

# Mason Competitive Cyber

## Antiforensics - Covering Your Tracks



# Upcoming Competitions & Events



- PatriotCTF
  - Saturday
  - HUB rooms 1-5
  - [patriotctf.gmu.io](http://patriotctf.gmu.io)
- Shmocon First Round of Tickets
  - Noon today (already sold out RIP)
  - DC in January
  - Schmooze a Student
- RUCTFE
  - Nov 10
  - Online Attack/Defense

# Antiforensics



- Forensics
  - Logs
  - Forensic artifacts
  - Network Traffic/Logs
  - Malware Analysis
  - Timelining
- Antiforensics
  - Making that ^ more difficult

# Antiforensics on your own systems

- Why?
  - Privacy
  - Sketchy things
  - Sensitive dat

# Antiforensics on your own systems

- Encryption
  - Local
    - sticky keys hack
    - mac single user mode
  - Network Protocols
    - sniffing, MiTM
    - Tor/VPN
- Data Destruction
  - Digital
  - Magnetic
  - Physical
- Don't do things on main system
  - Raspberry Pi, server somewhere, compromised website
  - TAILS

# Rookie Moves

- Binary that runs on startup
- Getting caught by AV
- Using RDP without clearing event logs
  - teamviewer, VNCs, etc.
- Renaming and/or moving files to keep secret
  - File Carving
- Move to Trash
  - U fool
  - Easily recovered. MacOS even stores the filepath where it came from
- Move to Trash + empty trash
  - File marked to be overwritten. Until that happens recoverable
- Leaving command history on Linux
  - Use a different shell for max sneakiness

# Steganography



- Webshell in an image
- PHP in JPEG EXIF headers
  - exif\_read\_data

A screenshot of a web browser displaying a webshell interface. The address bar shows a URL from 'anadolu.edu.tr'. The interface has a dark background with a terminal-like display. On the left, there's a sidebar with a file size 'b374k' and version '2.8', and buttons for 'xpl', 'ps', 'eval', 'info', 'db', and 'rs'. The main area shows system information: 'Linux web\_birim1 2.6.32-431.29.2.el6.x86\_64 #1 SMP Tue Sep 9 13:45:55 CDT 2014 x86\_64', 'nginx/1.6.2', and server/client IP addresses. Below this is a directory listing table.

```
Linux web_birim1 2.6.32-431.29.2.el6.x86_64 #1 SMP Tue Sep 9 13:45:55 CDT 2014 x86_64
nginx/1.6.2
server ip : 212.175.41.71 | your ip : .0.10 | Time @ Server : 03 Jan 2017 23:26:27

o / var / www /

nginx > - shell command -
```

	name	size	perms	modified
<input type="checkbox"/>	[ . ]	LINK	drwxr-xr-x	08-Dec-2016 13:11:46
<input type="checkbox"/>	[ .. ]	LINK	drwxr-xr-x	13-Nov-2012 15:54:42
<input type="checkbox"/>	[ ab2015 ]	DIR	drwxr-xr-x	22-Aug-2014 15:01:20
<input type="checkbox"/>	[ abc ]	DIR	drwx-----	25-Jan-2014 17:14:23

# Fileless Malware



- Runs in memory
  - Doesn't exist when shut down
    - Can set to run on startup
  - Evade AV signatures
  - PS Empire, WMI
- Capturing RAM
  - Volatility





# Forensic Artifact Fuckery



- Timestomping
  - NTFS
    - Created, Accessed, Modified, Metadata Changed
    - \$STDINFO and \$FILENAME
  - Disabling Last Accessed
    - HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate
- Deleting them
  - Files
    - Thumbnail cache, Bitmap cache, PSReadline
  - Registry, NTFS Reserved Folders (\$Extend)
- Generate random activity
  - Some artifacts roll data

# Destruction



- Encryption
- Wiping
  - overwrite files
  - overwrite Master Boot Record (MBR)
- Wipe patient 0
  - Initial method of compromise
  - Data exfiltration

# Obfuscation



- Make code harder to read
  - Variable/function names
  - String manipulation
- Rookie Move: passing everything to one big IEX/eval/whatever
  - Eval + gzip + Base64 = PHP noob tier
- Invoke-Obfuscation
- Msfvenom
- Veil Framework
- Behavioral analysis

# Practical Exercises



- New TCTF Challenges
  - Obfuscation Sensation (php)
  - Unzip
  - [tctf.competitivecyber.club](https://tctf.competitivecyber.club)

# Proud Sponsors



Thank you to these organizations who give us their support:

***BATTELLE***

**It can be done™**

**CRYPSIS™**