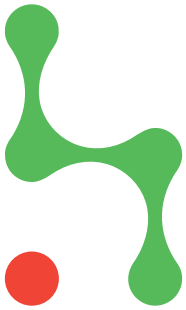
thinkst
applied research
info@thinkst.com
research@thinkst.com
http://www.thinkst.com

ThinkstScapes Ad-hoc Information Update 2015/ AH3

Big Breaches: OPM and Hacking Team



ThinkstScapes Ad-hoc Information Update

2015 / AH3

OPM & HackingTeam

Introduction

In the last month, two massive (and massively different) compromises have come to light: both the United States Office of Personnel Management (OPM) and Italian spyware company “Hacking Team” were revealed to be breached. Although the compromises have been widely covered and have even moved into the consciousness of the general public, we believe that both incidents contain some subtle lessons that are worth considering.

This ad-hoc update will aim to avoid both the general hyperbole or the moral judgements surrounding the hacks, and will focus instead on the tangible lessons we should be learning from both these incidents.

The OPM Hack

Background

The Office of Personnel Management (OPM) is a US federal agency responsible for a number of human resources functions that crosscut the US federal government. From their site, they are responsible for, among others:

1. [Conducting] background investigations for prospective employees and security clearances across government.
2. [Managing] pension benefits for retired Federal employees and their families. We also administer health and other insurance programs for Federal employees and retirees.[1]

If someone has been employed by the US federal government, it is almost certain their information has been processed by OPM. This data includes biographical information, social security numbers and so on. Health and insurance programs include medical information too, dating back to 1985.[2]

If either a military or civilian has applied for a security clearance, then the data they include along with their application is stored by OPM. [3] This is extremely sensitive, and applicants are required to disclose potentially damaging or embarrassing information, and is certainly personal (e.g. one million fingerprints were in the dataset).[4] Such information in the hands of foreign intelligence at the very least provides ammunition for blackmail and recruitment of intelligence assets.

On June 4th, 2015, OPM announced that it had suffered a breach in which records relating to 4 million people had been stolen.[5, 6] On Jun 22nd, that number was revised upwards to 18 million,[7] and on July 9th this was expanded to over 22 million people.[8] The later revisions came about as a separate but related breach was uncovered.

In trying to determine the scope of the breaches, it soon becomes clear that OPM and its contractors have suffered a series of breaches going back to at least March 2014.[9]

How the breach was discovered is not clear. Initial reports credited the Einstein intrusion detection system managed by US-CERT on behalf of the Department of Homeland Security.[10] However, a news report[11] and subsequent press release[12] suggest that the breach was uncovered by a vendor of forensic software during a product demonstration. However, OPM has denied that the vendor was responsible for the discovery.

What is clear is that the US has suffered a significant breach that affects its intelligence operations.

It is almost certain that the OPM breach was conducted by a foreign government given the targeted information and long term persistence. As always, attribution is tricky and public evidence in this regard has been non-existent; however this hasn't stopped the finger-pointing at China. What is interesting in the OPM breach is the difference in tone. Commentators like former head of the CIA and NSA,Michael Hayden, pointed out that such an attack would be both expected and acceptable from an intelligence point of view: "This is what serious nation-states do. All of them. There is no shame for China here. This is shame on us."[13]

In the interim, the director of the agency has resigned.

---

1 https://www.opm.gov/about-us/

2 http://www.reuters.com/article/2015/06/06/us-cybersecurity-usa-idUSKBN0OL1V320150606?irpc=932

3 Reportedly the CIA maintains its own clearance database separate from OPM, so this breach does not

4 This form, SF-86, is 127 pages long and includes plenty of opportunities to report personal sensitive information: http://www.opm.gov/Forms/pdf_fill/sf86.pdf

5 http://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html?_r=0

6 http://www.reuters.com/article/2015/06/06/us-cybersecurity-usa-idUSKBN0OL1V320150606?irpc=932

7 http://edition.cnn.com/2015/06/22/politics/opm-hack-18-milliion/index.html

8 http://www.reuters.com/article/2015/07/09/us-cybersecurity-usa-idUSKCN0PJ2M420150709

9 https://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/

10 http://www.bloomberg.com/news/articles/2015-06-06/china-hackers-got-past-costly-u-s-computer-security-with-ease

11 http://fortune.com/2015/06/12/cytech-product-demo-opm-breach/

12 http://www.prweb.com/releases/2015/06/prweb12787823.htm

13 http://www.washingtontimes.com/news/2015/jun/24/michael-hayden-opm-security-breach-blame-belongs-t/?page=all

Did OPM know what mattered?

