



Anatomy of a Malware Attack

The New Malware Ecosystem

Tom Bowers
Senior Security Evangelist

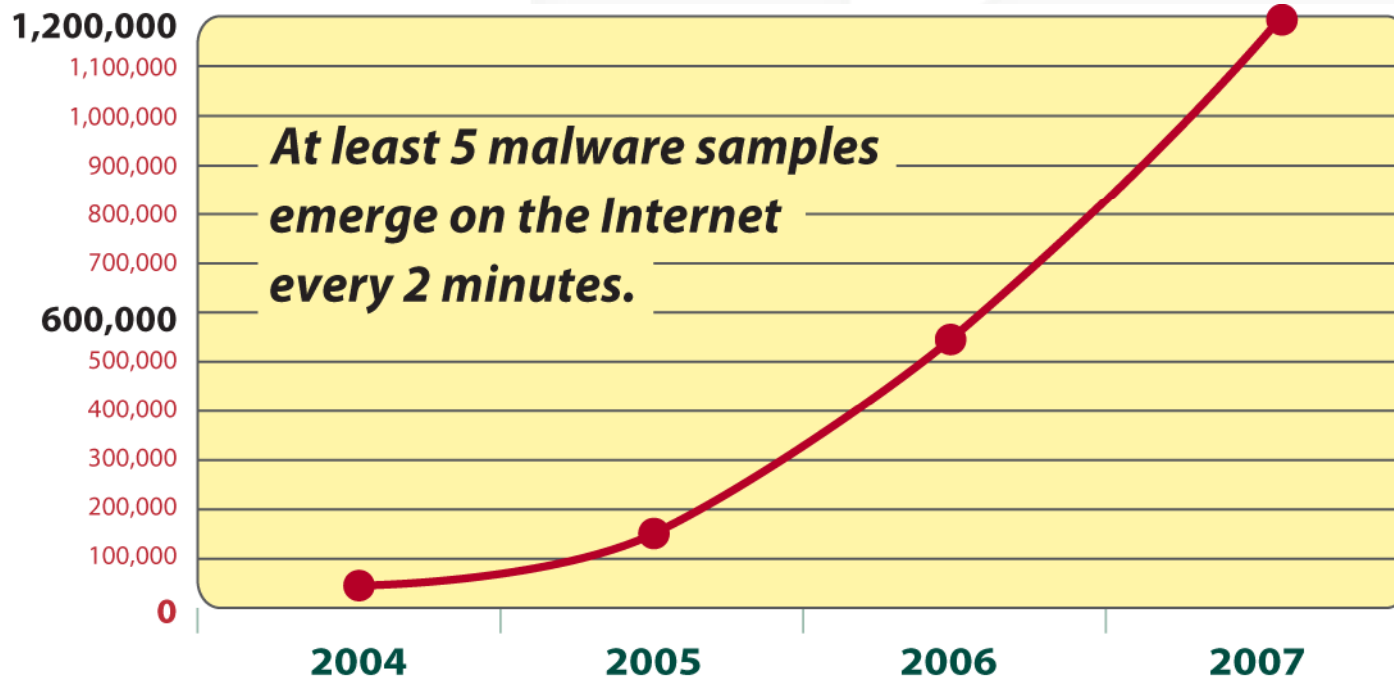
April 29, 2008

INTEROP[®]
LAS VEGAS | APRIL 27–MAY 2, 2008

Introduction

- Malware growth rates
- Evolution from nuisance to monetized threat
- Malware as a business
- Malware Ecosystem

