Hunting worms with honeypots

Philipp Seidel

DinoTools.de

29. November 2011

Table of contents

Malware?

- Malware short form for malicious software
- Intentionally harm an infected computer or computer system
- Example: worms, viruses, trojan horses, and many more

Trojan horses

- Application with a feature a user wants
- Does unwanted tasks in the background
- Functions
  - Spy on private data
  - Use it for further attacks
  - Open a backdoor
- Characteristic
  - No replications
  - No population growth
  - Parasitism

Virus

- Spread on execution
- Copy code into new host applications
- Sometimes spread by other malware e.g. trojan horses (Dropper)
- Functions
  - Delete or modify files
  - Break the system
- Characteristic
  - Replication
  - Population growth
  - Parasitism

Worm

- Uses networks and other ways to spread its self
- Infects the host system
- Independent from other applications
- Functions
  - Spreads automatically by E-Mail, ICQ, IRC, ...
  - Sometimes functions from other types of malware
- Characteristic
  - Replication
  - Population growth
  - No parasitism

Exploit

- Code/Program to exploit a system
- Used to document security bugs
- Functions
  - Exploit a system in combination with extra shellcode
  - Some worms use exploits

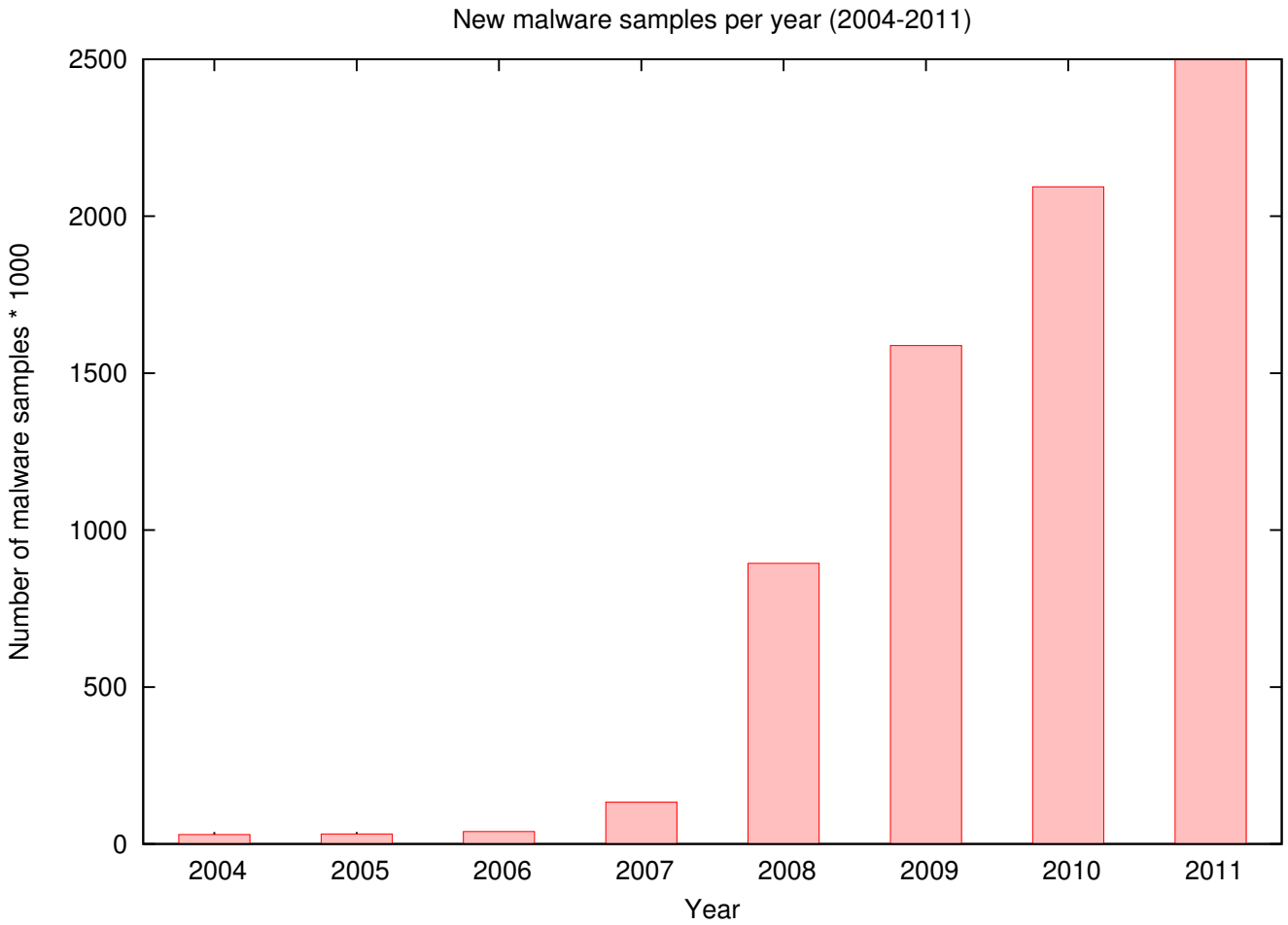
Shellcode

- Opcode generated by an assembler
- Can be executed directly on the CPU
- Sometimes in combination with exploits
- Functions
  - Download a malware or extra shellcode
  - Open backdoors

Further types

- Various combinations
- Hacker-tools (Viruskits)
- Rootkits
- ArcBombs
- Spyware
- Dialer
- RemoteAdmin

G Data Malware-Report



Honeypot

- Application or System
- Simulates services, networks or single applications and its behaviour

Client

- Acts like a desktop operating system or a single application
- Example: Browser

Server

Simulate ...

- Network services
- Computer networks
- Hardware (servers, routers, switches, printers, ...)

Honeypots - Classification by interaction

Low-Interaction

- Limited way for interaction
- Simulates only parts of a service, system, application
- Only functions to successfully run an attack against the honeypot

High-Interaction

- High interaction
- Real operating system
- All applications and services are not simulated
- Monitored from outside

PhoneyC

- Low-Interaction Client Honeypot
- Written in Python
- Framework to detect attacks against a client application
- Crawler functionality to download a web page or a web document
- Uses ClamAV to search for malware
- Execute dynamic content by using SpiderMonkey Engine
- Use vb2py to convert VisualBasic code into Python
- Detect buffer overflows while executing the code

Amun

- Low-Interaction Honeypot
- Used to capture malware
- Developed using Python
- Emulates various vulnerabilities

Dionaea

- Low-Interaction Honeypot
- Nepenthes successor
- Core in C, but module and extensions in Python
- Protocols are fully implemented
- libemu to detect shellcode
- Supported protocols: HTTP, TFTP, FTP, Mirror, SMB, EQMAP, SIP und MSSQL

