malware analysis
for the enterprise

jason ross
yesterday: “impenetrable defense”
today: tourist attraction
obligatory narcissism

• worked in IT security for > 10 years

• employed with the BT ethical hacking team

• contribute to various malware research groups & internet security communities

• PoC for the 585 defcon group
what are we talking about?

we are awesome at compliance!

so why are we getting owned?

because the current security mindset sucks.

- do you know when a host is compromised?
- can you tell if other hosts were?
- what data was taken?
- do you have any idea where it went?
compliance != security

• we’re not getting better at securing systems

• we *are* becoming adept at evading the average security auditor.
"has data loss jumped the shark?"

Despite the statements in the prior slide, we are seeing a decrease in data loss incidents
• Websense states in their 2009 Q1 "State of the Internet" report:
  – 671% growth in malicious web sites in the past year.
  – 77% of these were legitimate sites that had been compromised.
what does that mean?

attackers may not be interested in your data at all.

the intended victim may not even be your customer.

they may be looking to use your brand image.
industry:
let’s use signatures!

malware:
i can has packing, crypto, and some polymorphism?

arms race ++

protection fail.
heuristics won't save you

- they can be useful and effective
- they miss things
- especially if multiple stages are involved
some ways malware defeats AV

• encrypt the code with strong ciphers and randomized keys

• alter the codebase in an automated fashion (polymorphism)

• pack the executable
The state of anti-malware is abysmal.

Reactive technology is, by definition, not going to be securing proactively.

- Examples of suckage:
- Different signatures for the same malware.
- Vendors can't even agree on a name!
but...

my AV suite alerts me constantly!

think about that for a minute...
at least AV is catching stuff. that's good, right?

the host was probably compromised before AV caught whatever it alerted on.

that's because malware does not infect a host using a single stage process.

prepare for HolyCrap!
how malware works (really!)

image taken from the FireEye Research Blog:
it's a business, not a kiddie

- payroll
- support models
- distribution channels
- strategic partnerships
downloads & droppers & rootkits, oh my!

• stage one: drive-by download
• stage two: load more malware
• stage three: profit!
pfft. only mom & pop sites are being used for droppers, right?
um. wow. that sucks.

• yes. yes it does.

• still think you’re safe because IDS, AV, or even a QSA says so?

• that’s OK, so did these guys:

  records lost by these companies : 264 million
  percentage of population “owned” : ~86 %
more lessons from heartland

- malcode authors are invested in long term solutions
- malware is increasingly targeted
scary example time

• URLZone
  – My balance is fine!

• Monkif / DIKhora
  – Nothing here but us JPEGs
where does malware analysis fit in?

• virus protection is familiar to us
  
• as a result, we treat infection casually

• a virus alert is a security incident

• does your incident response policy address virus alerts?
a clever transitional slide

- malware is bad
- analyzing it is necessary
- how do we do that?
  - static analysis
  - run-time analysis
sandnets

playing with fire is cool!
what is a sandnet?

• a test environment using multiple hosts

• isolated from the production network

• used to analyze malicious software
what are the options?

• online labs
• virtual machines
• bare metal
online labs

- convenient
- little skill required
- may not be comprehensive
- may be problematic from a security POV
roll your own

- more comprehensive
- potentially less problematic
- more expensive
- harder
vm, or bare metal?

- vm is cheaper & more efficient
- bare metal may be more accurate
jumping the shark!

(demo of shark 3.1)
how many hosts?

• At least 2 probably
  – Victim
  – Services / Monitoring

> VBoxManage list vms
  "linux" {ad59f194-585e-49c5-a54c-5e92322b1188}
  "winxp_sp3_01" {7a554f4e-6aea-42f1-a3c5-488d43f161ff}
network configuration

- isolated from production networks
  — including the Internet
- but the multi-stage download process requires access to malicious servers

haven't found a "good" solution for that yet

(IPS on outbound traffic?)
use the internal network feature

> VBoxManage showvminfo winxp_sp3_01

Name: winxp_sp3_01
Guest OS: Windows XP
UUID: 7a554f4e-6aea-42f1-a3c5-488d43f161ff
Memory size: 512MB
VRAM size: 12MB
Number of CPUs: 1
NIC 1: MAC: 080027D32767,
        Attachment: Internal Network 'intnet'
dhcp - because dynamic is easy

> VBoxManage dhcpserver add
--netname intnet
--ip 192.168.3.1
--netmask 255.255.255.0
--lowerip 192.168.3.100
--upperip 192.168.3.250
--enable
monitoring traffic

• let the VM do the work for you

> VBoxManage modifyvm linux --nictrace1 on --nictracefile1 "C:\Users\Test\linux.pcap"
- configured to be SOA for *

- returns the IP of the monitoring host for all resource requests
Remember the MX

db.wildcard
$TTL 604800
@ IN SOA localhost. root.localhost. ( 2010012201 ; serial
604800 ; refresh
86400 ; retry
2419200 ; expire
604800) ; negative

cache ttl

@ IN NS localhost.
* IN MX 10 192.168.3.101
* IN A 192.168.3.101
• mod_forensic is your friend

• configuration is easy:
ForensicLog /var/log/apache2/forensic_log

• Enable and reload:
  # a2enmod log_forensic
  # apache2ctl reload
sample forensic log

+2021:4adf8568:0
|GET / HTTP/1.1
|Accept:*/*
|Accept-Language:en-us
|Accept-Encoding:gzip, deflate
|User-Agent:Mozilla/4.0
 | (compatible; MSIE 6.0;
 | Windows NT 5.1; SV1)
|Host:192.168.3.101
|Connection:Keep-Alive
|Cache-Control:no-cache
-2021:4adf8568:0
fun with netcat

• very easy to set up:

# netcat –nvlp 8080 –o tcp_8080.txt

< 00000000 47 45 54 20 2f 20 48 54 50 20 31 31 0d 0a # GET / HTTP/1.1..
< 00000010 41 63 65 70 3a 20 61 70 70 6c 69 76 65 2c 20 4d 6f 7a 69 6c # Accept: Mozilla/4.0
< 00000020 49 54 20 36 2e 30 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 53 56 31 29 0d 0a 48 6f # NT 5.1; SV1)..Host 1:8080..Connecti
• SpiderMonkey rules

• biggest issue is no ‘document’ object

• Didier Stevens’ port is even better
  – adds features specific to malware analysis
  – including document.write()
victim host

- iDefense malcode analyst pack
- Regshot
- strings
- wireshark
Demo!
online resources

Anubis:  
http://anubis.isclab.org/

Virus Total  
http://www.virustotal.com/

CERT.at Do-It-Yourself Kit  
if you want to contact me for some crazy reason, here's how you can:

https://twitter.com/rossja
algorythm@gmail.com