

iSCSP

International Society of Cyber Security Professionals

Advanced Persistent Threat

Presented by the

International Society of Cyber Security Professionals

<http://www.iscsp.org>

iSCSP.org Contributing Members

Joey Hernandez
CISSP, MBCI, ISFS
San Antonio, Texas

Noelia Prieto Morales,
CISSP, CISM, ITIL
Spain

Dave Barnett, CISSP,
CISM, CSSLP, CSDP
San Francisco,
California

Tas Wake CISSP
CISM CEH
Chester, United
Kingdom

Angel Tabano Redoble
CEH, CHFI
Madrid, Spain

Introduction

- Too often a presentation of ideas begins with a historical analysis of the threat, and focuses on where or who could be causing the problems. We believe the focus on understanding the Cyber Advanced Persistent Threat (APT) is better assessed by taking a snapshot of your current environment.
- The baselined approach provides information security professionals the capability to hear what's on the line. Threats have proven successful against information systems since the early 90's and continue to haunt users, commercial enterprises, and government entities despite technological advances, and media attention.

Introduction

- APT ability and global rate of host infestation is not modeled using kinetic and epidemiology approaches. Useful models to convey minute understanding can be pulled from the World Health Organizations efforts to control infectious disease. Additionally, we believe there is an uncommon understanding of the APT in relation to different areas of Cyber Security. We would be remiss if we simply state that APT is a sophisticated and structured cyber attack without addressing key areas of concern.
- APT thrives because the 3 stake approach (people, process, and technology) to thwarting the threat continues to focus more on technology than the people and process. This is nothing new in the art of defense however; the penalty for mis-focus in the cyber realm has dire consequences. The community as a whole understands the theory, yet continues to fall short in defense implementation.

Addressing the Areas of Concern

- Anatomy of Attack
 - Knowing the “Actors” and their methodology
- Managing Risk
 - Understanding and Identifying the Risk
- Compliance
 - Right direction but alone insufficient
- Policy
 - Institutionalizing a *Cyber Defensive Mindset*

AOA

- **Anatomy of the Attack (AOA)** The APT attack is targeted and persistent the approach often follows the common methodology & anatomy of attack. However, a major difference resides in the concept of time. The initial inability to backtrack the attack has been the continuous point of contention. In addition the ROI is not a major concern and attackers approach is stick and move on if the victim is well defended. Time is on their side and it must be conveyed that they will be back.
- So how would we defend against an APT? Top-down, Bottom-up techniques have always been the discussion point however, we believe it (efforts to mitigate the APT) are best implemented when both factors are considered along with harnessing the defense of every OSI layer. Every attack surface has to be guarded
- So what are we going to tell people?
- We tell them to understand “The Anatomy of Attack”

Information Gathering Stage

- **Reconnaissance – As every successful attack in cyber space, everything starts with cyber intelligence gathering..or the reconnaissance stage. In this phase the attacker uses everything in his disposal to gather as much information as he can and use it to compromise and gain access to a system**
 - Google hacking – a method of using google to gather information about the target without directly making contact with the target
 - Passive network scanning – a method used by an attacker to launch a passive scan on the target's network without the risk of being detected. Although this type of scan do not provide the attacker a very accurate result, it could provide the attacker enough information that can be used to attack the target in the next steps, such as network range, hosts, open ports and services.

Penetration Stage

- **Vulnerability scan and identification** – This phase is launched after gathering enough information about the target. Usually, to avoid being detected a technique is used to launch a vulnerability identification method on the target's network, devices, applications, etc.
- **Perimeter compromise** – Once vulnerabilities are identified, the attacker will try to compromise the network devices used by the target using exploits or other means to take control of the devices.
- **Wireless attacks** – This attack is launched against the wireless network implemented. If the target is using a weak and vulnerable authentication method, the attacker will be able to take control of the device and possibly attack the internal devices as well as the users.
- **Web application attacks** – In a more secure network environment, a layer 7 attack or application attack is more likely successful compared to network level attacks. Most firewalls and IDS/IPS do not have the capability to detect and prevent attacks launched on the application level, as most of these devices functions only the network level.
- **Client-side attacks** – In most cases of a security breach, the weakest link is always the user. Launching a client-side attack using the vulnerabilities of the web application could provide the attacker enough credentials to access the system.

