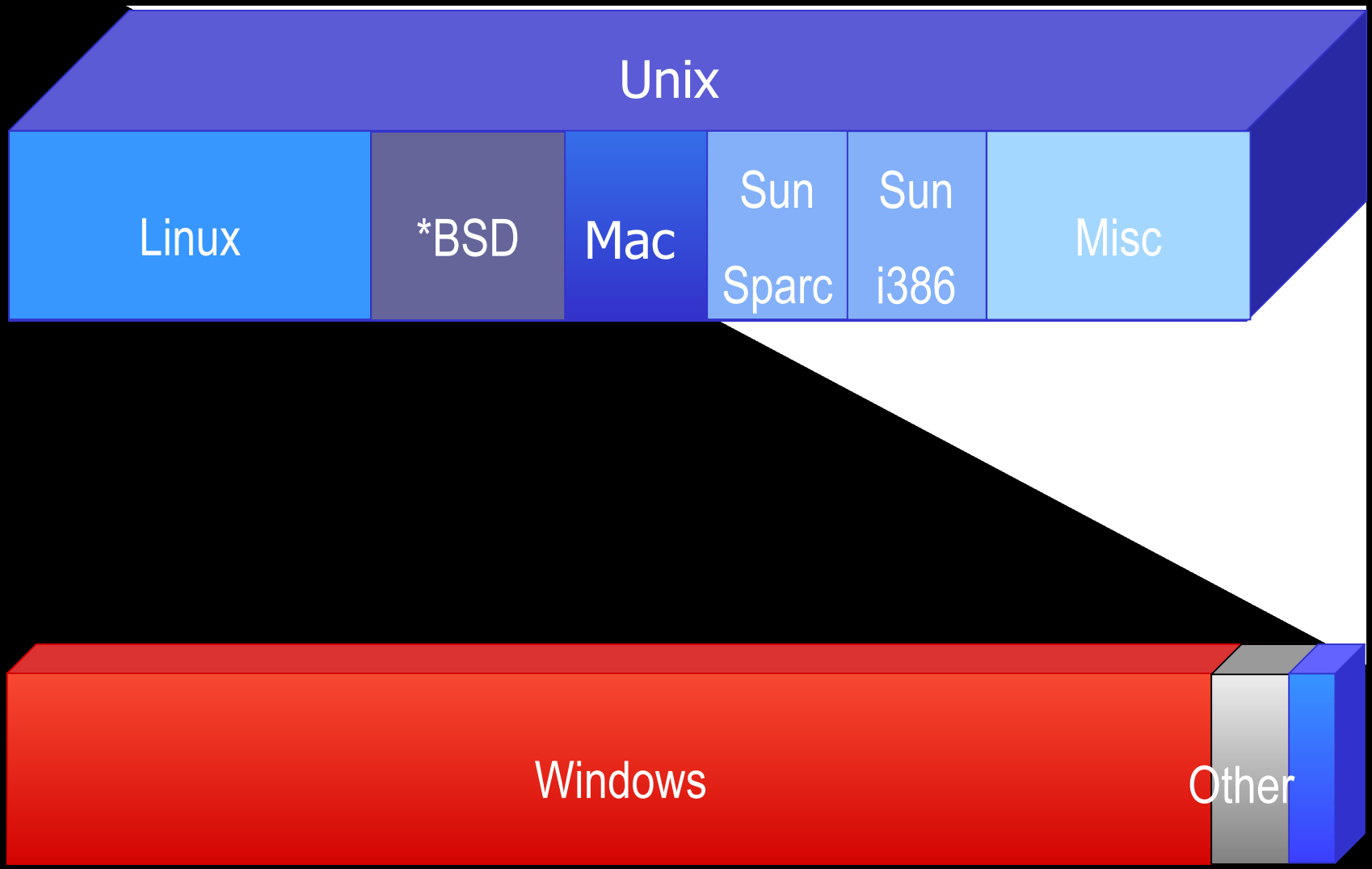
Analysis and Replication of Unix Malware ("The other white meat")

Patrick L. Knight
Authentium, Inc

Introduction

Virus Collection Breakdown



Unix Malware File Types

- ELF/Mach-O native executable format
- Dynamic/Shared object libs
  - .so
  - .dylib
- Shell scripts (BASH, TCSH, CSH, etc.)
- Perl and Python scripts
- HTML, JS, PHP
- Java classes

Attack Vectors

Vulnerable/poorly configured services:

- httpd, PHP (directory traversal, XSS)
- sshd (weak passwords)
- Telnet, ftpd (weak/cleartext passwords)
- portmap (buffer overflows)

HTTP attack signatures

[**] [1:1122:2] WEB--MISC /etc/passwd [**]

[**] [2001785] BLEEDING-EDGE EXPLOIT PHP

```
GET ../../../etc/passwd%00 HTTP/1.0

GET /cgi-bin/blahblah/../some.cgi HTTP/1.0

GET %65%74%63/%70%61%73%73%77%64 HTTP/1.0
```

