Absolutely Positively NOT ‘Hacking Back’ with Pcap

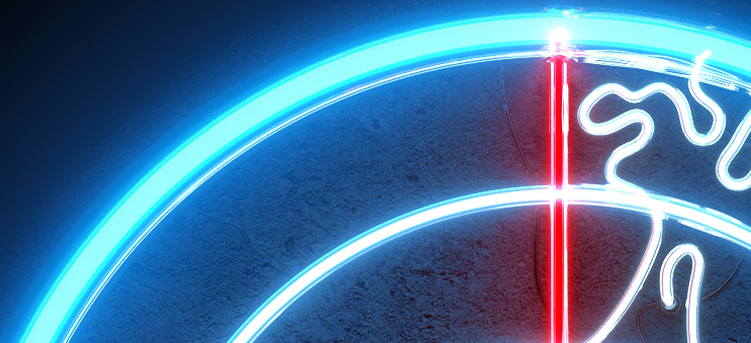
Streaming Unexpected Network Byte Sequences with High Probability of Blue Screening or Otherwise Crashing Attacker Command-and-Control Nodes

THE SAS CON

Steve Miller

Principal Applied Security Researcher

FIREEYE™



Absolutely Positively NOT Hacking Back with Pcap

Agenda

- Who am I and why I'm here
- Disclaimer
- C2 ecosystems and controllers
- Exploring C2 "robustness" with network traffic
- Defensive options for the ambitious

About me

FIREEYE™

ADVANCED PRACTICES

- **Worked @**: U.S. Army/NSA, Cornell U, DHS, U.S. State Dept.
- **Stuff I do:** incident response -> research -> discovery 
- **Things I like:** Pcap, Snort, Yara, Battlefield V, 1960s-80s sci-fi
- **Tweeps: @stvemillertime**

Tiny Wall of Thesis Points

Malware is software, but worse

- Just-good-enough code to work, kind of
- Buggy AF **(which I hope to illustrate)**
- Not built for robustness/availability under duress
- Controller programs are more fragile than the implant programs
- *Command-and-control ecosystems are extremely vulnerable, with little oversight*

Defenders can flex on weaknesses to put attackers at disadvantage

- You can play very, very rough to create chaos, confusion, stress on C2 infrastructure
- During a real attack/incident response, you have more power than you think…

Disclaimer on ‘Hacking Back’

- This is my personal research, and it is purely academic in nature
- FireEye does not hack back nor will it
- I do not endorse hacking back
- My research is intended to demonstrate the fragile nature of C2 ecosystems and advocate for defensive actions only

Img source: wsj.com

Malware “C2 Ecosystem”

2

CONTROLLER

“C2 server”
“C2 panel”
“manager”
On evil infra

controller.exe

3

“Hello from the other side”

“Heyo! What’s poppin?”

“I must’ve called a thousand times-”

“Yea sry my phone was on silent-”

“to tell you I’m sorry…”

“oh…are we really doing this now?”