To Do List of an Attacker Once Access is Obtained

- **Privilege escalation** Once inside the system, an attacker will immediately try if he has an admin or super user access. If not, a privilege escalation method is launched. Using the TFTP file transfer protocol together with netcat, the attacker can upload a malicious code to be able to gain admin or root account. Once an attacker is already inside the system, uploading a malicious code is not far from happening.
- **Add an admin or super user account** The attacker then creates a user account and include it in the admin or super user group. This way, the attacker can do anything he wishes.
- **Creating a backdoor** To ensure that access in the future is possible, the attacker will then create a backdoor for himself so he can access anytime he wants in the future.
- **Covering tracks** Once everything is in place, the attacker then removes all possible traces that can be obtained by the administrators. Deleting all the log files or renaming it will provide a hard time to the administrators to identify and trace the attack.
- **Steal everything** Steal all information needed

APT Attack Prevention

- **Application level**
 - Implement secure programming
 - Implement IPS on application level
 - Implement a reverse proxy
 - Monitor
 - Security update
- **Network level**
 - Perimeter and Internal security
 - Network segregation
 - Prevent tunneling

APT Attack Prevention

- **Network level (Cont'd)**

- Monitoring – All network traffic, internal /external must be monitored & logged 24X7.
- HoneyNet – Implement a honeynet on the internal and external part of the network. Honeynets are designed to be open to attacks while recording all the attacks are being recorded on the background. Having a honeynet on the network entices an attacker.

- **Server level**

- Server hardening
- Admin account
- Security patches
- Antivirus

- **Users**

- User privileges – Do not allow users to install non-company approved software or hardware
- Antivirus – Workstation antivirus must be in place and updated at all times.

APT Attack Prevention

- **Audit**

- Risk assessment – a regular risk assessment on the entire infrastructure must be conducted.
- Penetration testing – A regular attack simulation by way of penetration testing must be conducted regularly. A critical infrastructure must implement this exercise at least once per quarter or every time there is change or reconfiguration done on the infrastructure.

- **Trainings and Information Dissemination**

- A company wide training and information dissemination directed to all employees must be conducted on a regular basis. An electronic way of passing critical security information to users must be in place.
- Administrators must be trained and well versed in advanced information security issues. Understanding how hackers attack an infrastructure would enable them to protect the infrastructure effectively.

APT & Risk

- There is no realistic way to completely eliminate the threat that an hostile source will mount an APT style attack
- Risk management allows the business to take cost effective measures to reduce the risk to a manageable level.
- There are several Risk Management Models available and each organisation should adopt the one that best suits their business process
- The basic Risk Management process is:
 1. ***Identify the Risk***
 2. Assess the risk
 3. Mitigate the risk
 4. Review and report the risk
- For the purposes of APT this will concentrate on risk identification

Identify the risk

- The level of risk is identified by the following processes:
 - Business Knowledge
 - Threat Knowledge
 - Threat Assessment

Identify the risk

Business Knowledge

- Business processes need to be fully understood to determine risks
- Catalogue all assets (hardware, data etc)
- Identify critical areas (link to business continuity management work)
- Fully document all external and internal connections
- Determine the value of assets being protected

Threat Knowledge

- Identify Threat Sources
 - There are a variety of threat sources: e.g. foreign Governments, Organised Crime, commercial competitors, activist groups, disgruntled employees, curious hackers
- Determine Threat Capability
 - Professional judgement based on knowledge of threat source: e.g. foreign Government is likely to have the highest level of capability, while an average internet user will be more limited

Identify the risk

Threat Knowledge

- Determine Threat Motivation
 - Once all threat sources are identified, a realistic assessment needs to be made as to their motivation to attack: e.g. An animal rights activists will be highly motivated to attack an organisation that conducts experiments, but a foreign Government will be indifferent

Threat Assessment

- Each source provides a differing level of threat. Sources with good resources and high motivation are more of a threat than one with neither.
- At this stage it is important to remember you are determining the threat not the level of risk posed.

