Operationalized Purple Teaming

THE HITCH HACKERS GUIDE TO CYBER SECURITY
Don't Panic
CACTUSCON 2021

CactusCon 9

Partners

BISHOPFOX PayPal

BlackBerry

Early Warning

Sponsors

AXON

Supporters

digital shadows_

New Genesis Solutions

In-Kind Sponsors

HACKTHEBOX

no starch press

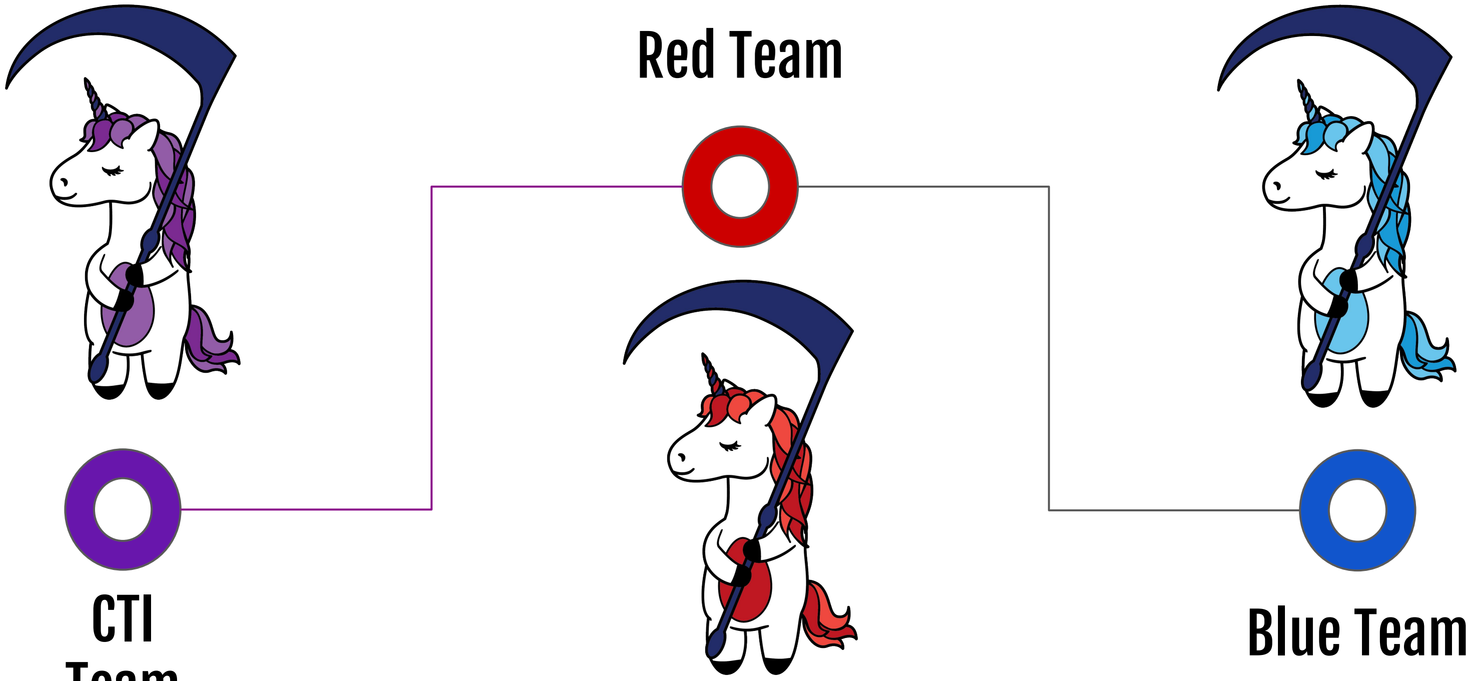
OFFENSIVE security SANS

The Full Purple Juice, Not the Watered-Down Stuff

Jorge Orchilles
@jorgeorchilles

Bryson Bort
@brysonbort

InfoSec Teams Today

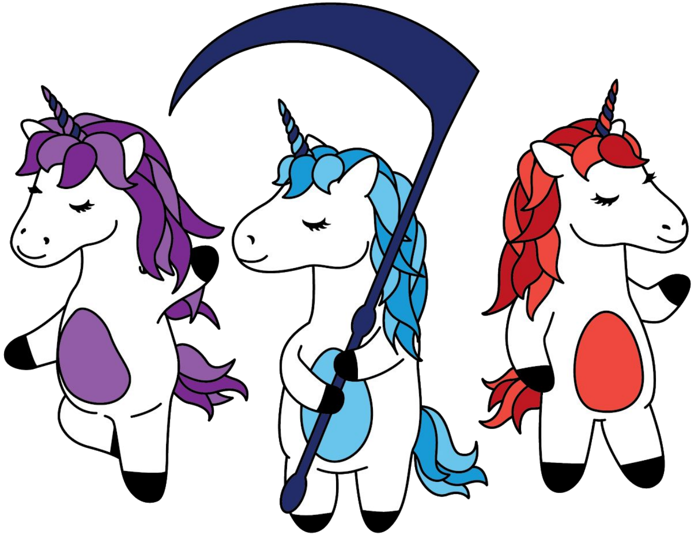


Red Team

CTI
Team

Blue Team

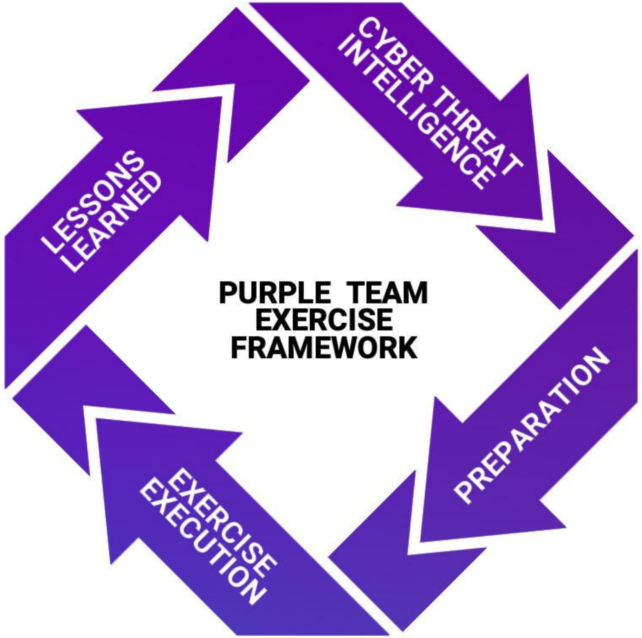
Bring them together by Purple Teaming



Intro to Purple Team

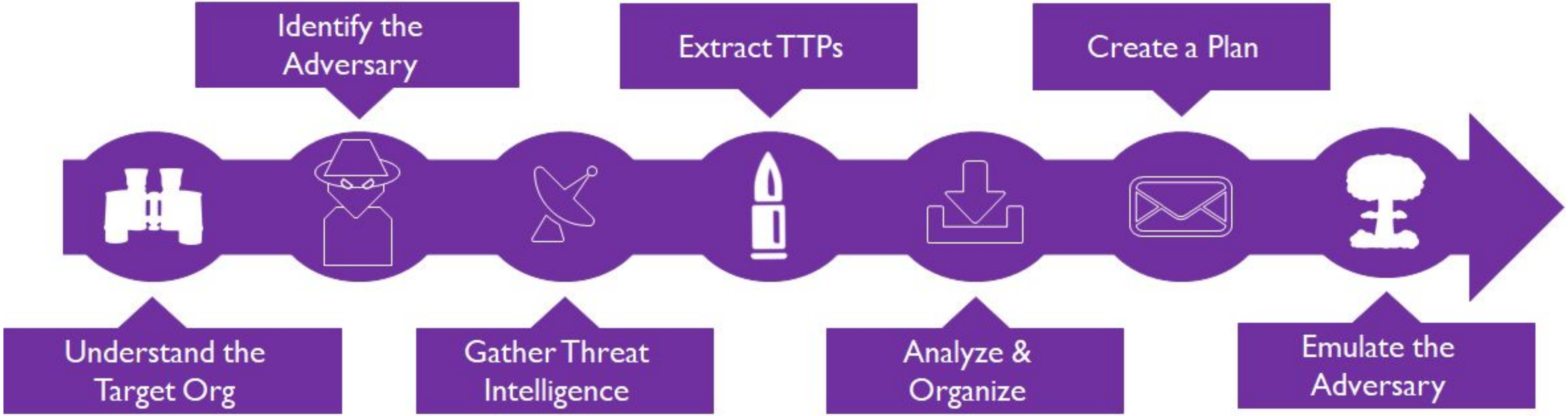
A Purple Team is a virtual team where the following teams work together

