WHAT SHOULD BE KEEPING YOU AWAKE AT NIGHT
LESSONS FROM THE DARK SIDE
(Thinkst Applied Research - 2012)
Who am i ?
&
What this talk is about ?
Who am i?
Why this talk ?
Because we are drowning
Info-Sec News?
Because we are drowning
Info-Sec Conferences
Setec Astronomy

Setec Confer 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...

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
Because we are drowning
Experts?

LinkedIn search for 'security experts' showing 50,627 results.
Because we are drowning
“Please realize we are in desperate trouble - moving at a snails pace against an avalanche of malice”

Brian Snow - 2012
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?
“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
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.
### Maui – Zero-Day Vulnerability and CNE/CNA Program

<table>
<thead>
<tr>
<th>Maui</th>
<th>$2,500,000 per contract year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum of 25 deliverables per year</td>
<td></td>
</tr>
<tr>
<td>Deliverable contents - Software</td>
<td></td>
</tr>
<tr>
<td>Software CNE/CNA</td>
<td></td>
</tr>
<tr>
<td>Metasploit module</td>
<td></td>
</tr>
<tr>
<td>VMware image for testing</td>
<td></td>
</tr>
<tr>
<td>Deliverable contents - Documentation</td>
<td></td>
</tr>
<tr>
<td>Vulnerability information</td>
<td></td>
</tr>
<tr>
<td>CNE/CNA information</td>
<td></td>
</tr>
<tr>
<td>Demo instructions</td>
<td></td>
</tr>
<tr>
<td>Revision history</td>
<td></td>
</tr>
</tbody>
</table>

### Cayman – Global Vulnerability Analytics

<table>
<thead>
<tr>
<th>Cayman Basic</th>
<th>$1,500,000 per contract year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worldwide &quot;bot&quot; infection analytics</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>Organization name</td>
<td></td>
</tr>
<tr>
<td>Geolocation</td>
<td></td>
</tr>
<tr>
<td>C&amp;C protocol</td>
<td></td>
</tr>
<tr>
<td>C&amp;C additional information</td>
<td></td>
</tr>
<tr>
<td>Botnet identification</td>
<td></td>
</tr>
<tr>
<td>Enhanced malware tracking</td>
<td></td>
</tr>
<tr>
<td>Downadup/Conflickr infection analytics</td>
<td></td>
</tr>
<tr>
<td>Enhanced compromised host tracking</td>
<td></td>
</tr>
<tr>
<td>Compromised host IP address</td>
<td></td>
</tr>
<tr>
<td>Probable infection status</td>
<td></td>
</tr>
<tr>
<td>Probably re-infection solution</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cayman Enhanced</th>
<th>$1,750,000 per contract year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worldwide &quot;bot&quot; infection analytics</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td></td>
</tr>
</tbody>
</table>
“One, we are not doing the right things .... and two, the things we are doing are wrong”

Bruce Schneier
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!
https://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
Conferences..
Setec Astronomy
Setec Confer 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
Google

blackhat conference standing room only

Search

About 16,500 results (0.57 seconds)

Everything

Images

Maps

Videos

News

Shopping

thinkst applied research
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
SLEEP WELL, AMERICA!

TSA Is On Guard!

—Slings and Arrows
What is your company's 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
I Am a malware coder and botnet operator, AMA

368

Submitted 19 days ago by throwaway236236

self.IAmA

- 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 (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
(Customer View)
For Sale
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
Most people just are not tested
(not an ad for pentesting)
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Agnitum (Outpost)</td>
<td></td>
<td></td>
<td>Virus 100</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>AhnLab</td>
<td></td>
<td></td>
<td>Virus 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auslogics Antivirus</td>
<td></td>
<td></td>
<td>Virus 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avast</td>
<td></td>
<td></td>
<td>Virus 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avertive</td>
<td></td>
<td></td>
<td>Virus 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AVG</td>
<td></td>
<td></td>
<td>×</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avira</td>
<td></td>
<td></td>
<td>Virus 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avira Personal</td>
<td></td>
<td></td>
<td>Virus 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BeyondTrust</td>
<td></td>
<td></td>
<td>Virus 100</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Bitdefender</td>
<td></td>
<td></td>
<td>Virus 100</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Bitdefender BKA V Home</td>
<td></td>
<td></td>
<td>×</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BullGuard</td>
<td></td>
<td></td>
<td>Virus 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Central Command (Vexira)</td>
<td></td>
<td></td>
<td>Virus 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check Point (ZoneAlarm)</td>
<td></td>
<td></td>
<td>Virus 100</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Check Point (ZoneAlarm) Extreme</td>
<td></td>
<td></td>
<td>Virus 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cleargrass</td>
<td></td>
<td></td>
<td>Virus 100</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>CMC Internet Security</td>
<td></td>
<td></td>
<td>Virus 100</td>
<td></td>
<td>×</td>
</tr>
</tbody>
</table>
Many people don’t understand the nature of the threat
Microsoft / Apple HACKED!
Georgia: Russia 'conducting cyber war'

Russia has been accused of attacking Georgian government websites in a cyber war to accompany their military bombardment.
Conducting cyber war'
attacking Georgian government websites in a cyber war to ombardment.
Los Angeles Times

LinkedIn investigating hack reports, 6.5 million leaked passwords

Our team is currently looking into reports of stolen passwords. Stay tuned for more.

Password ReUse?

Questions

Pass the ReUse?
Room for more Questions
Adobe Secure Software Engineering Team (ASSET) Blog / Inappropriate Use of Adobe Code Signing Certificate

by Brad Arkin

We recently received two malicious utilities that appeared to be digitally signed using a valid certificate. The discovery of these utilities was isolated to a single source. As soon as we uncovered the signatures, we immediately decommissioned the existing Adobe code signing infrastructure. A forensic investigation to determine how these signatures were created. We have identified a specific server with access to the Adobe code signing infrastructure. We are working with plans to revoke the certificate and publish updates for existing Adobe software signed using the impacted certificate. This does not affect the Adobe software signed with the impacted certificate that runs on the Windows platform or Adobe AIR applications that run on both Windows and Macintosh. The revocation does not prevent Adobe software for Macintosh or other platforms.

Sophisticated threat actors use malicious utilities like the signed samples during highly targeted privilege escalation and lateral movement within an environment following an initial malicious exploit. Our result, we believe the vast majority of users are not at risk. We have shared the samples via the Adobe Active Protection Program (MAPP) so that security vendors can detect and block the malicious activity.

Adobe's Connect User
ITPNewsPort - Nov 15, 2012
The reason for the hack is to quickly. According to ViruS_
Room for more Questions
Room for more Questions
Questions?

http://thinkst.com | @haroonmeer