Trap a Spam-Bot
for fun and profit

Attila Marosi
Senior Threat Researcher
OSCE, OSCP, ECSA, CEH

DEEPSEC

SOPHOS

About the needs

DEEPSEC

- As a security product which works mostly by patters, collecting patterns (samples) in a right way is fundamental
  - SPAM patterns
  - malware patters
  - behaviors patters
  - network patterns
- So we need good and up-to-date patters
  - it must be “clear” to avoid false-positives
  - we get 300.000 new sample each day
    - but we do not have information about the samples

SPAMs

how serious is

DEEPSEC

SOPHOS

SPAM and malwares

- most of the malware are deliver by infected machines
  - malwares produce SPAM
  - SPAM produce malwares
  - they are hand in hand
    - we don’t ignore the SPAM
    - it is not just annoying, it is harmful

SPAM and malwares

- we may dived the SPAMs in two
  - SPAMs
    - quite annoying, mostly related with scams and frauds
      - advertising something you should buy (Viagra)
      - pump-and-dump, which is a form of microcap stock fraud
  - SPAMs with malwares
    - there is no need to explain
    - the target is to pawn the system

Honeypots

DEEPSEC

SOPHOS

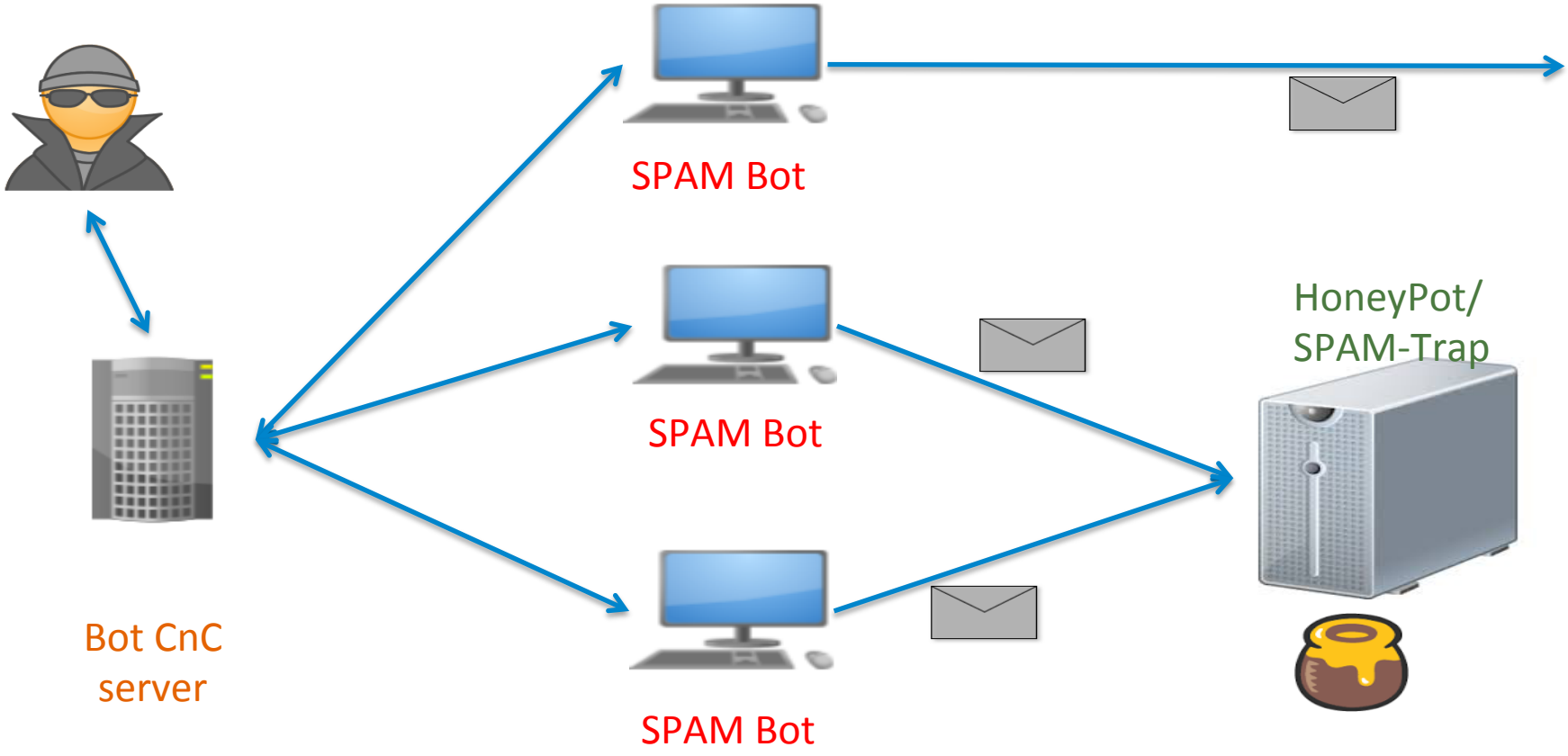
Honeypots

- honeypot systems are very important for IT security
  - collect information about offensive actors on the network
  - collecting new version of spam messages
  - collecting new exploits which are actively used in the wild
- levels of interaction
  - high-interaction honeypots
    - very close to real systems
  - low-interaction honeypots
    - mostly service emulation not system emulation
    - SMTP / POP3 / FTP … etc.
  - I used a combination of both (VPs + INetSIM)