C2 PROTOCOL

Implant beacons/hellos/heartbeats
Controller commands, instructions

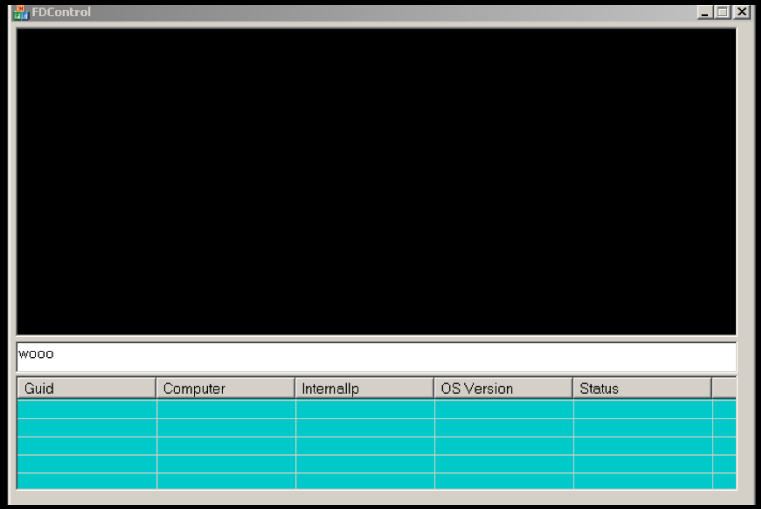
1

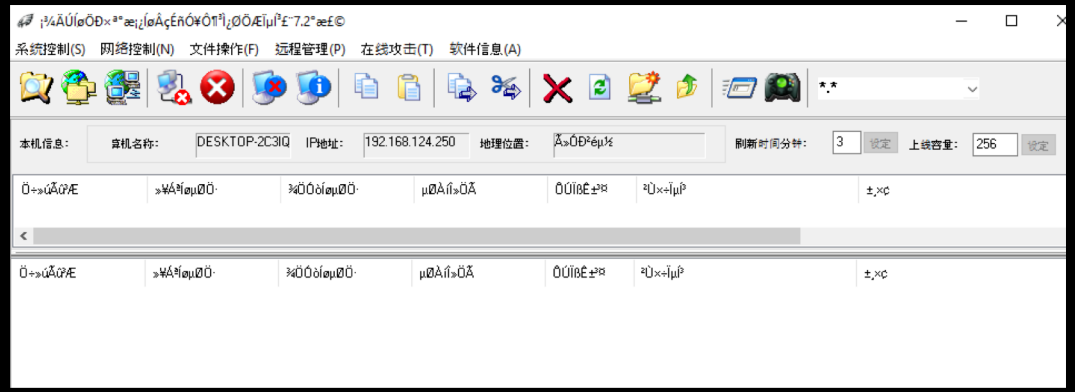
IMPLANT

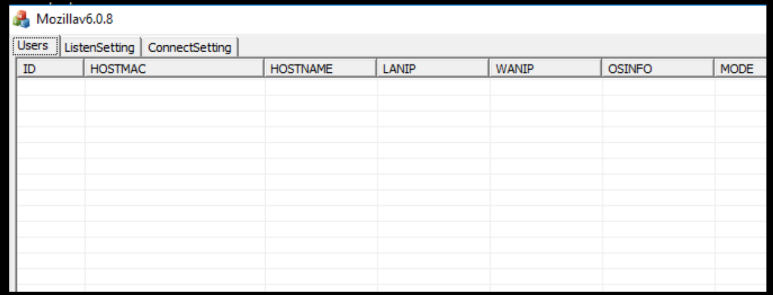
“backdoor”
“malware”
On victim infra

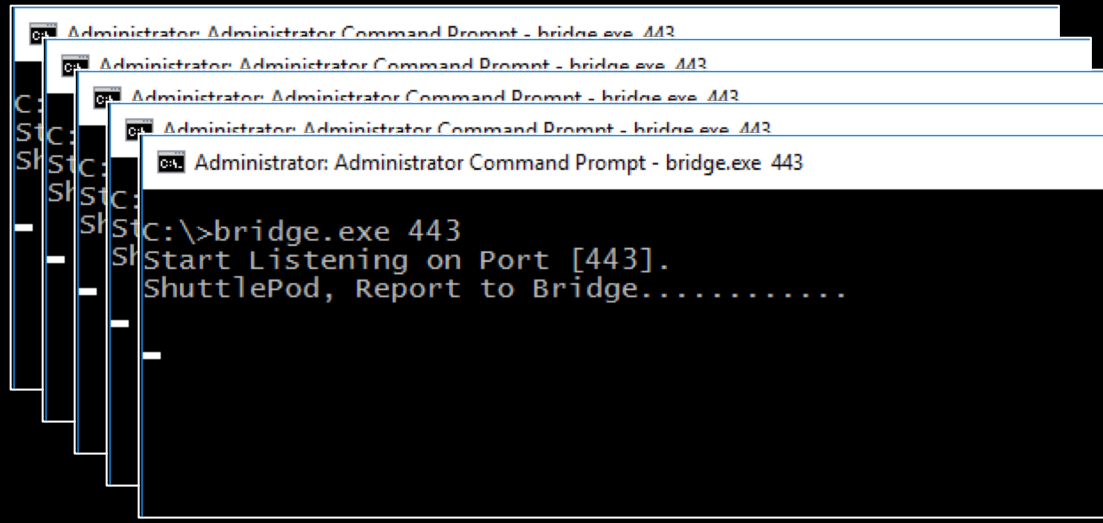
1234.exe

Controller Features



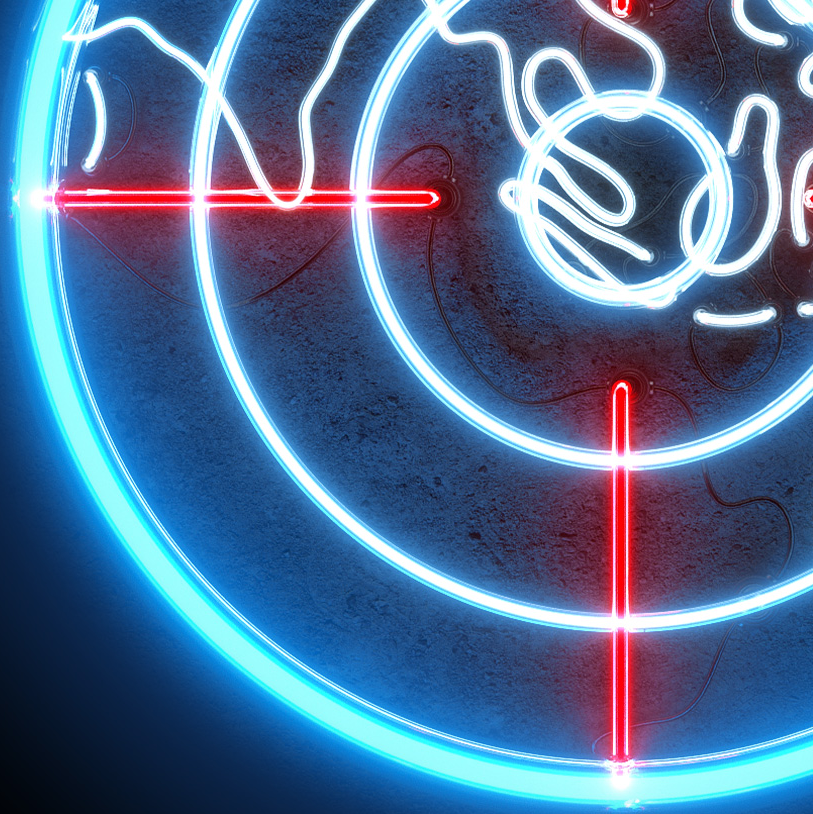






Exploring C2 Robustness

Using unexpected network bytes to defend your enterprise is easier than you may think

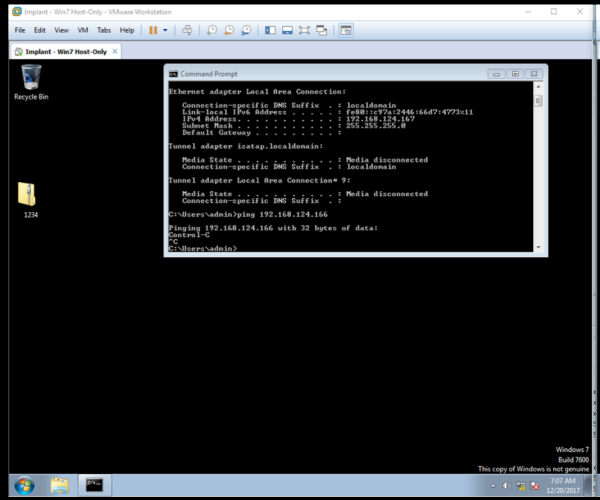


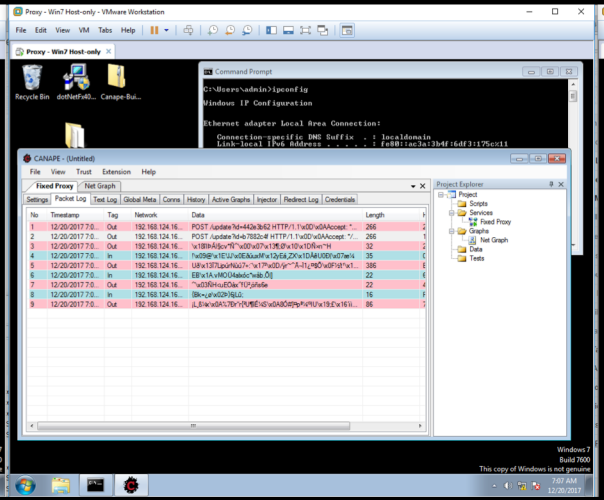
Exploring C2 Ecosystem “Robustness”