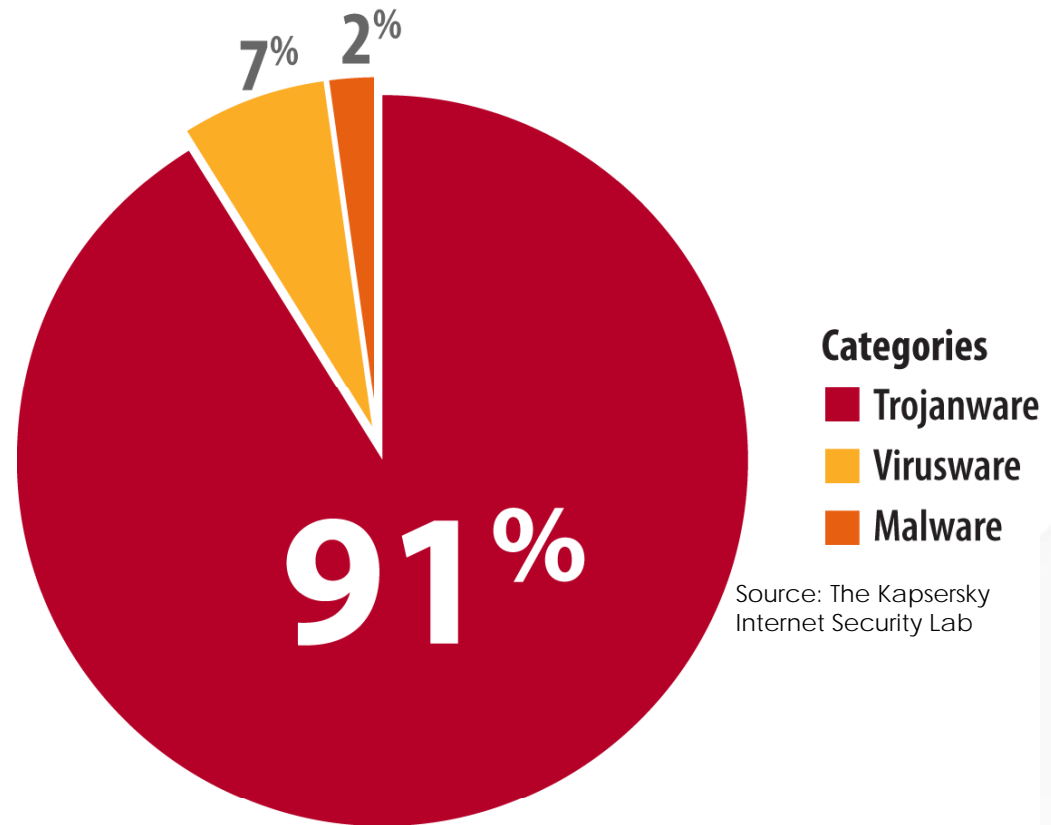
Malware Samples per Year



Source: The Kaspersky Internet Security Lab

What We Are Seeing

Distribution of Malware Categories in the First Half of 2007



Source: The Kaspersky Internet Security Lab

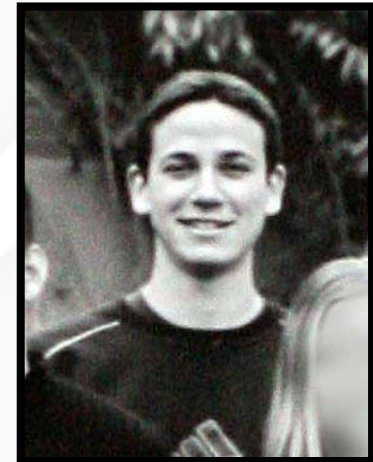
The Rogues' Gallery – The Script Kiddies



Chen Ing-Hau
Age 24 (Taiwan)
Arrested
September 21, 2000
for the CIH virus



Jeffrey Lee Parson
Age 18 (USA)
Arrested
August 29, 2003
for the Lovesan.b virus



Sven Jaschan
Age 18 (Germany)
Arrested
May 7, 2004 for
NetSky and Sasser viruses

The Rogues' Gallery – Two-Bit Thieves



Jeanson James Ancheta
Age 20 (USA)

Arrested November 3, 2005 for creating zombie networks and leasing them for spam mailing and DDoS attacks on websites



Farid Essebar
Age 18 (Morocco)

Arrested on August 26, 2005 for creating zombie networks using Mytob and Zotob (Bozori) worms



Atilla Ekici
Age 21 (Turkey)

