Outsourcing Malicious Infrastructure to the Cloud

Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis

Institute of Computer Science (ICS)
Foundation for Research & Technology Hellas (FORTH)

kondax@ics.forth.gr

A Few Examples… (2009-2010)

- Researchers analyze botnets which coordinates and updates through Twitter (Base64-encoded Data in Tweets)
- KOOBFACE Botnet spreads over Social Networks, has malware repositories and stores stolen information on the Web.
- 10K Passwords and Credit Card numbers leak in public areas of the Web.

The Pastebin Incident

Pastebin

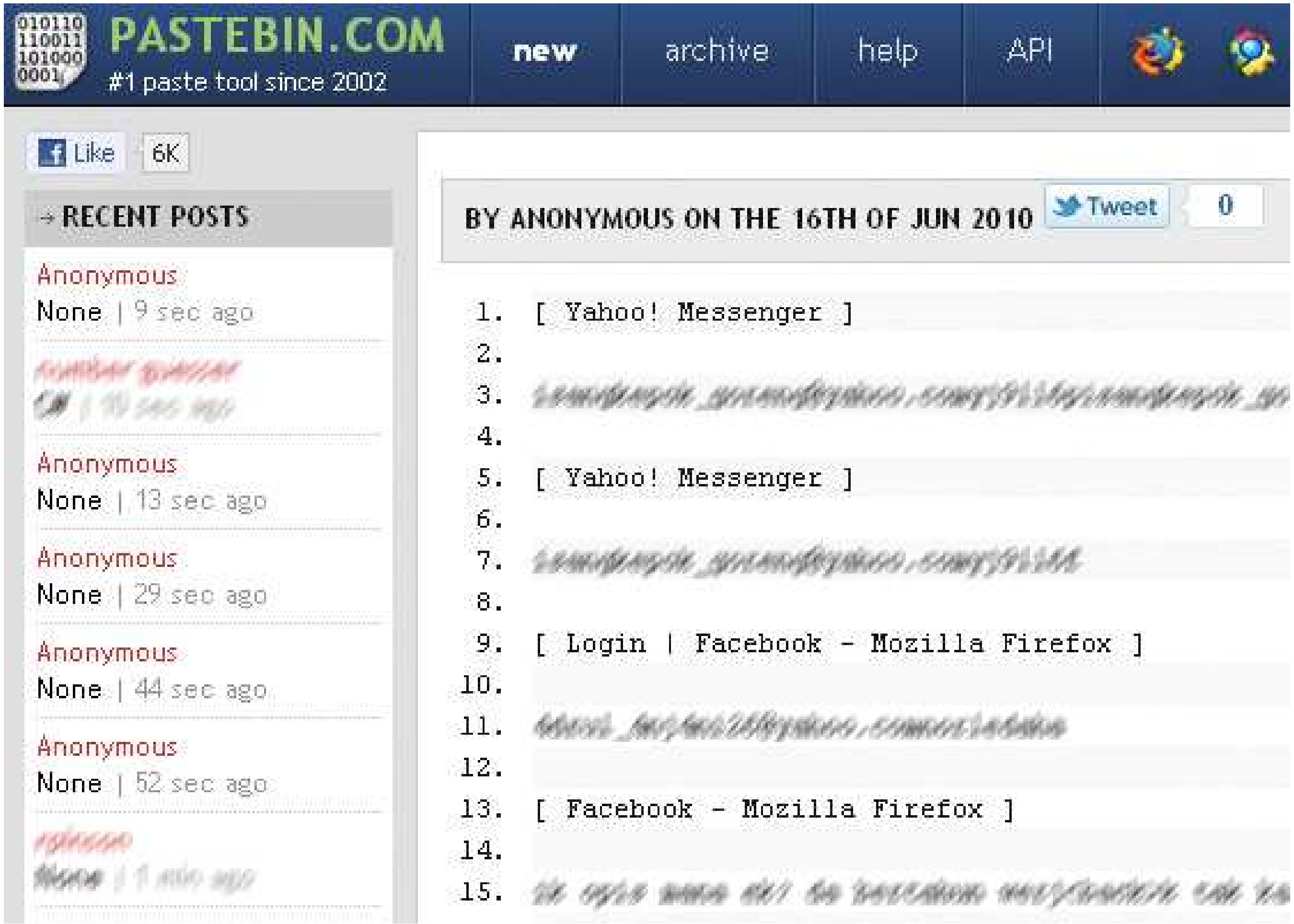
- Online collaboration Service
- Designed so that users can share snippets of code
  - Instead of a copy-paste in the body of an e-mail
  - Alice uploads code in Pastebin, receives a URL
  - Alice sends that URL to Bob
  - Bob accesses the code on Pastebin

- Today it's more a general-purpose service hosting user-generated text content.
- **Basically one big online clipboard**

The Pastebin Incident

- May 2010
- Large number of Pastebin entries:
  - raw streams of keystrokes.
- Constantly Increasing in Volume.
- Dominated the content being uploaded to the Service.

