info@thinkst.com
research@thinkst.com
http://www.thinkst.com

Client : **ThinkstScapes Trial**

# ThinkstScapes Ad-hoc Information Update 2014 / AH4

## Sony Pictures – Hidden Lessons

# ThinkstScapes Ad-hoc Information Update

## 2014 / AH4

## Sony Pictures – Hidden Lessons



## Introduction


*Sony Login Defacement*

On the 24th of November 2014, employees at Sony Pictures were greeted by a strange picture during their morning login which claimed that Sony had been hacked. Several social media accounts belonging to Sony Pictures were also hijacked, sending out tweets announcing the attack.

Unlike most garden variety attacks, the hackers leaked a combination of internal memos, sensitive information (belonging to both staff and celebrities) and Sony Pictures proprietary assets (upcoming unreleased movies were shared over BitTorrent).

Analysts have linked the attack to both Iran and/or North Korea (the DPRK) which has added even more drama to an already “hot” news story .We usually avoid commenting on news stories just because they are “hot” but we believe that there are a number of lessons hidden inside this incident that are worth paying attention to.


*Headlines*

We hope you enjoy this ad-hoc update!

*The explosion of security events worldwide means that industry participants are increasingly swamped by speakers vying for our attention. Ad-hoc updates are sent out to customers throughout the year as events worthy of notice transpire. Ad-hoc updates are usually brief, bursty and bustled out while events unfold.*

# Background

## Details on the Attack

Details on the attack are still fairly scant, with no indication of the original attack vector. While a few pundits have loudly proclaimed that this began with a phishing attack, at this stage, that is speculation driven by recent compromises. Actual forensic investigation results have not been released so far and, in at least one case, someone claiming to have participated in the attack intimated at inside help. So the vector by which malware made its way inside Sony Pictures is unknown.

What we do know however is that on 24 November, Sony Pictures staff were greeted with a desktop defacement instead of their login screens.[1] Some machines had been wiped, and Sony Pictures social media accounts were tweeting defacement messages.[2] URLs contained on the defacement page led to Zip files which included two long lists of filenames (showing strong evidence that the attackers had access to Sony Pictures files) plus a file containing contact information for the GOP group. On 28 November, 5 unreleased movies were seeded on torrent sites in an incident presumed to be related to the attack, and a trove of internal confidential documents were released on 1 December after being uploaded from a luxury hotel in Bangkok, Thailand.[3] On 5 December, the situation took a strange turn when Sony Pictures employees received an emailed threat from the group claiming responsibility for the hack, which urged them to denounce Sony or risk “danger” to themselves and their families.[4] Sony Pictures email and voice mail systems were down for a week while they tried to recover, and employees resorted to pencil and paper.[5]

In total the attackers claim to have pilfered 100TB of data, of which about 40GB has been released (and the rest is promised).[6] In any dump of this size there is bound to be a very wide variety of interesting data, and this dump is no exception. Journalists and security researchers trawling through the data have found *prima facie* evidence of gender pay disparities, passwords, strategy documents, critical self-reflection on the novelty of Adam Sandler movies, private keys, severance package details, personal information for employees past and present, and for actors and actresses (including passports, addresses and social security numbers).

Few details about the malware have been published except that the FBI released a memo shortly after the attack warning about new “destructive” malware.[7] AV companies have used various names in reference to the malware behind the Sony attack, including Volgmer, Destover,[8] and BKDR_WIPALL.[9] It’s also been tied to the DarkSeoul and Shamoon attacks due to its wiper behavior.[10]

With the paucity of information about the actual attack, we are left to speculate. The exploit or compromise vector has not been revealed, but according to the FBI alert, once installed the malware uses Windows Management Instrumentation (WMI) to spread. WMI usually requires administrator privileges (either local or domain). This, along with the extensive listings of files, implies that administrator level access was obtained in at least parts of the network. Curiously, the malware apparently included hardcoded IP addresses of internal servers as well as internal credentials, which in our view implies a period of observation and reconnaissance, or insider help.[11]

The final curiosity was that a good number of torrent seeders for the leaked data were traced to EC2 servers that appeared to be part of the Sony Playstation Network infrastructure. Considering the two companies are independent, it’s not clear what to make of this. If indeed PSN does suffer in this breach, then the fallout will be greater. One thing is clear: this story has yet to reach its climax, never mind its denouement.