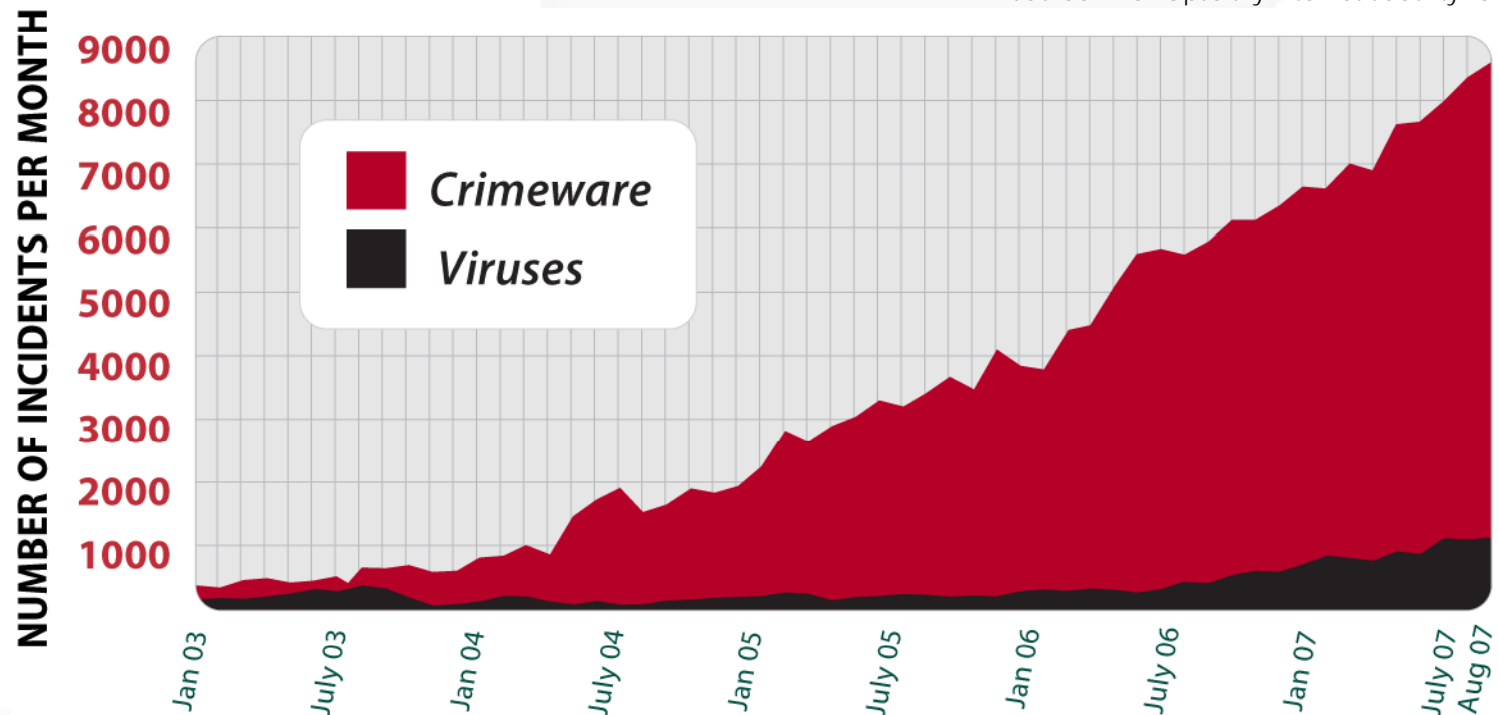
The Rogues' Gallery – Big Business

- Yaron Bolondi, aged 32 (Israel)
- Attempted to withdraw £220 million (more than \$420 million in 2005) from the bank's accounts the network of a London branch of Sumitomo Bank
- Arrested March 16, 2005



