THREAT INTELLIGENT ANALYSIS

@tr1ana

- Juan Garrido
- MVP Enterprise Security
- http://windowstips.wordpress.com

Agenda

Security Consultant

MVP Enterprise Security

Writer in digital and press media

Twitter: @tr1ana

Agenda

Introduction
Malware public information
TRIANA
Conclusions

Agenda

One new malware every 2 seconds
It’s like epidemic
Many variety of vectors:
- APT
- Drive by downloads
- USB
- Rootkits, Bootkits, etc...

Introduction

Many variety of technology:

- MS Office
- PDF
- Windows
- Apple based
- Mobile

Big problem when analyze a lot of samples

Introduction

- Some questions:
  - The Malware analyst have tools to perform analysis?
    - Like a sandbox, scripts, little unit tools
  - The Malware analyst have a deep know in the malware analysis art?
    - Static analysis, dynamic analysis, reversing, etc..
  - It's possible reduce the analysis time?
  - Is a sample available for analyze?

Introduction

- Is a sample available for analyze?

Hello list,

I'm looking for any samples of Zitmo, Spitmo, or Citmo you may have.

Best regards,

--

Looking for MD5 DAA758DD53EFDD12104C130F8A56313C

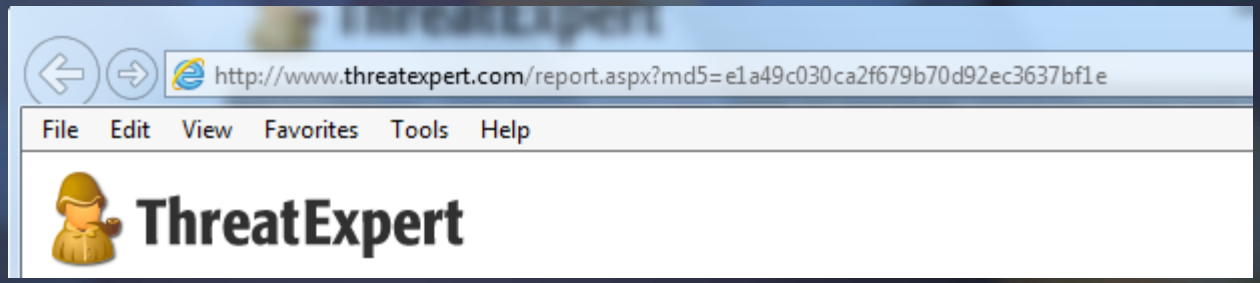
Hi All,

I'm looking for a couple of samples (IDS testing).

- Zeroaccess
- Dorkbot
- Andromeda
- Jeefo
- DirtJumper
- Pushdo
- Smoke
- Tedroo
- Lethic

Malware Public Information

- Why need MD5 instead of SHA1 or SHA256?
  - Easy: For URL based search



Retrieving file scan reports

In order to retrieve a scan report on a given file you must perform an HTTP POST request to the following URL:

https://www.virustotal.com/vtapi/v2/file/report

With the following two HTTP POST parameters:

- **resource:** a md5/sha1/sha256 hash will retrieve the most recent report on a given sample. You may also specify a *scan_id* (sha256-timestamp as returned by the file upload API) to access a specific report. You can also specify a CSV list made up of a combination of hashes and *scan_ids* (up to 4 items with the standard request rate), this allows you to perform a batch request with one single call.
- **apikey:** your API key.

Malware Public Information

```
[DNSMalware]
mhr = .malware.hash.cymru.com
sans = .md5.dshield.org
owasp = .hash.sapao.net

[Malware]
CleanMX = http://support.clean-mx.com/clean-mx/viruses.php?md5={0}
ThreatExpert = http://www.threatexpert.com/report.aspx?md5={0}&xml=1
ShadowServer = http://innocuous.shadowserver.org/api/?query={0}
MalwareControl = http://www.malware-control.com/statics-pages/{0}.php
VirusTotal = https://www.virustotal.com/vtapi/v2/file/report
MalcOde = http://malcOde.com/database/index.php?search={0}
Malekal = http://malwaredb.malekal.com/index.php?hash={0}
ssdsandbox = http://xml.ssdsandbox.net/index.php/{0}
xandora = http://www.xandora.net/xangui/malware/view/{0}
malwr = https://malwr.com/
malwaretrackerdoc = http://www.malwaretracker.com/docapirep.php?hash={0}&type=json
malwaretrackerpdf = http://www.malwaretracker.com/pdfapirep.php?hash={0}&type=json
vxvault = http://vxvault.siri-urz.net/ViriList.php?MD5={0}
sarvam = http://sarvam.ece.ucsb.edu/info/{0}.json
```

DEMO

Malware based search

WHERE IS MY SAMPLE

- In many cases:
  - The sample is located in public site
  - The sample is located in hacking site
  - The sample is located in Web Access tool (Like VT, Malwr, etc…)
  - The sample is located in a public repository

