APT(Advanced Persistent Threat) 공격의 현재와 대응 방안

2014. 07. 03

장 영 준 책임
Senior Security Engineer, CISSP, CHFI
yj0819.chang@samsung.com, zhang_95@hotmail.com
㈜ 삼성전자, 시스템기술팀, 정보전략그룹

Contents

Contents

02 주요 APT(Advanced Persistent Threat) 공격 사례

1) 농협 침해사고
2) SK 커뮤니케이션즈 침해사고
3) 이란 원자력 발전소의 Stuxnet 감염
4) Google 침해사고
5) EMC/RSA 침해사고
6) 시리아 정부 관련 악성코드 유포
7) 2013년 주요 APT(Advanced Persistent Threat) 공격 사례

Contents

03 APT(Advanced Persistent Threat) 공격 형태의 특징

1) APT(Advanced Persistent Threat) 공격 형태의 증가

2) APT(Advanced Persistent Threat) 공격 대상의 확장

3) 고도화된 사회 공학 기법(Social Engineering) 개발과 적용

4) 악성코드 및 취약점 관련 기술의 발전

5) APT(Advanced Persistent Threat) 공격 기법의 다변화

Contents

04 APT(Advanced Persistent Threat) 공격 대응 방안

1) APT(Advanced Persistent Threat) 공격 Lifecycle

2) APT(Advanced Persistent Threat) 공격 Timeline

3) APT(Advanced Persistent Threat) 통합 대응 전략

4) APT(Advanced Persistent Threat) 공격 예방적 System Hardening

5) APT(Advanced Persistent Threat) 공격 탐지적 Network Control

01 APT(Advanced Persistent Threat)

1) APT (Advanced Persistent Threat)

- APT는 2006년 무렵 미국 공군 사령부에서 사용하였던 군사 통신 용어
- 미국 공군 사령부에서는 미국 국방부와 통신시 확인된 특정 보안 위협 형태를 지칭
- 2010년 무렵 APT라는 용어가 민간 부분으로 전달 되며 의미가 확장
- 현재 민간 부분에서는 일반적으로 APT를 다음과 같이 정의

“다양한 보안 위협들을 양산하여 특정 대상에게 지속적으로 가하는 일련의 행위”

미국 공군사령부와 미국 국방부 문장

2) 과거APT(Advanced Persistent Threat) 공격사례

- 2004년 6월 국내 정부 및 민간 기관들을 대상으로 PeepViewer 트로이목마 유포
- 국정원에서는 "**6개 공공기관의 PC 64대와 민간 분야 PC 52대 감염**" 보고
- 이메일의 첨부 파일로 "**워크샵 내용과 일정.MDB**" 전송 후 악성코드 감염 시도
- 정부 및 민간 기관을 대상으로 정부 기밀 탈취 목적의 APT 공격 사례

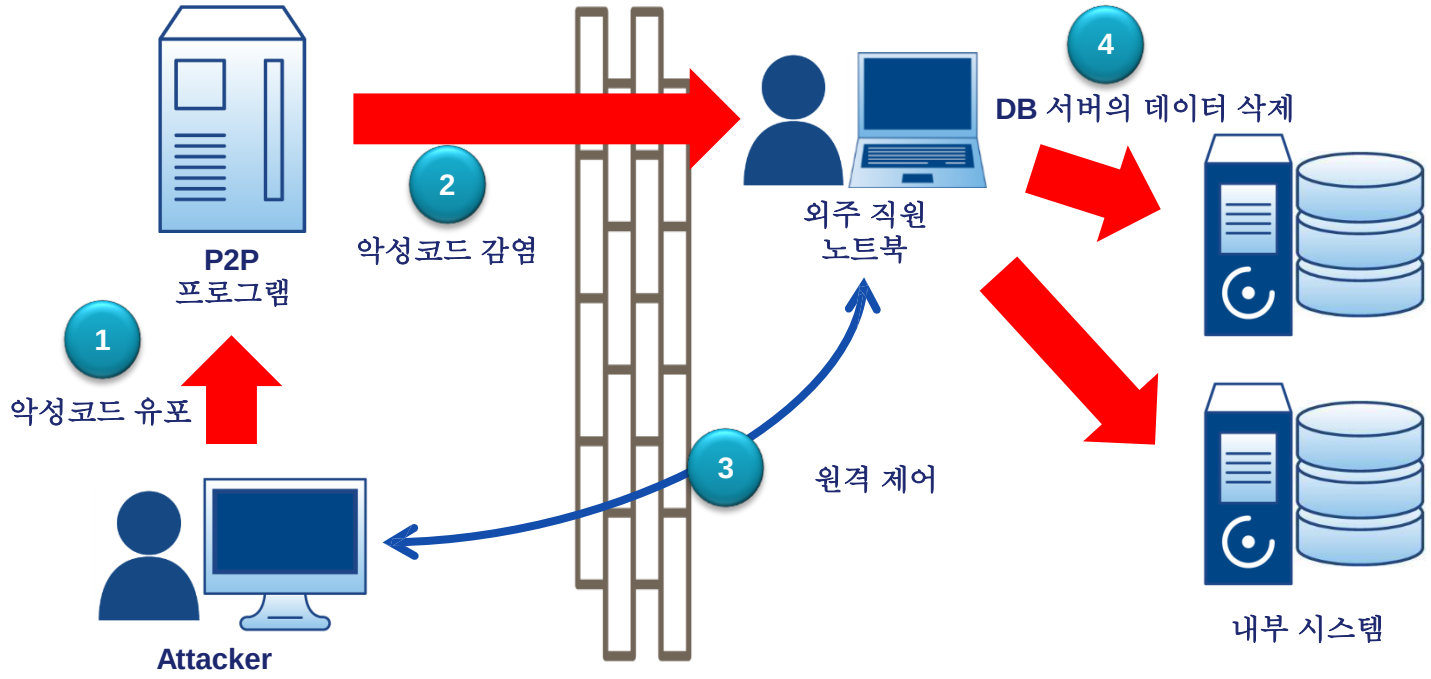
Process	Protocol	Local Address	Remote Address	State
[System Process]:0	TCP	192.168.24.128:1035	192.168.24.1:139	TIME_WAIT
alg.exe:1748	TCP	127.0.0.1:1029	0.0.0.0:0	LISTENING
lsass.exe:756	UDP	0.0.0.0:500	*:*	
lsass.exe:756	UDP	0.0.0.0:4500	*:*	
secura.exe:2416	TCP	192.168.24.128:1052	203. 200:80	SYN_SENT
svchost.exe:1100	UDP	192.168.24.128:123	*:*	
svchost.exe:1100	UDP	127.0.0.1:123	*:*	
svchost.exe:1144	UDP	0.0.0.0:1025	*:*	
svchost.exe:1252	UDP	192.168.24.128:1900	*:*	
svchost.exe:1252	UDP	127.0.0.1:1900	*:*	
System:4	TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
System:4	TCP	192.168.24.128:139	0.0.0.0:0	LISTENING
System:4	UDP	192.168.24.128:137	*:*	
System:4	UDP	192.168.24.128:138	*:*	
System:4	UDP	0.0.0.0:445	*:*	