Many organizations find it hard to secure their important data because they fail to truly understand what their important data is. They lack any sort of data classification, which makes it difficult to understand their threat model. It is interesting in the extreme therefore, that the OPM's *raison d'etre* is to be the central location for the collection and handling of classified personnel records. With the benefit of hindsight, it is painfully obvious that the data stored in the OPM needed to be afforded the greatest of protection. It certainly needed more protection than could be afforded to a bureaucratic government agency looking to hire "cybersecurity experts" post the breach.[14] So how did they get there, and are they outliers?

In our experience they are not. We have performed many assessments where the customers' crown jewels were trivially obtainable. It often happens because of the disconnect between people in the organisation who know what data and systems really matter, and people who know how compromises happen. We have also seen numerous penetration tests where red-teams gleefully point out their path to Domain Admin, which might get a slight rise out of the guys in the IT department but fails to have the desired effect on the board or C-Suite.

We need to ensure that we find a way to collaboratively understand our exposure, not just by having people perform penetration-tests, but by guiding the testing (and defence building) around the data and assets that matter most.

Did they know when it mattered?

By all accounts, this OPM breach appears to have taken place between March and December of 2014. The breach was supposedly discovered while evaluating security software in April of 2015 meaning that attackers were trawling through OPM system unnoticed for at least 4 months. While months (or even years) of undetected attacker activity is not unusual for breaches today, it remains a ridiculous and unacceptable position to be in.

It is probably the most repeated phrase in our ThinkstScapes issues, but bears repeating once more: Compromise is inevitable. We need to make sure that we are able to detect (and hopefully contain) malicious actors when they do (eventually) get through.

All your eggs in "a" basket?

A non-conventional idea has emerged over the last few years amongst security philosophers with the rise in popularity of WikiLeaks, "doxing" and leaks in general. The emerging thought lacks specifics on how it can be accomplished but suggests the following:

> If we can agree that everyone can be breached, and can agree that our data is what makes us worth attacking, then perhaps a solution is to no longer hold that data.

It sounds counter-intuitive initially, especially since the past few decades of management theory have largely served to convince us that more data is always useful. However with the flood of breaches in no danger of drying up, consider that holding some data is in itself an attack surface that on reflection might not be worth the risk.

Although a relatively new school of thought, we should carefully examine if we need to hold all the data we do. It is beyond contestation that merely collecting (or holding) some of this data increases our exposure to risk. What remains then is a reasonable examination if the benefits of holding the data outweigh the risk (or if it is technically possible to do without)

14 https://www.opm.gov/news/latest-news/announcements/cybersecurity-report/

The Hacking Team Hack

Background

On the night of Sunday July 5th, 2015 (European time), the Twitter account for Italian surveillance software vendor Hacking Team was taken over and used to announce a document drop of 400GBs of internal data including mails, source code and other files.[15] They had been thoroughly compromised. The choice of Twitter to announce the breach was particularly cunning, and news spread rapidly; the timing of the announcement was also fortuitous in that the company did not respond or acknowledge the incident until the following day, providing plenty of space for other commentators and speculators to fill the void.

Their response was to ask customers to stop using the software, putting investigations into limbo.[16]

The dump included source code to their commercial surveillance product, Remote Control System (RCS), in both the server installation as well as droppers and implants for numerous operating systems and platforms. Within the dump were at least two 0day exploits, for Flash and Windows. The Flash 0day was promptly included in malware kits.[17] Since then, a further Flash 0day has been uncovered.[18] It's likely further 0day will be uncovered, as the dump is really quite large.

Hacking Team is putting on a brave face, and claims they haven't lost any customers to the breach thus far.[19]

Late in the week, Wikileaks posted a searchable archive of the Hacking Team emails, covering more than a million emails sent both internally and externally. This has drawn in further journalists poring through the dump for reference to their countries or interests.[20]

The breach is interesting for a number of reasons which we touch on, and stands separate from breaches of other companies because Hacking Team operates at the nexus of information security research, vulnerability and exploit markets, law enforcement and intelligence. The players in this space are opaque, their tools shielded and their rules shrouded. The inclusion of the mail dump in the breach has already publicized exploit sales between companies forcing a hasty retreat by Netragard,[21] and it's again likely that further examples will be found.

