Better Tools Through Intelligence, Better Intelligence Through Tools

Reid Gilman
MITRE Cyber Threat Analysis Cell

22 March 2013
MITRE Cyber Threat Analysis Cell

- MITRE is an FFRDC (not-for-profit, nothing to sell)
- Create, instrument and deploy capabilities to detect and track the actions of adversaries operating against MITRE’s unclassified computing systems.
  - Assimilate threat research
  - Identify gaps in detection capabilities
  - Create, deploy and instrument detection systems
  - Work with developers of MITRE standards (e.g., CVE, MAEC)

- **Key Principles**
  - Tradecraft
  - Data
  - Analysts
  - Tools

© 2013 The MITRE Corporation. All rights reserved.
CTAC Principles

1. Cyber Intelligence Program
   - Rich set of sources
   - Disciplined Indication and Warning process
   - Good understanding of threat actors in your sector

2. Quality Malware Analysis Program
   - Large repository of samples which extracts unique signatures
   - Works with larger malware community

3. Development team working side-by-side with operators (DevOps)

4. Incident response “baked into” defensive posture
   - Chopshop

5. Workforce culture of “cyber aware”
   - SANS Secure the Human

© 2013 The MITRE Corporation. All rights reserved.
CTAC Intelligence Tools

- **CRITs**: track adversary artifacts over time
- **ChopShop**: understand how adversaries use tools
Remote Access Tools and Intelligence

- Understand what a RAT can do by reversing it
  - Transfer files
  - Take screenshots
  - Command shell

- Understand what a RAT operator did by decoding the protocol
  - Run “net” commands
  - Search for files
  - Look around local network

- Don’t confuse actions taken by an operator with actions taken automatically by the malware!
Key Elements of Threat-Based Approach

1. Understanding of Threat Building Blocks
2. Effective Threat Sharing Model
3. Agile defensive posture aligned with threat
Threat Building Blocks – Intrusion Attempts

Intrusion Attempt

Atomic Indicator
Email
File Metadata

Domain
IP Address
From
X-Mailer
Malware
Attachments

© 2013 The MITRE Corporation. All rights reserved.
Threat Building Blocks – TTPs

TTPs

Targeting

Tools

Infrastructure

Kill Chain

© 2013 The MITRE Corporation. All rights reserved.
Threat Building Blocks - Campaigns

Campaign

Intrusion Attempt

TTP

Atomic Indicator
Email
File metadata
Targeting
Tools
Infrastructure
Kill Chain

© 2013 The MITRE Corporation. All rights reserved.
CRITs in 30 Seconds

- Cyber threat artifact database
- Pivot on threat data for rapid analysis
- Allow many users to tag data and see updates while restricting access based on releasability
- Rapid malware triage and correlation for non-reverse engineers
- One view of data for intel, malware, IDS analysts
- Leverage standard representations to facilitate sharing
Using and Sharing CRITs

- Internally developed for
  - Indicator management
  - Malware triage
  - Advanced intel analysis
  - Managing the “Sharing Problem”
  - Implementing threat sharing standards

- Not a finished product
  - MITRE does not make products, only prototypes
  - Evolving community development model
  - Moderated discussion forum with 150+ members
  - No formal support

- Non-commercial, no-fee license (Free as in beer)
  - 40+ private companies
  - Grants MITRE a license to redistribute submitted code
  - Interested? More information on that in a minute.
# CRITs Demo - Sample

