curity Systems Fail:
t Line of “Defense”

SO Member’s Meeting
NN 40, San Francisco
March 16, 2011

Rodney Joffe
and Senior Technologist
Neustar, Inc.

# of Modern CyberCrime

993

Miscreant

cker

for “fun/bragging

public acclaim

ch other

Mid-1990’s

Rise of the Spammer

- SPAM discovered by marketers as being effective in generating business
- Over time, anti-spam movement became more effective
- Spammers needed technical options

Late 19

Spammers H

- Miscreant creates m generate and send s
- Miscreant utilizes bo
- Miscreants create “S
- Miscreants develop sophistication – usec attack anti-spammer

ne Evolves

nters

spam
noney
otential

a tool
an

2004

Data Theft is a New Vector

- Criminals realize that there is significant value in Data – Financial Credentials and Intellectual Property
- Keyloggers and data exfiltration become the focus

2007

Nation States Enter

- Criminals volunteer (for political favor) or are being hired by Nation State actors
- Estonia, Georgia, Kyrgyzstan

Li

- Nation s
or grow
to build
weapor
- Botnets
informa
- APT: Fo
Patient

ne

ools Are Not Enough

s know that today a layered approach is mandatory…yet even that does not guarant

anti-malware applications are no longer sufficient

stems are mostly based on known behavior

e dynamic / polymorphic

Exploits (announced vulnerabilities that have not yet been patched) continue

oits are outside of your network and control

what you do, the numbers say that at some stage you will be compromised

me and Security Survey Report; Computer Security Institute; "…Respondents did not seem to feel that their challenges were attributable to a lack of i satisfaction with security tools, but rather, despite all their efforts, they could not be certain about what was really going on in their environments, nor w

histicated Attacks

threats is emerging that requires only one
network to cause extreme damage

: If a Transportation Security Officer told you that he
and disarmed 99.999% of the bombs on board an
d *you* board?

have to be right thousands of times a day –
’ only have to be right once!

t is to your DATA.

e the value of Malware designed for a single purpose: the exfiltration and theft of your da

ly accounted for 38% as a type of breach (vs. misuse, error, etc.) but accou
ed data[1]

0 Global Fraud Report reports that digital information theft has become the
ud for the first time (surpassing physical theft)[2]

loss for an organization due to cyber-attacks was $3.8 Million (ranging fro
ectation of one successful attack per week[3]

uring the life cycle of an attack, the span of time from “entry to compromise
n minutes, yet the span of time measuring a company’s “discovery and co
n months[1]

tigations Report; Verizon and US Secret Service. [2] Global Fraud Report; Kroll; July 2010 [3] First Annual Cost of Cyber Crime Rep

uld You Do?

r layered approach using all the best practices you

r Firewalls are in place, up-to-date, and patched

virus/Anti-malware solutions

best IDS/IPS systems you can

d enforce professional standards

everyone understands and recognizes **social g** attacks

employees continually to be security aware

nitor, Monitor

Despite these
defenses yo
compromised.
prepare

ne

?

neck: there is no such thing as perfect security.

urity world, failure is not only an option,
it is practically *guaranteed*.

Layer in Security - Failure Sensors

s inevitable, you DARE NOT ignore it…

it head on, plan on it, and prepare for it by…

g a new layer in the security model that is rom your norms:

stem of sensors that tell you that your nses have failed by watching for the ts of the failure.

Science™

Reflective Science is the technique used to identify the potential or actual occurrence o information security event based not on the observation of the event itself but on the artifacts left by or the precursors to the eve

Science™ and You

implements all of the best practices for security; however if you are compromised y

Reflective Science™ will:

(1) prepare you for the worst;

(2) act as a last line of defense;

(3) give you warnings as the compromise is in progress; and

(4) allow you to mitigate the effects of the attack, hopefully in
time

o you use Reflective Science™ for your Regi

operates on the assumption that the patient has died, and asks “What went

Gary Klein, Chief Scientist - ARA Klei

Why PreMortem?:

(1) abandon the “we are invincible” defensive mentality

(2) Work back from the end assumption that you failed;