Criminal Attacks on the Rise

Source: The Kaspersky Internet Security Lab

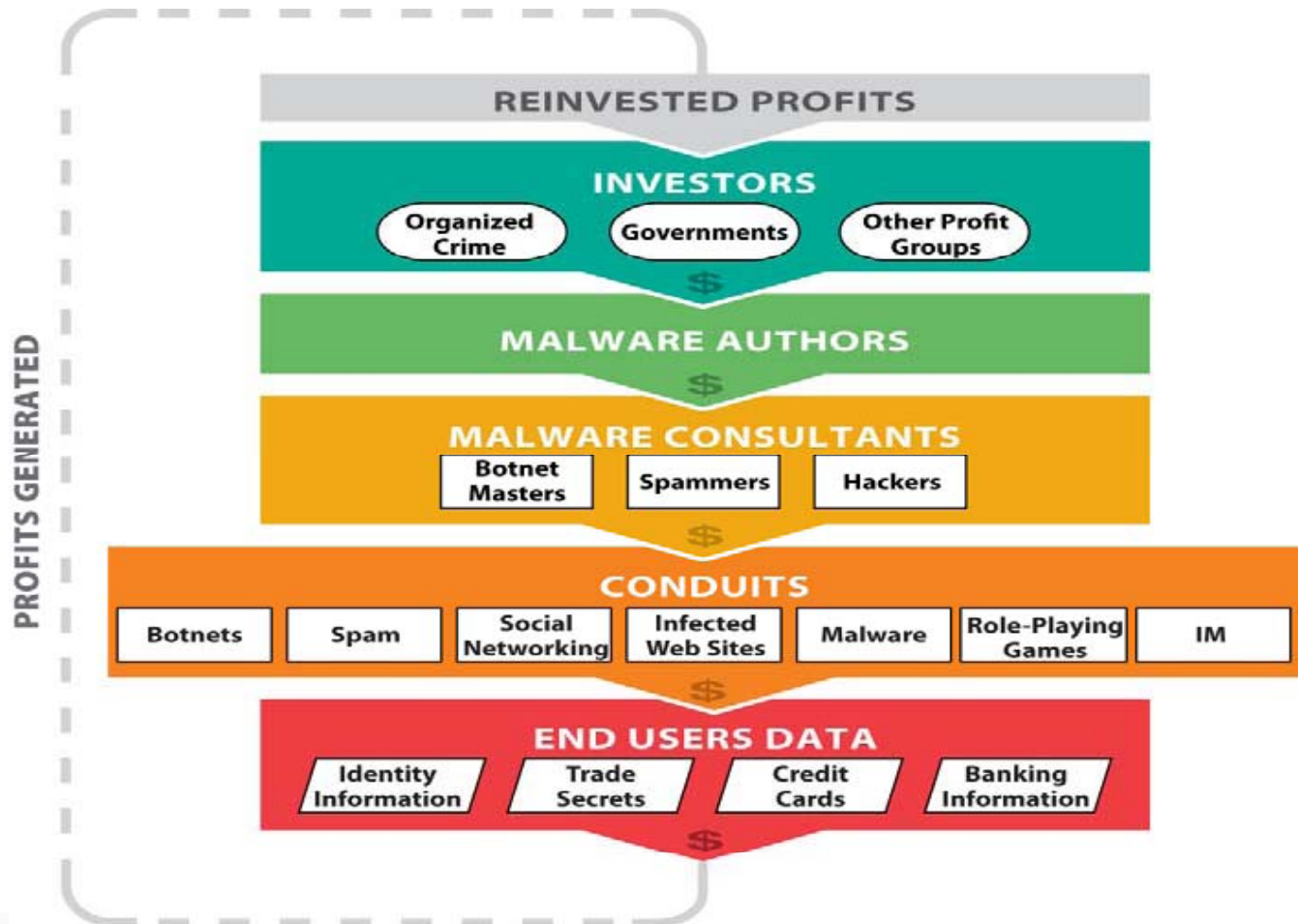


A Great Low Risk Business

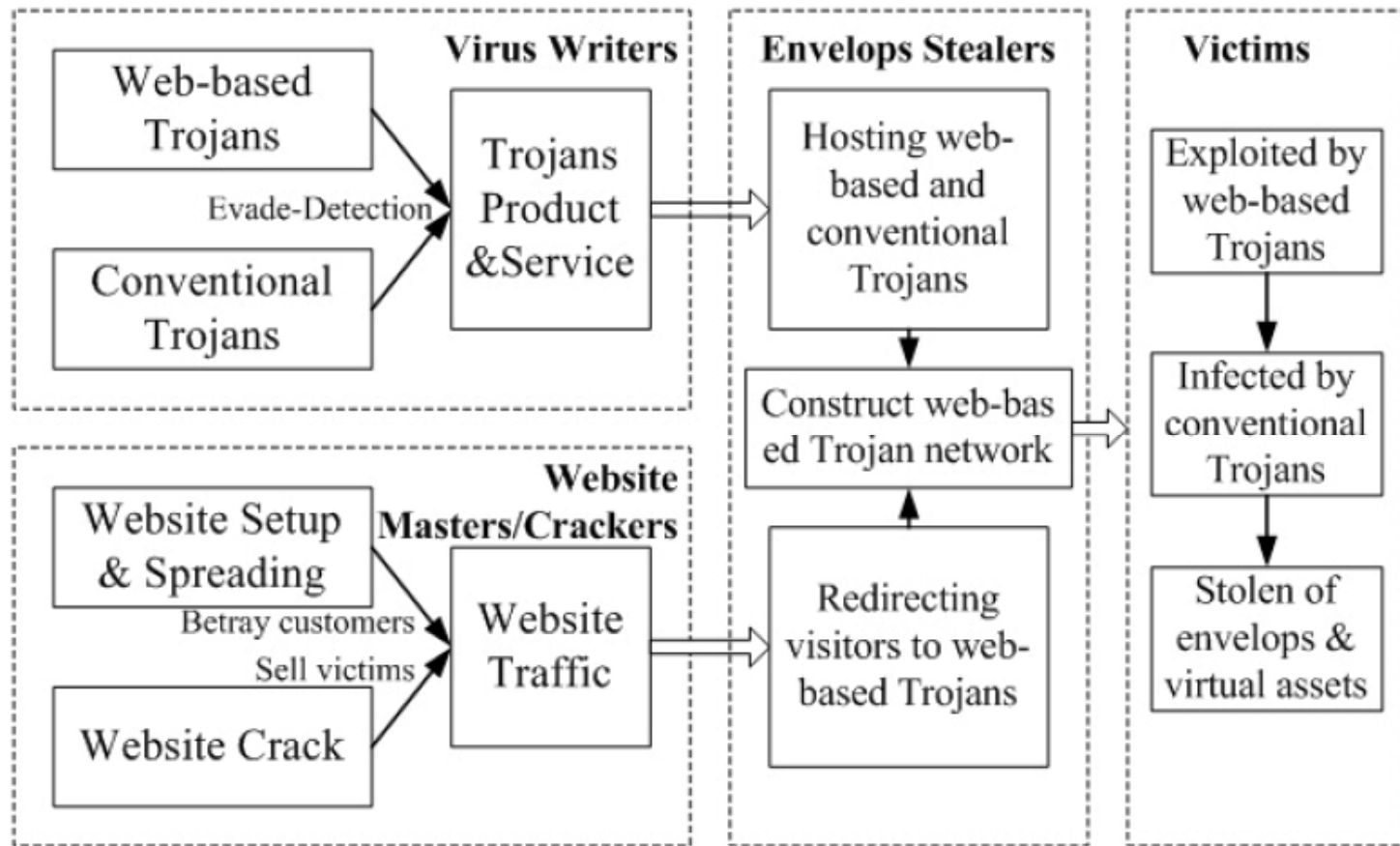
Cybercriminals feel relatively safe because:

- There are gaps in legislation
- Law enforcement understaffed and under-equipped
- Victims rarely inform police about crimes.
- Insignificant damages – incidents are not interesting to police (despite the huge number of these crimes)
- The crimes are international

Malware Ecosystem



Chinese Underground



Source: TR-2007-011: Reihe Informatik. December 3, 2007

Malware Business Portal

PROFESSIONAL SOCKS 4/5 SERVICE

LOGIN: PASSWORD:

HOME TARIFS LOGIN

Tariff Rates

| Daily plans *** | | | | | | Per Use plans | | | | | |
|-----------------|----------------|---------------|-------------|----------------------|--------------|---------------|---------------|-------------|----------------------|--------------|--|
| 1 Proxy Price | Daily Limit ** | Monthly Price | Tariff Name | Quantity Per Month * | Proxy Helper | 1 Proxy Price | Monthly Price | Tariff Name | Quantity Per Month * | Proxy Helper | |
| 0.13¢ | 5 | \$20 | Daily 5 | 150 | \$10 | 0.50¢ | \$9.95 | PerUse 1 | 20 | \$10 | |
| 0.11¢ | 10 | \$35 | Daily 10 | 300 | \$10 | 0.30¢ | \$15 | PerUse 2 | 50 | \$10 | |
| 0.08¢ | 20 | \$50 | Daily 20 | 600 | \$10 | 0.25¢ | \$20 | PerUse 3 | 80 | \$10 | |
| 0.07¢ | 30 | \$65 | Daily 30 | 900 | free ! | 0.15¢ | \$29.95 | PerUse 4 | 200 | \$10 | |
| 0.06¢ | 50 | \$95 | Daily 50 | 1500 | free ! | 0.10¢ | \$50 | PerUse 5 | 500 | free ! | |
| 0.05¢ | 75 | \$125 | Daily 75 | 2250 | free ! | 0.07¢ | \$69.95 | PerUse 6 | 1000 | free ! | |

* Quantity of proxies, involved in monthly payment.
 ** Quantity restriction on proxies which you can use for a day
 *** Tariffs have a refund system implied to a proxy that goes dead while work

PAYMENT IS ACCEPTED VIA : [Webmoney](#), [Egold](#)

[Support \(only in English\)](#) & demo accounts: **ICQ : 555019, 990100**

Terms of Service

Peculiar Properties of Tariff Rates :

per use:
 The **Per Use Tariff Rate** includes one month payment; the payment involves a certain amount of proxy servers which you can take from the base as many as you wish without any restrictions. If you have not used the proxies included in the monthly payment, these proxies are not extended to the next month. In these Tariffs you can see all proxies which are online at a moment .

Daily:
 The **Daily Tariff Rate** includes one month payment; the amount of proxy servers which you can take from the base within 24 hours is limited in your Tariff Rate-related quantity. With these Tariff Rates, you can see all proxy servers which are online at a moment. If the system finds out for the first 10 minutes* of using a proxy that the proxy has stopped responding, this proxy will not be billed, and the system will automatically refund you . **

* Typically, this time is enough to see if a proxy can go on working
 ** At present the system is working in a test mode

Information about Proxy Helper:
[Proxy Helper manual \(ENGLISH VERSION\)](#)

PROHIBITED:

1. Account may not be used by more than 1 person (Daily Tariff Rates)
2. Proxy Helper may not be used by more than 1 person (All Tariffs)
3. A proxy server may not be used for mass mailing (not only in terms of spam)
4. A proxy may not be taken from the base by using programs other than your browser (Daily Tariff Rates)

Offers:

- Specific node counts
- Guaranteed infection rates
- SLAs
- Technical Support

Malware Control Console

Storm Worm

| Attacked hosts (total - uniq) | | Traffic (total - uniq) | |
|-------------------------------|----------------|----------------------------|-----------------|
| IE XP ALL | 114721 - 96104 | Total traff | 159073 - 129089 |
| QuickTime | 2175 - 2048 | Exploited | 44804 - 35574 |
| Win2000 | 7033 - 6260 | Loads count | 17408 - 15968 |
| Firefox | 12885 - 12514 | Loader's response | 38.85% - 44.89% |
| Opera7 | 1271 - 1264 | Efficiency 10.94% - 12.37% | |

| Browser stats (total) | | Modules state | |
|-----------------------|---------|------------------|-------------|
| MSIE | 4 0% | Statistic type | MySQL-based |
| Opera | 1 0% | User blocking | ON |
| | | Country blocking | OFF |

| Country | Traff | Loads | Efficiency |
|-------------------------|-----------------|----------------|------------|
| RU - Russian federation | 112793 70.9% | 12653 72.7% | 11.22% |
| UA - Ukraine | 16666 10.5% | 1670 9.6% | 10.02% |
| IT - Italy | 7045 4.4% | 593 3.4% | 8.42% |
| GE - Georgia | 5775 3.6% | 673 3.9% | 11.65% |
| BY - Belarus | 5419 3.4% | 657 3.8% | 12.12% |
| KZ - Kazakstan | 3098 1.9% | 376 2.2% | 12.14% |
| US - United states | 1117 0.7% | 50 0.3% | 4.48% |
| AZ - Azerbaijan | 1060 0.7% | 128 0.7% | 12.08% |

