SIDEKICK
Suspicious Domain Classification

Master Thesis
at SIDN
by Moritz Mueller
Agenda

• Misuse of Domain Names
• Malicious domains in .nl
• Malicious Domain Characteristics
• What does SIDEKICK do?
• Outlook
Misuse of Domain Names
Redirection, Exploitation, Infection

Exploit Kit Infection Chain
Command and Control

C&C Address Resolution and Communication

Who has baddomain.nl

A 10.5.3.1
A 192.168.666.5
A 172.16.123.3
Motivation for SIDN

- Trust
- Reputation
- Overall Internet Security
Phishing

Age of .nl phishing domains

1,923 domains

- one week or younger
- between one week and one year
- one year or older

Age of .nl phishing domains
Botnets

Known Botnet Domains

82 domains
- Sinkhole
- Other Sources
- Quarantainenet

2015-08-14
Malicious Domain Characteristics
Geographic Characteristics

95.5% Dutch registrants

88.5% Dutch content
Query Origin

Benign .nl Domains

2015-08-14
Query Origin

Benign .nl Domains  Andromededa Domains

2015-08-14
Query Frequency

Popular .nl domains
Query Frequency

Flashback-Botnet domains
Query Frequency

Unpopular .nl domains
Query Frequency

New benign domains
Query Frequency

![Query Frequency Graph]

- **New benign domains**
- **New phishing domains**

2015-08-14
Domains in Quarantine

The graph shows the number of domains in quarantine and the number of free domains. The histogram indicates that there is a significant number of domains in quarantine compared to free domains.

- **In Quarantine**: The dark blue bar represents the mean number of queries, which is much higher than the light blue bar for the median number of queries.
- **Free**: The dark blue bar for the mean number of queries is still present, but the light blue bar for the median number of queries is very small, indicating a smaller range of values.

The data suggests that there is a larger variability in the number of queries for domains in quarantine compared to those that are free.
Catching Bad Domains With SIDEKICK
General Approach

Training
General Approach

Training

Classification
SIDEKICK Architecture
New Domains

• 61,000 Domains classified
• 33 Malicious domains detected
• False Positive Rate 0.3 %

More domains detected than by professional Phishing Feed
SIDEKICK Architecture
Old Domains

- 1,7 Million Domains Classified
- 14,000 Malicious domains detected

Can't verify suspicious domains
Next Steps
Improvements

- Early Detection
- Additional Features
  - Non-DNS-related sources (Social Media, Search Engines, CMS and Webserver)
  - EDNS Client Subnet Extension
  - Resolver Reputation
Outlook

• Post Detection
  – Block Content
    • Google Safe Browsing, Netcraft
  – Notify (Registrant, Registrar, Web-Hosting-Firm)

• Post Suspicion
  – Cooperation
SIDEKICK

- Based on geographic location and query patterns
- Effective detection of new domains
- Detection of suspicious compromised domains

Thank You For Your Attention