(3) Identify all possible methods of failure from that position;

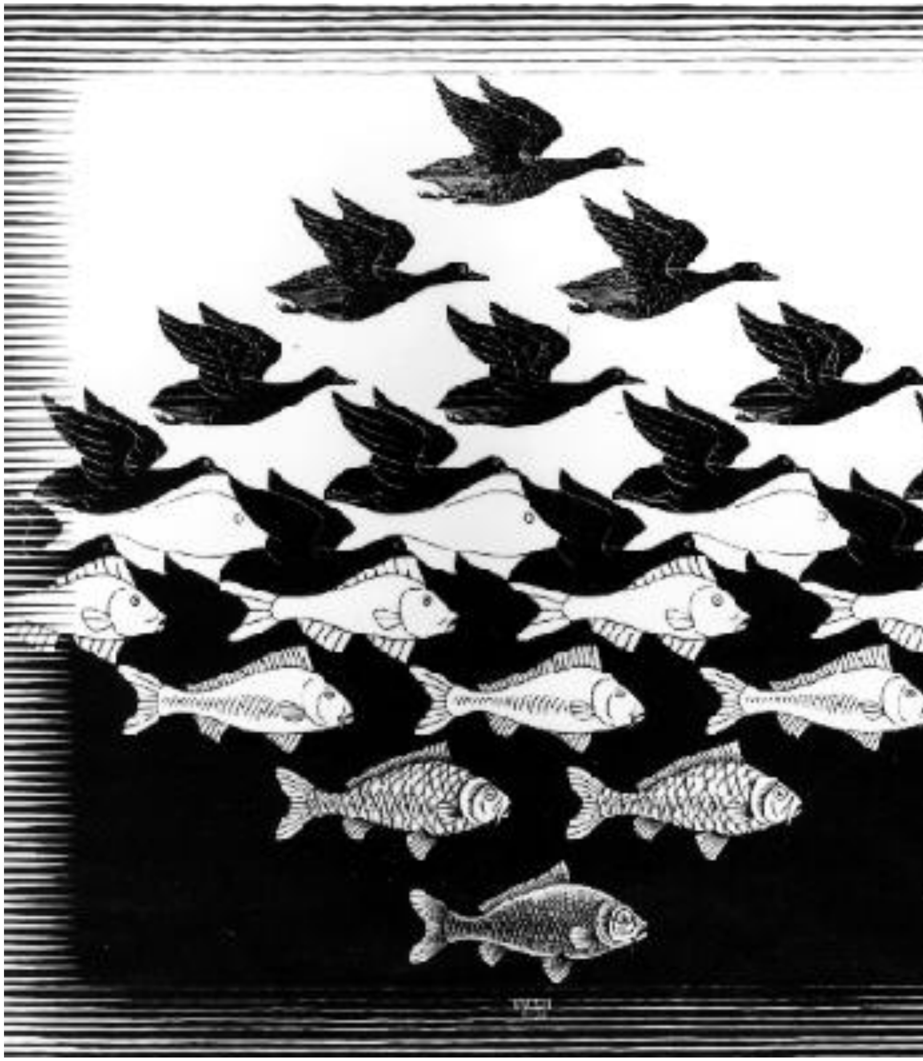
(4) Analyze all vulnerabilities that could have caused the failu

(5) Correct your processes so that these failures cannot occu

(6) Rinse, repeat

w is to
ure…

…and make sure you know how to recognize it.



ne

ernal Markers of Breeches

- **Precursors:**
  - Cache poisoning of recursive DNS servers
  - Hijacking of Network Route Announcements
- **Artifacts:**
  - Contact by your systems with DarkNets or Honey
    behavior that indicates a keystroke logger, or data
    malware
  - Appearance of your credentials or intellectual pro
    "Underground Economy"

ell:

ossibility of failure

ow you would know it had occurred

 build up, or happen

ells

ontinuining

Thank You

Rodney Joffe
and Senior Technologist

Neustar, Inc.
5 Pennsylvania Ave, NW
/ashington DC 20006

odney.joffe@neustar.biz