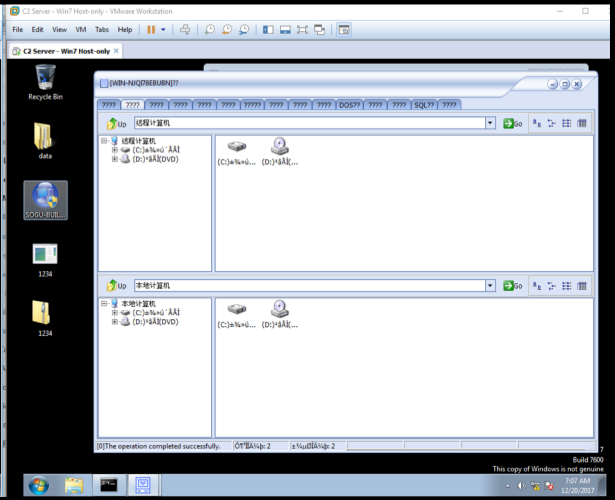
IMPLANT 

PROXY 

CONTROLLER







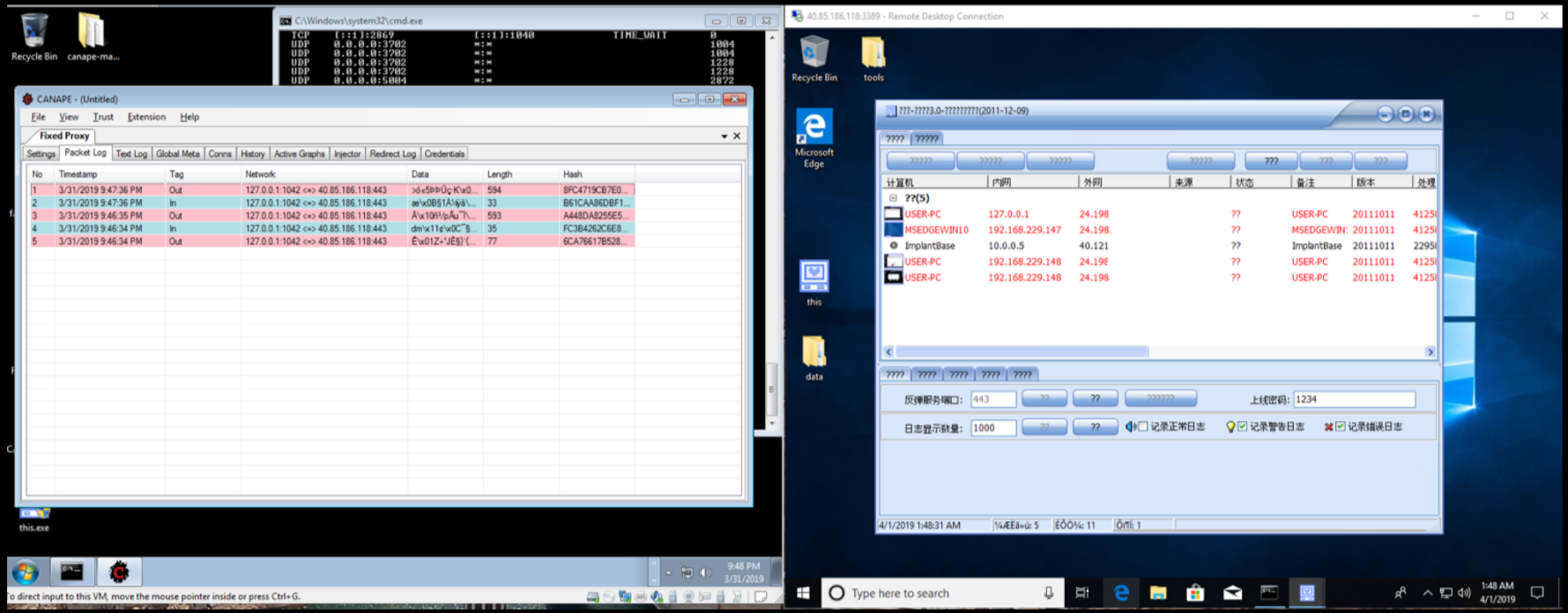
PlugX

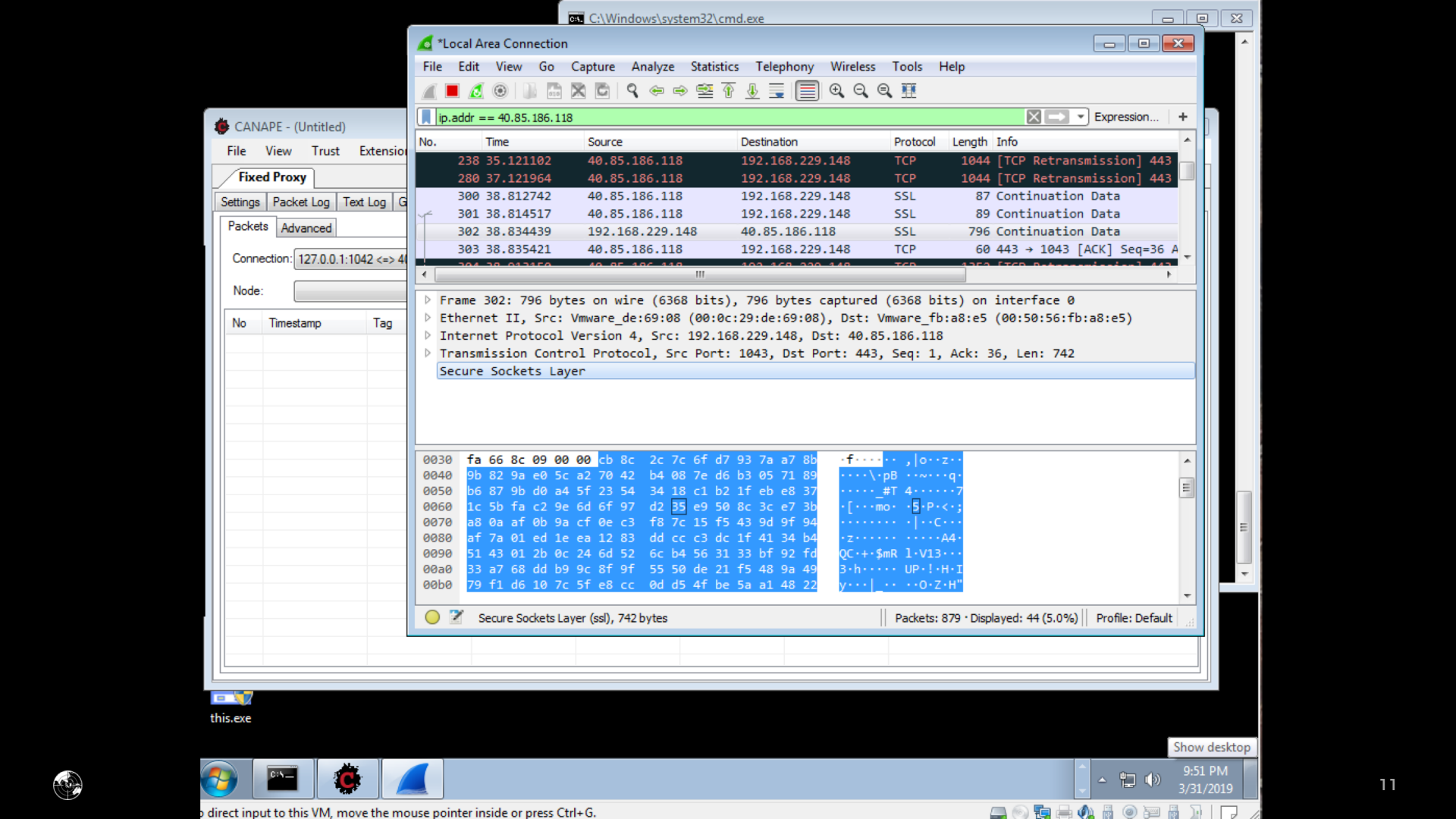
CANAPE

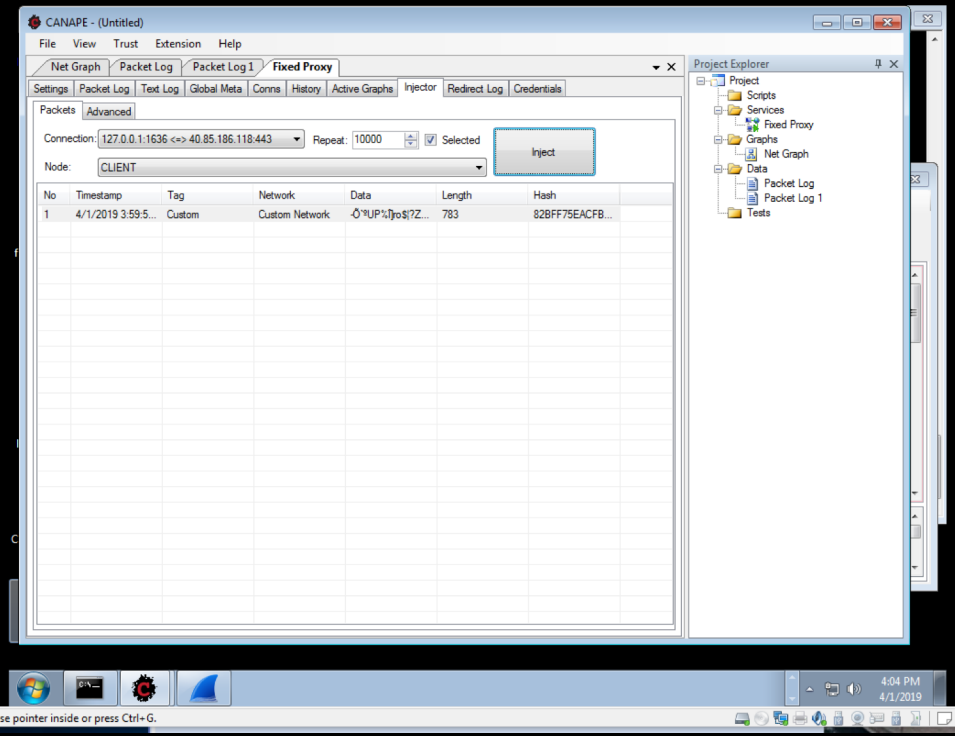
PlugX Controller
Type3 “SafeGui”