PeepViewer 트로이목마의 리버스 커넥션 동작

02 주요APT(Advanced Persistent Threat) 공격 사례

1) 농협 전산망마비사고

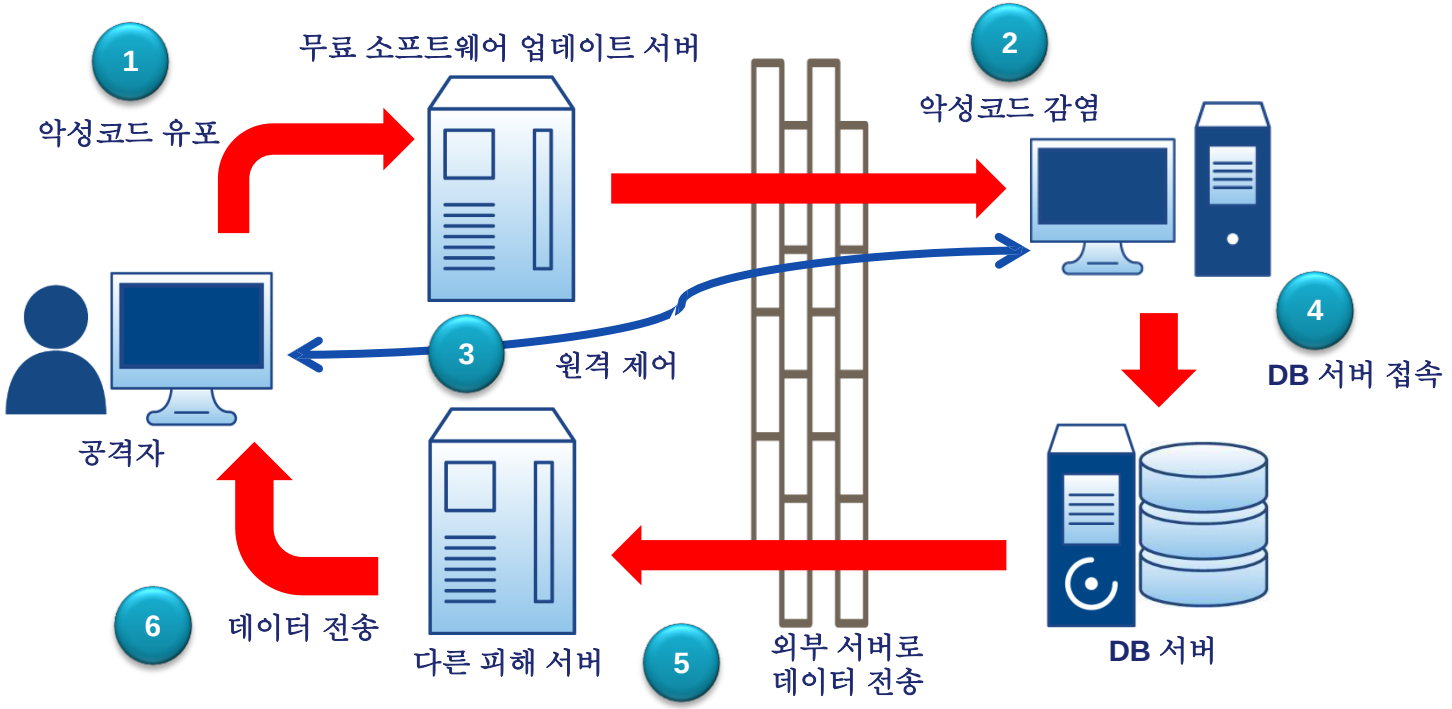
- 2011년 4월 농협 전산망이 외부 공격으로 인한 시스템 손상으로 모든 업무 마비
- 외주 직원 노트북에 감염된 악성코드를 이용해 내부 시스템 침입
- 공격자는 P2P 프로그램으로 악성코드 유포 이후 7개월 동안 감시 후 공격 진행