Will Wassenaar help?

The recent inclusion of exploits and intrusion software under the Wassenaar agreement has been hotly debated as more and more security experts have begun to go on record warning against it.[22] The argument generally holds that the regulations will usher in "chilling effects" on researchers while being relatively toothless against bona fide "cyber arms dealers". The Hacking Team archives make it clear that they were:

a) Selling spyware that could be used against anyone;

b) Selling this spyware to everyone from slightly unlikable to despots to heavily sanctioned governments like Sudan;

c) Confident they were still complying with Wassenaar.

---

15 http://motherboard.vice.com/read/spy-tech-company-hacking-team-gets-hacked?as

16 http://motherboard.vice.com/read/hacking-team-asks-customers-to-stop-using-its-software-after-hack

17 http://www.securityweek.com/chinese-apt-group-uses-hacking-team%E2%80%99s-flash-player-exploit

18 https://www.fireeye.com/blog/threat-research/2015/07/cve-2015-5122_-_seco.html

19 http://arstechnica.com/security/2015/07/days-after-hacking-team-breach-nobody-fired-no-customers-lost/

20 https://wikileaks.org/hackingteam/emails

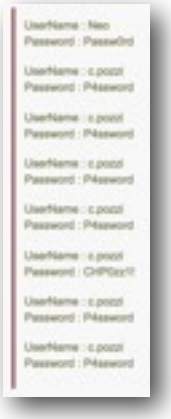
21 http://www.netragard.com/the-hackingteam-breach-eap

22 http://www.wired.com/2015/06/arms-control-pact-security-experts-arms/

Company spokesman Eric Rabe is now on record as saying that they cancelled the internal panel they previously used to decide on appropriateness of sales to certain clients once they began complying with Wassenaar.[23] This comes mere days after headlines were made of a university student who was coaxed into redacting portions of his thesis, for fear of running foul of Wassenaar.[24]

We remain convinced that regulation (especially when vaguely worded and far reaching) is a dangerous tool that should be used sparingly. It seems clear from both listed incidents that agreements like Wassenaar will weigh heavily on the minds of researchers while causing little trouble to actual arms dealers.

Passwords and Password ReUse.



Like most of the public hacks against well known security companies, the Hacking Team compromise exposed a number of horrible internal security practices. Chief amongst them is the oft demonstrated weak password management bugbear. One of the Hacking Team staff (a senior systems and security engineer according to LinkedIn) had his password list exposed revealing a number of weak permutations of the word “password”. This allowed the attack to spread (which makes it little surprise that the same engineer had his Twitter account hijacked in the attack). Horrible. Common. And yet so easily preventable.

A quality password manager is worth its weight in gold. If your organization is not using some sort of password vault for shared access accounts, its almost certain they are doing this horribly too.

The need for compartmentalization

The attacker who compromised Hacking Team appears to be the same attacker who compromised the Gamma Group (makers of the FinFisher spyware suite) in August of 2014.[25] It is worth noting that while that attack also resulted in the release of about 40GB of data to the world, the full impact of the attack was not as all encompassing as the data released against Hacking Team. Gamma appeared to be doing some reasonable form of compartmentalization, so a single breach did not result in *everything* being exposed.

We should take this lesson to heart. Compromises will happen, but a single compromise should not easily lead to it being a complete security melt-down. Different zones of trust that are enforced is ancient, obvious advice that is still disturbingly absent.

400gb!

The Hacking Team breach resulted in 400GB of internal data being distributed to the world. The Sony Pictures hackers claimed to have exfiltrated over 100 terabytes of data from the Sony network[26] and the FinFisher hack resulted in a 40GB release. Almost everyone who hears this, would first react with: *How do you not notice 400gb of data leaving your network?* But an honest reflection would point out how few companies would actually realize that this was happening.

Anomaly detection on networks has largely over promised and under delivered, but some simple heuristics should be identified and reacted to.

