Attack is easy, let's talk defence

From threat modelling to intelligence driven defence.

Teodor Cimpoesu
Technical Director
UTI-CERT, certSIGN

Cosmin Anghel
CERT Services Manager
UTI-CERT, certSIGN
@Teodor:
• 0x01 – Worked at GeCAD / RAV
• 0x02 – Moved to Kaspersky Lab for development
• 0x03 – Investigations / forensics enthusiast
• 0x04 – Linux / OSX main land
• 0x05 – Speaker at various cyber conferences / LE training
• 0x06 – Consultant and advisor on cyber security topics
• 0x0a – Building first private SOC/CSIRT at UTI Grup

@Cosmin:
• 0x01 - CERT Services Manager at certSIGN
• 0x02 - Former Cyber Threats Expert at National CyberInt Center
• 0x04 Interests in: Incident response/ Digital forensics/ Malware analysis/ Cyber investigations
Agenda

1. Attack vs. Defence
2. Structured Defence Approach
3. Defence Best Practices
4. Live Incident Response
5. Demo – GRR & Volatility
1. Attack vs. Defence
From 0-day to 1-year

- In a Symantec study*, 11 of 18 identified vulns were not known 0-days.
- Attacks with 0-days lasted b/w 19 days – 30 months, with a MED of 8 and AVG of 10 month.
- After disclosure, the variants exploiting them explode 183-85k times, and attacks increase 2-100k times
- Exploits for 42% of vulns are detected within 30 days after disclosure
- 200+ days MED, 243 days AVG, the attackers reside within a victim network before detection
- 1 in 5 (~20%) of threat actors are internal
- 75%+ of all network intrusions are due to compromised user credentials
- 84% with no admin rights
- 60% of cases attackers compromise the org within minutes
- Discovery done within days or less is below 25%
- 94% of the breaches are reported by a 3rd party

* Source: Before We Knew It - An Empirical Study of Zero-Day Attacks In The Real World, Tudor Dumitras et al., Symantec Research Labs

Sources: Microsoft Advanced Threat Analytics, HP Security, Verizon DBIR2015, ObserveIT
99.9% of the exploited vulns were compromised more than a year after the CVE was published.

Source: Verizon DBIR2015
Attack vs. Defence - detection deficit

- Cyberspace favors offense
- Shift from total security to assume compromise

A: “We only have to be lucky once. You will have to be lucky always.” (IRA,’84)

D: “There’s no way that we are going to win the cybersecurity effort on defense. We have to go on offense.” (Steven Chabinsky, former head of FBI CyberIntelligence, CRO at CrowdStrike)
Cyber threats dynamics

- Freelance hackers
- Small criminal groups
- Organized crime
- Terrorist groups
- Cyber espionage
- Nation-state cyber attacks
- Kinetic cyber-attacks
“The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position **unassailable.**”

- Sun Tzu, The Art of War, 513 BC

“Attack and defence are things differing in kind and of unequal force. Polarity is, therefore, not applicable to them”

“Everything in war is very simple but the simplest thing is difficult”

- Carl von Clausewitz, On War, 1823

“War in general is **not declared.** It simply begins with already developed military forces.”

– Georgy Isserson, New forms of combat, 1937

“Action taken to **disrupt, deny, degrade** or **destroy** information resident in a computer and/or computer network, or the computer and/or computer network itself.”

- NATO AAP-06 Edition 2014
2. Structured Defence Approach
Intelligence-driven defense

<table>
<thead>
<tr>
<th>Phase</th>
<th>Detect</th>
<th>Deny</th>
<th>Disrupt</th>
<th>Degrade</th>
<th>Deceive</th>
<th>Destroy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnaissance</td>
<td>Web analytics</td>
<td>Firewall ACL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weaponization</td>
<td>NIDS</td>
<td>NIPS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delivery</td>
<td>Vigilant user</td>
<td>Proxy filter</td>
<td>In-line AV</td>
<td>Queuing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitation</td>
<td>HIDS</td>
<td>Patch</td>
<td>DEP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Installation</td>
<td>HIDS</td>
<td>“chroot” jail</td>
<td>AV</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td>NIDS</td>
<td>Firewall ACL</td>
<td>NIPS</td>
<td>Tarpit</td>
<td>DNS redirect</td>
<td></td>
</tr>
<tr>
<td>Actions on Objectives</td>
<td>Audit log</td>
<td>Quality of Service</td>
<td>Honeypot</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”, Eric M. Hutchins et al.
# IDD - From Threat Model to Controls

