Battlefield Network

Speaker Info – Tal Be’ery

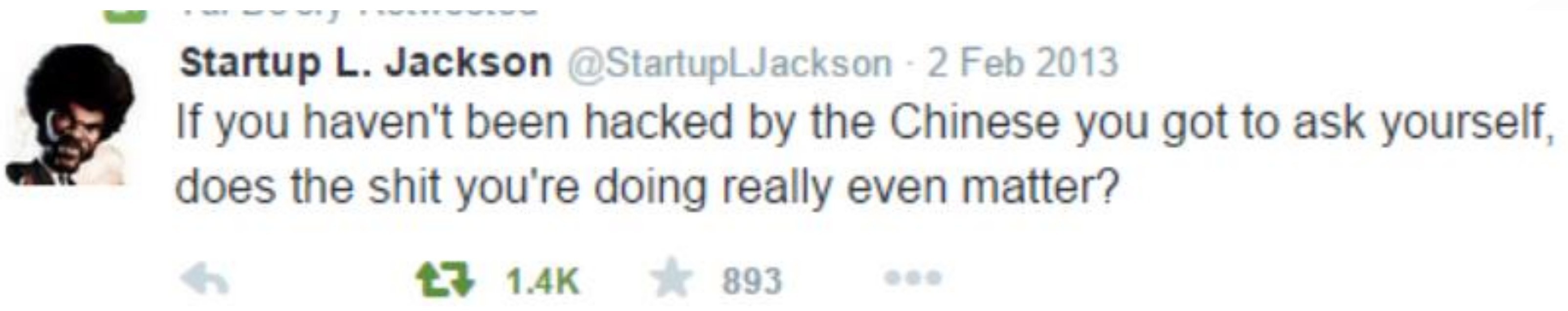
- Senior Security Research Manager @Microsoft
- Former VP for Research @Aorato (Acquire by Microsoft)
- 15 years of security research
- Author of the TIME attack on SSL
- Regular speaker in Industry’s top conventions
- Named a “Facebook Whitehat”
- Twitter: @TalBeerySec

Agenda

- Intro
  - Current state of affairs
  - Why do we fail
- Know the enemy
  - The modified Kill chain
- Know thyself
  - What is normal?
- Choose the right battlefield
  - Network based detection of Reconnaissance and Lateral Movement

State of affairs

- 90% of large organizations and 74% of small businesses reporting a security breach
- Data breach incidents experienced by large businesses cost at least £1.5 million on average and in some cases more than £3m
- Average time to breach detection: eight months
- Most breaches are not detected internally

