

Shark: Spy Honeypot with Advanced Redirection Kit

Ion Alberdi and Eric Alata and Philippe Owezarski and
Vincent Nicomette and Mohamed Kaâniche

5th of November 2007



Plan

- 1 Measurement and Internet security
- 2 Getting malicious traffic
- 3 Shark



Plan

- 1 Measurement and Internet security
- 2 Getting malicious traffic
- 3 Shark



Plan

- 1 Measurement and Internet security
- 2 Getting malicious traffic
- 3 Shark



Plan

- 1 Measurement and Internet security
- 2 Getting malicious traffic
- 3 Shark



Measurement purpose

Need: Internet services need more and more QoS guarantees.

Problems:

- 1 Internet is only best effort,
- 2 How to provide multimedia/streaming content, what is done nowadays: `oversize` network infrastructure
- 3 What is actually going through these huge cable/networks \implies ???

Measurement solution:

- 1 Take traffic snapshots and measure what's happening \simeq Live debugging network infrastructures to improve their efficiency.



If it was only the best effort issue...

Problem Internet has not been built with potential malicious Internet users in mind.

Bigger problem Oversizing means: more and more people interconnected, more and more bandwidth available for legal but illicit traffic too.

Biggest problem Some people are willing to pay for D(D)oS and spams.

A partial answer “What is actually going through these huge cable/networks” \implies We can found polluting traffic that:

- consumes bandwidth,
- could aim to decrease network efficiency.

Measurement solution needs to handle this problem too.



Malicious traffic example

Example of malicious flows generated from a corrupted network node: [▶ Back](#)

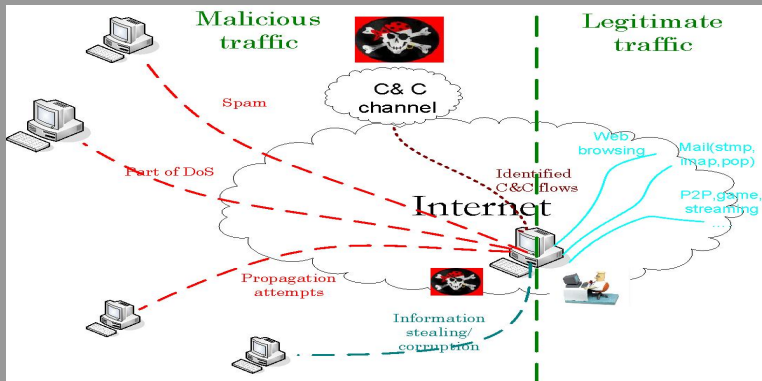


Figure: Some malicious flow examples

Measurement of illicit traffic

Manager roadmap:

- 1 Let's get such traffic,
- 2 Let's analyze it,
- 3 Let's find some detection models, build IDSeS and solve this problem.



Engineers and scientists getting to work

- 1 Let's get such traffic.
Well... how ?
 - Capture normal traffic, and find malicious traffic inside [1] \implies why analyze malicious traffic we already detected ?
 - Put a honeypot on unused IP address [2, 3] \implies only random propagation attempts.
 - Generate malicious traffic by hand¹ [4] \implies does it reflect realistic malicious traffic ?
- 2 Go back to manager, modify predicted deadlines.

¹http://www.ll.mit.edu/IST/ideval/data/data_index.html

Plan

- 1 Measurement and Internet security
- 2 Getting malicious traffic
- 3 Shark



The information contained in malwares

- 1 “Put a honeypot on unused IP address[2, 3] \implies only random propagation attempts”, well. . .
- 2 If the honeypot simulates the attack success, we get post attack traces ▶ Illicit traffic
- 3 First try on malicious traffic collecting: collect with `nepenthes` malwares targetting some server-side vulnerabilities, and observe them.



How to handle malwares to extract their malicious traffic

- idea: malwares are the most accurate malicious traffic generator we have,
- why not use/execute them ?
- but:
 - 1 we cannot let propagation attempts access the Internet,
 - 2 blocking traffic has side effects: for example without DNS the malware cannot do anything.



A first scope of traffic dissection

Necessary outgoing traffic:

- DNS
- C&C
- malware updates
- ...

Forbidden outgoing traffic:

- Propagation attempts
- DDoS
- Spam
- ...



How to recognize traffic ?

- What should we do with an outgoing TCP SYN segment to port 1025 ?
- Let's redirect analyze and assume the next malware execution will have the same pattern.
- How to redirect ?



