PROJECT INFOSYS 3848

Please have a 1 1/2 Page, Single spaced, written by next Thursday (11/2) on the assigned topic:

- Andrew - Impact on Business
- Ahmed - How malware are being deployed, and what the attacker collect from the user (1 3 2b)
- Omar - How malware are being deployed, and what the attacker collect from the user (1 3 2b)
- Alex - Provide evidence on why this issue is important (2a)
- Jibril- Existing measures of malware (pegasus) (2c)
- Roul - how to create end user awareness on malware in correlation to (Pegasus)

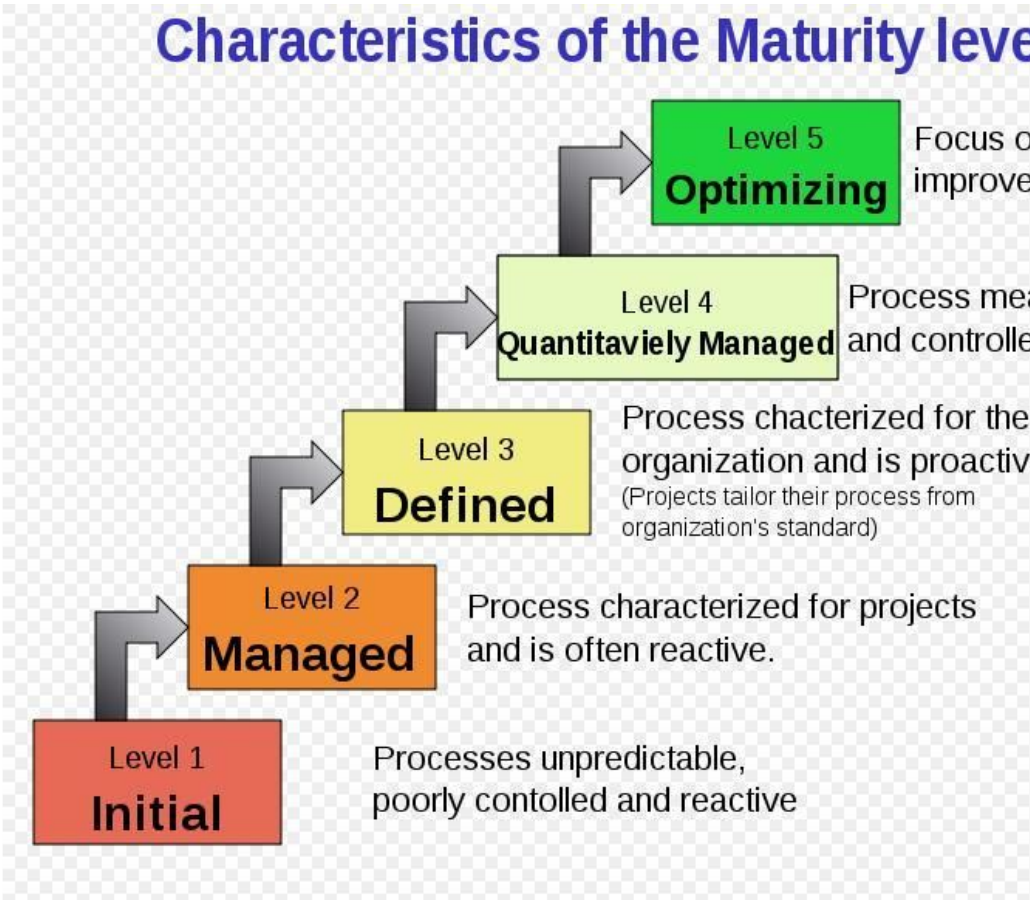
COLLECTIVE EFFORT

- 2D - I identify a Gap with the existing measures, and if the current measure is not efficient state why (COLLECTIVE)
- 2E - Provide an innovative approach that fill the gap that was identified above.