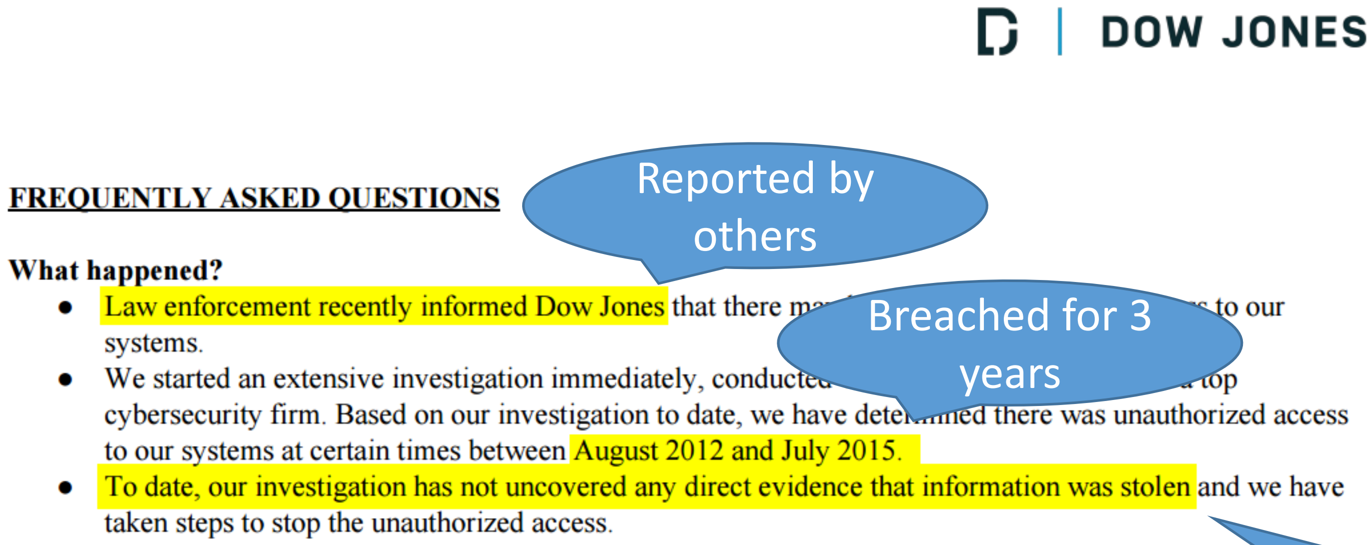


Startup L. Jackson @StartupLJackson · 2 Feb 2013

If you haven't been hacked by the Chinese you got to ask yourself, does the shit you're doing really even matter?

Test Case: The Dow Jones Breach

- Reported this month (October 9th 2015)



DOW JONES

FREQUENTLY ASKED QUESTIONS

What happened?

- Law enforcement recently informed Dow Jones that there ma s to our systems.
- We started an extensive investigation immediately, conducted top cybersecurity firm. Based on our investigation to date, we have dete ned there was unauthorized access to our systems at certain times between August 2012 and July 2015.
- To date, our investigation has not uncovered any direct evidence that information was stolen and we have taken steps to stop the unauthorized access.

Reported by others

Breached for 3 years

In other words:
We still don’t know what happened

Why do we Fail?

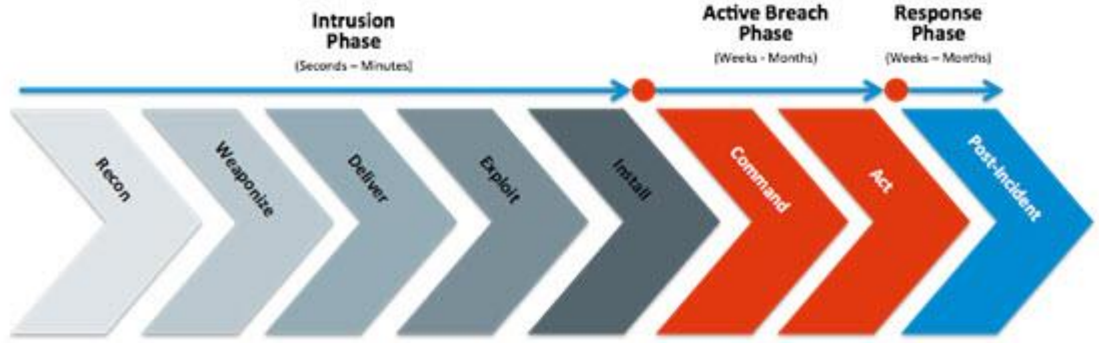
- “If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”
- **We don’t Know the Enemy**
- **We don’t know ourselves**

