Well here we are… It’s the beginning of the cyber wars my friends. POTUS came out on stage and said that we would have a “proportionate response” to the hacking of Sony and that in fact the US believes that it was in fact Kim Jong Un who was behind this whole thing. Yup, time to muster the cyber troops and attack their infrastructure!

*chortle*

So yeah, let’s take a step back here and ponder the FBI statement today on colonel mustard in the study with the laptop before we go PEW PEW PEW ok?

FBI Statement:
Update on Sony Investigation

Today, the FBI would like to provide an update on the status of our investigation into the cyber attack targeting Sony Pictures Entertainment (SPE). In late November, SPE confirmed that it was the victim of a cyber attack that destroyed systems and stole large quantities of personal and commercial data. A group calling itself the “Guardians of Peace” claimed responsibility for the attack and subsequently issued threats against SPE, its employees, and theaters that distribute its movies.

The FBI has determined that the intrusion into SPE’s network consisted of the deployment of destructive malware and the theft of proprietary information as well as employees’ personally identifiable information and confidential communications. The attacks also rendered thousands of SPE’s computers inoperable, forced SPE to take its entire computer network offline, and significantly disrupted the company’s business operations.

After discovering the intrusion into its network, SPE requested the FBI’s assistance. Since then, the FBI has been working closely with the company throughout the investigation. Sony has been a great partner in the investigation, and continues to work closely with the FBI. Sony reported this incident within hours, which is what the FBI hopes all companies will do when facing a cyber attack. Sony’s quick reporting facilitated the investigators’ ability to do their jobs, and ultimately to identify the source of these attacks.

As a result of our investigation, and in close collaboration with other U.S. government departments and agencies, the FBI now has enough information to conclude that the North Korean government is responsible for these actions. While the need to protect sensitive sources and methods precludes us from sharing all of this information, our conclusion is based, in part, on the following:

- Technical analysis of the data deletion malware used in this attack revealed links to other malware that the FBI knows North Korean actors previously developed. For example, there were similarities in specific lines of code, encryption algorithms, data deletion methods, and compromised networks.
- The FBI also observed significant overlap between the infrastructure used in this attack and other malicious cyber activity the U.S. government has previously linked directly to North Korea. For example, the FBI discovered that several Internet protocol (IP) addresses associated with known North Korean infrastructure communicated with IP addresses that were hardcoded into the data deletion malware used in this attack.
- Separately, the tools used in the SPE attack have similarities to a cyber attack in March of last year against South Korean banks and media outlets, which was carried out by North Korea.

We are deeply concerned about the destructive nature of this attack on a private sector entity and the ordinary citizens who worked there. Further, North Korea’s attack on SPE reaffirms that cyber threats pose one of the gravest national security dangers to the United States. Though the FBI has seen a wide variety and increasing number of cyber intrusions, the destructive nature of this attack, coupled with its coercive nature, sets it apart. North Korea’s actions were intended to inflict significant harm on a U.S. business and suppress the right of American citizens to express themselves. Such acts of intimidation fall outside the bounds of acceptable state behavior. The FBI takes seriously any attempt—whether through cyber-enabled means, threats of violence, or otherwise—to undermine the economic and social prosperity of our citizens.

The FBI stands ready to assist any U.S. company that is the victim of a destructive cyber attack or breach of confidential business information. Further, the FBI will continue to work closely with multiple departments and agencies as well as with domestic, foreign, and private sector partners who have played a critical role in our ability to trace this and other cyber threats to their source. Working together, the FBI will identify, pursue, and impose costs and consequences on individuals, groups, or nation states who use cyber means to threaten the United States or U.S. interests.

Parsing the language:

- Technical analysis of the data deletion malware used in this attack revealed links to other malware that the FBI knows North Korean actors previously developed. For example, there were similarities in specific lines of code, encryption algorithms, data deletion methods, and compromised networks.
- The FBI also observed significant overlap between the infrastructure used in this attack and other malicious cyber activity the U.S. government has previously linked directly to North Korea. For example, the FBI discovered that several Internet protocol (IP) addresses associated with known North Korean infrastructure communicated with IP addresses that were hardcoded into the data deletion malware used in this attack.
- Separately, the tools used in the SPE attack have similarities to a cyber attack in March of last year against South Korean banks and media outlets, which was carried out by North Korea.