농협에서 발생한 침해 사고

2) SK 커뮤니케이션즈 침해사고

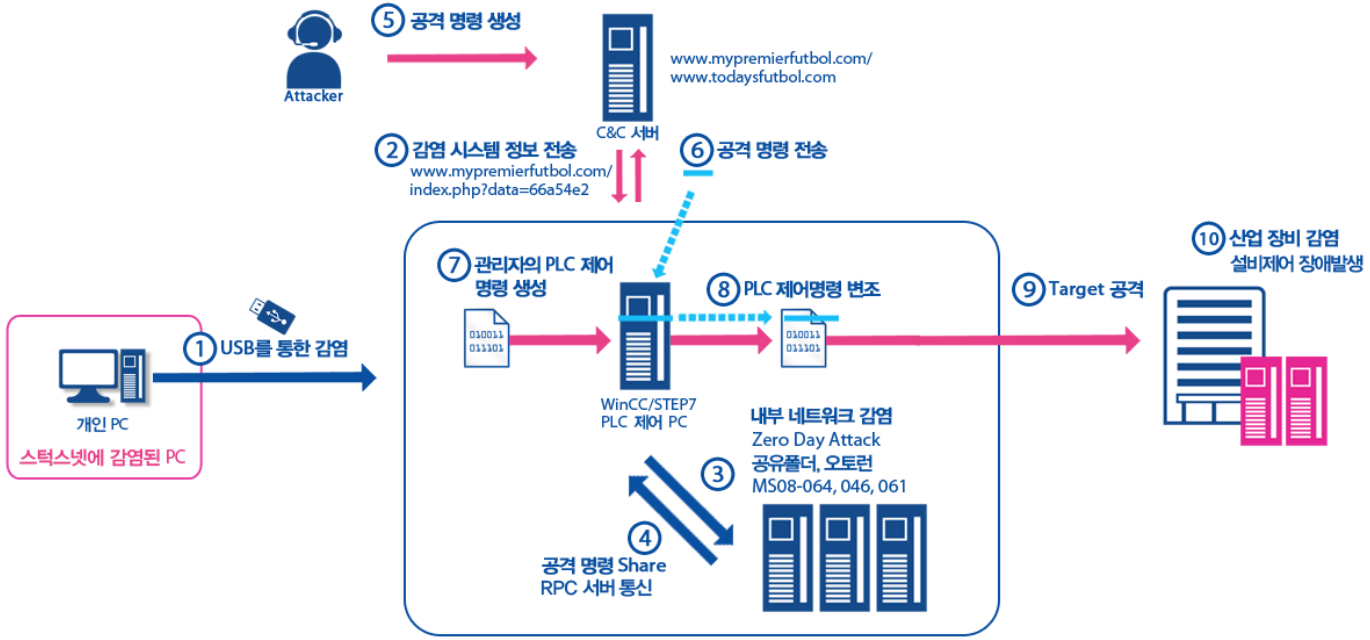
- 2011년 7월 SK 커뮤니케이션즈 침해 사고로 3500만 명 고객 개인 정보 유출
- 무료 소프트웨어 업데이트 서버 해킹 후 정상 파일을 악성코드로 변경 후 유포
- 공격자는 8일만에 DB 관리자 권한 획득 후 DB 데이터를 분할 압축 후 외부 유출



