WARNING! Disruptive Thoughts Ahead
WARNING! Block Diagrams Ahead
About Me

Saumil Shah
CEO, Net Square
@therealsaumil
hacker, trainer, speaker, photographer, rebel

educating, entertaining and exasperating audiences since 1999
The Evolution of Attacks: 2001-17
The Evolution of Targets: 2001-17

- Servers
- Applications
- Desktops
- Browsers
- Pockets
- Populations
<table>
<thead>
<tr>
<th>Security Measures</th>
<th>Techniques Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewalls</td>
<td>One-way Attacks</td>
</tr>
<tr>
<td>IDS/IPS</td>
<td>FragRouter</td>
</tr>
<tr>
<td>Antivirus</td>
<td>Obfuscation</td>
</tr>
<tr>
<td>WAF</td>
<td>Char Encoding</td>
</tr>
<tr>
<td>DLP, EPS</td>
<td>DNS Exfil</td>
</tr>
<tr>
<td>DEP, ASLR</td>
<td>ROP, Infoleak</td>
</tr>
<tr>
<td>Sandbox</td>
<td>Jailbreak</td>
</tr>
</tbody>
</table>

Different.... but Same Same
Example: ROWHAMMER
Example: STEGOSPLOIT

- **EXPLOIT CODE**
  - **IMAGE**
    - **PIXEL ENCODER**
      - **ENCODED IMAGE**
        - **STEGO-DECODER JAVASCRIPT**
          - **IMAJS**
            - **POLYGLOT**
              - **TARGET BROWSER**

http://stegosploit.info
There will be Vulnerabilities
Nakatomi Space

wherein buildings reveal near-infinite interiors, capable of being traversed through all manner of non-architectural means

http://www.bldgblog.com/2010/01/nakatomi-space/
Attacks succeed because today’s defense is REACTIVE.
Exploit Development - 2002

Individual effort.
1 week dev time.
3-6 months shelf life.
Hundreds of public domain exploits.

"We did it for the LOLs."
TWO TIMELINES
The evolution of a new species

MitiGator. The well-intentioned, but short-sighted and not terribly effective alligator, always working to make exploitation harder. pic.twitter.com/iUdaeaaur8P

Credit @halvarflake

#HITB2017AMS
The MitiGator raises the bar...

...until it sees no more exploits

Credit @halvarflake
#HITB2017AMS
A long time ago in a galaxy far, far away...

It’s Time to End Information Anarchy

By Scott Culp
October 2001

*Code Red. Lion. Sadmind. Ramen. Nimda.* In the past year, computer worms with these names have attacked computer networks around the world, causing billions of dollars of damage. They paralysed computer networks, destroyed data, and in some cases left infected computers vulnerable to future attacks. The people who wrote them have been rightly condemned as criminals. But they needed help to devastate our networks. And we in the security community gave it to them.

It's high time the security community stopped providing blueprints for building these weapons. And it's high time computer users insisted that the security community live up to its obligation to protect them. We can and should discuss security vulnerabilities, but we should be smart, prudent, and responsible in the way we do it.
Organization for Internet Safety

Security and IT Industry Leaders Form Organization for Internet Safety

New Alliance Will Propose Best Practices for Handling Security Vulnerabilities

Sept. 26, 2002 — The Organization for Internet Safety (OIS), a unique alliance of leading technology vendors, security researchers and consultancies, today announced its formation. The OIS was formed to propose and institutionalize industry best practices for handling security vulnerabilities to ensure that security and technology vendors, and security researchers, can more effectively protect Internet users. Founding members of the OIS include @stake, BindView Corp., Caldera International, Inc. (The SCO Group), Foundstone, Guardent, Internet Security Systems, Inc., Microsoft Corp., Network Associates, Oracle Corporation, SGI and Symantec.
Cisco Harasses Security Researcher

I’ve written about full disclosure, and how disclosing security vulnerabilities is our best mechanism for improving security -- especially in a free-market system. (That essay is also worth reading for a general discussion of the security trade-offs.) I’ve also written about how security companies treat vulnerabilities as public-relations problems first and technical problems second. This week at BlackHat, security researcher Michael Lynn and Cisco demonstrated both points.

Lynn was going to present security flaws in Cisco’s IOS, and Cisco went to inordinate lengths to make sure that information never got into the hands of the their consumers, the press, or the public.

Cisco threatened legal action to stop the conference’s organizers from allowing a 24-year-old researcher for a rival tech firm to discuss how he says hackers could seize control of Cisco’s Internet routers, which dominate the market. Cisco also instructed workers to tear 20 pages outlining the presentation from the conference program and ordered 2,000 CDs containing the presentation destroyed.