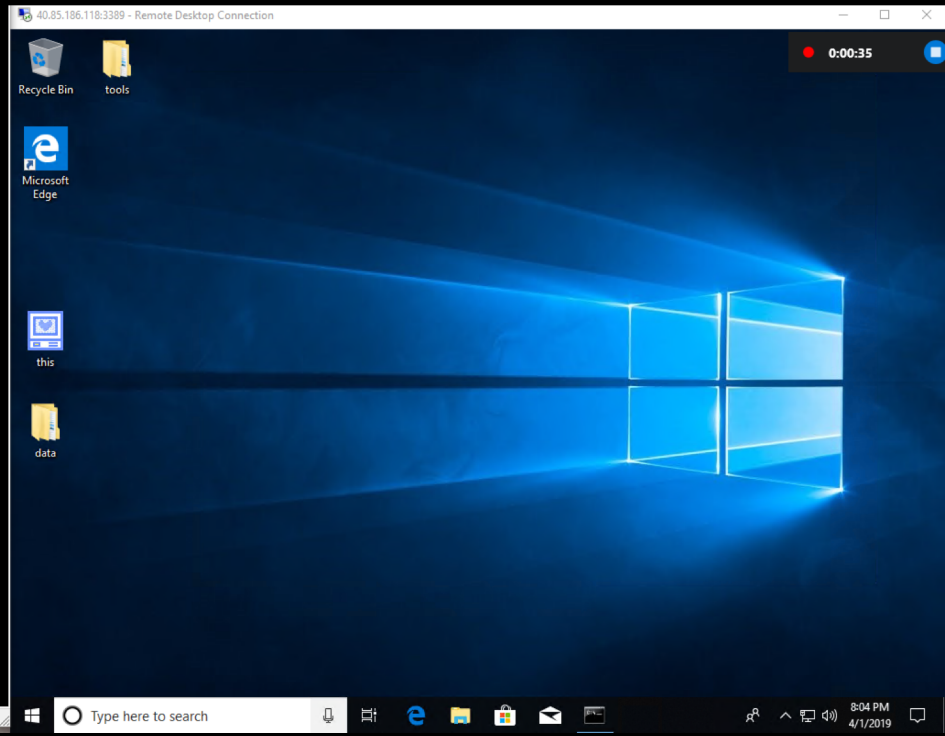
IMPLANT + PROXY

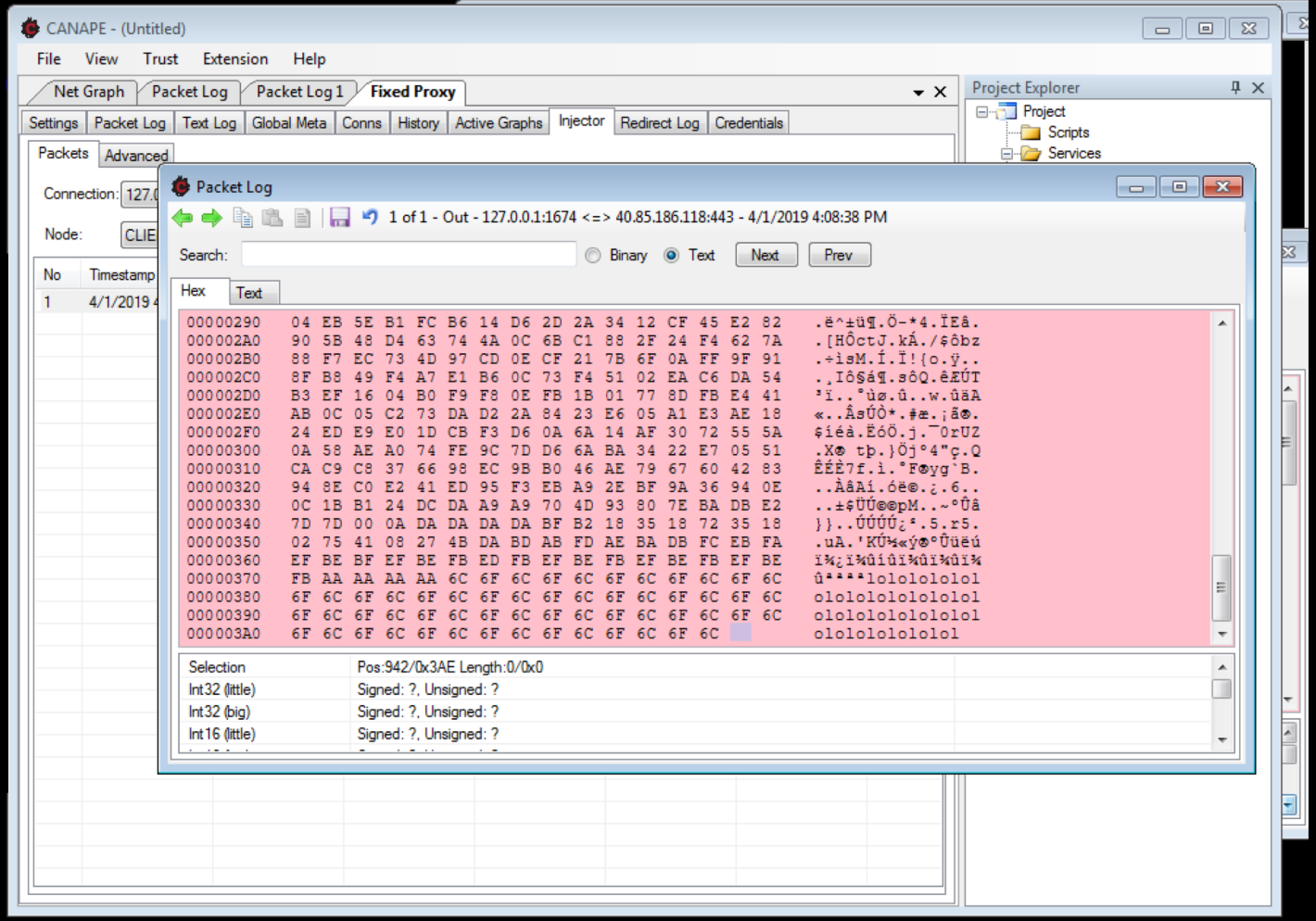
CONTROLLER

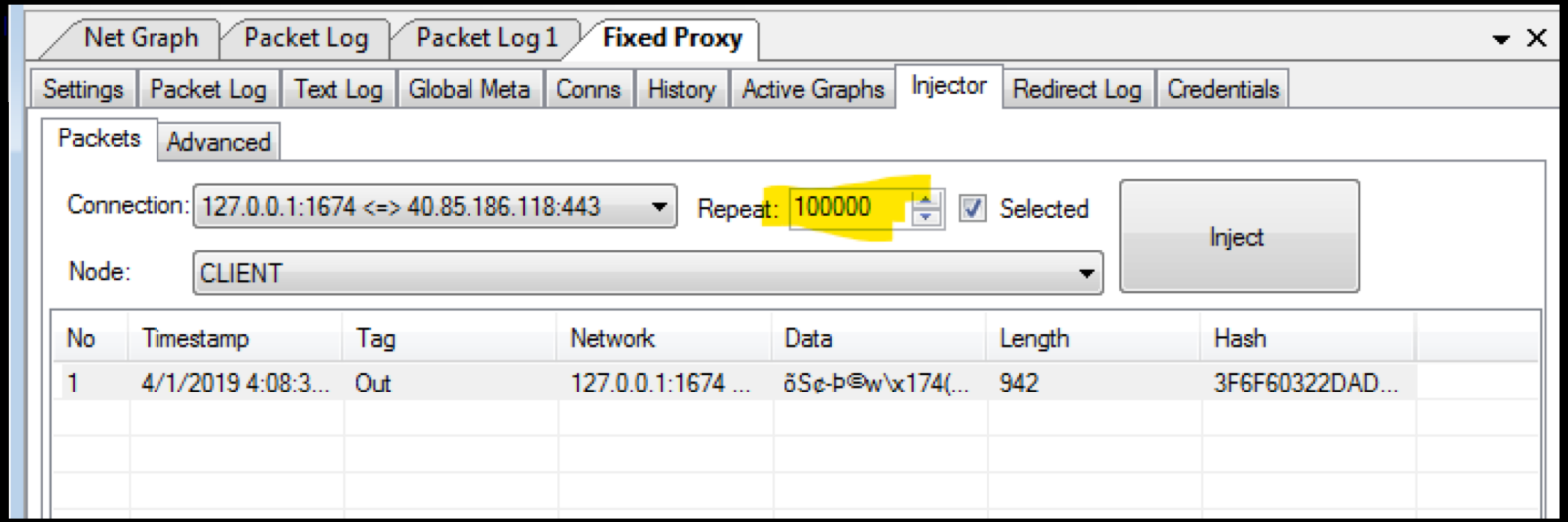


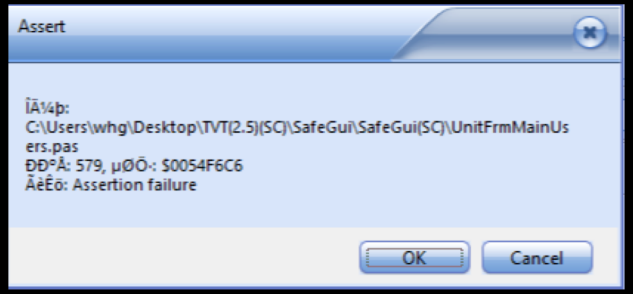

C:\Windows\system32\cmd.exe
*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 40.85.186.118
Expression...
No. Time Source Destination Protocol Length Info
238 35.121102 40.85.186.118 192.168.229.148 TCP 1044 [TCP Retransmission] 443
280 37.121964 40.85.186.118 192.168.229.148 TCP 1044 [TCP Retransmission] 443
300 38.812742 40.85.186.118 192.168.229.148 SSL 87 Continuation Data
301 38.814517 40.85.186.118 192.168.229.148 SSL 89 Continuation Data
302 38.834439 192.168.229.148 40.85.186.118 SSL 796 Continuation Data
303 38.835421 40.85.186.118 192.168.229.148 TCP 60 443 → 1043 [ACK] Seq=36 A
Frame 302: 796 bytes on wire (6368 bits), 796 bytes captured (6368 bits) on interface 0
Ethernet II, Src: Vmware_de:69:08 (00:0c:29:de:69:08), Dst: Vmware_fb:a8:e5 (00:50:56:fb:a8:e5)
Internet Protocol Version 4, Src: 192.168.229.148, Dst: 40.85.186.118
Transmission Control Protocol, Src Port: 1043, Dst Port: 443, Seq: 1, Ack: 36, Len: 742
Secure Sockets Layer
0030 fa 66 8c 09 00 00 cb 8c 2c 7c 6f d7 93 7a a7 8b
0040 9b 82 9a e0 5c a2 70 42 b4 08 7e d6 b3 05 71 89
0050 b6 87 9b d0 a4 5f 23 54 34 18 c1 b2 1f eb e8 37
0060 1c 5b fa c2 9e 6d 6f 97 d2 35 e9 50 8c 3c e7 3b
0070 a8 0a af 0b 9a cf 0e c3 f8 7c 15 f5 43 9d 9f 94
0080 af 7a 01 ed 1e ea 12 83 dd cc c3 dc 1f 41 34 b4
0090 51 43 01 2b 0c 24 6d 52 6c b4 56 31 33 bf 92 fd
00a0 33 a7 68 dd b9 9c 8f 9f 55 50 de 21 f5 48 9a 49
00b0 79 f1 d6 10 7c 5f e8 cc 0d d5 4f be 5a a1 48 22
Secure Sockets Layer (ssl), 742 bytes
Packets: 879 · Displayed: 44 (5.0%)
Profile: Default
CANAPE - (Untitled)
File View Trust Extensio
Fixed Proxy
Settings Packet Log Text Log G
Packets Advanced
Connection: 127.0.0.1:1042 <=> 4
Node:
No Timestamp Tag
this.exe
Show desktop
9:51 PM
3/31/2019
direct input to this VM, move the mouse pointer inside or press Ctrl+G.