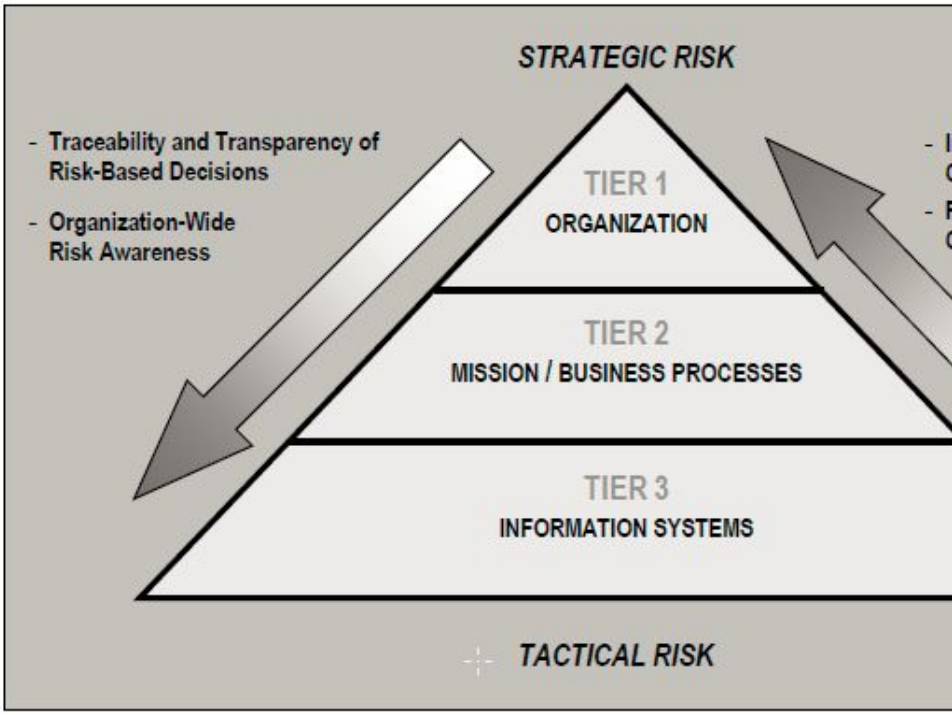
1) END-USER RESPONSIBLITIES
    - Business Goals and Objectives: Alignment
        - Corporate Governance: the set of responsibilities exercised by the board and executive management to ensure business goals are met, risk is managed, the enterprise is managed responsibly, etc.
        - InfoSec governance is a subset of Corporate Governance.
        - InfoSec must support and align with Corporate Governance.
        - Governance framework usually consists of:
            - Comprehensive security strategy;
            - Governing security policies;
            - Procedures, Standards, and Guidelines supporting the policies;
            - InfoSec organizational structure that has sufficient authority and resources and that avoids conflicts of interest;
            - Metrics and monitoring processes.
    - Roles and Responsibilities: Executive Leadership
        - Board of Directors
            - Ultimate responsibility for all governance.
            - Need to be versed on the organization’s information assets.
            - Establish “tone at the top” conducive to security.
            - Ongoing oversight; legal/ethical obligation of “due care”.

        - Establishment of an Audit Committee (usually a subcommittee of the board; required of publicly traded companies by Sarbanes Oxley)
- Roles and Responsibilities: Executive Leadership
    - C-Level Management
        - Executing the Board's governance objectives.
        - Consistent "tone at the top".
        - Resolving security-vs-performance conflicts.
        - Providing appropriate resource levels.
            - With actionable input from InfoSec, including education of Senior Management.
        - Maintain visible commitment to and involvement in security.
    - Steering Committee
        - Committee of Senior representatives of all groups affected by InfoSec. Not present in all organizations.
        - Involve all stakeholders.
        - Foster consensus (not the same as unanimity).
        - Foster cross-functional communication.
    - CISO
        - All organizations have a CISO, whether or not anyone has that title. Whether they know it or not, there is *someone* in the organization who has ultimate responsibility for the security of the organization's data assets. It might be a CISO, CIO, CFO, CEO, etc.
        - According to PWC surveys: in 2006, 22% of organizations had a designated CISO; in 2011, more than 80% did (*CISM Review Manual 2015).*
        - Historically, CISOs have often reported to the CIO. It's becoming more common for them to report to the CEO or BoD (*CISM Review Manual 2015).*
        - Overall functional responsibility for InfoSec. Day-to-day leadership. Managing budgets and resources, etc.
- Roles and Responsibilities: Management
    - Take ownership of security directives.
    - Enforce discipline and compliance with security standards.
    - Providing support and resources for security compliance.
    - Support security awareness and training (e.g., ensure employees have time to take the training).
    - Support incident response (e.g., release employees from daily tasks when there is a critical security incident).
    - Set a positive example of adherence to security standards.
    - Maintain awareness and understanding of security issues affecting their functional area.
- Roles and Responsibilities: Business Process Owners
    - Take responsibility for data ownership.
    - Handle data classification.

