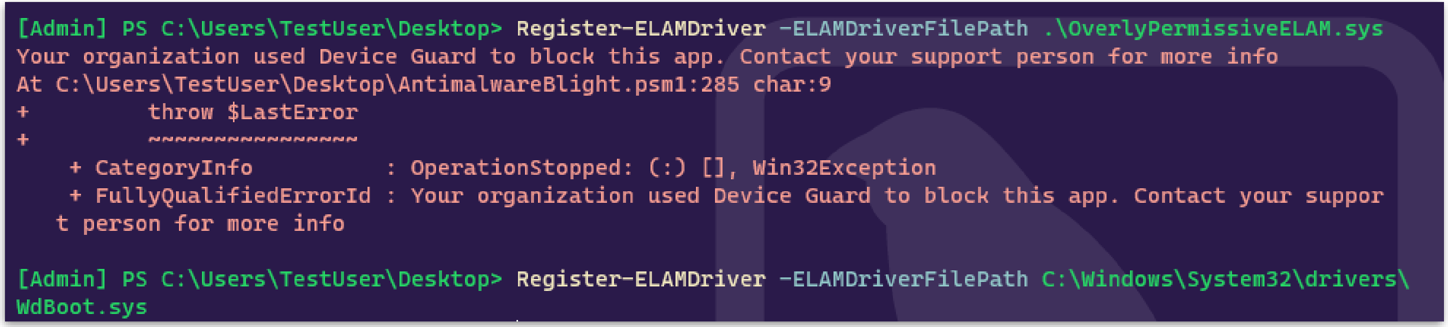
Demo #2 – Killing Defender AV Protected Process

https://youtu.be/i2aM7jGDZsw

Mitigations and Detection

Mitigations

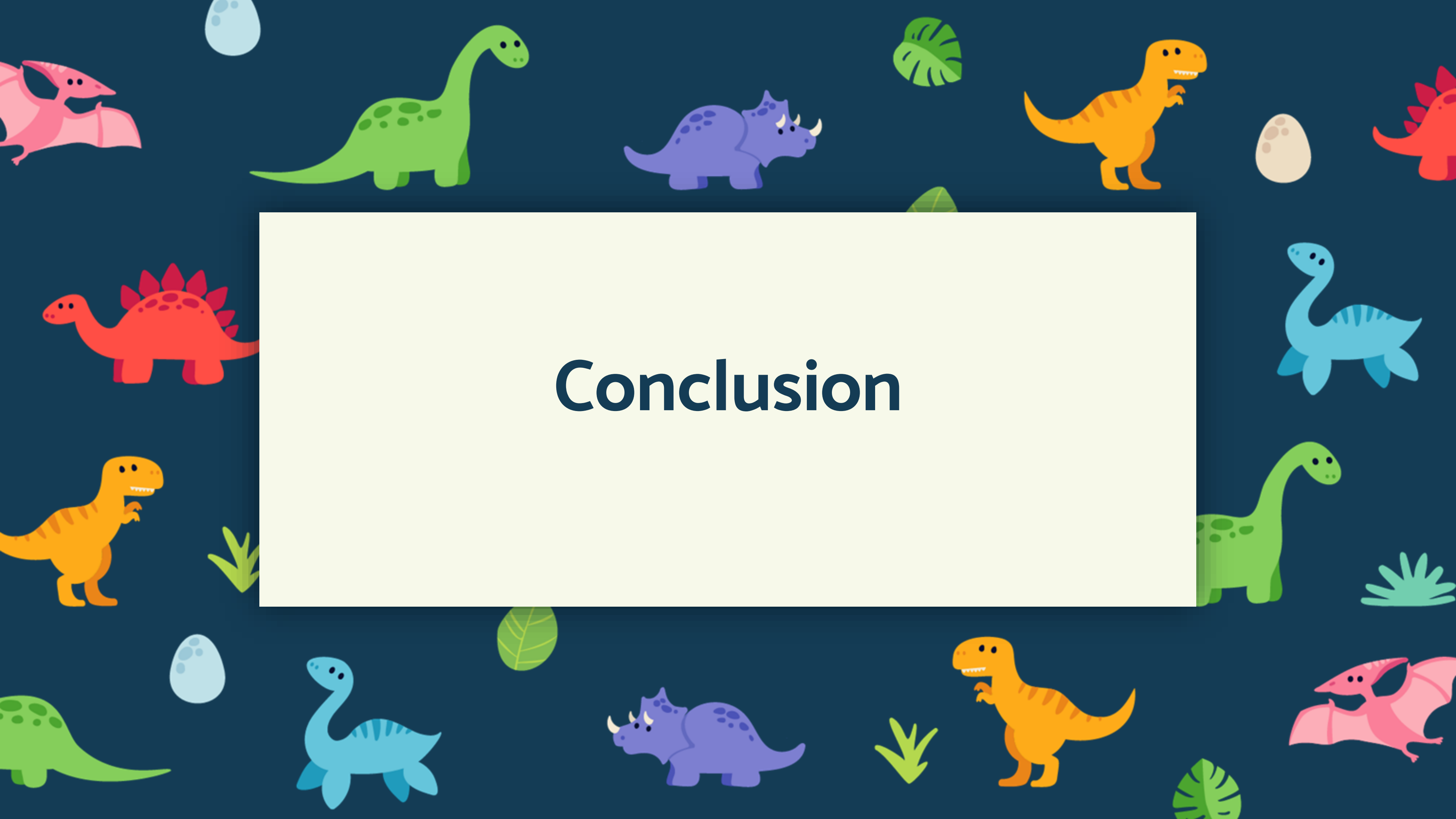
- A robust fix from Microsoft in the future?
- WDAC blocks loading/execution of disallowed ELAM drivers.



```
[Admin] PS C:\Users\TestUser\Desktop> Register-ELAMDriver -ELAMDriverFilePath .\OverlyPermissiveELAM.sys
Your organization used Device Guard to block this app. Contact your support person for more info
At C:\Users\TestUser\Desktop\AntimalwareBlight.psm1:285 char:9
+         throw $LastError
+         ~~~~~~~~~~~~~~~~
    + CategoryInfo          : OperationStopped: (:) [], Win32Exception
    + FullyQualifiedErrorId : Your organization used Device Guard to block this app. Contact your suppor
   t person for more info