SK 커뮤니케이션즈에서 발생한 침해사고

3) 이란원자력 발전소 Stuxnet 감염

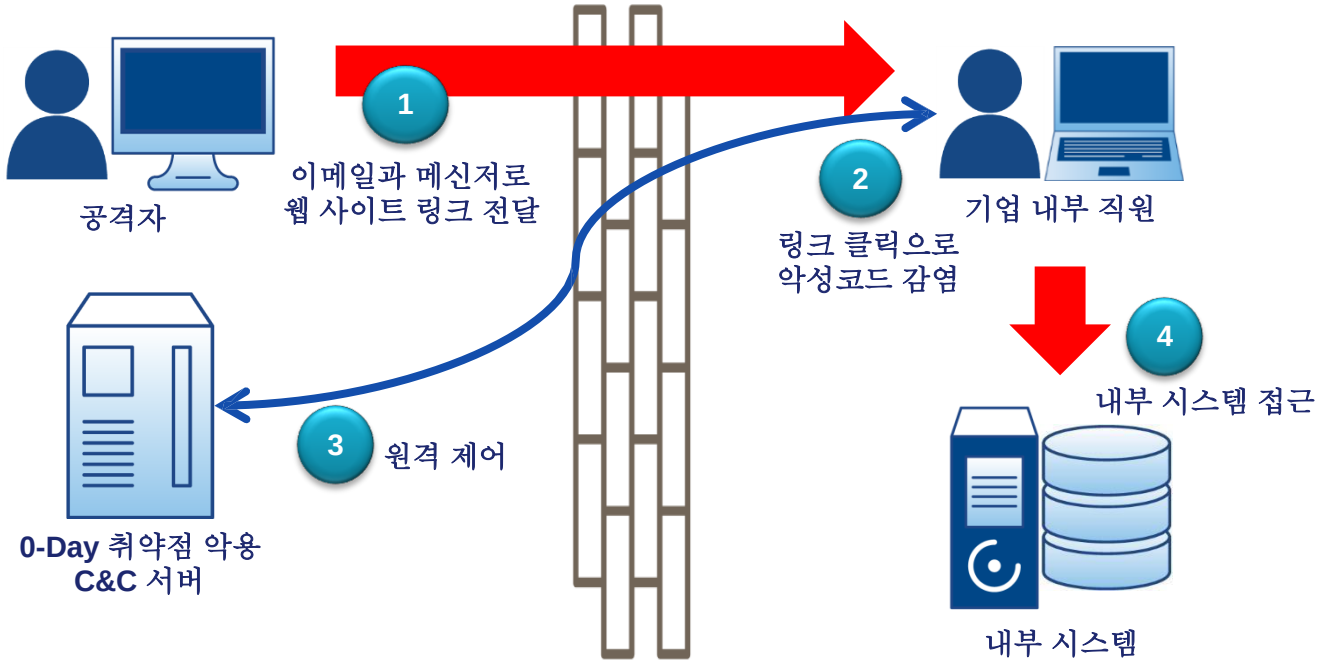
- 2010년 7월 이란 원자력 발전소 시스템 파괴 목적의 Stuxnet 발견
- MS 윈도우의 알려진 취약점 3개와 0-Day 취약점 2개를 악용해 유포
- 2011년 발견된 Duqu와 2012년 발견된 Flame 모두 이란 원자력 발전소 관련 정보 수집 목적으로 유포



스턱스넷 악성코드의 감염과 동작 원리

4) 오퍼레이션 오로라(Operation Aurora) 침해사고

- 2011년 1월 Google 기업 기밀 정보 탈취 목적의 침해 사고 발생
- 해당 침해 사고는 Google 외에 첨단 IT 기업 34개도 공격의 대상
- 공격은 Microsoft Internet Explorer의 0-Day 취약점 악용
- 이메일과 메신저로 악의적인 웹 사이트로 접속하는 링크 전달



첨단IT 기업 대상Operation Aurora 침해사고

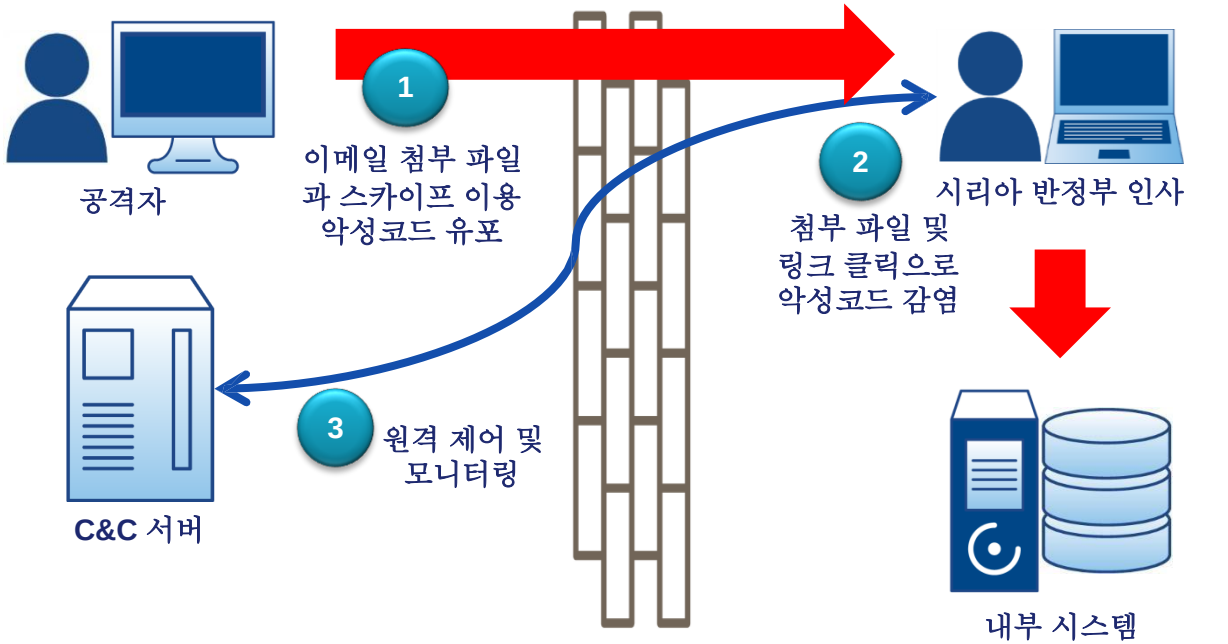
5) EMC/RSA 침해사고

- 2011년 3월 EMC/RSA의 OTP(One Time Password) 관련 기업 기밀 정보 탈취 시도
- 공격 대상 선정을 위해 Social Network로 내부 직원 개인 정보 확보
- 이메일 첨부 파일은 Adobe Flash 0-Day 취약점 악용
- 사회 공학 기법(Social Engineering)으로 내부 직원의 악성코드 감염 유도