APT RISK

- We know that the Advanced Persistent Threat has some common characteristics:
 - Expensive
 - Resource intensive
 - Needs a motivated attacker
 - Difficult to detect and identify
 - Uses multiple attack vectors
 - Normally uses an external (to the target organisation) agent to mount the attack

APT RISK

Identifying the risk from APT

- Any organisation can be at risk from an APT but all will have greater or lesser probabilities of being attacked
- Identifying threat sources is key to determining the risk posed by APT
- APT is made up of a series of smaller risks which may not be obviously part of a bigger picture attack
- APT can pose a risk anywhere on the network – not just obvious locations
- All systems are vulnerable to APT and must be risk assessed accordingly
- Risk management must take into consideration full asset lifecycle – improperly disposed of assets provide a wealth of information to an attacker
- Document everything to help inform risk management decision: e.g. access logs will give an idea of probing etc.

Compliance Issues

- Common view of APT is of a persistent and purposeful penetration by a well-funded nation-state for
 - Espionage
 - Intelligence gathering (e.g., on dissidents)
- In this context, there is little applicability to most regulatory compliance requirements, such as PCI, HIPAA, GLBA and other privacy regulations.
- However, APT is a **methodology**, and is not restricted to any particular purpose or target
- Possible threat scenarios include using APT for
 - Cyber warfare
 - Terrorism
 - Criminal gain
 - Political gain

Compliance Issues

- Mounting an APT attack is expensive and resource intensive.
 - At this time, it would not be cost effective for most criminals to replace current opportunistic attacks of content, and which are covered by most regulatory requirements.
- Not all uses of APT have regulatory implications, but there is no reason to believe it couldn't happen, given sufficient motivation, e.g.
 - Embarrassing a political opponent by disclosing medical records
 - Massive theft of Credit Card information and disruption of financial services
- The controls associated with current compliance requirements, while sufficient for most threats, are inadequate protection against an APT.
- For companies governed by regulatory compliance, the current protection against an APT is lack of attention or interest on the part of the attackers.
 - **This may change.**

Creating Policy

- **Attack Feature:** They try to access valuable information that is available on the computers of an organization.
- **Policy:** Restrictions compromising data access based on the principle of need to know by which a user / pc only has access to data necessary to their work.
- **Conclusion:** Constrain and restrict location and distribution of valuable information.

Creating Policy

- **Feature:** Send the information collected from victims through authorized protocols like HTTP and encrypted packets.
- **Policy:** Use of next-generation firewalls to allow inspection of data packets according to protocol.
- **Conclusion:** Detection of malicious traffic over standard protocols is required.

Creating Policy

- **Feature:** APTs avoid detection by most antivirus and so remain as long as possible on the computers of the organization.
- **Policy:** Keep computer operating system of the organization updated. Having an advanced anti-virus behavior oriented technology can help detect zero-day attacks.
- **Conclusion:** Currently there are no anti-virus capable of detecting all APT attacks. But these attacks make use of vulnerabilities in operating systems which can be solved by patching, and by use of anomalous behavior detection.

Creating Policy

- **Feature:** Attacks extend through the organization using approved protocols in most LAN networks such as netbios, dns, http
- **Policy:** It is important to avoid spreading wide LANs networks at Layer 2. Thus the commercial department should not have physical access to the development department.
- **Conclusion:** Segregate networks to allow an infection to be restricted to a particular segment.

Prevention

- Prevention of the APT continues to be a collaborative effort, with the standing methodology being a focus on
 - **People**
 - **Process**
 - **Technology**
- Added to the to this methodology **must be**
 - **Global Collaboration**
 - More similarities than differences
 - Need to believe we all have a “common enemy”
 - Not a nation
 - Not a person
 - A threat
- *Protecting Cyberspace is protecting the Economic Future*