The OPM Breach of 2014 -2015

By Sophia Lionberger
CITC-1351 025
Principles of Information Assurance
Spring Semester, 2019
Professor George Meghabghab

Identify:
Office of Personnel Management

- Government human resources company.
- Performs background checks for all secret clearances issued by the U.S. Government and appoints impartial judges to oversee each US government agency
- Not directly funded by the US government; however it has contracts with every US government agency and collects about $2 billion in revenue from the government every year.
- Executive officer is appointed by the President.

Protect:
The First Failures

- Even though OPM was warned by US-CERT about APTs as early as 2005, they failed to maintain up-to-date best practices; they did not even have two-factor authentication until early 2015. By this point, a rootkit had already been installed.
- OPM did not implement the software solutions recommended by its board of IT directors until a year after the first attack was detected-- far too late.

Detection:
The Glass is Half Empty

- OPM detected hacker X1 in March 2014 as they exfiltrated reference materials on OPM server architecture. X1 is identified as PRC-sponsored hacker group Axiom based on the use of the HiK[illegible] software and attack strategy.
- The second hacker, likely coordinating with the first, was not detected until over a year later, in April 2015. Once installed, up-to-date threat detection software “lit up like a Christmas tree”, finally revealing the extent to which OPM servers had been compromi[illegible].
- Malicious activity was detected referring to domain names registered to “Steve Rogers” and other Marvel superhero aliases – an attack pattern characteristic of the PRC-sponsored hacker group Deep Panda.

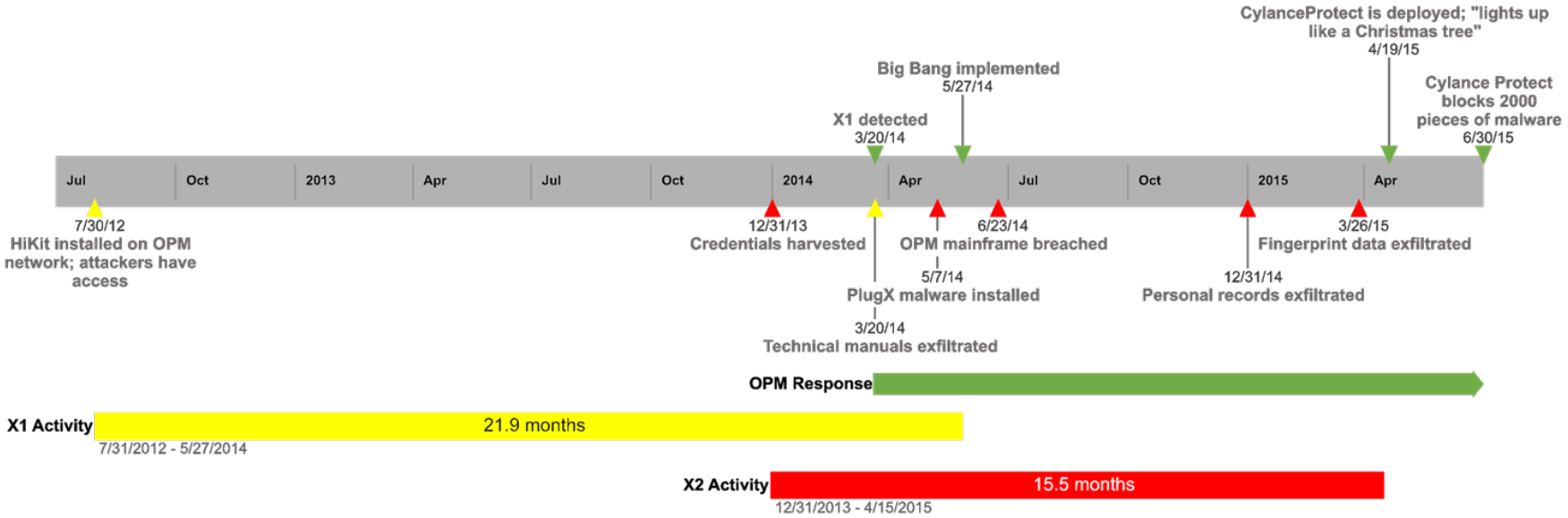
Response:
Too little, too late

- In May 2014, OPM was able to shut hacker X1 (Axiom) out of their system through the implementation of “Big Bang”, a strategy that involved shutting down and resetting the servers.
- Unfortunately, a rootkit installed by hacker X2 (Deep Panda) survived the purge and they were able to maintain their foothold for a year to come.
- By the time OPM detected and took the decisive action to remove X2 in April of 2015, the damage was already done.

