Advanced & Persistent Threat Analysis - I

Burak Ekici
ekcburak@hotmail.com

Department of Computer Engineering,
Yaşar University,
Turkey.

April 21, 2012

Agenda

Conventional Cyber Attacks

Definition: Conventional Cyber Attacks

Conventional Cyber Attacks *are the gain or destroy-control based attempts that aim to use* **well-known vulnerabilities** *of any* **arbitrarily detected or un-specified system** *to exploit it within the scope of attacker's at that moment needs or demands* **without the permissions of real system users**.

Example: Conventional Cyber Attacks

1. *Hacking or Cracking.*
2. *Malware Attacks:*
   - *Viruses*
   - *Trojans*
   - *Worms*

Conventional Cyber Attacks

Definition: Conventional Cyber Attacks

Conventional Cyber Attacks *are the gain or destroy-control based attempts that aim to use* **well-known vulnerabilities** *of any* **arbitrarily detected or un-specified system** *to exploit it within the scope of attacker's at that moment needs or demands* **without the permissions of real system users**.

Example: Conventional Cyber Attacks

1. *Hacking or Cracking.*
2. *Malware Attacks:*
   - *Viruses*
   - *Trojans*
   - *Worms*

Conventional Cyber Attacks

Definition: Conventional Cyber Attacks

Conventional Cyber Attacks *are the gain or destroy-control based attempts that aim to use* **well-known vulnerabilities** *of any* **arbitrarily detected or un-specified system** *to exploit it within the scope of attacker's at that moment needs or demands* **without the permissions of real system users**.

Example: Conventional Cyber Attacks

1. *Hacking or Cracking.*
2. *Malware Attacks:*
   - *Viruses*
   - *Trojans*
   - *Worms*

Conventional Cyber Attacks

Definition: Conventional Cyber Attacks

Conventional Cyber Attacks *are the gain or destroy-control based attempts that aim to use* **well-known vulnerabilities** *of any* **arbitrarily detected or un-specified system** *to exploit it within the scope of attacker's at that moment needs or demands* **without the permissions of real system users**.

Example: Conventional Cyber Attacks

1. *Hacking or Cracking.*
2. *Malware Attacks:*
   - *Viruses*
   - *Trojans*
   - *Worms*

Advanced & Persistent Threats

Definition: Advanced & Persistent Threats

Advanced & Persistent Threats *are the cyber attacks based on* **do not have to be known vulnerabilities** *(mostly by* **exploiting 0-day vulnerabilities***) of a* **specifically defined target or system** *to extract* **already defined critical data**.

0-day Vulnerability

Definition: Zero-day Vulnerability

A zero-day vulnerability is the one that there is **exactly zero days** *in between the vulnerability in question has become known by the vendors of vulnerable H/W or S/W and the attack performed by using that vulnerability such as the ones in:*

- *Internet-Explorer*
- *Adobe*
- *Mozilla*
- *Apache Software Foundation*

Note

For more information about currently known 0-day vulnerabilities; please Google : 0-day list!

0-day Vulnerability

Definition: Zero-day Vulnerability

A zero-day vulnerability is the one that there is **exactly zero days** *in between the vulnerability in question has become known by the vendors of vulnerable H/W or S/W and the attack performed by using that vulnerability such as the ones in:*

- *Internet-Explorer*
- *Adobe*
- *Mozilla*
- *Apache Software Foundation*

Note

For more information about currently known 0-day vulnerabilities; please Google : 0-day list!

Crucial Terms

Terms

Advanced: the term used to indicate the level of attack in question standing ahead of basic level.

- *skilled attacker,*
- *developing resources to exploit zero-day vulnerabilities,*
- *variety of attack tools in order to avoid the detection or prevention measures of many organizations have in place.*

ADAPTATIONS FOR DEFENDERS' EFFORTS IN ORDER TO RESIST THEM.

Crucial Terms

Terms

Advanced: the term used to indicate the level of attack in question standing ahead of basic level.

- *skilled attacker,*
- *developing resources to exploit zero-day vulnerabilities,*
- *variety of attack tools in order to avoid the detection or prevention measures of many organizations have in place.*

ADAPTATIONS FOR DEFENDERS' EFFORTS IN ORDER TO RESIST THEM.

Crucial Terms

Terms

Advanced: the term used to indicate the level of attack in question standing ahead of basic level.

- *skilled attacker,*
- *developing resources to exploit zero-day vulnerabilities,*
- *variety of attack tools in order to avoid the detection or prevention measures of many organizations have in place.*

ADAPTATIONS FOR DEFENDERS' EFFORTS IN ORDER TO RESIST THEM.

Crucial Terms

Terms

Persistent: the term demonstrates that attack in question insists to resume until beforehand well-defined goal is achieved.

PURSUES ITS OBJECTIVES REPEATEDLY OVER AN EXTENDED PERIOD OF TIME.

Crucial Terms

Terms

Persistent: the term demonstrates that attack in question insists to resume until beforehand well-defined goal is achieved.

PURSUES ITS OBJECTIVES REPEATEDLY OVER AN EXTENDED PERIOD OF TIME.

Crucial Terms

Terms

Threat: the term used to define the source of danger representing the more concerted and directed effort. NOT LIKE:

- *script kiddies performing port scanning on edge devices*
- *the odd SQL injection attack coming in through a poorly maintained web application*

Crucial Terms

Terms

Threat: the term used to define the source of danger representing the more concerted and directed effort. NOT LIKE:

- *script kiddies performing port scanning on edge devices*
- *the odd SQL injection attack coming in through a poorly maintained web application*

Dimensions of APTs by A Traditional Threat Vector with Additional Properties

Definition: Threat Vectors

A **Threat Vector** *is a path or a tool that a threat actor or the* **attacker** *uses to attack the target.*

Phil Withers.

Process of Designing A Traditional Threat Vector

1. *Discovering the vulnerability*
2. *Exploiting the vulnerability*
3. *Information Collection*
4. *Information Analysing*

Lukas Ruf.

Dimensions of APTs by A Traditional Threat Vector with Additional Properties

Definition: Threat Vectors

A **Threat Vector** *is a path or a tool that a threat actor or the* **attacker** *uses to attack the target.*

Phil Withers.

Process of Designing A Traditional Threat Vector

1. *Discovering the vulnerability*
2. *Exploiting the vulnerability*
3. *Information Collection*
4. *Information Analysing*

Lukas Ruf.

Dimensions of APTs by A Traditional Threat Vector with Additional Properties

Definition: Threat Vectors

A **Threat Vector** *is a path or a tool that a threat actor or the* **attacker** *uses to attack the target.*

Phil Withers.

Process of Designing A Traditional Threat Vector

1. *Discovering the vulnerability*
2. *Exploiting the vulnerability*
3. *Information Collection*
4. *Information Analysing*

Lukas Ruf.

Dimensions of APTs by A Traditional Threat Vector with Additional Properties

Definition: Threat Vectors

A **Threat Vector** *is a path or a tool that a threat actor or the* **attacker** *uses to attack the target.*

Phil Withers.

Process of Designing A Traditional Threat Vector

1. *Discovering the vulnerability*
2. *Exploiting the vulnerability*
3. *Information Collection*
4. *Information Analysing*

Lukas Ruf.

Dimensions of APTs by A Traditional Threat Vector with Additional Properties

Definition: Threat Vectors

A **Threat Vector** *is a path or a tool that a threat actor or the* **attacker** *uses to attack the target.*

Phil Withers.

Process of Designing A Traditional Threat Vector

1. *Discovering the vulnerability*
2. *Exploiting the vulnerability*
3. *Information Collection*
4. *Information Analysing*

Lukas Ruf.