https://upload.wikimedia.org/wikipedia/commons/3/37/Enchoen27n3200.jpg

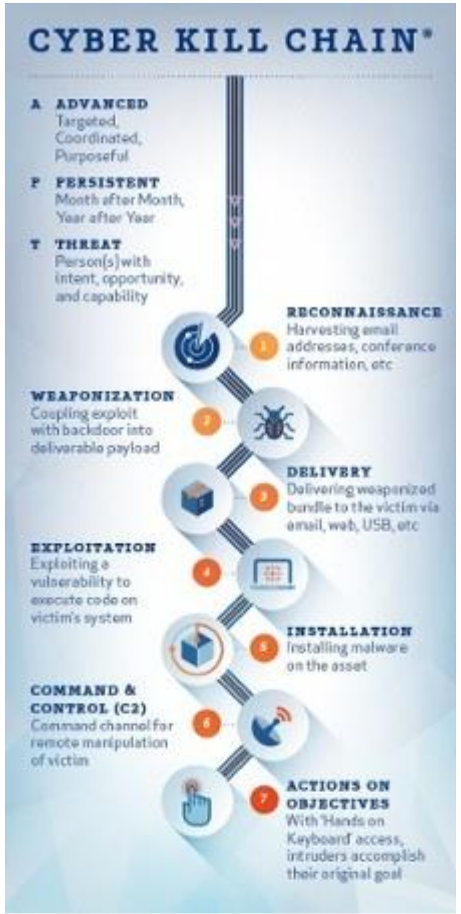
Know the Enemy

The Cyber Kill-chain

- Presented by Lockheed Martin, 2010
- Main achievements
  - Knowing the enemy: The first widely accepted model of APT attackers
  - Important insight: It’s a chain!
    - The chain is as strong as its weakest link
    - Defender get to choose where to break the chain

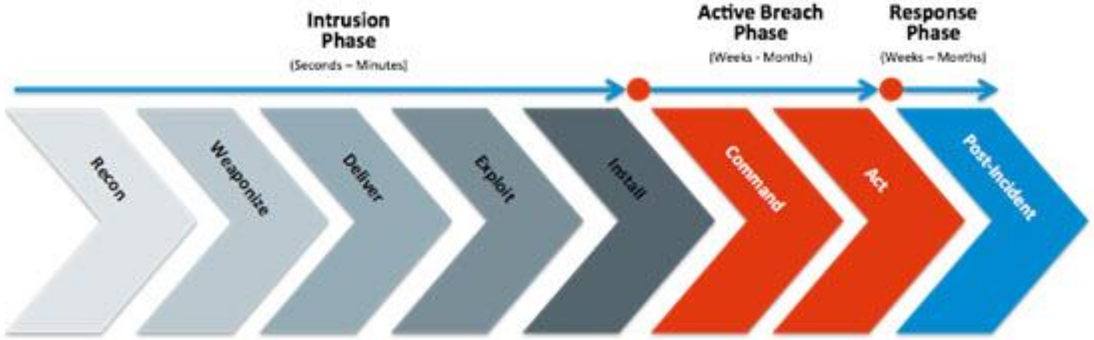


Graphic 1 - Lockheed Martin Cyber Kill Chain


CYBER KILL CHAIN®
A ADVANCED
Targeted, Coordinated, Purposeful
P PERSISTENT
Month after Month, Year after Year
T THREAT
Person(s) with intent, opportunity, and capability
1 RECONNAISSANCE
Harvesting email addresses, conference information, etc
2 WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3 DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc
4 EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5 INSTALLATION
Installing malware on the asset
6 COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7 ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goal

