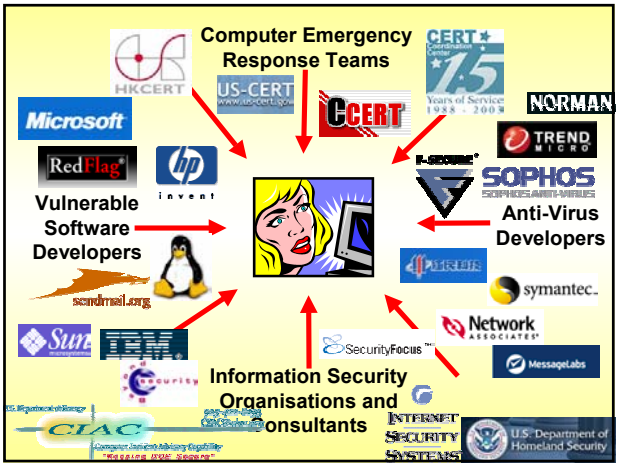
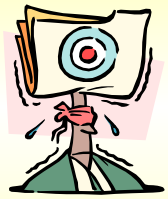
How Soon Do You Want To Know?

Allan G. Dyer
CISSP, MHKCS, MIAP, AIDPM, MSc (tech), BSc
Chief Consultant, Yui Kee Computing
President, AVAR
adyer@yuikee.com.hk



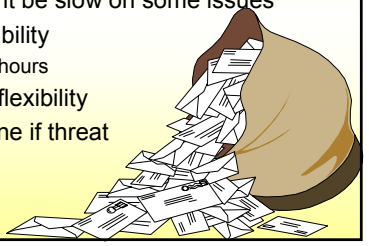
Too Many Sources?

- Free / Subscription
- Relevant?
- Complete?
- Timely?



Alert Problems

- Too Many Sites to monitor
- Too time-consuming to visit sites frequently
- Not always checking email
- Single source might be slow on some issues
- Lack of timing flexibility
  - Timezones, office hours
- Lack of alert level flexibility
- Difficult to determine if threat applies



YKAlert

- Website Monitoring Service
  - Originally developed for internal use
  - Running > 2.5 years
- Sends alert on interesting change
  - email
  - SMS
- XML based
- Highly Configurable

Humble Beginnings

- Problem:
  - Tender requirement
  - Monitor list of AV websites during office hours, take action on important alerts
- Solutions
  - Manual
  - Scripts

First Iteration

- Schedule using crontab

```
0,15,30,45 7-19 * * mon-fri /home/check/bin/check
0,15,30,45 7-12 * * sat     /home/check/bin/check
```

- Use Perl, LWP::Simple for web download
  - Download list of pages
  - Compare with stored copies, using diff
  - Extract alert information with regular expressions
  - Pipe output to mail

Wrong Approach!

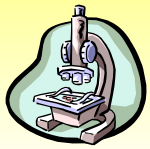
Finding the Alerts

- diff:
  - Looses the context information
  - Difficulty with multi-line alerts
- Better approach:
  - Use regular expressions to find the alerts
  - Compare the alerts

Site Processing

- Specific routine for each site
- Sites (occasionally) change structure
- Moved into own Perl module
  - eval routine to catch:
    - Expression errors
    - Infinite loops (watchdog timer)
- Now stored as XML

Alert Storage



```
<alerts>
  <alert level="L3"
   url="http://www.sarc.com/avcenter/venc/data/w32
   .mimail.c@mm.html" title="W32.Mimail.C@mm"
   modified="1067641374" />
  <alert level="L1"
   url="http://www.sarc.com/avcenter/venc/data/w32.
   jermy.a.html" title="W32.Jermy.A"
   modified="1067298437" />
</alerts>
```

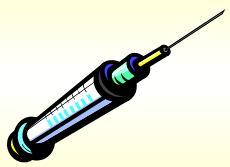
Character Sets

- ASCII, Big5, GB2312
- Convert to UTF-8 for storage and comparison
- Convert according to destination's preference when sending

Comparing Alerts

- Matching titles
- Comparison is site specific
  - F-Secure: 3, 2, 1
  - SARC: 1, 2, 3, 4, 5
  - Trend: Low, Medium, High
- Send alert when:
  - ≥ target level

  AND
  - > previous level
- Problem: "Top five" list
  - A virus may drop off the bottom and reappear because of a short outbreak of something else
  - Persistence: remember the last observed level for comparison



