Anthem Hack

PREPARED BY:

RASHA ALTAMIMI

NIHARIKA ARORA

AMAL KADI

What happened?

Earlier this year, the major health insurance company Anthem (previously known as WellPoint Inc.) have confirmed it had suffered a cyberattack (a phishing attack), leading to the theft of tens of millions of records.

How many people are impacted?

Approximately 80 million customers' personal information may have been compromised. This includes employee, Anthem's affiliated health plan members and other consumers within their system.

Timeline

- April 2014: attackers gained access to the Anthem's database. (*undisclosed*)
- Dec 10 2014: a query retrieving 80 mil records was initiated.
- Jan 27 2015: the compromise was discovered.
- Jan 29 2015: Anthem alerted federal authorities and other entities.
- Feb 4 2015: the company disclosed the breach to the public.

What did the cyber attackers access?

Accessed information may have included:

- Names
- Dates of birth
- Social Security numbers
- Health care ID numbers
- Home addresses
- Email addresses
- Work information like income data

Source:
www.anthemfacts.com

We don't believe these kinds of information were targeted or accessed:

- Credit card or banking information
  Medical information like claims, test results or diagnostic codes

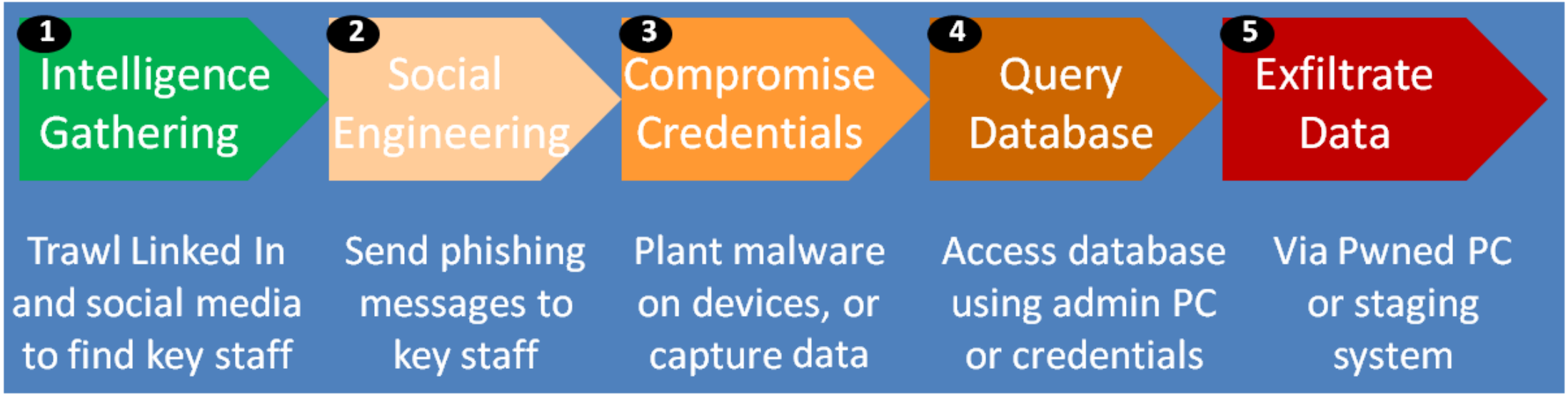
Data wasn't encrypted

Some like the Wall Street Journal were making claims that this attack was possible because the personal data in this database was not encrypted.

But if the attacker had access of the system and had the required credentials to decrypt the data, then encrypting data would not have avoided this attack.

Under the federal Health Insurance Portability and Accountability Act (HIPAA), health insurance companies are not required to encrypt the data stored on their servers.

How could a phishing attack like this happen?