Design Pattern for APTs

Dimensions of APT

- *The primary dimensions of an APT are:*
  - *Method (traditional threat vector):* **HOW?**
  - *Time:* **WHEN?**
  - *Organization:* **WHO?**

An Important Notice: Process of Designing an APT

The iteration of Method as the traditional threat vector within the course of Time for an already specified Target, one can get the **design pattern** *for APTs.*

Design Pattern for APTs

Dimensions of APT

- *The primary dimensions of an APT are:*
  - *Method (traditional threat vector):* **HOW?**
  - *Time:* **WHEN?**
  - *Organization:* **WHO?**

An Important Notice: Process of Designing an APT

The iteration of Method as the traditional threat vector within the course of Time for an already specified Target, one can get the **design pattern** *for APTs.*

Design Pattern for APTs

Dimensions of APT

- *The primary dimensions of an APT are:*
  - *Method (traditional threat vector):* **HOW?**
  - *Time:* **WHEN?**
  - *Organization:* **WHO?**

An Important Notice: Process of Designing an APT

The iteration of Method as the traditional threat vector within the course of Time for an already specified Target, one can get the **design pattern** *for APTs.*

Design Pattern for APTs

Dimensions of APT

- *The primary dimensions of an APT are:*
  - *Method (traditional threat vector):* **HOW?**
  - *Time:* **WHEN?**
  - *Organization:* **WHO?**

An Important Notice: Process of Designing an APT

The iteration of Method as the traditional threat vector within the course of Time for an already specified Target, one can get the **design pattern** *for APTs.*

Design Pattern for APTs

Dimensions of APT

- *The primary dimensions of an APT are:*
  - *Method (traditional threat vector):* **HOW?**
  - *Time:* **WHEN?**
  - *Organization:* **WHO?**

An Important Notice: Process of Designing an APT

The iteration of Method as the traditional threat vector within the course of Time for an already specified Target, one can get the **design pattern** *for APTs.*

Characteristics of Advanced & Persistent Threats

APT Characteristics

- *Characteristics of Advanced & Persistent Threats could be analyzed via four crucial factors:*
  - *Actors*
  - *Motives*
  - *Targets*
  - *Goals*

Characteristics of Advanced & Persistent Threats

APT Characteristics

- *Characteristics of Advanced & Persistent Threats could be analyzed via four crucial factors:*
  - *Actors*
  - *Motives*
  - *Targets*
  - *Goals*

Characteristics of Advanced & Persistent Threats

APT Characteristics

- *Characteristics of Advanced & Persistent Threats could be analyzed via four crucial factors:*
  - *Actors*
  - *Motives*
  - *Targets*
  - *Goals*

Characteristics of Advanced & Persistent Threats

APT Characteristics

- *Characteristics of Advanced & Persistent Threats could be analyzed via four crucial factors:*
  - *Actors*
  - *Motives*
  - *Targets*
  - *Goals*

Characteristics of Advanced & Persistent Threats

APT Characteristics

- *Characteristics of Advanced & Persistent Threats could be analyzed via four crucial factors:*
  - *Actors*
  - *Motives*
  - *Targets*
  - *Goals*

Characteristics of Advanced & Persistent Threats: Actors

APT: Actors

APT has a wide variety of actor types:

- *terrorists,*
- *organized crime groups,*
- *malicious insiders,*
- *ex-employees,*
- *nation-states.*
- *...*

Example: APT Actors

- *A group commanded by Vladimir Putin: NASHI*
- *In May 2007, Cyberattacks in Estonia by Russian Mafia.*
- *In April 2008, Botnet AntiCNN.exe.*

Characteristics of Advanced & Persistent Threats: Actors

APT: Actors

APT has a wide variety of actor types:

- *terrorists,*
- *organized crime groups,*
- *malicious insiders,*
- *ex-employees,*
- *nation-states.*
- *...*

Example: APT Actors

- *A group commanded by Vladimir Putin: NASHI*
- *In May 2007, Cyberattacks in Estonia by Russian Mafia.*
- *In April 2008, Botnet AntiCNN.exe.*

Characteristics of Advanced & Persistent Threats: Actors

APT: Actors

APT has a wide variety of actor types:

- *terrorists,*
- *organized crime groups,*
- *malicious insiders,*
- *ex-employees,*
- *nation-states.*
- *...*

Example: APT Actors

- *A group commanded by Vladimir Putin: NASHI*
- *In May 2007, Cyberattacks in Estonia by Russian Mafia.*
- *In April 2008, Botnet AntiCNN.exe.*

Characteristics of Advanced & Persistent Threats: Actors

APT: Actors

APT has a wide variety of actor types:

- *terrorists,*
- *organized crime groups,*
- *malicious insiders,*
- *ex-employees,*
- *nation-states.*
- *...*

Example: APT Actors

- *A group commanded by Vladimir Putin: NASHI*
- *In May 2007, Cyberattacks in Estonia by Russian Mafia.*
- *In April 2008, Botnet AntiCNN.exe.*

Characteristics of Advanced & Persistent Threats: Actors

APT: Actors

APT has a wide variety of actor types:

- *terrorists,*
- *organized crime groups,*
- *malicious insiders,*
- *ex-employees,*
- *nation-states.*
- ...

Example: APT Actors

- *A group commanded by Vladimir Putin: NASHI*
- *In May 2007, Cyberattacks in Estonia by Russian Mafia.*
- *In April 2008, Botnet AntiCNN.exe.*

Characteristics of Advanced & Persistent Threats: Actors

APT: Actors

APT has a wide variety of actor types:

- *terrorists,*
- *organized crime groups,*
- *malicious insiders,*
- *ex-employees,*
- *nation-states.*
- *...*

Example: APT Actors

- *A group commanded by Vladimir Putin: NASHI*
- *In May 2007, Cyberattacks in Estonia by Russian Mafia.*
- *In April 2008, Botnet AntiCNN.exe.*

Characteristics of Advanced & Persistent Threats: Actors

APT: Actors

APT has a wide variety of actor types:

- *terrorists,*
- *organized crime groups,*
- *malicious insiders,*
- *ex-employees,*
- *nation-states.*
- *...*

Example: APT Actors

- *A group commanded by Vladimir Putin: NASHI*
- *In May 2007, Cyberattacks in Estonia by Russian Mafia.*
- *In April 2008, Botnet AntiCNN.exe.*

Characteristics of Advanced & Persistent Threats: Motives

APT: Motives

Motivations of APTs are mostly center upon economical expectations:

- *Primarily motivated by money: 69%*
- *Ideology: 22%*
- *Coerced: 5%*
- *Importance: 4%*

Espionage by the Numbers: Richard J. & Heuer Jr.

Characteristics of Advanced & Persistent Threats: Motives

APT: Motives

Motivations of APTs are mostly center upon economical expectations:

- *Primarily motivated by money: 69%*
- *Ideology: 22%*
- *Coerced: 5%*
- *Importance: 4%*

Espionage by the Numbers: Richard J. & Heuer Jr.

Characteristics of Advanced & Persistent Threats: Motives

APT: Motives

Motivations of APTs are mostly center upon economical expectations:

- *Primarily motivated by money: 69%*
- *Ideology: 22%*
- *Coerced: 5%*
- *Importance: 4%*

Espionage by the Numbers: Richard J. & Heuer Jr.

Characteristics of Advanced & Persistent Threats: Motives

APT: Motives

Motivations of APTs are mostly center upon economical expectations:

- *Primarily motivated by money: 69%*
- *Ideology: 22%*
- *Coerced: 5%*
- *Importance: 4%*

Espionage by the Numbers: Richard J. & Heuer Jr.