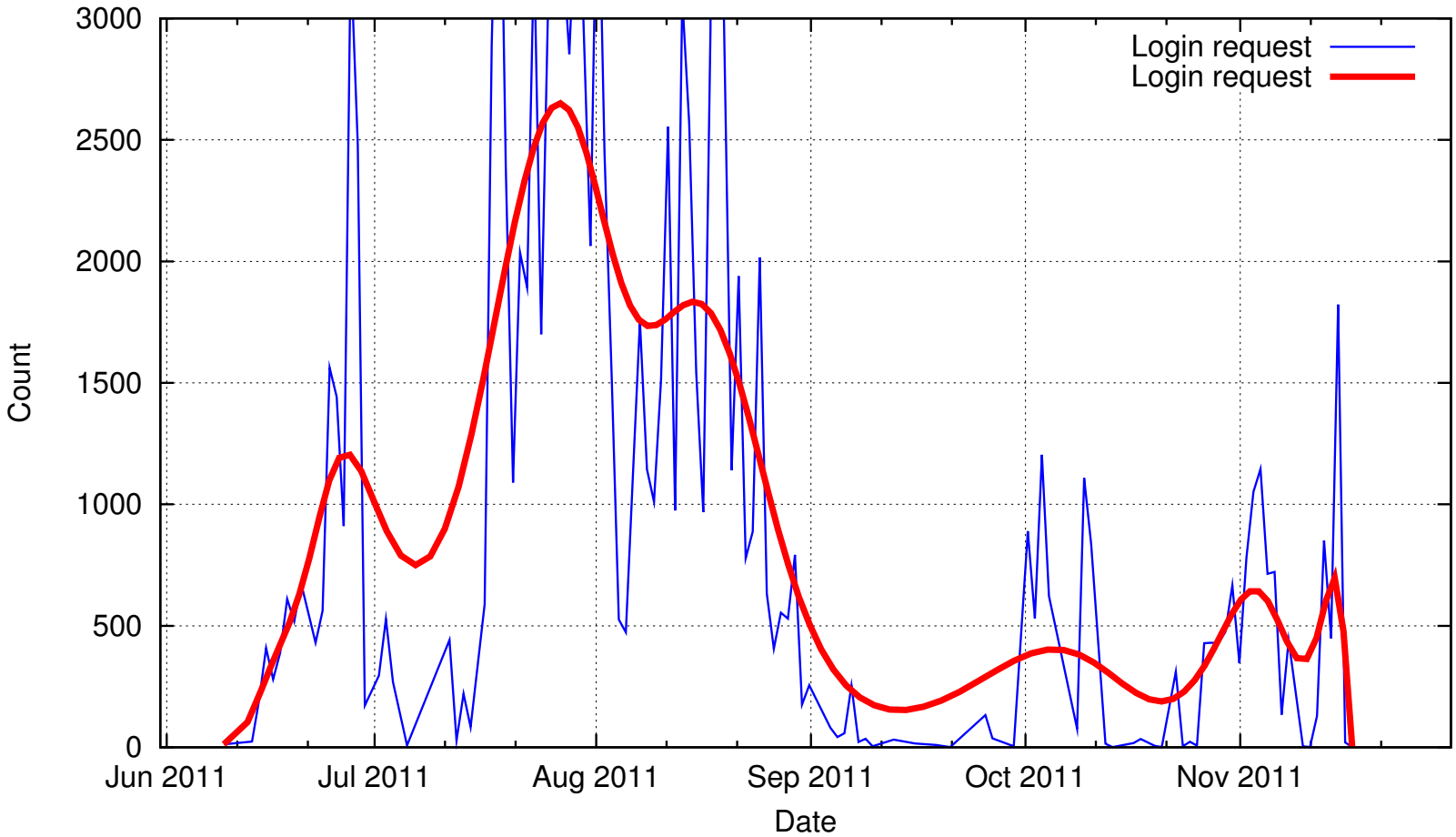
Dionaea - libemu

- Execute x86 opcode
  - Read x86 opcode
  - Emulate CPU registers and FPU
- Execute Shellcode
  - Use GetPC heuristics
  - Win32 Hooking

