EURECOM
Sophia Antipolis

The Role of Web Hosting Providers in Detecting Compromised Websites

Davide Canali, Davide Balzarotti, Aurélien Francillon

Software and System Security Group
EURECOM, France

Motivations

EURECOM
Sophia Antipolis

- **Shared web hosting** is used by **millions of users**
  - Host personal and small business websites
  - Users often have little or no security background
  - Even experienced users have little control/visibility
- Millions of websites, unexperienced users, outdated/vulnerable web apps → **huge attack surface**!
- Hosting providers should play a key role in helping the user in case of a compromise
  - Is this the case?

Goal

EURECOM
Sophia Antipolis

- Study how shared web hosting providers handle the security of their customers
  - By **detecting the compromise** of their websites
  - By testing their **reactions to abuse complaints**

- We also tested six **specialized security services**
  - Provided as an add-on for hosting accounts
  - Monitor security issues on websites
  - For a small fee

Testing methodology (1/2)

EURECOM
Sophia Antipolis

- **Register** multiple shared hosting accounts
- Install real web applications
- Simulate a number of **compromise scenarios**
  - Infected by botnet
  - Data exfiltration (SQL injection)
  - Phishing kit
  - Code inclusion (Drive-by-download)
  - Compromised account (upload of malicious files)
- **Tests** designed to be noisy and **easily detectable**

Testing methodology (2/2)

EURECOM
Sophia Antipolis

- Phase 1: observe the provider's reaction
- Phase 2: send **abuse complaints** regarding our websites
  - **Real complaints** about phishing and malicious executables
  - **Illegitimate complaints**, about offending or malicious content, while the account was clean

Ethical Issues

EURECOM
Sophia Antipolis

- We used real vulnerabilities, a real phishing kit, and a real drive-by javascript code
- But
  - we modified the sources to be **exploitable only by us** (special parameters)
  - **not indexable** by search engines (robot.txt)
  - malicious content was **not accessible from the web** or disabled

Tested Providers

EURECOM
Sophia Antipolis

- **12** among the **top global ones** (mostly US-based)
- **10 regional ones**
  - From Europe, US, India, Russia, Algeria, Hong Kong, Argentina, Indonesia
- 6 add-on security services
  - Less than 30 $/month subscription fee
  - Two come in *basic* and *pro* version
  - 10 days detection threshold
    (we expected them to be quick at detecting security issues)

Scenarios details

EURECOM
Sophia Antipolis

- Infected by botnet
- Data exfiltration (SQL injection)
- **Phishing kit**
- Code inclusion (Drive-by-download)
- **Compromised account (upload of malicious files)**

Remote File Upload of a Phishing Kit

EURECOM
Sophia Antipolis

Setup

- OsCommerce installation mimicking a known **Remote File Upload** vulnerability
- Performs the upload a real Bank of America **phishing kit** (disabled back-end code)

Attack

- *Attacker phase*, run every 6 hours: uploads the phishing kit by triggering the vulnerability
- *Victim phase,* every 15': simulates a victim falling prey of the phishing attack
  - The forms on the phishing pages are filled up with a set of fake personal details (manually pre-generated)

Compromised account
(upload of known malicious files)

