APT 공격과 대응책

김용철
관제솔루션팀장
ychkim@sk.com

에스케이인포섹(주)

[목차]

1. APT 특성

Advanced Persistent Threat

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

nteraction
Help
About Wikipedia
Community portal
Recent changes
Contact page

ools
What links here
Related changes
Upload file
Special pages
Permanent link

Article Talk Read Edit View history Search

Advanced persistent threat

From Wikipedia, the free encyclopedia

An **advanced persistent threat** (**APT**) is a set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity. An APT usually targets organizations and/or nations for business or political motives. APT processes require a high degree of covertness over a long period of time. The "advanced" process signifies sophisticated techniques using malware to exploit vulnerabilities in systems. The "persistent" process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The "threat" process indicates human involvement in orchestrating the attack.[1]

APT usually refers to a group, such as a government, with both the capability and the intent to target, persistently and effectively, a specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information,[2] but applies equally to other threats such as that of traditional espionage or attacks.[3] Other recognized attack vectors include infected media, supply chain compromise, and social engineering. The purpose of these attacks is to place custom malicious code on one or multiple computers for specific tasks and to remain undetected for the longest possible period. Knowing the attacker artifacts, such as file names, can help a professional make a network-wide search to gather all affected systems.[4] Individuals, such as an individual hacker, are not usually referred to as an APT, as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target.[5]

키워드 / 특성

- ❑ A specific entity
- ❑ Persistent, a long-term, remain undetected
- ❑ To exfiltrate sensitive infor.
- ❑ Social Engineering
- ❑ in 2005, in 2006
- ❑ Deep log analysis and log Collection from various sour.

2. APT 또 다른 시각

키워드 / 특성

- ❑ A specific entity
- ❑ Persistent, a long-term, remain undetected
- ❑ To exfiltrate sensitive infor.
- ❑ Social Engineering
- ❑ in 2005, in 2006
- ❑ Deep log analysis and log Collection from various sour.

시사점

- ❑ APT 공격, 기존 보안 체계로 막을 수 있다.
- ❑ APT는 사람에 대한 공격이다.
- ❑ APT는 전혀 새로운 공격이 아니다.
- ❑ 무조건적인 사전 탐지보다는 다양한 정보원을 통한 사후 탐지가 효과적일 수 있다.

3. 효과적인 APT 대응 방안

Mind Set

100% 방어 "No"	▪ 공격 방식은 수 만가지… 방어 기술은 제한적, 공격 기술보다 늦게 개발(Zero Day) : 경영자 인식 ▪ 단지 가능성을 낮추는 것… ROI 고려, 지속적 투자, 신속 대응으로 피해 최소화 ▪ 이상 징후 포착을 위한 사전 활동… 지속적인 관제/Cert, 다양한 보안 센서 통합 View
사람에 대한 공격	▪ 현실성 있는 보안 정책… '울타리'가 있으면 80~90%는 넘지 않는다. ▪ 교육이 가장 효과적… 지속적인 보안 교육과 연습이 최선의 사전 대책 ▪ 업무 편의? 예의 정책? … 스스로 Gate을 열어 주는 것은 아닌지?
기존 보안체계 효과적 활용	▪ 방화벽/I·DPS/WAF and so on + 정책… 책임 회피용인가? 실전용인가? ▪ 이상 징후를 인지할 능력… 관제/Cert/Forensic ? 없다면 도움이라도 받는 것이… ▪ 효율성 향상을 위해 전문 시스템 도입 검토도 필요.
사전 탐지?	▪ 100% 방어가 불가능하다면… 사전 탐지와 더불어 잠복기에라도 탐지하면 되지… (Unknown ?) ▪ 침투 성공 후 탐지가 더욱 효과적일 수 있다… 어떤 공격일지 모르는 상태 vs 침투한 공격 인지 ▪ 피해 최소화도 한 가지 전략 ! … 공격 당했더라도 최대한 빨리 탐지 및 신속한 조치
공격 성공 후 대책	▪ 공격 성공에 따라 자료가 유출되었다… 그런데 공격자가 유출한 자료를 활용 할 수가 없다… ▪ 피해 최소화도 한 가지 전략 ! … 공격 당했더라도 최대한 빨리 탐지 및 신속한 조치

4. 주의사항

눈 뜬 봉사로 만드는 마케팅

❑ Unknown Attack 탐지

- 알려지지 않았는데 어떻게 탐지?
- 소 뒷걸음 치다 쥐 잡았다.
  소가 뒷걸음만 치면 쥐를 잡을 수 있나?

❑ 만능 솔루션

- 인터넷 침투 + 암호화 트래픽 + e-mail + 매체 + 사람
  ➔ 원하는 수준만큼 잘 되는 것이 하나도 없을 수도…

❑ 정탐 높고, 오탐 낮고, 미탐 없고…

- AlphaGo 인가?

❑ 100% 탐지

- 보안 회사인지 해커 조력자 인지…

정보 유출 vs APT 대응

▲바 에 올라와 있는 문서 캡쳐화면(22일 본지 입수) ※ 보안뉴스(2015/4)

보안 교육, 어떻게?

- ❑ 정기적/수준별/직관적… 오프 교육
- ❑ e-learning 등 동영상을 통한 온라인 교육
- ❑ **모의 훈련**
- ❑ **실제 탐지 내역을 사용자가 직접 확인**

5. 우선순위

【 APT 주요 침투 경로 】

Internet Malware Infections

- Drive-by Download
- e-Mail Attachment
- File Sharing
- Pirated software & keygen
- Spear Phishing
- DNS & routing Mods

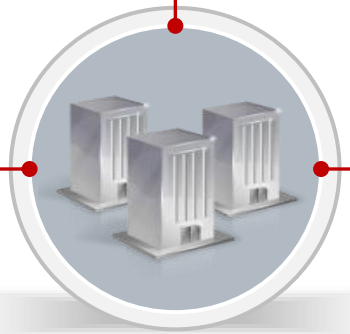
External Exploitation

- Professional Hacking
- Mass vulnerability exploit
- Co-location Host Exploitation
- Cloud provider penetration
- Rogue WiFi penetration
- SmartPhone Bridging

Physical Malware Infections

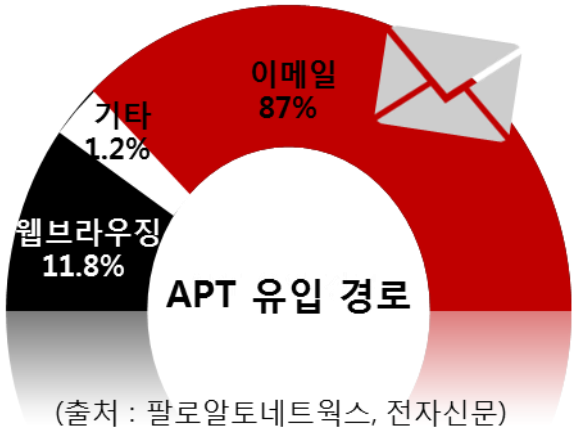
- Infected USB Memory Stick
- Infected CD's & DVD's
- Infected memory card
- Infected appliances
- Backdoor IT equipment

Internet(N/W) 영역



Physical(매체) 영역

출처 : 2010, Damballa



(출처 : 팔로알토네트웍스, 전자신문)

시사점

시사점

- ❑ ROI 고려
- ❑ 단위 보안 센서 및 통합 분석 툴 활용
- ❑ Physical 영역과 같은 수준으로

Security

...is a good biz **supporter**...

...Not a **disrupter**.

감사합니다.

에스케이인포섹(주)