- Cyber Threat Intelligence - team to research and provide adversary TTPs
- Red Team - offensive team in charge of emulating adversaries
- Blue Team - the defenders. Security Operations Center (SOC), Hunt Team, Digital Forensics and Incident Response (DFIR), MSSPs.



https://github.com/scythe-io/purple-team-exercise-framework

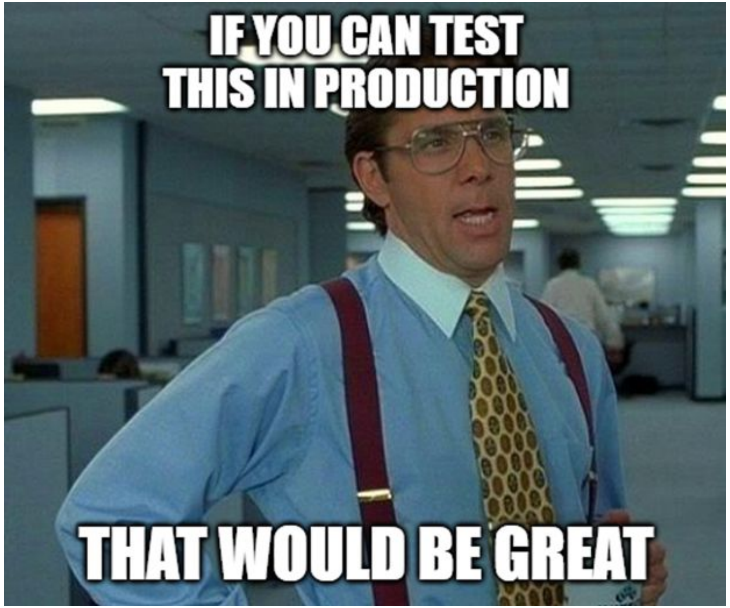
Cyber Threat Intelligence



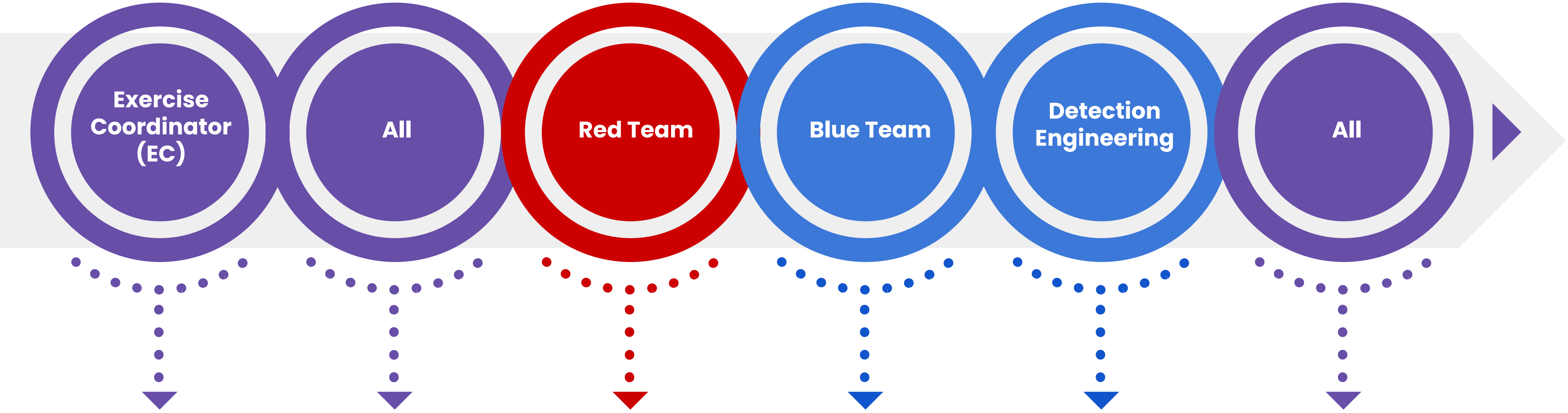
ATT&CKing the Status Quo: Threat-Based Adversary Emulation with MITRE ATT&CK - Katie Nickels and Cody Thomas

Preparation

- Pitch Purple Team Exercise to sponsors
  - Focus on value
- Preparation Meetings
- Target Systems
  - Security Tools
  - Target Accounts
- Attack Infrastructure
- Metrics
  - Data Sources
  - Detection
  - Response
  - Time Metrics



Exercise Execution



Exercise Coordinator (EC)

Present adversary, TTPs, and technical details

All

Table-top discussion of security controls and expectations for TTP execution

Red Team

Emulate the TTP while sharing the screen so everyone sees and learns what an attack looks like

Blue Team

Follow process to detect and respond to TTPs, share screen to confirm identification of artifacts

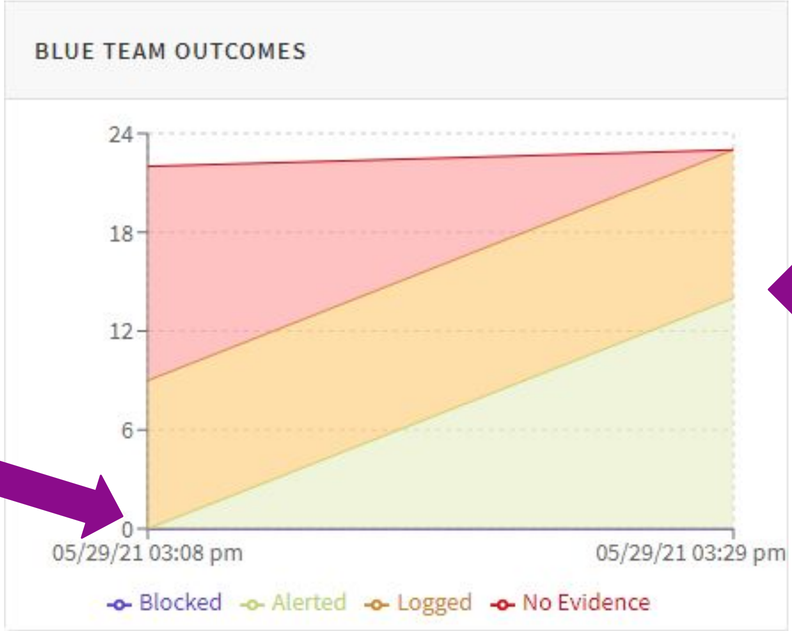
Detection Engineering

Can any adjustments or tuning to security controls and/or logging be made to increase visibility

All

Repeat procedure and record new results, move to next TTP

Focus on Value



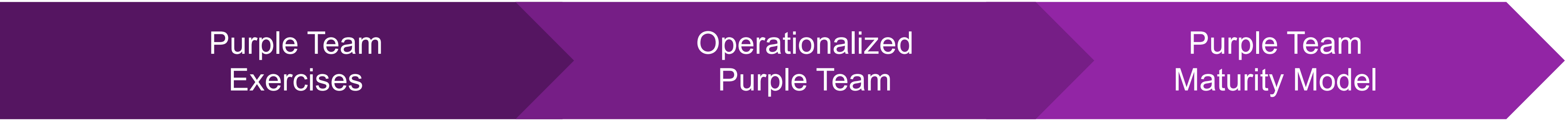
No alerts = no response

13 alerts

- Our team saw them
- They followed process
- Responded before impact

https://plextrac.com/

Great First Exercise! What now?