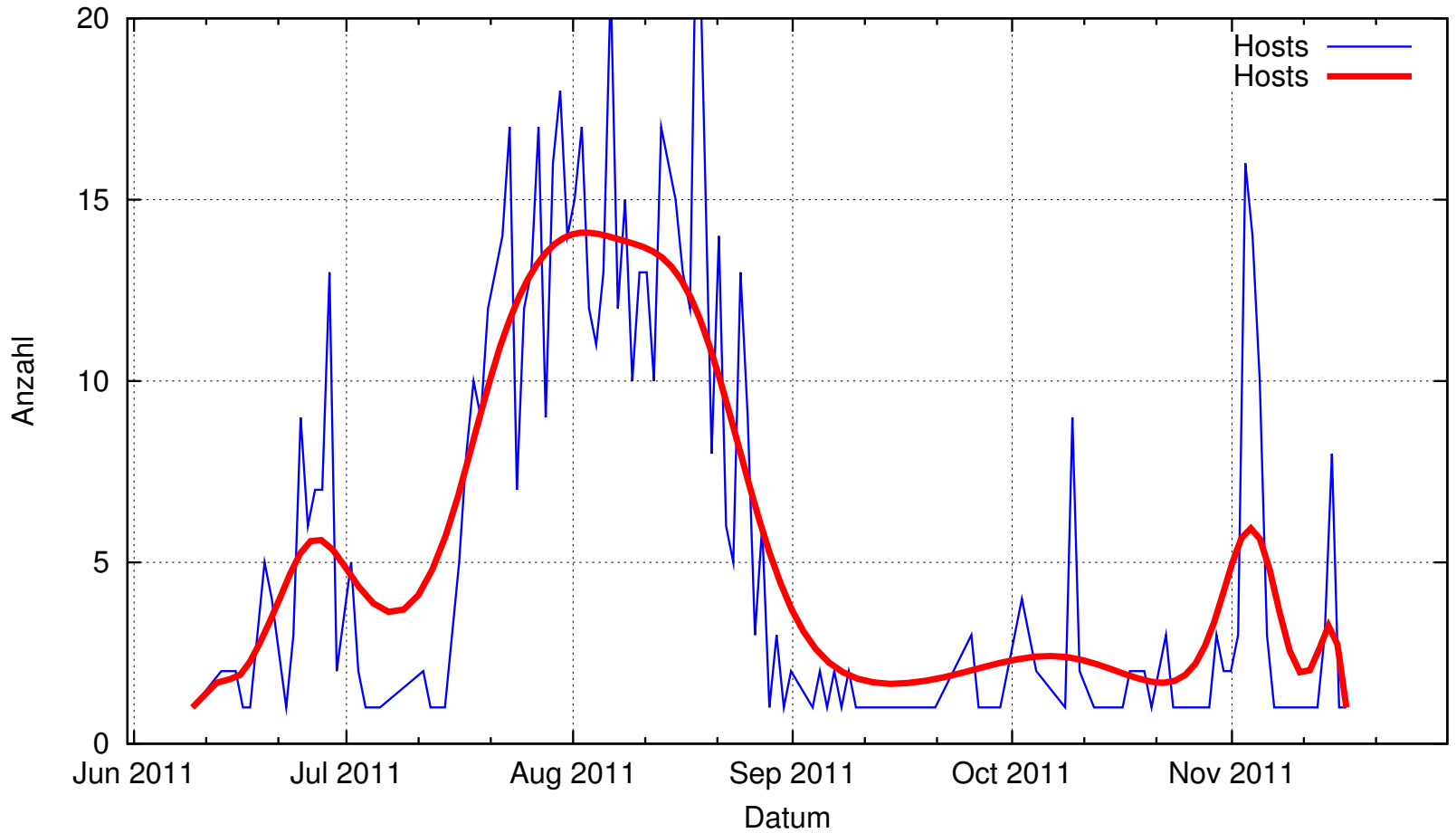
Kippo

- Low-Interaction Honeypot but called Medium-Interaction Honeypot by its developer
- SSH-Honeypot
- Developed in Python using the Twisted framework
- Attacker can do things in a sandbox
- Some applications are emulated or static files