Plan

- 1 Measurement and Internet security
- 2 Getting malicious traffic
- 3 Shark**



Netfilter hooks

Redirection Kit based on Linux's netfilter firewall hooks.

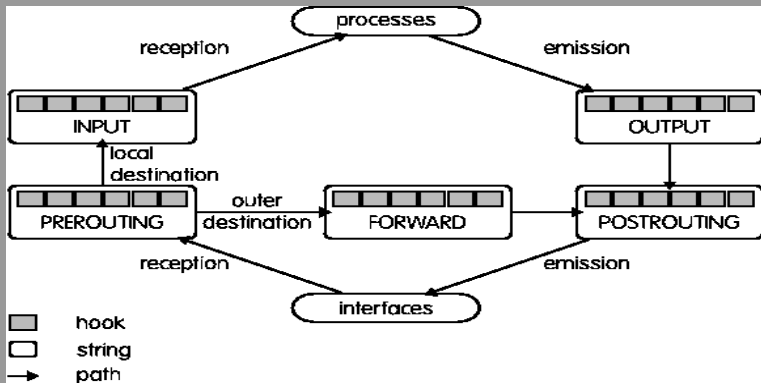


Figure: Netfilter hooks

Shark

How the redirection software is implemented

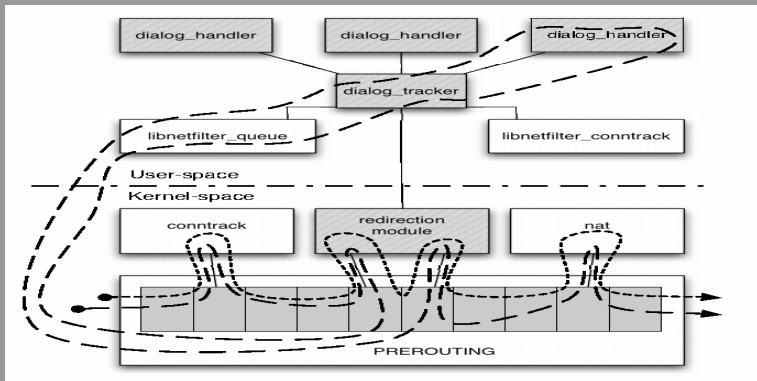
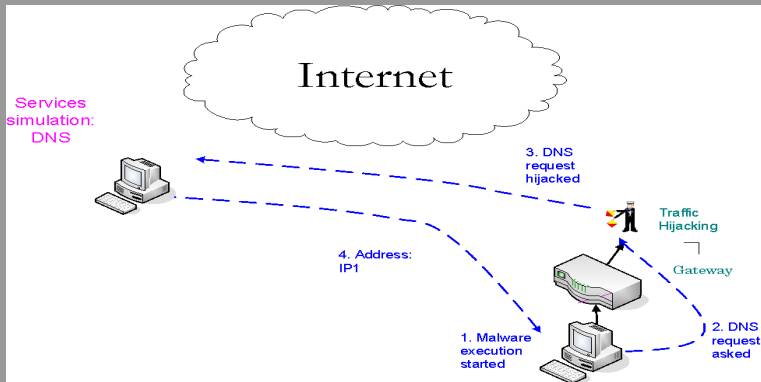
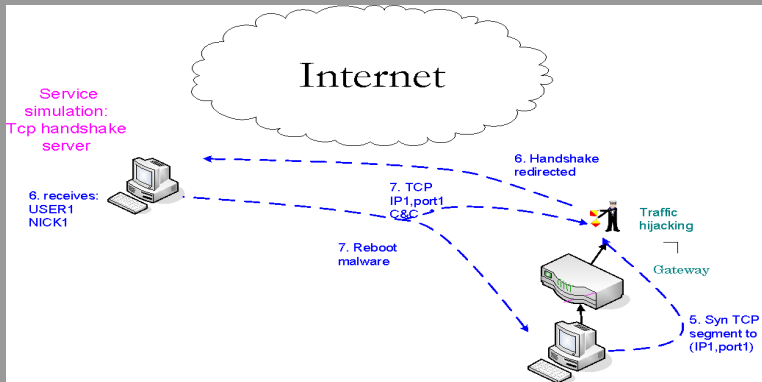


