DCSO

Engineering Security.
Together.

Are We Ready?

Methods for Testing Breach Preparedness

Jeff Hamm, DCSO, Business Director IR

jeff.hamm@dcso.de

2021-10-14

TLP:GREEN

Shaping community-driven cyber defense

It is our mission to protect European companies and institutions from cyber threats through trusted advice and unique managed security solutions.

Our diverse and committed team works closely with our partners on shaping a trust-based cyber-defense community.

By doing so, we make a positive impact for customers, authorities and society.

Testing in an Operational Environment

Goals:

- How to Provide Insight and Guidance
- Utilizing Existing Tools and Skill Sets
- Determining Priorities of Projects

Feedback:

- Does the Community believe this is a good approach?

DCSO
Engineering Security. Together.

Jeff Hamm

Director Cyber Defense Services

Languages: English, German (conversational)

+49-151-72140869
jeff.hamm@dcso.de

Experience

- 10 Years Incident Response Consultant
- 20 Years in Digital Forensics
- Assistant professor for cybercrime investigation and digital forensics
- 15 years law enforcement experience as a supervisor, patrolman, and computer crime detective
- Published contributing author "Digital Forensics" (2017 edited by André Årnes)

Qualifications

- MS Cybersecurity and Information Assurance, Western Governors University, Salt Lake City, Utah
- BS Information Technology Security Emphasis, Western Governors University, Salt Lake City, Utah

Additional Qualifications

- Court Expert Witness Digital Forensics (3rd Circuit Court, Michigan)
- Certified Ethical Hacker (EC-Council)

Incident Response should take a proactive approach

Proactive

- Compromise Assessment
- IR Readiness Assessment
- IR Readiness Exercise

Active Incident Response

- Investigation
- Posturing
- Remediation

Sustainability

- Post Remediation

Readiness Exercise

Objective: identify improvement potential in existing setups with a realistic scenario (white box approach)

What: We provide a controlled set of artifacts that help to jointly execute a realistic scenario.
Practicing using your own setup helps to reveal gaps in technology and processes.

Practicing response to an incident before experiencing the pressure of an actual attack helps to raise confidence and maturity throughout the organization.

Ransomware Scenario Example

Cobalt Strike Implant

- Using a Cobalt Strike implant
- The exercise could consist of a scenario with an attacker attempting to:
  - Gain privileged account access
  - Gather reconaissance information
  - Install a persistent backdoors
    - Beacons to C2
  - Moving laterally to critical systems
    - IT operations / Domain Controllers
    - Sensitive file servers
  - Extracting / exfiltrating data
  - Encrypting and Compressing Data for “theft” or Ransom

Assumptions

- An attacker was able to gain a foothold in the network
- The initial compromise is NOT the focus of the exercise

Environmental Variables

Operational Considerations

- **permission to run scenario implant**
- participants
- 3rd party dependencies (IT operations / managed security providers)

IR Capabilities

- **Endpoint Security Capabilities / AV**
  - clients / workstations
  - servers
- log management / SIEM
- SOAR
- Monitoring Capabilities (e.g., Network)
- Analysis capabilities
- TI providers

IT Infrastructure

- **Proxy**
- **IP-Range** (Cloud Proxy (zscaler)?)
- firewall rules
- network segmentation
- **default route vs. proxy enforcement**
- DNS
- AD Setup (hybrid?)

Ideal Setup

Workstation

- Test Deployment
- In Production Environment
- User and Local Admin logins

Server

- Test Deployment
- In Production Environment
- Admin logins

Web Server

- Test Deployment
- In Production Environment
- Not Facing Externally
- Admin logins

Can this identify improvement potential for quick wins?

1 → 2 → 3

Preparation

- scenario selection (e.g., ransomware attack 2nd stage)
- define needed skill set / participants
- rules of engagement
- communication
- pre-requisites

Workshop Content

- explanation of specific tactics, techniques, procedures of the attacker scenario (theory)
- joint inject of a realistic implant with a "call home" functionality (execution: IT + security staff)
- theory: how to detect the specific (just planted) (benign) software emulating malicious behavior

- technical hunting / contextualization using "domestic" tools

- clean-up
- procedural questions for such cases (who to involve and what good practices to adhere to)

Summary

- lessons learned
- areas for improvement & recommendations
- practical considerations
- potential next steps

*no red-teaming, no stress – everything will be discussed transparently up-front

Results from an exercise can fuel future improvements

Example: White Box Attack Simulation of a Ransomware Actor

- illustrative -

Security Operations Capabilities

- ✓ **implant was detected** (when made aware to AV solution)
- ✓ implant‘s **C2 communication** is visible
- o further **telemetry log data** is available
- \- containment possible

Processes

- ✓ **incident management process** (case managent)
- • **Corporate functions** involvement process
- o **Containment** decision process
- o **Lessons learnt cycle** implemented
- \-

✓ sufficient
o partly sufficient
\- not available

Recommendations

- \+ E1: Enable EDR telemetry data acquisition / logging
- \+ E2: Create process checklist for SOC to interact with data protection office (GDPR obligations)
- o E3: Ensure visiblity / monitoring of security events
- o E4: Implement containment capabilities (with IT supplier)
- \- E5: harden Active Directory infrastructure & Trusts
- \- E6: implement Tier model for privileged access management

\+ recommended activities
o optional activities
\- strong advice

Useful Resources for Testing

Mileage May Vary

- https://www.cobaltstrike.com/
- https://caldera.mitre.org/
- https://redcanary.com/getting-started-with-atomic-red-team/
- https://securitytrails.com/blog/red-team-tools
- https://labs.bishopfox.com/industry-blog/9-red-team-tools-for-a-successful-red-teaming-engagement

Internal or External Resource Advantages

- Internal:
  - Cost
  - Institutional Knowledge
- External:
  - Broad Spectrum of Industry Verticals
  - Experience with a Range of Targeted Attacks
  - Executive Buy In

DCSO

OCTOBER 12–14

it-sa 2021

Hall 7 / Booth Number 7-312 (TeleTrust)

Questions?