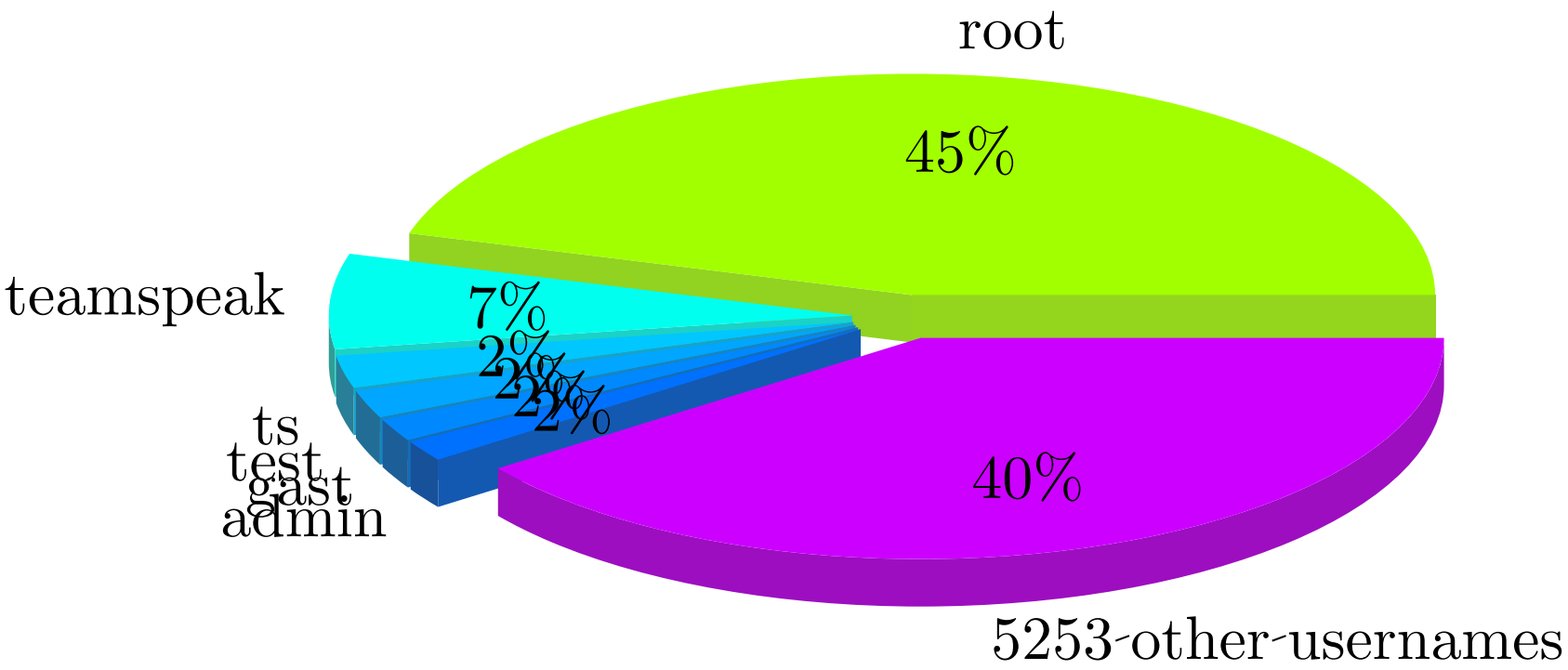
Kippo - Logins



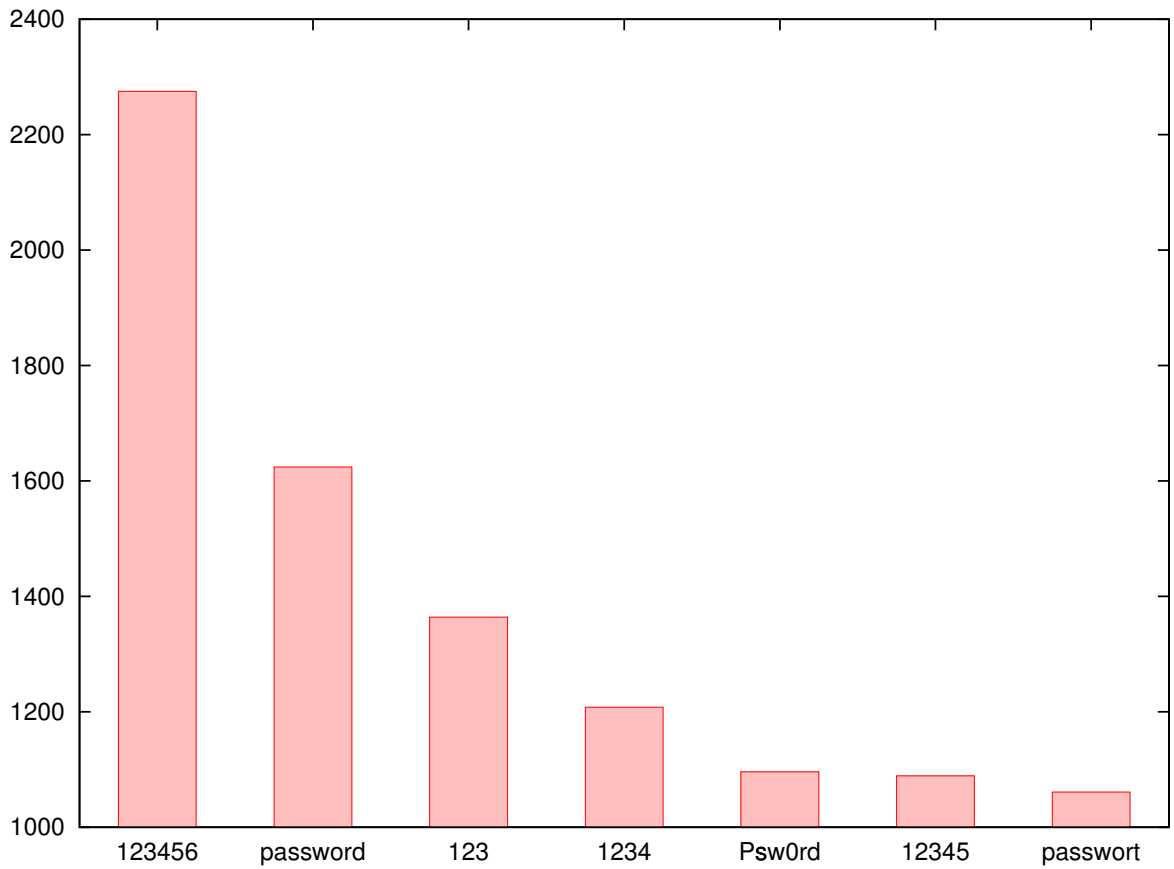
Kippo - Hosts


Hosts
Hosts
Anzahl
Datum
0
5
10
15
20
Jun 2011
Jul 2011
Aug 2011
Sep 2011
Oct 2011
Nov 2011