## File Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>c87f8721ed800a37e8146356f9fd7b21</td>
</tr>
<tr>
<td>Filetype</td>
<td>CDF V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 936, Author: 7, Template: Normal.dot, Last Saved By: 7, Revision Number: 2, Name of Creating Application: Microsoft Office Word, Total Editing Time: 01:00, Create Time/Date: Sun Apr 3 07:50:00 2011, Last Saved Time/Date: Sun Apr 3 07:51:00 2011, Number of Pages: 1, Number of Words: 0, Number of Characters: 0, Security: 0</td>
</tr>
<tr>
<td>Mimetype</td>
<td>application/msword</td>
</tr>
<tr>
<td>Size</td>
<td>167456</td>
</tr>
<tr>
<td>Sources</td>
<td>2012-01-13 07:05:16.296000 (Fireeye) (Command line add_file.py)</td>
</tr>
<tr>
<td>MD5</td>
<td>c87f8721ed800a37e8146356f9fd7b21</td>
</tr>
<tr>
<td>SHA1</td>
<td>613618d820d729f549c57c3629a4293991e435ce</td>
</tr>
<tr>
<td>SHA256</td>
<td>cdb9734bab7e12680f840964572f93c1901e1fab2e1b6f293ce90851462d058e</td>
</tr>
<tr>
<td>SSDeep</td>
<td>1536:NcxdhkEBTMzEy+cjyivHiErQjFCwjPP7fkpZDt18IPWzWy:2VB1ij3QXbfkTD3BuzW</td>
</tr>
</tbody>
</table>
Standards-Based Repositories

External Feeds of Threat Information

OSINT
Sharing partners
Antivirus vendors

MITRE CRITs: Structured Threat DB
Where to Learn More

- **STIX Website** (whitepapers, documentation, schemas, etc.)
  - [http://stix.mitre.org](http://stix.mitre.org)
- **STIX Discussion List**
  - [http://stix.mitre.org/community/registration.html](http://stix.mitre.org/community/registration.html)
- **STIX GitHub site** (bindings, APIs, utilities)
  - [https://github.com/STIXProject](https://github.com/STIXProject)

- **TAXII Website** (whitepapers, specifications, etc.)
  - [http://taxii.mitre.org](http://taxii.mitre.org)
- **TAXII Discussion List**
  - [http://taxii.mitre.org/community/registration.html](http://taxii.mitre.org/community/registration.html)
- **TAXII GitHub site** (bindings, APIs, utilities, implementations)
  - [https://github.com/TAXIIProject](https://github.com/TAXIIProject)

- **Questions**
  - [stix@mitre.org](mailto:stix@mitre.org)
  - [taxii@mitre.org](mailto:taxii@mitre.org)
ChopShop in 30 Seconds

- Answers “What happened?”
  - Who said what?
  - Any information stolen?
  - Additional malware uploaded?
  - Any unknown C2?

- Protocol analysis/decoding framework
- Python
- Open source
  - https://github.com/MITRECND/chopshop
- Modular & extensible
ChopShop Design Goals

1. Stop reinventing the wheel
2. Modular
3. Standardize
4. Simple to use
5. Simple to write
6. Share the core
   – The secret sauce is in the modules
Command and Control Analysis

- Malware protocols change
- Protocols hide in plain sight
  - So much HTTP based malware!
- Need to understand layer 7
  - Other options: tcpdump, wireshark, vortex, commercial tools
  - All have various tradeoffs
- Process layer 7 data
  - Human readable output
  - Structured data (dns_extractor, http_extractor)
Gh0st

- Leaked source malware
- 33,400 results for “gh0st rat” on Google
- AV companies write about it a lot
- Attributed to Chinese hacking group
- Great example for this talk
  - If your malware is on wikipedia it isn’t a secret!
- The VOHO Campaign: An In Depth Analysis (RSA)
- Know Your Digital Enemy: Anatomy of a Gh0st RAT (McAfee)
- The Many Faces of Gh0st Rat (Norman ASA)
Demo Time

ChopShop

Tap

Server* (Victim Laptop)

Client* (Evil Operator)
Summary

- **CRITs: standards-based malicious artifact database**
  - Facilitate intelligence analysis across many sources
  - Reversing for non-reversers
  - Track TTPs over time

- **ChopShop: protocol decoder to answer “what happened”**
  - Layer 7 network protocol decoder
  - Open source framework, modules shared at-will
  - Determine what an adversary did with their tools

- **CRITs and ChopShop feed each other**
  - Intelligence drives tools, tools drive intelligence
More Information

- CRITs: crits@mitre.org
- ChopShop: https://github.com/MITRECND/chopshop
- TAXII:
  - http://taxii.mitre.org
  - taxii@mitre.org
- STIX:
  - http://stix.mitre.org
  - stix@mitre.org
- MITRE’s Cyber Blog
  - http://www.mitre.org/work/cybersecurity/blog.html
- Awareness: http://www.mitre.org/work/cybersecurity/training.html