In the end, the researcher, Michael Lynn, went ahead with a presentation, describing flaws in Cisco’s software that he said could allow hackers to take over corporate and government networks and the Internet, intercepting and mishandling data communications. Mr. Lynn, wearing a white hat emblazoned with the word "Good," spoke after quitting his job at Internet Security Systems Inc. Wednesday. Mr. Lynn said he resigned because ISS executives had insisted he strike key portions of his presentation.
NO MORE FREE BUGS
Exploit Development - 2012

2-12 month dev time. 24h to 10d shelf life. Public domain exploits = zero. Cost, value of exploits has significantly risen.

- COMMERCIALIZED
- WEAPONIZED
- POLITICIZED
The defenders tried to buy back their bugs...
Bug Bounties: high stakes game

Chris Evans – Pwnium: Element 1337
Bug Bounties tried to fill a REACTIVE need.
Bug Bounties Backfiring?

Breaking News: We offer one million US dollars ($1,000,000) for iOS9 exploits/jailbreak: zerodium.com/ios9.html #bugbounty #Jailbreak #0day

Zerodium @Zerodium 2h

Our price range for 0days we acquired so far: Mobile $100K. Browsers $50K-30K. Sandboxes/Kml $50K-30K, Flash $45K-25K, Office $40K-25K, Java $0

Alex Stamos @alexstamos

Bug Bounty researchers are incredibly short-sighted and keep acting in a way that discourages new programs.

Poll: If you had an expensive 0day, would you sell it & feed your family, or give it for free to software vendors to feed their shareholders

Dan Guido @dguido

The researcher responses to this bug bounty are awful. They're not there to pay your salary, it's a thank you. forbes.com/sites/thomasbr...

Chaouki Bekrar @cBekrar

I fully support my family 80%
I suck shareholders dicks 20%

422 votes Final results
01/10/16, 13:38
HELLO

A STRANGE GAME.
THE ONLY WINNING MOVE IS NOT TO PLAY.
More Reactive Security
Compliance != Security
HITB2017AMS

TARGET

ed!

DATA BREACH

Michaels

Neiman Marcus

100% PCI-DSS compliant
Security = "RISK REDUCTION"

Rules

Signatures

Updates

Machine Learning
Cylance stops 99% of malware attacks before they happen.

Let us prove it. cylance.com

THE OTHER 1% OF MALWARE

1% WOULD OWN THIS

9% WOULD OWN THIS

30% WOULD OWN THIS

20% WOULD OWN THIS

40% WOULD OWN THIS RED DOT
Existing defense measures do not match attacker tactics.
Attackers don’t follow compliance standards and certifications.
The CISO: 2001-2017

Jack Daniel
@jack_daniel

You know, standard definition, Chief (Information) Scapegoat Officer

24/03/17, 07:59
In 2001...

CIO

CIO

CISO

INFOTECH = BUSINESS ENABLER

INFOSEC = RISK REDUCTION

C.Y.A.
Dear CISO, Who are Scarier ATTACKERS or AUDITORS?
It is time we...not by building firewalls...
@therealsaumil's
SEVEN AXIOMS of Security
Intelligence Driven Defense

From REACTIVE to PROACTIVE
Seven Axioms of Security: I

Defense doesn’t mean Risk Reduction
Seven Axioms of Security: I

The CISO’s job is DEFENSE
Compliance is NOT the CISO's job

"Not my circus, Not my monkeys"

http://rafeeqrehman.com/2016/10/07/announcing-ciso-mindmap-2016/

90% TIME SPENT ON COMPLIANCE!
In 2017...

CISO → CISO
INFOSEC = DEFENSE
DEFEND AGAINST ATTACKERS

CISO → CCO
CHIEF COMPLIANCE OFFICER
DEFEND AGAINST AUDITORS
Seven Axioms of Security: 2

Intelligence begins by collecting everything!
Collect Everything!

- Retention is CHEAPER than Deletion.
- Importance of HISTORICAL DATA increases exponentially with time.
Sources of Security Intelligence?

Threatbutt Internet Hacking Attack Attribution Map

```
Jpn (224.44.51.219) uses A *BRILLIANT* Guarantee That It Has NOT The Russians against gbr (78.25.42.134) -- IT'S SUPER EFFECTIVE!

use (121.18.117.165) uses Morris worm against std (149.159.48.177) -- IT'S SUPER EFFECTIVE!
use (2.220.57.200) uses tp (u=tp) = tp against gnn (172.137.35.150) -- It's probably fine "_(ツ)_/";
use (241.209.46.210) uses WordPress plugins against usa (85.194.79.242) -- It's good for business!
use (66.77.84.118) uses Advanced Persistent Red Day against gnn (132.146.71.123) -- We'll just call it a "glitch".
phl (131.41.185.156) uses something we don't have in our feed against chn (148.142.154.142) -- it's probably fine "_(ツ)_/"
```
Sources of Security Intelligence

"The Universe tells you everything you need to know about it, as long as you are prepared to watch, to listen, to smell, in short to OBSERVE."
Get CREATIVE, Get ORGANIC

Performant Endpoint Visibility
osquery allows you to easily ask questions about your Linux, Windows, and OS X infrastructure. Whether your goal is intrusion detection, infrastructure reliability, or compliance, osquery gives you the ability to empower and inform a broad set of organizations within your company.