Depth

- Alert level not always on the list page
- Follow links
- Filter routine for the linked pages
- Could proceed for any depth
  - Not yet necessary

http://www.f-secure.com/

F-Secure

- Radar Levels listed in individual virus descriptions
- Radar Levels also in comment on main webpage:

```
<td width="95%"><h4><small><a href="/v-
descs/sober.shtml">Sober worm going
around</a></small></td>
   </tr>
<!-- Summary
Radar : 2
October 26, 2003 :

// -->
```

Store

- Keep pages & alerts for 1 month
  - Subdirectory for each time point
- Can compare any interval
- Useful for troubleshooting
  - Troubled by repeating alerts
  - site was served from two webservers: out of sync.
- Disk space requirements large
  - Esp. when following links
  - Use MD5 checksums & symbolic links

Error Reporting

- Errors written to a status alert file
- YKAlert monitors itself
  - Missing html files
  - Site routine errors
  - Site routine infinite loops
  - No alerts found
  - etc…

Simultaneous Requests

- Problem: Duration is sum of download times
- Solution: download queue and multiple download processes

XML Configuration

```
<webalert service="YKVAlert"
    store="/home/webalert/virus"
    proxy="http://proxy.yuikee.com.hk:8080"
    sender="ykalert@yuikee.com.hk"
    subject="YKVAlert"
    tail="&lt;p&gt;&lt;a href='http://www.yuikee.com.hk/info-
  ctr/YKVAlert.html'&gt;Abbreviations&lt;/a&gt;"
    module="Virus"
    statusfile="/home/webalert/status/current/alert/virus-
  alert.alert"
    maxthreads="4"
    destinationstore="/home/webalert/cfg/virus">
<webalert>
```

Site Configuration

```
<site url="http://www.sarc.com/avcenter/vinfodb.html"
    baseurl="http://www.sarc.com"
    localfile="sarc"
    shortname="SARC" />
<site url="http://www.jiangmin.com/exec/virusinfo/index.asp"
    baseurl="http://www.jiangmin.com"
    localfile="jiangmin"
    shortname="JIANGMIN"
    encoding="GB2312" />
```

Site Configuration

```
<site url=
  "http://ww3.messagelabs.com/data/flashmovies/data/snapshot/snapshot.txt"
    baseurl="http://www.messagelabs.com/"
    localfile="messagelabsss"
    shortname="MLss" />
<site url=
  "http://ww3.messagelabs.com/data/flashmovies/data/topfive/topfive.txt"
    baseurl="http://www.messagelabs.com/"
    localfile="messagelabstop"
    shortname="MLtop"
    persistent="Y" />
```

User Configuration

```
<webalert>
 <destination address="adyer@yuikee.com.hk" format="long"
     output="html" encoding="Big5"
     content-transfer-encoding="base64">
 </destination>
 <destination address="97455866" method="SMSq" format="short"
     structure="1" encoding="Big5" >
   <site shortname="TREND" target="medium"/>
   <site shortname="NAI" target="medium"/>
   <site shortname="SARC" target="L3"/>
   <site shortname="NORMAN" target="medium"/>
   <site shortname="JIANGMIN" target="2"/>
   <site shortname="MLss" target="8000,20,100"/>
   <site shortname="MLtop" target="medium"/>
   <site shortname="SOPHOS" target="2"/>
 </destination>
</webalert>
```

Delivery

- Email: LWP::Simple
- SMS
  - Public email → SMS gateway
    - Free, Now closed
  - Mobile Operator XML → SMS service
    - Tested OK
    - Expensive charging
    - Internet dependant
  - Gnokii

Gnokii

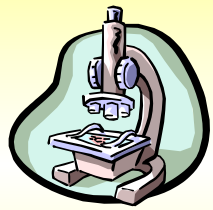
- GPL driver for Nokia mobile phones
- Connect phone using serial cable
- Speed limited by mobile network response
  - ~8 messages / minute
- 3 methods
  - XML → SMS
  - Direct library calls
  - Queued
    - Separate process sends messages
    - Can add more phones & processes

Current Services

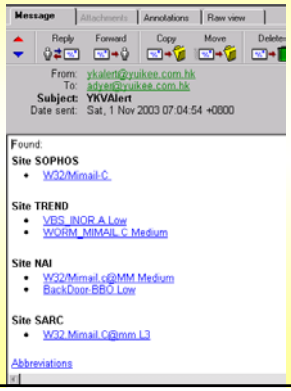
- YKVAlert
- YKSAlert
- Others

YKVAlert

- Monitors Virus Alert Webpages
  - Symantec
  - Trend Micro
  - Network Associates
  - F-Secure
  - Sophos
  - MessageLabs
  - Norman
  - Computer Associates
  - HKCERT/CC
  - Jianmin
  - Beijing Rising
- Configure alert levels by site and destination