EMC/RSA에서 발생한 침해 사고

6) 시리아정부관련악성코드유포

- 2012년 2월 CNN은 시리아 정부가 반정부 인사 감시를 위한 악성코드 유포를 폭로
- 이메일 첨부 파일, 허위 YouTube 페이지 그리고 Skype로 악성코드 유포
- 언더그라운드에 공개된 DarkComet RAT 악성코드 생성기로 악성코드 제작
- 감염 PC의 국가별 분포는 시리아, 이스라엘, 사우디 아라비아와 레바논이 다수



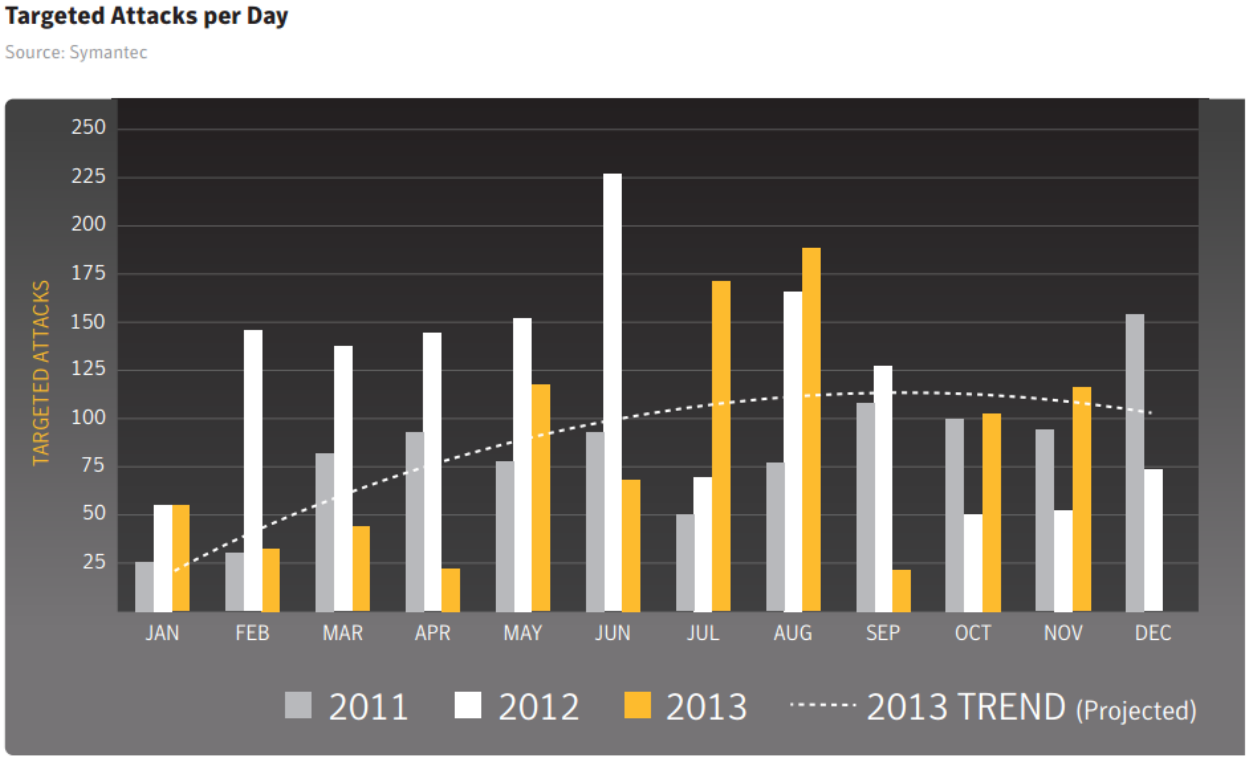
시리아 정부의 반정부 인사 감시를 위한 악성코드 유포

7) 2013년 주요APT(Advanced Persistent Threat) 공격사례

03 APT(Advanced Persistent Threat)
공격 형태의 특징

1) APT(Advanced Persistent Threat) 공격 형태의 증가

- 인터넷과 컴퓨터의 발달로 정부 기관 및 각 기업체에서 업무 자동화 시스템 도입
- 모든 업무 및 기밀 문서 역시 전자 문서와 같은 데이터 형태로 파일 서버에 보관
- 공격 목적의 다양화로 APT 형태의 Targeted Attack이 과거에 비해 증가



Symantec에서 공개한 Targeted Attack 증가수치

2) APT(Advanced Persistent Threat) 공격 대상의 확장(1)

- ❖ 공격 목적이 과거에 비해 확대 됨으로 공격 대상 역시 확대
- ❖ 과거 정부 및 군사 기관만이 공격 대상 이었으나 현재는 민간 기업으로까지 확대

