SANS 504-B Incident Response Cycle: Cheat-Sheet v1.0, 11.5.2016 – kf / USCW

Preparation – Identification – Containment – Eradication – Recovery – Lessons Learned (PICERL)

Preparation

- People
- Notes
- Relationships
- Policies
- Procedures
- Coms plan
- Tools
- Mgt Tng
- Training
- Jump Bag

Identification

- Awareness
- Need to Know
- Unusual processes
- Unusual Security Evts
- Alert Early
- Use OOB Comms
- New Accts / Privs
- Primary IR Handler
- Passive monitoring
- Odd Sch Tasks
- Unusual Files
- Analyze Logs
- Chain of Custody

Containment

- Stop Bleeding
- Categorize
- Notify Mgt
- Remove LAN Cbl
- Memory Captures
- Chg Pswds
- Short-term
- Criticality
- Asgn Primary IRH
- FW/IDS Filters
- Adjacent Host Logs
- Kill Backdoors
- Back-up
- Sensitivity
- Low Profile
- ISP coord
- Patch Exploited Vuln(s)
- Long-term
- Document Actions
- Infected Vlan
- Forensic Images

Eradication

- Del Artifacts
- Apply All Patches
- Black Hole IP's
- Root Cause
- Addl FW / IDS Filters
- Seek other Host footholds
- Restore Back-up
- Chg DNS Names
- Wipe/Format/Rebuild
- Remove Malware
- Rescan network

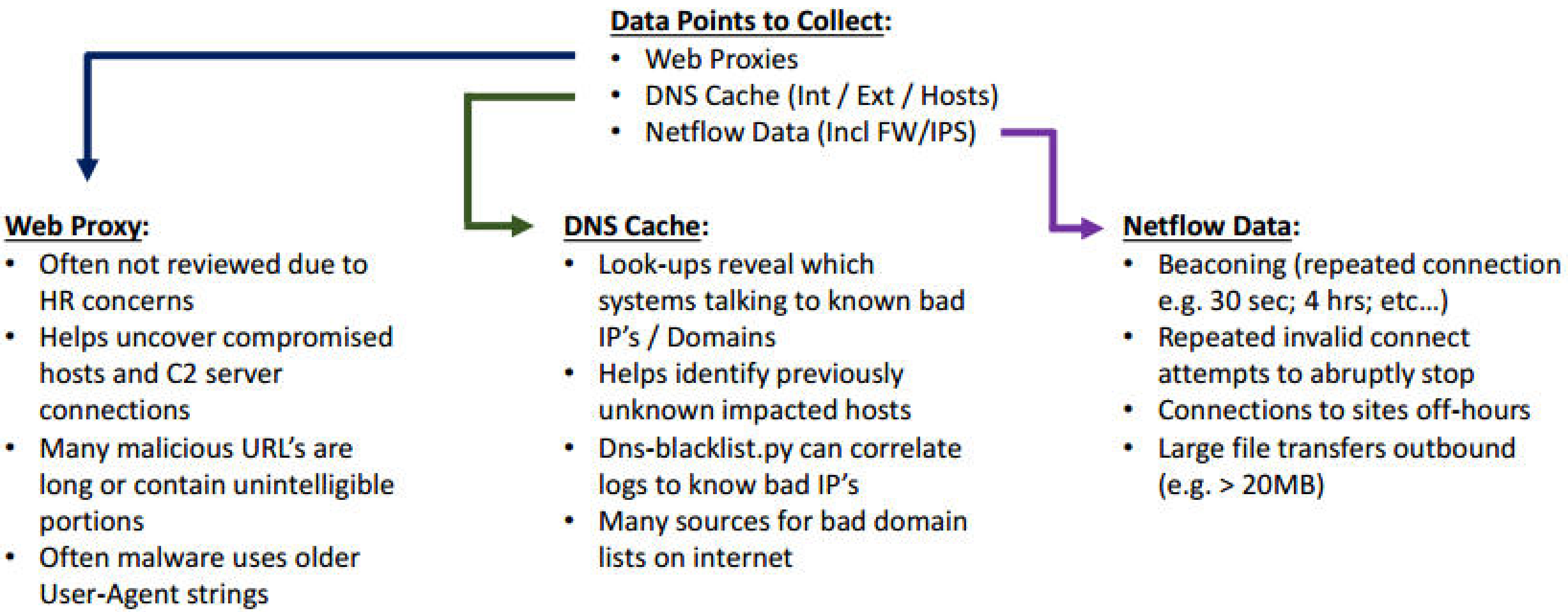
Recovery

- Return to Ops
- Test /Doc Baseline
- Move to Production (Approval)
- Monitor (signs/shells/artifacts/events)
- Script searches for attacker artifacts

Lessons Learned

- Document Incident
- Immediately upon recovery Phase
- Assign to on-Scene IRH
- All affected parties review / comment on draft
- Reach Report Consensus
- Finalize Report
- Provide Exec Summary
- Address Process not people
- Seek Required Changes
- Seek Funding
- Update Procedures

Enterprise-Wide Incident Response Considerations



Data Points to Collect:

- Web Proxies
- DNS Cache (Int / Ext / Hosts)
- Netflow Data (Incl FW/IPS)

Web Proxy:

- Often not reviewed due to HR concerns
- Helps uncover compromised hosts and C2 server connections
- Many malicious URL's are long or contain unintelligible portions
- Often malware uses older User-Agent strings

DNS Cache:

- Look-ups reveal which systems talking to known bad IP's / Domains
- Helps identify previously unknown impacted hosts
- Dns-blacklist.py can correlate logs to know bad IP's
- Many sources for bad domain lists on internet

Netflow Data:

- Beaconing (repeated connection e.g. 30 sec; 4 hrs; etc...)
- Repeated invalid connect attempts to abruptly stop
- Connections to sites off-hours
- Large file transfers outbound (e.g. > 20MB)

Tools for Enterprise IR:

- WMIC Scripting (e.g. *wmic /node@systems.txt get {values} /format:csv > output.csv*)
- SCCM Reporting (e.g. Inventory reports, drivers installed, services, etc...)
- Kansa –Powershell: (e.g. load targets into txt file, launch desired pre-canned scripts, review output)
- Cyber-CPR: Commercial Tool; Free use for limited IR Team members
- Google Rapid Response (GRR): Free; Nix/OSX/Win Clients; Python-based; Collects data from targets; central mgt