---

1 http://www.reddit.com/r/hacking/comments/2n9zhv/i_used_to_work_for_sony_pictures_my_friend_still/

2 http://www.theverge.com/2014/11/24/7277451/sony-pictures-paralyzed-by-massive-security-compromise

3 http://www.bloomberg.com/news/2014-12-07/sony-s-darkseoul-breach-stretched-from-thai-hotel-to-hollywood.html

4 http://variety.com/2014/film/news/hackers-threaten-sony-employees-in-new-email-your-family-will-be-in-danger-1201372230

5 http://fusion.net/story/31116/inside-sony-pictures-employees-are-panicking-about-their-hacked-personal-data/

6 http://www.buzzfeed.com/tomgara/sony-hack

7 http://www.reuters.com/article/2014/12/02/us-sony-cybersecurity-malware-idUSKCN0JF3FE20141202

8 https://securelist.com/blog/research/67985/destover/

9 http://blog.trendmicro.com/trendlabs-security-intelligence/an-analysis-of-the-destructive-malware-behind-fbi-warnings/

10 https://securelist.com/blog/research/67985/destover/

11 http://arstechnica.com/security/2014/12/inside-the-wiper-malware-that-brought-sony-pictures-to-its-knees/?

## DPRK Unit 121


*North Korea attracting headline*

The press was quick to establish links between the hack and North Korea's Unit 121. The ostensible reason for the link: Sony Pictures has an upcoming movie release that displeases the North Korean government and could have motivated them into attacking the company to show its unhappiness.

To this end, unit 121 (and indeed North Korea) makes the perfect bogeyman: *"Cyber warfare provides [North Korea] a strategic advantage since outbound attacks are possible, but inbound attacks would have limited reach"*.[12] Much of the hype around their "hacking unit" however, seems wrapped in a typical news-flash borne hysteria. Re/Code documented their ability to jam GPS signals and their use of "auto-players" in some online games, which appears at odds with the direction of this attack.[13]


*A low-key headline from Vocativ*

A 2013 academic analysis ("Playing Blind-Man's Buff: Estimating North Korea's Cyber Capabilities") of the strength of North Koreas cyber capabilities posted reasonable looking numbers of a unit with around 3000 members, while sites today inflate that number to possibly 17,000 people.[14]

We believe however, that part of the hype over the cyber-capability of the DPRK is misplaced. As stated in past updates, we believe that the capacity to effectively attack organizations is purchasable on the open market and is not limited to nation states. In that sense, arguing over whether to attribute this attack to North Korea or copyright hacktivists or criminal extortionists distracts from looking forward and figuring out how to prevent future attacks (or at least detect them).

*Irrespective of whether or not this was the DPRK, recent events have shown the world that attack is a game everyone can play. It is clear that these sorts of attacks will happen more and more.*

12 http://h30499.www3.hp.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf

13 http://recode.net/2014/12/01/heres-what-we-know-about-north-koreas-cyberwar-army/

14 https://www.aspi.org.au/publications/journal-articles/playing-blind-mans-buff-estimating-north-koreas-cyber-capabilities

# Points worth Considering

## Attacks beyond DDoS and Defacement

For a long time companies have gotten away with lax security because attacks translated to DDoS or defacements. While these certainly had some impact, most companies figured out how to deal with DDoS a decade and a half ago. It is widely believed that defacements damage reputations but this doesn't particularly ring true, with the exception of a few notable cases. In some ways, this has filled security teams the world over with a type of complacency: Even if things went perfectly wrong, they were ok.

This has changed!

In previous updates we pointed out that the combination of WikiLeaks and Snowden revelations would work in concert to make potential attackers more aware of the benefits of hacking. Attackers who were historically technically focused, tended to focus on technical compromises, like “obtaining domain admin” or “gaining root on the web server”. Even when successful, the attacks needed to be translated to business-speak, but this information divide led to obvious (in hindsight) blind spots. The people who understood the importance of the company’s crown jewels didn't understand the technical ways these could be reached (or breached) and the people who understood the technical details made up their own rules for what was important.