2) APT(Advanced Persistent Threat) 공격 대상의 확장(2)

- 경제적 고부가 데이터를 보유한 첨단 기업들이 주요 대상
- 한국과 일본은 금융 기관, 언론사 및 온라인 게임 업종 기업 등이 주요 대상

Top 10 Industries Attacked

Source: Symantec

Industry	Percent
Services - Professional	20.3%
Services - Non Traditional	18.8%
Public Administration	15.3%
Finance, insurance & Real Estate	13.2%
Manufacturing	10.3%
Transportation, communications, electric, gas & Sanitary Services	8.0%
Wholesale	5.0%
Retail	2.3%
Nonclassifiable Establishments	2.0%
Logistics	1.9%

Attacks by Size of Targeted Organization

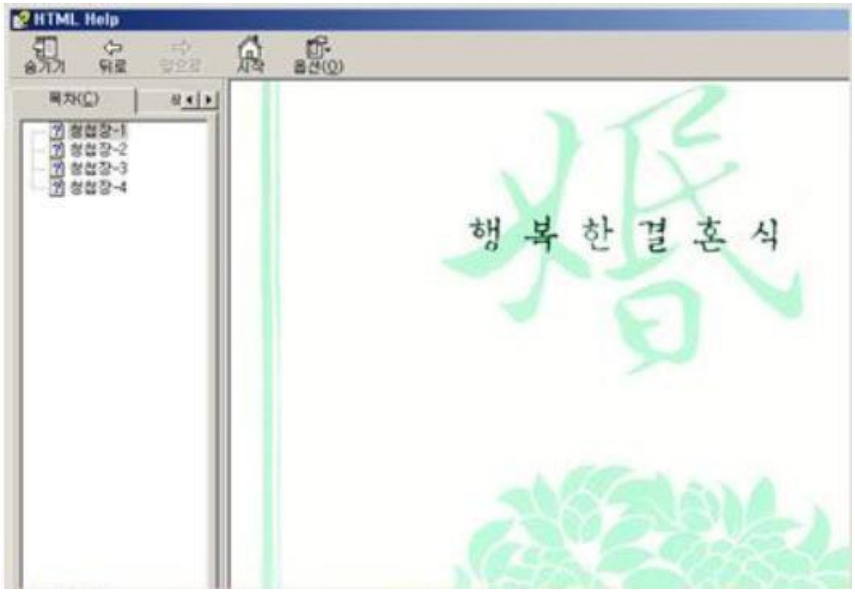
Source: Symantec

Company Size	Percent
1-250	29.6%
251-500	10.8%
501-1000	9.5%
1001-1500	3.2%
1501-2500	7.9%
2500+	39.0%

Symantec에서 공개한2013년 Targeted Attack 발생산업군 및 기업규모

3) 고도화된 사회 공학기법(Social Engineering) 개발과 적용

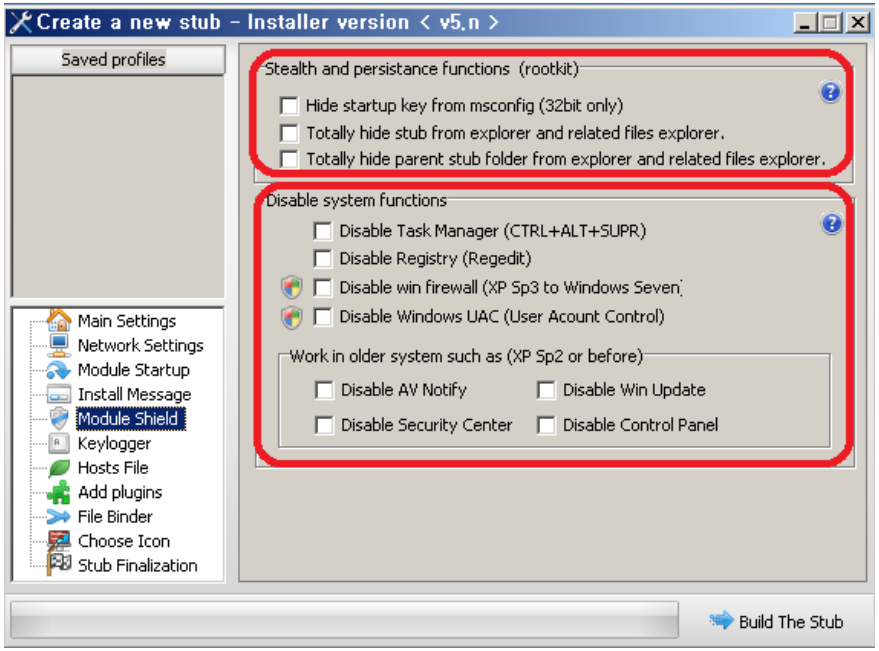
- Web과 Social Network 발달은 공격 대상의 개인 정보 수집 용이
- 수집한 개인 정보들로 공격 대상에게 최적화된 사회 공학 기법(Social Engineering) 개발 및 적용
- EMC/RSA 침해 사고의 경우 내부 직원들에게 채용 정보 관련 메일로 위장