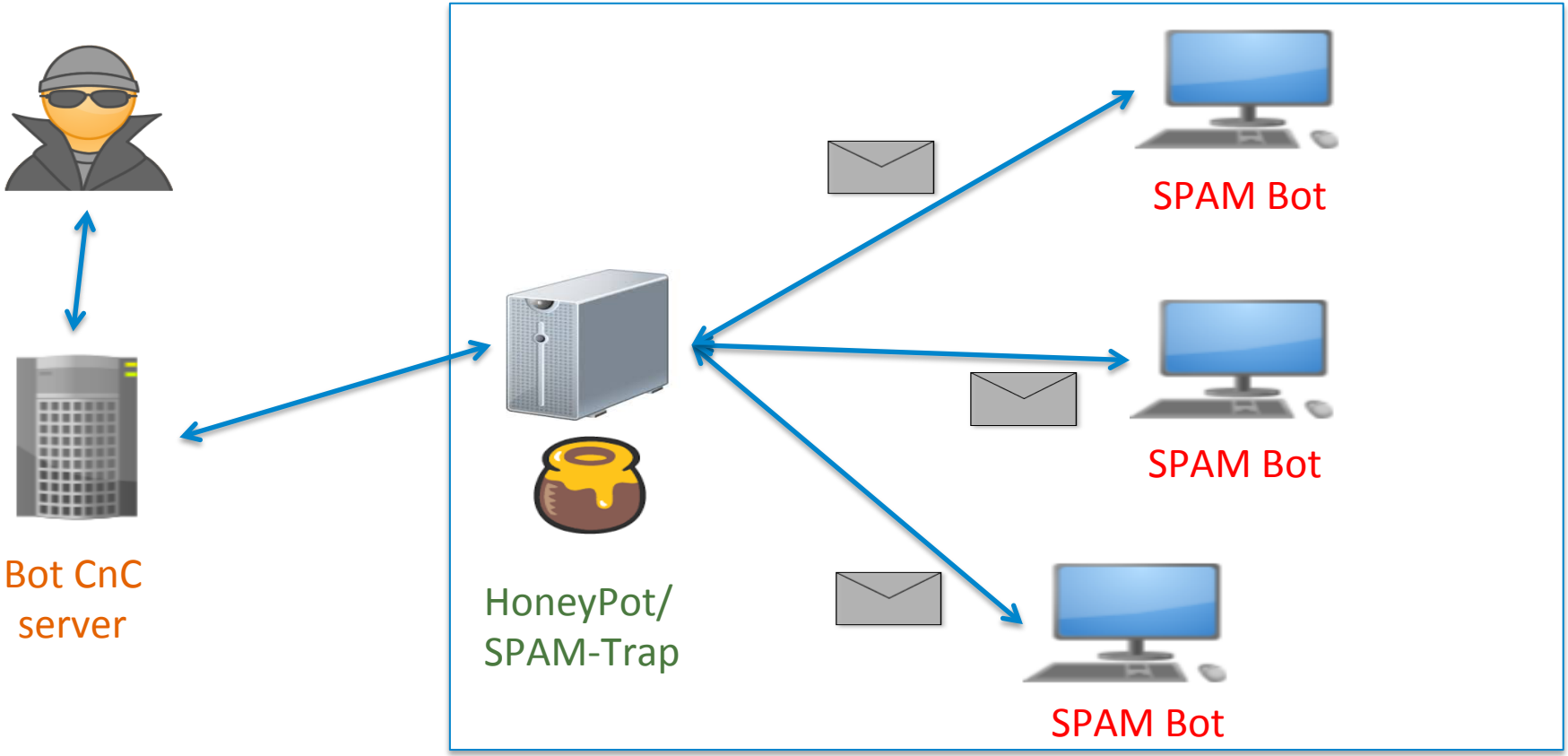
SPAM traps

- collecting SPAMs from different sources
  - SPAMs feeds could be
    - abandoned (but valid) email addresses
    - fake servers which pretend that they are badly configured (relay server)

SPAM traps



Bot-Breeder ☺



My questions

- I wanted to measure who many spams could be delivered by only one infected machine?
- How frequently the Spams are changed?
- How frequently malicious attachments are changed?
- How old are a malware variant when we get it from other sources (VirusTotal, other vendors, other traps..)?
- I focused to the malwares more than the “simple” SPAMs

The Trap

how to breed a malware

DEEPSEC

SOPHOS

Requirements – knowledge

DEEPSEC

- You should know your malware (how it behaves) ☹
  - to prevent that it is threatening the world
  - emulate / block all malicious and unwanted connection but
  - allow all the 'feeding' ways to be informed by the bad guys
- Dofoil SPAM-bot
  - it uses the 9997 port to be contacted with the CnC and get the new commands
  - it turns the infected machines in to a gateway by SOCKS proxy – that is the "data" channel