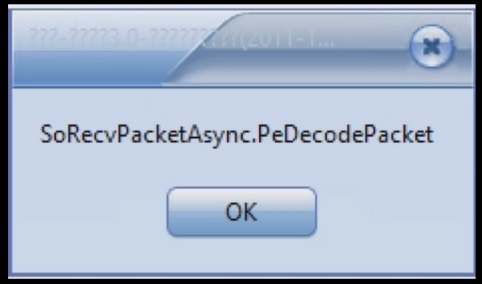

CANAPE - (Untitled)
File View Trust Extension Help
Net Graph Packet Log Packet Log 1 Fixed Proxy
Settings Packet Log Text Log Global Meta Conns History Active Graphs Injector Redirect Log Credentials
Packets Advanced
Connection: 127.0.0.1:1636 <=> 40.85.186.118:443
Repeat: 10000
Selected
Inject
Node: CLIENT
No Timestamp Tag Network Data Length Hash
1 4/1/2019 3:59:5... Custom Custom Network 783 82BFF75EACFB...
Project Explorer
Project
Scripts
Services
Fixed Proxy
Graphs
Net Graph
Data
Packet Log
Packet Log 1
Tests
4:04 PM
4/1/2019
ouse pointer inside or press Ctrl+G.

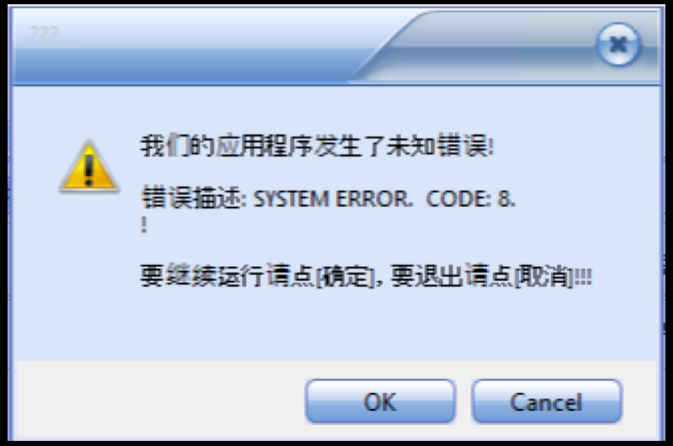

40.85.186.118:3389 - Remote Desktop Connection
0:00:35
Recycle Bin
tools
Microsoft Edge
this
data
Type here to search
8:04 PM
4/1/2019

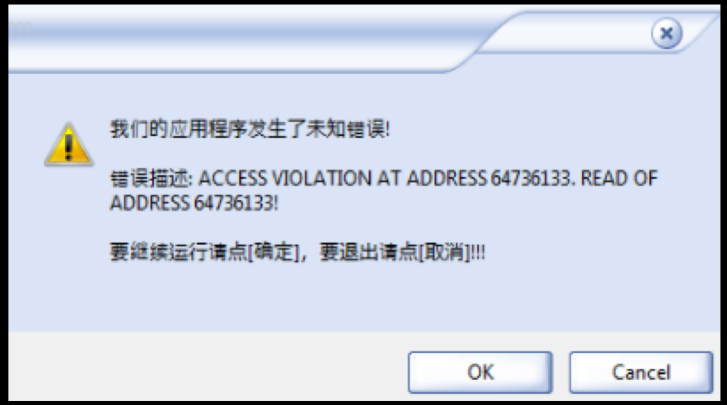

CANAPE - (Untitled)
File View Trust Extension Help
Net Graph Packet Log Packet Log 1 Fixed Proxy
Settings Packet Log Text Log Global Meta Conns History Active Graphs Injector Redirect Log Credentials
Packets Advanced
Connection: 127.0
Node: CLIE
No Timestamp
1 4/1/2019 4
Project Explorer
Project
Scripts
Services
Packet Log
1 of 1 - Out - 127.0.0.1:1674 <=> 40.85.186.118:443 - 4/1/2019 4:08:38 PM
Search:
Binary Text Next Prev
Hex Text
00000290 04 EB 5E B1 FC B6 14 D6 2D 2A 34 12 CF 45 E2 82 .ë^±ü¶.Ö-*4.ÏEâ.
000002A0 90 5B 48 D4 63 74 4A 0C 6B C1 88 2F 24 F4 62 7A .[HÔctJ.kÁ./$ôbz
000002B0 88 F7 EC 73 4D 97 CD 0E CF 21 7B 6F 0A FF 9F 91 .÷ìsM.Í.Ï!{o.ÿ..
000002C0 8F B8 49 F4 A7 E1 B6 0C 73 F4 51 02 EA C6 DA 54 .¸Iô§á¶.sôQ.êÆÚT
000002D0 B3 EF 16 04 B0 F9 F8 0E FB 1B 01 77 8D FB E4 41 ³ï..°ùø.û..w.ûäA
000002E0 AB 0C 05 C2 73 DA D2 2A 84 23 E6 05 A1 E3 AE 18 «..ÂsÚÒ*.#æ.¡ã®.
000002F0 24 ED E9 E0 1D CB F3 D6 0A 6A 14 AF 30 72 55 5A $íéà.ËóÖ.j.¯0rUZ
00000300 0A 58 AE A0 74 FE 9C 7D D6 6A BA 34 22 E7 05 51 .X® tþ.}Öjº4"ç.Q
00000310 CA C9 C8 37 66 98 EC 9B B0 46 AE 79 67 60 42 83 ÊÉÈ7f.ì.°F®yg`B.
00000320 94 8E C0 E2 41 ED 95 F3 EB A9 2E BF 9A 36 94 0E ..ÀâAí.óë©.¿.6..
00000330 0C 1B B1 24 DC DA A9 A9 70 4D 93 80 7E BA DB E2 ..±$ÜÚ©©pM..~ºÛâ
00000340 7D 7D 00 0A DA DA DA DA BF B2 18 35 18 72 35 18 }}..ÚÚÚÚ¿².5.r5.
00000350 02 75 41 08 27 4B DA BD AB FD AE BA DB FC EB FA .uA.'KÚ½«ý®ºÛüëú
00000360 EF BE BF EF BE FB ED FB EF BE FB EF BE FB EF BE ï¾¿ï¾ûíûï¾ûï¾ûï¾
00000370 FB AA AA AA AA 6C 6F 6C 6F 6C 6F 6C 6F 6C 6F 6C ûªªªªlololololol
00000380 6F 6C 6F 6C 6F 6C 6F 6C 6F 6C 6F 6C 6F 6C 6F 6C olololololololol
00000390 6F 6C 6F 6C 6F 6C 6F 6C 6F 6C 6F 6C 6F 6C 6F 6C olololololololol
000003A0 6F 6C 6F 6C 6F 6C 6F 6C 6F 6C 6F 6C 6F 6C olololololol
Selection Pos:942/0x3AE Length:0/0x0
Int32 (little) Signed: ?, Unsigned: ?
Int32 (big) Signed: ?, Unsigned: ?
Int16 (little) Signed: ?, Unsigned: ?

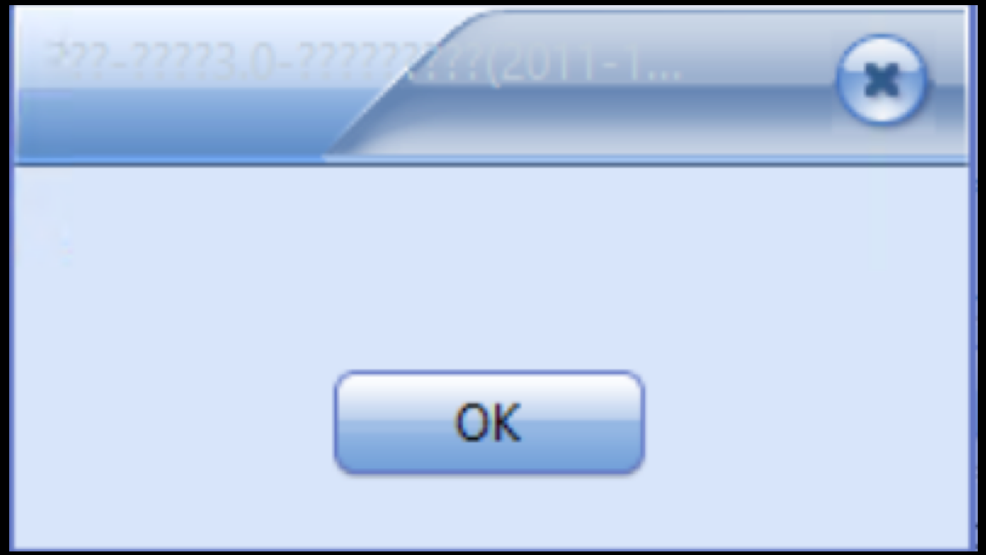

Net Graph
Packet Log
Packet Log 1
Fixed Proxy
Settings
Packet Log
Text Log
Global Meta
Conns
History
Active Graphs
Injector
Redirect Log
Credentials
Packets
Advanced
Connection: 127.0.0.1:1674 <=> 40.85.186.118:443
Repeat: 100000
Selected
Inject
Node: CLIENT
No
Timestamp
Tag
Network
Data
Length
Hash
1
4/1/2019 4:08:3...
Out
127.0.0.1:1674 ...
õSȼ-Þ©w\x174(...
942
3F6F60322DAD...