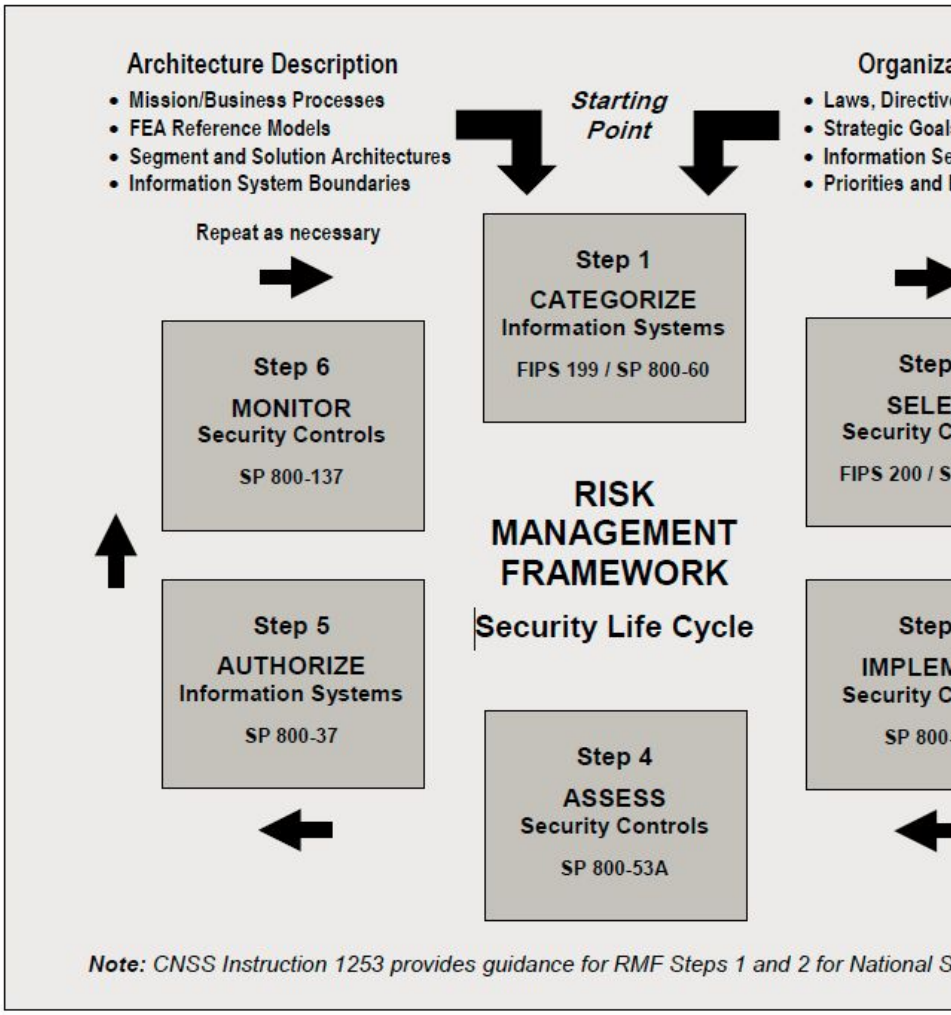
        - Maintain a detailed, current knowledge of business process, infrastructure dependencies, data inventory, etc.
    - Roles and Responsibilities: All Employees
        - Adhere to policies, procedures, standards, and guidelines.
        - Attend security awareness training.
        - Be vigilant for suspicious activity.
        - Practice safe computing.
2) I InfoSec Strategy Overview
    - Six typical target outcomes of the InfoSec strategy (derived from the governance framework, which we will discuss in a later class)
        - Strategic Alignment
        - Effective Risk Management
        - Value Delivery
        - Resource Optimization
        - Performance Measurement
        - Function and Process Integration
    - What do each of these mean for the organization? How will they be achieved? What constitutes success?
    - InfoSec Strategy: Desired State
        - Desired State: “A complete snapshot of all relevant conditions at a particular point in the future” (CISM Review Manual 2015)
        - Combines quantitative and qualitative characteristics.
            - May include items such as policies, procedures, infrastructure controls, specific metrics benchmarks, service offerings, etc.
            - Example: Attain full compliance with PCI DSS.
            - Example: Reduce malware-related downtime to X person-hours per month.
            - (You would want more details in these examples.)
        - Industry frameworks like COBIT, CMMI, Balanced Scorecard, and ISO can be helpful.