Requirements – knowledge

DEEPSEC

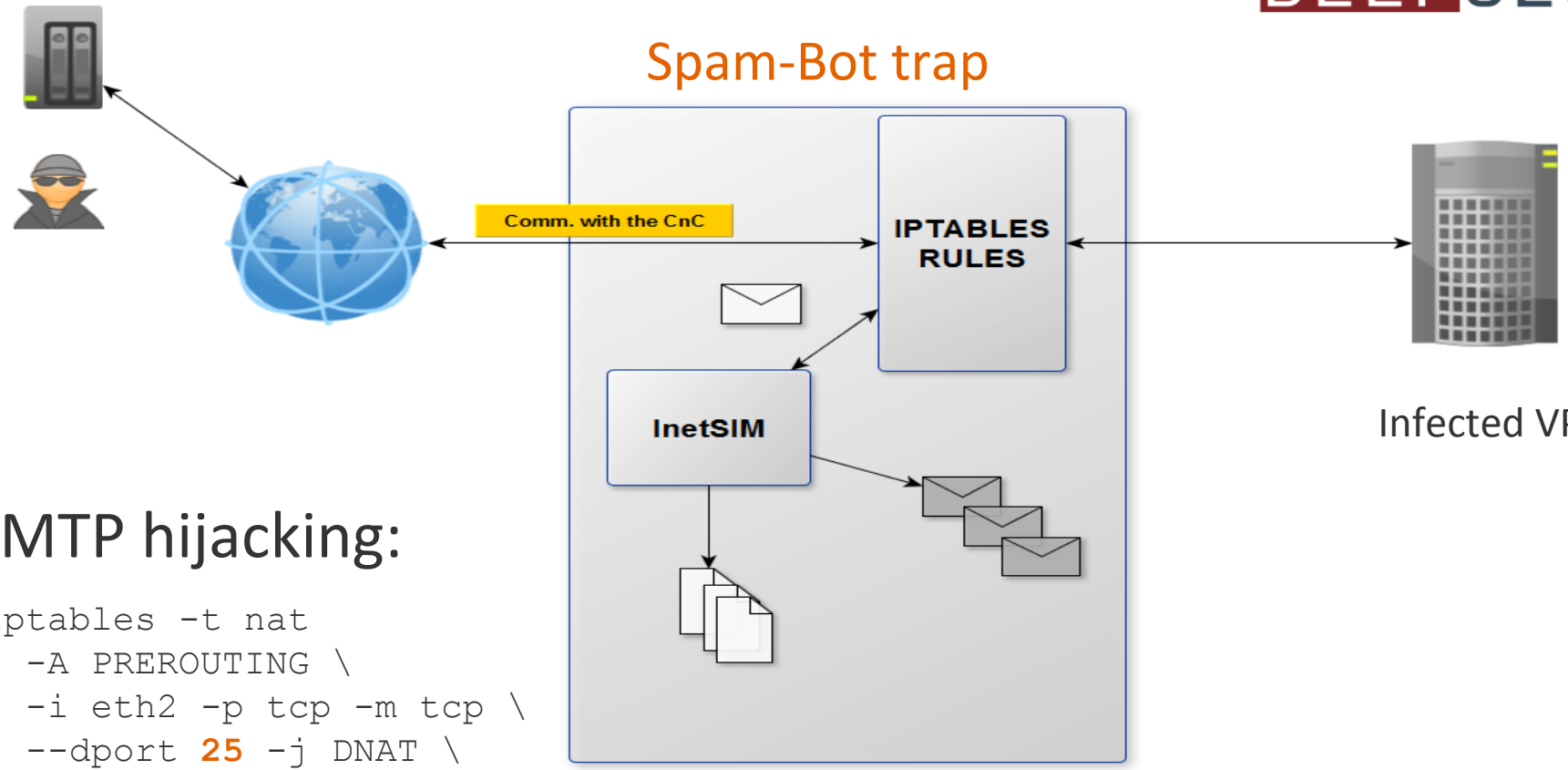
- problematic ☺ malwares
  - e.g.: Pushdo/Cutwail
    - it can use multiple ways to be contacted with the bad guys (HTTP, encrypted TCP connection…etc.)
    - mostly, it is controlled by infected sites (hidden HTML comments on the source code)
      - who can you select that
        - one query may about to download the new SPAM version ☺
        - another may exploit a site which is vulnerable ☹

Requirements – tools

DEEPSEC

- Tools
  - Virtual or real system to infect them
  - INetSIM
    - HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, DNS, FTP/FTPS, TFTP,IRC, NTP...
  - IPTABLES
  - some python scripts to parse the raw email message and extract the message attachment
  - Kibana + Logstash + Elasticsearch

Spam-Bot trap



SMTP hijacking:

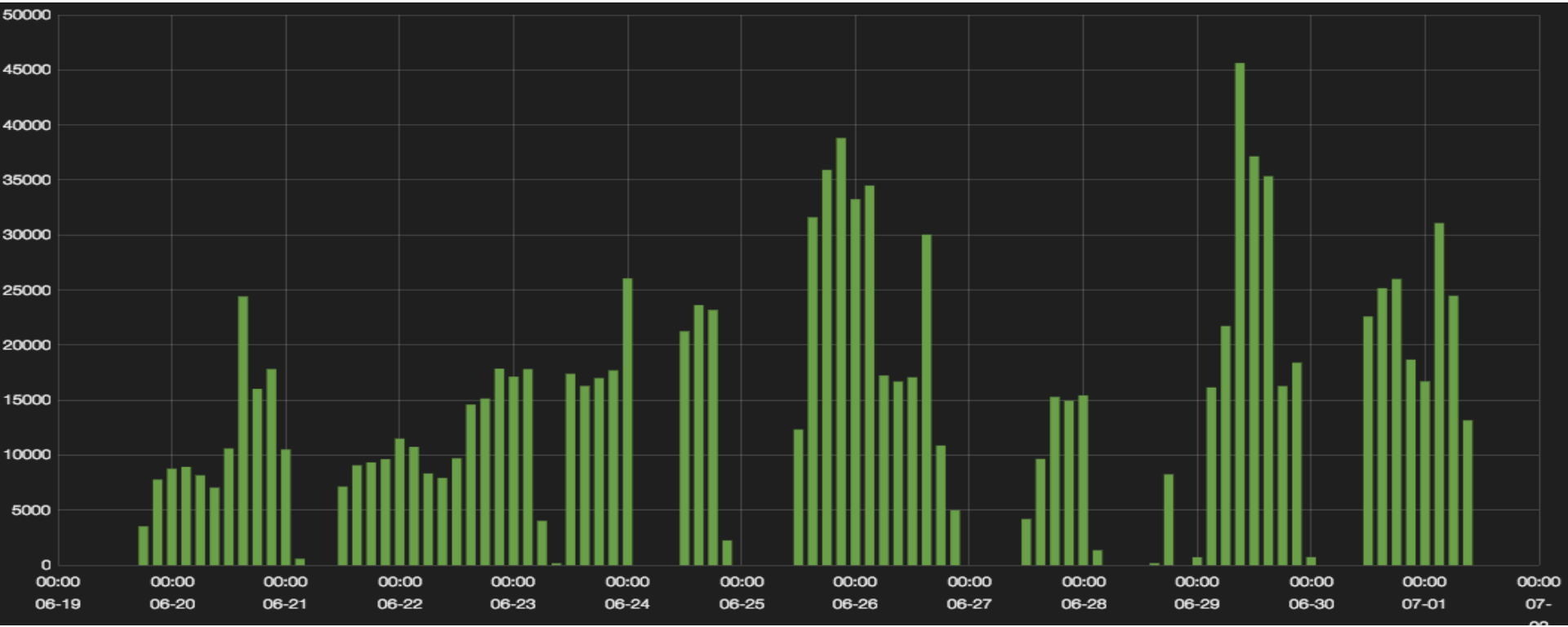
```
iptables -t nat
  -A PREROUTING \
  -i eth2 -p tcp -m tcp \
  --dport 25 -j DNAT \
  --to-destination 127.0.0.1:25
```

The Results

DEEPSEC

SOPHOS

Intercepted emails



Overall results

DEEPSEC

- the first sample was this:
  - 29dec18b8821b4966c0b2d373bc6f694610bee76
- we started to breed this at Jun 19th 2014
- and finished it at Jul 1st 2014
  (less than 2 weeks)
- intercepted 1.181.370 unique SPAM mails
- 239.441 SPAM mails had malicious attachment

Subjects of the SPAM messages

DEEPSEC

- **SPAMs without malwares (~940.000):**
  - Pharmacy online 35% discount
- **SPAMs with malwares (~239.000):**
  - Order Details
  - Order details {radom}
  - Order report
  - Your Amazon.co.uk order {radom}
  - Your order {radom}

Email addresses

- 7.646.686 email addresses was targeted (RCPT TO)
  - 6.931.017 unique addresses

1.379.549	yahoo.com
1.074.008	hotmail.com
790.432	aol.com
784.352	earthlink.net
530.562	gmail.com
92.792	msn.com
88.663	hotmail.co.uk
66.731	sbcglobal.net
64.908	btinternet.com
49.946	live.com