Characteristics of Advanced & Persistent Threats: Targets

APT: Targets

APTs have well-defined targets, such as:

- *Governmental Agencies*
  - *to steal critical data from* **intelligence** *and/or* **military services**.
- *Financial Industry*
  - *to steal* **bank account informations**.
- *Organizations with Intellectual Properties.*
  - *to access* **confidential intellectual property**.
- *Critical Infrastructures*
  - *to collapse* **working infrastructure** *down.*

Characteristics of Advanced & Persistent Threats: Targets

APT: Targets

APTs have well-defined targets, such as:

- *Governmental Agencies*
  - *to steal critical data from* **intelligence** *and/or* **military services**.
- *Financial Industry*
  - *to steal* **bank account informations**.
- *Organizations with Intellectual Properties.*
  - *to access* **confidential intellectual property**.
- *Critical Infrastructures*
  - *to collapse* **working infrastructure** *down.*

Characteristics of Advanced & Persistent Threats: Targets

APT: Targets

APTs have well-defined targets, such as:

- *Governmental Agencies*
  - *to steal critical data from* **intelligence** *and/or* **military services**.
- *Financial Industry*
  - *to steal* **bank account informations**.
- *Organizations with Intellectual Properties.*
  - *to access* **confidential intellectual property**.
- *Critical Infrastructures*
  - *to collapse* **working infrastructure** *down.*

Characteristics of Advanced & Persistent Threats: Targets

APT: Targets

APTs have well-defined targets, such as:

- *Governmental Agencies*
  - *to steal critical data from* **intelligence** *and/or* **military services**.
- *Financial Industry*
  - *to steal* **bank account informations**.
- *Organizations with Intellectual Properties.*
  - *to access* **confidential intellectual property**.
- *Critical Infrastructures*
  - *to collapse* **working infrastructure** *down.*

Characteristics of Advanced & Persistent Threats: Targets

APT: Targets

APTs have well-defined targets, such as:

- *Governmental Agencies*
  - *to steal critical data from* **intelligence** *and/or* **military services**.
- *Financial Industry*
  - *to steal* **bank account informations**.
- *Organizations with Intellectual Properties.*
  - *to access* **confidential intellectual property**.
- *Critical Infrastructures*
  - *to collapse* **working infrastructure** *down.*

Characteristics of Advanced & Persistent Threats: Targets

Example: APT Targets

- *F-35 Joint Strike Fighter: In 2009, The Wall Street Journal reported that the Pentagon's $300 billion project had terabytes of data stolen.*
- *Titan Rain: is the series of attacks in 2003 to extract the data from Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, NASA, and several other government organizations.*
- *Citibank: Targeted attacks in December 2009 on Citibank infrastructure initiated by Russian organized crime.*
- *Operation Aurora: Attacks that were performed against more than 20 companies including Google to steal their intellectual properties.*
- *Stuxnet: Attacks targeting PLCs used in Supervisory Control and Data Acquisition (SCADA) Systems.*

Characteristics of Advanced & Persistent Threats: Targets

Example: APT Targets

- *F-35 Joint Strike Fighter: In 2009, The Wall Street Journal reported that the Pentagon's $300 billion project had terabytes of data stolen.*
- *Titan Rain: is the series of attacks in 2003 to extract the data from Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, NASA, and several other government organizations.*
- *Citibank: Targeted attacks in December 2009 on Citibank infrastructure initiated by Russian organized crime.*
- *Operation Aurora: Attacks that were performed against more than 20 companies including Google to steal their intellectual properties.*
- *Stuxnet: Attacks targeting PLCs used in Supervisory Control and Data Acquisition (SCADA) Systems.*

Characteristics of Advanced & Persistent Threats: Targets

Example: APT Targets

- *F-35 Joint Strike Fighter: In 2009, The Wall Street Journal reported that the Pentagon's $300 billion project had terabytes of data stolen.*
- *Titan Rain: is the series of attacks in 2003 to extract the data from Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, NASA, and several other government organizations.*
- *Citibank: Targeted attacks in December 2009 on Citibank infrastructure initiated by Russian organized crime.*
- *Operation Aurora: Attacks that were performed against more than 20 companies including Google to steal their intellectual properties.*
- *Stuxnet: Attacks targeting PLCs used in Supervisory Control and Data Acquisition (SCADA) Systems.*

Characteristics of Advanced & Persistent Threats: Targets

Example: APT Targets

- *F-35 Joint Strike Fighter: In 2009, The Wall Street Journal reported that the Pentagon's $300 billion project had terabytes of data stolen.*
- *Titan Rain: is the series of attacks in 2003 to extract the data from Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, NASA, and several other government organizations.*
- *Citibank: Targeted attacks in December 2009 on Citibank infrastructure initiated by Russian organized crime.*
- *Operation Aurora: Attacks that were performed against more than 20 companies including Google to steal their intellectual properties.*
- *Stuxnet: Attacks targeting PLCs used in Supervisory Control and Data Acquisition (SCADA) Systems.*

Characteristics of Advanced & Persistent Threats: Targets

Example: APT Targets

- *F-35 Joint Strike Fighter: In 2009, The Wall Street Journal reported that the Pentagon's $300 billion project had terabytes of data stolen.*
- *Titan Rain: is the series of attacks in 2003 to extract the data from Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, NASA, and several other government organizations.*
- *Citibank: Targeted attacks in December 2009 on Citibank infrastructure initiated by Russian organized crime.*
- *Operation Aurora: Attacks that were performed against more than 20 companies including Google to steal their intellectual properties.*
- *Stuxnet: Attacks targeting PLCs used in Supervisory Control and Data Acquisition (SCADA) Systems.*

Characteristics of Advanced & Persistent Threats: Goals

Example: APT Goals

Goals intended to be achieved:

1. *Penetrating into the target system without being detected.*
2. *Trying to detect other backdoors to seize the sytem completely.*
3. *Starting the primary objective:*
   - *Grab the sensitive data.*
   - *Monitor other possibly critical connections.*
   - *Break the important operations.*
4. *Leaving undetected.*

Characteristics of Advanced & Persistent Threats: Goals

Example: APT Goals

Goals intended to be achieved:

1. *Penetrating into the target system without being detected.*
2. *Trying to detect other backdoors to seize the sytem completely.*
3. *Starting the primary objective:*
   - *Grab the sensitive data.*
   - *Monitor other possibly critical connections.*
   - *Break the important operations.*
4. *Leaving undetected.*

Characteristics of Advanced & Persistent Threats: Goals

Example: APT Goals

Goals intended to be achieved:

1. *Penetrating into the target system without being detected.*
2. *Trying to detect other backdoors to seize the sytem completely.*
3. *Starting the primary objective:*
   - *Grab the sensitive data.*
   - *Monitor other possibly critical connections.*
   - *Break the important operations.*
4. *Leaving undetected.*

Characteristics of Advanced & Persistent Threats: Goals

Example: APT Goals

Goals intended to be achieved:

1. *Penetrating into the target system without being detected.*
2. *Trying to detect other backdoors to seize the sytem completely.*
3. *Starting the primary objective:*
   - *Grab the sensitive data.*
   - *Monitor other possibly critical connections.*
   - *Break the important operations.*
4. *Leaving undetected.*

Characteristics of Advanced & Persistent Threats: Goals

Example: APT Goals

Goals intended to be achieved:

1. *Penetrating into the target system without being detected.*
2. *Trying to detect other backdoors to seize the sytem completely.*
3. *Starting the primary objective:*
   - *Grab the sensitive data.*
   - *Monitor other possibly critical connections.*
   - *Break the important operations.*
4. *Leaving undetected.*

Characteristics of Advanced & Persistent Threats: Goals

Example: APT Goals

Goals intended to be achieved:

1. *Penetrating into the target system without being detected.*
2. *Trying to detect other backdoors to seize the sytem completely.*
3. *Starting the primary objective:*
   - *Grab the sensitive data.*
   - *Monitor other possibly critical connections.*
   - *Break the important operations.*
4. *Leaving undetected.*

Characteristics of Advanced & Persistent Threats: Goals

Example: APT Goals

Goals intended to be achieved:

1. *Penetrating into the target system without being detected.*
2. *Trying to detect other backdoors to seize the sytem completely.*
3. *Starting the primary objective:*
   - *Grab the sensitive data.*
   - *Monitor other possibly critical connections.*
   - *Break the important operations.*
4. *Leaving undetected.*

Schema of the APT Execution

APT Execution Steps

Obviously no two attacks are following the same methods , but it is possible to illustrate a set of common execution steps of APTs:

1. *Phase 1:* **Reconnaissance, Launch, and Infect**.
2. *Phase 2:* **Control, Discover, Persist**.
3. *Phase 3:* **Extract and Take Action**.

