Identifying Infections with Spamming Malware in a Network, based on Analysis of DNS MX Requests

Bas Vlaszaty
Bas.Vlaszaty@os3.nl

Universiteit van Amsterdam

July 2014

Acknowledgement

Research conducted at Quarantainenet BV, supervised by Casper Joost Eyckelhof

Outline

- Introduction
- Research Question
- Background
  - DNS MX
- Dataset
- Approach
  - Theory
  - Analysis tools
- Results
  - Frequency
  - Periodicity
  - Entropy
  - Flow
- Conclusion

Introduction

Spam:

Introduction

Spam:

"Unsolicited means that the Recipient has not granted verifiable permission for the message to be sent. Bulk means that the message is sent as part of a larger collection of messages, all having substantively identical content."
- Spamhaus

Introduction(2)

Spam worldwide problem

- Global email: 150-200 billion per day

Sources: Symantec and Radicati Group

Introduction(2)

Spam worldwide problem

- Global email: 150-200 billion per day
- Almost 2/3 is spam

Sources: Symantec and Radicati Group

Introduction(2)

Spam worldwide problem

- Global email: 150-200 billion per day
- Almost 2/3 is spam
- Most spam blocked by spamfilters

Sources: Symantec and Radicati Group

Introduction(2)

Spam worldwide problem

- Global email: 150-200 billion per day
- Almost 2/3 is spam
- Most spam blocked by spamfilters
- Average business user receives 85 emails a day, 10 are spam.

Sources: Symantec and Radicati Group

Introduction(3)

- 80% generated by botnet (Symantec)

Introduction(3)

- 80% generated by botnet (Symantec)
- Network of infected computers

Introduction(3)

- 80% generated by botnet (Symantec)
- Network of infected computers
- Owner controlled

Introduction(3)

- 80% generated by botnet (Symantec)
- Network of infected computers
- Owner controlled
- Sold as a service

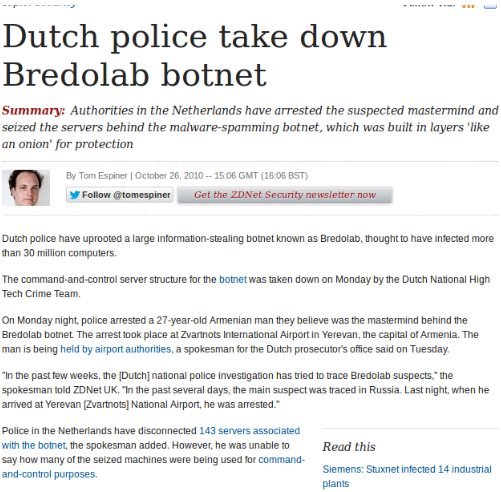
Introduction(3)

- 80% generated by botnet (Symantec)
- Network of infected computers
- Owner controlled
- Sold as a service
- Used for DDoS, Clickfraud, spam

Introduction(3)

- 80% generated by botnet (Symantec)
- Network of infected computers
- Owner controlled
- Sold as a service
- Used for DDoS, Clickfraud, spam
- Reputation loss, costs for bandwidth, energy

Introduction(4)



Topic: Security Follow via:

Dutch police take down Bredolab botnet

***Summary:** Authorities in the Netherlands have arrested the suspected mastermind and seized the servers behind the malware-spamming botnet, which was built in layers 'like an onion' for protection*

By Tom Espiner | October 26, 2010 -- 15:06 GMT (16:06 BST)

Dutch police have uprooted a large information-stealing botnet known as Bredolab, thought to have infected more than 30 million computers.

The command-and-control server structure for the botnet was taken down on Monday by the Dutch National High Tech Crime Team.

On Monday night, police arrested a 27-year-old Armenian man they believe was the mastermind behind the Bredolab botnet. The arrest took place at Zvartnots International Airport in Yerevan, the capital of Armenia. The man is being held by airport authorities, a spokesman for the Dutch prosecutor's office said on Tuesday.

"In the past few weeks, the [Dutch] national police investigation has tried to trace Bredolab suspects," the spokesman told ZDNet UK. "In the past several days, the main suspect was traced in Russia. Last night, when he arrived at Yerevan [Zvartnots] National Airport, he was arrested."