Recovery: Impossible

- The attackers, likely employed by the People's Republic of China, were able to steal background information on twenty million people.
- The information includes all the "dirt", compromising information, that could possibly be found on anybody who applied for a security clearance in the last twenty years, along with their families.
- This puts the currently existing US intelligence community at a disadvantage relative to PRC and its allies that will last a generation or more.
- Five million fingerprints were also stolen, along with identity documents such as Social Security Numbers.

OPM Breach Timeline



“The Damage Done”

“We cannot undo this damage. What is done is done and it will take decades to fix.”

-- John Schindler, former NSA officer

“My SF-86 lists every place I’ve ever lived since I was 18, every foreign travel I’ve ever taken, all of my family, their addresses. So it’s not just my identity that’s affected. I’ve got siblings. I’ve got five kids. All of that is in there.”

-- James Comey, former Director of the FBI

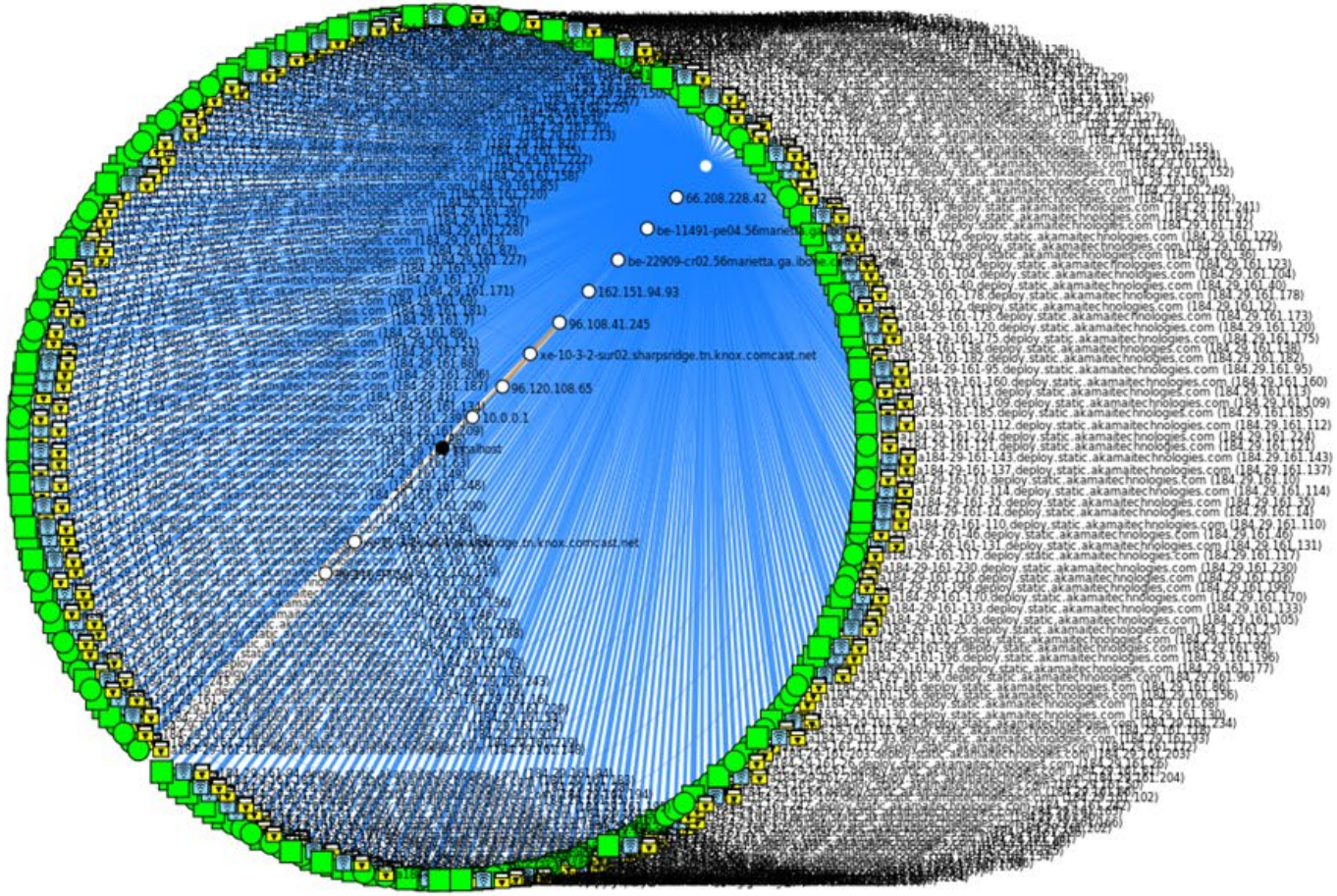
“[OPM data] remains a treasure trove of information that is available to the Chinese until the people represented by the information age off. There’s no fixing it.”