EURECOM
Sophia Antipolis

Setup

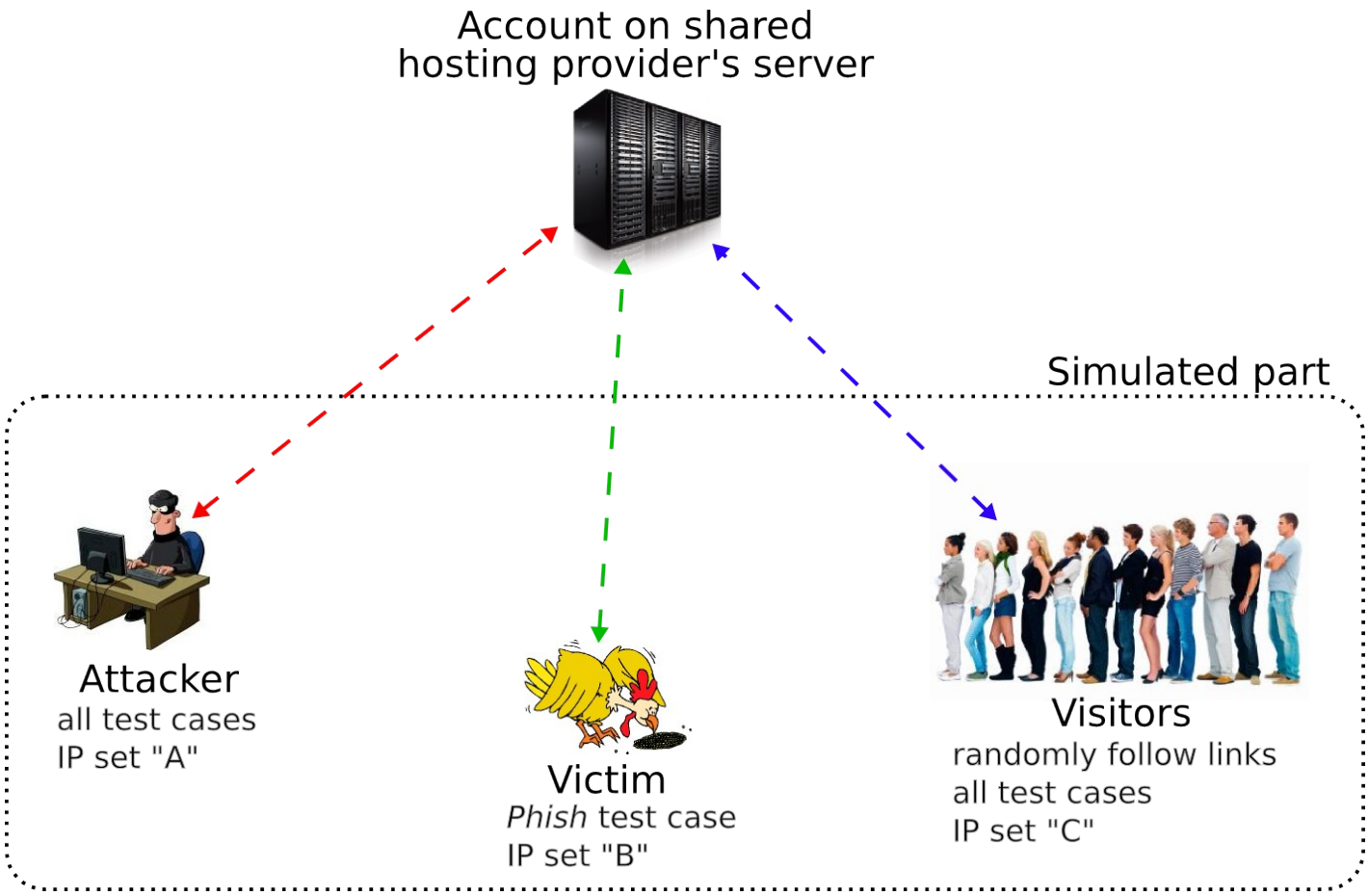
- Static HTML page with random English sentences and some pictures
- Two **known malicious files** (PHP and executable)
  - *c99.php*: a real c99 web shell
  - *sb.exe*: Ramnit worm
  - Both detected by most antiviruses

Attack

- **Uploads** the two malicious files to the shared hosting account **via FTP** (attacker using stolen credentials)
- Run every 6 hours

Experiment scheme

EURECOM
Sophia Antipolis



Results

EURECOM
Sophia Antipolis

- Registration
- Attack prevention
- Compromise detection
- Response to abuse complaints

Results: registration

EURECOM
Sophia Antipolis

- Some providers **discourage abusive** user **registrations**
  - Phone calls, ID scan, 3rd party fraud protection services
- **Global providers** are **more cautious** than regional ones
  - 58% of them manually verified at least one of our accounts (10% for regional)
- **Three regional** providers have a very simple **“1-step” signup process**
  - Never verified our information upon registration

Results: prevention and detection

EURECOM
Sophia Antipolis

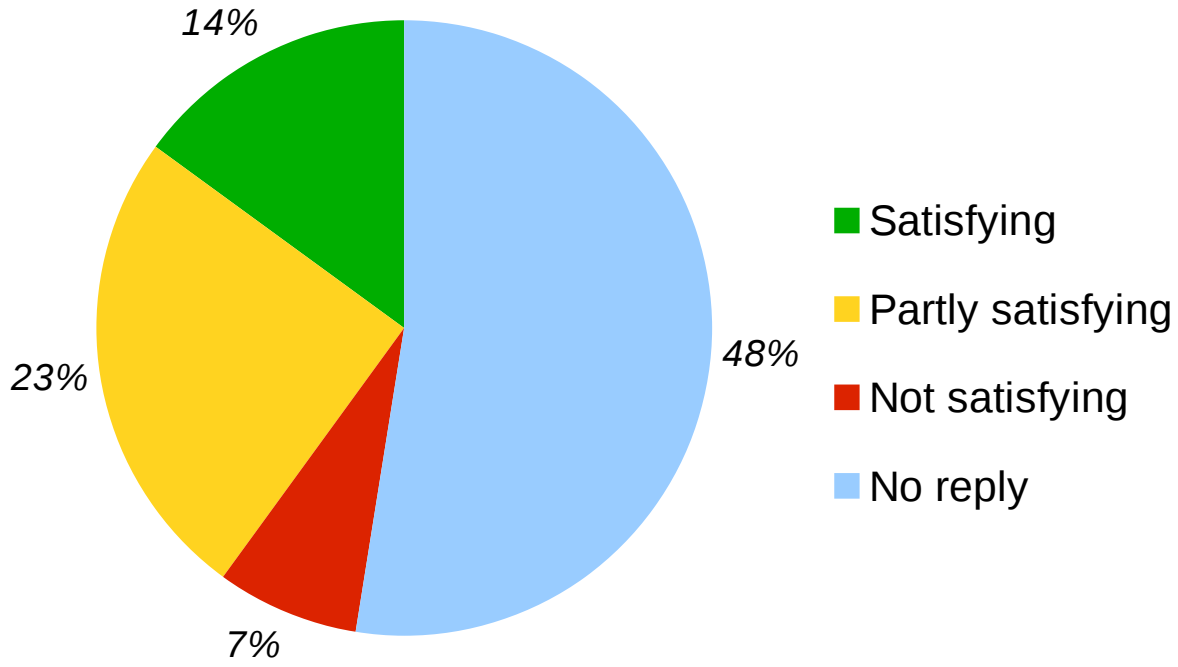
- Attack **prevention measures work to some extent**
  - **URL blacklists** to block SQL injections and File Uploads
    - SQLi,SH, Phish in ~30% of the cases
  - Connection and OS-level **filtering** are effective (Bot)
  - Some providers seem to employ the same (commercial) rule sets for blocking attacks
- Attack **detection results** are quite **disappointing**
  - **Only one provider** was able to detect **one** of our attacks
  - Received alert for **test AV after 17 days** it was running