Messages



Scheduling

- 15 minute checking interval
  - 24 x 7
  - "Extended Office Hours"
    - 7am - 7pm Mon - Fri
    - 7am - 12am Sat
- Summary
  - 4 messages daily
- Choose your own

YKSAlert

- Monitors Security Webpages
  - CERT/CC
  - Security Focus
  - CIAC
  - NIPC
  - SecuriTeam
  - X-Force
  - CCERT

Other Monitoring

- Testing / Internal use
- YKAlert
  - Reports problems
- Weather (HK Observatory)
  - Mobile operators provide similar service
- Zone-H - Defacements
- World Cup Scores
- Newspapers
  - Requires deeper scanning and intelligent keyword processing to be really useful

YKAlert Users

- Internally
- A CERT
- Independent Consultants
- A small number of Commercial Organisations

FAQ

- Understanding the Abbreviations?
  - Link to definitions in HTML
- Multiple Alerts for one problem?
  - Yes
  - Comparison of sources' rating
  - Rough idea of sources' speed

Comparable Services

Not a comprehensive list

- CERT/CC
- HKCERT/CC
- Microsoft
- F-Secure
- Jiangmin
- Network Associates
- Sophos
- Symantec
- Security Focus

CERT/CC Resources

- Mailing List
  - majordomo@cert.org
- WAP Site
  - http://wap.cert.org/
  - Current Activity, Advisories
- RSS Channel
  - –http://www.cert.org/channels/certcc.rdf

HKCERT/CC Other Resources

- Mailing List
  - hkcert@hkcert.org
- SMS Alerts
  - https://www.hkcert.org/subscribe/smsalert.html

Microsoft

- Email Alert
  http://register.microsoft.com/subscription/subscribeme.asp?id=166

F-Secure

- F-Secure Radar
  - Four Alert Levels
    - Level 1: Worldwide epidemic
    - Level 2: New virus, large infections
    - Level 3: New technique or platform, might not be widespread
    - No number: No current alert for the virus
  - Delivery methods: Phone, Fax, Pager, Mobile Phone, Email, SMS
  - Annual Subscription

Jiangmin

- SMS Virus Alerts
  - Free registration
    - http://sms.jiangmin.com/register.asp
  - Charged 0.3□ per message
  - Options for Virus alerts, security alerts, summaries etc.
  - Must be a customer of□□□□

Network Associates

- AVERT Virus News
  - http://vil.nai.com/vil/join-list.asp
  - Free Email service
  - Message when virus is Low-profiled or above
- PrimeSupport
  - Subscription service
  - Includes alerts and other support

Sophos

- Email Notification
  - http://www.sophos.com/virusinfo/notifications/
  - IDE notification for new viruses in the wild
  - Emergency information
  - Sophos enews
  - Support news
- RSS Channel
  - http://www.sophos.com/virusinfo/infofeed/rss_index.html

Symantec

- Email Alert
  - Free
  - http://nct.symantecstore.com/virusalert/
- DeepSight
  - Subscription services
  - http://enterprisesecurity.symantec.com/SecurityServices/content.cfm?ArticleID=1522
  - Threat Management System - incident & attack info
  - Alert Services - vulnerability alerts

Security Focus

- Mailing Lists
  - http://www.securityfocus.com/archive
  - 32 security-related lists
- RSS Channels
  - http://www.securityfocus.com/rss/index.shtml
    - Vulnerabilities
    - Bugtraq
  - 48 hour delay on free vulnerability channel

YKAlert Future

- Multiple site fail-over
- Secure user self-configuration
- WML output option
- RSS Channel
- Support for Chinese SMS

Future

- More sites monitored
- Increasing number of threats
- … More alerts
- Not "How soon do you want to know?"
  - "Immediately!"

"What Do You Want To Know?"

- A Decision is Required
- An Action is Required
- Supporting Information

How to Filter?