Targeted Attacks

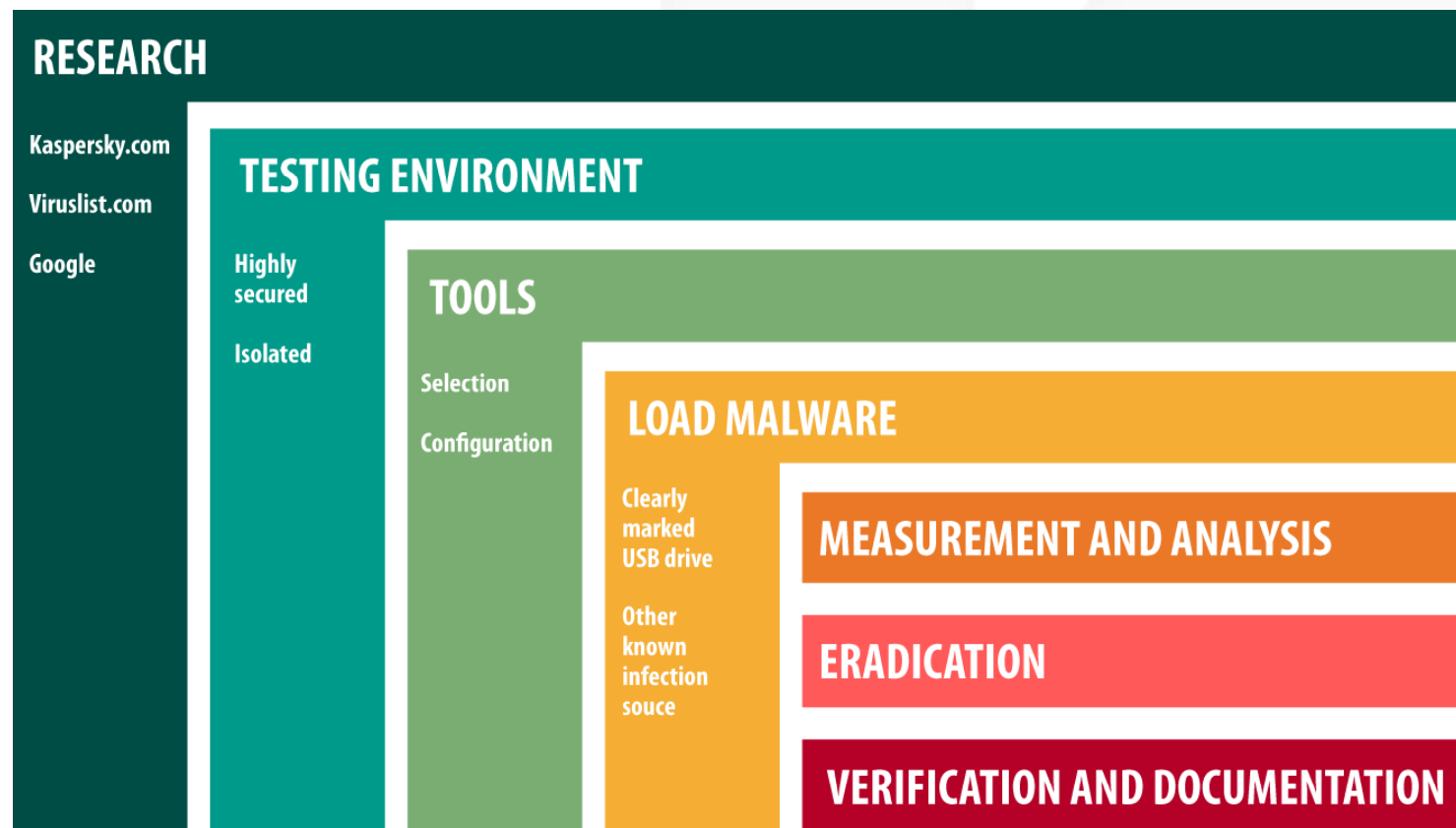
- Los Alamos and Oak Ridge Spear Phishing attack
 - Visitor database only
 - 12 different attackers, 7 emails to 1000's of employees
 - 11 emails opened
- What about your business?
 - Specific companies being targeted
 - Specific groups within a company
 - Denotes social engineering skill
 - Solid research (competitive intelligence) skills
 - Job sites
 - User forums...



