THEHIVE, CORTEX & MISP
UNSHACKLING CTI AND DFIR

Saâd Kadhi
TheHive Project Leader
WHAT’S WRONG?

OBSERVATIONS
STATING THE OBVIOUS...

PREVENT

DETECT

SHARE

REACT

RECOVER

CTI
DRIVE DOWN THE TIME TO REACT

Continuous improvement

- AUTOMATION
- COLLABORATION

- FAST-PACED THREAT LANDSCAPE
- HIGH NUMBER OF SECURITY EVENTS
- TALENT SHORTAGE
- LIMITED MONEY & TIME
- COMPLEXITY

Continuous improvement
FACTS

- Threat Intelligence, Digital Forensics, Incident Response = team work
- We shall seek to drive these activities and continuously improve them
- Thanks to operational, meaningful statistics
Investigation performed, IOCs collected and proper response done

Is it time to rest? No

Some if not all IOCs should be shared

They might prove useful to peers for defending themselves

Hopefully, they will come up with complementary IOCs that were unbeknownst to us
Security Incident Response Platform (SIRP)
- Collaboration
- Task & work log
- Analysis and IOC storage
- Authentication: LDAP, Active Directory, API keys & local accounts
- Used by several cybersecurity teams throughout the world
Query analyzers through a Web UI to quickly assess the malicious nature of observables

Automate bulk observable analysis

Analyzers can be developed in any programming language that is supported by Linux

Invoke MISP expansion modules

Can be queried from MISP to enrich events
<table>
<thead>
<tr>
<th>27 ANALYZERS (AND COUNTING)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASSIVETOTAL</td>
</tr>
<tr>
<td>CIRCL PSSL</td>
</tr>
<tr>
<td>MISP SEARCH</td>
</tr>
<tr>
<td>DOMAINTOOLS</td>
</tr>
<tr>
<td>FILEINFO</td>
</tr>
<tr>
<td>OUTLOOK MSG PARSER</td>
</tr>
<tr>
<td>SPLUNK SEARCH</td>
</tr>
</tbody>
</table>
MAIN FEATURES / RECAP

▸ Import from and export to multiple MISP instances
▸ Preview alerts from multiple sources (SIEM, IDS, email...)
▸ Analyze observables through several Cortex instances
▸ Leverage statistics to drive the activity
▸ Use webhooks to open tickets in IT ticketing systems
▸ Work as a team thanks to the real-time stream
ADDITIONAL SOFTWARE

- **TheHive4Py** - Python lib to create alert/case from multiple sources
- **Splunk App** - create alerts out of Splunk. dev. by Miles Neff
- **Elastalert Hive Alerter** - use a custom Elastalert Alert to create alerts. contributed by Nclose
- **Cortex4py** - Python lib to submit observables in bulk mode through the Cortex REST API from alternative SIRP platforms & custom scripts
SHOW TIME?
# List of cases (16 of 2320)

1 filter(s) applied: status: Open

<table>
<thead>
<tr>
<th>Title</th>
<th>Severity</th>
<th>Tasks</th>
<th>Observables</th>
<th>Assignee</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>#2301 - WannaCry</td>
<td>4</td>
<td>12 Tasks</td>
<td>1145</td>
<td>AB</td>
<td>05/15/17 9:11</td>
</tr>
<tr>
<td>#2280 - [Redacted] #1700236 Anti Public Combo List</td>
<td>4</td>
<td>2 Tasks</td>
<td>0</td>
<td></td>
<td>05/11/17 11:50</td>
</tr>
<tr>
<td>#2319 - #7155 New XData ransomware</td>
<td></td>
<td>No Tasks</td>
<td>12</td>
<td></td>
<td>05/20/17 7:12</td>
</tr>
</tbody>
</table>

Merged from Case #2300 and Case #2299

Tags:
- malware_classification
- malware-category="Ransomware"
- circ-incident-classification="vulnerability"
- misp-galaxy-ransomware="WannaCry"
- misp-incident-classification="vulnerability"
- malware-type="Ransomware"
- enisa.relations-activity-abuse="ransomware"
- ont-source-type="technical report"
- arc4CrimeLabs_3666
- ont-source-type="blog post"
- wannacrypt
- admerity- settling-score-reliability="b"
- arcCERT_Bund
LIVE STREAM

#7156 OSINT - New SMB Worm Uses Seven NSA Hacking Tools. WannaCry Used Just Two
artifacts: 0
tlp: 0
caseTemplate:
description: Imported from MISP Event #7156, created at Sun May 21 09:53:45 CEST 2017
tags: ["src:CIRCL_65"]
lastSyncDate: 1495354503000
status: Updated
severity: 3
title: #7156 OSINT - New SMB Worm Uses Seven NSA Hacking Tools. WannaCry Used Just Two