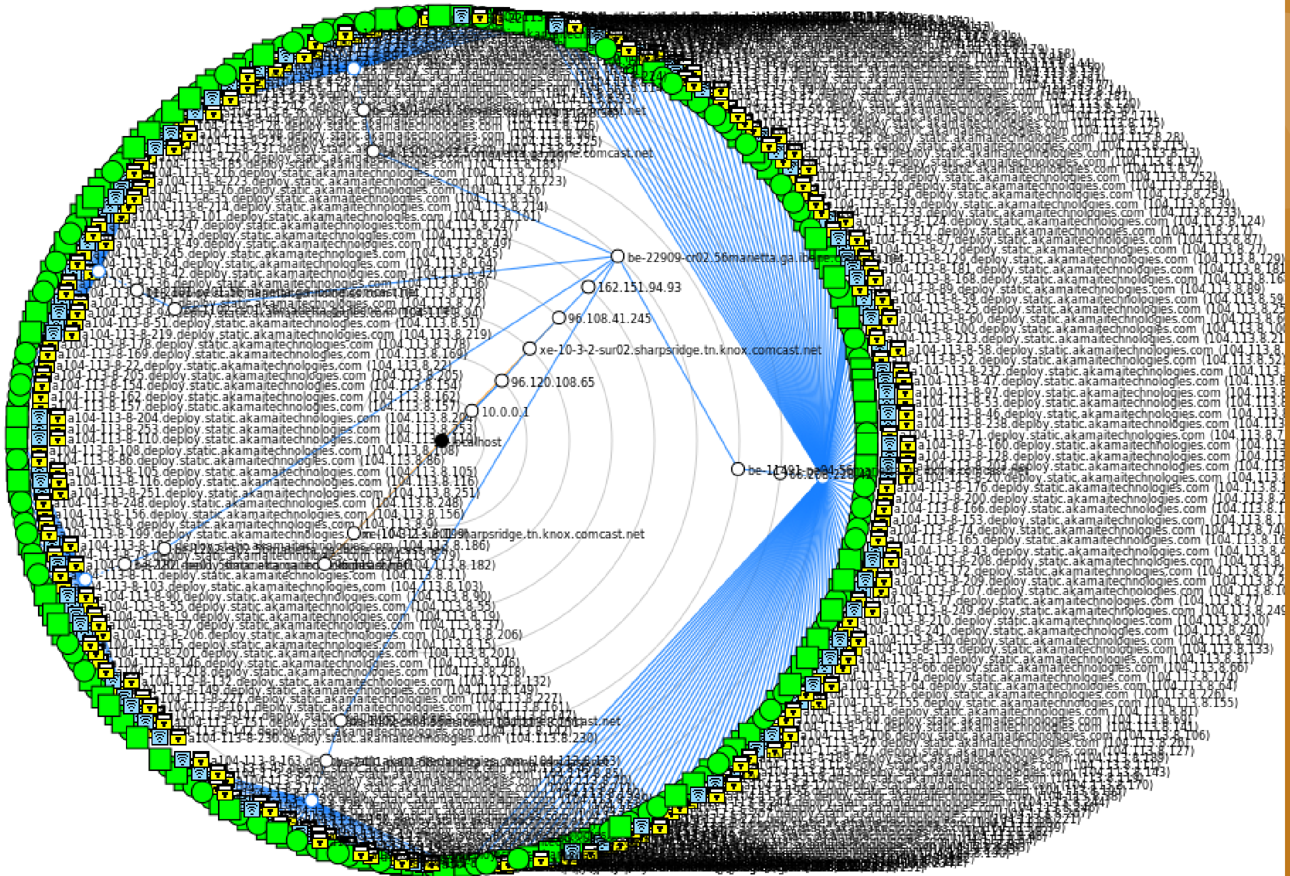
-- Michael Hayden, former Director of the CIA

