THINGS WE DON’T SAY
(Thinkst Applied Research - 2012)
Who am i ?
&
What this talk is about ?
Who am i?
Who am I?
Why this talk?
Reality
“I’m here to tell you that your cyber systems continue to function and serve you not due to the expertise of your security staff but solely due to the sufferance of your opponents”

Brian Snow - 2012
Isn’t that a little alarmist?
If our industry is so broken, why are you still in it? Become a cook or a truck driver then! #infosec
OLD MAN YELLS AT CLOUD
“You must never confuse faith that you will prevail in the end — which you can never afford to lose — with the discipline to confront the most brutal facts of your current reality, whatever they might be.”

Admiral James Stockdale
“Please realize we are in desperate trouble - moving at a snails pace against an avalanche of malice”

Brian Snow - 2012
We are in really bad shape..
SONY hacked.again

Hackers break into 55,000 Twitter accounts, leaving passwords bare

8th May 2012 by Alex Wilhelm
A new approach to China

1/12/2010 03:00:00 PM

Like many other well-known organizations, we face cyber attacks of varying degrees on a regular basis. In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a security incident—albeit a significant one—was something quite different.
<table>
<thead>
<tr>
<th>Maui – Zero-Day Vulnerability and CNE/CNA Program</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Maui</td>
<td>$2,500,000 per contract year</td>
</tr>
<tr>
<td></td>
<td>- Minimum of 25 deliverables per year</td>
</tr>
<tr>
<td></td>
<td>- Deliverable contents - Software</td>
</tr>
<tr>
<td></td>
<td>- Software CNE/CNA</td>
</tr>
<tr>
<td></td>
<td>- Metasploit module</td>
</tr>
<tr>
<td></td>
<td>- VMware image for testing</td>
</tr>
<tr>
<td></td>
<td>- Deliverable contents - Documentation</td>
</tr>
<tr>
<td></td>
<td>- Vulnerability information</td>
</tr>
<tr>
<td></td>
<td>- CNE/CNA information</td>
</tr>
<tr>
<td></td>
<td>- Demo instructions</td>
</tr>
<tr>
<td></td>
<td>- Revision history</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cayman – Global Vulnerability Analytics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cayman Basic</td>
<td>$1,500,000 per contract year</td>
</tr>
<tr>
<td></td>
<td>- Worldwide &quot;bot&quot; infection analytics</td>
</tr>
<tr>
<td></td>
<td>- IP address</td>
</tr>
<tr>
<td></td>
<td>- Organization name</td>
</tr>
<tr>
<td></td>
<td>- Geolocation</td>
</tr>
<tr>
<td></td>
<td>- C&amp;G protocol</td>
</tr>
<tr>
<td></td>
<td>- C&amp;G additional information</td>
</tr>
<tr>
<td></td>
<td>- Botnet identification</td>
</tr>
<tr>
<td></td>
<td>- Enhanced malware tracking</td>
</tr>
<tr>
<td></td>
<td>- Downadup/Conflickr infection</td>
</tr>
<tr>
<td></td>
<td>- analytics</td>
</tr>
<tr>
<td></td>
<td>- Enhanced compromised host tracking</td>
</tr>
<tr>
<td></td>
<td>- Compromised host IP address</td>
</tr>
<tr>
<td></td>
<td>- Probable infection status</td>
</tr>
<tr>
<td></td>
<td>- Probably re-infection solution</td>
</tr>
<tr>
<td>Cayman Enhanced</td>
<td>$1,750,000 per contract year</td>
</tr>
<tr>
<td></td>
<td>- Worldwide &quot;bot&quot; infection analytics</td>
</tr>
<tr>
<td></td>
<td>- IP address</td>
</tr>
</tbody>
</table>
“One, we are not doing the right things .... and two, the things we are doing are wrong”

Bruce Schneier
People, Process, Technology
Education

Something smell phishy?

“Phishing” emails pretend to be from a legitimate source, and try to trick you into volunteering your personal or credential-related information. Don’t fall for it!
http://safe.bank.com
https://bank.safe.com
https://safe.bank.com
https://bank.safe.com
https://198.3.1.5/bank.com
Do we reward the right behavior?
The Curious Case of MSFT
The Curious Case of MSFT
Conferences
Setec Astronomy
Setec Confere Moan (yo!)

Number of Industry Related InfoSec conferences in 1997 vs.
Number of Industry Related Infosec conferences in 2010

Number of Conferences per year (1984-2010)

The Established Conferences keep getting bigger...

Speakers (BlackHat 1997)
Speakers (BlackHat 2010)

At Least one InfoSec Conference is going on in any given month (with 19 in October alone!)

That means an infosec conference is taking place for 205/365 days of the year

http://blog.thinkst.com
blackhat conference standing room only
Rutkowska faces '100% undetectable malware' challenge

By Ryan Naraine | June 27, 2007, 5:38pm PDT
Hackers Can Now Make Your Laptop Explode

Posted on July 26, 2011 by Josh
What is your companies password change policy?
What types of attachments can you get in your corporate email?
Penetration Testing ?
Everyone needs a Pen-Test..
Right?

http://blog.thinkst.com/2012/03/penetration-testing-considered-harmful.html
Client-Sides in Assessments
MS08-XX vs. Flash Version ?
We were supposed to be simulating attackers

These days we just simulate other Pen-Testers
Pen-Test Attack Complexity & Getting a Result!
Still one 0day away from the worst day of our lives
Who here is concerned with MOBILE?

Who here is concerned with CLOUD?
Are you running FDE?
Are you running TripWire?
We know these solutions work..
Anti virus
IAmA a malware coder and botnet operator, AMA  (self.IAmA)

submitted 19 days ago by throwaway236236

• UPDATE: Lulz, saw it on twitter and some news pages, answering now.
• UPDATE2: Taking a break, my eyes hurt from the horizontal text lines lol, I will check back in soon™
• UPDATE3: Shit just hit russian hacker news, I better stop this AmA lol

I operate a ~10k botnet using a ZeuS software I modified myself, including IRC, DDoS and bitcoin mining (13GH/s - 20GH/s atm). Everything operating tru TOR hidden service so no feds will take my servers down. (Don't worry, traffic intensive stuff is not tru TOR and the bots work as relays too, enhancing your TOR experience!) Some screens: [http://i.imgur.com/yxMDx.jpg](http://i.imgur.com/yxMDx.jpg) (Yes, Rainbow Dash is best pony) Ask me anything!
Measuring the in-the-wild effectiveness of antivirus against ZeuS - Trusteer - Sep 2009
as an aside..
Give you an example: You don't see Mikko saying "AV is dead" or "AV is wrong" like others are..
@mikko @dakami easy test: will F-Secure (or any product) protect my computer against any variant of that specific malware family?
@wimremes @dakami Answer: probably, no. Do not underestimate the malware gangs. They have the budget and the resources to play this game.
so the experts actually have a good understanding of its effectiveness.. its the other people that don't..
clearly impressive..
but actually not helpful
(sounds familiar?)
It’s ok for what it is..
We are just stretching what it is...
People want Simple Contracts
From people who knew
(but ignored it)
to People who don’t even know..
a “market for lemons”

For Sale
For Sale
(Customer View)
For Sale
mini conclusion
Is it all gloomy?
Fortunately Not...
Not everyone needs to care as much..
Sometimes.. tech can be a Panacea!
Board Awareness
Detection is making a comeback
Return of the SysAdmin
Room for innovation!
Room for more Questions
Questions?

http://thinkst.com  |  @haroonmeer