The Pastebin Incident



Anonymous
None | 9 sec ago

[redacted]

Anonymous
None | 13 sec ago

Anonymous
None | 29 sec ago

Anonymous
None | 44 sec ago

Anonymous
None | 52 sec ago

[redacted]

BY ANONYMOUS ON THE 16TH OF JUN 2010

```
[ Yahoo! Messenger ]

[redacted]

[ Yahoo! Messenger ]

[redacted]

[ Login | Facebook - Mozilla Firefox ]

[redacted]

[ Facebook - Mozilla Firefox ]

[redacted]
```

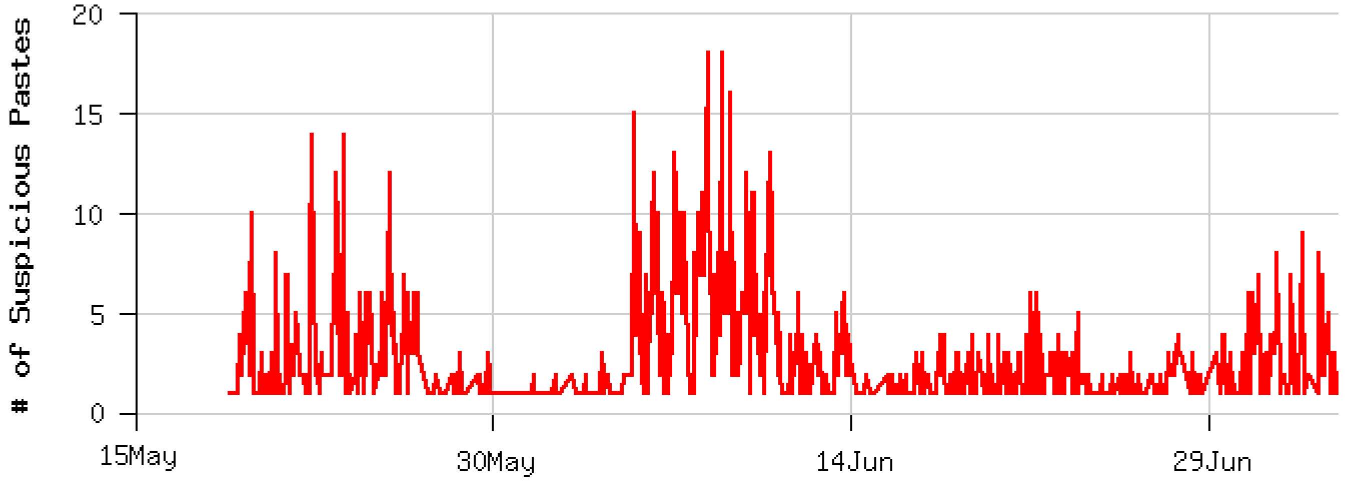
The Pastebin Incident: Data Collection

- Active Crawling
  - Scrape in real-time the
    “Recent Posts” section of the site.

- Back-in-Time Crawling
  - The Web gets Indexed! ☺
  - Google search “site:pastebin.com <term>”,
    limited scope to one month at a time,
    going backwards.