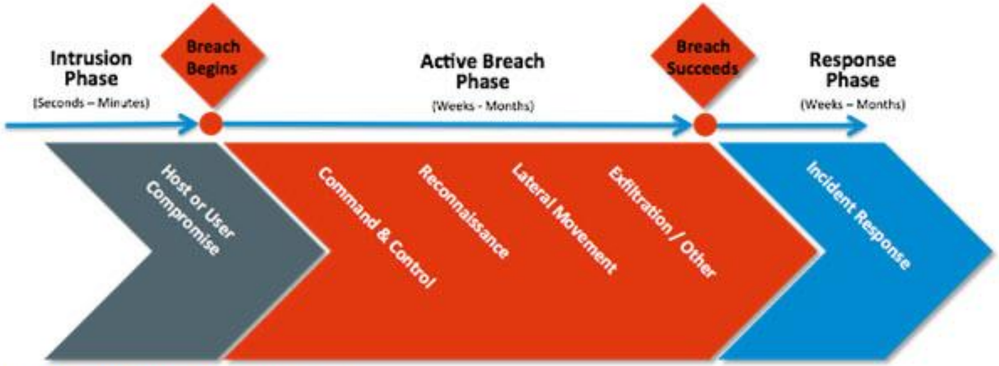
Modifying The Kill-chain #1

- The original kill chain puts too much emphasis on initial infection



Graphic 1 - Lockheed Martin Cyber Kill Chain

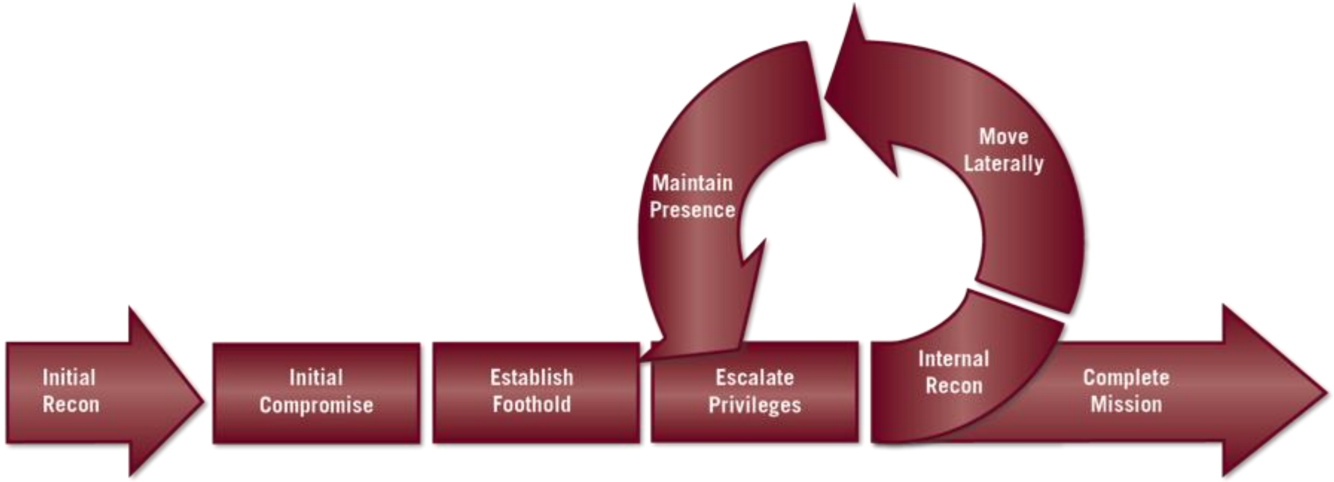
- LightCyber's version:



Graphic 2 - Modified Cyber Kill Chain

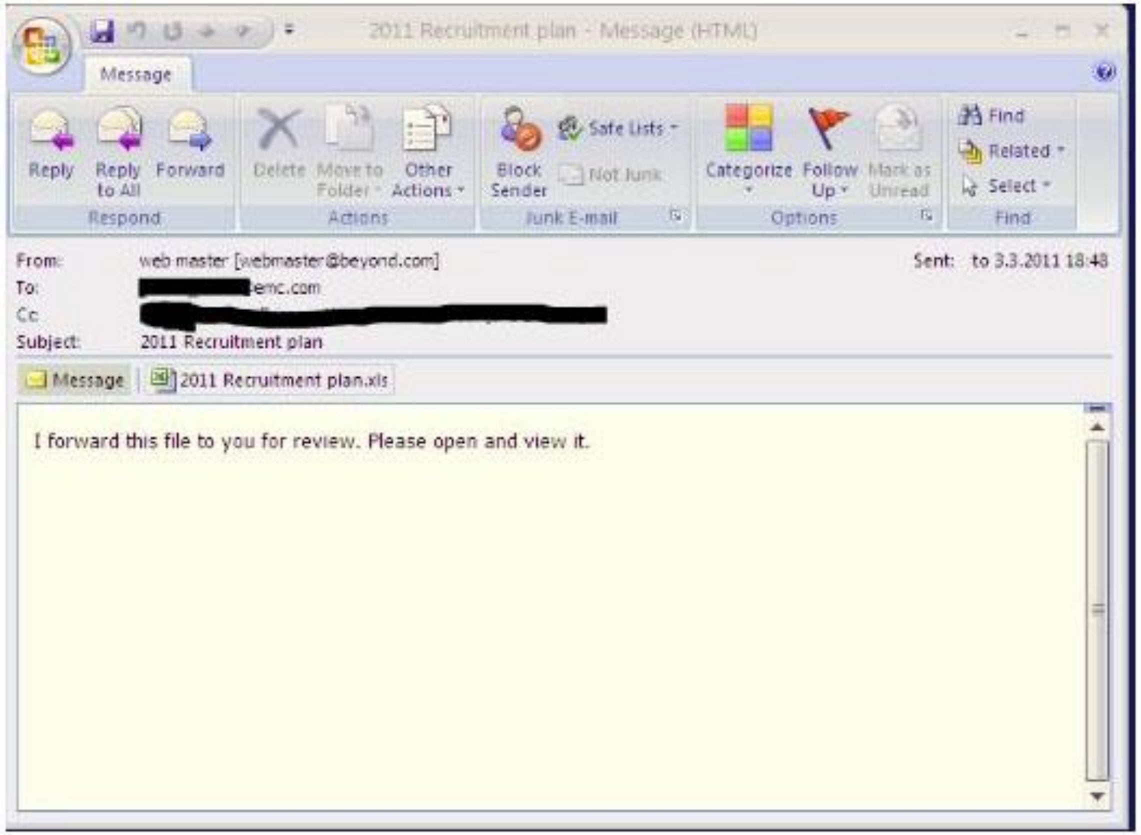
Modifying The Kill-chain #2

- The process is not linear
- Mandiant's version:



The start: Initial compromise & foothold

- Attackers **move** from the Internet to initial, arbitrary foothold in victim’s network
- Through interfaces open to the internet:
  - E-Mail:
    - The most popular method
    - phishing E-mail bearing a malware
  - Web:
    - Watering hole attack: malware “Drive-by download” on relevant sites
  - Enterprise Web App
    - Using WebApp vulnerabilties



From: web master [webmaster@beyond.com]
Sent: to 3.3.2011 18:48
To: [redacted]emc.com
Cc: [redacted]
Subject: 2011 Recruitment plan

Message | 2011 Recruitment plan.xls

I forward this file to you for review. Please open and view it.

The middle #1: Lateral Movement

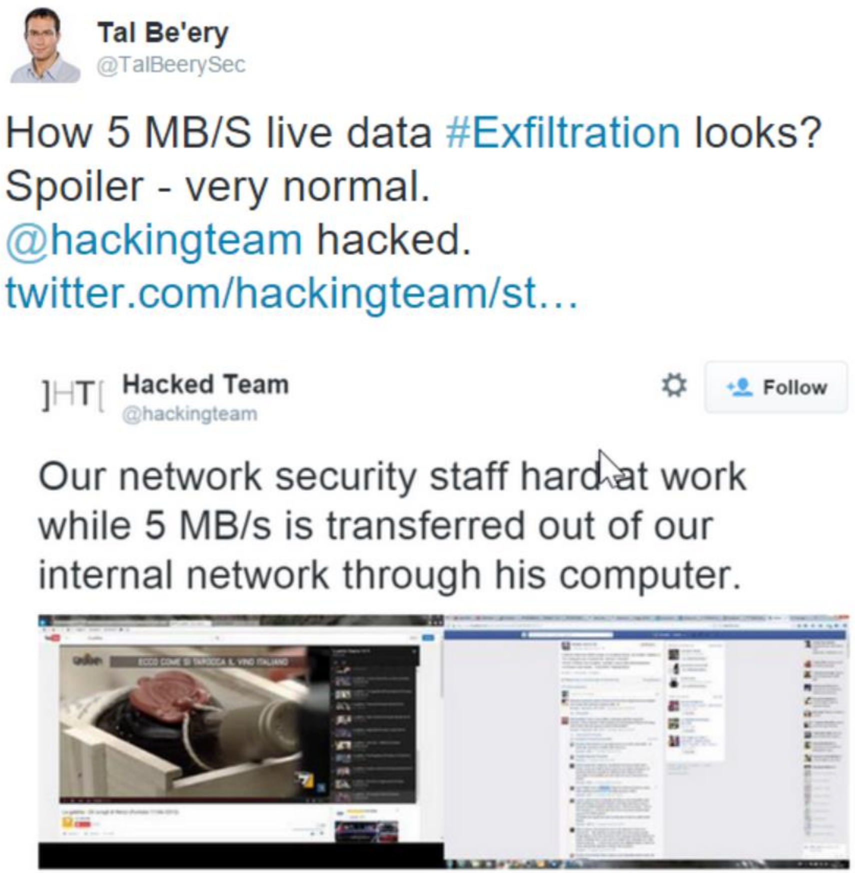
- Attackers **move** from the arbitrary foothold in victim’s network to its destination
- Using the following vehicle
  - The engine is Lateral Movement using stolen credentials
  - The wheel is the data obtained in the Recon phase
- The Lateral Movement + Privileges Escalation methods are standard:
  - Steal credentials from infected computer
  - Expand to other computers using these creds
  - Steal other creds from the computer
  - Repeat