Purple Team Exercises

Operationalized Purple Team

Purple Team Maturity Model

Purple Team Exercises

- Seperate teams (CTI, Red, Blue) come together for an exercise
- Threat informed adversary emulations
- Performed on a scheduled basis (e.g. every 3 months)

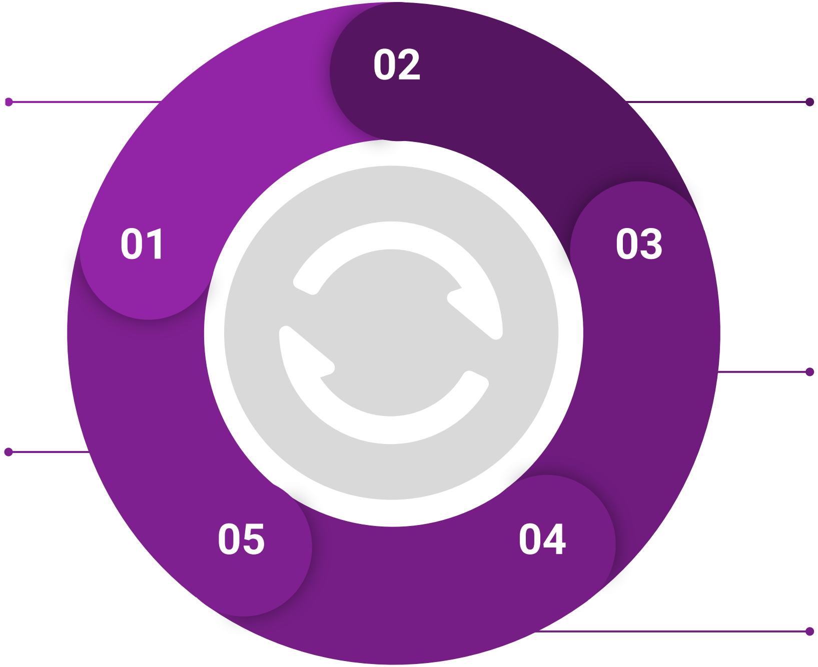
Operationalized Purple Team

- Dedicated, internal CTI, Red, and Blue teams work together as virtual team
- As new TTPs are discovered, they are analyzed and tested to build detections in a continuous cycle

Purple Team Maturity Model

- Dedicated role that has knowledge and experience with Cyber Threat Intelligence, Attack, Detection, and Response.
- Focus on threat and detection understanding

Operationalized Purple Team



New CTI or TTPs

- CTI, Red, or Blue discover/share/notify
- Assign CTI, Red, and Blue Team member

Analyze & Organize TTPs

- Map to MITRE ATT&CK
- Correlate with previous tests

Tabletop Discussion

- Expected Detection and Response

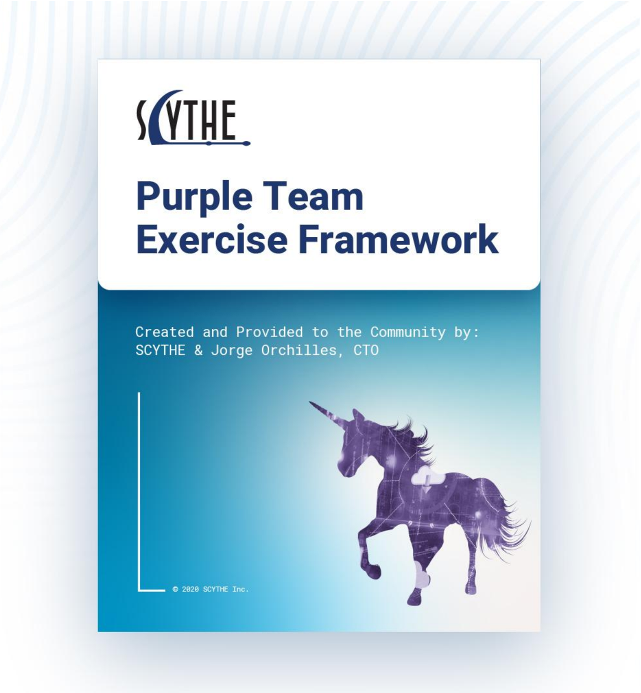
Emulate Attack

- Threat Understanding
- Deployment, Integration, Creation

Detection Engineering

- Detection Understanding
- Deployment, Integration, Creation
- Repeat attack for training and validation

Purple Team Exercise Framework v2

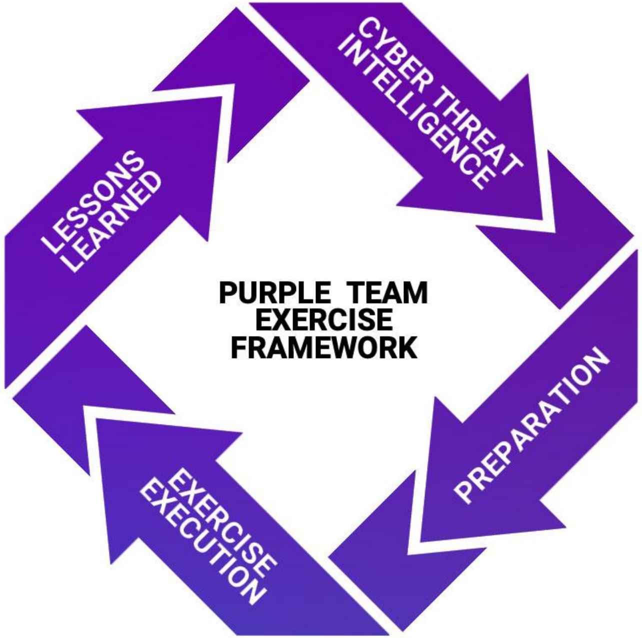


SCYTHE

Purple Team Exercise Framework

Created and Provided to the Community by: SCYTHE & Jorge Orchilles, CTO

© 2020 SCYTHE Inc.



PURPLE TEAM EXERCISE FRAMEWORK

CYBER THREAT INTELLIGENCE

PREPARATION

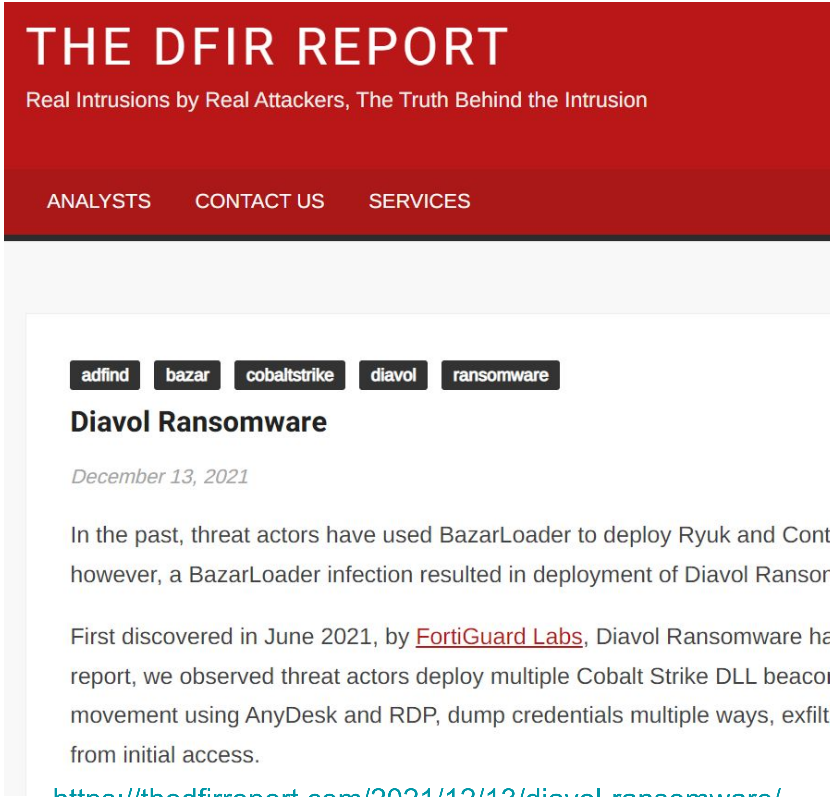
EXERCISE EXECUTION

LESSONS LEARNED

https://github.com/scythe-io/purple-team-exercise-framework/blob/master/PTEFv2.md