청첩장과 입사 지원서로 위장한 취약한 전자문서 파일들

4) 악성코드 및 취약점 관련 기술의 발전

- 악성코드 제작 및 취약점 개발 기술들의 발전은 보안 제품 탐지 우회와 APT 공격의 성공률을 높이는데 기여
- 악성코드는 Self-Update, 보안 제품 무력화 등 다수의 개별 기능을 가진 파일들의 조합
- 취약점은 다양한 일반 소프트웨어의 알려진 취약점 또는 0-Day 취약점들을 악용

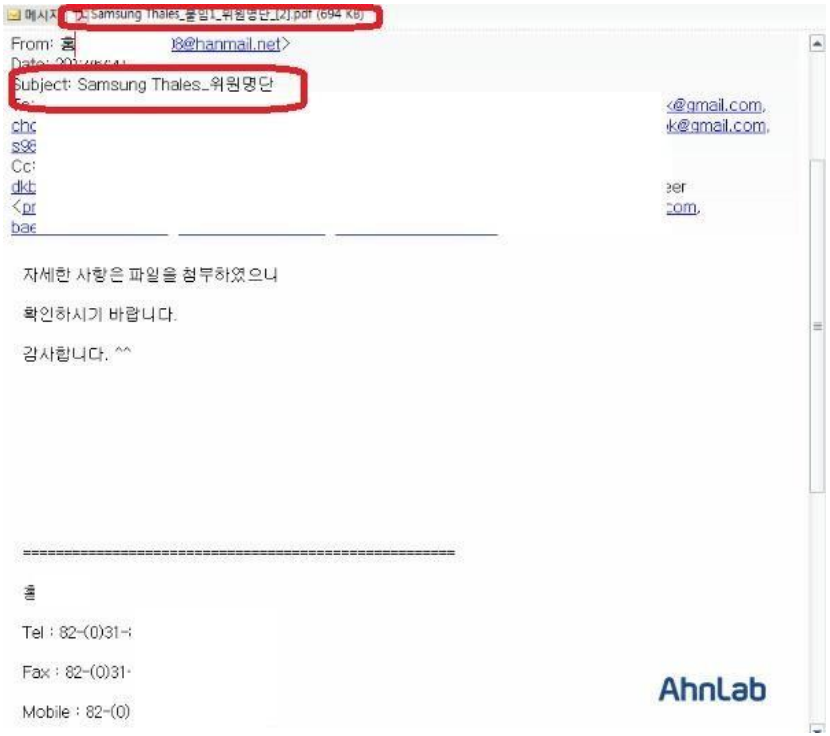


DarkComet RAT의 보안 기능 무력화 옵션

MS10-087 워드 취약점 악성코드 생성기

5) APT(Advanced Persistent Threat) 공격 기법의 다변화

- ❖ 현재까지 APT 공격의 주요 공격 기법은 이메일의 첨부 파일을 이용하는 형태
- ❖ 과거 첨부 파일이 실행 가능한 파일이었으나 최근에는 전자문서 형태로 변경
- ❖ 한국의 경우 무료 소프트웨어의 자동 업데이트 기능과 한국산 P2P 프로그램 악용