Kippo - Usernames

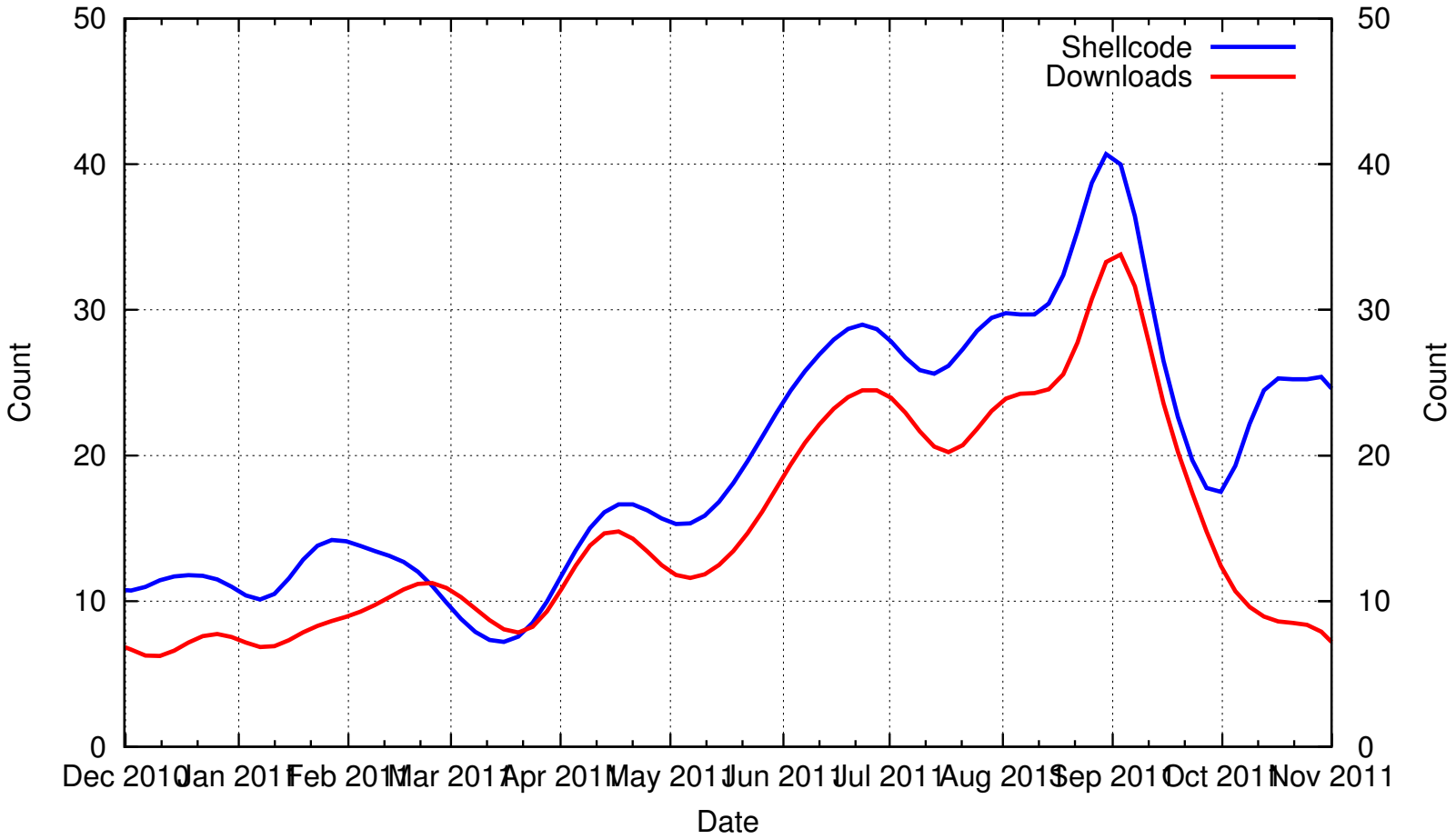


Kippo - Passwords

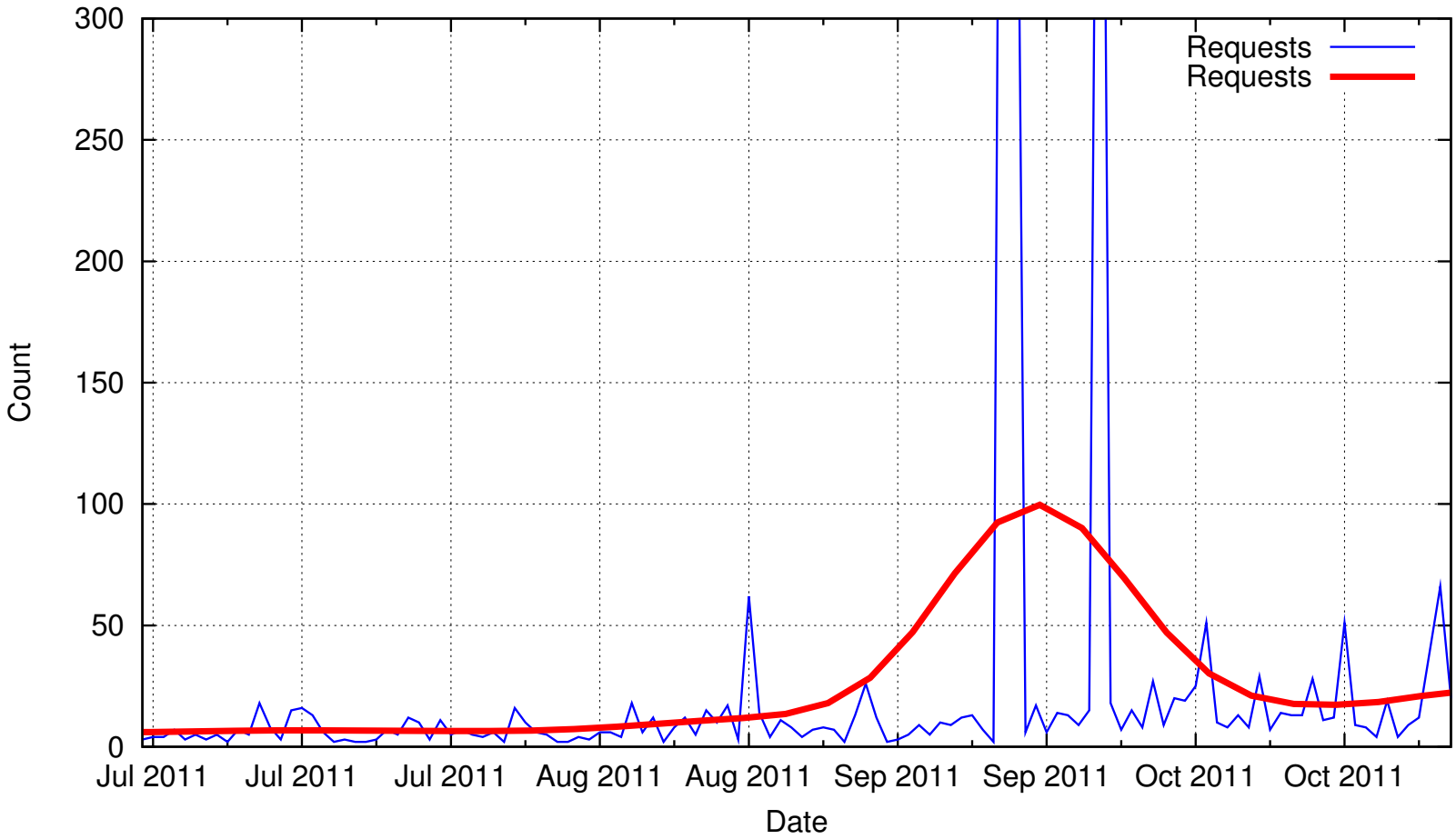


Out of 119859 login requests

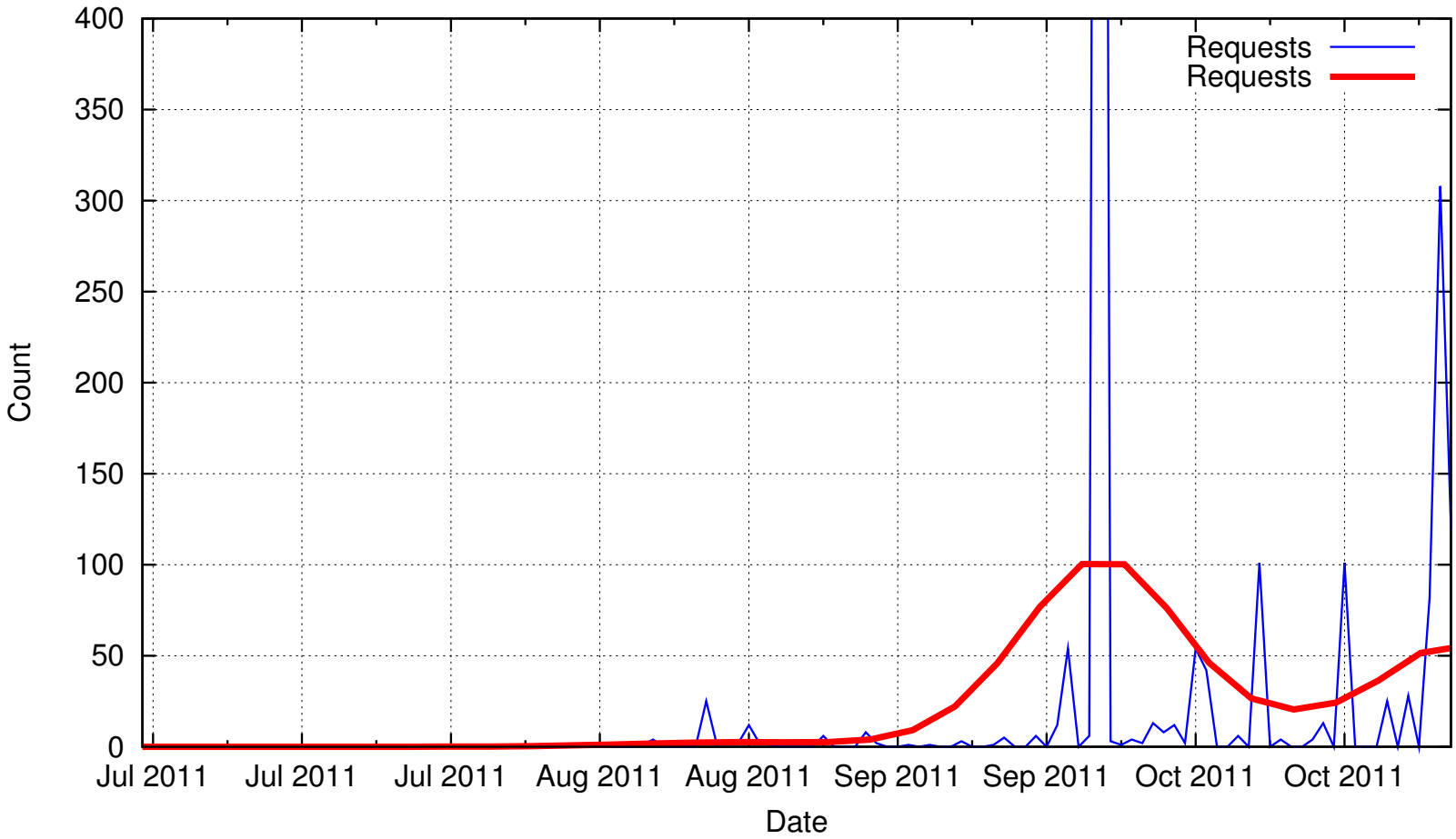
Dionaea - Attacks against the SMB Service



Dionaea - Sip Session



Dionaea - Sip Call



Analyze - Antivirus engine

- ClamAV
  - Open Source antivirus engine
  - Detects less malware than proprietary software
  - URL: `http://www.clamav.net/`
  - Submit new files: `http://cgi.clamav.net/sendvirus.cgi`
- VirusTotal
  - Online service to analyze suspicious files
  - Upload files to the service