Hunting Malware

INTEROP[®]
LAS VEGAS | APRIL 27–MAY 2, 2008

Virus Hunting Protocol



Regmon

| # | Time | Process | Request | Path | Result | Other |
|-------|-------------|----------|------------|------------------------------------|----------|-------------|
| 16089 | 45.16078186 | oocca... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16090 | 45.16093063 | oocca... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16091 | 45.16102219 | oocca... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16092 | 45.16110611 | oocca... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16093 | 45.20592117 | mozyb... | QueryKey | HKU\DEFAULT\Software\Microsoft\... | SUCCE... | Subkeys = 0 |
| 16094 | 45.22343826 | mozyb... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16095 | 45.31533432 | mozyb... | QueryKey | HKU\DEFAULT\Software\Microsoft\... | SUCCE... | Subkeys = 0 |
| 16096 | 45.33087158 | vmwar... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16097 | 45.33101273 | vmwar... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16098 | 45.33109665 | vmwar... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16099 | 45.33116531 | vmwar... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16100 | 45.33123016 | vmwar... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16101 | 45.33164597 | vmwar... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16102 | 45.33192825 | vmwar... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16103 | 45.33215714 | vmwar... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16104 | 45.33242798 | vmwar... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16105 | 45.33266068 | vmwar... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16106 | 45.33289719 | vmwar... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16107 | 45.33313751 | vmwar... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16108 | 45.33337784 | vmwar... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16109 | 45.33361816 | vmwar... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16110 | 45.33386230 | vmwar... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16152 | 45.34593582 | vmwar... | QueryValue | HKLM\SOFTWARE\Microsoft\Windo... | NOT F... | |
| 16153 | 45.34853745 | mozys... | QueryValue | HKLM\SOFTWARE\mozy\scheduling\... | NOT F... | |
| 16154 | 45.42453384 | mozyb... | QueryKey | HKU\DEFAULT\Software\Microsoft\... | SUCCE... | Subkeys = 0 |

What

- What registry changes are made

Why

- Covers all registry entries

When

- Setup before infection, measurement afterward

Filemon

The screenshot shows the File Monitor application window with a menu bar (File, Edit, Options, Volumes, Help) and a toolbar. The main area displays a table of file system events.

| # | Time | Process | Request | Path | Result | Other |
|-----|-------------|---------------|-------------------|---------------------------------|---------|------------------------------|
| 833 | 11:36:42 AM | svchost.ex... | QUERY INFORMATION | C:\PROGRAM FILES\LOGITECH\MO... | SUCCESS | FileInternalInformation |
| 834 | 11:36:42 AM | svchost.ex... | CLOSE | C:\PROGRAM FILES\LOGITECH\MO... | SUCCESS | |
| 835 | 11:36:42 AM | svchost.ex... | OPEN | C:\PROGRAM FILES\MEMEO\ | SUCCESS | Options: Open Access: 000... |
| 836 | 11:36:42 AM | svchost.ex... | QUERY INFORMATION | C:\PROGRAM FILES\MEMEO\ | SUCCESS | FileInternalInformation |
| 837 | 11:36:42 AM | svchost.ex... | CLOSE | C:\PROGRAM FILES\MEMEO\ | SUCCESS | |
| 838 | 11:36:42 AM | svchost.ex... | OPEN | C:\PROGRAM FILES\OO SOFTWARE\ | SUCCESS | Options: Open Access: 000... |
| 839 | 11:36:42 AM | svchost.ex... | QUERY INFORMATION | C:\PROGRAM FILES\OO SOFTWARE\ | SUCCESS | FileInternalInformation |
| 840 | 11:36:42 AM | svchost.ex... | CLOSE | C:\PROGRAM FILES\OO SOFTWARE\ | SUCCESS | |
| 841 | 11:36:42 AM | svchost.ex... | OPEN | C:\PROGRAM FILES\VMWARE\ | SUCCESS | Options: Open Access: 000... |
| 842 | 11:36:42 AM | svchost.ex... | QUERY INFORMATION | C:\PROGRAM FILES\VMWARE\ | SUCCESS | FileInternalInformation |
| 843 | 11:36:42 AM | svchost.ex... | CLOSE | C:\PROGRAM FILES\VMWARE\ | SUCCESS | |
| 844 | 11:36:42 AM | svchost.ex... | OPEN | C:\PROGRA~1\ | SUCCESS | Options: Open Access: 000... |
| 845 | 11:36:42 AM | svchost.ex... | QUERY INFORMATION | C:\PROGRA~1\ | SUCCESS | FileInternalInformation |
| 846 | 11:36:42 AM | svchost.ex... | CLOSE | C:\PROGRA~1\ | SUCCESS | |
| 847 | 11:36:42 AM | svchost.ex... | OPEN | C:\PROGRA~1\GOOGLE\ | SUCCESS | Options: Open Access: 000... |
| 848 | 11:36:42 AM | svchost.ex... | QUERY INFORMATION | C:\PROGRA~1\GOOGLE\ | SUCCESS | FileInternalInformation |
| 849 | 11:36:42 AM | svchost.ex... | CLOSE | C:\PROGRA~1\GOOGLE\ | SUCCESS | |
| 850 | 11:36:42 AM | svchost.ex... | OPEN | C:\PROGRA~1\GOOGLE\GOOGLE~1\ | SUCCESS | Options: Open Access: 000... |