The language of this report is loose and very much like an FBI statement would be when they are not so sure. Remember that the FBI did not originally link all of this to DPRK. Now though, with the same data as we all had before they are definitively tentatively saying “It’s DPRK” which makes people like me mental. So let’s look at these IP’s that were hard coded into the malware and take the idea to task that they are assets that ONLY the DPRK could use or has used and how that very idea has so much cognitive dissonance where “evidence” is concerned. Especially evidence where a nation state is going to “respond proportionally” to another for actions they claim they perpetrated.

The key here is to pay attention to the GEO-IP stuff they are using:
A summary of the C2 IP addresses:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Country</th>
<th>Port</th>
<th>Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>203.131.222.102</td>
<td>Thailand</td>
<td>8080</td>
<td>Diskpartmg16.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>igfxtray.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>igfxtpers.exe</td>
</tr>
<tr>
<td>217.96.33.164</td>
<td>Poland</td>
<td>8000</td>
<td>Diskpartmg16.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>igfxtray.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>igfxtpers.exe</td>
</tr>
<tr>
<td>88.53.215.64</td>
<td>Italy</td>
<td>8000</td>
<td>Diskpartmg16.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>igfxtray.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>igfxtpers.exe</td>
</tr>
<tr>
<td>200.87.126.116</td>
<td>Bolivia</td>
<td>8000</td>
<td>File 7</td>
</tr>
<tr>
<td>58.185.154.99</td>
<td>Singapore</td>
<td>8080</td>
<td>File 7</td>
</tr>
<tr>
<td>212.31.102.100</td>
<td>Cyprus</td>
<td>8080</td>
<td>File 7</td>
</tr>
<tr>
<td>208.105.226.235</td>
<td>United States</td>
<td>-</td>
<td>igfxtpers.exe</td>
</tr>
</tbody>
</table>

See now all of these IP’s could be used by just about anyone. They are not in country at the DPRK and they are not on Chinese soil either. In fact here is the dope on each one:

**Thailand: 203.131.222.102: Thailand port 8080 is a proxy:**

<table>
<thead>
<tr>
<th>203.131.222.102</th>
<th>203.131.222.102</th>
<th>203.131.222.102</th>
<th>203.131.222.0/23</th>
<th>THAMMASAT-BORDER-AS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>THAMMASAT</td>
<td></td>
<td>THAMMASAT-BORDER-AS</td>
<td>Thailand</td>
</tr>
<tr>
<td></td>
<td>Thammasat</td>
<td></td>
<td>Thammasat University</td>
<td>Thailand</td>
</tr>
<tr>
<td></td>
<td>University 2 Phrachan Road, Phranakorn, Bangkok 10200, Thailand</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

It has also been seen as a very dirty player in SPAM and other nefarious actions.. Not just DPRK/CN APT Activities

So really, this one could be used by anyone and everyone.

**Poland: 217.96.33.164 8080:**

<table>
<thead>
<tr>
<th>217.96.33.164</th>
<th>217.96.33.164</th>
<th>217.96.33.164</th>
<th>TPNET INTER-PARTS INTER-PARTS IMPORT EKSPORT WALDEMAR BACLAWSKI UL. JARZEBINOWA 4 11-034 STAWIGUDA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AS5567 TPNET Orange Polska Spolka Akcyjna</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Olstyn, Poland</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Poland too is known to be dirty and used for SPAM and malware C&C's as well. Many different groups are using this and it too is a proxy. So once again, this does not prove out solidly that this is DPRK. It could in fact be anyone who is in the know about it’s being there and use. Many of these addresses are on sites all over the web for use in this and other capacities.