Schema of the APT Execution

APT Execution Steps

Obviously no two attacks are following the same methods , but it is possible to illustrate a set of common execution steps of APTs:

1. *Phase 1:* **Reconnaissance, Launch, and Infect**.
2. *Phase 2:* **Control, Discover, Persist**.
3. *Phase 3:* **Extract and Take Action**.

Schema of the APT Execution

APT Execution Steps

Obviously no two attacks are following the same methods , but it is possible to illustrate a set of common execution steps of APTs:

1. *Phase 1:* **Reconnaissance, Launch, and Infect**.
2. *Phase 2:* **Control, Discover, Persist**.
3. *Phase 3:* **Extract and Take Action**.

Schema of the APT Execution

APT Execution Steps

Obviously no two attacks are following the same methods , but it is possible to illustrate a set of common execution steps of APTs:

1. *Phase 1:* **Reconnaissance, Launch, and Infect**.
2. *Phase 2:* **Control, Discover, Persist**.
3. *Phase 3:* **Extract and Take Action**.

The APT Execution Process: Reconnaissance, Launch, Infect

APT Execution Steps: Phase 1

Phase 1 involves three sub-phases:

- *Reconnaissance: Specifications of* **key assets** *and* **vulnerabilities** *of the system to be attacked.*
- *Launch: Gaining access to a* **privileged host** *via some methods such as:*
  - *Fake e-mails with embedded links, .pdf or .doc extended files involving zero-day attack mal-wares.*
  - *Performing social engineering to gain access of privileged user accounts.*
- *Infect: is said to be completed when the* **attacking mal-ware** *is installed onto the privileged host.*

The APT Execution Process: Reconnaissance, Launch, Infect

APT Execution Steps: Phase 1

Phase 1 involves three sub-phases:

- *Reconnaissance: Specifications of* **key assets** *and* **vulnerabilities** *of the system to be attacked.*
- *Launch: Gaining access to a* **privileged host** *via some methods such as:*
  - *Fake e-mails with embedded links, .pdf or .doc extended files involving zero-day attack mal-wares.*
  - *Performing social engineering to gain access of privileged user accounts.*
- *Infect: is said to be completed when the* **attacking mal-ware** *is installed onto the privileged host.*

The APT Execution Process: Reconnaissance, Launch, Infect

APT Execution Steps: Phase 1

Phase 1 involves three sub-phases:

- *Reconnaissance: Specifications of* **key assets** *and* **vulnerabilities** *of the system to be attacked.*
- *Launch: Gaining access to a* **privileged host** *via some methods such as:*
  - *Fake e-mails with embedded links, .pdf or .doc extended files involving zero-day attack mal-wares.*
  - *Performing social engineering to gain access of privileged user accounts.*
- *Infect: is said to be completed when the* **attacking mal-ware** *is installed onto the privileged host.*

The APT Execution Process: Control, Discover, Persist

APT Execution Steps: Phase 2

Phase 2 also has three sub-phases that are:

- *Control: the phase which attacker starts controlling the privileged host via* **command-and-control service**.
- *Discover: in this stage; attacker uploads some number of additional components that are able to discover the strength of the privileged host. It may involve:*
  - *the right to access PKI servers.*
  - *active directories.*

  By this way; other network locations of the privileged host could be identified.
- *Persist: the mal-ware tries to be kept undetected and it is designed to insist on attacking although it had already identified.*

THE POINT IN WHICH ITERATION IS BEING INSISTED.

The main difference between a traditional threat and an APT.

The APT Execution Process: Control, Discover, Persist

APT Execution Steps: Phase 2

Phase 2 also has three sub-phases that are:

- *Control: the phase which attacker starts controlling the privileged host via* **command-and-control service**.
- *Discover: in this stage; attacker uploads some number of additional components that are able to discover the strength of the privileged host. It may involve:*
  - *the right to access PKI servers.*
  - *active directories.*

  By this way; other network locations of the privileged host could be identified.
- *Persist: the mal-ware tries to be kept undetected and it is designed to insist on attacking although it had already identified.*

THE POINT IN WHICH ITERATION IS BEING INSISTED.

The main difference between a traditional threat and an APT.

The APT Execution Process: Control, Discover, Persist

APT Execution Steps: Phase 2

Phase 2 also has three sub-phases that are:

- *Control: the phase which attacker starts controlling the privileged host via* **command-and-control service**.
- *Discover: in this stage; attacker uploads some number of additional components that are able to discover the strength of the privileged host. It may involve:*
  - *the right to access PKI servers.*
  - *active directories.*

  By this way; other network locations of the privileged host could be identified.
- *Persist: the mal-ware tries to be kept undetected and it is designed to insist on attacking although it had already identified.*

THE POINT IN WHICH ITERATION IS BEING INSISTED.

The main difference between a traditional threat and an APT.

The APT Execution Process: Control, Discover, Persist

APT Execution Steps: Phase 2

Phase 2 also has three sub-phases that are:

- *Control: the phase which attacker starts controlling the privileged host via* **command-and-control service**.
- *Discover: in this stage; attacker uploads some number of additional components that are able to discover the strength of the privileged host. It may involve:*
  - *the right to access PKI servers.*
  - *active directories.*

  By this way; other network locations of the privileged host could be identified.
- *Persist: the mal-ware tries to be kept undetected and it is designed to insist on attacking although it had already identified.*

THE POINT IN WHICH ITERATION IS BEING INSISTED.

The main difference between a traditional threat and an APT.

The APT Execution Process: Extract, Take Action

APT Execution Steps: Phase 3

There are two sub-phases of the third phase:

- *Extract: in this stage* **captured data is imported** *to the attacker's side and then* **evaluated**.
- *Take Action:* **the inferences of the evaluation** *could be used against victim in a wide-variety of ways such as:*
  - *Ransom: As a correspondence of the stolen information; attacker might ask for a ransom.*
  - *Share or sell attack methods: methods of the attack might be sold to other criminal groups.*
  - *Sell information: handled information might be sold to the other criminals.*
  - *Public Disclosure: inferences might be announced in public by attackers to show their power off or to collapse the victim organization down.*

The APT Execution Process: Extract, Take Action

APT Execution Steps: Phase 3

There are two sub-phases of the third phase:

- *Extract: in this stage* **captured data is imported** *to the attacker's side and then* **evaluated**.
- *Take Action:* **the inferences of the evaluation** *could be used against victim in a wide-variety of ways such as:*
  - *Ransom: As a correspondence of the stolen information; attacker might ask for a ransom.*
  - *Share or sell attack methods: methods of the attack might be sold to other criminal groups.*
  - *Sell information: handled information might be sold to the other criminals.*
  - *Public Disclosure: inferences might be announced in public by attackers to show their power off or to collapse the victim organization down.*

Possible Impacts of an APT as a Kinetic Warfare

An Imagination

Imagine an APT against **the main electric grid** *of a country and the analyze the possible outcomes:*

1. *Electric power goes off.*
2. *Due to the safety of power-producing plants like nuclear plants that are provided by electric systems, to avoid any accident, should also be shut down.*
3. *After a few days; gas stations, ATMs, and grocery stores are depleted.*
4. *Looting and rioting begins.*
5. *Hospitals and emergency services collapse down.*
6. *Military forces seize the situation so national-defense gets negatively effected, if any military attack happens.*