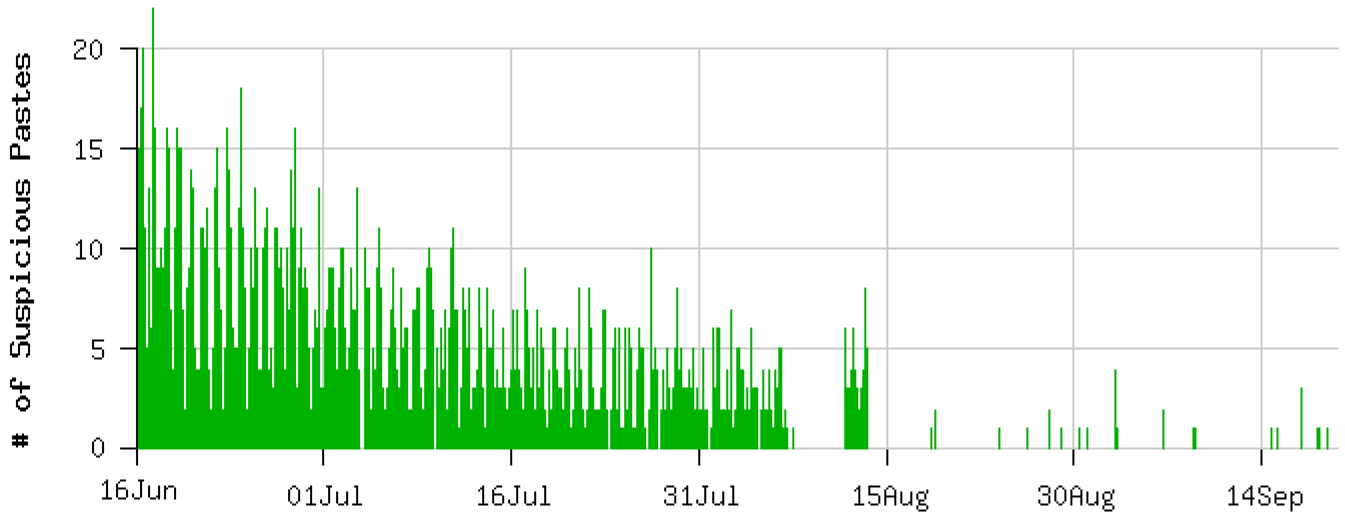
The Pastebin Incident: Data Analysis

- Back-in-Time Crawling
  - Volume of Stolen Information per Hour



The Pastebin Incident: Data Analysis

- Active Crawling
  - Volume of Stolen Information per Hour

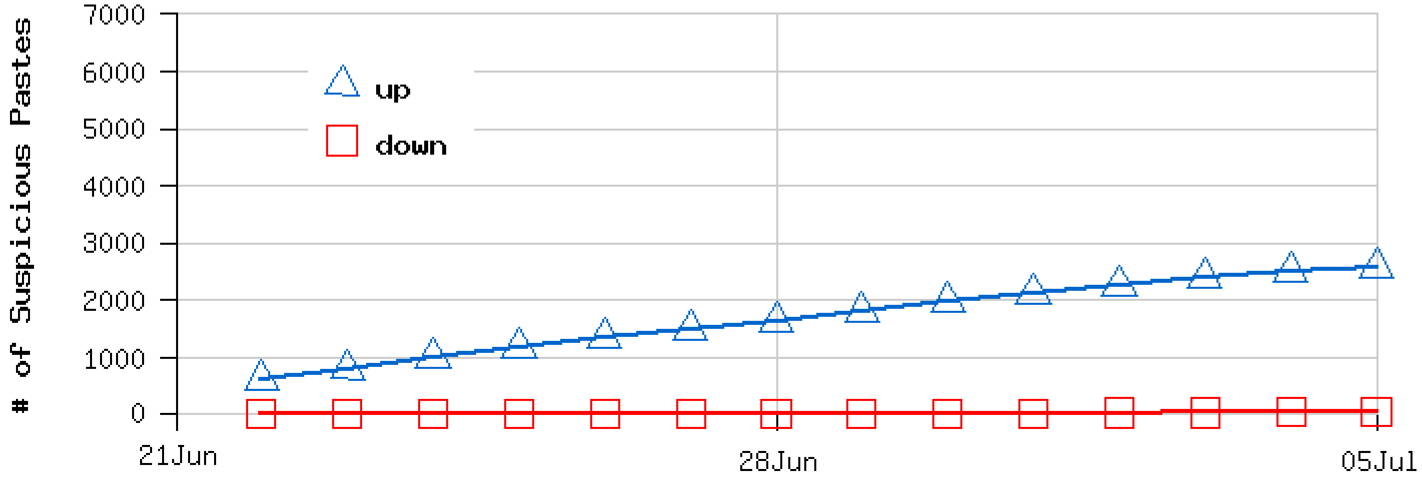


The Pastebin Incident: Data Analysis

- Stolen Information Gathered
  - Hundreds of
    - URLs
    - Usernames
    - Passwords
    - E-Mail Addresses
    - Instant Messenger Conversations

The Pastebin Incident: Data Analysis

- Takedown Rate of Stolen Information



The Pastebin Incident

- In Summary:
  - Keylogger uploading stolen information
    - URLs, Usernames, Passwords,
      E-Mail addresses, Private Conversations
  - Lasted 3 Months
  - Takedown rate could not keep up with incoming the volume.
  - Even after takedown, stolen information was available in Web caches and replicas.

Why Outsource to the Cloud?

Why Outsource to the Cloud?

- Economics
  - Cloud Services cheap or free to use.
    - Twitter, Facebook, Pastebin, Rapidshare, etc.
  - No need for dedicated hardware or network connection.
- Reliability
  - Cloud aims at 99% uptime
  - Compromised Computers can be shut down or fixed.

Why Outsource to the Cloud?

- Scalability
  - Cloud scales in terms of storage, processing power and network capacity.
  - Compromised infrastructures may run out of resources.
- Unobservability
  - Accessing a Cloud service does not necessarily raise any red flags.
  - There’s enough noise on the Cloud to “blend-in”.

Why Outsource to the Cloud?

- Plausible Deniability
  - No direct connection between Attacker and Victim.
- Unique Features and Flexibility
  - e.g. Pastebin
    - Arbitrary Pastebin Subdomains
      - http://<anything>.pastebin.com is valid
      - DGA allow dynamic Malware, resilient to Black-listing

What does all of this mean to Security Researchers?

What does all of this mean to Security Researchers?

- Attackers leveraging the public Cloud will get indexed (e.g. by search engines).

- Massive and automated nature of malware (e.g. botnets) could be detected on a single site.

What does all of this mean to Security Researchers?

- Anomaly Detection on Cloud Services
  - Heuristics exist to prevent service abuse.
  - Extension of heuristics to identify threats in the payload and/or produce alerts, signatures.
  - e.g. querying search engine with certain keywords will reveal lists of stolen information, compromised and vulnerable machines.

What does all of this mean to Security Researchers?

- Global View of Attacks
  - Traditional security practices aim for large telescopes.
  - A single laptop can inspect the Cloud for attacks.

Questions?

Thank you!

Georgios Kontaxis

kondax@ics.forth.gr