- Capability Maturity Model Integration (CMMI) from Carnegie Mellon
  - http://people.cs.pitt.edu/~chang/153/images/cmml.jpg
  - http://cmmiinstitute.com/


STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
TACTICAL RISK

- NIST 800-53



- NIST 800-53

3) **InfoSec Strategy: Pitfalls**

- Some obvious reasons strategies fail:
  - Poor planning
  - Insufficient funding
  - Poor execution
  - Neglect
  - Unexpected corporate events
  - Misconduct, merger/acquisition, business failure, etc.
- Some less obvious reasons strategies fail:
  - Overconfidence in predictions/estimates.
  - Unrealistic optimism: corporate culture rewards optimism.
  - Anchoring bias: once you put a number out, discussion anchors to that number, whether or not it is relevant.
  - Status Quo bias: we like the familiar.
  - Herding Instinct: Following fads; “an idea whose time has come!”
  - False consensus: overestimating the degree to which others agree
  - Other cognitive biases: confirmation bias, selective recall, groupthink.

- Security Decay
  - Tension between stated policies/risk tolerance and actual practice.
  - Gradual decay in processes and controls.
  - Easily granted exceptions.
  - Individuals are incentivized to meet budgets and deadlines, not security controls.
  - "Getting things done" presents a tangible, immediate reward. Skipping a security check presents a low risk to the individual.
  - Employees do what they are paid to do.

4) Security Controls: Overview
   - **Control (aka Countermeasure)*:** Actions, devices, procedures, or techniques that meet or oppose (i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.
     (NIST IR 7298 Revision 2, Glossary of Key Information Security Terms)
   - Administrative
   - Technical
   - Physical
   - * Some sources, such as ISACA, draw a distinction between *control* and *countermeasure.* ISACA says a countermeasure is a targeted control. In this terminology, *control* is used at a strategic level, and *countermeasure* is used at a tactical level. In practice in the corporate setting, the terms are used interchangeably.

TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

   -
     - *(NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations)*
   - Security Controls: What to include in the Strategy
     - Administrative controls
     - Policies
     - Procedures
     - Standards
     - Guidelines

- Technical controls
    - Anything from a simple configuration change to a massive implementation.
    - Largest time and resource expense.
    - Biggest source of “security decay” issues.
- Personnel
    - Ensuring trustworthiness and integrity of employees.
    - Mitigate insider abuse.
    - Background checks.
        - (be aware of legal issues especially in other countries)
    - Make employees aware of standards, monitoring, and consequences.
    - Needs heavy involvement of HR and Legal
- Organizational structure
    - Effective reporting structure (e.g., CISO reporting to CIO, CEO, etc.)
    - Clear lines of authority
    - Centralized vs. decentralized
        - Centralized gives more control to CISO and more consistency but may be unworkable in large and/or multination organizations
        - Decentralized is more flexible and puts local security staff closer to users but quality varies by location and visibility into issues is reduced.
- Awareness and education
    - Required by many compliance regimes.
    - Humans will almost always be the weakest link.
    - End users are also important in detecting incidents.
    - Compliance with administrative controls requires understanding.
    - Education has to be ongoing.
    - Need realistic expectations of outcome.
- Audits
    - Internal and external.
    - Often under the direction of Finance.
    - Valuable, but not adequate by themselves.
    - Approach collaboratively.
- Compliance
    - Internal and external
    - Enforced by audits
- Threat Assessment
    - Part of overall risk assessment.
    - Becoming more of a focus of security teams.
    - Prioritizing vulnerability remediation is influenced by threats you face.