- Know about the Threat's Profile and Effects
- Know about the Recipient's Systems & Policies
- Alert when there is a match

Categorising the Threats

- Platform / Application
  - No standard way of describing the affected systems
- Matching Information from Multiple Sources
  - No standardised virus names
  - Many Vulnerability Numbering schemes

CERT/CC Resources

- Vulnerabilities, Incidents & Fixes
  - News items
  - http://www.cert.org/nav/index_red.html
- Advisories
  - "limited to vulnerabilities that meet a certain severity threshold"
  - http://www.cert.org/advisories/
- Current Activity
  - "summary of the most frequent, high-impact types of security incidents currently being reported "
  - http://www.cert.org/current/current_activity.ht

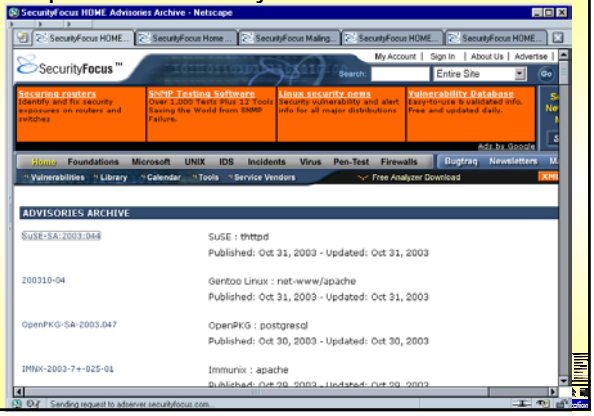
CERT/CC Numbering

- Advisories
  - CA-*year-number*
  - CA-2003-09 :Buffer Overflow in Core Microsoft Windows DLL
- Vulnerability Notes
  - VU#*number*
  - VU#575892 Buffer overflow in Microsoft Messenger Service
- Incident Notes
  - IN-*year-number*
  - IN-2003-03: W32/Sobig.F Worm
- Summaries
  - CS-*year-quarter*
  - CS-2003-03

Microsoft

- Security Bulletins
  - MSYY-XXX *year*, *number*
  - Knowledge Base Articles (KB*number*) now refer to Security Bulletins
  - http://www.microsoft.com/security/security_bulletins/
  - Released 2nd Tuesday each month
- Product Security Bulletin Summaries
  - Microsoft <product family name> Security Bulletin Summary for <month> <YYYY>

http://www.securityfocus.com/advisories



Security Focus

- Bugtraq
  - Full Disclosure
  - Numeric ID's
- Vulnerabilities
  - Announcer's ID:
    - Announcement-ID: SuSE-SA:2003:044
    - Advisory ID: IMNX-2003-7+-025-01
    - Reference: a102803-1

US Department of Energy Computer Incident Advisory Capability (DOE-CIAC)

- Bulletins and Advisories
  - *letter-number*
  - Fiscal Year 2003 (N Series)
    - N-132: Wu-ftpd Buffer Overflow Vulnerability (July 31, 2003)
  - Fiscal Year 2004 (O Series)
    - O-005: Microsoft Exchange Server Vulnerabilities (October 15, 2003)
- C-Notes
  - computer security articles and information
  - less time critical nature
  - http://www.ciac.org/cgi-bin/cnotes

Common Vulnerabilities and Exposures (CVE)

- Assigns identifiers to vulnerabilities and exposures
- Useful for cross-referencing other resources
- Candidates: CAN-*year-number*
  - Assignment of CAN number takes 1 day - 1 month
- CVE: CVE-*year-number*
  - CAN → CVE minimum 2 weeks
- CVE versions released quarterly

CVE

- A dictionary **not** a database
- Distinguishes between:
  - Vulnerabilities ("universal vulnerabilities")
    - a vulnerability under any commonly used policy
    - e.g. phf (remote command execution as user "nobody")
  - Exposures
    - A vulnerability under some reasonable policies
    - e.g. running services such as finger (useful for information gathering, though it works as advertised)
- Does not include or name viruses
  - Recognises they are vulnerabilities
  - Chooses not to include them
  - Leaves naming to the anti-virus community

Knowing About the Recipients Systems

- List the OS's
  - and versions
  - and service packs…
- List the Applications
  - and installation options…
- Many administrators don't know
  - e.g. Slammer
  - Add the dependencies
- Checksum everything executable?
  - Add all the configuration info…

Rather Reactive?

- Shouldn't we be Proactive?

Questions?

Other Modules

- use bytes;
- use strict;
- use LWP::Simple qw(mirror is_success status_message $ua);
- use MIME::Base64;
- use MIME::QuotedPrint;
- use Getopt::Std;
- use XML::Simple;
- use Data::Dumper;
- use Sys::Syslog;
- use Digest::MD5;
- use YuiKee::charconv;
- use YuiKee::Alert;
- use YuiKee::AlertDelivery;

Computer Emergency Response Teams

- CERT/CC
- HKCERT/CC
- CNCERT/CC
- CCERT
- US-CERT

http://www.cert.org/nav/index_red.html