Source: The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation

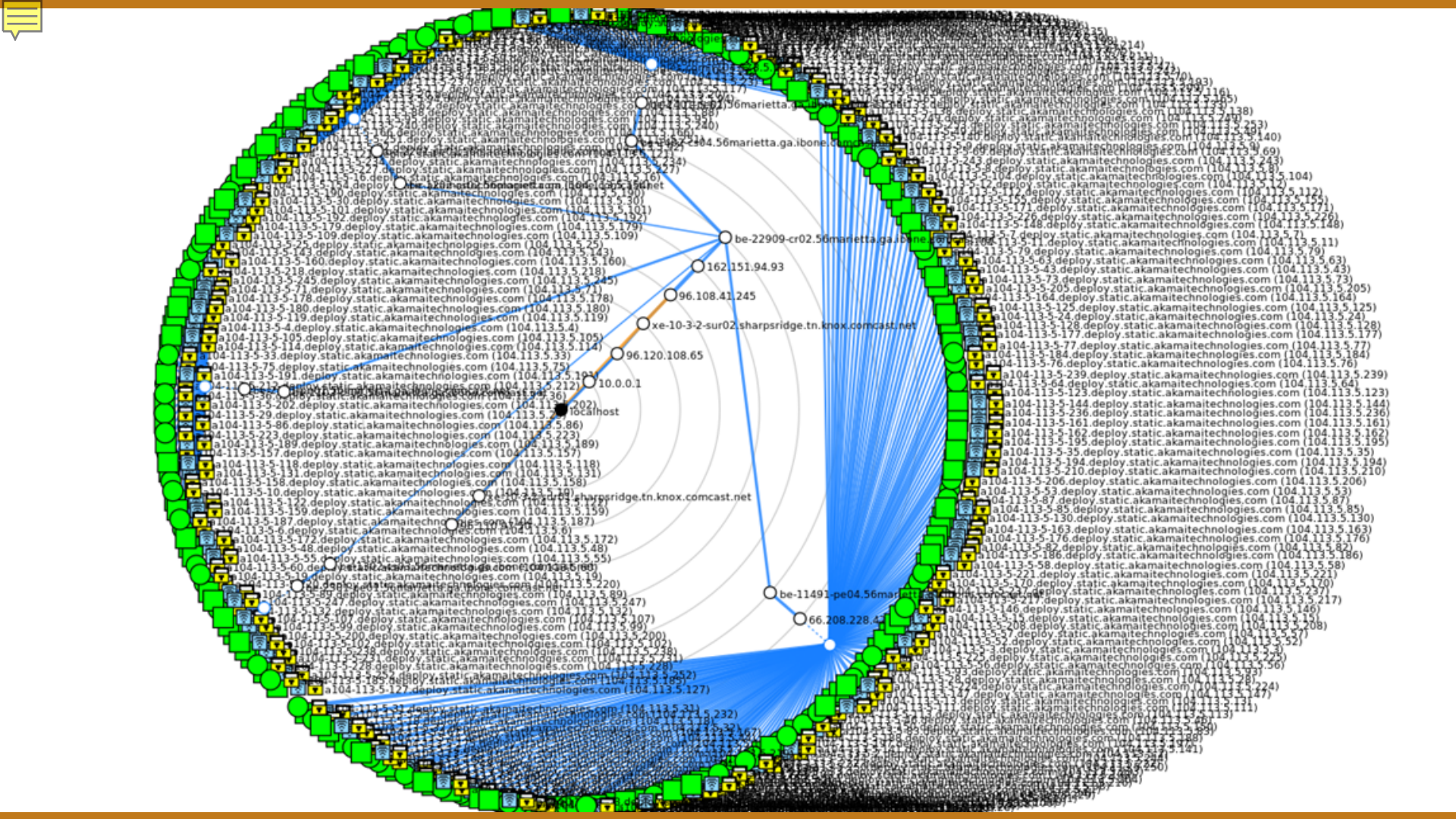
OPM.gov: Present security profile

- OPM's servers are routed through a massive network of geographically localized proxies, hosted by Akamai GHost.
- None of OPM's own servers appear to be directly accessible via the Internet.
- Open ports: 80, 443.


66.208.228.42
be-11491-pe04.56marietta.ga.ibone.
be-22909-cr02.56marietta.ga.ibone.
162.151.94.93
96.108.41.245
xe-10-3-2-sur02.sharpsridge.tn.knox.comcast.net
96.120.108.65
10.0.0.1
localhost



162.151.94.93
96.108.41.245
xe-10-3-2-sur02.sharpsridge.tn.knox.comcast.net
96.120.108.65
10.0.0.1
a104-113-8-204.deploy.static.akamaitechnologies.com (104.113.8.204)
a104-113-8-253.deploy.static.akamaitechnologies.com (104.113.8.253)
a104-113-8-105.deploy.static.akamaitechnologies.com (104.113.8.105)
a104-113-8-116.deploy.static.akamaitechnologies.com (104.113.8.116)
a104-113-8-251.deploy.static.akamaitechnologies.com (104.113.8.251)
a104-113-8-230.deploy.static.akamaitechnologies.com (104.113.8.230)


be-22909-cr02.56marietta.ga.ibone.comcast.net
162.151.94.93
96.108.41.245
xe-10-3-2-sur02.sharpsridge.tn.knox.comcast.net
96.120.108.65
10.0.0.1
localhost
be-11491-pe04.56marietta.ga.ibone.comcast.net
66.208.228.42

Sources

https://web.archive.org/web/20160907174011/https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf

http://www.opm.gov