

D3FCON



# Down the Rabbit Hole: 10 Lessons Learned from a Year in the Trenches

---

Andrew Costis

## >> whois <<

---

- Andrew Costis / “AC”
- Senior Cyber Threat Consultant **ATTACKIQ**®
- 20+ Years industry experience
  - 5+ years threat research, malware RE, DFIR



@ox4143



/andrewcostis/



/ox4143

## >> Motivation <<

---

- To share some practical tips, tricks and advice based on my own journey and experiences
- Applicable to both technical and non-technical peers
- Applicable to:
  - Breach and Attack Simulation (BAS)
  - Threat/Adversary emulation
  - Red/Blue/Purple teaming
  - Security Control Validation
  - Security Optimization
  - Threat-Informed Defense
  - DIY/in-house/BYOTTPs<sup>©</sup>
  - Related new/upcoming/trending buzz-words/acronyms/terms

## >> Misc <<

---

- Top 10 Lessons are in no particular order
- Assumed *basic conceptual* understanding of key terms
- Random British pictures added for good measure

# >> 1: Understand the Environment <<

- Inventory, map, document as much as possible
- Business structure, departments, regions, business units
- Network topology
- Data flow, patterns, users
- Cloud, on-prem assets
- Crown jewel applications
- Security controls
- Eases pain when scaling out, planning assessments, triaging and remediating



## >> 2: Understand the Security Objectives <<

---

- Regulatory / compliance
- Threat of the week
- Targeted attacks, TA specific
- OS specific
- Insider threats
- SOC augmentation
- Cloud threats
- Security control validation
- Warning: goal posts likely to change!



## >> 3: Stakeholder Support <<

---

- Critical for long term success and adoption
- Gets on everybody's radar
- Helps in staying aligned
- Break through barriers
- People come and go (churn)
- Meet regularly to:
  - Prioritize work
  - Identify challenges
  - Scope creep
  - Discuss progress
  - Set action items



## >> 4: Information Sharing & Collaboration <<

---

- Decide and agree on a central place to store your work
  - E.g. Teams, GitHub, Jira, Vectr.io, SharePoint, Excel
- Decide on access control early on (due to sensitivity)
- Junior (green) audience
- Plan for scale/growth in mind
- Be as granular as possible
- Likely to include:
  - Security control configuration
  - Assessment/test specific configuration
  - Detection info / log, alert output
  - Mitigation/remediation notes
  - TTPs tested



## >> 5: Detection vs Prevention <<

---

- Prevention is often the preferred choice
- Some TTPs may be too complex to prevent
- Detection will likely be a more realistic near-term goal
- Detection provides invaluable and much needed visibility
- Not easy to patch/mitigate/remediate legacy systems
- Defense in depth approach