- Vulnerability Assessment
    - Technical scanning is one piece of the puzzle.
        - Automated scanning is a snapshot in time.
        - Will not find all vulnerabilities
        - e.g., may not detect input validation problems like SQLi
    - Assess system life cycle (development and purchasing processes)
    - Assess vulnerabilities in other processes, people, physical sites, as well.
- Business Impact Assessment
    - The bottom line if a threat source exploits a vulnerability
- Risk Assessment
    - Combines Threat, Vulnerability, and Impact assessments.
    - Needs to be repeated.
    - Big topic. We will discuss in more detail in a later class.
- Insurance
    - Risk transfer.
    - Usually appropriate for rare, high-impact events.
    - Value of insuring against InfoSec incidents is debated.
    - Policies often have exclusions if the insured did not meet certain standards of due care.
- Outsourced services
    - Outsourcing some security controls is increasingly common.
    - May gain security expertise and capacity.
    - May lose control and clear lines of responsibility.

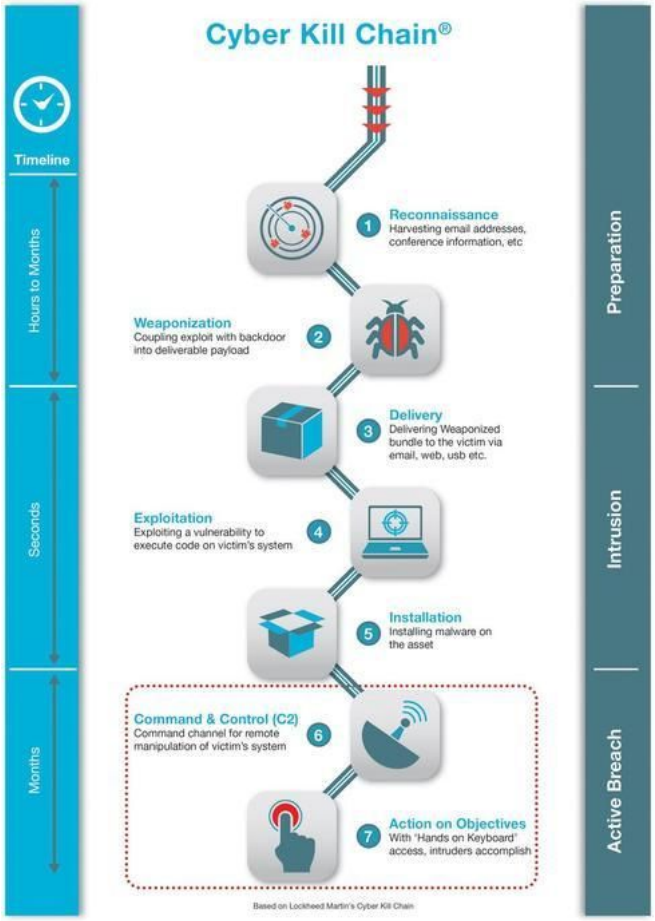
- Security Controls: Layered Defenses
    - Defense in Depth.
    - Can't rely on a single control.
    - Layers should be independent. Ensure failure of one layer doesn't cause failure of another.
    - http://www.sans.edu/research/security-laboratory/article/security-controls

Preventative	Detective	Corrective	Compensatory
Security Awareness Training	System Monitoring	OS Upgrade	Backup Generator
Firewall	IDS	Backup Data Restoral	Hot Site
Anti-virus	Anti-Virus	Anti-Virus	Server Isolation
Security Guard	Motion Detector	Vulnerability Mitigation	
IPS	IPS		