Police in the Netherlands have disconnected 143 servers associated with the botnet, the spokesman added. However, he was unable to say how many of the seized machines were being used for command-and-control purposes.

Read this

Siemens: Stuxnet infected 14 industrial plants

Introduction(5)

What to do?

- Prevention

Introduction(5)

What to do?

- Prevention
- Network monitoring

Introduction(5)

What to do?

- Prevention
- Network monitoring
- Quarantainenet

Introduction(5)

What to do?

- Prevention
- Network monitoring
- Quarantainenet
- Different sensors

Introduction(5)

What to do?

- Prevention
- Network monitoring
- Quarantainenet
- Different sensors
- Accumulate score

Introduction(5)

What to do?

- Prevention
- Network monitoring
- Quarantainenet
- Different sensors
- Accumulate score
- Restrict network acces, put machine in quarantaine

Research question

Research question

`Is it possible to identify a machine that is in infected with spamming malware by analysing DNS MX requests?`

DNS

- Domain Name System

DNS

- Domain Name System
- Links domain name (google.com) to ip address (74.125.136.138)

DNS

- Domain Name System
- Links domain name (google.com) to ip address (74.125.136.138)
- Comparable to De Telefoongids, you can look up a person and you will get back the phone number belonging to the person.

DNS MX

- MX requests are specific for mail address

DNS MX

- MX requests are specific for mail address
- Which server to deliver mail to

DNS MX

- MX requests are specific for mail address
- Which server to deliver mail to
- Compare to the Gouden Gids, which will return an address so you know where to send your mail to.

Dataset

Data from 3 different institutes. Clients of Quarantainenet.

Dataset

Data from 3 different institutes. Clients of Quarantainenet.

- Dataset A, 3028 log entries
- Dataset B, 67.386 log entries
- Dataset C, 1.975.765 log entries

Dataset

Data from 3 different institutes. Clients of Quarantainenet.

- Dataset A, 3028 log entries
- Dataset B, 67.386 log entries
- Dataset C, 1.975.765 log entries

During a period of 2 weeks all DNS MX requests were captured, timestamped and logged.

Dataset

Data from 3 different institutes. Clients of Quarantainenet.

- Dataset A, 3028 log entries
- Dataset B, 67.386 log entries
- Dataset C, 1.975.765 log entries

During a period of 2 weeks all DNS MX requests were captured, timestamped and logged.

Structure: [Timestamp, source ip, requested domain]

Verification data

No truth to check findings:

Verification data

No truth to check findings:

- Incident log from Qmanage

Verification data

No truth to check findings:

- Incident log from Qmanage
- Spam blacklists (dnsbl.sorbs.net, cbl.abuseat.org, bl.spamcop.net, zen.spamhaus.org)

Verification data

No truth to check findings:

- Incident log from Qmanage
- Spam blacklists (dnsbl.sorbs.net, cbl.abuseat.org, bl.spamcop.net, zen.spamhaus.org)
- Reports of issues by customers

Hypotheses

Dataset not annotated. Had to start from hypotheses.

Hypotheses

Dataset not annotated. Had to start from hypotheses.

- Spambot will generate a lot of DNS MX requests as it sends a lot of mail.

Hypotheses

Dataset not annotated. Had to start from hypotheses.

- Spambot will generate a lot of DNS MX requests as it sends a lot of mail.
- Spambot is an automatic process, so it will show (at least somewhat) periodic behaviour.

Hypotheses

Dataset not annotated. Had to start from hypotheses.

- Spambot will generate a lot of DNS MX requests as it sends a lot of mail.
- Spambot is an automatic process, so it will show (at least somewhat) periodic behaviour.
- Spambot infection is a malware infection so it should correlate with incidents from other sensors.

Hypotheses

Dataset not annotated. Had to start from hypotheses.

- Spambot will generate a lot of DNS MX requests as it sends a lot of mail.
- Spambot is an automatic process, so it will show (at least somewhat) periodic behaviour.
- Spambot infection is a malware infection so it should correlate with incidents from other sensors.

