*PHYSICAL MALWARE ATTACK

CASE STUDY : GERMAN STEEL PLANT ATTACK

*INTRODUCTION

- Attack occurred at a German steel plant
- Spear phishing is a common form of phishing attack usually targeting corporations and military organizations
- Mostly due to human error that could have been avoided
- IT infrastructure was not up-to-date with latest technology
- Mostly government security agencies and elite hackers hired by corporations conduct such attacks
- Background knowledge of employees are somehow obtained and then used by the hackers in their social engineering exploit
- Group behind attack advanced persistent threat(APT)

from Gmail- Accounts info.service@google-accounts.com hide details 12:45 PM (2 minutes ago) Reply

to [redacted]

date Sun, Jun 5, 2011 at 12:45 PM

subject Online Service Message

mailed-by omega.fuzzymonkey.net

Gmail by Google

Google Account Phishing Scam

Dear Gmail User,

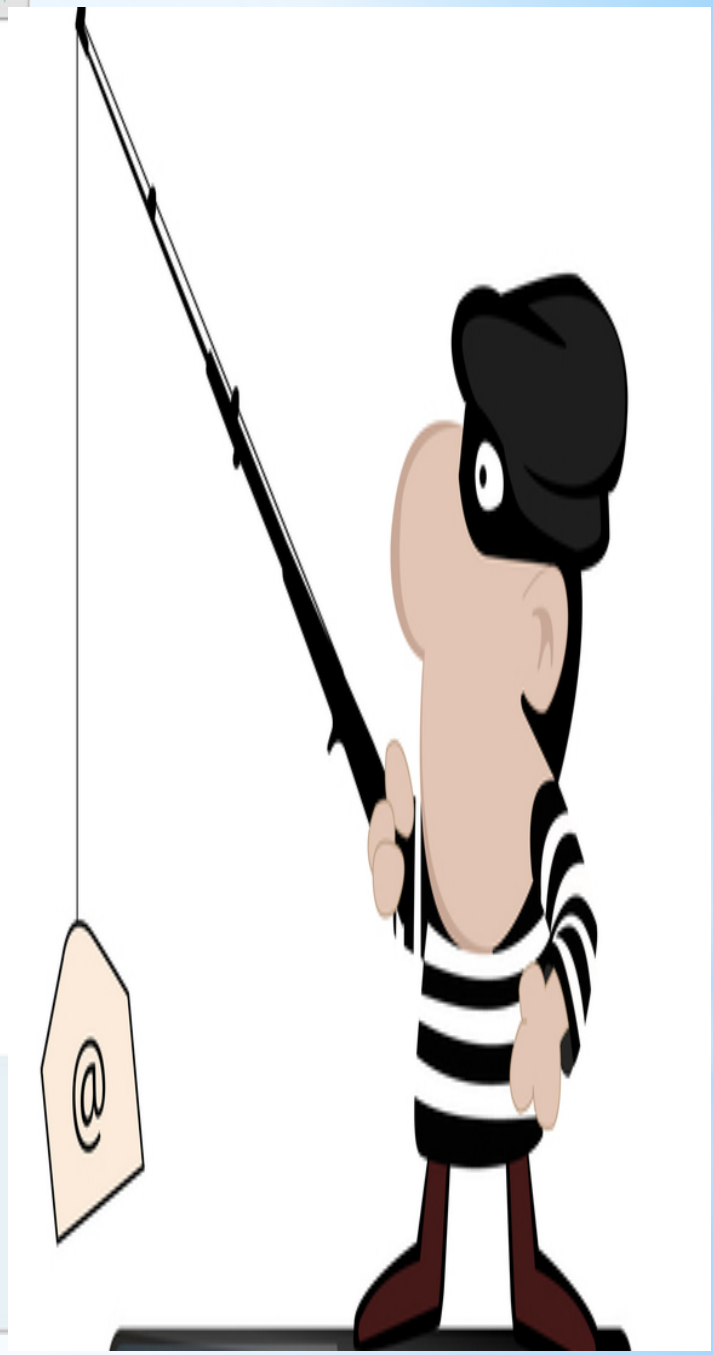
We are informing you about a regular routine maintenace of our servers. Pls verify your email account by clicking below

Verify your Account

This upgrade process would ensure your Google Account is stable even after long periods of inactivity.