This changes dramatically when faced with knowledgable insiders gone rogue, or informed outside attackers focused on well-chosen goals. It doesn't matter whether or not the Sony attackers achieved root privileges on the local file-server, since they were able to get read-access to the data store holding upcoming movies. It doesn't matter if the attackers were able to get remote code-execution on the HR system, as they were able to get ahold of memos that showed the inequities of staff salaries. It doesn't matter if the attackers obtained domain administrator privileges on the internal network, as they were able to grab passports and social security numbers of high profile celebrities.

*We believe that more and more attackers will focus less on technical wizardry and more on real world results. We believe that these attacks, in many cases will require less work, but will have disproportionately large results.*

## Sony and Accepted Risk

In 2007, Sony Pictures’ executive director of Security documented his attitude to risk and compliance in an article for CIO Online.[15] In an exchange that is bound to haunt them, Jason Spaltro said: “We’re trying to remain profitable for our shareholders, and we literally could go broke trying to cover for everything. So, you make risk-based decisions: What’re the most important things that are absolutely required by law?”


FEATURE

Your Guide To Good-Enough Compliance

Noncompliance is a fact of life as the list of security and privacy regulations grows. The key is knowing how to comply just enough so that you don't waste your time or bankrupt your company.

By Allan Holmes

CIO | Apr 6, 2007 8:00 AM PT

MORE LI

The Global

*Public statement of Sony Pictures’ approach*

That minimum compliance is the goal speaks volumes about Sony Pictures’ attitude towards the security of their data. Sony subsidiaries have fallen victim to tens of successful attacks in recent years, leading us to question the importance of security in the broader conglomerate.[16] That one can’t protect against all threats is a truism, and it is equally obvious that spending $10 to protect $5 worth of assets makes no sense, but breaches like Sony are a shining beacon leading to the inescapable conclusion that an appetite for risk cannot be determined in vacuum without considering *all* the assets being protected.

Were Sony able to calculate the impact of exposing Cameron Diaz and Sylvester Stallone’s passports?

When doing calculations, did they consider the possibility of having a number of potential Christmas blockbusters leaked to the world in early December?

15 www.cio.com/article/2439324/risk-management/your-guide-to-good-enough-compliance.html

16 http://attrition.org/security/rant/sony_aka_sownage.html

Did they calculate what it would cost to take a network that was as thoroughly compromised as theirs currently is, back to one they could trust? (We have been doing this for years and are not even sure it can be done without razing large tracts of the network to the ground.)

*A common theme over the past few years has been to chastise "technical-geeks" for failing to consider business needs while falling back to "risk-based calculations". It is our belief that while risk-based calculations make total sense, in many cases these risks are impossible to quantify without a deep understanding of the technical possibilities too. People who understand both sides of this deeply are unicorns that need to be sought out and used.*

## Pen Tests, AV and Assessments

Reports on the makeup of the Sony Pictures security team show a top heavy structure: *"Three information security analysts are overseen by three managers, three directors, one executive director and one senior-vice president"*.[17] While many have chosen to focus on the flaws inherent to this composition, we believe that no sane criticism can be made without knowing other (unavailable) pieces of information, like how many contractors were employed or how often they engaged with external security teams.

What can be criticized however is the press that seems surprised that Sony's investments in anti-virus technology and regular assessments failed to save them blushes (or pain). Many of the headlines around the attack mention the "destructive malware" which serves to bolster the fact that this is a malware problem (which then leads to the thinking that there could have been an anti-malware based solution).

*We have dedicated several previous issues to the fact that anti-virus software fares poorly against determined, sentient opponents. In the past few years, the general infosec population has largely, grudgingly accepted this. It seems that the trade press has yet to get the memo.*

The fact that Sony made use of assessments, also allows us to jump on top of an old soapbox of ours. The value (and danger) of penetration tests and assessments.[18]

*It is our firm belief that the way we perform security assessments is in desperate need of reform. At the very least, assessments need to be re-aimed to be more goal focused than their current incarnation.*

## Attribution is still hard

Although some analysts and media houses jumped immediately to the conclusion that the attacks were conducted by the DPRK, we would caution against leaping to such conclusions. Attribution is still difficult and false flag operations are trivial to pull off. At this point, it cannot even be conclusively shown if the attacks were indeed state sponsored, or just carried out by a single motivated individual or group.