WHERE IS MY SAMPLE

- IP, Host, Domain:
  - Useful for discover new samples
    - Whois
    - Domain Lookup
    - Etc…
  - Useful for discover APT Threats, Malware located by country, etc…

WHERE IS MY SAMPLE

```
[DomainReputation]
abuse = http://www.abuse.ch/zeustracker/blocklist.php?download=domainblocklist
nothink = http://www.nothink.org/blacklist/blacklist_malware_dns.txt
malhost = https://secure.mayhemiclabs.com/malhosts/malhosts.txt
spyeye = https://spyeyetracker.abuse.ch/blocklist.php?download=domainblocklist
malwaredomains = http://mirror1.malwaredomains.com/files/BOOT
malwaredomainlist = http://www.malwaredomainlist.com/hostslist/hosts.txt
malwarecom = http://www.malware.com.br/cgi/submit?action=list
malwarepatrol = http://www.malwarepatrol.net/cgi/submit?action=list
JoxeanKoret = http://malwareurls.joxeankoret.com/normal.txt

[IpReputation]
AlienVault = https://reputation.alienvault.com/reputation.generic
NoThink = http://www.nothink.org/blacklist/blacklist_malware_http.txt
ciarmy = http://www.ciarmy.com/list/ci-badguys.txt
emergingthreat = http://rules.emergingthreats.net/blockrules/rbn-malvertisers-ips.txt
MalwarePatrol = http://malware.com.br/cgi/submit?action=list_dguard
martinciber = http://intel.martincyber.com/ip/
MalwareGroup = http://www.malwaregroup.com/ipaddresses
sri = http://www.mtc.sri.com/live_data/attackers/
blocklist = http://www.blocklist.de/lists/all.txt
rabidmonkey = http://rabidmonkey.org/ips.txt
rbn = http://rules.emergingthreats.net/blockrules/rbn-malvertisers-ips.txt
ZeusTracker = https://zeustracker.abuse.ch/blocklist.php?download=ipblocklist
SpyEye = https://spyeyetracker.abuse.ch/blocklist.php?download=ipblocklist
Palevo = http://amada.abuse.ch/palevotracker.php
badguys = http://www.ciarmy.com/list/ci-badguys.txt
blackip = http://blackip.ustc.edu.cn/byip.txt
JoxeanKoret = http://malwareurls.joxeankoret.com/normal.txt
```

DEMO

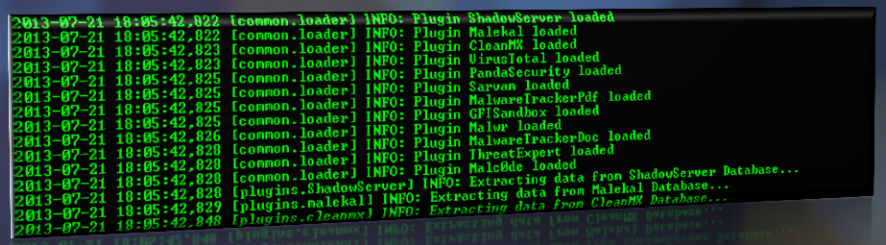
Malware sample search

TRIANA

- Python based script:
  - Perform HASH and File Hash search
  - Many public information reference
  - Ability to download the sample if found it
  - Many sources →One JSON source
  - DOCX Report

TRIANA

- IP & Domain collector:
  - Check in IP and Domain reputation lists
- Plugin based:
  - VirusTotal plugin
  - Malwr plugin
  - ThreatExpert plugin
  - Etc, etc…



TRIANA

```
#-------------------------------------------------------------------------------
# Name:         ExampleClass
# Purpose:      Example Class
# Author:       Juan Garrido (A.K.A silverhack)
# Created:      22/04/2013
# Copyright (C) 2013 Threat Intelligent Analysis.
# This file is part of TRIANA http://www.innotecsystem.com
# See the file 'docs/LICENSE' for copying permission.
#-------------------------------------------------------------------------------
import sys,os
import logging

log = logging.getLogger()

class Example:
    def __init__(self):
        self.legend = "Example Class for Triana"
        self.genreport = dict()
    def run(self):
        log.info(self.legend)
        try:
            self.genreport["status"] = True
            self.genreport["example_malwarefound"] = "http://urlmalware.com"
            self.genreport["example_analysis"] = "FOO"
            self.genreport["example_peinfo"] = "BAR"
            return self.genreport
        except Exception as error:
            self.genreport["status"] = False
            log.error(error)
            return self.genreport
    def __del(self):
        pass
```

CONCLUSIONS

- It’s possible reduce time in malware analysis
  - Automate unit test
  - Automate malware analysis
  - Automate static analysis
  - Automated search based malware
- It’s useful to attach like annex
  - JSON results
  - DOCX report
- It’s useful to search malware
  - Many public information sites
  - Different public sandbox perform different analysis
  - Many public repositories

THANKS ;)

Juan Garrido

Juan_garrido@innotecsystem.com

http://www.innotecsystem.com