Network Security

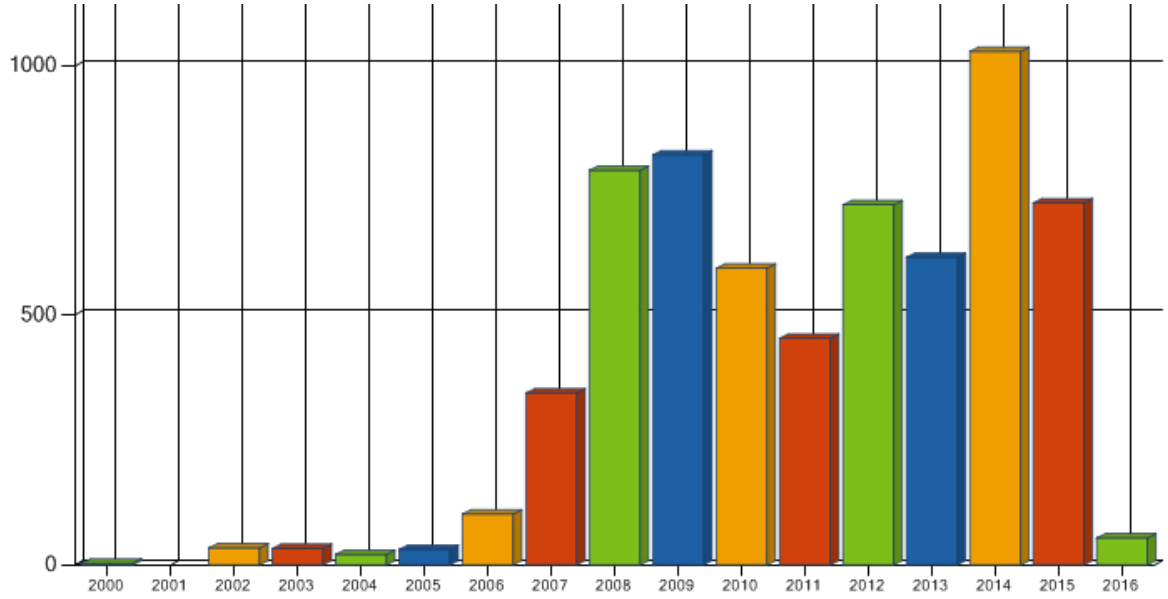
AA 2015/2016

Vulnerabilities (b)

Dr. Luca Allodi

Cross-site-scripting (XSS)

- Among the most common if not perhaps the most common web-based attack
- By exploiting this vulnerability, the attacker can modify the content delivered to a user's browser
  - The vulnerability is on the server, but the attack affects the user



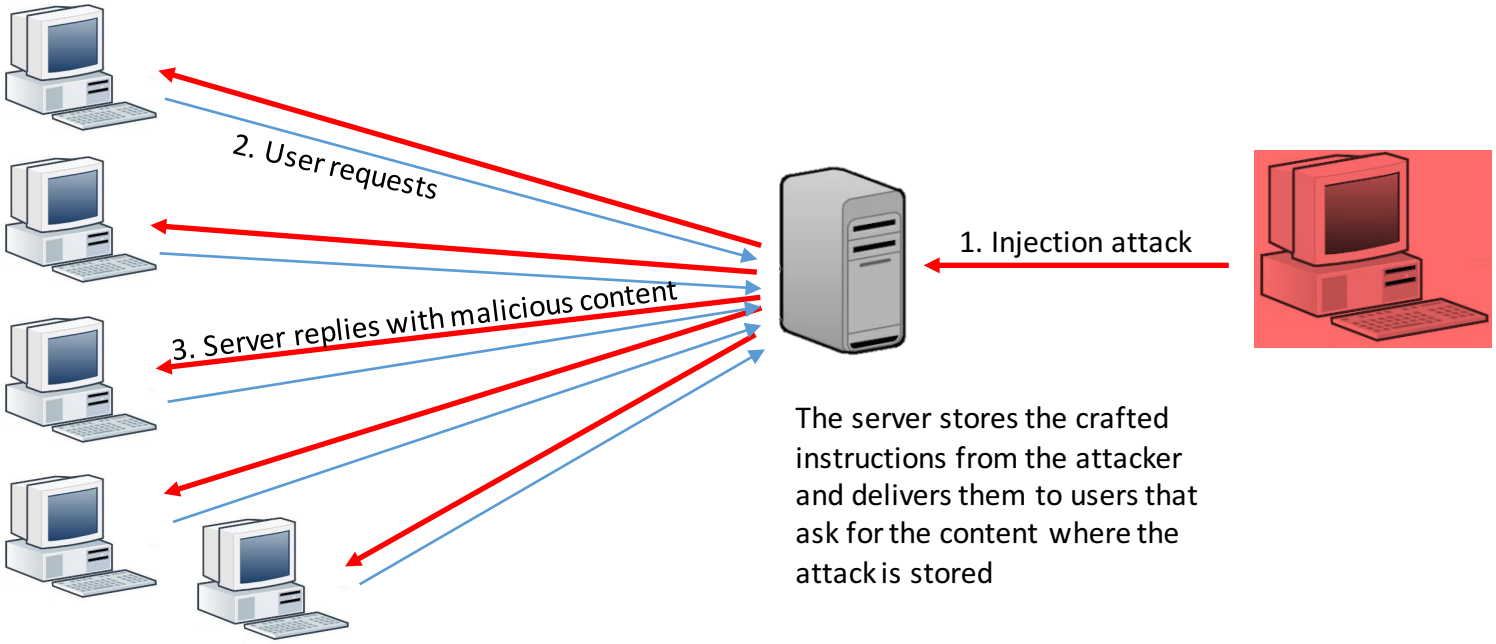
Stats from NVD (Feb 2016)