<table>
<thead>
<tr>
<th>Test</th>
<th>Points</th>
<th>Date</th>
<th>Extra</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spamhaus Negatives</td>
<td>-1.4</td>
<td>Dec 19, 2014 10:15 PM</td>
<td>SBL</td>
</tr>
<tr>
<td>Virus Total</td>
<td>10</td>
<td>Dec 20, 2014 12:11 AM</td>
<td>2 pages found, triggering on average 3% antiviruses</td>
</tr>
<tr>
<td>Listed in DMOZ</td>
<td></td>
<td>Dec 19, 2014 10:15 PM</td>
<td></td>
</tr>
<tr>
<td>HostKarma Negatives</td>
<td></td>
<td>Dec 19, 2014 10:15 PM</td>
<td></td>
</tr>
<tr>
<td>HostKarma Positives</td>
<td></td>
<td>Dec 19, 2014 10:15 PM</td>
<td></td>
</tr>
<tr>
<td>Project Honeypot Negatives</td>
<td></td>
<td>Dec 19, 2014 10:15 PM</td>
<td></td>
</tr>
<tr>
<td>Project Honeypot Positives</td>
<td></td>
<td>Dec 19, 2014 10:15 PM</td>
<td></td>
</tr>
<tr>
<td>SORBS Negatives</td>
<td></td>
<td>Dec 19, 2014 10:15 PM</td>
<td></td>
</tr>
<tr>
<td>Google Safe Browsing</td>
<td></td>
<td>Dec 19, 2014 10:15 PM</td>
<td></td>
</tr>
<tr>
<td>Yandex Safe Browsing</td>
<td></td>
<td>Dec 19, 2014 10:15 PM</td>
<td></td>
</tr>
<tr>
<td>Domain Name Service</td>
<td>N/A</td>
<td>Dec 19, 2014 10:15 PM</td>
<td></td>
</tr>
<tr>
<td>Analyzed</td>
<td></td>
<td>Dec 19, 2014 10:15 PM</td>
<td></td>
</tr>
<tr>
<td>Grand total</td>
<td>0-11</td>
<td>Dec 19, 2014 10:15 PM</td>
<td></td>
</tr>
</tbody>
</table>

In fact here is a site that has the password to the system (Chinese)

**Italy 88.53.215.64 8000**

<table>
<thead>
<tr>
<th>88.53.215.64</th>
<th>88.53.215.64</th>
<th>88.53.215.64</th>
<th>88.52.0.0/15 INTERBUSINESS IT-INTERBUSINESS-20050930</th>
<th>AS3269 ASN-IBSNAZ Telecom Italia S.p.a.</th>
<th>Italy</th>
</tr>
</thead>
</table>

Once again, Italy has the same issue. It is a known dirty address/system and has been used for SPAM and Malware C&C’s before. This does not mean that it is in fact solely under the control of DPRK.
Site listing the proxy as available and the qualities of the anonymity

Here’s another listing: [http://dogdev.net/Proxy/IT](http://dogdev.net/Proxy/IT)

### Bolivia 200.87.126.116 8000

<table>
<thead>
<tr>
<th>200.87.126.116</th>
<th>200.87.126.116</th>
<th>200.87.126.116</th>
</tr>
</thead>
</table>

200.87.112.0/20 200.87.126.0/24 This is a DiViNetworks customer route-object which is being exported under this origin AS6568 (origin AS). This route object was created because no existing route object with the same origin was found. Please contact support@divinetworks.com if you have any questions regarding this object.

BO-ESN-ENTEL ENTEL S.A. – EntelNet

AS6568 ENTEL- SA-BOLIVIA

La Paz, Bolivia

Here’s a listing from 2012 on the Bolivian proxy (blackhat forum)

Another listing: [http://www.vipsocks24.com/2012/01/20-01-12-l1l2-anonymous-proxies-list.html](http://www.vipsocks24.com/2012/01/20-01-12-l1l2-anonymous-proxies-list.html)

Starting Nmap 6.47 ([http://nmap.org](http://nmap.org)) at 2014-12-20 05:15 EST

Nmap scan report for 200.87.126.116

Host is up (0.17s latency).