What

- What files are changed, added, deleted... from a system

Why

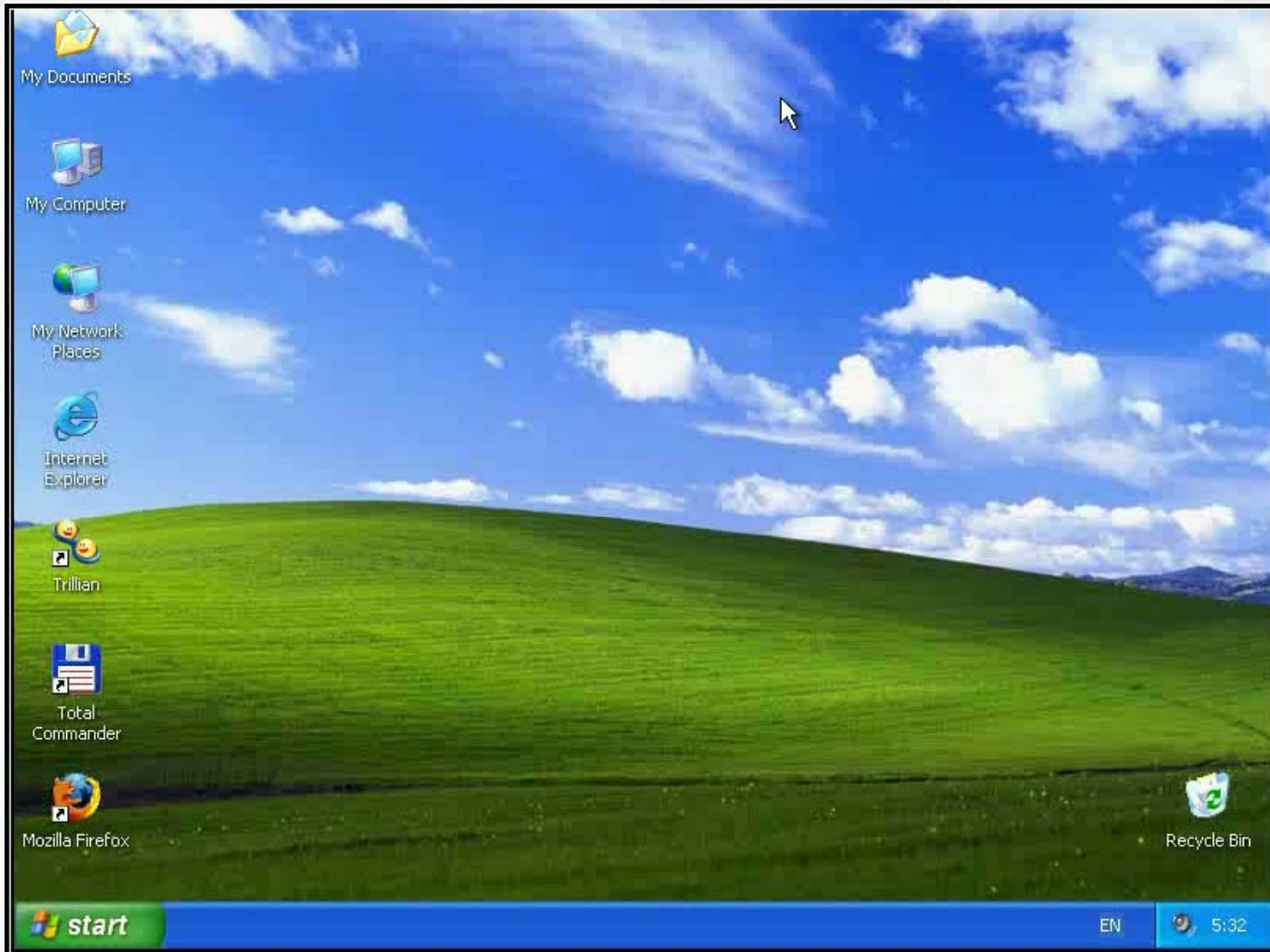
- Typical Windows XP system has 50,000 to 100,000 files

When

- Setup before infection, measure afterward

Other Tools

- Netcat – the Swiss Army Knife
 - Monitor Port 80 communications
 - Create Log files of that communication
- B64Dec – Base 64 decoder
- Process Explorer – View Tasks and Task Trees



Pinch Password stealer

Pinch Highlights

- Infection Vectors
 - ICQ
 - Email
- Purpose
 - Collect victim system information
 - Collect cached passwords
 - Send collected data to Internet server

Conclusions

- Malware has evolved
- Highly organized, profitable, low risk business
- Organized ecosystem
- Basic incident response tools

Questions?

- Tom.Bowers@kaspersky.com
- Search engine query: "Tom Bowers" "information security"