XSS attacks

- Regardless of execution, are based on the implicit notion of trust that exists between a browser and a server
  - The browser executes whatever the contacted website says
  - “Same-origin-policy”
    - Applied also to browser cookies, JS execution, etc.
- Vulnerability allows the attacker to inject content on a webpage
  - When victim browser loads webpage it executes injected content
  - The browser can not distinguish between legitimate and ”malicious” instructions → all coming from a trusted source

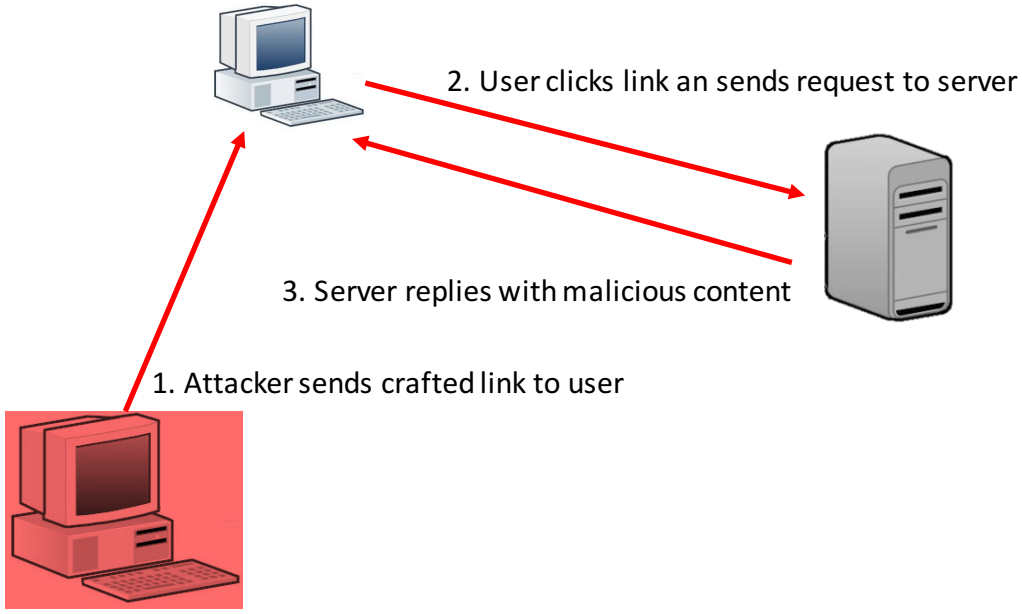
Stored XSS (Persistent XSS)

- This XSS variant is stored on the remote server
  - E.g. a forum thread, a newsletter, a database
- Whenever a user retrieves a certain webpage, the malicious content is delivered to their browser