# >> Techniques with Mitigations <<

| Reconnaissance  | Resource Development  | Initial Access  | Execution  | Persistence  | Privilege Escalation  | Defense Evasion  | Credential Access  | Discovery  | Lateral Movement   | Collection   | Command and Control  | Exfiltration   | Impact   |
|---|---|---|--|--|---|--|--|--|--|--|--|--|--|
| 10 techniques   | 7 techniques  | 9 techniques  | 12 techniques  | 19 techniques  | 13 techniques   | 42 techniques  | 16 techniques  | 30 techniques  | 9 techniques   | 17 techniques  | 16 techniques  | 9 techniques   | 13 techniques  |
| Active Scanning (3/3)<br>Gather Victim Host Information (4/4)<br>Gather Victim Identity Information (3/3)<br>Gather Victim Network Information (6/6)<br>Gather Victim Org Information (4/4)<br>Phishing for Information (3/3)<br>Search Closed Sources (2/2)<br>Search Open Technical Databases (5/5)<br>Search Open Websites/Domains (2/2)<br>Search Victim-Owned Websites | Acquire Infrastructure (6/6)<br>Compromise Accounts (2/2)<br>Compromise Infrastructure (6/6)<br>Develop Capabilities (4/4)<br>Establish Accounts (2/2)<br>Obtain Capabilities (6/6)<br>Stage Capabilities (5/5) | Drive-by Compromise<br>Exploit Public-Facing Application<br>Compromise Accounts (2/2)<br>External Remote Services<br>Hardware Additions<br>Replication Through Removable Media<br>Supply Chain Compromise (3/3)<br>Trusted Relationship<br>Valid Accounts (4/4) | Command and Scripting Interpreter (8/8)<br>Container Administration Command<br>Deploy Container<br>Exploitation for Client Execution<br>Inter-Process Communication (3/3)<br>Native API<br>Scheduled Task/Job (5/5)<br>Shared Modules<br>Create or Modify System Process (4/4)<br>Event Triggered Execution (10/16)<br>External Remote Services<br>Hijack Execution Flow (12/12)<br>Implant Internal Image<br>Modify Authentication Process (5/5)<br>Office Application Startup (6/6)<br>Pre-OS Boot (5/5)<br>Scheduled Task/Job (5/5)<br>Server Software Component (5/5)<br>Traffic Signaling (1/1) | Account Manipulation (5/5)<br>BITS Jobs<br>Boot or Logon Autostart Execution (10/14)<br>Boot or Logon Initialization Scripts (5/5)<br>Browser Extensions<br>Compromise Client Software Binary<br>Create Account (3/3)<br>Create or Modify System Process (4/4)<br>Domain Policy Modification (2/2)<br>Escape to Host<br>Event Triggered Execution (10/16)<br>Exploitation for Privilege Escalation<br>File and Directory Permissions Modification (2/2)<br>Hide Artifacts (7/10)<br>Hijack Execution Flow (12/12)<br>Impair Defenses (9/9)<br>Indicator Removal on Host (3/6)<br>Indirect Command Execution<br>Masquerading (4/7)<br>Modify Authentication Process (5/5)<br>Steal or Forge Kerberos Tickets (4/4)<br>Steal Web Session Cookie<br>Unsecured Credentials (7/7)<br>Modify Registry<br>Modify System Image (2/2) | Abuse Elevation Control Mechanism (4/4)<br>Access Token Manipulation (4/6)<br>BITS Jobs<br>Boot or Logon Autostart Execution (10/14)<br>Build Image on Host<br>Debugger Evasion<br>Deobfuscate/Decode Files or Information<br>Deploy Container<br>Direct Volume Access<br>Domain Policy Modification (2/2)<br>Execution Guardrails (1/1)<br>Exploit for Defense Evasion<br>File and Directory Permissions Modification (2/2)<br>Hide Artifacts (7/10)<br>Hijack Execution Flow (12/12)<br>Impair Defenses (9/9)<br>Indicator Removal on Host (3/6)<br>Indirect Command Execution<br>Masquerading (4/7)<br>Modify Authentication Process (5/5)<br>Steal or Forge Kerberos Tickets (4/4)<br>Steal Web Session Cookie<br>Unsecured Credentials (7/7)<br>Modify Registry<br>Modify System Image (2/2) | Adversary-in-the-Middle (3/3)<br>Brute Force (4/4)<br>Credentials from Password Stores (4/5)<br>BITS Jobs<br>Build Image on Host<br>Debugger Evasion<br>Deobfuscate/Decode Files or Information<br>Deploy Container<br>Direct Volume Access<br>Domain Policy Modification (2/2)<br>Execution Guardrails (1/1)<br>Exploit for Defense Evasion<br>File and Directory Permissions Modification (2/2)<br>Hide Artifacts (7/10)<br>Hijack Execution Flow (12/12)<br>Impair Defenses (9/9)<br>Indicator Removal on Host (3/6)<br>Indirect Command Execution<br>Masquerading (4/7)<br>Modify Authentication Process (5/5)<br>Steal or Forge Kerberos Tickets (4/4)<br>Steal Web Session Cookie<br>Unsecured Credentials (7/7)<br>Modify Registry<br>Modify System Image (2/2) | Account Discovery (3/4)<br>Application Window Discovery<br>Browser Bookmark Discovery<br>Cloud Infrastructure Discovery<br>Cloud Service Dashboard<br>Cloud Service Discovery<br>Cloud Storage Object Discovery<br>Container and Resource Discovery<br>Input Capture (2/4)<br>Modify Authentication Process (5/5)<br>Execution Guardrails (1/1)<br>Exploit for Defense Evasion<br>File and Directory Permissions Modification (2/2)<br>Group Policy Discovery<br>Network Sniffing<br>OS Credential Dumping (8/8)<br>Steal Application Access Token<br>Peripheral Device Discovery<br>Masquerading (4/7)<br>Modify Authentication Process (5/5)<br>Steal or Forge Kerberos Tickets (4/4)<br>Steal Web Session Cookie<br>Unsecured Credentials (7/7)<br>Modify Registry<br>Modify System Image (2/2) | Adversary-in-the-Middle (3/3)<br>Internal Spearphishing<br>Lateral Tool Transfer<br>Remote Service Session Hijacking (2/2)<br>Cloud Service Discovery<br>Cloud Storage Object Discovery<br>Container and Resource Discovery<br>Input Capture (2/4)<br>Modify Authentication Process (5/5)<br>Execution Guardrails (1/1)<br>Exploit for Defense Evasion<br>File and Directory Permissions Modification (2/2)<br>Group Policy Discovery<br>Network Sniffing<br>OS Credential Dumping (8/8)<br>Steal Application Access Token<br>Peripheral Device Discovery<br>Masquerading (4/7)<br>Modify Authentication Process (5/5)<br>Steal or Forge Kerberos Tickets (4/4)<br>Steal Web Session Cookie<br>Unsecured Credentials (7/7)<br>Modify Registry<br>Modify System Image (2/2) | Exploitation of Remote Services<br>Internal Spearphishing<br>Lateral Tool Transfer<br>Remote Service Session Hijacking (2/2)<br>Cloud Service Discovery<br>Cloud Storage Object Discovery<br>Container and Resource Discovery<br>Input Capture (2/4)<br>Modify Authentication Process (5/5)<br>Execution Guardrails (1/1)<br>Exploit for Defense Evasion<br>File and Directory Permissions Modification (2/2)<br>Group Policy Discovery<br>Network Sniffing<br>OS Credential Dumping (8/8)<br>Steal Application Access Token<br>Peripheral Device Discovery<br>Masquerading (4/7)<br>Modify Authentication Process (5/5)<br>Steal or Forge Kerberos Tickets (4/4)<br>Steal Web Session Cookie<br>Unsecured Credentials (7/7)<br>Modify Registry<br>Modify System Image (2/2) | Adversary-in-the-Middle (3/3)<br>Internal Spearphishing<br>Lateral Tool Transfer<br>Remote Service Session Hijacking (2/2)<br>Cloud Service Discovery<br>Cloud Storage Object Discovery<br>Container and Resource Discovery<br>Input Capture (2/4)<br>Modify Authentication Process (5/5)<br>Execution Guardrails (1/1)<br>Exploit for Defense Evasion<br>File and Directory Permissions Modification (2/2)<br>Group Policy Discovery<br>Network Sniffing<br>OS Credential Dumping (8/8)<br>Steal Application Access Token<br>Peripheral Device Discovery<br>Masquerading (4/7)<br>Modify Authentication Process (5/5)<br>Steal or Forge Kerberos Tickets (4/4)<br>Steal Web Session Cookie<br>Unsecured Credentials (7/7)<br>Modify Registry<br>Modify System Image (2/2) | Application Layer Protocol (4/4)<br>Communication Through Removable Media<br>Data Encoding (2/2)<br>Data Obfuscation (3/3)<br>Dynamic Resolution (1/3)<br>Encrypted Channel (2/2)<br>Fallback Channels<br>Ingress Tool Transfer<br>Multi-Stage Channels<br>Non-Application Layer Protocol<br>Non-Standard Port<br>Protocol Tunneling<br>Data Staged (0/2)<br>Proxy (4/4)<br>Email Collection (3/3)<br>Input Capture (2/4)<br>Screen Capture<br>Video Capture | Automated Exfiltration (1/1)<br>Data Transfer Size Limits<br>Exfiltration Over Alternative Protocol (3/3)<br>Exfiltration Over C2 Channel<br>Exfiltration Over Other Network Medium (1/1)<br>Exfiltration Over Physical Medium (1/1)<br>Inhibit System Recovery<br>Network Denial of Service (2/2)<br>Resource Hijacking<br>Service Stop<br>System Shutdown/Reboot | Account Access Removal<br>Data Destruction<br>Data Encrypted for Impact<br>Data Manipulation (3/3)<br>Defacement (2/2)<br>Disk Wipe (2/2)<br>Endpoint Denial of Service (4/4)<br>Firmware Corruption<br>Inhibit System Recovery<br>Network Denial of Service (2/2)<br>Resource Hijacking<br>Service Stop<br>System Shutdown/Reboot |