Not shown: 92 closed ports
PORT      STATE     SERVICE                     VERSION
80/tcp    open      http                     Apache httpd 2.2.3 ((Win32))
135/tcp   open      msrpc                    Microsoft Windows RPC
139/tcp   filtered   netbios-ssn
145/tcp   filtered   microsoft-ds
1720/tcp  filtered   H.323/Q.931
5800/tcp  open      vnc-http                 RealVNC 4.0 (resolution: 400x250; VNC TCP port: 5900) (remote auth bypass)
5900/tcp  open      vnc                      RealVNC Personal (protocol 4.0)
10000/tcp open      http                     GeoVision GeoHttpServer for webcams

Singapore 58.185.154.99 8080

Cyprus 212.31.102.100 8080
USA 208.105.226.235 (no port listed)

208.105.226.235 - 208.105.226.235
208.105.226.235

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-19 21:13 EST
Nmap scan report for rrcs-208-105-226-235.nys.biz.rr.com (208.105.226.235)
Host is up (0.070s latency).
Not shown: 94 filtered ports
PORT       STATE SERVICE
135/tcp    open  msrpc
443/tcp    open  https
3128/tcp   closed squid-http <— OOOOH A PROXY GO FIGURE
5000/tcp   open  upnp
5800/tcp   open  vnc-http
5900/tcp   open  vnc

This one seems to be a communications company in NY. An Nmap shows that there is a VNC session on here. Likely a compromised box. I wonder if anyone has looked at this.. It is still up so the FBI has not seized it.

Conclusions:

At the end of the day, if these are all the IP’s that the US is using as evidence that DPRK carried out this attack I think it is pretty weak as evidence goes. The majority of these systems are proxies and known to be such and the others are weak systems that have likely been compromised for use in this attack and maybe others because hackers share a lot of these C&C boxes. They do so to muddy the waters so to speak, the more groups using them the more confusion can be sewn.

The machine in NY is interesting in that it is still online. I would have thought that the authorities would want to take that into evidence but there it is, still online. Maybe they are still getting round to that… Or maybe they are just happy to make the pronouncement that it was DPRK and leave it be. I personally think that all of these systems together do not lead me or anyone using logic to believe that these are known infrastructures for DPRK unit 128.

Even if the likes of Crowdstrike and others may claim that DPRK has been known to use the same tactics or things like them or any other vague adjectives about the data that they have seen in the past none of it is anything that would be considered evidence in court. It is all considered circumstantial and that evidence is inadmissible. So, the US is going to base a theoretical response on a nation state level, as I said above, on circumstantial evidence?
Now that’s statecraft… Of course I remember a time a while back when we all were told that Iraq had massive WMD stocks and was in kahoots with Al Qaeda. In fact it was a SLAM DUNK according to the then CIA director.

Of course you all know how that all ended.

UPDATE:

After a nights sleep I woke up this morning thinking about all this yet again. I just wanted to add to this article the idea that similar code and tactics also do not an actor make as well. Remember that all of this could lead to a cold war if not a warmer war with actors like DPRK and we are going to hang our hats on “similarities” This just does not bode well for anyone.

There is a thing in intelligence called “cognitive bias” and I fear that our intelligence agencies fall prey to this a lot as it is. However, where the information and network warfare comes into play it is even worse. This is because it’s such a slippery subject not only on a technical level, but also because it is so easy to obfuscate means, methods, and actions with technology today. Another aphorism in the IC is that of being “lost in the forest of shadows” which means that nothing is clear and it is easy to be confused. Well, this is the same thing.

Like I said on Twitter last night, I can see my way to saying that DPRK was behind this. I can use Occams Razor to apply the logic of who had motive, look at their actions on the face of it, and say “most likely” it is them. However, would I want to go to war over that? Look at the people out there like Dave Aitel screaming that we need to go to cyber war and drop logic bombs in their infrastructure over this. Over a hack and destruction of data along with a healthy dose of schadenfreude over what.. Hollywood?

Come one!

It’s time for this community (INFOSEC) to really teach these people about what it is to be BLUE TEAM as well as sell them 0day. I am sorry, but we need to be better and so far we are just a bunch of warring parties looking for attention and the almighty dollar. We are in a perilous time because of people like Aitel and his ilk as well as the people who will blindly follow them because they are cyber warriors or thought leaders and know no better. If this keeps escalating, and it will, then we will see attacks by non state and state actors that will just be for anarchy’s sake.

I wrote earlier this month about the “Laughing Man Effect” with regard to the SONY incident as it was unfolding. This attack mimicked the LulzSec attack on HB Gary. It seems we did not learn from this. They too had some bad practices going on that lead to their compromise and utter destruction. In fact Sabu and the LulzSec crew were nicer to HB Gary than the attackers in the Sony case. At least they did not raze their network altogether. Though HB Gary Federal went down in flames due to the attack.