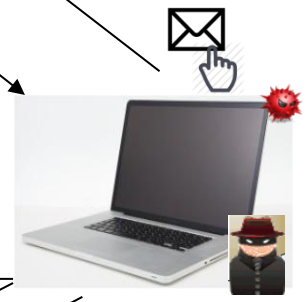


2. The victim clicks on the link to we11point.com from the email

3. Installs several malware on victim's system

Attacker

1. Sends an email with link to we11point.com (impersonating as Wellpoint)



Victim

5b. Sends the credentials and access to the victim's system

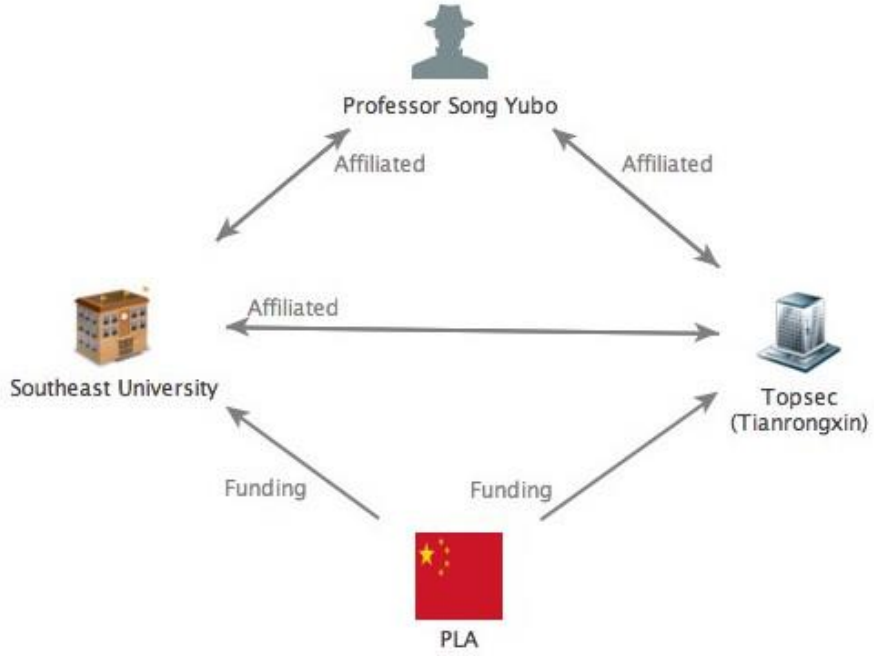
5a. Accesses the Anthem database using credentials

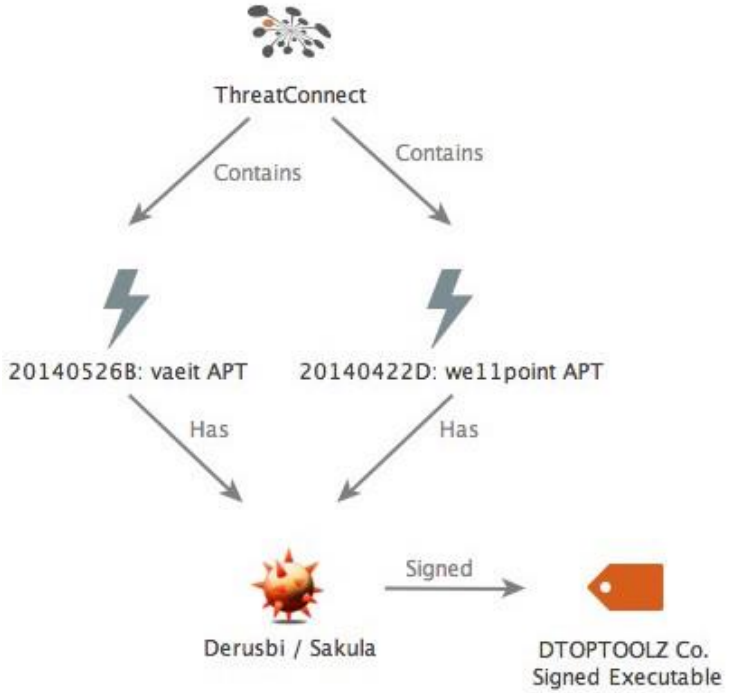
6. Query resulting in 80 million rows as output

1	Domain Name: WE11POINT.COM	1	Domain Name: WE11POINT.COM
2	Registry Domain ID: 1855543298_DOMAIN_COM-VRSN	2	Registry Domain ID: 1855543298_DOMAIN_COM-VRSN
3	Registrar WHOIS Server: whois.godaddy.com	3	Registrar WHOIS Server: whois.godaddy.com
4	Registrar URL: http://www.godaddy.com	4	Registrar URL: http://www.godaddy.com
5	Update Date: 2014-04-21 03:13:19	5	Update Date: 2014-04-21 03:21:23
6	Creation Date: 2014-04-21 03:13:19	6	Creation Date: 2014-04-21 03:13:19
7	Registrar Registration Expiration Date: 2015-04-21 03:13:19	7	Registrar Registration Expiration Date: 2015-04-21 03:13:19
8	Registrar: GoDaddy.com, LLC	8	Registrar: GoDaddy.com, LLC
9	Registrar IANA ID: 146	9	Registrar IANA ID: 146
10	Registrar Abuse Contact Email: abuse@godaddy.com	10	Registrar Abuse Contact Email: abuse@godaddy.com
11	Registrar Abuse Contact Phone: +1.480-624-2505	11	Registrar Abuse Contact Phone: +1.480-624-2505
12	Domain Status: clientTransferProhibited	12	Domain Status: clientTransferProhibited
13	Domain Status: clientUpdateProhibited	13	Domain Status: clientUpdateProhibited
14	Domain Status: clientRenewProhibited	14	Domain Status: clientRenewProhibited
15	Domain Status: clientDeleteProhibited	15	Domain Status: clientDeleteProhibited
16	Registry Registrant ID:	16	Registry Registrant ID:
17	Registrant Name: wen ben zhou	17	Registrant Name: ad fire
18	Registrant Organization:	18	Registrant Organization:
19	Registrant Street: wen ren zheng fei ren chun 120hao	19	Registrant Street: fdsbcacfdt43
20	Registrant City: xiamen	20	Registrant City: new
21	Registrant State/Province: fu jian	21	Registrant State/Province:
22	Registrant Postal Code: 366115	22	Registrant Postal Code: 366512
23	Registrant Country: China	23	Registrant Country: Cayman Islands
24	Registrant Phone: +86.5925035801	24	Registrant Phone: +65.561235001

Who?

