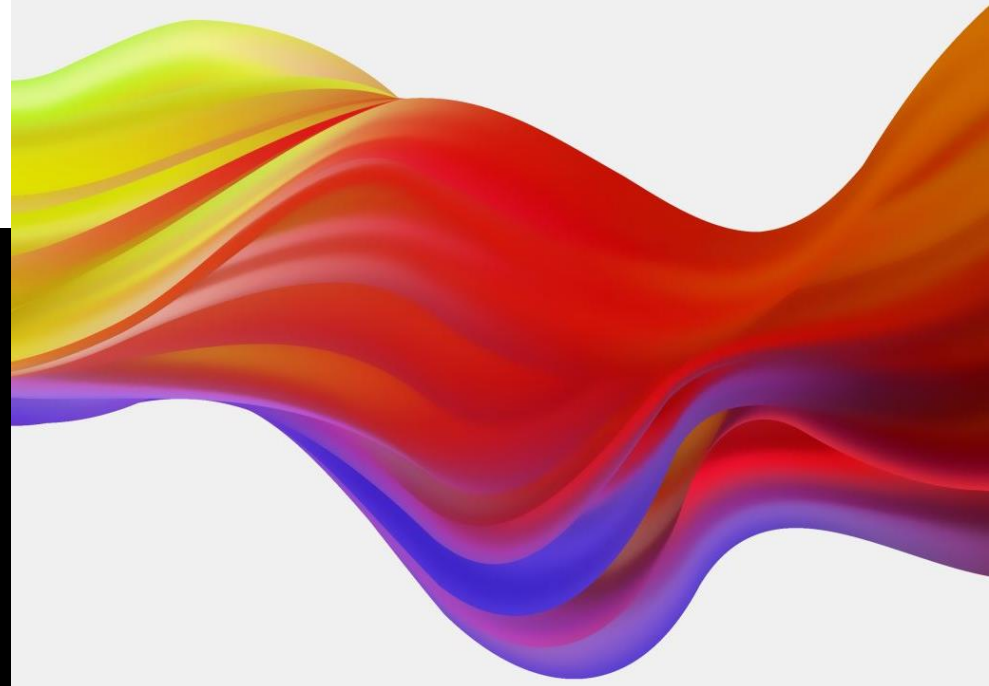
PWNDEFEND

KILL CHAINS

Event Abstractions to support cyber defence



SCENARIOS

1. Internal System Enumeration
2. Ransomware
3. Phishing
4. Malicious Link
5. Malware download and execute
6. Business Email Compromise
7. Denial of Service
8. Evil Maid

INTERNAL ENUMERATION

1. Gain access to target system
2. Run enumeration commands (LOLBINS) as described in the GitHub repo 1.0 step
3. Review Detections

[cyberwar/1.0_warfare_2.0_enum at main · mr-r3b00t/cyberwar (github.com)]

*It's not really a cyber war, it's just code execution on a computer!

RANSOMWARE

1. Enumerate Services
2. Enumerate Valid Usernames
3. Brute Force Credentials or Phish
4. Bypass MFA/SE MFA
5. Gain Access to VPN
6. Establish beachhead on workstation/server if required
7. LDAP Auth to Active Directory
8. Gain Foothold
9. Privesc via known AD Vuln/Server/Workstation Vuln
10. Drop Tools/Payloads
11. Obtain Domain Admin
12. Find backup servers
13. Gain access to backup services
14. Delete/Encrypt Backups
15. Exfiltrate Data
16. Deploy Scheduled Task
17. Encrypt Target Environment

PHISHING

1. Email sent
2. SPF/DMARC Checks
3. Mail hygiene allows email
4. Delivered to mailbox
5. Mail opened
6. URL Clicked
7. >>>HEAD TO : Malicious Link Workflow

MALICIOUS LINK

1. Link Clicked
2. Protective DNS (PDNS) Lookup
3. Web Content Filtering
4. Blocked Domain Check
5. Visit page
6. Credential harvester
7. User Enters Credentials
8. Conditional Access
9. MFA Prompt
10. User Response
11. Auth Token Granted
12. Proactive Monitoring
13. SOC Responds

MALWARE DOWNLOAD & EXEC

1. Link Clicked
2. Protective DNS (PDNS) Lookup
3. Web Content Filtering
4. Blocked Domain Check
5. Visit page
6. File Downloaded
7. File hash checked
8. File writes to disk
9. AV Scan
10. Process Launched
11. EDR Analysis
12. Code Execution

BUSINESS EMAIL COMPROMISE

1. Mailbox accessed by unauthorised actor
2. Mailbox rules created
3. Mailbox contents downloaded
4. Financial transaction/conversation tampering
5. Man in the Middle Invoice communications
6. Attempt to change bank details/invoice details with third party

DENIAL OF SERVICE

1. Large volume of traffic from multiple source IPs or Large volume of traffic from a single source IP
2. Web server resource consumption
3. Database server resource consumption

EVIL MAID

1. Malicious USB Device plugged into computer
2. Payload execution (either malware of HID)
3. C2 Comms
4. Backdoor access by external threat actor

EXTERNAL RESOURCES

Cyber Incident Response – Have you planned to fail? – PwnDefend

IRM/EN at main · certsocietegenerale/IRM · GitHub

Exercise in a Box - NCSC.GOV.UK

NCSC EXERCISE IN A BOX

1. A ransomware attack delivered by phishing email
2. Mobile phone theft and response
3. Being attacked from an unknown Wi-Fi network
4. Insider threat leading to a data breach
5. Third party software compromise
6. BYOD
7. Threatened leak of sensitive data
8. Supply chain risks
9. Home & remote working
10. Managing a vulnerability disclosure
11. Supply chain software
12. Supply chain ransomware attack
13. Technical scenario