The Paradigm Shift: APTs vs Conventional Threats

	CONVENTIONAL THREATS	**vs. ADVANCED PERSISTENT THREATS**
		ADDITIVE:
Who are the attackers?	Opportunistic hackers or cyber criminals	Well-resourced and determined adversaries: nation-states (and associated groups), globally connected organized crime, nefarious corporations, hacktivists
What data do they target?	Custodial data: credit card data, bank account data, personal information Generically valuable information that could be used by or sold to many interested parties	High-value digital assets: intellectual property, national-security data, trade secrets, source code, R&D material, market and customer information, financial systems, business and manufacturing plans, access to mission-critical operations, and so forth Specifically valuable information that is pursued by or could be sold to a defined party
What organizations do they target?	Broad-based attacks on banks, card-data processors, online retail and services, general industry, and their customer bases	A selected organization in government, defense, oil & gas, energy, technology, financial services, and so on
Why?	Financial gain, identity theft, fraud, spam, recognition	Market manipulation, strategic advantage in national defense, economic advantage in an industry, competitive position in business negotiations, damage to critical infrastructure, politically driven causes

The Paradigm Shift: APTs vs Conventional Threats

How?	Gain entry by attacking perimeter	Gain entry by exploiting end users and end points; carry out attack using multiple vectors
Malware used	Typically off-the-shelf malware Propagate malware as broadly as possible to improve the chances of landing in a profitable place	Often custom-designed or tailored malware Targeted use of malware in attacking one organization: to hijack systems, create diversions, establish back doors, and communicate with command-and-control servers
Skills	Technical skills	Reconnaissance: in-depth knowledge of an organization's people, business processes, and network topology
Reaction to counter-measures	Move to an easier target	Modify attack to pursue the target further

Source: Security for Business Innovation Council Report — RSA, The Security Division of EMC

Defending Against Advanced & Persistent Threats: The Big Picture

The Big Picture

1. *Evaluation process resulting in the detection of* **risky components** *or* **vulnerabilities** *of the system should be performed.*
2. *In order to mitigate the attack risk;* **proper tools** *should be well-defined and put in the* **proper places**.
3. **Monitoring and Analyzing!!!**
4. **Security Awareness**.

The strategy of using tools providing security should be iteratively determined together with monitoring and periodical analyzing processes.

THE DEFENSE PROCESS MUST ALSO BE ITERATIVE!!!

Defending Against Advanced & Persistent Threats: The Big Picture

The Big Picture

1. *Evaluation process resulting in the detection of* **risky components** *or* **vulnerabilities** *of the system should be performed.*
2. *In order to mitigate the attack risk;* **proper tools** *should be well-defined and put in the* **proper places**.
3. **Monitoring and Analyzing!!!**
4. **Security Awareness**.

The strategy of using tools providing security should be iteratively determined together with monitoring and periodical analyzing processes.

THE DEFENSE PROCESS MUST ALSO BE ITERATIVE!!!

Defending Against Advanced & Persistent Threats: The Big Picture

The Big Picture

1. *Evaluation process resulting in the detection of* **risky components** *or* **vulnerabilities** *of the system should be performed.*
2. *In order to mitigate the attack risk;* **proper tools** *should be well-defined and put in the* **proper places**.
3. **Monitoring and Analyzing!!!**
4. **Security Awareness**.

The strategy of using tools providing security should be iteratively determined together with monitoring and periodical analyzing processes.

THE DEFENSE PROCESS MUST ALSO BE ITERATIVE!!!

Defending Against Advanced & Persistent Threats: The Big Picture

The Big Picture

1. *Evaluation process resulting in the detection of* **risky components** *or* **vulnerabilities** *of the system should be performed.*
2. *In order to mitigate the attack risk;* **proper tools** *should be well-defined and put in the* **proper places**.
3. **Monitoring and Analyzing!!!**
4. **Security Awareness**.

The strategy of using tools providing security should be iteratively determined together with monitoring and periodical analyzing processes.

THE DEFENSE PROCESS MUST ALSO BE ITERATIVE!!!

Defending Against Advanced & Persistent Threats: The Big Picture

The Big Picture

1. *Evaluation process resulting in the detection of* **risky components** *or* **vulnerabilities** *of the system should be performed.*
2. *In order to mitigate the attack risk;* **proper tools** *should be well-defined and put in the* **proper places**.
3. **Monitoring and Analyzing!!!**
4. **Security Awareness**.

The strategy of using tools providing security should be iteratively determined together with monitoring and periodical analyzing processes.

THE DEFENSE PROCESS MUST ALSO BE ITERATIVE!!!

Defending Against Advanced & Persistent Threats: Tools

Tools

The key tools needed are those that **enable logging** *and* **monitoring** *to be carried out, and the ones could* **examine the results** *of such efforts.*

The combination of **three strategies** *given below could define the* **selection of tools** *to be used:*

- *Content Awareness: Since the APT content involving malware is carried over commonly allowed protocols; the solution requires deep content awareness.*
- *Context Awareness: Since the APT is performed by specifically developed codes using a zero-day vulnerability, solution should be capable of identifying it.*
- *Data Sensitivity Awareness: Any organization has to aware of its data level sensitiveness. At least sensitive data should be kept and transferred encrypted. Cryptographic protocols should be involved into the solution.*

Defending Against Advanced & Persistent Threats: Tools

Tools

The key tools needed are those that **enable logging** *and* **monitoring** *to be carried out, and the ones could* **examine the results** *of such efforts. The combination of* **three strategies** *given below could define the* **selection of tools** *to be used:*

- *Content Awareness: Since the APT content involving malware is carried over commonly allowed protocols; the solution requires deep content awareness.*
- *Context Awareness: Since the APT is performed by specifically developed codes using a zero-day vulnerability, solution should be capable of identifying it.*
- *Data Sensitivity Awareness: Any organization has to aware of its data level sensitiveness. At least sensitive data should be kept and transferred encrypted. Cryptographic protocols should be involved into the solution.*

Tools

- *Firewalls* $\Longrightarrow$ **Content Awareness**

  Preferences of firewalls should be set according to specific components of the system to be kept secure.

- *Anti Virus Systems* $\Longrightarrow$ **Content Awareness**
- *Intrusion Detection and Prevention Systems (IDS and IPS)* $\Longrightarrow$ **Context Awareness**

  Each suspicious indicator, caught by IPS, in the context of other indicators should be evaluated to gather enough evidence for the reliable identification of malicious activity.

- *Network Analyzers* $\Longrightarrow$ **Analyzing the network traffic**

Tools

- *Firewalls* $\Longrightarrow$ **Content Awareness**

  Preferences of firewalls should be set according to specific components of the system to be kept secure.

- *Anti Virus Systems* $\Longrightarrow$ **Content Awareness**
- *Intrusion Detection and Prevention Systems (IDS and IPS)* $\Longrightarrow$ **Context Awareness**

  Each suspicious indicator, caught by IPS, in the context of other indicators should be evaluated to gather enough evidence for the reliable identification of malicious activity.

- *Network Analyzers* $\Longrightarrow$ **Analyzing the network traffic**

Defending Against Advanced & Persistent Threats: Tools

Tools

- *Firewalls* $\Longrightarrow$ **Content Awareness**

  Preferences of firewalls should be set according to specific components of the system to be kept secure.

- *Anti Virus Systems* $\Longrightarrow$ **Content Awareness**
- *Intrusion Detection and Prevention Systems (IDS and IPS)* $\Longrightarrow$ **Context Awareness**

  Each suspicious indicator, caught by IPS, in the context of other indicators should be evaluated to gather enough evidence for the reliable identification of malicious activity.

