Thought-provoking and inspiring

EMERGENT IDEAS IN CYBER THREAT INTELLIGENCE

Michael Cloppert
Chief Research Analyst, Lockheed Martin CIRT
The George Washington University
Mo’ CTI, Mo’ Problems

- Detection
- Kill Chain Completion / IR
- Campaign Correlation
- People, Process, Technology Decisions
- CTI Organizational Operations

CTI Problem Spectrum (by abstraction)

Products

R&D
Research conducted in conjunction with The George Washington University for

Intelligence Valuation through Volatility Analysis
Review: Campaign Correlation

Consistent attributes ("key indicators") between distinct attacks define campaign
 predict properties of future attacks
 Guide investment, analysis, development

How do we measure, formally define key indicators?
 Automatic campaign correlation
 Unsupervised campaign detection

[Cloppert, Hutchins, Amin, 2011]
Current Challenges

- Inconsistent indicator identification in CKC Analysis
- Manual campaign correlation
- No standards for identifying key indicators
- Campaign definitions, attacks which correlate to them are often unclear/inconsistent
- Inconsistent language describing correlations

Subjective results provided from qualitative analytical process
So... what?

Key indicators are **consistent**

**Volatility** is a measure of **inconsistency**

Thus...

Key indicators have **low volatility**

So...

How does one measure low volatility?

Seek to establish empirical basis for indicator measurement and comparison.
General Approach

- Collect indicators from multiple intrusions
  - Intrusions grouped by campaign (supervised)
  - Intrusions not grouped (unsupervised)
- Group indicators from each into useful general categories
- Temporally order intrusions
- Measure volatility of categories over sequential intrusions
- Minimize change in volatility when grouping new intrusions
Indicator grouping

- Cyber Kill Chain™
- Diamond Model

- Each KC phase has four indicator groupings according to Diamond model
  - 1a…1d
Change & Volatility

- Indicator Change (IC): Detected change in indicator category from one intrusion to next
- Volatility: Aggregate measure of IC
Indicator Volatility Analysis

Definitions & Theory
Indicator Volatility

Indicator volatility can be easily measured

Indicators measured objectively over time, or sequence

Absolute scalar valuation of all indicators

Results dependent on only three parameters
Some types of volatility

1. Aggregate/overall volatility (completely new value)
2. Sequential volatility (different value than last observation)
3. Derivative volatility (change in value trends)

We focus on the first. Anecdotally…

Volatility is the probability of observing a completely new indicator value in a subsequent attack correlating to a given campaign.
Indicators, Formally

Indicator $I = <aid, t, val, phase, diam>$

- $aid$: Attack identifier
  - $0x01$
- $t$: Time of indicator observation
  - $1/1/2011 0000$
- $val$: Indicator value
  - $10.1.235.15$
- $phase$: CKC phase of indicator
  - $3$
- $diam$: Diamond model classifier
  - Adv Infra

All indicator values must be objectively measurable, or deterministically calculated.
Attack Definition

Set of all indicator types & corresponding values for a given attack

Attack $A = \{I_1, I_2, I_3, \ldots, I_n\}$, such that

$I_1$<aid> = $I_2$<aid> = $I_3$<aid> = \ldots = $I_n$<aid>

$n = \text{all indicator types}$

- May be NULL
- Every type has 1 and only 1 value in $A$
  - Limitation is not always true in practice
  - Can be addressed in implementation
FAIL
Indicator Volatility (IV)

IV is a measure of distinct values for a given indicator type in a set of attacks.

\[ IV_{type\{A_1 \ldots m\}} = \frac{d(type, A_1 \ldots m) - 1}{m - 1} \]

\( d(type, \{A\}) \): count of distinct values for type in \( \{A\} \)
Aggregate Indicator Volatility (AIV)

Mean IV for select indicator types, over select attacks

Or, formally:
\[ AIV = \frac{\text{IV}_{\{\text{type1..n}\}\{A_{1..m}\}}}{n} \]

For campaigns (denoted cAIV)
- AIV over \( \tau \)-most-recent attacks for all indicator types
- \( cAIV = \frac{\text{IV}_{\{<\text{all types}>\}\{A_{m-\tau..m}\}}}{\tau} \)

\[ \mu = AIV \]
Formalized Campaigns

*Using IV, we can now formalize campaigns*

A set of attacks with indicators matching in a certain number of CKC phases where cAIV is minimized

A campaign is a set of attacks $A_{1..n}$ s.t.:

- $n \geq \alpha \geq \tau$
  - $\alpha$: correlated attacks necessary for campaign designation
- For each attack $A$:
  - $A$ contains indicators matching one of $A_{i-\tau..i-1}$ in $\rho$ or more Kill Chain phases, and
  - cAIV{$A$} is minimized amongst all campaigns at that point in time

If $\tau \leq n < \alpha$, campaign may be “provisional”
Parameter Summary

Three controlling parameters defining campaigns

Must remain static

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \alpha ) (alpha)</td>
<td>Minimum number of correlated attacks needed to designate a “campaign”</td>
</tr>
<tr>
<td>( \tau ) (tau)</td>
<td>Number of previous sequential attacks in a campaign across which volatility of an indicator type is calculated</td>
</tr>
<tr>
<td>( \rho ) (rho)</td>
<td>Necessary number of CKC phases containing indicator matches for correlation to campaign to be considered</td>
</tr>
</tbody>
</table>
Correlating New Attacks