SSH scan signatures

[**] [1:1012:3] SSH --> BLEEDING-EDGE Potential SSH Scan

```
Jul 14 02:12:19 test sshd[47297]: Illegal user admin from 10.1.1.10
Jul 14 02:12:25 test sshd[47299]: Illegal user test from 10.1.1.10
Jul 14 02:12:30 test sshd[47301]: Illegal user guest from 10.1.1.10
Jul 14 02:12:41 test sshd[47305]: Illegal user mysql from 10.1.1.10
Jul 14 02:12:45 test sshd[47307]: Illegal user oracle from 10.1.1.10
Jul 14 02:12:50 test sshd[47309]: Illegal user library from 10.1.1.10
Jul 14 02:12:54 test sshd[47311]: Illegal user info from 10.1.1.10
Jul 14 02:12:59 test sshd[47313]: Illegal user shell from 10.1.1.10
```

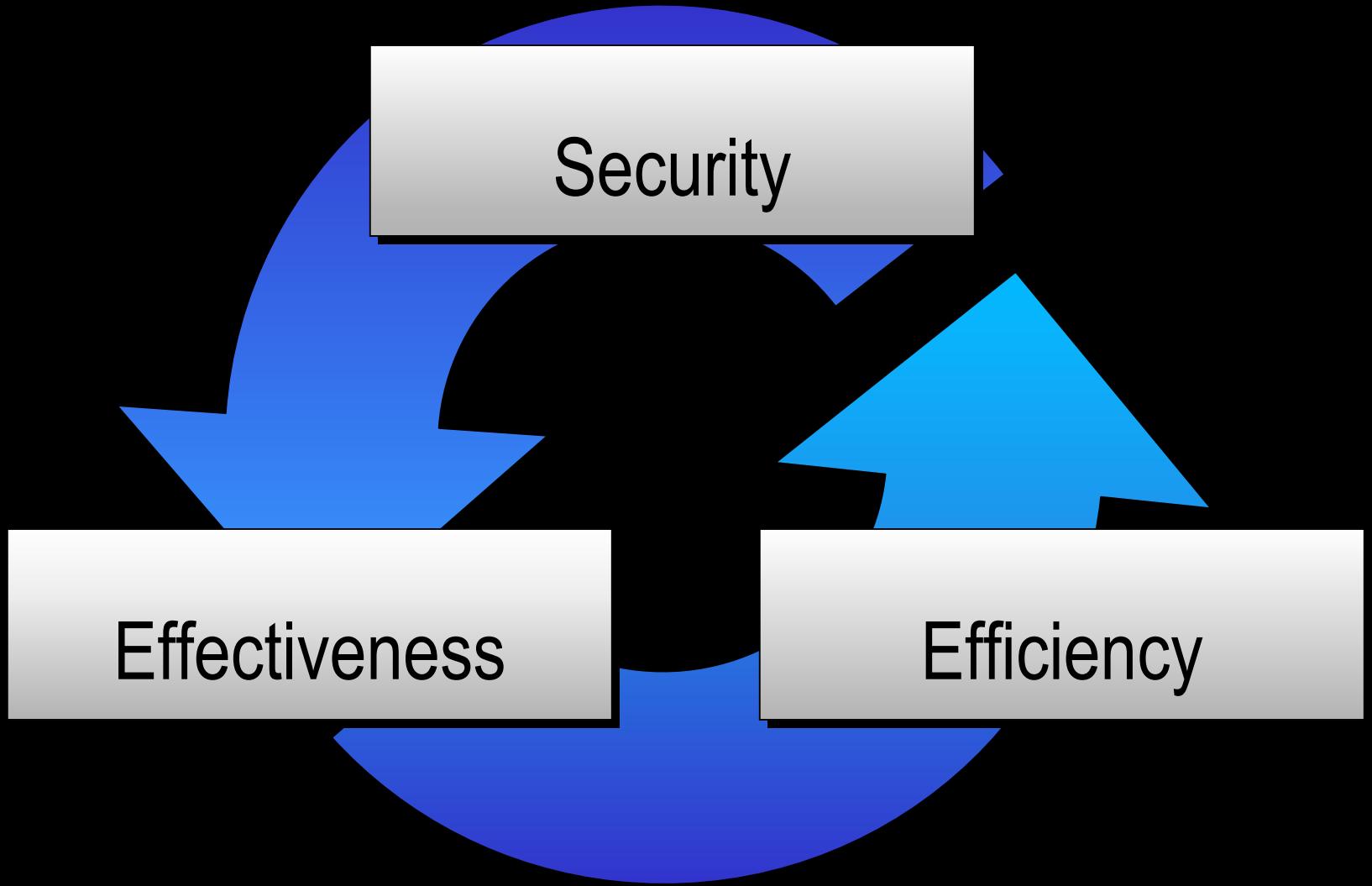
Attack Vectors

Social Engineering

- Not much
- some mass-mailers
- phishing sites not usually geared toward the Unix user