The Chinese say “May you live in interesting times” and that is not meant to be a pleasant thing. I fear that pandora’s box just opened up a little more with yestertdays pronouncement on shaky evidence. Unless the IC has more information that is solid to point the finger at DPRK for this I just can’t get behind any kind of response, proportional or otherwise. What really needs to happen is that Sony get’s their own shit together once they re-constitute their network and really have a working security model. Not the utter crap they had before but something that will actually mandate that personal information and IP be protected at least moderately.

This week I spoke with someone in the IC who does actual information warfare. In talking to him over the week I saw his frustration grow to the point that he put in his papers to separate. He plans on just going into teaching. Why? Because he said that all of this talk, this call to action over Sony was just so ridiculous that it would be hard for him to carry out an order of attack on this “evidence” His answer was to retire to teaching.

That about sums it up with me too of late. I look at the Twitter and the news feeds and see just marketing, hype, and faustribution. And it will be to our collective doom.

UPDATE 2 12/22/14

Seeing tweets that are implying that I am implying that the IP addresses above are DPRK assets. I never claim that. In fact the whole post says that they are not owned assets. The tweets also implies that I was wrong and that there must be secret knowledge of infrastructure being talked to by the IP’s in question....

So how does that actually work? A proxy by it’s very definition, especially an ANONYMOUS one is. Well... ANONYMOUS. So what records are we talking about here? If indeed the FBI has logs from Sony (which mind you, was pw3d sideways to Sunday) can they even be trusted? What I am saying here is that NOTHING provided to the American public on this issue nor the rest of the world sums up to evidence that could be used in a court of law here or anywhere except maybe DPRK.

So, like we say on the internet “Pics or it didn’t happen”

It all is moot anyway it seems as reports are coming in that DPRK networks are down (mind you again, those networks only really cover the elite of KJU’s inner circle so meh) Meanwhile it seems that “maybe” there has been some monkeying around with TOR by the FBI. RUMINT is at present that there are a couple of TOR boxes that have been seized in relation to the Sony investigation.

More when it is confirmed.

Let me leave you with a visual representation of how this all feels...
4th 2009). And it looks like we are facing the same weak evidence again. I highly recommend reading Fauxtribution by Krypt3ia, who really lays out the evidence, and the highly speculative nature of the attribution […]

**When a door is not a door | I Am Security**

2014/12/20 at 14:48

Reblogged this on To Inform is to Influence and commented:

Very good analysis of the Sony hack and the DPRK announcement!

**Joel Harding**

2014/12/20 at 18:28

“retire to teaching”

It’s funny, the way teaching is framed here comes across as almost a ‘cop out’.

But I say it’s not.

I’m not talking about being tucked away in a dusty corner of a university whiling away the days preaching to the choir (sounds nice eh), but teaching wrapped in multi-media (akin to CBT Nuggets) and distributed globally at a price those of us normal self-funded folk can reach.

I’ve made no secret of the impact of your thinking and writing on me. I’m no fool (believe it or not), nobody is right about everything all of the time, but there is a krypt3ia framework lens through which to view security, borne of 14yrs of hard accumulated knowledge and experience.

I have absorbed through this blog a way of thinking and that is the key.

I thought it was all about technical knowledge and this is important of course, but there’s so much more, that’s just half the story, and you have a more complete story tucked away in that brain of yours.

You have the knowledge, you have the communication skills, blimey, you even have an artistic bent.

Pick a topic, do a mini-series, record yourself whilst you talk and scribble all over digital pad, package it and sell it at an AFFORDABLE price.

I’m only bold enough to say this because if anybody takes the time to look at what you’re really communicating as I have, it is blatantly obvious you really do care.

I know you don’t want to half the time, but you do, and I don’t think there’s much you can do about that, because, well, you care.

I’ll admit now I was taken in by all the cyberwar talk and blinking lights mindset; not now, thanks to you……FUD!

This industry, especially those aspiring, inexperienced, training themselves, as I am, need access to your mindset, philosophy and knowledge, and they need it FAST, before they’re taken in by the charlatans.