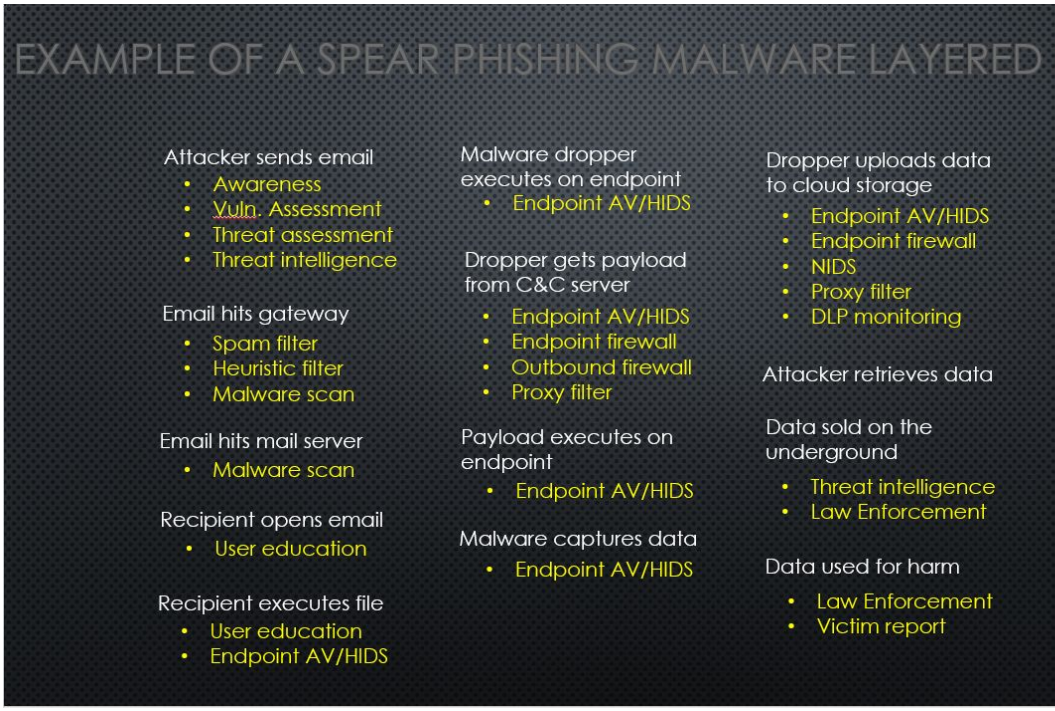
- Lockheed Martin "Kill Chain"

- Focused on malware
- Seven stages
    - Reconnaissance: The attacker finds a gap in security of the social network
    - Weaponization: Attacker builds a malicious attachment
    - Delivery: Attacker delivers it using social media or email targeting an employee
    - Exploitation: The employee opens the file and the vulnerability is exposed
    - Installation: Malware immediately installs on the client
    - Command & Control: The attacker takes control of the system
    - Actions on Objectives: Attacker is able to pinpoint and access critical data
    - http://www.lockheedmartin.com/us/what-we-do/information-technology/cybersecurity/tradecraft/cyber-kill-chain.html
- Useful model.
- Helpful taxonomy.
- Has been criticized for relying on "old school" prevention/intrusion philosophy.
- Based on defense industry but influential across industries.
- *Lockheed Martin*

- DarkReading.com



- Example of a Layered Defense



- What's the catch with layered defenses?
  - Additional complexity
    - "The proliferation of best of breed technologies creates security technology sprawl in pursuit of layered security and defense in depth. We see plenty of examples and sprawl and operational cost rising, where the technologies tend to conflict with each other."
    - Complexity is an enemy of security.
    - Without a good plan in place, it's easy to overspend.
    - Companies focus on filling an immediate control gap and fail to plan for long term maintenance.
  - User pushback
  - Integration challenges
    - Often seen when trying to get all products to log to a SIEM
    - Inconsistent communication standards or taxonomy
  - http://www.csoonline.com/article/3004856/data-protection/the-dark-side-of-layered-security.html#tk.rss_all

PEGASUS

In 2016 Apple patched all public beta and full versions of iOS releases as well as the developer environments of the Pegasus Spyware. It just scrubbed all the carriers chances of getting the spyware on one of their devices.