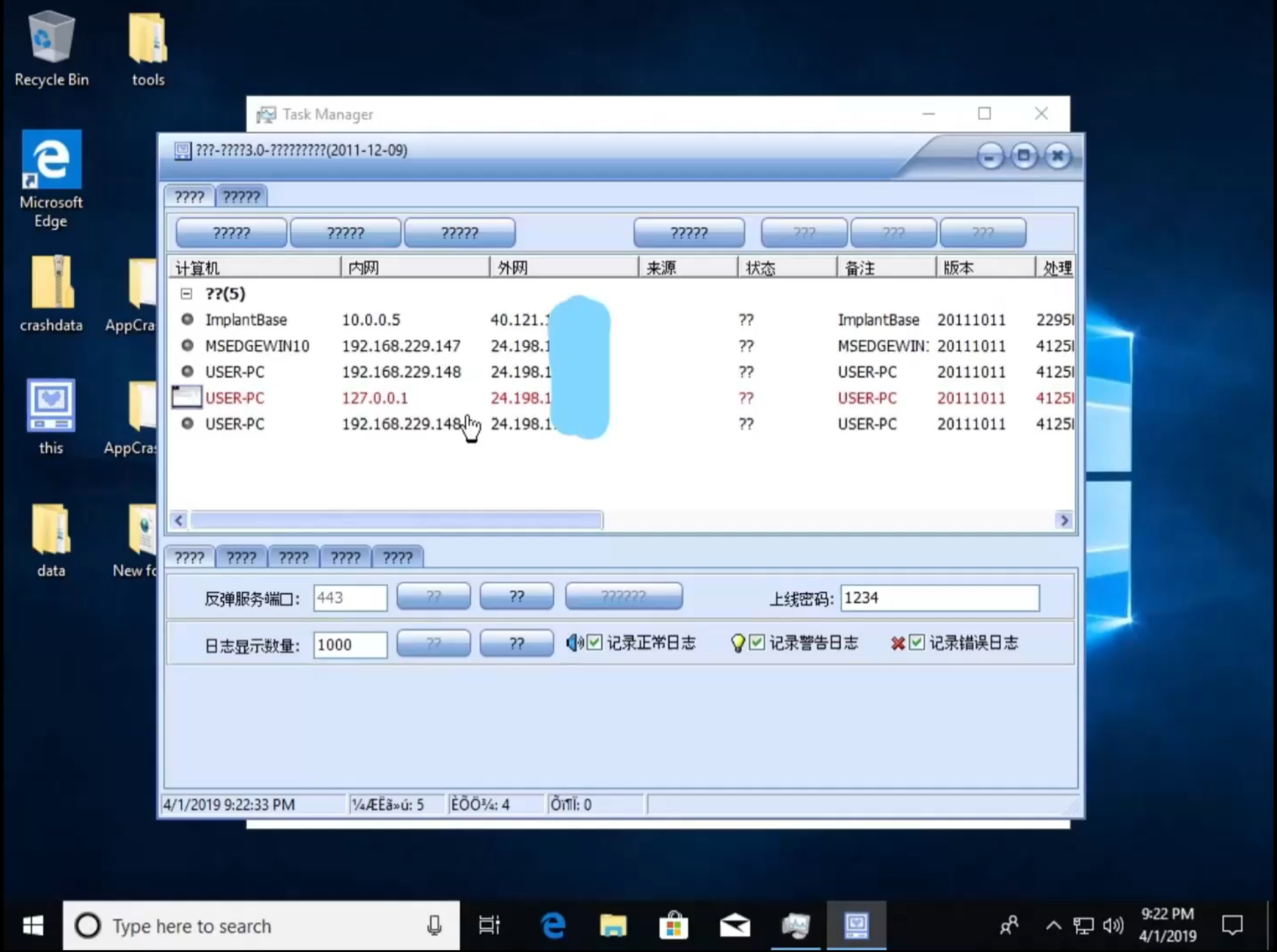

Assert
ÌÃ¼þ:
C:\Users\whg\Desktop\TVT(2.5)(SC)\SafeGui\SafeGui(SC)\UnitFrmMainUsers.pas
ÐÐ°Å: 579, µØÕ·: $0054F6C6
ÃèÊö: Assertion failure
OK
Cancel


SoRecvPacketAsync.PeDecodePacket
OK

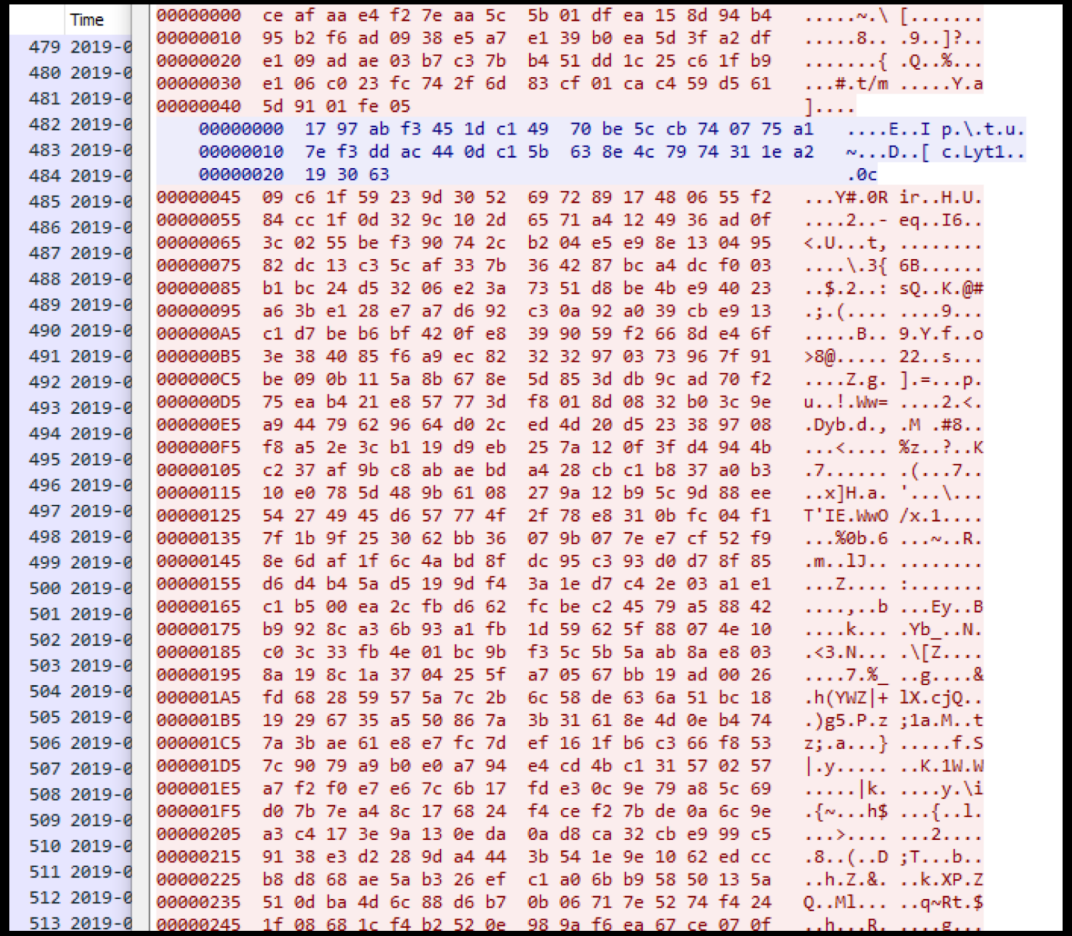

我们的应用程序发生了未知错误!
错误描述: SYSTEM ERROR. CODE: 8.
!
要继续运行请点[确定], 要退出请点[取消]!!!
OK
Cancel