Without access to internal Sony data, attributing the attack in this case is largely a red herring. Does the DPRK possess the skills to conduct such an attack? Sure they do, as do most other sovereign nation-states that have seen the obvious benefits of Computer Network Attacks (CNA) over the past few years. At this point, we should take for granted that most nations are in possession of skills to conduct CNA operations, and should realize that such skills will be up for hire to traditional criminals too.

*Attribution is still difficult and while the thought of state-funded attackers may make the attack seem more acceptable to Sony stakeholders, we need to accept that this hack is well within the reach of motivated enthusiasts.*

17 http://fusion.net/story/31469/sony-pictures-hack-was-a-long-time-coming-say-former-employees/

18 http://www.youtube.com/watch?v=GvX52HPAfBk

## Asymmetry and Power

This attack will cost Sony pictures many millions of dollars. Some of the damage (like the loss of key staff who have now seen sensitive management issues exposed in public) may well be completely unrecoverable. Sony Pictures will in all likelihood spend millions determining the causes, effects and reach of the breach and will then still have to deal with the loss of income from the leaked blockbusters and possible lawsuits from staff and celebrities who were exposed. For all of this damage, it is entirely conceivable that the attackers were a small group of moderately funded (or completely un-funded) hackers.

None of the attacker TTPs yet revealed required exclusive skills or nation-state resources which should be highly alarming. The force multiplier inherent to technology allows small groups of smart individuals to achieve disproportionately large results. This force multiplier allows 11 people to build an Instagram (worth billions of dollars) but also allows a small group of attackers to yield massive wins if correctly aimed. This makes attacks like this attractive to a number of players, and we are sure that we will see the frequency of such attacks rise.

> *It is entirely likely that the cost of attacking Sony Pictures was less than Sony Pictures spends on their annual company wide coffee purchases. This asymmetry is a fact which we have to live with until we learn how to successfully alter the economics of the game.*

## Detection and Response

Current reports hold that the attackers exfiltrated about 100 terabytes of data from the Sony network. This is both staggering and (to be completely honest) unsurprising. A default, holier-than-thou reaction to the report of the breach, is to ask: “how did they not notice all that data leaving their network?” But an honest assessment of many companies would reveal precious few that would. This paints a poor picture of the visibility we have on our networks, and is a solid indication of why we are in the state we are.

> *You should honestly determine if you would have noticed your companies crown jewels being exfiltrated over a prolonged period. Is this scenario covered in security testing and assessments?*

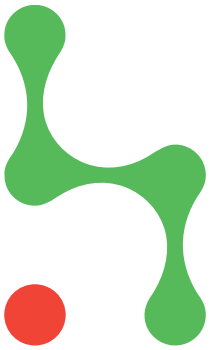
What is abundantly clear from the attack, is that Sony’s detection and response capabilities were about as poor as possible. The public timeline of events implies that the intrusion was only discovered when the attackers moved from theft to destruction, announcing their presence bombastically with the altered desktop.

> *Once more, an often repeated ThinkstScapes line is that while effort should definitely be expended in preventing compromise, it is increasingly obvious that this is a losing game. We should focus heavily in detecting, and responding to attacks instead.*

# Conclusion

This drama is far from over, and we are sure that more information will come to light. What we can say conclusively though, is that Sony Pictures has been comprehensively compromised, and recovering from this attack will cost millions of dollars and many man hours. Although we have seen lots of compromises in the past, this attack was different as it combined technical destruction with deliberate tactical “leaking” and asset theft.

We believe that these sorts of attacks will only increase in frequency, and suspect that many organizations are far from ready for them. We believe that a good deal of rethinking is necessary to re-aim corporate security efforts to handle these sorts of attacks.



thinkst
applied research