At the end of the day, I wish you were teaching and I an recipient of your knowledge and lectures etc.

Ironic, eh.
Stuart (@StegoPax)
2014/12/21 at 09:32
[... ] https://krypt3ia.wordpress.com/2014/12/20/fauxtribution/ [...]

Why I *still* don't think it's likely that North Korea hacked Sony, | Marc's Security Ramblings
2014/12/21 at 10:51
[... ] “Fauxtribution ?” at Krypt3ia (pseudonymous hacker), 20 December [...]

The FBI told their story about North Korea attacking Sony, Before we retaliate, read what they didn’t tell you, | Fabius Maximus
2014/12/21 at 22:38
Could be the work of a group that wants greater investments in anti hacker systems from corporations like Sony. A kind of indirect extortion process.

Sal
2014/12/22 at 00:02
Reblogged this on josephdung.

joskid
2014/12/22 at 06:19
[... ] Startup article found at: https://krypt3ia.wordpress.com/2014/12/20/fauxtribution/ [...]

2 – Analysis of some of the IP addresses in the Sony hack – Official Offeryour.com Blog
2014/12/22 at 08:34
[... ] available and easy to use, and noted that almost all the IP addresses used in the Sony attack were proxies that were again open to the [...]

China slams cyberattacks after Sony job leads US to ask for help * The New World
2014/12/22 at 12:47
Nice blog entry! any chance for a link to the reputation checker you use?

Patrick
2014/12/22 at 14:41
I was using robtex

Krypt3ia
2014/12/22 at 14:45
[... ] un’impronta digitale degli hacker nordcoreani. Scettico anche un altro specialista noto come Dr.Krypt3ia. Ma anche Rob Graham e [...]

Tutto quello che c’è da sapere sul Sony Hack – enerdi.it
2014/12/22 at 15:08
[... ] as Rogers and fellow hacker “Dr. Krypt3ia” assert, the IP addresses cited by the FBI (in its earlier flash alert) are proxy addresses that, [...]

Ceiba3D Studio | These experts still don’t buy the FBI claim that North Korea hacked Sony
2014/12/22 at 15:26
I think occam’s razor takes you as far as “it is most likely someone who really wanted to hurt Sony” (it could still be someone counting on profiting from a side-effect of this saga, or otherwise, but somewhat unlikely, as many cogs in many systems have made this to be the shitstorm of FUD that it is, and they couldnt have been sure from the get-go).

Occam’s razor doesn’t take you from “someone who wanted to hurt Sony” to “most likely NK” – it just doesn’t. Loads of groups would have axes to grind with Sony.

yourad
2014/12/22 at 16:49
[... ] “Fauxtribution ?” at Krypt3ia (pseudonymous hacker), 20 December [...]

The FBI told their story about North Korea attacking Sony, Before we retaliate, read what they didn’t tell you, | Under the gray line
2014/12/22 at 17:20
[... ] Further, the FBI claimed that IP addresses of the hackers used were known to be used by North Korea. But that’s just silly. To start, hackers almost never attack from their own machines. Or rather, there is a Darwinian aspect here: hackers who attack from their own machines get arrested. Dr Krypt3ia took on the whole issue in some depth, FAUXTRIBUTION? [...]

We Don’t Know if North Korea is the Sony Hacker | Frankly Curious
556 Forensics » More on Sony and North Korea

Geography of Cyber Crime | Constant Geography

There’s certainly some missing evidence in the FBI report. Regarding the IP’s used, please have a read here:
https://krypt3ia.wordpress.com/2014/12/20/fauxtribution/

skepxx comments on “Attack Is Suspected as North Korean Internet Collapses” – Official Offervour.com Blog

Sometimes, there are just genius things that are said, but this has to be one of the best I’ve read in a long damn time:
“Let’s take a step back here and ponder the FBI statement today on Colonel Mustard in the study with the laptop before we go PEW PEW PEW ok?”
Just plain genius.