Step 1: New Cyber Threat Intelligence

- CTI, Red Team, or Blue Team can discover and share new intel
- Notification to Purple Team via new ticket/tracker
- Assign a CTI, Red, and Blue Team member
  - Self assigned or manager assigned



THE DFIR REPORT

Real Intrusions by Real Attackers, The Truth Behind the Intrusion

Diavol Ransomware

December 13, 2021

In the past, threat actors have used BazarLoader to deploy Ryuk and Cont
however, a BazarLoader infection resulted in deployment of Diavol Ransor

First discovered in June 2021, by FortiGuard Labs, Diavol Ransomware ha
report, we observed threat actors deploy multiple Cobalt Strike DLL beacoı
movement using AnyDesk and RDP, dump credentials multiple ways, exfilt
from initial access.

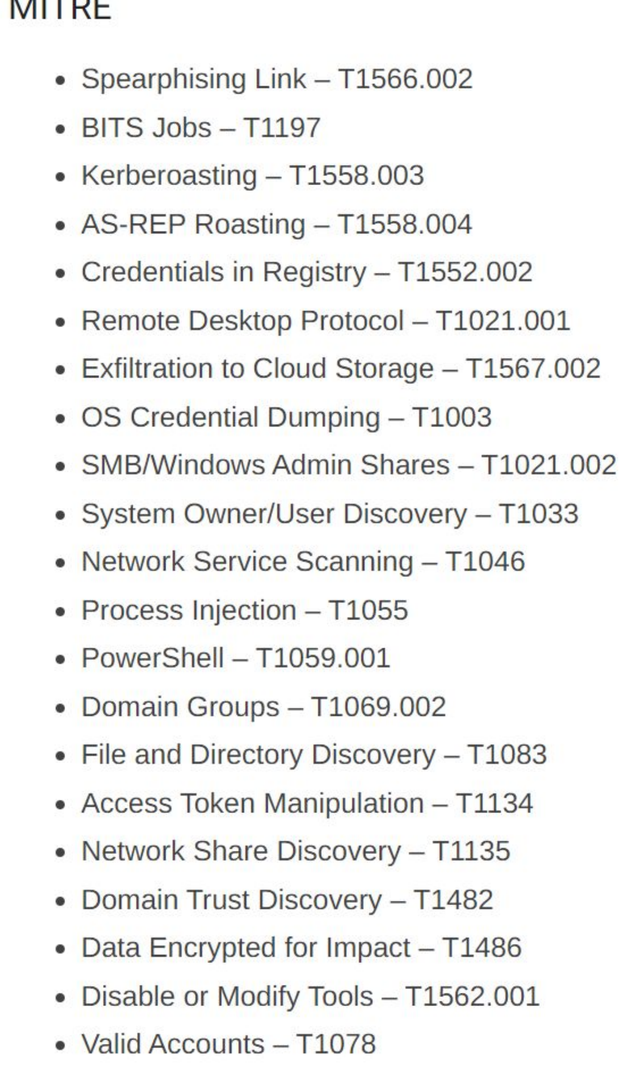
https://thedfirreport.com/2021/12/13/diavol-ransomware/

Initiate the Purple Team

Step 2: Analyze & Organize the TTPs

Extract TTPs & Map to MITRE ATT&CK

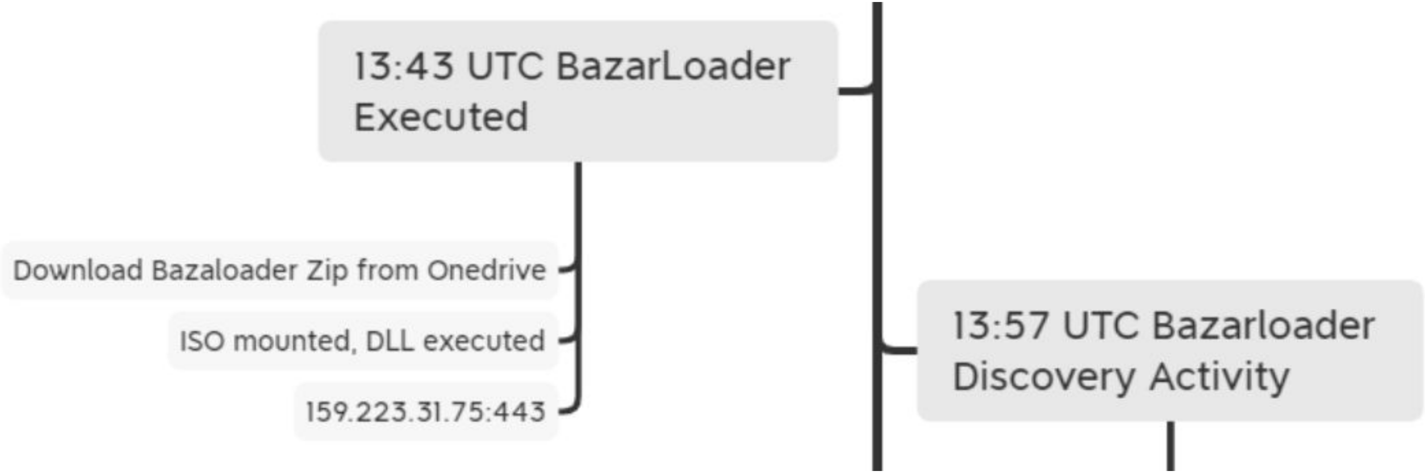
The malware (BazarLoader) was delivered to an endpoint via email, which included a link to OneDrive. The OneDrive link, directed the user to download a file that was a zip, which included an ISO inside. Once opened (mounted) on the users system, it was determined the ISO contained a LNK file and a DLL. The LNK file masqueraded as a Document enticing the user to click/open it. Once the user executed the LNK file, the BazarLoader infection was initiated.



MITRE

- Spearphising Link – T1566.002
- BITS Jobs – T1197
- Kerberoasting – T1558.003
- AS-REP Roasting – T1558.004
- Credentials in Registry – T1552.002
- Remote Desktop Protocol – T1021.001
- Exfiltration to Cloud Storage – T1567.002
- OS Credential Dumping – T1003
- SMB/Windows Admin Shares – T1021.002
- System Owner/User Discovery – T1033
- Network Service Scanning – T1046
- Process Injection – T1055
- PowerShell – T1059.001
- Domain Groups – T1069.002
- File and Directory Discovery – T1083
- Access Token Manipulation – T1134
- Network Share Discovery – T1135
- Domain Trust Discovery – T1482
- Data Encrypted for Impact – T1486
- Disable or Modify Tools – T1562.001
- Valid Accounts – T1078