Figure: Shark implementaion

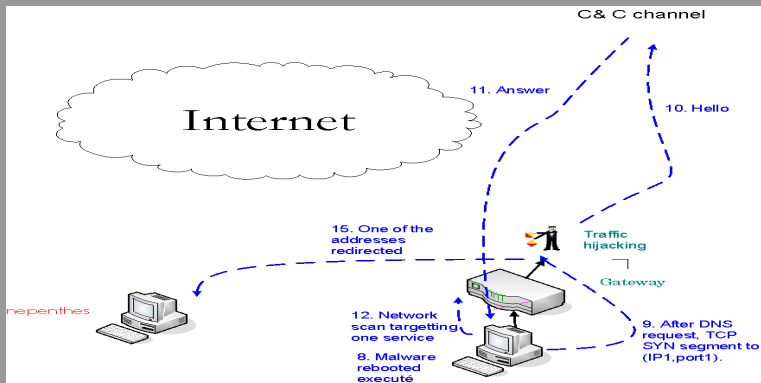
How it works



How it works



How it works



What we learnt

Ports information is useless for traffic detection We found C&C IRC channels on the range [22-65520].

Information obfuscation on C&C :hub.24324.com 332 seivNbtC
#last:=BGX5tCMI9HMuPIQRIf7ZDvrWvjsrx3Qc
TGwmkNACosllT7o+6BL/FkEl1LzB/AkO7BSNYd1y
cZi/zOu/AWHE5fJNT02YoaGogFZbH03O9Z/OVp4b
DrWR3gJylug2Eee3JVQHBn/fWG6ANlrYr0mZbtKuh
Means:

try to exploit a class B network using a flaw on
dcom service(tcp,135).

Other flows used for malware updating :STA 332 Bot|2153
#server# :.dl http://url/malware.exe>
<malware2.exe> 1



They are not so dumb

Some log after using shark on ssh honeypot:

```
sh$ ./unix 66..
```

```
[+][+][+][+][+] UnixCoD Atack Scanner [+][+][+][+][+]
```

```
[+] SSH Brute force scanner : user & password [+]
```

```
... [+] Scanam: 66.221.4.* (total: 2) (1.6% done)
```

```
66.221.8.* (total: 2) (3.1% done)
```

```
...
```

```
66.221.60.* (total: 2) (23.1% done)
```

⇒ Two scan hit, but none tested by ssh bruteforcer

Did they try these addresses from another network point to avoid local redirection ?



Report to the manager

Well it's not that easy to automatize, because:

- 1 Traffic filtering policy influences traffic malware generates.
- 2 By letting traffic outside, we take risks but different protocols must be allowed.
- 3 The redirection scheme can be detected[5], and this influences the traffic we get.



Proposed roadmap to manager

Redirection was needed, we got it, now we should have a firewall that monitors outgoing traffic:

manager But you've got snort !

engineers But we've got polymorphism and metamorphism and 0days

manager Ok I extend the deadline.

- Is it impossible ?
- DPI is needed, and this is costfull, but we only need to inspect outgoing packets from one host.
- Why follow this difficult path ? Because a lot of (most of ?) the information is hidden in post intrusion traces.



Conclusion

Any question, advice, criticisms
would be very welcome





Paul Barford, J.Kline, D.Plonka, and A.Ron.

A signal analysis of network traffic anomalies.

*In ACM/SIGCOMM Internet measurment workshop, in
Marseille,France, 2002.*



Micheal Bailey, Evan Cooke, Farnam Jahanian, Niels
Provos, Karl Rosaen, , and David Watson.

Practical darknet measurement.

*In Proceedings of the 2006 Conference on Information
Sciences and Systems (CISS'06), University of Michigan,
An Arbor,MI 48109-2122, 2006.*



Fabien Pouget, Marc Dacier, and Van Hau Pham.

**Leurre.com: on the advantages of deploying a large scale
distributed honeypot platform.**

*In ECCE'05, E-Crime and Computer Conference, 29-30th
March 2005, Monaco, Mar 2005.*





J.Aussibal, P.Borgnat, Y.Labit, G.Dewaele, N.Larieu, L.Gallon, P.Owezarski, P.Abry, and K.Boudaoud.

Base de traces d'anomalies légitime et illégitimes.

In *SAR SSI*, pages 153–168, Annecy France, 2007.



Cliff C.Zou and Ryan Cunningham.

Honeypot-aware advanced botnet construction and maintenance.

In *Proceedings of the 2006 International Conference on Dependable Systems and Networks (DSN'06)*, Orlando, FL 32816-2362, 2006.