The middle #2: Recon

- The recon phase is the most non standard part, as every victim’s network is different:
  - Attacks destinations, networks’ topology, naming conventions
  - Therefore it involves more manual work:
    - More time
    - Attackers’ mistakes
- Recon methods are standard
  - Scan the vicinity: near-by (network-wise) computers
  - Query central repositories: Active Directory, DNS

The end: Exfiltration

- Attackers **move** data to the internet using standard open channels
- Mostly through web
- But also FTP or any other protocol



Tal Be'ery
@TalBeerySec

How 5 MB/S live data #Exfiltration looks? Spoiler - very normal. @hackingteam hacked. twitter.com/hackingteam/st…

]HT[Hacked Team
@hackingteam

Our network security staff hard at work while 5 MB/s is transferred out of our internal network through his computer.

Know Thyself

Learn what is normal

- Per entity and containing groups
- Access patterns
  - Logged-on Computers
  - Accessed resources
- Working period
  - Working days
  - Working hours
- Physical location
  - Where is the user’s home
  - In case of travel makes sense

http://seanheritage.com/blog/profiling-normal/

Choose the Battlefield

Time for another Sun Tzu Quote

- “"...And therefore those skilled in war bring the enemy to the field of battle and are not brought there by him."

https://upload.wikimedia.org/wikipedia/commons/3/37/Enchoen27n3200.jpg

It’s a battle of movement

- All phases involve **move**ment
- Movement in IT = Network
- Therefore the battle must take place over the network
- But we have a limited budget: in which phase we should invest more and in which we should invest less?

Where to invest less

- Exfiltration – too late
  - The information is already making its way out
- Infiltration – too much attack surface
  - Too many users and end systems
  - We already investing a lot of budget there, mainly in anti-malware
- And both
  - Very generic to the attacker, very similar for all victims
  - Very rapid, compared to the middle section

Where to invest more

- In the middle part:
  - Not generic: Attacker does not know internal network
  - Intelligence gaps: Attacker does not what is normal within the internal network
  - Before any real damage has been done
  - The longest of phases: Takes weeks or event months

Weapons #1: Monitoring Traffic

- Detect known attacker pattern
- Learn normal traffic to identify anomalies
- Monitoring everything does not scale and we must prioritize
- Invest more in monitoring central repositories
  - E.g. Active directory, DNS, DHCP
- Invest more in monitoring sensitive servers
  - E.g. relevant file servers, Data bases, Active directory

Weapons #2: Deception

- Confuse the attacker with deception
- Use as network tripwires and landmines
- Deploy honeypots
  - Fake servers
- Deploy honeytokens
  - Fake entries in real servers
- Monitor access and use to honeypots/honeytokens over the network

Putting it all together

- You know thyself
    - You learn what is normal
- You know the enemy
    - You know what the attacker is doing and able to detect it
- You had chosen the right battlefield
    - The middle of the attack: recon + lateral movement
- You have the right weapons:
    - Network monitoring to detect Known attackers’ patterns, anomalies and deception tripwires and landmines
- Sun Tzu promises victory!