Step 2: Analyze & Organize the TTPs



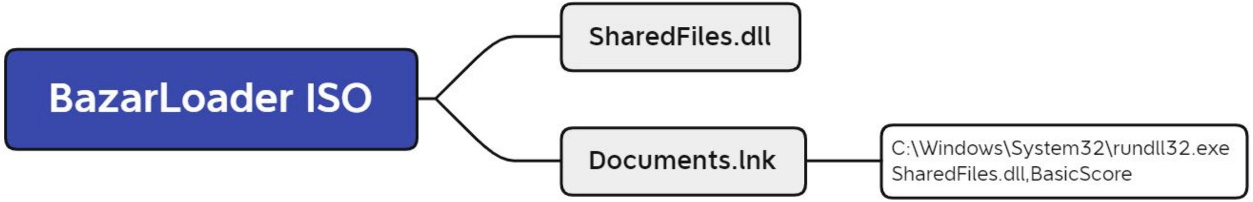
13:43 UTC BazarLoader Executed

Download Bazaloader Zip from Onedrive

ISO mounted, DLL executed

159.223.31.75:443

13:57 UTC Bazarloader Discovery Activity



BazarLoader ISO

SharedFiles.dll

Documents.lnk

C:\Windows\System32\rundll32.exe SharedFiles.dll,BasicScore

For real now... Analyze & Organize

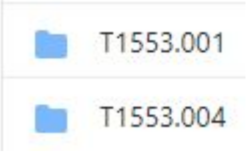
Tactic	Technique	Procedure
TA0001 Initial Access	T1566.002 Phishing: Spearphishing Link	The malware was delivered to an endpoint via email, which included a link to OneDrive
TA0005 Defense Evasion	T1553.005 Subvert Trust Controls: Mark-of-the-Web Bypass	The OneDrive link directed the user to download a file that was a zip, which included an ISO inside
TA0005 Defense Evasion	T1218.011 Signed Binary Proxy Execution: Rundll32	Once opened (mounted) on the users system, it was determined the ISO contained a LNK file and a DLL
TA0002 Execution	T1204.002 User Execution: Malicious File	The LNK file masqueraded as a Document enticing the user to click/open it
TA0011 Command and Control	T1071.001 Application Layer Protocol: Web Protocols	After the initial execution, the malware contacted two of its C2 IPs
TA0005 Defense Evasion	T1497.003 Virtualization/Sandbox Evasion: Time Based Evasion	BazaLoader was observed executing the well known battery of Windows discovery commands around 10 minutes after execution on the beachhead host.

DEMO

SCYTHE

Anything Net New?

- T1553.005 - Subvert Trust Controls: Mark-of-the-Web Bypass (ISO image)
  - Create an ISO image to bypass Mark-of-the-Web
  - Include a shortcut that executes a DLL via RunDLL32.exe
  - Zip the ISO
  - Upload to public OneDrive link
- Have we tested this before?
  - No Atomic Red Team tests either:



T1553.001

T1553.004

Step 3: Tabletop Discussion

Test Case	Expected Detection & Response
ISO downloaded from browser (Internet)	Allowed by browser, proxy, and Next-Gen FW
ISO downloaded from browser (internal)	Allowed by browser
ISO attached to email (external)	Blocked by external email security provider
ISO attached to email (internal)	Allowed by Outlook, email server security, endpoint security
Mounting ISO	No detection expected
Execution from ISO	Possible detection based on execution method
Unmounting ISO	No detection expected

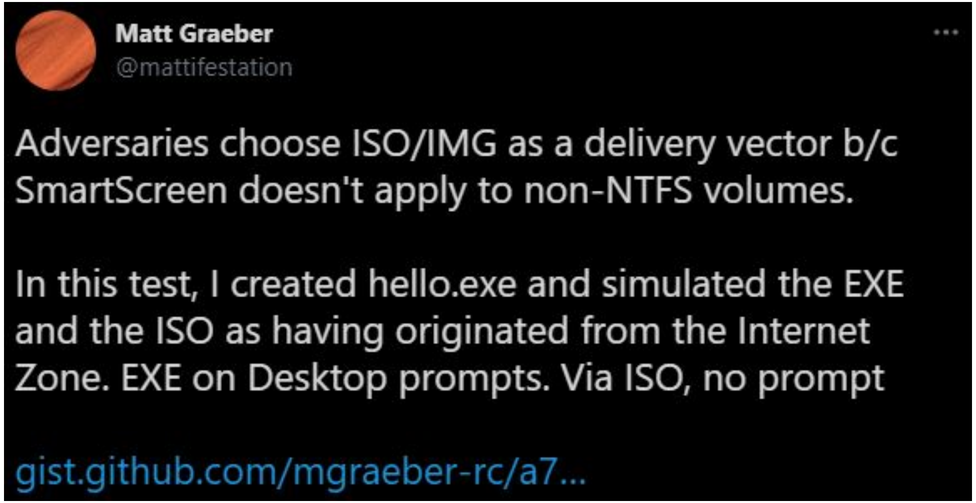
Step 4: Attack Plan

How do you create an ISO?

- https://twitter.com/mattifestation/status/1398323532988399620
- https://gist.github.com/mgraeber-rc/a780834c983bc0d53121c39c276bd9f3
- https://outflank.nl/blog/2020/03/30/mark-of-the-web-from-a-red-teams-perspective/
- https://www.scythe.io/library/defense-evasion-with-scythe

Thanks:

- @mattifestation
- @OutflankNL
- @scythe_io



Matt Graeber
@mattifestation

Adversaries choose ISO/IMG as a delivery vector b/c SmartScreen doesn't apply to non-NTFS volumes.

In this test, I created hello.exe and simulated the EXE and the ISO as having originated from the Internet Zone. EXE on Desktop prompts. Via ISO, no prompt

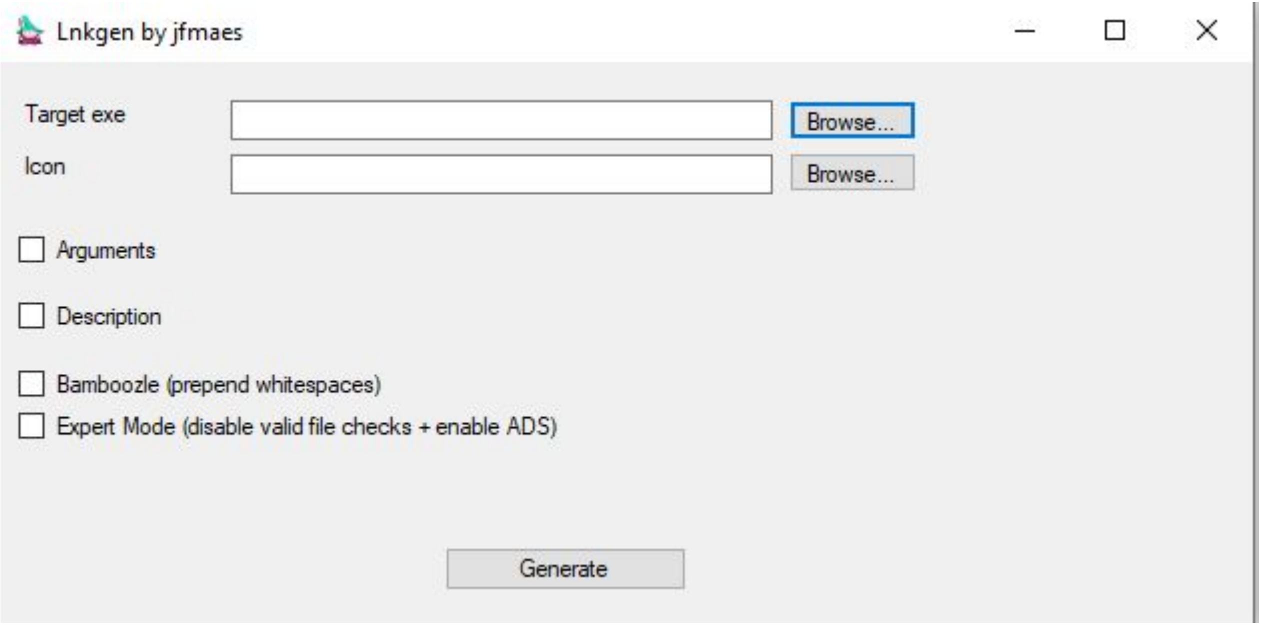
gist.github.com/mgraeber-rc/a7...

Step 4: Attack Plan

How do you create a .lnk?