Paper Overview

- Replication Environment Setup
- Analysis of an ELF Sample (Unix/Kaiten.AD aka Backdoor.Linux.Keitan aka Tsunami)
- Anti-AV Techniques used by malware authors


Security
Effectiveness
Efficiency

Anti-AV Tactics

Packers/Obfuscators

- UPX (upx.sf.net)
- decryfile (Phrack 58)
- build-your-own packer libs

Debugger/strace detection

- detection with ptrace()

Virtual Machine detection

Binary Packers/Obfuscators

UPX is still the major packer for Unix

- supports Linux ELF/AMD64/ppc32, vmlinuz/386, MAC OS X Mach-O/ppc32
- decompresses directly to memory
- command-line app usually unpacks samples with no problems
- Watch for edited UPX strings

UPX on Linux

Older versions have unpacked sample running in memory accessible from **`/proc`**

- get PID from '**`ps`**'
- copy sample from **`/proc`** directory

This *may* work with other packers

Packers and `/proc` filesystem

```
# ps ax | grep sample
5731 ?        Ss   0:00 sample

# ls -l /proc/5731/exe
lrwxrwxrwx 1 root root 0 Aug 29 23:14 \
/proc/5731/exe -> /tmp/upxDJDSAXFO50

# cat /proc/5731/exe > ~/sample.unp
```

Binary Packers/Obfuscators

decryfile (Phrack 58, 0x05)

- crashes on current Linux platforms

- possible source for custom cryptors

Virtual Machine Detection

- Known VMWare hardware address prefixes

  `00:05:69, 00:0C:29, 00:50:56`

- VMWare tools

  Adds easily-locatable files in **`/bin`**, **`/etc`** and **`/lib`**

- Redpill test

Hardware Address Check

```
struct ifreq  if_hw;
int           s;

s = socket(AF_INET, SOCK_DGRAM, 0);
strcpy (if_hw.ifr_name, "eth0");
ioctl (s, SIOCGIFHWADDR, &if_hw);

return if_hw.ifr_hwaddr.sa_data;
```

Redpill test

- http://invisiblethings.org

- Intel-specific test queries IDT register

- detects hosts running in VMWare
  and Virtual PC

Redpill test results

VM	Linux/VMWare	WinXP/VMWare	WinXP/Virtual PC
FreeBSD 4.9	X	X	X
FreeBSD 5.2.1	X		
Redhat 6.2	X	X	
Redhat 9	X	X	X
Solaris 8	X		
Solaris 10	X	X	
WinXP			X

Redpill test failures

- some flakiness on Windows host, even after VM powered off
- sometimes crashes on Fedora Core 2/4 w/ distro kernels
- only test with xen, the redpill test crashed
- does not detect applications running in Wine
- did not attempt test on 64-bit machines

Unix Rootkits

Unix Rootkits (Kernel Mode)

- adore for BSD – mucks up FreeBSD 4.9 process tables
- adore-ng on Linux 2.6 kernels (but not current kernels)
- linux kernels not all the same due to vendor patches
- linux 2.6 kernel enhancements thwarting malware behavior (e.g. stack randomization, sys_call hooking, memory mapping)

Unix Rootkits (User Mode)

- Continued use of trojaned network services and system apps
- Attack vectors consist mostly of vulnerable or poorly-configured network services
- Where are HIDS/ACLS?

Trojaned Shared Libraries

Simple Shared Library Analysis

```
# nm -a libsuspicious.so
         U dlclose@@GLIBC_2.0
         U dlopen@@GLIBC_2.1
         U fclose@@GLIBC_2.1
         U fread@@GLIBC_2.0
         U fseek@@GLIBC_2.0
         U fwrite@@GLIBC_2.0
         U Cryptor
```

Replicating Trojaned Shared Libraries

```
void *lib, *function;

lib = dlopen (“libsuspicious.so”, \
RTLD_LAZY);

function = dlsym (lib, “Cryptor”);

function();
```

File Infectors

- Usually target a specific file type (e.g. ELF, .html)
- Sometimes infect successfully; sometimes not
- Can infect your analysis tools
- Use hash database on another drive/partition to verify

Unix Malware Trends?

- Access through network-based attacks
- Use of userland rootkits/trojaned applications
- Custom jobs
- Mac OS X and Linux targets of choice
- More ?*better*? kernel mode rootkits
- Cross-platform viruses (Linux.BI.A or unix-unix)
- Hypervisor rootkit for Unix?

GNU tools for Unices

http://www.sunfreeware.com (Solaris/Intel)

http://www.freebsdsoftware.org (FreeBSD)

http://developer.apple.com (Mac OS X)

http://freeware.sgi.com (Irix)

Questions ?

Contact

Email: securehell@hushmail.com

MSN: securehell@hotmail.com

PGP ID: EA4BD471