Hypotheses

Dataset not annotated. Had to start from hypotheses.

- Spambot will generate a lot of DNS MX requests as it sends a lot of mail.
- Spambot is an automatic process, so it will show (at least somewhat) periodic behaviour.
- Spambot infection is a malware infection so it should correlate with incidents from other sensors.

Create tools to analyse this

Hypotheses

Dataset not annotated. Had to start from hypotheses.

- Spambot will generate a lot of DNS MX requests as it sends a lot of mail.
- Spambot is an automatic process, so it will show (at least somewhat) periodic behaviour.
- Spambot infection is a malware infection so it should correlate with incidents from other sensors.

Create tools to analyse this
Try to match findings with these tools to verification data
(Incidents, reports, spam blocklists)

Frequency analysis

- From records in a logfile to graphs.

Frequency analysis

- From records in a logfile to graphs.
- Create histogram over time.

Frequency analysis

- From records in a logfile to graphs.
- Create histogram over time.
- Count how many records are in the logfile between time A and B, between B and C etc..

Frequency analysis

- From records in a logfile to graphs.
- Create histogram over time.
- Count how many records are in the logfile between time A and B, between B and C etc..
- This results in activity plots

Frequency graph

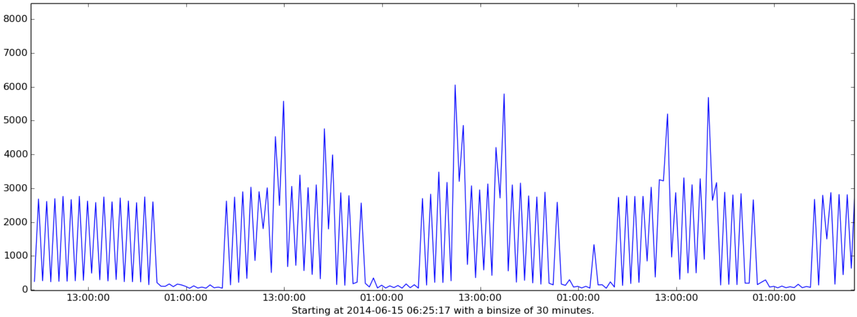


Figure: Daily pattern

Periodicity

- Find repeating pattern in data

Periodicity

- Find repeating pattern in data
- Autocorrelation: Cross correlating with itself shifted by lag.

Periodicity

- Find repeating pattern in data
- Autocorrelation: Cross correlating with itself shifted by lag.
- Similarity of $f(x)$ with $f(x+t)$, where t is called the "lag"

Periodicity example

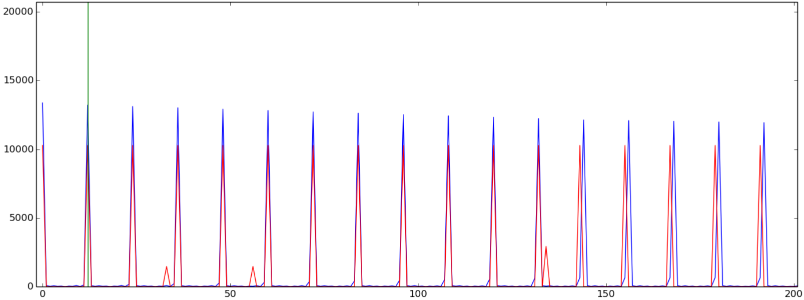


Figure: Autocorrelation good result

Entropy analysis

- Paper ”Entropy Based Analysis of DNS Query Traffic in the Campus Network”

Entropy analysis

- Paper ”Entropy Based Analysis of DNS Query Traffic in the Campus Network”
- Entropy will go down when spam run is in progress

Entropy analysis

- Paper ”Entropy Based Analysis of DNS Query Traffic in the Campus Network”
- Entropy will go down when spam run is in progress
- Based on Shannon entropy, given by:

Entropy analysis

- Paper ”Entropy Based Analysis of DNS Query Traffic in the Campus Network”
- Entropy will go down when spam run is in progress
- Based on Shannon entropy, given by:
- $H(X) = -\sum_{x} p(x) \log p(x).$

Entropy analysis

- Paper ”Entropy Based Analysis of DNS Query Traffic in the Campus Network”
- Entropy will go down when spam run is in progress
- Based on Shannon entropy, given by:
- $H(X) = -\sum_{x} p(x) \log p(x).$
- Higher entropy means the data is more random.

