APT Tactic Revealed:
The I.O.C. Cluster-bomb

Agenda

1) Cluster-bomb explained
2) Use Cases
3) Deployment Strategies
4) Detonation Styles
5) Prevention
6) Detection
7) Follow-up
8) Summary
9) Questions

Cluster-Bomb Explained

A Cluster bomb in kinetic warfare is a canister that "opens to release a number of small fragmentation explosives over a wide area."
http://www.dictionary.com/browse/cluster-bomb

The Anthko Definition of an IOC Cluster-bomb:

A logic bomb that is spread through automated or manual mechanisms across a segment or entire network of an organization that releases indicators of compromise (IOC or I.O.C.) when detonated. The indicators can be related to actual malware or false positives.

Use Cases

The uses for deploying IOC cluster bombs (ICBs) can include the following, (not an exhaustive list):

- **Create enough false positives to change detection thresholds**
- **Hide/Obfuscate Malicious Activity (exploit native services, applications, permissions, and/or accounts)**
- **Divert Incident Response (Create higher threat IOCs than malicious activity to accomplish goal without intervention)**
- **Destroy data and/or disrupt organization**

Deployment Strategies

The ICBs can be deployed using any standard intrusion technique to include:

- **Sending logic bombs, automated malware (down loaders, zombie ware, deleters, harvesters), or ransomware through email distributions**
- **Using compromised credentials**
- **Using native technologies (macros embedded in collaboration documents, etc.)**
- **Using zero days or unpatched vulnerabilities**

Detonation Styles

The styles for detonating ICB include, (but are certainly not limited to) the following:

- **Setting off all indicators at the same time (overwhelm IR staff)**
- **Setting off all indicators in short succession (fatigue IR staff)**
- **Setting off indicators by network segmentation (mock lateral movement)**
- **Setting off indicators by device type (mock changing tactics, abilities, or threat actors)**

Prevention

Due to the wide variety of malware, attack vectors, and publicly available exploitation frameworks, prevention is very difficult but some good recommendations include:

- **Using software whitelists to prevent unauthorized software**
- **Using host intrusion prevention systems, antivirus, netflow security, and security proxies.**
- **Scan for new/unauthorized software weekly**
- **Use phishing/email security best practices**

Detection

ICB detection considerations should include the following:

- **Are there an unusually high number of alerts in a short period?**
- **Are the alerts near strategic network positions and data or trivial areas?**
  (Trivial areas may indicate attackers don't want you to look at critical areas with any level of scrutiny.)
- **Does the progression of the alerts/compromises make logical sense, is this how malware or intruders normally move/progress?**
- **Is this level of false positives normal, have any alert signatures changed or been activated or is it an unknown cause?**

Follow-up

The follow-up (in a perfect world,) would include the following:

- **Inspect log data for missing time gaps**
- **Inspect new chron jobs or windows tasks (see clean tunneling slides)**
- **Review access authorization logs for unusual activity (logging in from 2 different geological locations near simultaneously; logging into unusual enterprise resources for employee type; etc.)**
- **ATP remediation (golden ticket roll; unauthorized account creations; email auto-rules; alternate data streams; covert channel analysis)**

Summary

ATPs can use ICBs as a tactical weapon to achieve strategic goals. ICBs can be used to give IR staff a false confidence or fatigue, confuse, and/or distract IR staff for the attacker's/attackers' real movements, goals, strategies, intentions, or malicious actions. Ensure that a strategic and proactive security architecture is employed to deter, prevent, deactivate, and minimize ICBs effectiveness is critical. Once an ICB is successfully deployed after-action steps should be taken to ensure any malicious activity that attempted to be hidden/obfuscated is discovered.

Questions