Reflected XSS (Non-persistent)

- The attacker somehow tricks the user in sending the forged input to the server
  - e.g. sends a link with a spam email



Reflected XSS example

Webpage code:

<?php $name = $_GET['name'];

echo "Welcome $name
";

echo "Click to Download"; ?>

Attacker sends this url to victim:

index.php?name=guest<script>alert('attacked')</script>

Session Hijack:

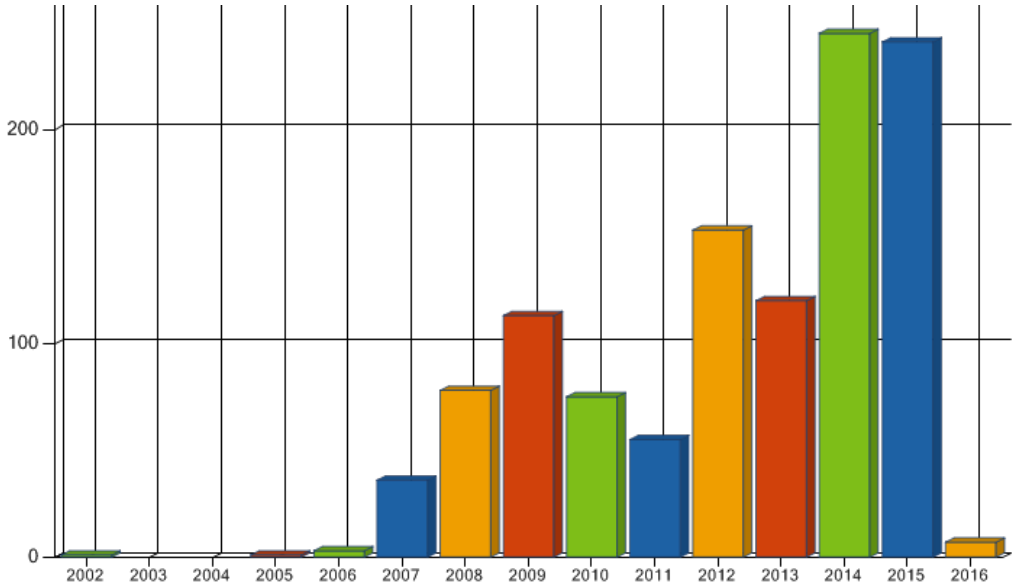
Click to Download

XSS - impacts

- disclosure of the user's session cookie,
  - Can be used to hijack user's session
- disclosure of end user files
- redirect the user to some other page or site
  - E.g. controlled by the attacker
  - Possible other attack vectors stored on that page
- modify webpage content/information
  - e.g. modify button functionalities
- ..

Cross-site request forgery

- Similar in principle to an XSS attack
- Rather than exploiting the browser's trust on server replies, it exploits server's trust on browser requests
  - Attack happens on the server → server "change state"
  - e.g. executes server-side operation not intended by user



Stats from NVD (Feb 2016)

CSRF

- Forged input to server executes actions on the server → changes server status
- Usually exploits a user's stored credentials to execute illegitimate actions on a website
  - Change email/password
  - Perform server operations (e.g. bank transfer)
- Example (https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF))
  - Imagine a web bank that operates through HTTP GET arguments
    - GET http://bank.com/transfer.do?acct=BOB&amount=100 HTTP/1.1
  - Attacker can trick the user in sending forged request
    - http://bank.com/transfer.do?acct=MARIA&amount=100000
    - e.g. embed link in HTML source code

Common source of vulnerability

- SQL injection → SQL backend trusts unsanitized input
- Buffer overflow → System can not distinguish between instructions and data, trusts the input to be correct
- XSS → the browser trusts the content sent by the server
- CSRF → the server trusts and executes the commands sent by the browser

Human vulnerabilities

"The biggest threat to the security of a company is not a computer virus, an unpatched hole in a key program or a badly installed firewall. In fact, the biggest threat could be you. What I found personally to be true was that it's easier to manipulate people rather than technology. Most of the time organizations overlook that human element"

Kevin Mitnick

Phishing

- The attacker aims at obtaining the credentials of users of a website/service
  - other types of private information can be gathered too
  - Typically through more sophisticated “spearphishing” attacks
- Attacker creates a *replica* of the original website
  - Replica is published online
  - Link typically sent through spam emails, social networks
  - Recipient may be fooled in opening the link and entering their credentials as in the genuine website
  - Credentials are of course sent to the attacker instead