Thanks:
@Jean_Maes_1994

- https://redteamer.tips/click-your-shortcut-and-you-got-pwned/



Target exe

Icon

□ Arguments

□ Description

□ Bamboozle (prepend whitespaces)

□ Expert Mode (disable valid file checks + enable ADS)

Step 4: Emulate Attack

- Set up Command and Control (C2) using HTTPS over 443/tcp & generate a DLL payload
- Copy the src folder from our GitHub for T1553.005 to a working directory on your Windows system. *Thanks to the Folder2Iso project for making it easy to create an ISO*
- Put the DLL in the Folder2Iso of the working directory
- In the Folder2Iso directory, create a shortcut called `Documents` and set the `Target` to: `C:\Windows\System32\rundll32.exe SharedFiles.dll,BasicScore`
- Run `Folder2Iso.exe "Folder2Iso" "new-documents-2005.iso" "Diavol" 0 0 0 "None"` This will take all the content of the Folder2Iso folder and create an ISO of it
- Zip the ISO and call it `new-documents-2005.zip`
- Upload the zip file to Microsoft OneDrive and copy the link
- Send a phishing email with the link to the Microsoft OneDrive zip file
- If the end user downloads the ZIP and double clicks the ISO, it will be mounted on their endpoint
- The user will need to double click the shortcut to begin execution

https://github.com/scythe-io/compound-actions/tree/main/T1553.005%20-%20Mark-of-the-Web%20Bypass

DEMO

Step 5: Detection Engineering

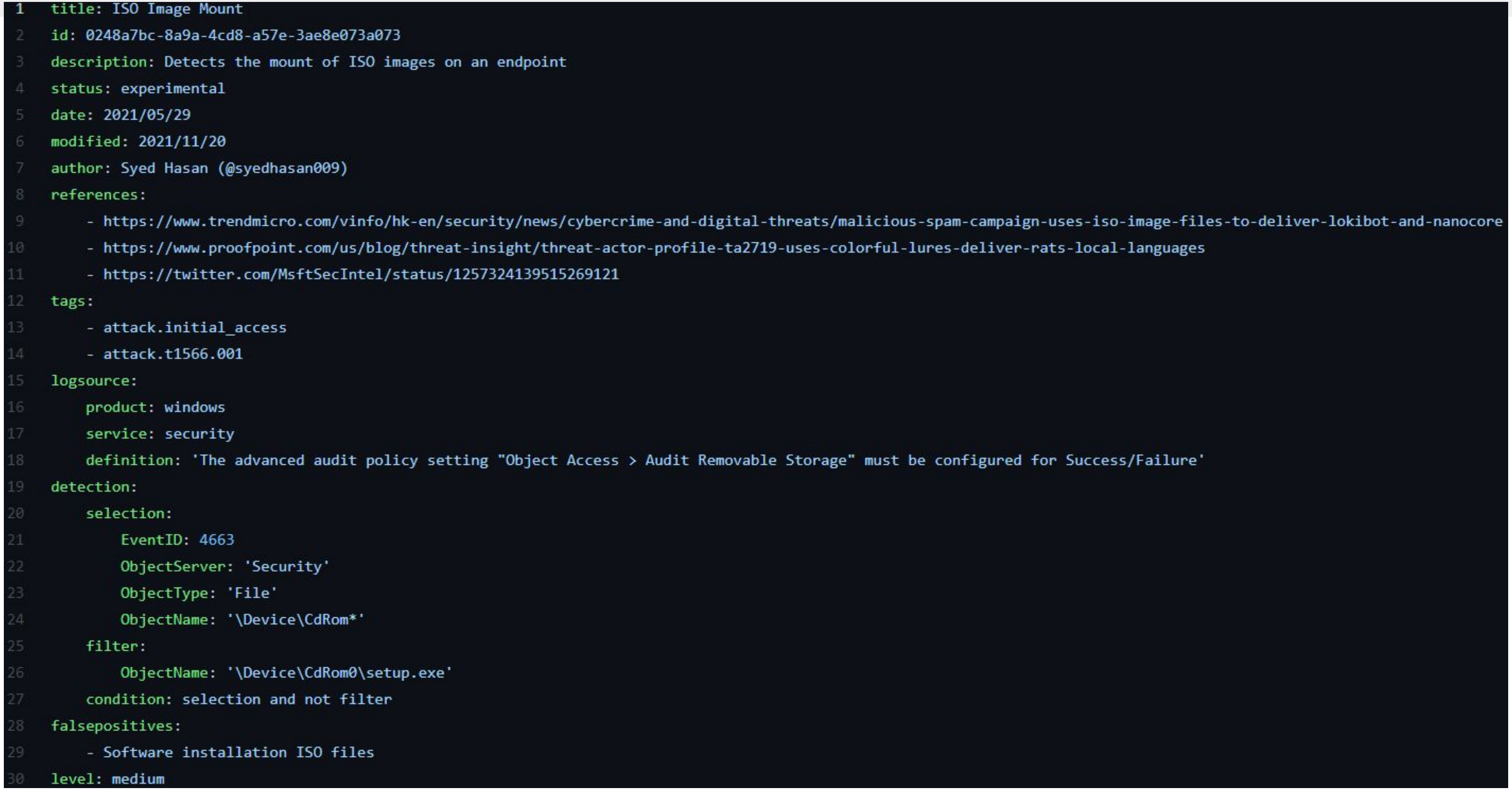
Hypothesis:

Thanks
@Cyb3rMonk
@SecurePeacock

- ISO file downloaded from Internet by non-IT user is suspicious
- ISO file sent via email is suspicious
- ISO mounted is suspicious on non-IT user systems
- Process execution from a mounted drive is suspicious
- Network connection from a process that runs from a mounted drive is suspicious

https://mergene.medium.com/detecting-initial-access-html-smuggling-and-iso-images-part-2-f8dd600430e2

Sigma Rule?

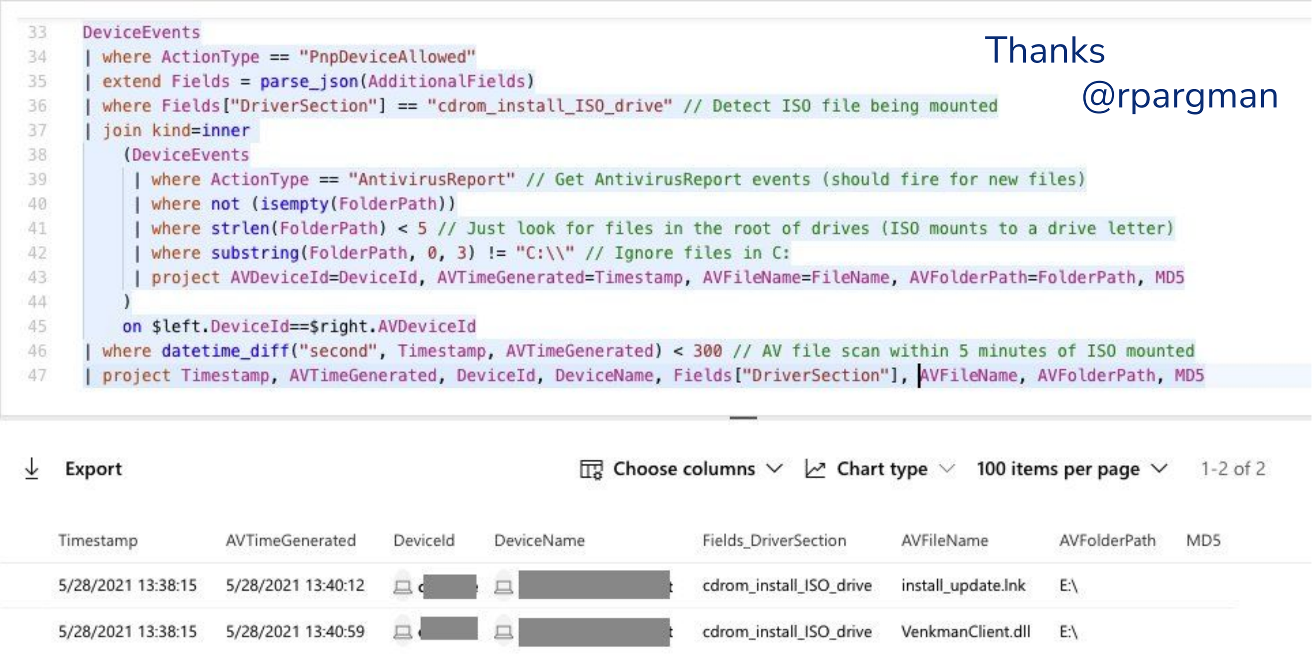


```
title: ISO Image Mount
id: 0248a7bc-8a9a-4cd8-a57e-3ae8e073a073
description: Detects the mount of ISO images on an endpoint
status: experimental
date: 2021/05/29
modified: 2021/11/20
author: Syed Hasan (@syedhasan009)
references:
    - https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/malicious-spam-campaign-uses-iso-image-files-to-deliver-lokibot-and-nanocore
    - https://www.proofpoint.com/us/blog/threat-insight/threat-actor-profile-ta2719-uses-colorful-lures-deliver-rats-local-languages
    - https://twitter.com/MsftSecIntel/status/1257324139515269121
tags:
    - attack.initial_access
    - attack.t1566.001
logsource:
    product: windows
    service: security
    definition: 'The advanced audit policy setting "Object Access > Audit Removable Storage" must be configured for Success/Failure'
detection:
    selection:
        EventID: 4663
        ObjectServer: 'Security'
        ObjectType: 'File'
        ObjectName: '\Device\CdRom*'
    filter:
        ObjectName: '\Device\CdRom0\setup.exe'
    condition: selection and not filter
falsepositives:
    - Software installation ISO files
level: medium
```