- Professor Song Yubo of Southeast University's Information Security Research Center, which is sponsored by Chinese government, posted a "Talent Cup" tournament challenge to his information security students.





VAEIT fake website

28	Registrant Email: li2384826402@yahoo.com	28	Registrant Email: yXDtqMRNdM@gmx.com
29	Registry Admin ID:	29	Registry Admin ID:
30	Admin Name: li ning	30	Admin Name: Natasha Romanoff
31	Admin Organization:	31	Admin Organization: vaeit
32	Admin Street: guangdongsheng	32	Admin Street: USA
33	Admin City: guangzhoushi	33	Admin City: USA
34	Admin State/Province: Alabama	34	Admin State/Province: American Samoa
35	Admin Postal Code: 54152	35	Admin Postal Code: 54321
36	Admin Country: United States	36	Admin Country: United States
37	Admin Phone: +1.4805428751	37	Admin Phone: +1.1234567890
38	Admin Phone Ext:	38	Admin Phone Ext:
39	Admin Fax:	39	Admin Fax:
40	Admin Fax Ext:	40	Admin Fax Ext:
41	Admin Email: li2384826402@yahoo.com	41	Admin Email: yXDtqMRNdM@gmx.com
42	Registry Tech ID:	42	Registry Tech ID:
43	Tech Name: li ning	43	Tech Name: Natasha Romanoff
44	Tech Organization:	44	Tech Organization: vaeit
45	Tech Street: guangdongsheng	45	Tech Street: USA
46	Tech City: guangzhoushi	46	Tech City: USA
47	Tech State/Province: Alabama	47	Tech State/Province: American Samoa
48	Tech Postal Code: 54152	48	Tech Postal Code: 54321
49	Tech Country: United States	49	Tech Country: United States
50	Tech Phone: +1.4805428751	50	Tech Phone: +1.1234567890

Topsec 2014 Talent Cup

25	Registrant Email: li2384826402@yahoo.com
26	Registry Admin ID:
27	Admin Name: li ning
28	Admin Organization:
29	Admin Street: guangdongsheng
30	Admin City: guangzhoushi
31	Admin State/Province: Alabama
32	Admin Postal Code: 54152
33	Admin Country: United States
34	Admin Phone: +1.4805428751
35	Admin Phone Ext:
36	Admin Fax:
37	Admin Fax Ext:
38	Admin Email: li2384826402@yahoo.com
39	Registry Tech ID:
40	Tech Name: li ning
41	Tech Organization:
42	Tech Street: guangdongsheng
43	Tech City: guangzhoushi
44	Tech State/Province: Alabama
45	Tech Postal Code: 54152
46	Tech Country: United States
47	Tech Phone: +1.4805428751

28	Registrant Email: TopSec_2014@163.com
29	Registry Admin ID:
30	Admin Name: Top Sec
31	Admin Organization: TopSec
32	Admin Street: china
33	Admin City: china
34	Admin State/Province: china
35	Admin Postal Code: 100000
36	Admin Country: China
37	Admin Phone: +1.82776666
38	Admin Phone Ext:
39	Admin Fax:
40	Admin Fax Ext:
41	Admin Email: TopSec_2014@163.com
42	Registry Tech ID:
43	Tech Name: Top Sec
44	Tech Organization: TopSec
45	Tech Street: china
46	Tech City: china
47	Tech State/Province: china
48	Tech Postal Code: 100000
49	Tech Country: China
50	Tech Phone: +1.82776666

What could have they done to prevent such an attack

- Educate employees on phishing attacks and other security measures.
- Use Principle of least privilege. And ensure that the programs asking for administration-level access are legitimate.
- Train employees not to open websites on the Internet unless they have been scanned for viruses. Simply visiting a compromised Web site can cause infection.
- Deny all incoming connections and only allow services they explicitly want to offer to the outside world.

References

- http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/
- http://abcnews.go.com/Business/anthem-cyber-attack-things-happen-personal-information/story?id=28747729
- http://www.theverge.com/2015/2/6/7991283/anthem-hack-encrypted-data
- http://www.cnet.com/news/anthems-hacked-customer-data-was-not-encrypted/
- http://www.washingtonpost.com/blogs/the-switch/wp/2015/02/27/security-firm-finds-link-between-china-and-anthem-hack/
- http://www.threatconnect.com/news/the-anthem-hack-all-roads-lead-to-china/
- http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?name=TROJANSPY:WIN32/DERUSBI.A
- http://www.symantec.com/security_response/earthlink_writeup.jsp?docid=2015-020623-0740-99
- http://whois.domaintools.com/
- http://security-architect.com/encryption-probably-wouldnt-have-prevented-the-anthem-breach/

Questions?

Thank you ☺