Phishing – attacker tools

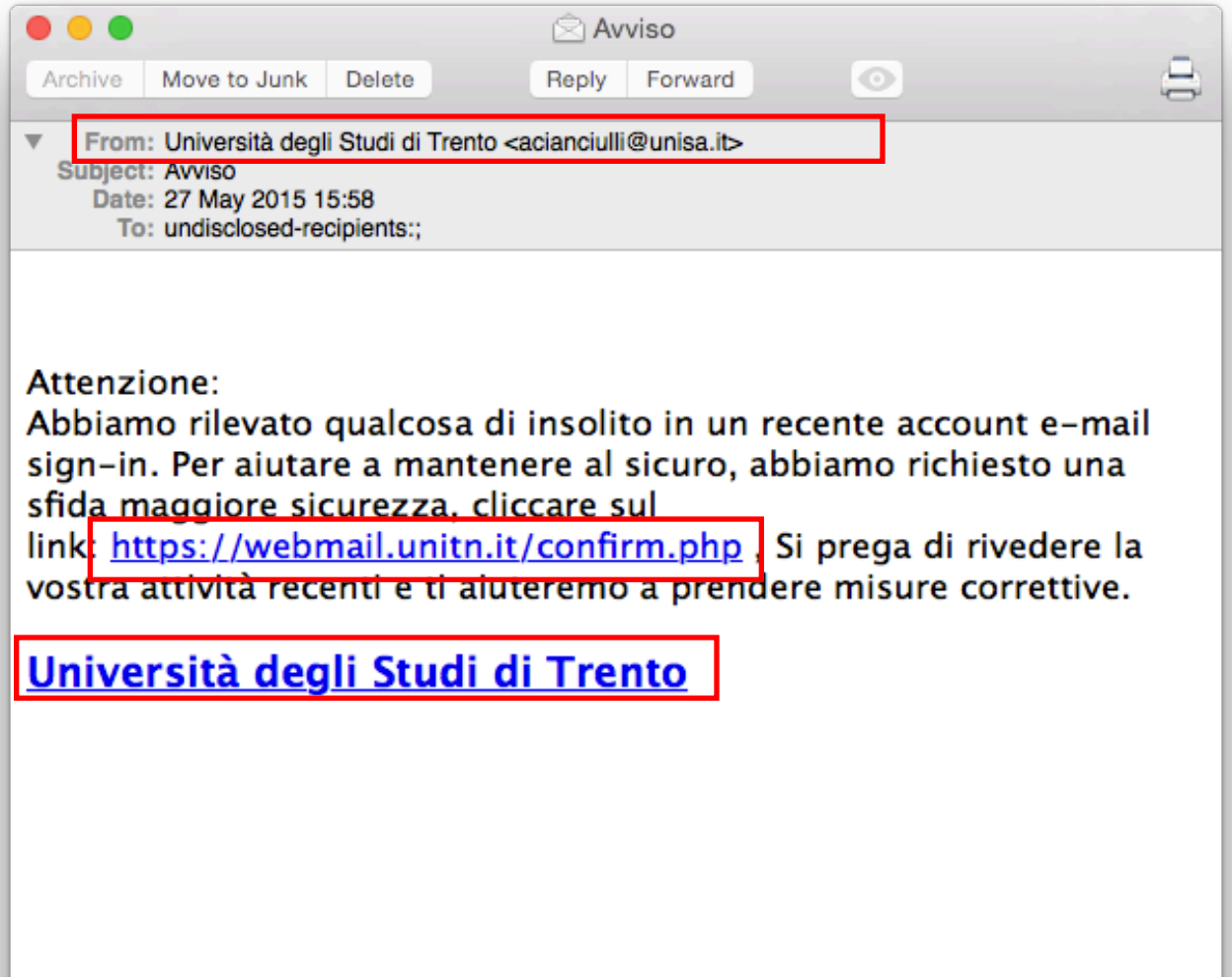
- Creating a working replica of a website is only as hard as creating a copy
  - Attacker needs to modify some of its components
    - e.g. send form HTTP POST to a webserver the attacker controls
  - Advanced attackers may remove JS/third party components to prevent exposing the phishing website
    - Advanced attackers vs script kiddies
- Automated tools exist that do this for the attacker
  - Few hundreds of dollars on black markets
  - Essentially a recursive wget

Phishing in a nutshell

Phishing example

Translation (including English reproduction of lexical and grammatical errors).