- *Network Analyzers* $\Longrightarrow$ **Analyzing the network traffic**

Defending Against Advanced & Persistent Threats: Tools

Tools

- *Firewalls* $\Longrightarrow$ **Content Awareness**

  Preferences of firewalls should be set according to specific components of the system to be kept secure.

- *Anti Virus Systems* $\Longrightarrow$ **Content Awareness**
- *Intrusion Detection and Prevention Systems (IDS and IPS)* $\Longrightarrow$ **Context Awareness**

  Each suspicious indicator, caught by IPS, in the context of other indicators should be evaluated to gather enough evidence for the reliable identification of malicious activity.

- *Network Analyzers* $\Longrightarrow$ **Analyzing the network traffic**

Defending Against Advanced & Persistent Threats: Tools

Tools

- *Firewalls* $\Longrightarrow$ **Content Awareness**

  Preferences of firewalls should be set according to specific components of the system to be kept secure.

- *Anti Virus Systems* $\Longrightarrow$ **Content Awareness**
- *Intrusion Detection and Prevention Systems (IDS and IPS)* $\Longrightarrow$ **Context Awareness**

  Each suspicious indicator, caught by IPS, in the context of other indicators should be evaluated to gather enough evidence for the reliable identification of malicious activity.

- *Network Analyzers* $\Longrightarrow$ **Analyzing the network traffic**

Tools

- *Firewalls* $\Longrightarrow$ **Content Awareness**

  Preferences of firewalls should be set according to specific components of the system to be kept secure.

- *Anti Virus Systems* $\Longrightarrow$ **Content Awareness**
- *Intrusion Detection and Prevention Systems (IDS and IPS)* $\Longrightarrow$ **Context Awareness**

  Each suspicious indicator, caught by IPS, in the context of other indicators should be evaluated to gather enough evidence for the reliable identification of malicious activity.

- *Network Analyzers* $\Longrightarrow$ **Analyzing the network traffic**

Defending Against Advanced & Persistent Threats: Baselines

Baselines

Baselines of the defense strategy *should be determined by using the* **logs of network traffic** *and* **host activities**. *When any* **anomaly** *is detected; baselines could be redefined within the context of the anomaly in question.*

By this way; **system is kept up to date against strategies that a skilled attacker could use**.

Defending Against Advanced & Persistent Threats: Baselines

Baselines

Baselines of the defense strategy *should be determined by using the* **logs of network traffic** *and* **host activities**. *When any* **anomaly** *is detected; baselines could be redefined within the context of the anomaly in question.*

By this way; **system is kept up to date against strategies that a skilled attacker could use**.

Testing

- *Testing is the most important defensive measure of the APTs to be able to repel them.*
- *Issues that a skilled attacker could use should be taken into account.*
  - *using web scanner tools like NMAP and NESSUS could be insufficient to detect APTs.*
- *Attacker, doubtlessly, try to exploit*
  - *zero-day vulnerabilities*
  - *social engineering and*
  - *client-side attacks*

IT IS WORTHWHILE TO GO THROUGH A VERY EXTENSIVE PENETRATION TEST DONE BY EXTERNAL TESTERS!!!

Testing

- *Testing is the most important defensive measure of the APTs to be able to repel them.*
- *Issues that a skilled attacker could use should be taken into account.*
  - *using web scanner tools like NMAP and NESSUS could be insufficient to detect APTs.*
- *Attacker, doubtlessly, try to exploit*
  - *zero-day vulnerabilities*
  - *social engineering and*
  - *client-side attacks*

IT IS WORTHWHILE TO GO THROUGH A VERY EXTENSIVE PENETRATION TEST DONE BY EXTERNAL TESTERS!!!

Testing

- *Testing is the most important defensive measure of the APTs to be able to repel them.*
- *Issues that a skilled attacker could use should be taken into account.*
  - *using web scanner tools like NMAP and NESSUS could be insufficient to detect APTs.*
- *Attacker, doubtlessly, try to exploit*
  - *zero-day vulnerabilities*
  - *social engineering and*
  - *client-side attacks*

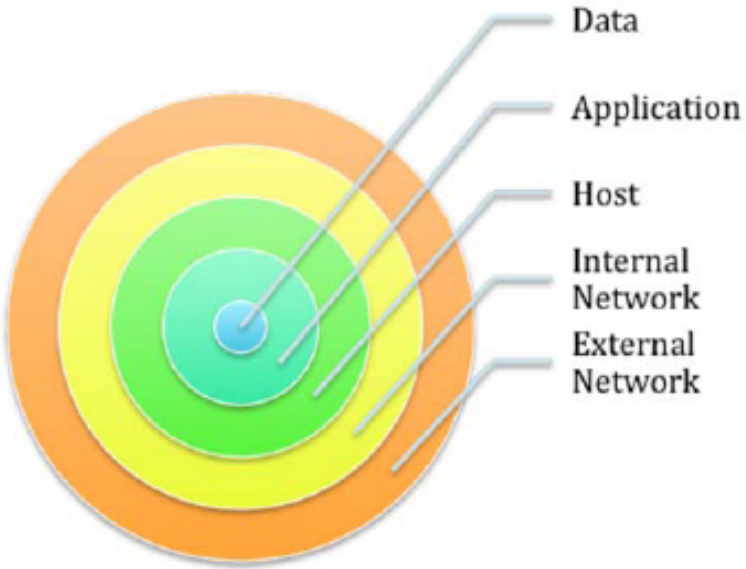
IT IS WORTHWHILE TO GO THROUGH A VERY EXTENSIVE PENETRATION TEST DONE BY EXTERNAL TESTERS!!!

Testing

- *Testing is the most important defensive measure of the APTs to be able to repel them.*
- *Issues that a skilled attacker could use should be taken into account.*
  - *using web scanner tools like NMAP and NESSUS could be insufficient to detect APTs.*
- *Attacker, doubtlessly, try to exploit*
  - *zero-day vulnerabilities*
  - *social engineering and*
  - *client-side attacks*

IT IS WORTHWHILE TO GO THROUGH A VERY EXTENSIVE PENETRATION TEST DONE BY EXTERNAL TESTERS!!!

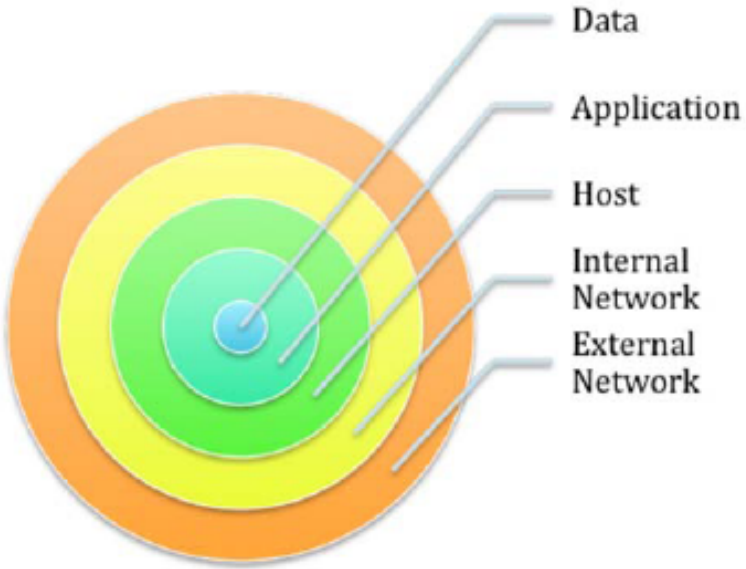
Defending Against Advanced & Persistent Threats: Defense-in-depth



Defense in Depth

1. *Firewalls on the externally-facing portions of networks*
2. *Additional firewalls and IDS/IPS on the internal portions of networks*
3. *Software firewalls and anti-malware tools on hosts*
4. *Access controls and logging on applications*
5. *Encryption on data*