#7153 Trojan
status: Ignored

#7152 Spam
status: Ignored

[MISP] #7154 HookAds Malvertising Campaign leads to RIG EK drops LatentBot and Ramnit
This case contains 2 tasks See all
This case contains 72 observables See all
description: Imported from MISP Event #7154, created at Fri May 19 17:43:47 CEST 2017
#2320 - [MISP] #7154 HookAds Malvertising Campaign leads to RIG EK drops LatentBot and Ramnit
You are about to close Case #2319. Are you sure you want to continue?

Status
- True Positive
- False Positive
- Indeterminate
- Other

There aren’t enough elements to tell that there is something malicious (original message has been deleted and not transmitted, IOC lookup with 0 hits...)

Summary

Close summary
Un mémo technique synthétisant les résultats actuels des analyses de l'attaque et fournissant des marques de compromission que vous pourrez utiliser pour faciliter la détection.
### List of observables (12 of 12)

<table>
<thead>
<tr>
<th>Type</th>
<th>Data/Filename</th>
<th>Analysis</th>
<th>Date added</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail</td>
<td><a href="mailto:bil@wonderfulday.com">bil@wonderfulday.com</a></td>
<td>No reports available</td>
<td>05/20/17 7:12</td>
</tr>
<tr>
<td></td>
<td>arcMISP-BOF</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IOCmisc</td>
<td>MISP: type = email-lst</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MISP: category = Network activity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mail</td>
<td><a href="mailto:bob@wonderfulday.com">bob@wonderfulday.com</a></td>
<td>No reports available</td>
<td>05/20/17 7:12</td>
</tr>
<tr>
<td></td>
<td>arcMISP-BOF</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IOCmisc</td>
<td>MISP: type = email-lst</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MISP: category = Network activity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mail</td>
<td><a href="mailto:trevor@wonderfulday.com">trevor@wonderfulday.com</a></td>
<td>No reports available</td>
<td>05/20/17 7:12</td>
</tr>
<tr>
<td></td>
<td>arcMISP-BOF</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IOCmisc</td>
<td>MISP: type = email-lst</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MISP: category = Network activity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mail</td>
<td><a href="mailto:bilbo@colocasia.org">bilbo@colocasia.org</a></td>
<td>No reports available</td>
<td>05/20/17 7:12</td>
</tr>
<tr>
<td></td>
<td>arcMISP-BOF</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IOCmisc</td>
<td>MISP: type = email-lst</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MISP: category = Network activity</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Observable Information**

- **TLP**: TLP:WHITE
- **Date added**: Sat, May 20th, 2017 7:09:34 +02:00
- **Is IOC**: 
- **Labels**: 
  - arch
  - backup
  - MISP type=sha256
  - MISP category=artifacts dropped
- **Description**: Not specified

**Observable Links**

Observable seen in 0 other case(s)

**Observable Analyzers**

<table>
<thead>
<tr>
<th>Analyzer</th>
<th>Cortex Server</th>
<th>Last analysis</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VirusTotal_GetReport_1_0</td>
<td>interne</td>
<td>None</td>
<td><img src="play_icon" alt="" /></td>
</tr>
<tr>
<td>PassiveTotal_Ssl_Certificate_History_1_0</td>
<td>interne</td>
<td>None</td>
<td><img src="play_icon" alt="" /></td>
</tr>
<tr>
<td>MISP_Search_1_0</td>
<td>externe</td>
<td>None</td>
<td><img src="play_icon" alt="" /></td>
</tr>
<tr>
<td>OTXQuery_1_0</td>
<td>interne</td>
<td>None</td>
<td><img src="play_icon" alt="" /></td>
</tr>
<tr>
<td>PassiveTotal_Ssl_Certificate_Details_1_0</td>
<td>interne</td>
<td>None</td>
<td><img src="play_icon" alt="" /></td>
</tr>
</tbody>
</table>
New XData ransomware

Event ID: 7155
UUID: 591f31e-8d94-4cc6-98da-76d9ae130003
Publish Date: Sat, May 20th, 2017 7:16:00
Tags: [TLP:WHITE] malware_classification malware-category="Ransomware"
# Observations View

## Summary

<table>
<thead>
<tr>
<th>Score</th>
<th>Last analysis date</th>
<th>Virus Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>45/61</td>
<td>2017-05-22 12:05:02</td>
<td>View Full Report</td>
</tr>
</tbody>
</table>