Warning:
We noticed something unusual in a recent email account sign-in. To help maintaining secure, we requested a challenge higher security. click the link {link}, We kindly ask to review your activities recent and we will help you taking correcting measures.



Combining phishing and software vulnerabilities

- In this case it's easy to notice that the domain I'm redirected to is not UniTn's
- However, there exist vulnerabilities in browsers that allow the malicious website to **spoof** the address displayed in the address bar
- Example:
  - The webpage is **gfcv-altervista.org**
  - The browser says it's **webmail.disi.unitn.it**

Example of address spoofing

- Safari 8 vulnerability under OSX < 10.10.5
  - PoC → http://www.deusen.co.uk/items/iwhere.950018225526788/
  - Other similar vulnerabilities exist for IE and Chrome
- If browser is vulnerable, attacker can manipulate address bar's content to his/her liking

Social engineering

- Phishing is only an application of a wider set of attacks that exploit human nature to (usually) breach data confidentiality
- "Social engineering" identifies a set of techniques that attack weaknesses in human psychology
  - The final goal is to *persuade a human being* in performing actions elicited by the attacker
- *Situational theory of publics* → why people would take action, or feel part of a collective
  - **Problem recognition** → subject thinks the problem is relevant to them
  - **Active involvement** → subject thinks they will suffer the consequences of the threat
  - **Constraint recognition** → subject thinks their actions are limited by factors outside of their control

Elaboration Likelihood Model (ELM)

- ELM describes the ways humans change their attitudes or decide to perform actions they would not perform without external *stimuli*
- Two routes to “persuasion”
  - Central route
    - *Stimuli* are weighted by the subject and final decision is carefully elaborated
    - High amount of cognitive effort
      - Associated with “rational perfectly informed decisions” in economics
    - Persuasion happens through carful elaboration of information
  - Peripheral route
    - Communication that typically does not result in careful cognitive effort in understanding the message
    - Subject is convinced by under-analyzing apparently relevant “cues” that are in reality unrelated to the subject matter
    - Persuasion happens through ”adjunct elements” to the communication
      - Likeability of subject, physical attractiveness, trust, …

Uses of the peripheral route

- Vastly used as a “cheap” route to convince people to perform an action
  - Buy a product
  - Subscribe to a service
  - Visit a location
  - …
- Especially effective when physical contact is not a factor
- Marketing strategies often rely on this mechanisms
  - TV ad must convince you to buy a shampoo in 30 seconds
- Social engineering differs from marketing in that attacks typically do not try to sell products
  - Rather, social engineers must *persuade* victims to disclose sensitive or private information

Hacking a human

- Six factors affect likelihood of human persuasion

1. Reciprocation
   - Subjects form implied or explicit obligations towards each other → **Normative commitment**
2. Consistency
   - Subjects tend to be consistent with previous decisions, even if all evidence shows that these were *bad* decisions → **Continuance commitment**
3. Social proof
   - Subjects tend to act similarly to their peers to "fit in" → **Affective commitment**
4. Likeability
   - Subjects tend to **trust** people they like, find convincing, or attractive
5. Authority
   - Subjects **fear** punishment (that an authority can impose) and will comply
6. Scarcity
   - Subjects will **react** quickly and possibly irrationally to stimuli when they believe that their freedom of choice is a function of time or resource availability

Normative commitment

- Subjects will perform an action because that's customary or mandated by law or contract
- Based on the notion of reciprocation of benefits
  - When subjects receives something they value, they feel "**cognitive dissonance**"
    - Essentially a "bug" of human psychology
    - Faced when subject must elaborate two contrasting forces or inputs simultaneously
      - Subject must elaborate evidence in contrast to his previous beliefs
      - E.g. "I do not need sun cream" → "here is a tester for you" → "thank you I should probably buy some"
- Promises count as "something of value"
  - I promise you a valuable good at the sole cost of shipping
- People tend to comply because they feel "gratitude" for the unsolicited proposal