Jen

Sony Pictures Hacked Including Co-Chairman’s Confidential Emails - Page 9

Reblogged this on stacygturner and commented:
More on the Hack.

stacygturner

 […] che un’impronta digitale degli hacker nordcoreani. Scettico anche un altro specialista noto come Dr.Krypt3ia. Ma anche Rob Graham e […]

Tutto quello che c’è da sapere sul Sony Hack | Zazoom Social News

" maybe they are just happy to make the pronouncement that it was DPRK and leave it be"
That’s it. The truth doesn’t matter. To think it does with these people is quaint. They roll out the trusty old bogey man for the computer security legislation they hope to pass. Patsies who fit the narrative they’re pushing. The reality really is that cynical.
Oh and today, with the NK internet outwage… I think we can say that American is run by small children. ‘You stole our b movie’ now we ddos you. Pathetic.

Siiiiggh

Reblogged this on Kevin McCready and commented:
The “evidence” FBI is willing to share on alleged DPRK hack seems weak. FBI refuses to share other evidence.

kmccready

 […] Krypt3ia zieht aus den Informationen andere Schlüsse: Er sieht die Schuld Nordkoreas als nicht so klar erwiesen an wie das FBI. So sei die Malware nur signifikant ähnlich. Zudem stehe einer der angreifenden Server in New York, warum das FBI diesen noch nicht vom Netz genommen hat, ist für den Blogger schleierhaft. […]

Sony Hack: Nordkorea soll der Übeltäter sein | WorldNews

 […] of the attacks, jury is still out. According to FBI, evidence strongly backs this theory, however some researchers, including Bruce Schneier, remains unconvinced. Those opinions however, often does not fully […]

War over Cyber Pacific | lawsec

…GeoVision on 200.87.126.116….? interesting as f.

herderp
pour mener à bien des opérations de piratage informatique. Un élément peu solide également : pour certains experts, la dizaine d’adresse IP retrouvées sont essentiellement des proxys, utilisables par à peu […]

» Piratage Sony : la thèse Corée du Nord mise en doute

But Rogers says the “naivety of this statement beggars belief.” Just because a system with a particular IP address was used for a cyber-crime doesn’t mean that it will always be associated with crimes, he says. Many IP addresses are dynamic, meaning they are part of a pool that internet providers draw from and assign randomly. And the fact that some of those IP’s are known proxies meant to throw security researchers off the trail doesn’t necessarily mean North Korea is involved (there’s more technical detail here). […]

Some experts don’t believe North Korea was involved in Sony hack — Gigaom Search

I don’t get why you’re pointing out that most of the infrastructure could be accessed by anyone, or implying that the FBI was saying this was North Korean infrastructure. The statement of the FBI was that they “discovered that several Internet protocol (IP) addresses associated with known North Korean infrastructure communicated with IP addresses that were hardcoded into the data deletion malware used in this attack.” That’s not saying that the hardcoded IP addresses were controlled by the DPRK, it’s saying the hardcoded IP addresses are addresses that are known to have communicated with DPRK infrastructure. The argument is, given what little access the DPRK has to the internet and what few resources they utilize, it’s significant that the IP addresses the malware was communicating with were all addresses that DPRK infrastructure has communicated with. It’s a little like “the defendants have a hot pink Lambo, and the culprits were witnessed leaving the scene in a hot pink Lambo.” That’s circumstantial evidence that absolutely could be introduced as evidence into a court of law that the defendants were the culprits. Heck, it could be something as common as a Silver Outback and it would pass the “probative and not unduly prejudicial” test.

Whey Standard

 […] Świetna analiza dowodów w sprawie włamania do Sony Pictures […]

Weekendowa Lektura 2014-12-26 | Zaufana Trzecia Strona

pour mener à bien des opérations de piratage informatique. Un élément peu solide également : pour certains experts, la dizaine d’adresse IP retrouvées sont essentiellement des proxys, utilisables par à peu […]

Piratage Sony, la thèse Corée du Nord mise en doute | Evanade

CNN Hack. Some Facts | sladisworld

FBI Busted Falsely Blaming North Korea for Sony Hack | peoples trust toronto

FBI Busted Falsely Blaming North Korea for Sony Hack | ZombieMarkets

FBI Busted Falsely Blaming North Korea for Sony Hack

FBI Busted Falsely Blaming North Korea for Sony Hack | Eyes Open Report

Chongryn and Sony | Krypt3ia

2015/01/02 at 20:03
Follow “Krypt3ia”