<table>
<thead>
<tr>
<th>STRIDE-LM</th>
<th>Threat</th>
<th>Property</th>
<th>Definition</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>Spoofing</td>
<td>Authentication</td>
<td>Impersonating someone or something</td>
<td>Authentication Stores, Strong Authentication mechanisms</td>
</tr>
<tr>
<td>T</td>
<td>Tampering</td>
<td>Integrity / Access Controls</td>
<td>Modifying data or code</td>
<td>Crypto Hash, Digital watermark/ isolation and access checks</td>
</tr>
<tr>
<td>R</td>
<td>Repudiation</td>
<td>Non-repudiation</td>
<td>Claiming to have not performed a specific action</td>
<td>Logging infrastructure, full-packet-capture</td>
</tr>
<tr>
<td>I</td>
<td>Information Disclosure</td>
<td>Confidentiality</td>
<td>Exposing information or data to unauthorized individuals or roles</td>
<td>Encryption or Isolation</td>
</tr>
<tr>
<td>D</td>
<td>Denial of Service</td>
<td>Availability</td>
<td>Deny or degrade service</td>
<td>Redundancy, failover, QoS, Bandwidth throttle</td>
</tr>
<tr>
<td>E</td>
<td>Elevation of Privilege</td>
<td>Authorization / Least Privilege</td>
<td>Gain capabilities without proper authorization</td>
<td>RBAC, DACL, MAC; Sudo, UAC, Privileged account protections</td>
</tr>
<tr>
<td>LM</td>
<td>Lateral Movement</td>
<td>Segmentation / Least Privilege</td>
<td>Expand influence post-compromise; often dependent on Elevation of Privilege</td>
<td>Credential Hardening; Segmentation and Boundary enforcement; Host-based firewalls</td>
</tr>
</tbody>
</table>

**Threat Modeling**

**IDDIL/ATC Methodology**

**I. Discovery**
- Identify ASSETS
- Define the ATTACK SURFACE
- Decompose the SYSTEM
- Identify ATTACK VECTORS
- List THREAT ACTORS (W&W)

**II. Implementation**
- Analysis & assessment
- Triage
- Controls
Covers critical security controls (SANS / ISO27001)

OWASP
The Open Web Application Security Project

Attack Modeling

Gain Access to Building

Window

Force
Convince
Threaten
Bribe
Act like them
Wear appropriate clothing

Door

Without Key

Follow authorized individuals

With Key

Steal Key
Borrow Key

Tree source: "Design and Implementation of a Support Tool for Attack Trees", Alexander Opel
Defense Cycle – CMMI Approach

- **Plan** – what to protect, what are your assets, policies, what type of protective controls. What data sources.
- **Build** – acquire competencies, build skills specialists, acquire tools (after teams). Implement the solutions in your company.
- **Monitor** – operate the technical solutions have operational NSM/SIEM systems, perform reviews and drills (incident response exercises).
- **Detect** – check the output of monitoring systems, validate the alerts and do proactive search of IoA (indicators of attack)
- **Respond** – exercise the incident response plans; investigate, contain and remediate
- **Report** – gather information, analyze it, communicate to the right people
- **Improve** – keep the tools, procedures and processes in a maturing loop
3. Defence Best Practices
✓ Covers critical security controls (SANS / ISO27001)
✓ Features modern NGGW / NGIPS / NGTP
✓ Features ATA with sandboxing before ETD
✓ Has information security mechanisms implemented (DLP/DRM)
✓ Has central SIEM with solid TI & integrated with (automated) IR
✓ Has account activity monitoring (e.g. MS ATA, Rapid7 UserInsight)
Making TI Actionable

- Commercial Feeds
- Law Enforcement
- Hash Databases
- GEOIP Data
- Reports
- Underground Forums

- Security Event Data
- Abuse Mailbox Info
- Vulnerability Data
- Sandboxes
- Fraud Investigations

- Malware Analysis
- Honeynets
- P2P Monitoring
- DNS Monitoring
- Whatchlist Monitoring

External Feeds

Cyber Threat Intelligence Collection Research and Analysis Process

Risk Assessment Process

Risk Mitigation

Urgent Security Control Updates

IP Reputation and Vulnerability Data for filtering

Infrastructure and application logs

Threat Intelligence Reporting

Stakeholders

Proactive Surveillance
TI Frameworks / Formats

**Indicators**
- **STIX** – Structured Threat Information eXpression (MITRE/OASIS)
- **TAXII** – Trusted Automated eXchange of Indicator Information (MITRE/OASIS)
- **CYBOX** – Cyber Observable eXpression (MITRE/OASIS)
- **OpenIOC** – Open Indicators of Compromise (FireEYE/Mandiant)
- **IODEF** – Incident Object Description Exchange Format (IETF – RFC5070).
- **YARA** - Yet Another Regex Analyzer – binary pattern scanning (OSS)
- **SNORT** - real-time analysis of network traffic (CISCO).

**Enumerations**
- **MMDEF** - Malware Metadata Exchange Format (IEEE)
- **MAEC** - Malware Attribute Enumeration and Characterization (MITRE).
- **CAPEC** – Common Attack Pattern Enumeration and Classification (MITRE).
- **CVE** - Common Vulnerabilities and Exposures (MITRE)
- **CVSS** - Common Vulnerability Scoring System (NIST)
- **CPE** – Common Platform Enumeration (NIST)
- **OVAL** - Open Vulnerability and Assessment Language (MITRE)
- **OSVDB** - Open Sourced Vulnerability Database (OSF)
Threat Intel Frameworks - STIX

- **STIX** - a language for the characterization and communication of cyber threat information
  - expressive, flexible, extensible, automatable, and human-readable

- **CybOX** - convey specific instances of cyber observation (either static or dynamic) or patterns of what could potentially be observed.