Unique domains:
108.878

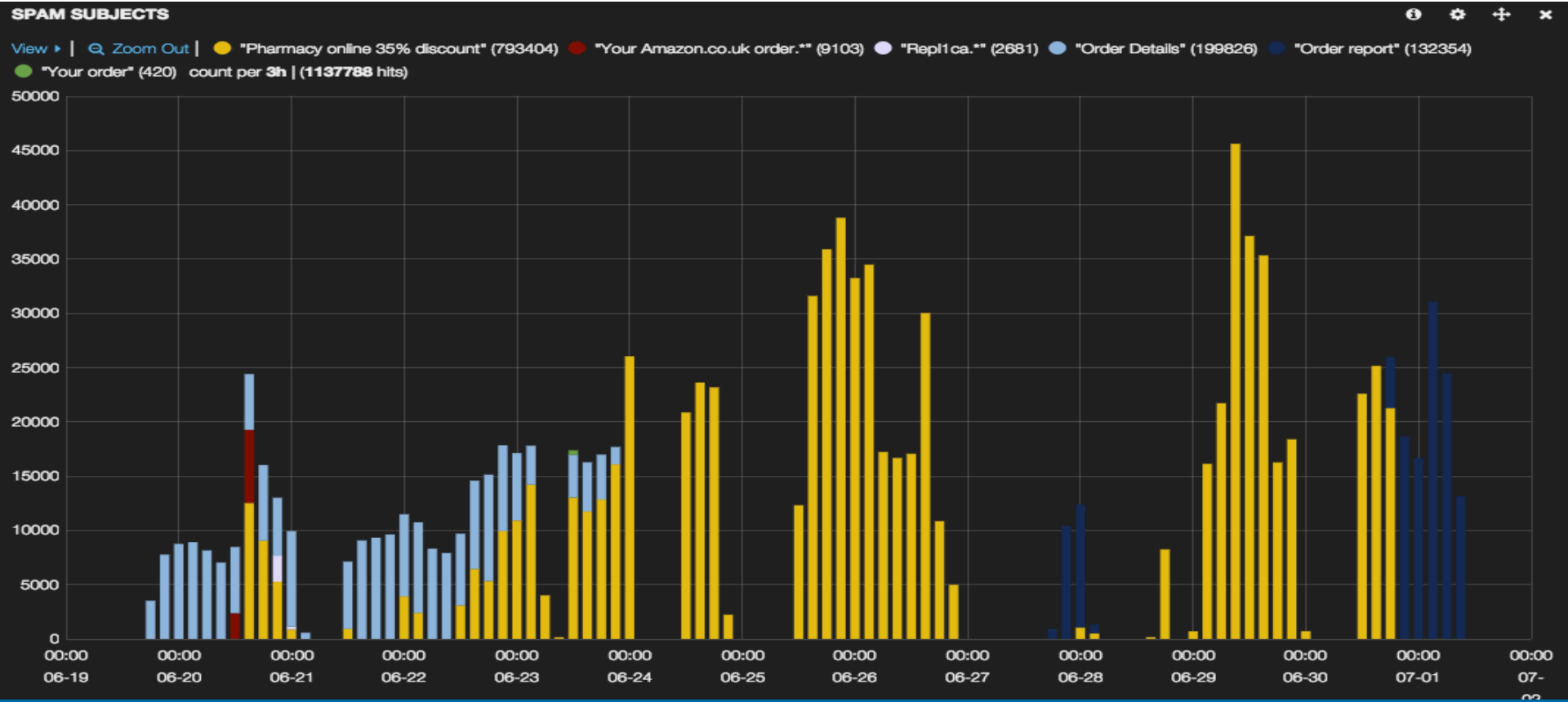
The Results

spams without attachment

DEEPSEC

SOPHOS

SPAM subjects



URLs in SPAM

DEEPSEC

http://t.co/**ZYehtz8qh7**

(HTTP 301 Moved Permanently)

3771 unique Twitter URL shorter

http://www.xxxxxxx.com.tr/**lost100.html**

58 – maybe infected – sites

```
<META HTTP-EQUIV="Refresh" CONTENT="0;
      URL=http://xfxomedics.com">
```

1 final destination

Intermediate sites

DEEPSEC

- There were 58 intermediate sites
  - on 30 of them the 100lost.html is still exist and work
  - all of them are very abandoned
    - out of updates
    - old configuration
    - rarely visited
    - so they are the perfect helper of bad guys