Read the deployment guide
or start contributing!

osquery> SELECT uid, name FROM listening_ports l, processes p WHERE l.pid=p.pid;

ORGANIC SECURITY = Grow It Yourself!
Seven Axioms of Security: 3

Schrödinger’s Hack: Systems exist in both SECURE and HACKED states at the same time.
Seven Axioms of Security: 3

Test Realistically
Forgone conclusion: 
"My System Is SECURE"

Test Strategy that will lead you this conclusion

• Wait for a new production build.
• Don’t test on production only UAT.
• Perform Non-intrusive testing.
• X,Y,Z,.. are all out of Scope.
• Test during off-peak hours only.
Seven Axioms of Security: 4

Can’t MEASURE?
Can’t Use.
Why Keep Metrics?

• To show you are succeeding
  – Corollary: to show you are failing
• To justify your existence and/or budget
• To argue for change
• For fun!

Marcus Ranum
Security Metrics: The Quest For Meaning
IT Defense 2016, Mainz
How to Establish Metrics

• Look at your process and make a list of what is quantifiable
• Ask yourself what quantities you are interested in
  – Once things are quantified they go up, or down – which is about the only convenient thing of metrics: they don't go sideways, too
• Which is a "good" direction: up or down?
• Do you know what constitutes a significant movement?
• Measure and iterate
The amount of energy necessary to refute bullshit is an order of magnitude bigger than to produce it.
Why Metrics Win

• Often information security becomes what I call a "battle of two narratives"
  – Your opponent has the advantage of lying:
  – "moving this to the cloud will save us $500,000/year!"
  – To defend your narrative you need facts (from metrics) and credible extrapolations (based on metrics) or your opponent controls the narrative! *

* Plan B is to respond with lies of your own

Marcus Ranum
Security Metrics: The Quest For Meaning
IT Defense 2016, Mainz
Seven Axioms of Security: 5

Users:
One Size Fits NONE!
The user's going to pick dancing pigs over security every time.

Bruce Schneier
Technology in the hands of users

My new credit card came in yay! And the security code is just like my birthday 527 #RichBitch pic.twitter.com/d5lW0NZ9OP

@needadebitcard

My new debit card!! Blue looks good

7:43 PM - 17 Aug 2016
the grugq @thegrugq

It's surprising how critical good phishing technique is with these APT attacks. Effective phishing is more important than 0day.

sp @LambdaCube

@thegrugq User-hardening efforts have made barely any progress compared to software-hardening efforts over the last years.
Identify your target users...

<table>
<thead>
<tr>
<th>HOPELESS</th>
<th>UNINFORMED</th>
<th>PROACTIVE</th>
<th>ROCK STARS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always going to be an enigma.</td>
<td>If properly guided, these users are willing to improve their usage habits.</td>
<td>The next Rock Star users.</td>
<td>Leave them alone, and possibly learn from them.</td>
</tr>
</tbody>
</table>

infosec maturity

number of users
...and improve their maturity
Seven Axioms of Security: 6

The Best Defense is a CREATIVE Defense.
Seven Axioms of Security: 6

A Creative Defense is an UNEXPECTED Defense.
Seven Axioms of Security: 7

Make Defense VISIBLE,
Make Defense COUNT.
Visible Defense

- Improve the User Maturity Curve.
- Reduce Blue Team’s Response Time.
- Money Saved = Money Earned
- Consistent Reduction in Frauds.
- Produce Creative Defense Tools.
- Attract Smarter Talent in Infosec.

- Weekly fitness check...
...The CISO Strength Test

- DEFEND & RECOVER
- TRACK ATTACKERS
- UNCOVER ATTACKERS
- DETECT INTRUSIONS
- ATTACKER CAPABILITY
- CLASSIFY UNAUTHORIZED ACTIVITY
- DETECT UNAUTHORIZED ACTIVITY
- REAL-TIME VISIBILITY OF EVENTS
- ASSET INVENTORY

https://github.com/swannman/ircapabilities
Is your Infosec team doing something creative every day?
Thank You, Drive Through

@therealsaumil
www.net-square.com
#HITB2017AMS