Continuance commitment

- Subjects tend to maintain congruence in their attitudes and decisions even in presence of evidence that these are *bad*
  - Subjects tend to maintain **cognitive consonance** as opposed to face cognitive dissonance
- In economics this is reflected in the concept of "loss aversion and sunk costs"
  - If an initial investment was bad, people will tend to keep on investing because they are convinced it will eventually pay-off
    - Pay (small) escalating costs to win a teddy-bear
- Upfront costs are low w.r.t promised benefit vs cost of taking precautions (or opportunity costs)
  - People are willing to give away personal information for negligible benefits or discounts (even if they claim they are willing to pay a premium to preserve their privacy) [Acquisti 2003]

Affective commitment

- People are influenced by the opinion of those they esteem or like
- Decision of action taken to be part of a clique or a circle of peers
  - Widely used for marketing too
- Emotional bond with interlocutor can be exploited to have the victim communicate personal details or perform certain actions
  - e.g. pretend you are on a vacation with a friend of the victim and ask money to solve an emergency
    - Social networks make these inferences possible for the attacker

Liking and Trust

- Similarly to affective commitment, people are willing to be liked by those whom the like
  - Take action to obtain consent from those they like
- People tend to extend "credibility" of subjects they perceive as successful beyond the reasonable boundaries of these subjects' actual expertise
  - e.g. famous actor that publicizes biscuits despite having no actual expertise or credibility as a baker, but only as an actor
- When physical/presence attraction is not a factor (e.g. email exchange), the likeability can emerge from a "friendly connection"
  - e.g. appeal or elicit common traits

Authority

- People tend to respond to authority especially when in fear of the outcomes of *not taking action*
  - E.g. Punishment or the cancellation of a privilege
    - *"Your email account is going to be deleted if your password is not confirmed."*
- Obedience to authority is a very powerful tool to persuade people in pertaining actions or behaviors
- In some (occasionally very controversial) cases people will obey to authority even against well-established moral values and ethics

Effects of authority – Milgram's experiment

- Experiment in the 1960s @ Yale, replicated several times
- Subject A deceived in participating in an experiment where they had to "teach" subject B combinations of English terms
  - Subject B is in reality a collaborator of the experimenter
  - Whenever subject B gives the wrong answer, subject A must inflict an electrical shock to B
    - Voltage increases with number of errors
    - No visual contact between A and B, but A can hear B screaming in pain for the shock
    - There is **no actual shock,** but A does not know
- To what extent will A collaborate?
  - 65% of subject As went all the way to highest shock level (when B effectively stopped answering)
  - Subject As felt **deeply concerned and stressed, expressed profound anxiety, had hysterical reactions**
  - Yet, the experimenter's (authority) power was enough to push them in continuing with the experiment in most cases
    1. **"Please continue."**
    2. **"The experiment requires that you continue."**
    3. **"It is absolutely essential that you continue."**
    4. **"You have no other choice, you must go on."**