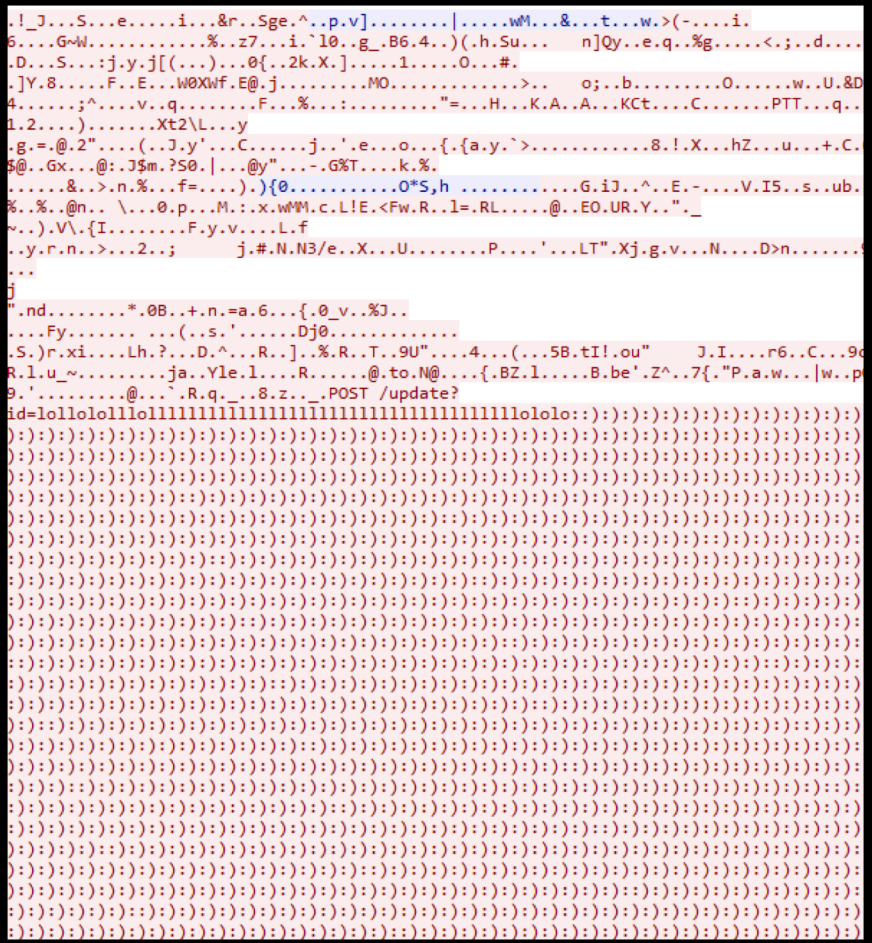

我们的应用程序发生了未知错误!
错误描述: ACCESS VIOLATION AT ADDRESS 64736133. READ OF ADDRESS 64736133!
要继续运行请点[确定], 要退出请点[取消]!!!
OK
Cancel


OK


Recycle Bin
tools
Microsoft Edge
crashdata
AppCra
this
AppCras
data
New fo
Task Manager
???-????3.0-?????????(2011-12-09)
???? ?????
????? ????? ????? ????? ??? ??? ???
计算机 内网 外网 来源 状态 备注 版本 处理
??(5)
ImplantBase 10.0.0.5 40.121.1 ?? ImplantBase 20111011 2295
MSEDGEWIN10 192.168.229.147 24.198.1 ?? MSEDGEWIN: 20111011 4125
USER-PC 192.168.229.148 24.198.1 ?? USER-PC 20111011 4125
USER-PC 127.0.0.1 24.198.1 ?? USER-PC 20111011 4125
USER-PC 192.168.229.148 24.198.1 ?? USER-PC 20111011 4125
???? ???? ???? ???? ????
反弹服务端口: 443 ?? ?? ??????
上线密码: 1234
日志显示数量: 1000 ?? ??
记录正常日志
记录警告日志
记录错误日志
4/1/2019 9:22:33 PM
¼ÆËã»ú: 5
ÈÕÖ¾: 4
ÕïÎ: 0
Type here to search
9:22 PM
4/1/2019

1. Start Wireshark
2. Run implant
3. Notice handshake routines
4. Replay handshake routine w/ some “amendments”
5. Go to 1





Experiment Results

Crashes	15
BSOD	1
Silent Failure	2

C2 Ecosystem Weakness Matrix

Pre-Hello

- Little presence
- Minimal weakness

Hello

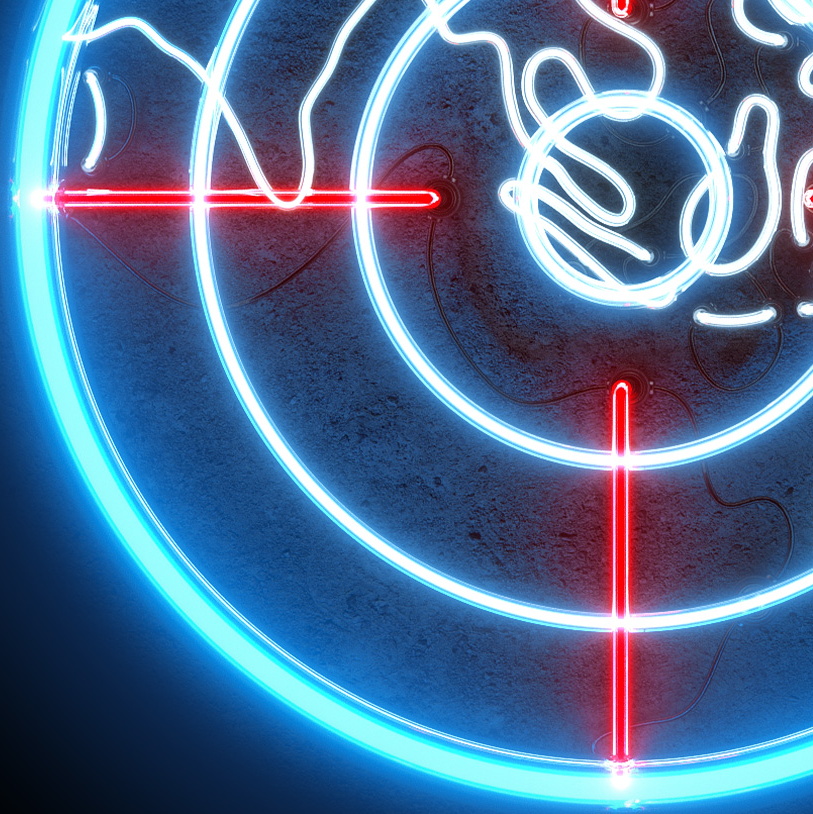
- “Hi”
- “Hello its me” implant auth
- Maximum validation
- Medium weakness

Post-Hello

- Minimal validation
- Maximum weakness
- Easy to break

Defensive options for the ambitious

Defensive use of proxies and unexpected network bytes



Scenario – You've Been Pwned, Time For IR

Implant monitored and left in place	→	Protect OPSEC, adopt other risks
Implant C2 address is sunk	→	Sacrifice some OPSEC, reduce risk of immediate and direct impact
Implant C2 altogether blocked, burned to the public	→	Sacrifice all OPSEC, get a little agro

What else can you do?

What Is An Implant?

It's an invitation to a party!

+ Address to the party
+ Secret password to get in
+ Added to the guest list

Proxy Operated Network Defense (POND)

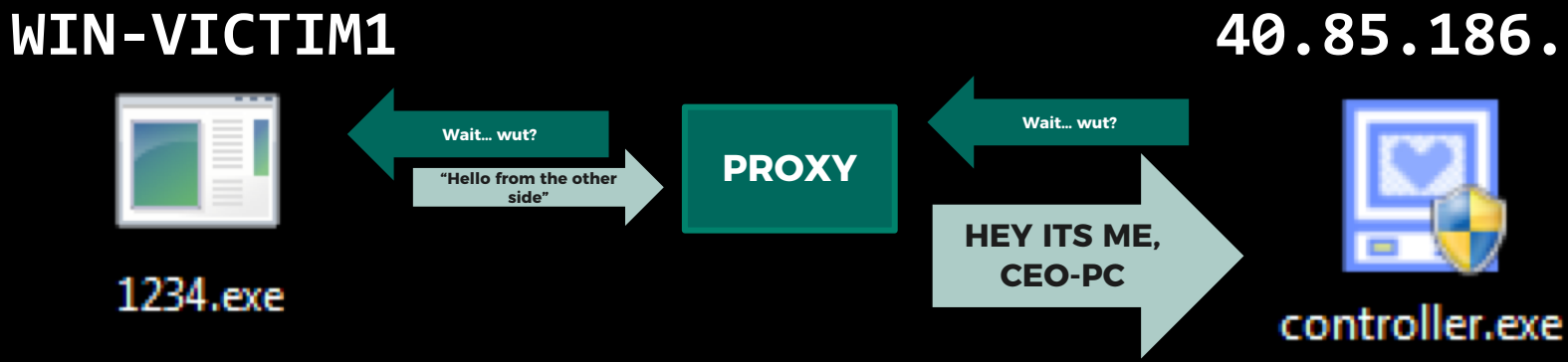
“PROXY”