Source: MITRE Org - https://stix.mitre.org
Threat Intel – IR Lifecycle with IOCs

Investigative Lifecycle:

- Initial Evidence
- Create IOCs for Host & Network
- Deploy IOCs in the Enterprise – e.g. IDS/SIEM
- Identify Additional Suspect Systems
- Collect Evidence
- Analyze Evidence
- Refine & Create new IOCs

Source: “An Introduction to OpenIOC”, Mandiant
Defense Security Metaphor

**Centered, Deep**

White moves first

Main strategic focus: the center, open fields
Objective: overwhelming attack (mate)
Asymmetric defense: obstruct
Key ability: master complexity / deep planning

**Fluid, Responsive**

Black moves first

Main strategic focus: the corners, key points
Objective: expand controlled territory
Asymmetric-game: extra steps
Key ability: understand the threat, react timely
4. Live Incident Response
IR Teams - Roles

- **Duty officer / Tier 1 Analyst** – takes care of all incoming requests. Ensure that all incidents have owners.

- **Triage officer / Tier 1 Analyst** – deals with the reported incidents, decides whether it is an incident and is to be handled, and by whom.

- **Incident handler / Tier 2 Incident Responder** – works on the incident: analyze data, create solutions, resolve the technical details and communicates about the progress to the manager and the constituents.

- **Incident handler / Tier 3 Subject Matter Expert** – advanced analyst that deals with complex cases that involve a cross-filed investigation.

- **Incident manager** – responsible for the coordination of all incident handling activities. Represents the team in communicating to the outside 3rd parties.

Source: “Ten Strategies of a World-Class Cybersecurity Operations Center” (MITRE)
- Time pressure - fast response
- Many compromised systems
- Large amounts & different kinds of data

Heterogeneous network with hundreds systems

Artifacts
Memory Dumps
HDDs images
Logs

Hacker Tim
Hacker Mike
Hacker John
IR Pressure

- What is the extent of the incident?
- Is it still active? Should we stop or follow?
- What information was exposed/exfil?
- How did the attacker(s) get in?
- How do we stop the attack and remediate?
- What is the financial/non-fin impact?
Memory Forensics Advantages

- **Best place to identify malicious software activity**
  - Study running system
  - Identify inconsistencies in system
  - Bypass packers, binary obfuscations, rootkits.
- **Analyze recent activity on the system**
  - Identify all recent activity in context
  - Profile user or attacker activities
- **Collect evidence that cannot be found anywhere else**
  - Memory-only malware
  - Chat threads
  - Internet activities

1. Identify rogue processes
2. Analyze process DLLs and handles
3. Review network artifacts
4. Look for code injections
5. Search for rootkits
6. Dump suspicious processes and drivers
<table>
<thead>
<tr>
<th>Volatility plugins</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>apihooks</td>
<td>Find API hooks</td>
<td>procexedump</td>
<td>Dump a process to an executable file sample</td>
</tr>
<tr>
<td>connections</td>
<td>Print list of open connections</td>
<td>procmemdump</td>
<td>Dump a process to an executable memory sample</td>
</tr>
<tr>
<td>dlllist</td>
<td>Print list of loaded dlls for each process</td>
<td>pslist</td>
<td>print all running processes by following the EPROCESS lists</td>
</tr>
<tr>
<td>dlldump</td>
<td>Dump a DLL from a process address space</td>
<td>orphanthread</td>
<td>Locate hidden threads</td>
</tr>
<tr>
<td>files</td>
<td>Print list of open files for each process</td>
<td>mutantscan</td>
<td>Scan for mutant objects KMUTANT</td>
</tr>
<tr>
<td>getsids</td>
<td>Print the SIDs owning each process</td>
<td>pstree</td>
<td>Print process list as a tree</td>
</tr>
<tr>
<td>malfind</td>
<td>Find hidden and injected code</td>
<td>sockets</td>
<td>Print list of open sockets</td>
</tr>
</tbody>
</table>

Complete list: https://code.google.com/p/volatility/wiki/Plugins
5. Demo

Getting a quick hint with GRR & Volatility
1. Starting point: infection alert from SIEM
2. Get access on the machine – run GRR hunt
3. GRR fundamentals
4. Getting the basics – memory dump
5. Preliminary analysis with Volatility
6. Get artifacts for IOCs
7. What next? Mandiant IOC Editor
Thank you.

Teodor.Cimpoesu@certsign.ro
+40722.754.319, @cteodor

Cosmin.Anghel@certsign.ro
+40766.514.112

Incidents: CERT@uti.ro