Scarcity

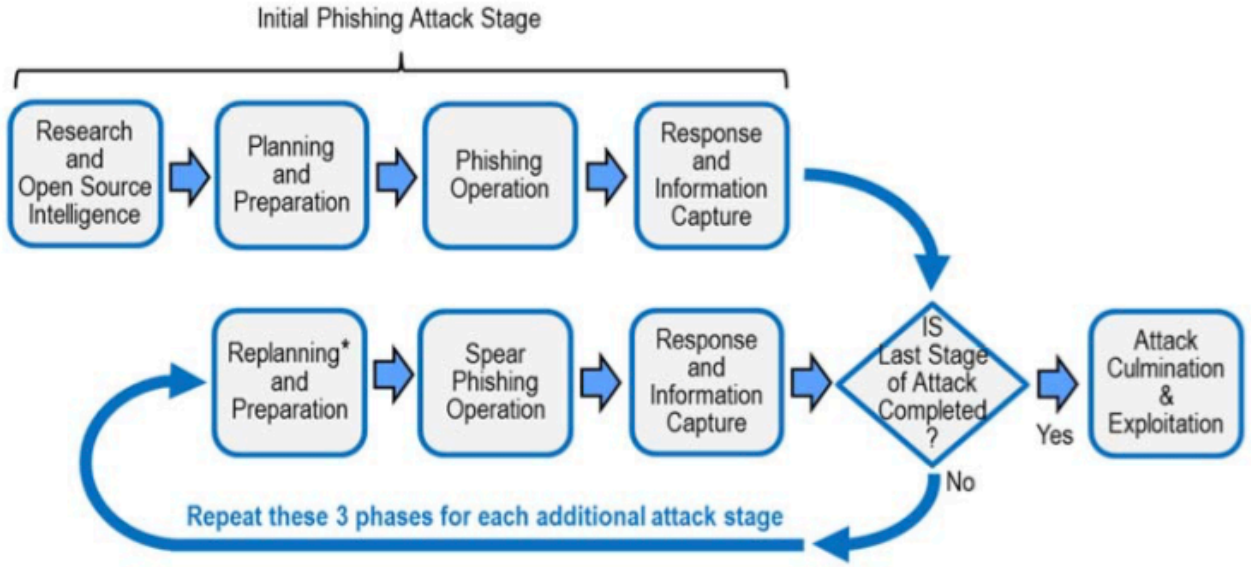
- Similarly to fear, scarcity leads people to take quick, potentially uninformed decisions in fear of losing an opportunity that will either disappear in time or that is scarce in quantity
- Can be used by social engineers to elicit unwise decisions from the victims
  - Threaten that if no decision is taken quickly, the opportunity may fade away
  - Attackers poses a “constraint” in the freedom of choice of the victim

Social engineering steps

- Can distinguish between single and multiple-stage social engineering attacks
- Single stage attacks usually aim at collecting sensitive information about “general” targets
  - No specificity in the attack
    - e.g. attack all costumers of mybank.com

Two(multiple) stage attacks

- Two-stage attacks involve an initial reconnaissance that gathers information needed for second stage
  - Used to increase credibility of attack
    - E.g. proper legal references, employee names, correct set of users in CC to phishing email, etc
  - Spearphishing against CEO/director/manager/person of interest



* Replanning and/or additional preparation may or may not be necessary depending on the particular context and the specific phishing objectives

Steps in detail (first stage)

Pattern Phase	Typical Activities	Pattern Interactions
1. Research and Open Source Intelligence	• Search for opensource intelligence • Establish attack objectives • Identify opportune targets	1.1 Attacker researches and strategizes about potential targets and specific objectives.
2. Planning and Preparation	• Develop attack strategy including means to avoid detection and mitigation by UIT organization • Prepare phishing attack artifacts	2.1 Attacker plans phishing attack and creates phishing artifacts (e.g., phishing email, mobile text message, phony website, malware to be implanted).
3. Phishing Operation	• Release phishing artifact via email, cellphone, rogue website, or other means • Wait for a response	3.1 Attacker initiates phishing attack through email, cellphone, rogue website, or other means.
4. Response and Information Capture	•Gain access and/or privileges to obtain greater information reach •Implant malware to achieve information objectives •Identify other opportune UIT targets and internal system information, and capture guarded and sensitive information	4.1 One or more targets unwittingly respond to phishing artifact and become a UIT. 4.2 Attacker detects or is alerted to UIT response and obtains initial information directly from UIT data entry. 4.3 Attacker implants malware on victim's machine or network. 4.4 Attacker obtains desired information via malware.

Unintentional Insider Threats: Social Engineering. CERT Insider Threat Center. January 2014
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=77455

Steps in detail (second stage)

Pattern Phase	Typical Activities	Pattern Interactions
5. Re-planning and Preparation	•Re-plan attack strategy including means to avoid detection and mitigation by UIT organization •Prepare spear phishing attack artifacts	5.1 Attacker uses information capture in Step 4 above to replan follow-on steps for spear phishing attack. This may entail creation of new artifacts or specific attack approaches.
6. Spear Phishing Operation	• Execute spear-phishing • Wait for a response	6.1 Attacker initiates spear phishing attack.
7. Response and Information Capture	•Gain access and/or privileges to obtain greater information reach •Exploit more specific insider targets: financial system, secure systems, etc.	7.1 One or more high-value targets unwittingly responds to the spear phishing artifact and becomes a UIT. 7.2 Phisher detects or is alerted to UIT response and obtains desired information directly from UIT data entry.
8. Attack Culmination and Exploitation	• Use captured information to directly attack UIT or UIT's organization to steal, manipulate, and/or destroy targeted assets	8.1 Attacker uses desired information in direct attack on UIT or UIT's organization to steal, manipulate, and/or destroy targeted assets.