- Proxy traffic to internet
- Detect C2 protocols
- Contain configurable IFTTT routines
- Could be a VM, server, or *built into security product (attn: vendors)*

- IF (tcp.stream == Backdoor.PlugX.TCP.Type3)
  - THEN
    - Allow outbound bytes { 36-48 }
  - THEN
    - Allow inbound bytes { 36-48 }
  - THEN
    - Allow outbound bytes { 200-900 }
    - Overwrite offset 35:68 with { 0x0A 0xF2 0x16 0xDA 0x1C }

Enhanced IR Strategy - Meaconing

protect opsec, deceive, confuse
show up to the party in costume



Intercept and rebroadcast
esp. w/ falsified data

Enhanced IR Strategy - Interference

protect opsec, frustrate, hinder
show up to the party reaaaall slowwwwwwww

WIN-VICTIM1

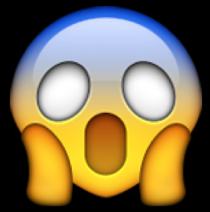
40.85.186.118

1234.exe

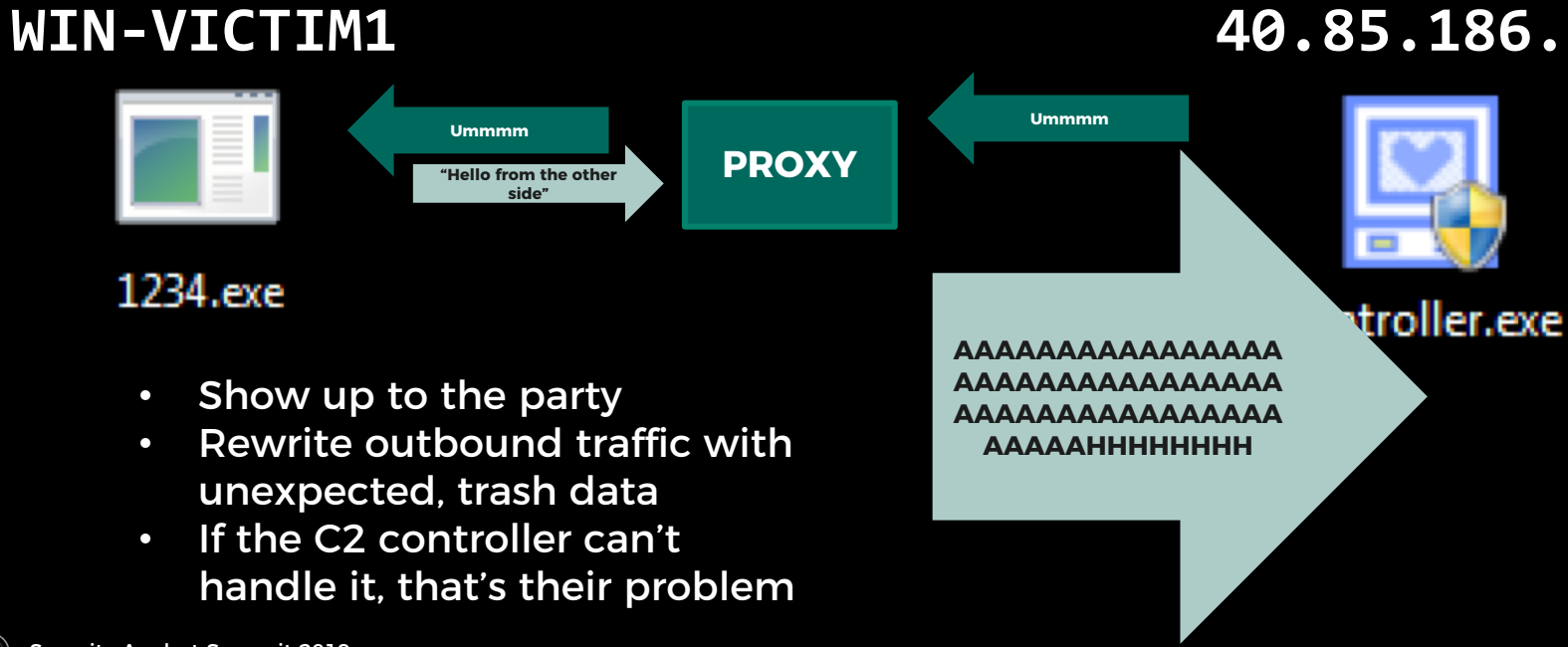
controller.exe

- Throttle inbound/outbound traffic to 10 bps
- Bit flipping to reduce likelihood of viable data theft
- Allow outbound heartbeats but deny inbound commands

Enhanced IR Strategy - Jamming



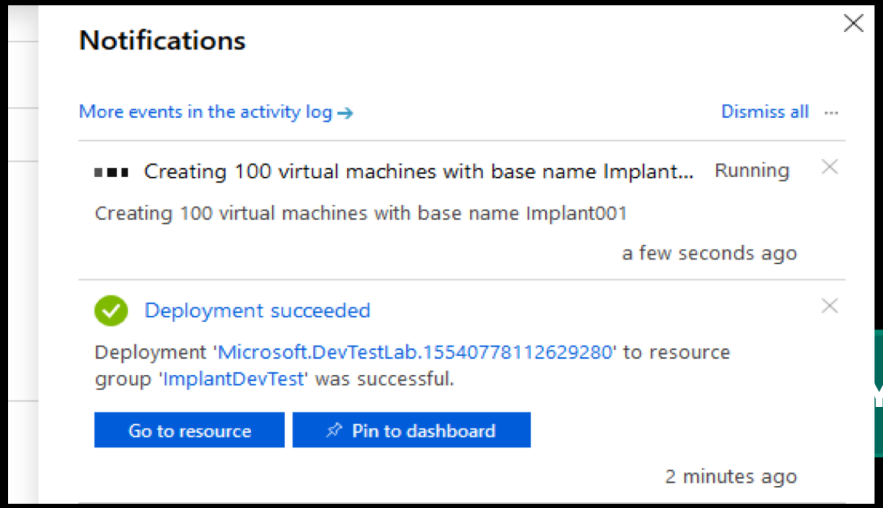
sacrifice some opsec, protect data, raise the noise floor at the party
...by yelling



- Show up to the party
- Rewrite outbound traffic with unexpected, trash data
- If the C2 controller can't handle it, that's their problem

Enhanced IR Strategy - Intrusion

what opsec? I'm just bringing a lotttttt of unexpected guests to the party.

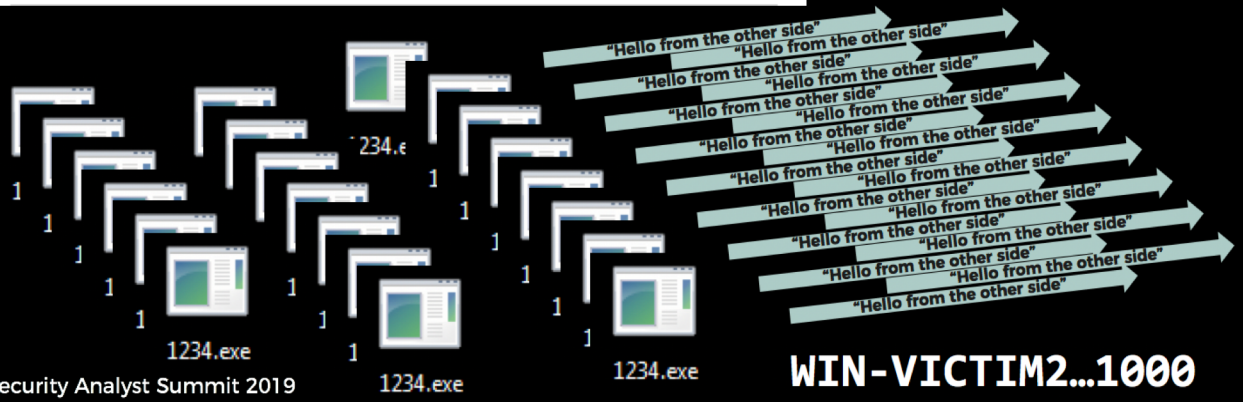


40.85.186.118

"Hey what's poppin"

"Hello from the other side"

controller.exe



WIN-VICTIM2…1000

Takeaways

- C2 ecosystems are fragile
- Your implant is your invitation
- You own your network traffic
- You have response actions with varying risk/reward options
- You *can* *marginalize* the operations of a live C2 node without ‘hacking back’
- Think MIJI ☺

#TheSAS2019

Wanna collaborate and definitely NOT hack back?

Steve Miller

@stvemillertime