The Results

spams with attachment

DEEPSEC

SOPHOS

Malicious attachments

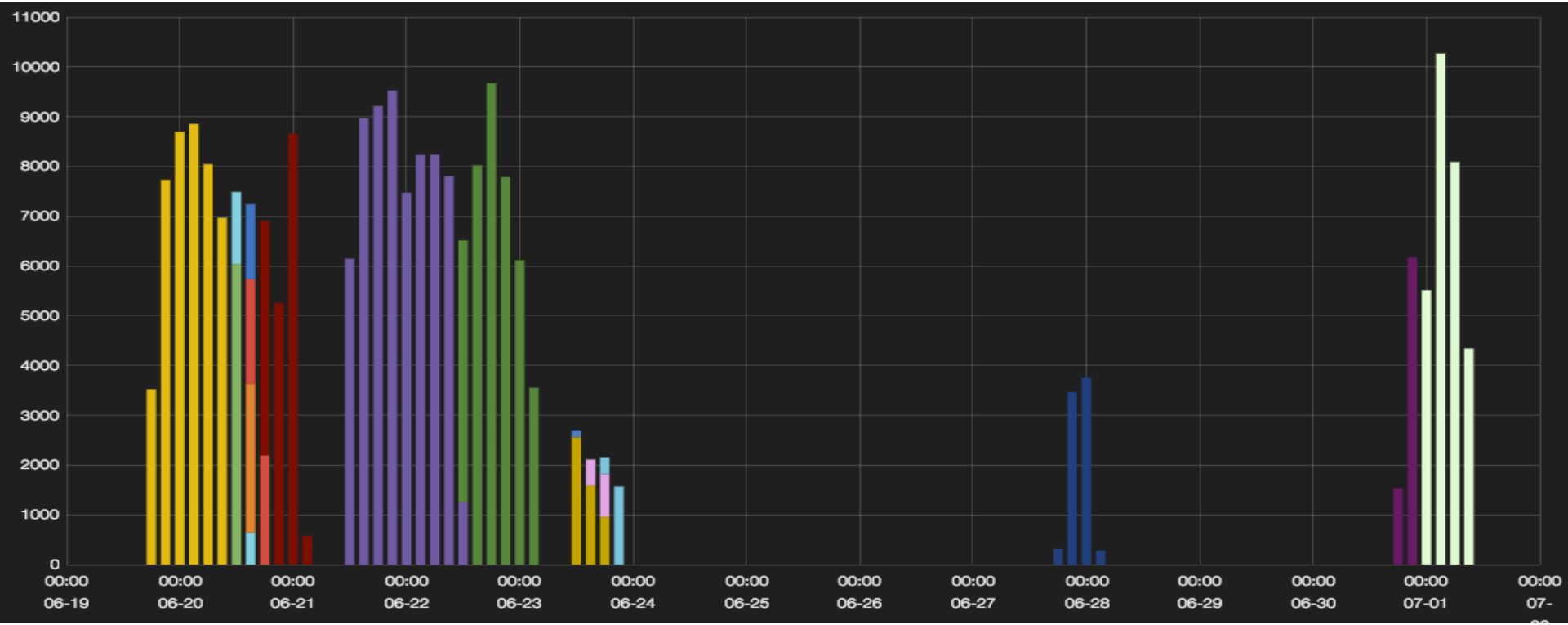
DEEPSEC

16 unique ZIP hashes	13 unique content (EXE) hashes
296ac679...	75e05f9b662724d385836751e3c35593c3bd4930
b53d9cca...	1d035c4e40f8754f019aa77687ad1163baa311f7
7a2f188f...	6400c7aa5ec1ea2546092c078e6eee30c1c5e7ba
5a1279ec...	6400c7aa5ec1ea2546092c078e6eee30c1c5e7ba
31fd8515...	0c825b4838f7476795ec97b37f6057d0749c31e3
8efe1893...	0c825b4838f7476795ec97b37f6057d0749c31e3
1fdd5704...	1535768fe3d4cbea2658206ed60ade8da41d2adc
2144b7f2...	7f99c30fc2a67e269b454b7f487ff84b21a7e806
854dbb22...	f1c072b41995371fc2ca93d8624c047a7199ca33
4dfaa645...	9d8280915f415b077fbeddddae2a7c0eca0589cb
143c451f...	9d8280915f415b077fbeddddae2a7c0eca0589cb
667a7d4a...	3c6e0032cc30466a6677ffdcb594b2481e28478f
6a7b879f...	717c394044d88d089fc8e4a76fcea5053eceb519
89bd6bc0...	4671f749ae11a9e246ad98032cd34352c0fcae89
2bfc873d...	c4e9e806089ae8504b99ae897722de43f23079a1
cd5cdd98...	5c0740cfc4ec97a7feb9f70f757ac152286df020

Malicious attachments (EXE file name)

EXE hashes	File names
75e05f9b...	order_id_report_89378973489578943758934.exe
1d035c4e...	order_id_report_89378973489578943758934.exe
6400c7aa...	**ORDER_AA1745643985.exe**
6400c7aa...	**order_id_report_89378973489578943758934.exe**
0c825b48...	**order_id_8239748923748923789423794823798.exe**
0c825b48...	**Order_AJ5344556781.exe**
1535768f...	order_id.exe
7f99c30f...	order_id_72389478923748923749823749823.exe
f1c072b4...	order_id_72389478923748923749823749823l.exe
9d828091...	**order_id_723894789237489237498237498231 23.exe**
9d828091...	**order_id_72389478923.exe**
3c6e0032…	order_id_23642368744234234236378.exe
717c3940...	order_id_32748923789472389472389479283.exe
4671f749...	order_id_78362478236784236784623875111 1.exe
c4e9e806...	order_id_783624782367842367846238751111 1.exe
5c0740cf...	order_id_78362478236784236784623875111 1.exe

Malicious attachments



Malicious attachments

DEEPSEC

Hashes	Count	First Seen	Last Seen	Duration
296ac679...	43823	14.06.19 17:26	14.06.20 10:14	16:48
b53d9cca...	6046	**14.06.20 10:14**	**14.06.20 12:57**	02:42
7a2f188f...	2078	**14.06.20 12:13**	**14.06.20 14:41**	02:28
5a1279ec...	2994	**14.06.20 13:07**	**14.06.20 14:28**	01:21
31fd8515...	4300	**14.06.20 14:30**	**14.06.20 16:48**	02:18
8efe1893...	1506	**14.06.20 14:41**	**14.06.20 15:10**	00:29
1fdd5704...	19196	**14.06.20 16:48**	14.06.21 10:24	17:35
2144b7f2...	**66850**	**14.06.21 10:24**	**14.06.22 10:26**	**24:01**
854dbb22...	40414	14.06.22 11:01	14.06.23 02:25	15:24