https://github.com/SigmaHQ/sigma/blob/04f72b9e78f196544f8f1331b4d9158df34d7ecf/rules/windows/builtin/security/win_iso_mount.yml

Step 5: Detection Engineering

- Logged locally
  - Proxy
  - Email
  - AV
  - EDR
  - sysmon
- Logged centrally
- Alert
- Detection
- Response

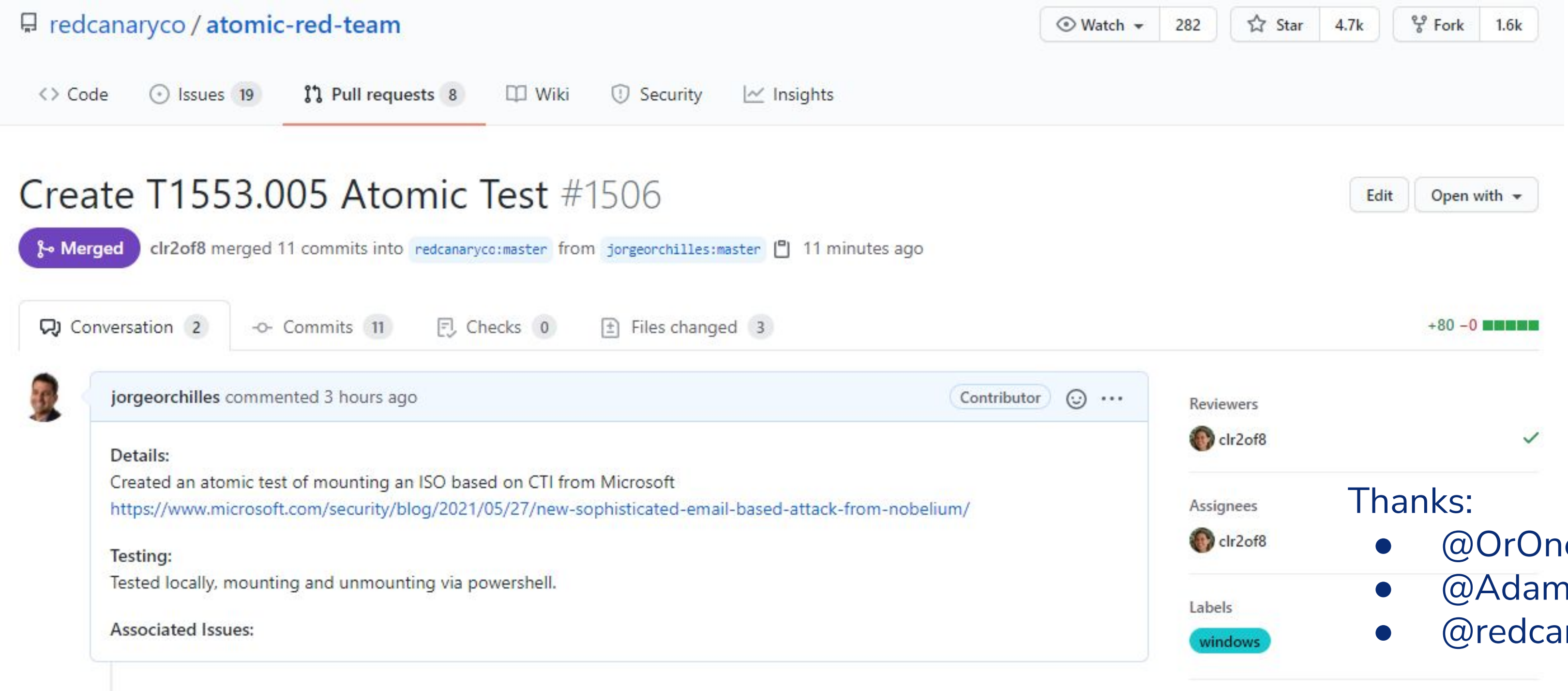


```
DeviceEvents
| where ActionType == "PnpDeviceAllowed"
| extend Fields = parse_json(AdditionalFields)
| where Fields["DriverSection"] == "cdrom_install_ISO_drive" // Detect ISO file being mounted
| join kind=inner
    (DeviceEvents
     | where ActionType == "AntivirusReport" // Get AntivirusReport events (should fire for new files)
     | where not (isempty(FolderPath))
     | where strlen(FolderPath) < 5 // Just look for files in the root of drives (ISO mounts to a drive letter)
     | where substring(FolderPath, 0, 3) != "C:\\" // Ignore files in C:
     | project AVDeviceId=DeviceId, AVTimeGenerated=Timestamp, AVFileName=FileName, AVFolderPath=FolderPath, MD5
    )
    on $left.DeviceId==$right.AVDeviceId
| where datetime_diff("second", Timestamp, AVTimeGenerated) < 300 // AV file scan within 5 minutes of ISO mounted
| project Timestamp, AVTimeGenerated, DeviceId, DeviceName, Fields["DriverSection"], AVFileName, AVFolderPath, MD5
```

Thanks
@rpargman

Timestamp	AVTimeGenerated	DeviceId	DeviceName	Fields_DriverSection	AVFileName	AVFolderPath	MD5
5/28/2021 13:38:15	5/28/2021 13:40:12	[redacted]	[redacted]	cdrom_install_ISO_drive	install_update.lnk	E:\	
5/28/2021 13:38:15	5/28/2021 13:40:59	[redacted]	[redacted]	cdrom_install_ISO_drive	VenkmanClient.dll	E:\	

Contribute: Atomic Red Team



redcanaryco / atomic-red-team

Create T1553.005 Atomic Test #1506

Merged clr2of8 merged 11 commits into `redcanaryco:master` from `jorgeorchilles:master` 11 minutes ago

jorgeorchilles commented 3 hours ago

Details:
Created an atomic test of mounting an ISO based on CTI from Microsoft
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

Testing:
Tested locally, mounting and unmounting via powershell.