Flow analysis

- Idea based on "Detection of Spam Hosts and Spam Bots Using Network Flow Traffic Modeling"

Flow analysis

- Idea based on "Detection of Spam Hosts and Spam Bots Using Network Flow Traffic Modeling"
- Flow is a session of activity.

Flow analysis

- Idea based on "Detection of Spam Hosts and Spam Bots Using Network Flow Traffic Modeling"
- Flow is a session of activity.
- Requests have to be close together to belong to the same flow

Flow analysis

- Idea based on ”Detection of Spam Hosts and Spam Bots Using Network Flow Traffic Modeling”
- Flow is a session of activity.
- Requests have to be close together to belong to the same flow
- $dt = 1$ minute

Flow analysis

- Idea based on "Detection of Spam Hosts and Spam Bots Using Network Flow Traffic Modeling"
- Flow is a session of activity.
- Requests have to be close together to belong to the same flow
- $dt = 1$ minute
- If there is more then 1 minute of "silence", the current flow ends and a new one will be started at the next activity

Results

Results

Truth very limited:

Results

Truth very limited:

- Customer reports?

Results

Truth very limited:

- Customer reports?
- Spam databases?

Results

Truth very limited:

- Customer reports?
- Spam databases?
- Correlation with incident logs?

Frequency result A

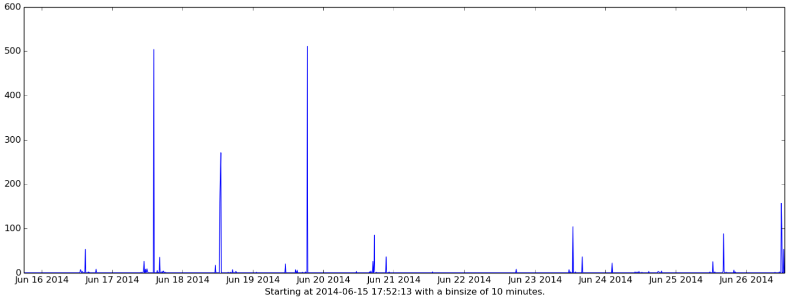


Figure: Frequency result A

Frequency result B

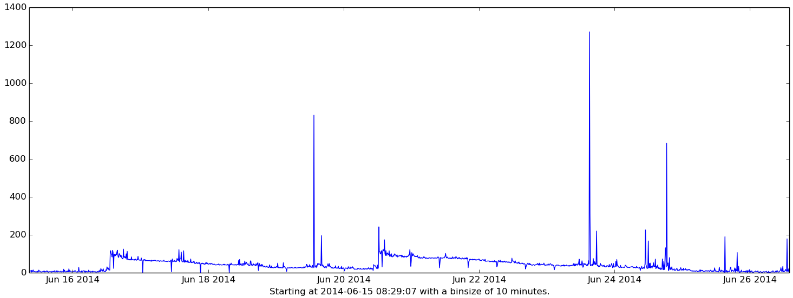


Figure: Frequency result B

Frequency result C

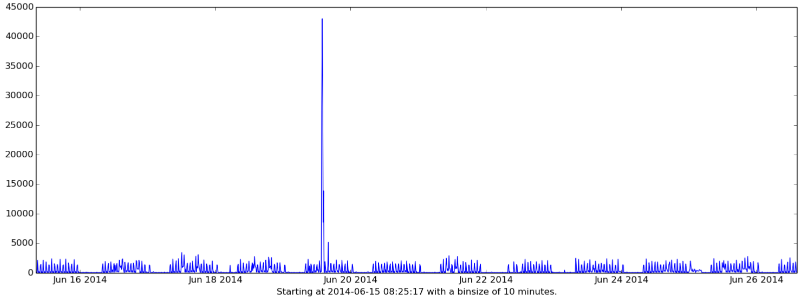


Figure: Frequency result C

Frequency spamrun ip

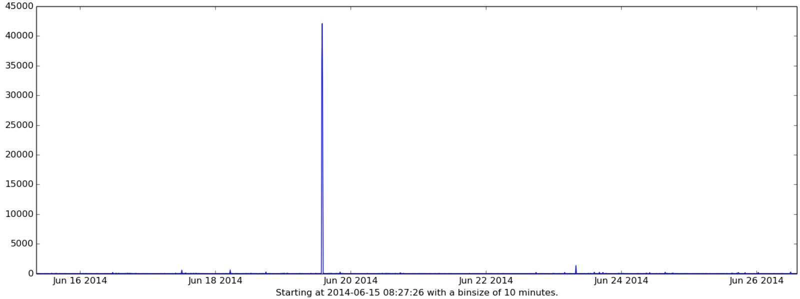


Figure: Frequency spamrun ip

Periodicity result

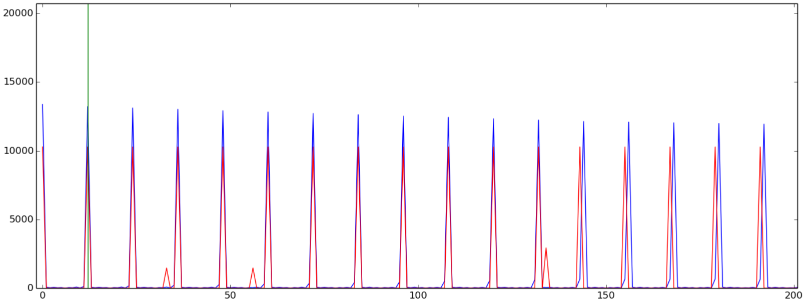


Figure: Periodicity Good example