## Scans

<table>
<thead>
<tr>
<th>Scanner</th>
<th>Detected</th>
<th>Result</th>
<th>Details</th>
<th>Update</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bkav</td>
<td>✔️</td>
<td></td>
<td></td>
<td>20170522</td>
<td>1.3.6.3376</td>
</tr>
<tr>
<td>MicroWorld-Scan</td>
<td>❌</td>
<td>Gen:Variant.Razy.175324</td>
<td></td>
<td>20170522</td>
<td>12.0.250.0</td>
</tr>
<tr>
<td>nProtect</td>
<td>✔️</td>
<td></td>
<td></td>
<td>20170522</td>
<td>2017-05-22.02</td>
</tr>
<tr>
<td>CMC</td>
<td>✔️</td>
<td></td>
<td></td>
<td>20170521</td>
<td>1.1.0.977</td>
</tr>
<tr>
<td>CAT-Quick Heal</td>
<td>✔️</td>
<td></td>
<td></td>
<td>20170522</td>
<td>14.00</td>
</tr>
<tr>
<td>McAfee</td>
<td>❌</td>
<td>RDN/Generic.chra</td>
<td></td>
<td>20170522</td>
<td>6.0.6.63</td>
</tr>
<tr>
<td>Malwarebytes</td>
<td>✔️</td>
<td></td>
<td></td>
<td>20170522</td>
<td>2.1.1.1115</td>
</tr>
<tr>
<td>VIPRE</td>
<td>❌</td>
<td>Trojan.Win32.Generic.BT</td>
<td></td>
<td>20170522</td>
<td>55266</td>
</tr>
</tbody>
</table>
Analyzers

**Abuse_Finder**  Version: 1.0  Author: CERT-BDF  License: AGPL-V3

Use CERT-SG's Abuse Finder to find the abuse contact associated with domain names, URLs, IPs and email addresses

Applies to: ip, domain, url, email

**CIRCLPassiveDNS**  Version: 1.0  Author: Nils Kuhner, CERT-Bund  License: AGPL-V3

Check CIRCL's Passive DNS for a given domain or URL

Applies to: domain, url

**CIRCLPassiveSSL**  Version: 1.0  Author: Nils Kuhner, CERT-Bund  License: AGPL-V3

Check CIRCL's Passive SSL for a given IP address or a X509 certificate hash

Applies to: ip, certificate_hash, hash

**DNSDB_DomainName**  Version: 1.1  Author: CERT-BDF  License: AGPL-V3

Provide history records for a domain using DNSDB Passive DNS service

Applies to: domain

**DNSDB_IPHistory**  Version: 1.0  Author: CERT-BDF  License: AGPL-V3

Provide history records for an IP address using DNSDB Passive DNS service

Applies to: ip
```json
{
    "artifacts": [
        {
            "data": "ae0e77a37236c6ef6349a970f3756de4d32049dc",
            "attributes": {
                "dataType": "hash"
            }
        },
        {
            "data": "2e8dc58a36886e13cd61e4a25f38c9ee",
            "attributes": {
                "dataType": "hash"
            }
        },
        {
            "data": "https://www.virustotal.com/file/8b3b8fba04773b40d9639ff57755c7f96d8359b23927d0f72654f81db67167d",
            "attributes": {
                "dataType": "url"
            }
        },
        {
            "data": "8b3b8fba04773b40d9639ff57755c7f96d8359b23927d0f72654f81db67167d",
            "attributes": {
                "dataType": "hash"
            }
        },
        {
            "data": "2e8dc58a36886e13cd61e4a25f38c9ee",
            "attributes": {
                "dataType": "hash"
            }
        },
        {
            "data": "1.3.0.8876",
            "attributes": {
                "dataType": "ip"
            }
        }
    ]
}
```
USE IT
TheHive, Cortex and MISP are available under a free, open source AGPL license.

TheHive and Cortex can be installed using RPM, DEB, Docker image, binary package or built from the source code.

Linux with JRE 8+, Chrome, Firefox, IE (11), and a decent computer.

https://thehive-project.org/

https://misp-project.org/
QUESTIONS?

THEHIVE PROJECT

CORE TEAM

NABIL ADOUANI  THOMAS FRANCO  SAÂD KADHI  JÉRÔME LEONARD

CONTRIBUTORS

CERT-BDF  CERT-BUND  RÉMI POINTEL  MILES NEFF

ERIC CAPUANO  MEHDI ASCHY  ANTOINE BRODIN  GUILLAUME ROUSSE  NICK PRATLEY