Associated Issues:

Reviewers
clr2of8 ✓

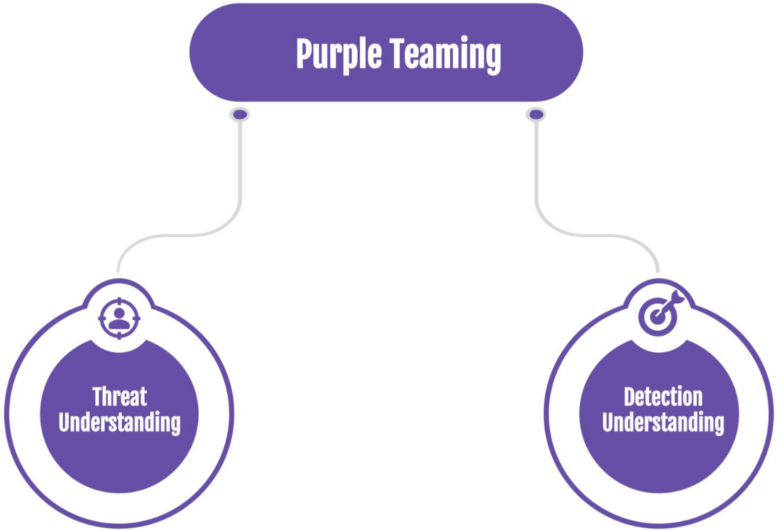
Assignees
clr2of8

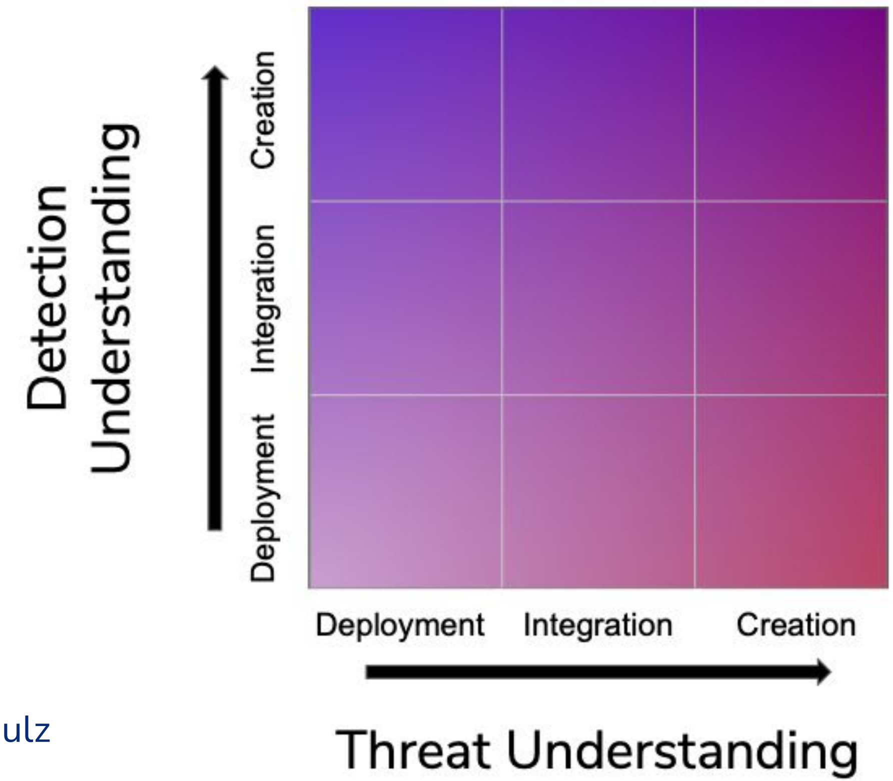
Labels
windows

Thanks:
- @OrOneEqualsOne
- @Adam_Mashinchi
- @redcanary

https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1553.005/T1553.005.md

Dedicated Purple Team – Maturity Model





Thanks
@teschulz

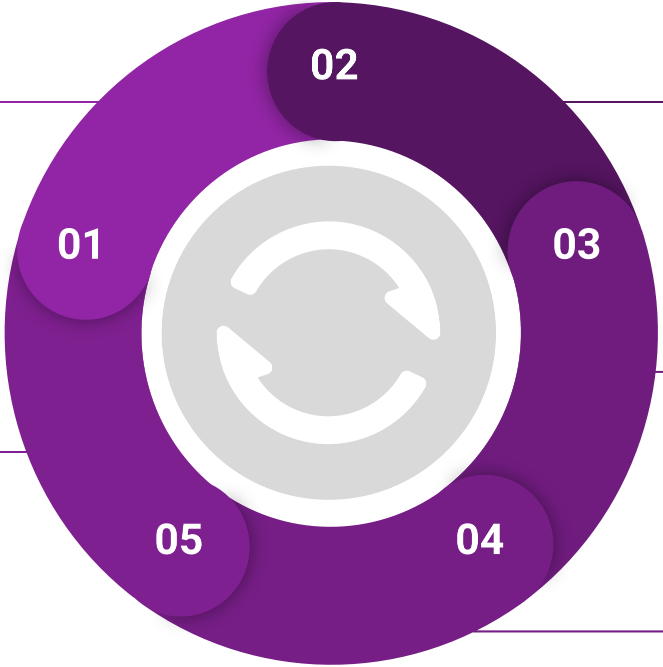
https://www.scythe.io/library/introducing-the-purple-team-maturity-model

Takeaways

Purple Team Exercises

Operationalized Purple Team

Purple Team Maturity Model



New CTI or TTPs

Analyze & Organize TTPs

Tabletop Discussion

Emulate Attack

Detection Engineering

MOAR Content? #ThreatThursday

- Introduce Adversary
- Consume CTI and map to MITRE ATT&CK
- Present Adversary Emulation Plan
- Share the plan on SCYTHE Community Threat Github
    - https://github.com/scythe-io/community-threats/
- Emulate Adversary
- Detect & Respond
- All available to the community for free:
    - https://www.scythe.io/threatthursday

Purple Team Training?

- SCYTHE Purple Team Workshops: https://www.scythe.io/purple-team-workshops
- Operation Purple: https://www.antisyphontraining.com/operation-purple-w-tim-schulz/
- SANS SEC599 Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses: https://sans.org/sec599
- SANS SEC699 Purple Team Tactics - Adversary Emulation for Breach Prevention & Detection: https://sans.org/sec699

References

- https://github.com/scythe-io/purple-team-exercise-framework
- https://thedfirreport.com/2021/12/13/diavol-ransomware/
- https://github.com/scythe-io/community-threats/tree/master/Diavol
- https://twitter.com/mattifestation/status/1398323532988399620
- https://twitter.com/rpargman/status/1398337541917450240
- https://gist.github.com/mgraeber-rc/a780834c983bc0d53121c39c276bd9f3
- https://github.com/scythe-io/compound-actions/tree/main/T1553.005%20-%20Mark-of-the-Web%20Bypass
- https://www.trustfm.net/software/utilities/Folder2Iso.php
- https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1553.005/T1553.005.md
- https://redteamer.tips/click-your-shortcut-and-you-got-pwned/
- https://mergene.medium.com/detecting-initial-access-html-smuggling-and-iso-images-part-2-f8dd600430e2
- https://github.com/SigmaHQ/sigma/blob/04f72b9e78f196544f8f1331b4d9158df34d7ecf/rules/windows/builtin/security/win_iso_mount.yml

Jorge Orchilles

- Chief Technology Officer - SCYTHE
- Author/Co-Creator
  - Purple Team Exercise Framework (PTEF)
  - C2 Matrix
  - SEC564: Red Team Exercises and Adversary Emulation
- Contributor
  - MITRE ATT&CK
  - Atomic Red Team
  - CVSSv3.1 Working Group Voting Member
  - GFMA: Threat-Led Pentest Framework
- ISSA Fellow; NSI Technologist Fellow

Microsoft Windows 7 Administrator's Reference

Jorge Orchilles

SCYTHE CTO

Operationalizing Purple Team

What happens after your first successful Purple Team Exercise?