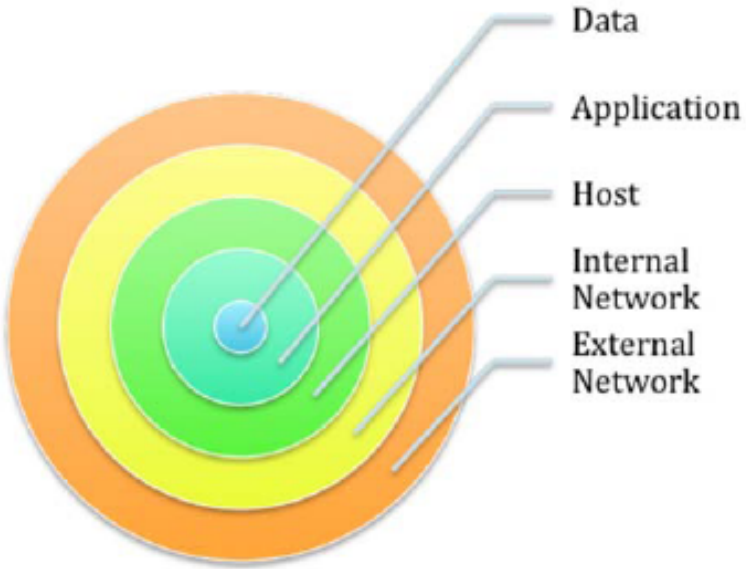
Defending Against Advanced & Persistent Threats: Defense-in-depth



Defense in Depth

1. *Firewalls on the externally-facing portions of networks*
2. *Additional firewalls and IDS/IPS on the internal portions of networks*
3. *Software firewalls and anti-malware tools on hosts*
4. *Access controls and logging on applications*
5. *Encryption on data*

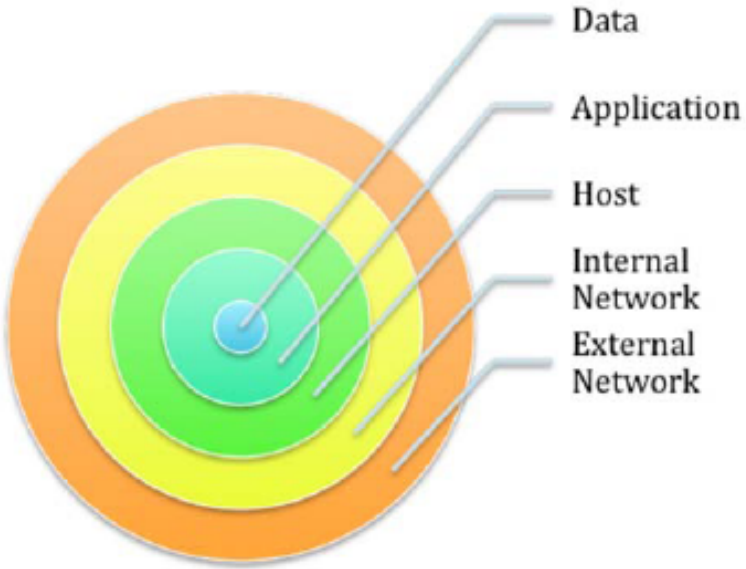
Defending Against Advanced & Persistent Threats: Defense-in-depth



Defense in Depth

1. *Firewalls on the externally-facing portions of networks*
2. *Additional firewalls and IDS/IPS on the internal portions of networks*
3. *Software firewalls and anti-malware tools on hosts*
4. *Access controls and logging on applications*
5. *Encryption on data*

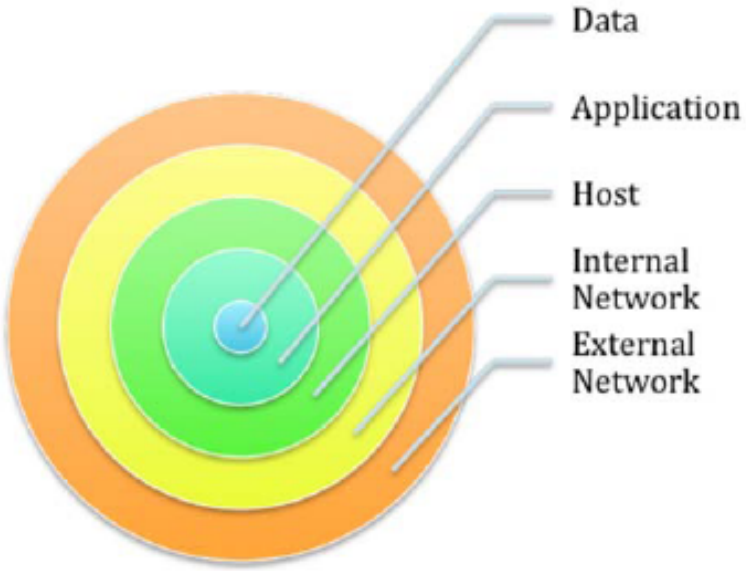
Defending Against Advanced & Persistent Threats: Defense-in-depth



Defense in Depth

1. *Firewalls on the externally-facing portions of networks*
2. *Additional firewalls and IDS/IPS on the internal portions of networks*
3. *Software firewalls and anti-malware tools on hosts*
4. *Access controls and logging on applications*
5. *Encryption on data*

Defending Against Advanced & Persistent Threats: Defense-in-depth



Defense in Depth

1. *Firewalls on the externally-facing portions of networks*
2. *Additional firewalls and IDS/IPS on the internal portions of networks*
3. *Software firewalls and anti-malware tools on hosts*
4. *Access controls and logging on applications*
5. *Encryption on data*

Defending Against Advanced & Persistent Threats: Security Awareness

Security Awareness

In spite of all these defense requirements provided, an attacker could still be succeeded in executing an APT due to the combinational usages of:

- *zero-day vulnerabilities and*
- *social engineering.*

SECURITY AWARENESS MIGHT LESSEN, OR ENTIRELY FOIL APT ATTACKS!!!

So What: The Crucial Points Against an APT

Crucial Points

- *Tools: Focus on logging and monitoring efforts*
- *Baselines: Be aware of what the environment should look like*
- *Testing: Test security measures like an attacker*
- *Defense-in-Depth: Close up the gaps*
- *Security Awareness: Foster the security mindset*

So What: The Crucial Points Against an APT

Crucial Points

- *Tools: Focus on logging and monitoring efforts*
- *Baselines: Be aware of what the environment should look like*
- *Testing: Test security measures like an attacker*
- *Defense-in-Depth: Close up the gaps*
- *Security Awareness: Foster the security mindset*

So What: The Crucial Points Against an APT

Crucial Points

- *Tools: Focus on logging and monitoring efforts*
- *Baselines: Be aware of what the environment should look like*
- *Testing: Test security measures like an attacker*
- *Defense-in-Depth: Close up the gaps*
- *Security Awareness: Foster the security mindset*

So What: The Crucial Points Against an APT

Crucial Points

- *Tools: Focus on logging and monitoring efforts*
- *Baselines: Be aware of what the environment should look like*
- *Testing: Test security measures like an attacker*
- *Defense-in-Depth: Close up the gaps*
- *Security Awareness: Foster the security mindset*

So What: The Crucial Points Against an APT

Crucial Points

- *Tools: Focus on logging and monitoring efforts*
- *Baselines: Be aware of what the environment should look like*
- *Testing: Test security measures like an attacker*
- *Defense-in-Depth: Close up the gaps*
- *Security Awareness: Foster the security mindset*