[Admin] PS C:\Users\TestUser\Desktop> Register-ELAMDriver -ELAMDriverFilePath C:\Windows\System32\drivers\
WdBoot.sys
```

Detection and Recommendations

- Defenders: Focus on antimalware-light service creation.
    - `HKLM\SYSTEM\CurrentControlSet\Services\SERVICE – LaunchProtected – 3`
- Vendors: Use code-signing certificates with dedicated EKUs only for service executables and DLLs that are absolutely necessary.
    - Perform an audit of ELAM rules and corresponding allowed binaries.



Conclusion

Why is this so bad?

- One overly permissive ELAM driver poisons the well across the entire 3rd party antimalware ecosystem.
- The vetting process for ELAM drivers is far from robust.
- Malware running as PPL
  - can kill security products
  - is afforded anti-tampering protection

Disclosure Timeline

- Dec 28, 2021 - Reported to MSRC
- Jan 11, 2022
  - MSRC closed report. Reason: not a security boundary
  - Passed on report to Defender Research team
- January to Present
  - Defender mitigation developed/implemented for Microsoft-signers
  - Issue and mitigation communicated to MVI vendors and engagement with vendors regarding affected ELAM drivers.
  - Communicated by us that scope extends beyond Microsoft-signers, making mitigation unviable.
  - Plan to treat overly-permissive ELAM drivers on an individual basis - e.g. potential blocking in CI/ASR

Thank you, David Kaplan, Gil Besso, and Philip Tsukerman @ Microsoft!!!

Microsoft’s Official Response

“Microsoft researchers have been collaborating with Matt Graeber on the findings and with Microsoft Virus Initiative (MVI) partners to address the issue from their own ELAM drivers. Customers using both Microsoft Defender Antivirus and Microsoft Defender for Endpoint are covered by potential abuse of the ELAM functionality.”

Resources

More information

- Protecting anti-malware services
- ELAM Driver Requirements
- Unknown Known DLLs
- The Evolution of Protected Processes Parts 1, 2, and 3
- Building a WDAC Driver Allowlist

Code

- ELAM driver allow list parser - Get-ElamCertInfo
- TBS hash calculator - Get-TBSHash
- Defanged PPL Runner - AntimalwareBlight
  - Bring your own MSBuild and overly-permissive ELAM driver.

Thanks!

Questions?

@mattifestation