

OSS and Security

Yoshiki Sugiura
CSIRT evangelist
Japan

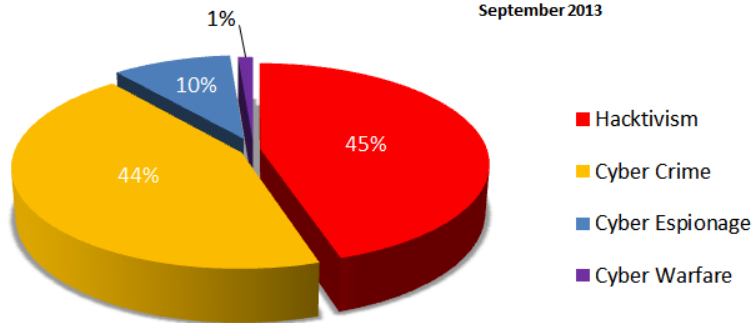
Agenda

- o World Wide Security Trend
- o OSS and Security
- o Vulnerability
- o OSS Security tools
- o Owing your own security team

World Wide Security Trend

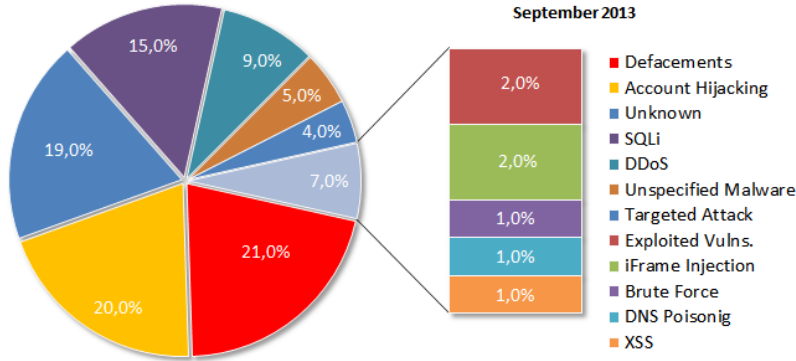
Motivations Behind Attacks

September 2013



Distribution of Attack Techniques

September 2013



- Highly motivated attackers
- Different motivations
- Sophisticated technical capability
- Anti-security cyber attacks are widely happen

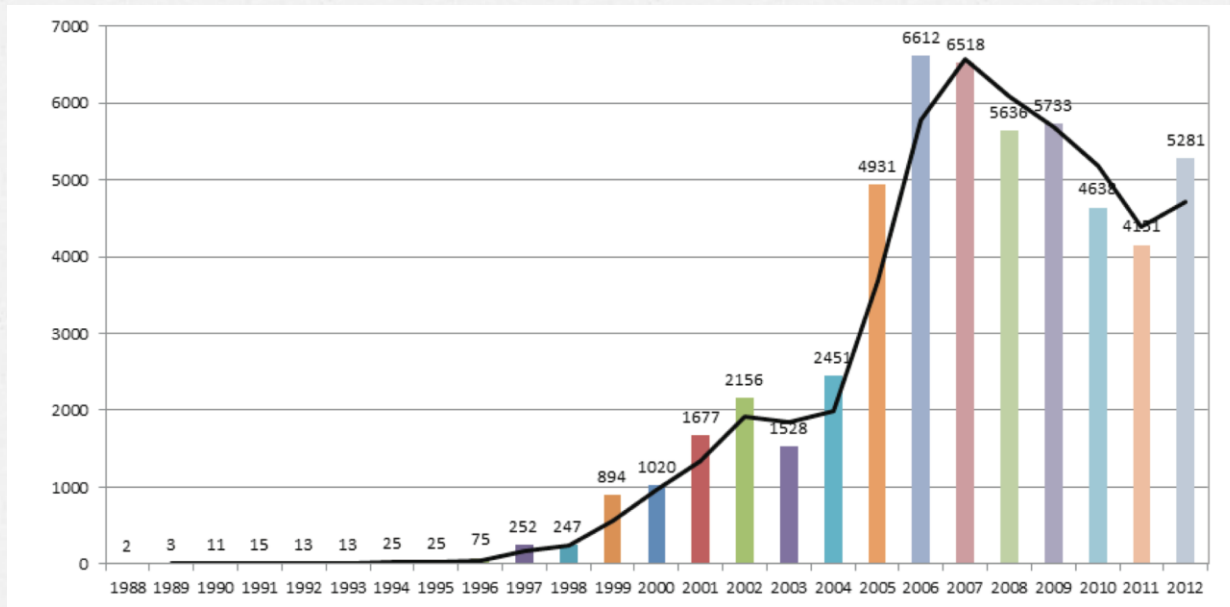
OSS and Security

- o Do you use OSS securely?
 - o Secure configuration
 - o Patch management
 - o Old version
 - o non-active OSS
- o Secure OSS development
 - o Secure coding
 - o Vulnerability handling



Vulnerability

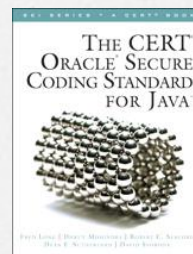
- o Root problems of most cyber security incidents



Source: 25 Years of Vulnerabilities: 1988-2012 by sourcefire

Vulnerability (cont.)

- To against vulnerability:
 - Secure coding (for developers)
 - Secure configuration
 - Security operation
 - Patch management



OSS Security tools

KALI LINUX®



argus

skipfish



metasploit®

OSS Security tools (cont.)

- o There are a lot of useful tools are available
 - o commercial level software are also there
 - o attacker are also using those tools...
 - o Know your enemy?
- o OSS security tool community
 - o different motivation from other OSS softs
 - o useful to share knowledge and information
 - o more security experts

Owing your own security team

- o Computer Security Incident Response Team
 - o A concept to have security professional team within an organization
 - o Become a center of security issues
 - o National level CSIRT is widely known
 - o CNCERT/CC, JPCERT/CC, KrCERT/CC
 - o Closely work together, help each other
- o Dedicated team is needed for high performance security initiatives.

Conclusion



Vulnerability



Security tools



CSIRT