Periodicity result

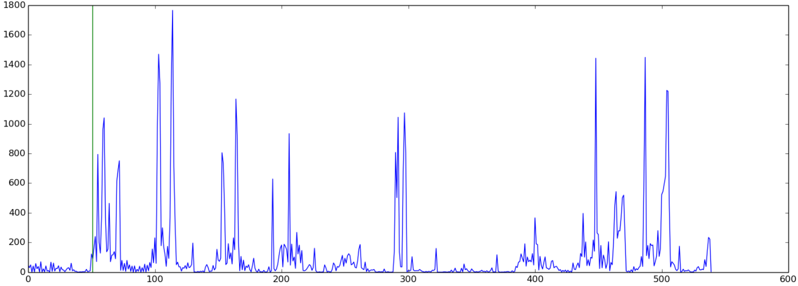


Figure: Periodicity Bad example

Entropy A

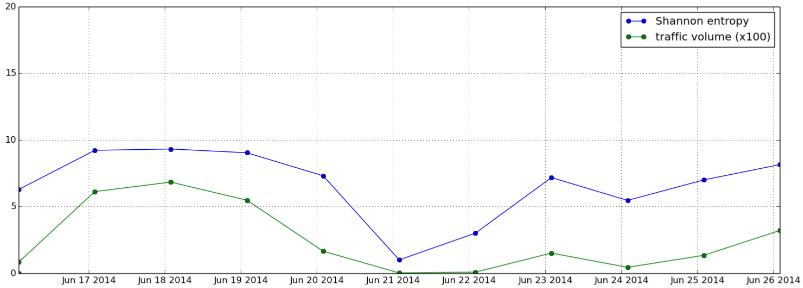


Figure: Entropy A

Entropy B

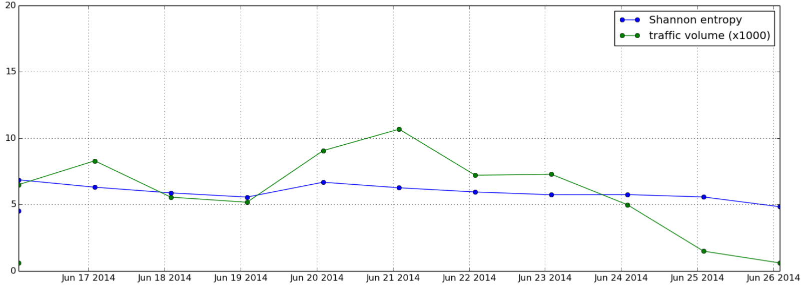


Figure: Entropy B

Entropy C

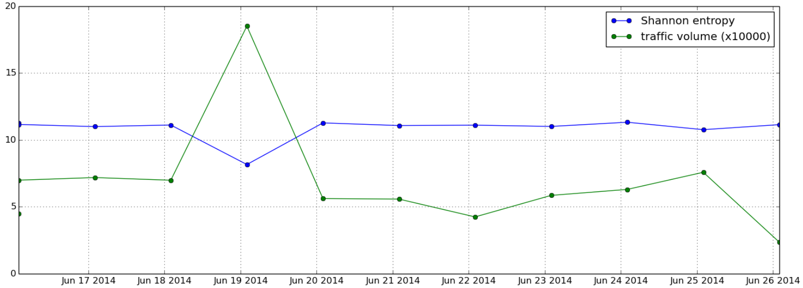


Figure: Entropy C

Results flow analysis

Dataset	# records	# Flows	Flows >10	Ratio
Set A	308	108	27	0.25
Set B	67.386	3356	1305	0.39
Set C	1.975.765	12240	2474	0.20

Table: Number of flows

Results from flow analysis C

Host	# Duration	Volume	Rate (req/s)
B	1456	**100983**	**69.36**
B	311	1376	4.42
A	509	**21920**	**43.06**
C	5083	3054	0.60
C	4242	2466	0.58
C	4857	2815	0.58
C	2387	1198	0.50
C	4689	3414	0.73
C	3844	2193	0.57
C	1172	2946	2.51
C	3853	2184	0.57
C	2258	1021	0.45

Conclusion

Conclusions on analysis methods

- Frequency analysis: identified spam session does show up in frequency.

Conclusion

Conclusions on analysis methods

- Frequency analysis: identified spam session does show up in frequency.
- Periodicity analysis: Periodicity can be found in traffic from certain machines, does not appear to say say a lot as spam runs do not appear to be a periodical event, rather a burst.

Conclusion

Conclusions on analysis methods

- Frequency analysis: identified spam session does show up in frequency.
- Periodicity analysis: Periodicity can be found in traffic from certain machines, does not appear to say say a lot as spam runs do not appear to be a periodical event, rather a burst.
- Entropy analysis shows the results described in the previous research.

Conclusion

Conclusions on analysis methods

- Frequency analysis: identified spam session does show up in frequency.