  - About 39 AV products
  - URL: `http://www.virustotal.com/de/`
- MAVScan
  - MAVScan = Multi AntiVirus Scan
  - Open Source
  - Runs on the local system and is extensible
  - Supports 5 AV products
  - URL: `http://dev.dinotools.org/projects/mavscan`

Sandbox

- Upload a suspicious file
- Execute the file in a safe environment
- Monitor all system changes and actions (Network, Registry, Files, ...)
- Generate a report

- CWSandbox
  - Free Sandbox
  - Provided by University of Mannheim
  - URL: `http://mwanalysis.org/`
- Anubis
  - Free Sandbox
  - Provided by International Secure Systems Lab
  - URL: `http://anubis.iseclab.org`

Honeypots - Advantages/Disadvantages

Low-Interaction

- Advantages
  - Simple deployment
  - Lower security risks
- Disadvantages
  - Detects only known attacks
  - Detects 0-Day attacks in a limited manner

High-Interaction

- Advantages
  - Detects 0-Day attacks
- Disadvantages
  - Higher security risks
  - Deployment more challenging

How to start

- **Pay attention to the laws!!!**
- honeyd and nepenthes are packaged for Debian und Ubuntu
- PPA for Ubuntu: `https://launchpad.net/~honeynet`

Questions

Thank you for your attention

Are there any questions?