23 https://www.instapaper.com/read/609292916

24 http://arstechnica.com/security/2015/07/student-claims-wassenaar-agreement-prevents-him-from-publishing-dissertation/

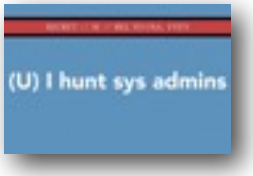
25 http://thehackernews.com/2014/08/company-that-sells-finfisher-spying.html

26 http://sonyhack.gawker.com/everything-you-need-to-know-about-sonys-unprecedented-h-1671217518

Offense vs Defense

An age old argument in infosec aims to pick a hero between offensive and defensive actors. As we have stated previously, we believe this is a false dichotomy and subscribe strongly to building defenses guided by (insights derived from) offense. If nothing else, the poor security practices employed by Hacking Team and the complete lack of detection of their comprehensive compromise should deflate arguments that ascribe super security powers to attack / red teams.

Watching the Watchers



Edward Snowden was a system administrator that (ab)used his access to ransack the NSA. Some of the information he leaked showed how intelligence agencies deliberately targeted sys-admins because of their privileged level of access.[27] The Hacking Team incident too shows signs that a sys-admin compromise played a large part of the problem. These are not isolated incidents. Targeting the people who administer your networks is a direct path to large scale network compromise. We should be aware of this, and should shape both architecture and detection processes around this.

It is clear that sys-admins are widely targeted by sophisticated attackers. Ensure that detection and containment around privileged access use is in place to limit the scope of compromises.

Everyone is vulnerable

It is generally accepted today that preventing compromise is impossible. We have all the proof now that everyone can be taken. What separates companies that can bounce back, from organizations that are devastated however, is largely how they detect and react to the compromises. Preparing for this happens long before the actual incident.

It is interesting to note that the evidence so far suggests that the same actor took down both GammaGroup and HackingTeam. It says a lot about the state of security world-wide, that a single determined attacker would be able to target and compromise multi-million dollar security companies (in what appears to be his spare time.)

This forces us to ask ourselves the obvious, awkward question: Would we do any better?

0days Happen

Once more (as with the HBGary compromise back in 2011) the HackingTeam hack gives us an insight into the normally veiled world of 0day purchases. An email dated October 2014, contains a 135 page PDF attachment titled “Assets Portfolio”[28] from “Vulnerabilities Brokerage International”. Thats about 120 pages of exploits from a single trader. Trawling through the emails reveals numerous other 0day traders, from one shot sales for $105,000 [29] to regular sales from groups like ExploitHub.

Some people have been quick to make headlines of 0days revealed in the dump and have rushed vendors to issue out of band patches for the revealed bugs. While patches would be good, the much bigger lesson to be learned here is that 0days exist *and are accessible*. They are easily distributed and there will be little chance of this trade disappearing. There is very little that we can to to stop being compromised by a 0day (or a series of chained 0days). We need to make sure though, that a single 0day would not immediately translate to being the worst days of our lives.

We need to make sure that our networks and defences are built with the full realization that 0days exist (and probably are in circulation) for the services we are exposing. We need to make sure that containment and detection are in place and that a single 0day does not result in our complete undoing.

---

27 https://firstlook.org/theintercept/2014/03/20/inside-nsa-secret-efforts-hunt-hack-system-administrators/

28 https://wikileaks.org/hackingteam/emails/fileid/45441/20892

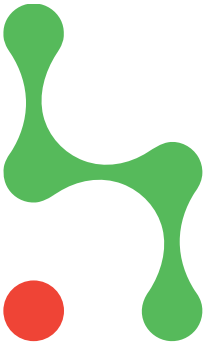
29 https://wikileaks.org/hackingteam/emails/emailid/15116

Conclusion

Two significant breaches occurred in the past month, the sounds of which will echo for some time to come. In the US Office of Personnel Management breaches, confidential data of over 22 million potential or actual employees of the US federal government was accessed. The breach is important as it's a clear example of cyber espionage, and a likely outcome is significant changes in US policy.

The second major breach was of a much smaller target, an Italian surveillance software vendor called Hacking Team. That breach has pulled back the curtain on the world of exploit markets and surveillance software, and shines a particularly bright light on how security research gets monetized and ultimately traded for tax revenues. The breach comes at a time when the US is discussing how to enforce the recent expansion of the Wassenaar agreement to include types of security software, and will likely inform proposals going into regulation.

Both breaches tread different types of ethical lines, and there are other publications in which those are explored in detail. As always, we've focused on the lessons to be learned from these breaches, to take into your own organization.



thinkst
applied research