# >> Techniques with Data Sources <<

## >> 6: Direct vs Indirect Findings <<

---

- Direct Finding:
  - **Event Triggered Execution: WMI Event Subscription (T1546.003)** using .mof files is prevented and/or detected by 'X' security control
- Indirect Finding:
  - **Application Layer Protocols: Web Protocols (T1071.001)** using exfil of dummy data is detected, **but** detection took >4 hours for the alert to arrive, resulting in the SOC missing the alert
  - **Windows Management Instrumentation (T1047)** using *wmic process call create* isn't prevented and/or detected **due to** Endpoint sensor not checking in, not installed, or wrong policy applied, subsequently resulting in a test binary executable being able to launch
- Will likely observe indirect findings throughout
- Continuous automated testing at scale will bring both to the surface
- Key to improving overall security posture and maturity



## >> 7: Start Small <<

---

- Requires careful planning and scoping
- Identify test hosts early on (dedicated or temp)
- Baseline where possible
- Test in production when confident
- Focus on a few TTPs, or a small section of an attack chain first, in order to test out your process and workflow
- Quality vs quantity
- The more you test, the more findings you will uncover
  - Not always a good thing...
- Network TTPs are a good place to start



## >> 8: Purple Teaming <<

---

- Establish early on
- Regular meeting cadence critical to continuity
- Ability to obtain a range of input
  - Intelligence-led
- What's keeping them up at night?
- Designed to support & augment each other's workloads and priorities
- Narrative/story
  - Useful in supporting wider initiatives
  - Top ATT&CK Techniques – CTID project



## >> 9: Automation <<

---

- If repeating a task more than once, automate where *feasible*
- Automate assessments
  - (integral to uncovering when drift occurs in the environment)
- Red team engagements >> adversary emulation
  - Procedural level details help
- Reporting
  - Assessments, weekly, monthly
- API integration with security controls
- CTI ingestion



## >> 10: Slow and Steady Wins the Race <<

---

- Rome wasn't built in a day
- Touches on all aspects and layers of security
- Enjoy the journey
- Don't make assumptions
- Motivation and persistence required
- Get familiar with free resources:
  -  /0x4143/adversaryemulation-gems





>> Thank You <<

---



@0x4143



/andrewcostis/



/0x4143