At 20th Jun there were 6 new hashes and 4 new EXE hashes

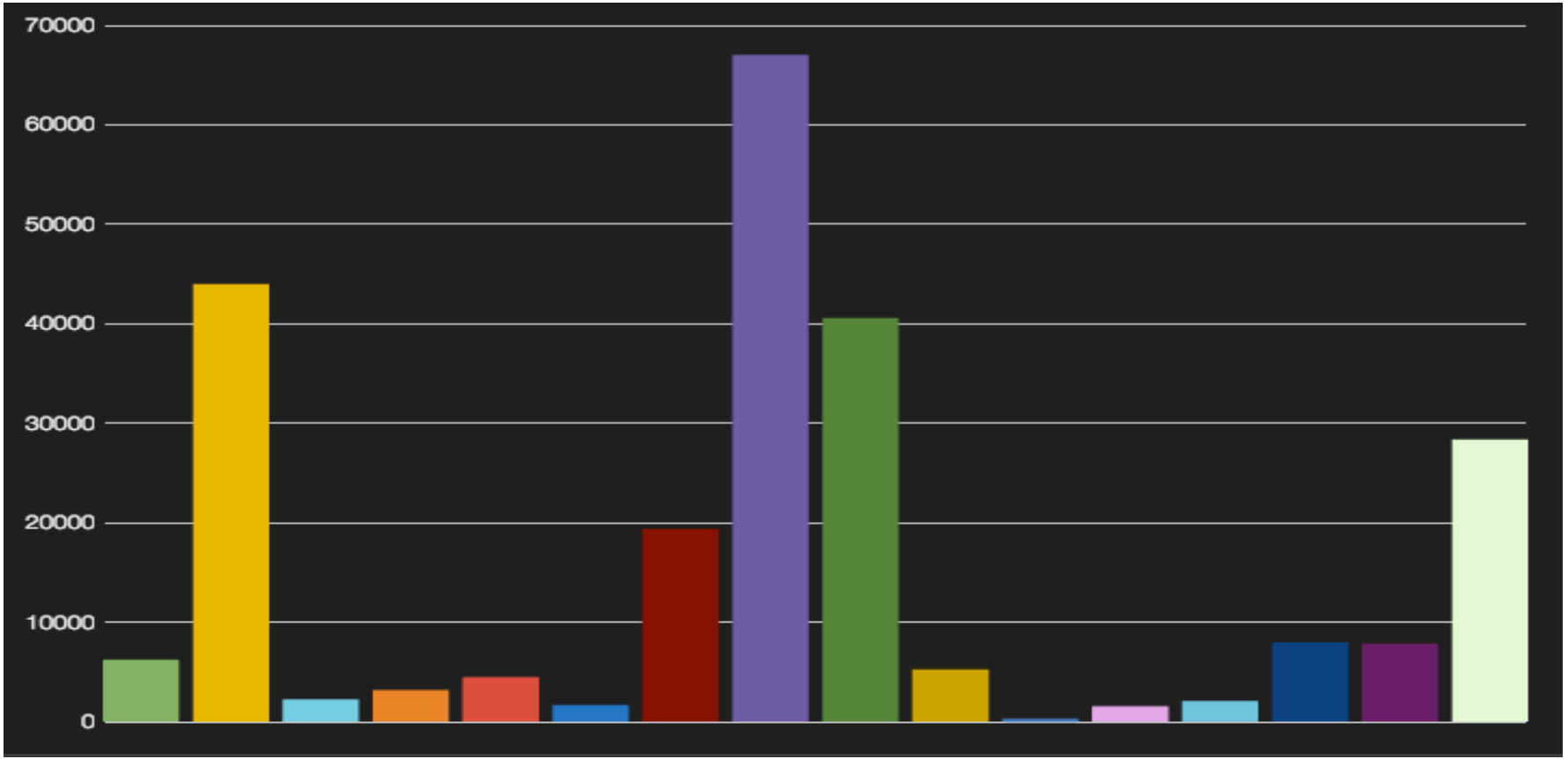
Malicious attachments

DEEPSEC

Hashes	Count	First Seen	Last Seen	Duration
4dfaa645...	5101	**14.06.23 10:12**	**14.06.23 18:47**	08:34
143c451f...	138	**14.06.23 11:42**	**14.06.23 11:50**	00:08
667a7d4a...	1386	**14.06.23 14:57**	**14.06.23 17:07**	02:09
6a7b879f...	1908	**14.06.23 17:27**	**14.06.23 20:38**	03:11
89bd6bc0...	7811	14.06.27 18:50	14.06.28 15:58	21:08
2bfc873d...	7709	14.06.30 18:04	14.06.30 23:24	05:19
cd5cdd98...	28212	14.06.30 23:24	14.07.01 08:34	09:09