In order to correlate a new attack $A_0$

1. Identify up to $\tau$ most recent attacks for all campaigns.
   - Include provisional campaigns
2. Determine which campaigns have matching indicators in $\rho$ or more CKC phases
3. Of campaigns in 2, determine which campaigns $cAIV(\text{with } A_0) \leq cAIV(\text{without } A_0)$
4. Lowest $cAIV$ from 3 is correlation.
   - If no campaigns match 2-3, compare to attacks not in a campaign matching $\rho$ condition
Evidence of Maturity and Growth

The following indicate a readiness for greater maturity in indicator use and campaign correlation:

- Reliable Kill Chain completion for all successful & unsuccessful intrusions
- Robust indicator knowledge management
  - Including metadata
  - Including discrete intrusion association
  - Etc…
- Existence of “Analyst Cheat Sheets”
  - Lists of key indicators for each tracked campaign
- Frequent campaign association of intrusions
Products and Capabilities of a Mature CTI Organization
Evidence of Maturity and Growth

- Metrics, metrics, metrics
- Leadership in Intel Sharing Forums
- Intrusion trend forecasting
- Campaign trending & trend analysis
- Unification of CTI and IR
- Valuation & prioritization of intelligence sources
- Automated indicator vetting & use
- Balance of utilized intel between internal & external
6-level Intel Sharing Maturity Model

- **Mission Integrated**
  - Embedded
  - Integrated intel/ops feedback loop

- **Mission Partner**
  - Trailblazing
  - Acts in the interest of community

- **Producer**
  - Creating Actionable Intel
  - CND leaders, intel-driven security

- **Consumer**
  - Active Defending
  - Disciplined, analyst-driven security

- **Spectator**
  - At the Table
  - Vendor-driven security

- **Ad-Hoc**
  - Set it and Forget It
  - No formal security capabilities

Credit: E. Hutchins
Evidence: Campaign Heatmap
## Evidence: Mitigation, detection scorecard

### Incident Vector Exploit

<table>
<thead>
<tr>
<th>Incident</th>
<th>Vector</th>
<th>Exploit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Word Doc Unattrib</td>
<td>Email+doc</td>
<td>Flash</td>
</tr>
<tr>
<td>Actor 1 Web</td>
<td>HTTP</td>
<td>Various</td>
</tr>
<tr>
<td>Actor 2 Web</td>
<td>Web driveby</td>
<td>Flash</td>
</tr>
<tr>
<td>Military Unattrib</td>
<td>Email+doc</td>
<td>Word</td>
</tr>
<tr>
<td>Foreign MitMBX</td>
<td>Email+doc</td>
<td>Word</td>
</tr>
</tbody>
</table>

### Present capabilities

#### Early
- IDS/SIM Recon
- Vendor Notification
- Firewall
- Intel-based email blocks
- Email AV
- HTTP Proxy
- Sourcefire IDS
- Custom Detections
- SIM
- FPC
- Shared Intel
- Employee Report

#### Inbound Protect Delivery
- Manual Inbox Cleanup
- Desired user action
- AV/HIPS
- Architecture (Proxy, etc)
- Intel-based Proxy blocks
- Proxy Category Blocks
- DNS Mitigations
- Firewall
- Vuln Patch/Best Practice
- Restricted User Rights
- Application Patch
- Off-network Restrictions

#### Detect All Phases
- Proposed Delivery All Phases Exploit, Installation, C2
- Inapplicable
- Could have blocked
- Would not block or n/a

<table>
<thead>
<tr>
<th>Incident</th>
<th>Vector</th>
<th>Exploit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Word Doc Unattrib</td>
<td>Email+doc</td>
<td>Flash</td>
</tr>
<tr>
<td>Actor 1 Web</td>
<td>HTTP</td>
<td>Various</td>
</tr>
<tr>
<td>Actor 2 Web</td>
<td>Web driveby</td>
<td>Flash</td>
</tr>
<tr>
<td>Military Unattrib</td>
<td>Email+doc</td>
<td>Word</td>
</tr>
<tr>
<td>Foreign MitMBX</td>
<td>Email+doc</td>
<td>Word</td>
</tr>
</tbody>
</table>

### Future

<table>
<thead>
<tr>
<th>Incident</th>
<th>Vector</th>
<th>Exploit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Word Doc Unattrib</td>
<td>Email+doc</td>
<td>Flash</td>
</tr>
<tr>
<td>Actor 1 Web</td>
<td>HTTP</td>
<td>Various</td>
</tr>
<tr>
<td>Actor 2 Web</td>
<td>Web driveby</td>
<td>Flash</td>
</tr>
<tr>
<td>Military Unattrib</td>
<td>Email+doc</td>
<td>Word</td>
</tr>
<tr>
<td>Foreign MitMBX</td>
<td>Email+doc</td>
<td>Word</td>
</tr>
</tbody>
</table>

### Legend

- •: Applicable
- •: Blocked Activity
- •: Could have blocked
- •: Would not block or n/a
- •: Inapplicable
- •: n/a

---

**Note:** The table above represents a scorecard for various incidents, vectors, and exploits, categorized under different mitigation and detection techniques. Each cell highlights whether the specific mitigation or detection is applicable, blocked, or inapplicable based on the incident details provided.
Evidence: KC-linked adversary & defender success

Monthly Email Delivery Vector Mitigations
Evidence: Intel in IR process
Evidence: Intel in IR summary

Some-named Incident
Three adversaries using 0 Day Exploit

Scope
- $(b_3 + c_4)$ compromised machines
- No successful C2, exfiltration
- Response, triage and clean-up within 24 hours
Evidence: Self-generating Intel

Pedigree of Intel leading to Detections

<month>/<year>

- DBU: 90%
- RTU: 10%