Results: abuse complaints

EURECOM
Sophia Antipolis

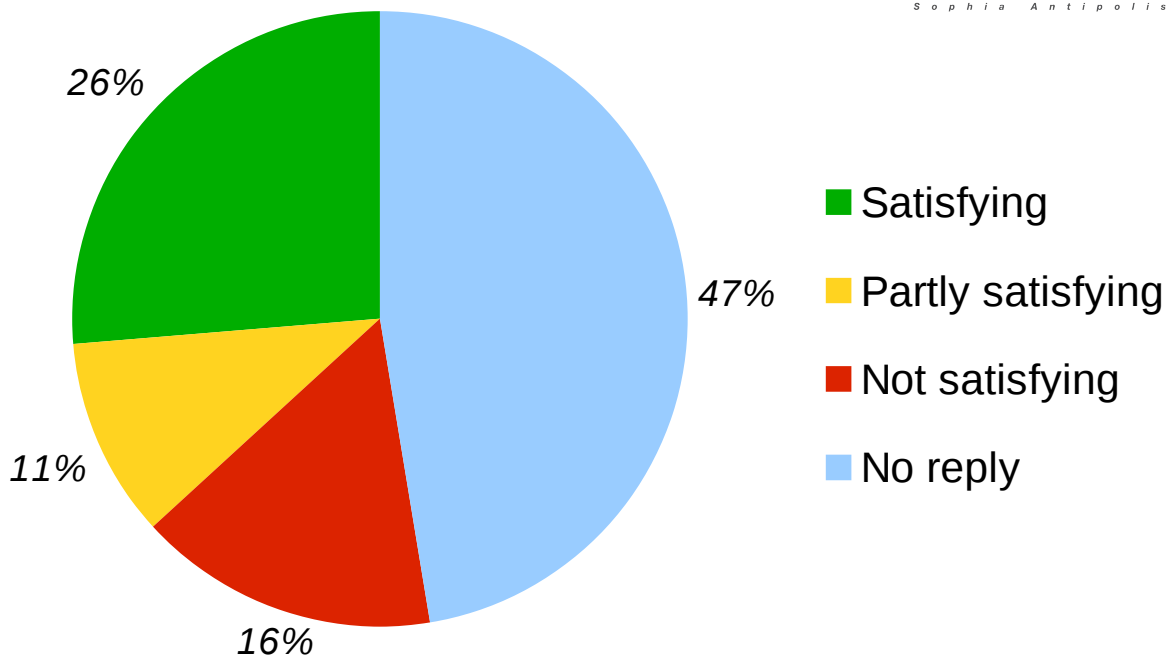
- **50%** of the tested providers **never replied** to any notification
- **64%** of the **replies** arrived **within one day** from the notification
- Average response delay:
  - **28h** for **global** providers
  - **79h** for **regional** providers
- Wide variety of reactions...

Real abuse notification handling



- **Only 3** providers **out of 22** handled them well
- Some **overreact** (e.g., two of them terminated the user's account)
  - Others sent an ultimatum to the user, but then did not check whether the user did anything to clean up the account

Illegitimate abuse notification handling



- **14** providers **out of 19** tested behaved well
  - » **Over estimation**
- 3 (regional) providers believed the complaint without checking
  - completely **wrong decisions** (e.g., account suspension, file removal)

Detection by Security add-on Services

EURECOM
Sophia Antipolis

- Some of the services we tested had a partnership with a **URL blacklisting service**
  - → We intentionally got our malicious pages blacklisted
- **Five out of six** services did **not detect anything**
- One detected
  - the malicious files (through an antivirus scan) but they did **NOT notify the user**
  - the blacklisted malicious page

Conclusions

EURECOM
Sophia Antipolis

- Quite a **lot of effort** is spent in **preventing** malicious **registrations**
  - Especially from **global** providers
- Most providers employ **basic** mechanisms to **prevent** some kinds of **attack** (e.g., URL blacklists)
- Almost **zero effort** in **detecting obvious** signs of **compromise**
- **Cheap security services are useless**
- **Half of the companies responded** to complaints
  - Only 14% in the appropriate way

Thank you

EURECOM
Sophia Antipolis

?

For further questions, suggestions, comments:

canali@eurecom.fr