- Periodicity analysis: Periodicity can be found in traffic from certain machines, does not appear to say say a lot as spam runs do not appear to be a periodical event, rather a burst.
- Entropy analysis shows the results described in the previous research.
- Flows very good way to look at traffic. Can detect interesting events with ease.

Conclusion contd.

General conclusions:

- Possible to detect that email is being sent

Conclusion contd.

General conclusions:

- Possible to detect that email is being sent
- Reliably classifying email as spam more difficult, as the information is very limited.

Conclusion contd.

General conclusions:

- Possible to detect that email is being sent
- Reliably classifying email as spam more difficult, as the information is very limited.
- In principle only mailservers should be doing DNS MX requests, so all other machines potential suspects.

Conclusion contd.

General conclusions:

- Possible to detect that email is being sent
- Reliably classifying email as spam more difficult, as the information is very limited.
- In principle only mailservers should be doing DNS MX requests, so all other machines potential suspects.
- DNS MX detection can serve as additional evidence in classification, but is not strong enough by itself.

Conclusion contd.

General conclusions:

- Possible to detect that email is being sent
- Reliably classifying email as spam more difficult, as the information is very limited.
- In principle only mailservers should be doing DNS MX requests, so all other machines potential suspects.
- DNS MX detection can serve as additional evidence in classification, but is not strong enough by itself.
- All results gained from a small dataset with one spamrun. Not enough examples of bad behaviour for good classification.

Questions?

Questions?