Defense Strategies Against APTs vs Conventional Threats

	CONVENTIONAL APPROACH	ADVANCED APPROACH
CONTROLS COVERAGE	Protect all information assets	Focus protection efforts on most important assets ("crown jewels")
CONTROLS FOCUS	Preventive controls (AV, firewall)	Detective controls (monitoring, data analytics)
PERSPECTIVE	Perimeter-based	Data-centric
GOAL OF LOGGING	Compliance reporting	Threat detection
INCIDENT MANAGEMENT	Piecemeal: find and neutralize malware or infected nodes	Big picture: find and dissect attack patterns
THREAT INTELLIGENCE	Collect information on malware	Develop deep understanding of attackers' current targets and modus operandi and your own organization's key assets and IT environment
SUCCESS DEFINED BY	No attackers get into the network	Attackers sometimes get in, but are detected as early as possible and impact is minimized

Source: Security for Business Innovation Council Report — RSA, The Security Division of EMC

Risk Mitigating Use Cases by McAfee

Incident 1: Theft

1. *Scenario: Stealing the intellectual property of a biotech company. Attacker recruits a trusted employee who has legitimate access to the desired material.*

Risk Mitigating Use Cases by McAfee

Incident 1: Theft

2. *Attack: The malicious insider uses his/her legitimate access to get raw or processed data from the servers or the databases of the company in question. The idea is to amass as much as possible data to his/her workstation then dump the data into a physical media to remove it outside of the company.*

Risk Mitigating Use Cases by McAfee

Incident 1: Theft

3. *Mitigation: In this case; risk mitigation strategy is to monitor the interactions of users with sensitive data. If any anomaly is captured such as* **users downloading excessive amounts of information in a short time period, accessing information at unusual times, or accessing high-value information of multiple types from too many different sources***; then flags could be raised.*

Risk Mitigating Use Cases by McAfee

Incident 2: Surveillance

1. *Scenario: A nation-state is trying to get information about the troop movements of a country with which it is currently having a debate.*

Risk Mitigating Use Cases by McAfee

Incident 2: Surveillance

2. *Attack: The attackers design a malware infrastructure that are able to log keystrokes, monitor network traffic, and take screen shots while periodically encrypting and sending the information to a centralized collection site. The attackers want to use the botnets for spear phishing targeting specific military personal and convince them into opening up an "image file" that is really an executable that will ultimately be downloaded and install the entirety of the malware.*

Risk Mitigating Use Cases by McAfee

Incident 2: Surveillance

3. *Mitigation: In this case; risk mitigation strategy depends mostly on having an* **Global Threat Intelligence** *that is aware of the* **tracking malicious IPs, domains, geographies, activities, and patterns, and generating real-time information** *about these threats to prevent phishing emails and instant messaging.*

Risk Mitigating Use Cases by McAfee

Incident 3: Sabotage

1. *Scenario: A terrorist organization is targeting the electric power grid of a country with contrary political beliefs. The terrorists' goal is to cause long-term blackouts in major cities.*

Risk Mitigating Use Cases by McAfee

Incident 3: Sabotage

2. *Attack: The terrorist group has created purpose-built malware designed to target and take over PLCs, which are responsible for managing critical areas within the electric power grid, by exploiting a zero-day vulnerability.*

Risk Mitigating Use Cases by McAfee

Incident 3: Sabotage

3. *Mitigation: The risk mitigating strategy in this case involves using* **dynamic white-listing**, *that is centrally managed without any network access, to register the privileged users that could execute programs over PLCs.*

Summary

Summarization

1. *Comparison of the traditional attack with APTs.*
2. *APTs in detail:*
   - *Characteristics*
   - *Execution Phases*
   - *An Imagination: Kinetic Warfare*
   - *General Defense Strategies against APTs*
3. *Some Risk Mitigating Cases Provided by McAfee*

Summary

Summarization

1. *Comparison of the traditional attack with APTs.*
2. *APTs in detail:*
   - *Characteristics*
   - *Execution Phases*
   - *An Imagination: Kinetic Warfare*
   - *General Defense Strategies against APTs*
3. *Some Risk Mitigating Cases Provided by McAfee*

Summary

Summarization

1. *Comparison of the traditional attack with APTs.*
2. *APTs in detail:*
   - *Characteristics*
   - *Execution Phases*
   - *An Imagination: Kinetic Warfare*
   - *General Defense Strategies against APTs*
3. *Some Risk Mitigating Cases Provided by McAfee*

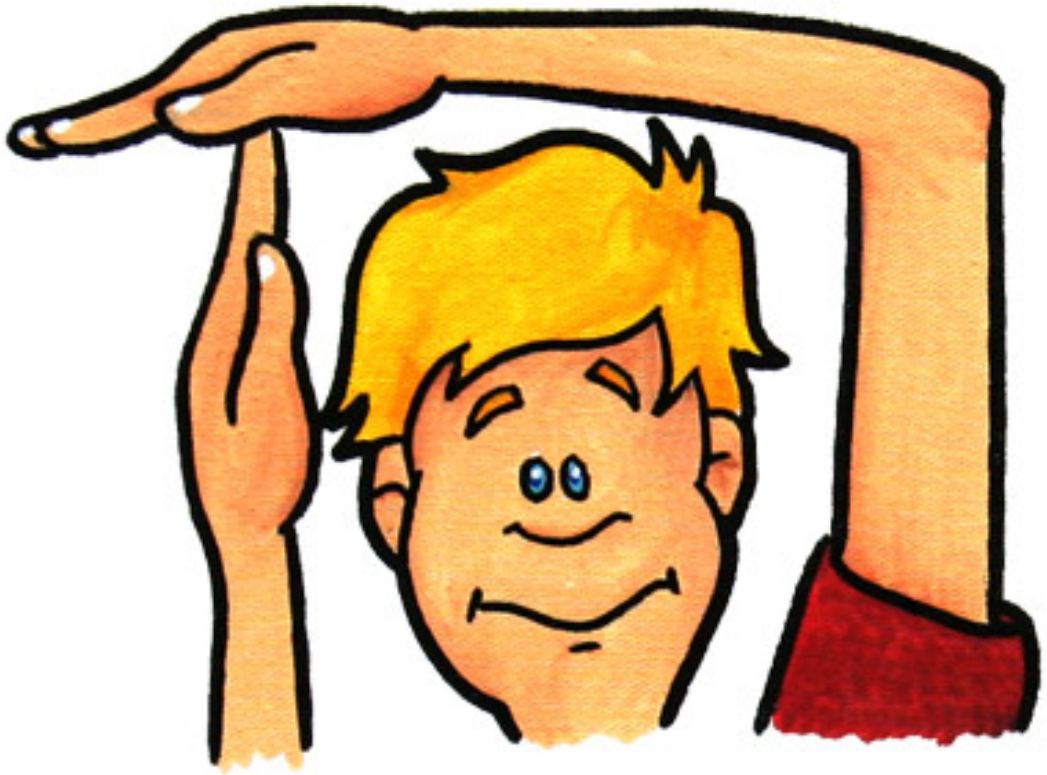
What is next?

Next Session

Well-known APTs performed against trade companies and critical infrastructures

- *Operation Aurora*
- *Stuxnet*
- *...*

Let's Have a Break!!!



Bibliography

[Websense2011] Websense
ADVANCED PERSISTENT THREATS AND OTHER ADVANCED ATTACKS.
THREAT ANALYSIS AND DEFENSE STRATEGIES FOR SMB, MID-SIZE, AND ENTERPRISE ORGANIZATIONS.

[Golshan2010] Ali Golshan
Advanced Persistent Threats
PRICEWATERHOUSECOOPERS.

[McAfeeSolutionBriefs]
Advanced Persistent Threats
Fight large-scale threats with unified solutions and advanced intelligence from McAfee.

Bibliography

[Ruf2011] Lukas Ruf
Advanced Persistent Threat
Information Security Society - Switzerland.

[Andress2011] Jason Andress
Advanced Persistent Threat: Attacker Sophistication Continues to Grow?
ISSA Journal, June 2011.