Thank You
Gmail Team

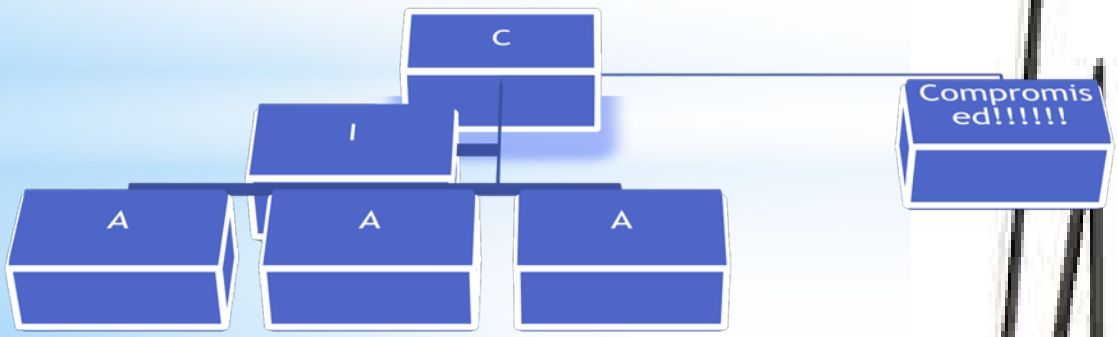
Reply Forward

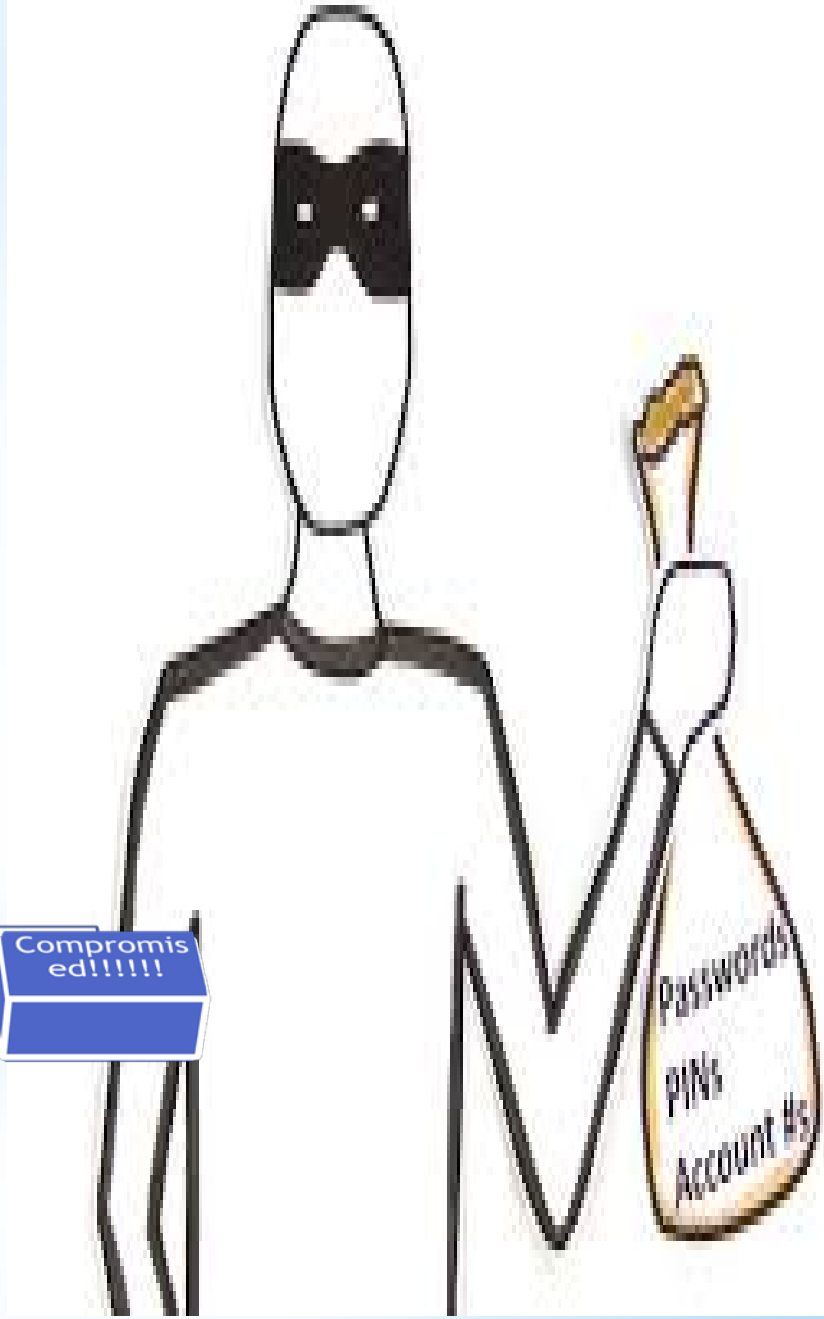


SPEARPHISING ATTACK

- This form of attack is directed towards specific organizations such as financial institutions and military organizations
- The spoofed email looks like it comes from a legitimate source
- Usually harvested by the top one percent elite
- Directed towards people with little or no technical background, it relies heavily on social engineering


shutterstock
www.shutterstock.com · 87490888


C
I
A
A
A
Compromised!!!!!!


Passwords
PINs
Account #s

*THE ATTACK

- Similar attack was used in the German steel plant. With malicious email, attackers were able to gain access into the company production network.
- The attackers were an expert in an industrial control systems and they were able to bypass various security systems provided by the company production network.
- They were able to tamper the blast furnace. And due to the system failure one of the blast furnaces could not be shutdown. (Overriding systems also fail , due to use of specialized software).

*Stuxnet attack on Iran

- Worm that attacks programmable logic computer that manage industrial complexes
- Fakes sensor signals so the system does not shut down when it should
- Worm that causes physical damage
- Was used to famously attack Iran's Nuclear centrifuges
- Huge change from regular uses of viruses and worms

*COUNTERMEASURES

- ✓ Business network connected to production network. Those two should be separate.
- ✓ Implement security policies to educate.
- ✓ Employ early intrusion detection systems and firewalls.

*QUESTIONS

1. Who will be interested in doing such a thing?

2. How do you protect Industrial control systems (ICS) from such attack?

3. How should the industry deal with such attacks?

*SOURCES

http://www.fbi.gov/news/stories/2009/april/spearphishing_040109

http://blog.lumension.com/9630/german-steel-works-suffered-massive-damage-after-hack-attack/

http://www.mirror.co.uk/news/technology-science/technology/malicious-hackers-use-simple-email-4977018

http://papers.duckdns.org/files/2011_IECON_stuxnet.pdf

http://www.securityweek.com/cyberattack-german-steel-plant-causes-significant-damage-report