Unintentional Insider Threats: Social Engineering. CERT Insider Threat Center. January 2014
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=77455

Example: well engineered, 2-stage social engineering attack

- On 19th of May 2015 I received an email from somebody attaching a "receipt". The email was in good Italian, and had seemingly meaningful law references regulating the emission of the receipt
  - However, I was not expecting a receipt
  - I discarded it right away as an attack → trashed
- The next day, I receive this email:

Dear costumer,

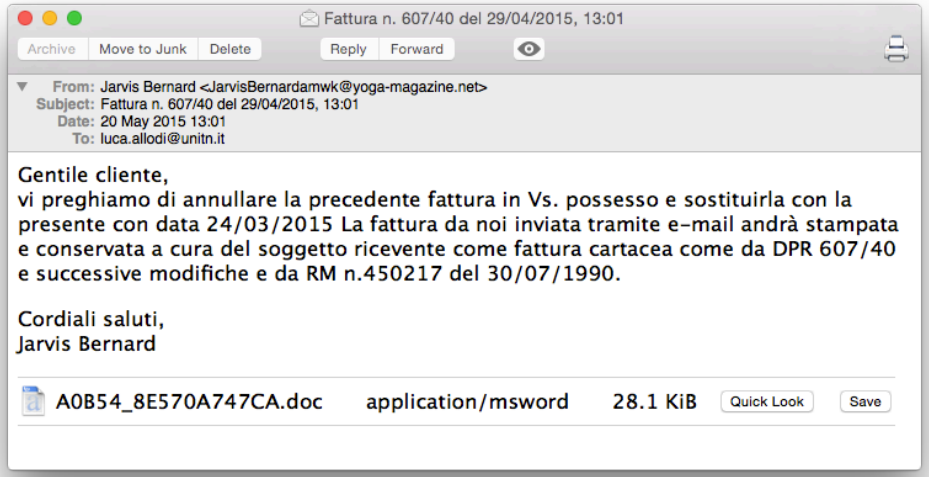
We kindly ask you to ignore the previous receipt and substitute it with the present, dated 24/03/2015 The receipt must be printed and archived by the receiving subject as prescribed by DRP 607/40 and subsequent changes, and by RM no. 450217, emitted on 30/07/1990

Best regards,
Jarvis Bernard

continuance commitment (variation of)

authority

normative commitment



Almost fell for it..

virustotal

SHA256:	fb4d983c26b0e5d13df260e5da4e9cddf780d2520bb7c4e3440a868b93ad6f94
File name:	99BCA6_B7C8B4025833.doc
Detection ratio:	2 / 57
Analysis date:	2015-05-20 11:09:00 UTC (2 weeks, 5 days ago)

AVware	Trojan.MHT.Agent.a (v)	20150520
VIPRE	Trojan.MHT.Agent.a (v)	20150520
ALYac	✓	20150520
AVG	✓	20150520
Ad-Aware	✓	20150520
AegisLab	✓	20150520
Agnitum	✓	20150519
AhnLab-V3	✓	20150519
Alibaba	✓	20150520
Antiv-AVL	✓	20150520

Reported results are for attachment of first email. Second attachment gave same results.

Reading List

- Arora, Ashish, et al. "Impact of vulnerability disclosure and patch availability-an empirical analysis." *Third Workshop on the Economics of Information Security*. Vol. 24. 2004.
- Miller, Charlie. "The legitimate vulnerability market: Inside the secretive world of 0-day exploit sales." *In Sixth Workshop on the Economics of Information Security*. 2007.
- http://phrack.org/issues/49/14.html
- OWASP resources
- Moore, Tyler, and Richard Clayton. "An Empirical Analysis of the Current State of Phishing Attack and Defence." *WEIS*. 2007.
- Workman, Michael. "Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security." *Journal of the American Society for Information Science and Technology* 59.4 (2008): 662-674.
- Acquisti, Alessandro, and Jens Grossklags. "Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior." *2nd Annual Workshop on Economics and Information Security-WEIS*. Vol. 3. 2003.