At 23th Jun there were 4 new hashes and 3 new EXE hashes

Malicious attachments



Malicious attachments – clusters

Hashes	Count	First Seen	Last Seen	Duration
296ac679...	43823	14.06.19 17:26	14.06.20 10:14	16:48
b53d9cca...	6046	14.06.20 10:14	14.06.20 12:57	02:42
7a2f188f...	2078	14.06.20 12:13	14.06.20 14:41	02:28
5a1279ec...	2994	14.06.20 13:07	14.06.20 14:28	01:21
31fd8515...	4300	14.06.20 14:30	14.06.20 16:48	02:18
8efe1893...	1506	14.06.20 14:41	14.06.20 15:10	00:29
1fdd5704...	19196	14.06.20 16:48	14.06.21 10:24	17:35
2144b7f2...	66850	14.06.21 10:24	14.06.22 10:26	24:01
854dbb22...	40414	14.06.22 11:01	14.06.23 02:25	15:24

Malicious attachments – clusters

Hashes	Count	First Seen	Last Seen	Duration
4dfaa645...	5101	14.06.23 10:12	14.06.23 18:47	08:34
143c451f...	138	14.06.23 11:42	14.06.23 11:50	00:08
667a7d4a...	1386	14.06.23 14:57	14.06.23 17:07	02:09
6a7b879f...	1908	14.06.23 17:27	14.06.23 20:38	03:11
89bd6bc0...	7811	14.06.27 18:50	14.06.28 15:58	21:08
c4e9e806...	7709	14.06.30 18:04	14.06.30 23:24	05:19
cd5cdd98...	28212	14.06.30 23:24	14.07.01 08:34	09:09

Attachments – VirusTotal time delta

ZIP Hashes	Count	First Seen	Used	VT FSeen	Delta
296ac679…	43823	14.06.19 17:26	16:48	14.06.19 21:04	3:38
b53d9cca…	6046	14.06.20 10:14	2:42	14.06.20 20:39	10:24
1fdd5704…	19196	14.06.20 16:48	17:35	14.06.20 17:51	1:02
2144b7f2…	66850	14.06.21 10:24	24:01	14.06.21 19:48	9:23
854dbb22…	40414	14.06.22 11:01	15:24	14.06.22 15:10	4:08
4dfaa645…	5101	14.06.23 10:12	8:34	14.06.24 08:15	22:03
667a7d4a…	1386	14.06.23 14:57	2:09	14.06.23 20:57	6:00
6a7b879f…	1908	14.06.23 17:27	3:11	14.06.23 19:46	2:19
2bfc873d…	7709	14.06.30 18:04	5:19	14.06.30 18:33	0:28
cd5cdd98…	28212	14.06.30 23:24	9:09	14.07.01 19:11	19:47

The campaign had already finished when VirusTotal got the files.

Attachments – the rest of it

ZIP Hashes	Count	First Seen	Used	VT FSeen	Delta
7a2f188f…	2078	14.06.20 12:13	2:28	14.11.19 15:29	3651:16
5a1279ec…	2994	14.06.20 13:07	1:21	14.11.19 15:31	3650:23
31fd8515…	4300	14.06.20 14:30	2:18	14.08.19 07:29	1432:59
8efe1893…	1506	14.06.20 14:41	0:29	14.11.19 15:32	3648:51
143c451f…	138	14.06.23 11:42	0:08	14.11.19 15:34	3579:51
89bd6bc0…	7811	14.06.27 18:50	21:08	14.06.27 18:40	----

There was a technical issue (storage was full) and the trap was down.

Malicious attachments

DEEPSEC

Overall:

- 16 unique files (zip)
- 13 unique malwares (exe),
- 4 different types of it (4 clusters)
- In average, each version of malware were sent 14.967 times

- average spreading duration: **8:10**
  - how frequently the malware changed
  - after this time, the malware is not used anymore

Conclusion

DEEPSEC

SOPHOS

Conclusion

DEEPSEC

- Pro
  - if you have a trap like this you would be able to monitoring the SPAM activities
  - if the bad guys release a new version of SPAMs or malware we get it immediately
  - you would be sure about your new sample is malicious (because of the source)
  - would be able to check that your detection is still working with the newest variant – if not rise and alert
- Cons
  - it requires big effort to run infected bots in your infrastructure
  - a malware could be use by many actors (group of bad guys) and in this concept you need to “subscribe” all of them to get all the “feeds”

Future research & development

DEEPSEC

- Create a system which could run alone
  - without initial information about the behavior of the malware
  - without information about that which way is used by the bad guys to feed the bots with new variants and samples

References

- **INetSIM** - http://www.inetsim.org/
- **Logstash** - http://logstash.net/
- **Kibana** - http://www.elasticsearch.org/overview/kibana/
- **Elasticsearch** - http://www.elasticsearch.org/

Questions?

SOPHOS

attila.marosi@sophos.com

attila.marosi@gmail.com

PGP ID: 3782A65A
PGP FP.:
4D49 1447 A4E1 F016 F833
8700 8853 60A7 3782 A65A

DEEPSEC