They patched 3 0day exploits after a human rights activist got a suspicious text on his iPhone that he took in to be investigated by Apple. Basically, the text did a remote jailbreak of the iPhone.

Here are the details on Pegasus from Lookout:

Lookout's analysis determined that the malware exploits three zero-day vulnerabilities, or Trident, in Apple iOS:

- CVE-2016-4655: Information leak in Kernel – A kernel base mapping vulnerability that leaks information to the attacker allowing him to calculate the kernel's location in memory.
- CVE-2016-4656: Kernel Memory corruption leads to Jailbreak – 32 and 64-bit iOS kernel level vulnerabilities that allow the attacker to silently jailbreak the device and install surveillance software.
- CVE-2016-4657: Memory Corruption in WebKit – A vulnerability in the Safari WebKit that allows the attacker to compromise the device when the user clicks on a link.

So, in this case, the attack tried to trick the receiver into clicking a link found in a message. Once it gained entry, it would escalate until it had enough control over the iPhone to begin eavesdropping on communications. This attack was being used by countries that could afford to try to find a such vulnerability.

End-Users need to be aware to never click on links received over messages or emails unless absolutely, 100% sure the link is safe. It's the exact same way you avoid phishing attacks — attempts to con you out of your log in or other private information — and the same advice that's been given for decades.

Since this is public now, it is possible for people to replicate, further advance or simply utilize these vulnerabilities in a deliberate manor. It is imperative that everyone keeps up with the updates and patches that are rolled out by the Operating System distributor. All Operating Systems, mainly Apple and Android, tend to always keep rolling out security improvements, bugs fixes and performance enhancements. So, it is best to always download and install all updates issued in order to ensure usage of the latest OS version.

Every vendor, is working to make it as hard as possible for this to ever happen. They're doing it in several ways:

Improving overall security. Vendors continue to roll out new and better security protocols, including hardening against JavaScript attacks in the latest versions of the current OS released. The goal is to make it more difficult to get onto devices and if anything does get on, even more difficult to do anything once on.

Working with external security experts. Android & Apple have recently announced a security bug bounty program to help independent researchers who find and responsibly disclose vulnerabilities in software. Reacting quickly when 0day exploits are found in the wild. Apple patched Pegasus quickly enough that the previous betas had barely shipped by the time the next versions were pushed out. Security is all about defense in depth, and by doing these things, OS distributors make security increasingly deep.

To get rid of Pegasus:

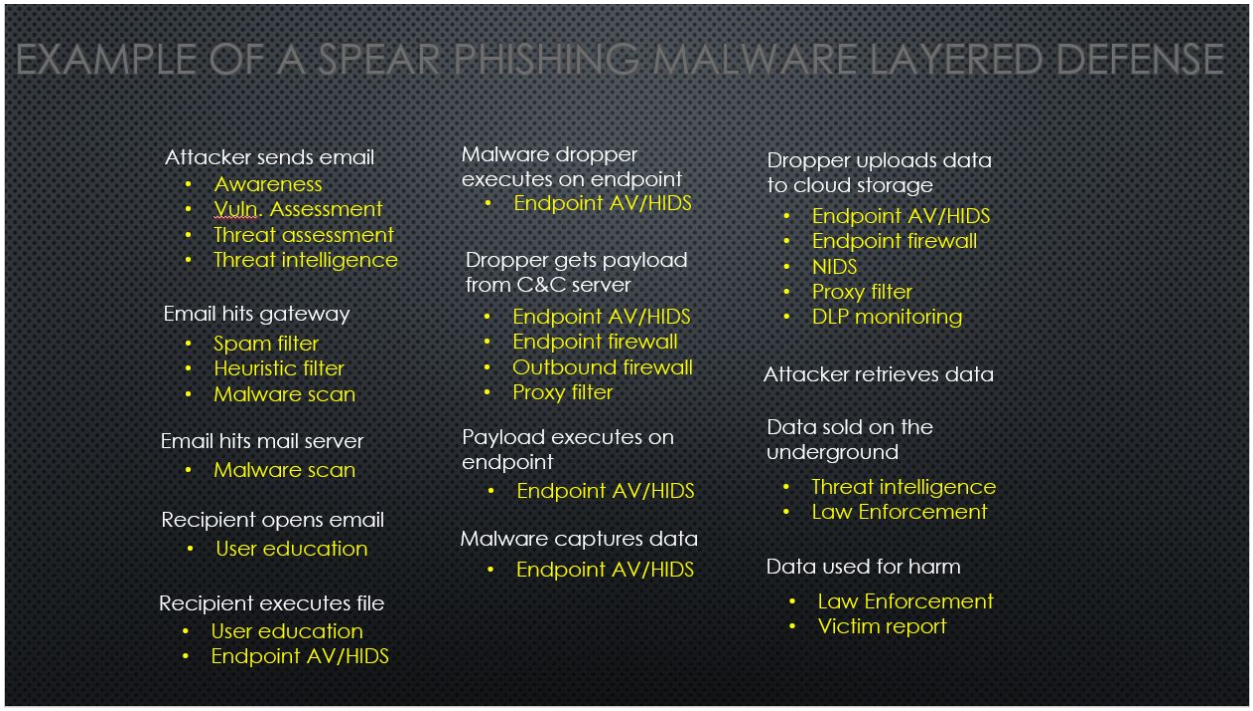
1. Erase the phone, by doing a complete factory reset and make a
    - brand new build or
    - restore from backup.
2. Buy a new phone from a trusted vendor, if you believe your phone is completely vulnerable, and set it up using a
    - backup or
    - brand new build using email in order to make a new sync to get back email, contacts and other information.

(If interested: Apple's talk at this year's Black Hat security conference for more.)

Omar –

1)Each group will engage in some heavy brainstorming and external research to first find out the many possible ways InfoSec could be breached due to end-user actions/behavior.

How are malware being deployed



InfoSec Strategy: Pitfalls

Some obvious reasons strategies fail:

- Poor planning
- Insufficient funding
- Poor execution
- Neglect
- Unexpected corporate events
- Misconduct, merger/acquisition, business failure, etc.

Some less obvious reasons strategies fail:

- Overconfidence in predictions/estimates.
- Unrealistic optimism: corporate culture rewards optimism.
- Anchoring bias: once you put a number out, discussion anchors to that number, whether or not it is relevant.
- Status Quo bias: we like the familiar.
- Herding Instinct: Following fads; “an idea whose time has come!”
- False consensus: overestimating the degree to which others agree
- Other cognitive biases: confirmation bias, selective recall, groupthink.

Security Decay

- Tension between stated policies/risk tolerance and actual practice.
- Gradual decay in processes and controls.
- Easily granted exceptions.
- Individuals are incentivized to meet budgets and deadlines, not security controls.

- “Getting things done” presents a tangible, immediate reward. Skipping a security check presents a low risk to the individual.
- Employees do what they are paid to do.

2) Narrow down/identify one particular area that seems to be relevant and is a cause of concern for organizational InfoSec. Examples, “end-users don’t use strong passwords,” or “end-users fall for phishing scams,” etc.

b) For the particular area you identify, provide an **in-depth technical description** of how an attacker may use/capitalize on end-user’s folly. What the attacker collects from the user (1 3 2b)

COLLECTIVE EFFORT

2D - I identify a Gap with the existing measures, and if the current measure is not efficient state why (COLLECTIVE)

2E - Provide an innovative approach that fill the gap that was identified above.

Business Goals and Objectives: Alignment

- Corporate Governance: the set of responsibilities exercised by the board and executive management to ensure business goals are met, risk is managed, the enterprise is managed responsibly, etc.
- InfoSec governance is a subset of Corporate Governance.
- InfoSec must support and align with Corporate Governance.

Governance framework usually consists of:

- Comprehensive security strategy;
- Governing security policies;
- Procedures, Standards, and Guidelines supporting the policies;
- InfoSec organizational structure that has sufficient authority and resources and that avoids
- conflicts of interest;
- Metrics and monitoring processes.