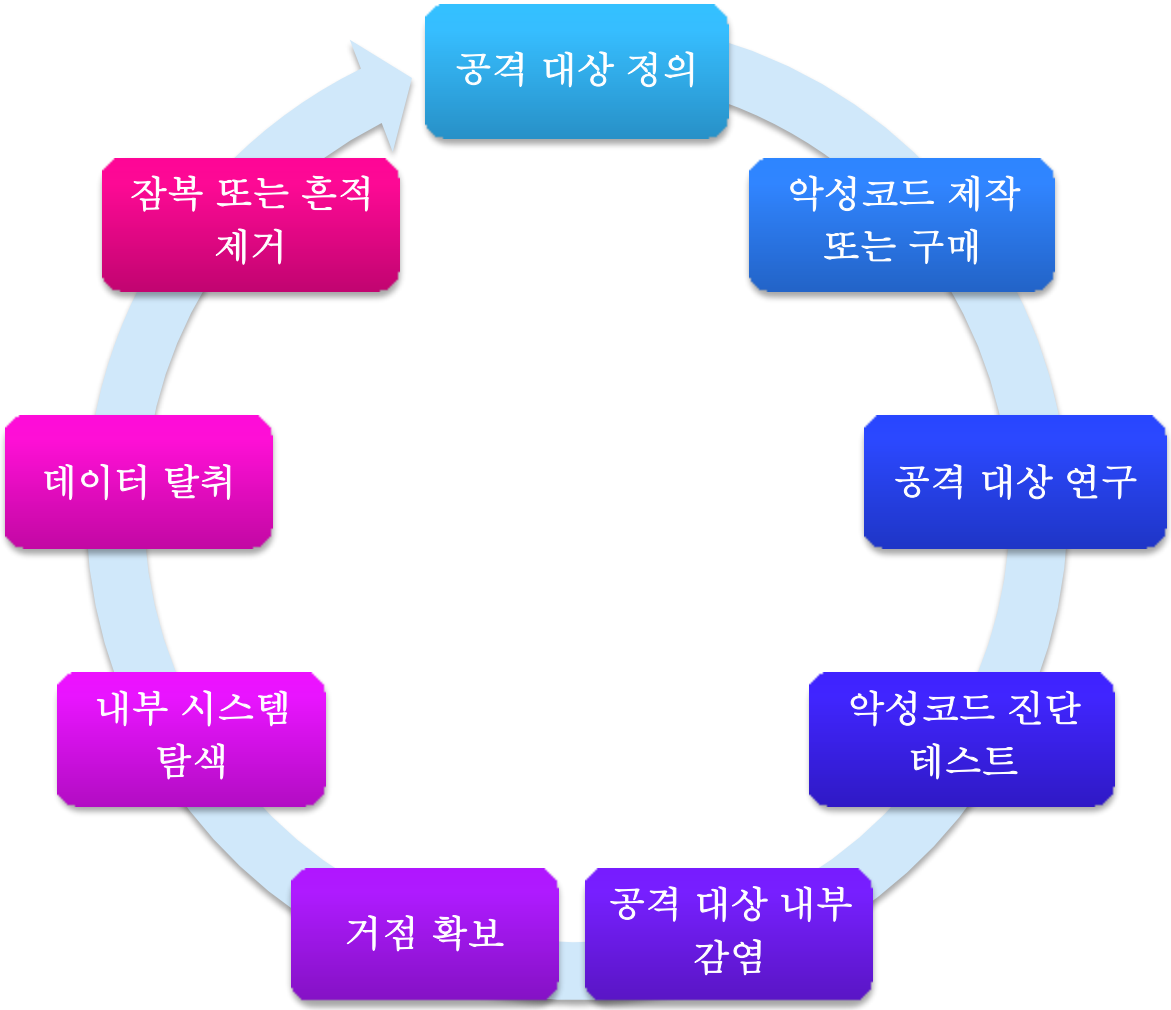


취약한PDF 파일이 첨부된 이메일

취약한 한글(HWP) 파일이 첨부된 이메일

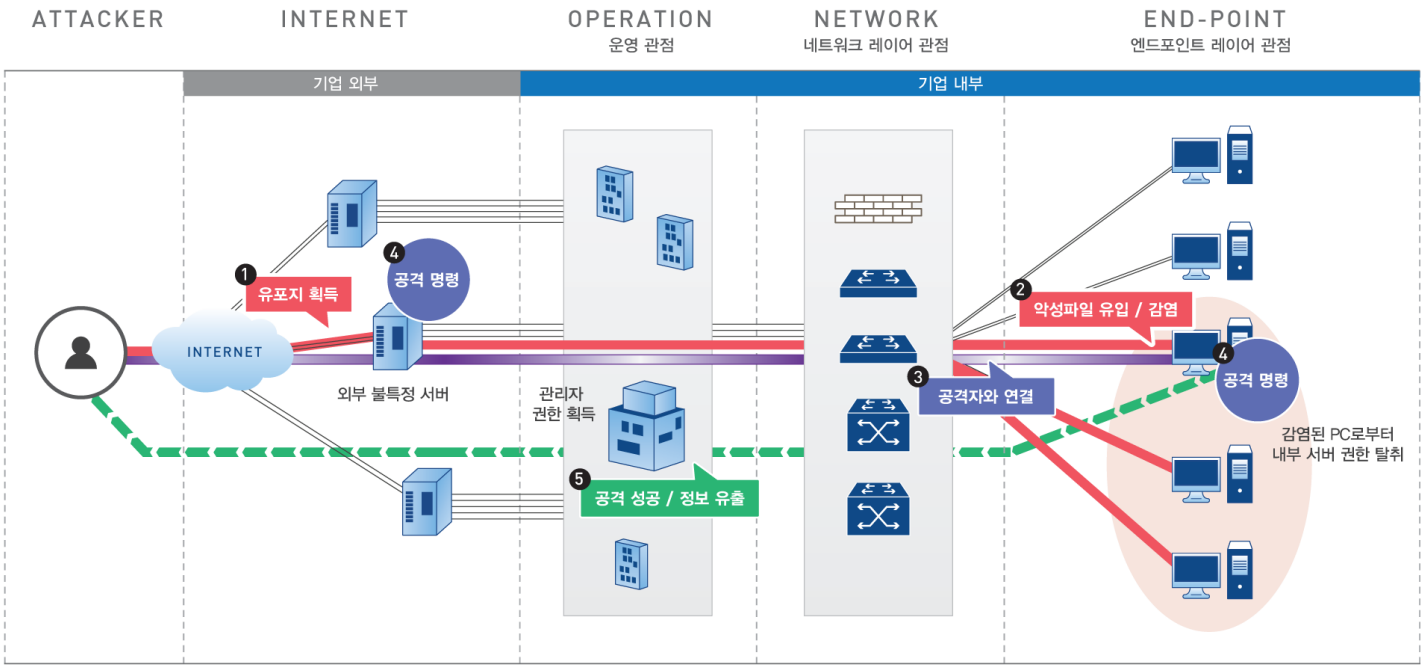
04 APT(Advanced Persistent Threat)
공격 대응 방안

1) APT(Advanced Persistent Threat) 공격 Lifecycle



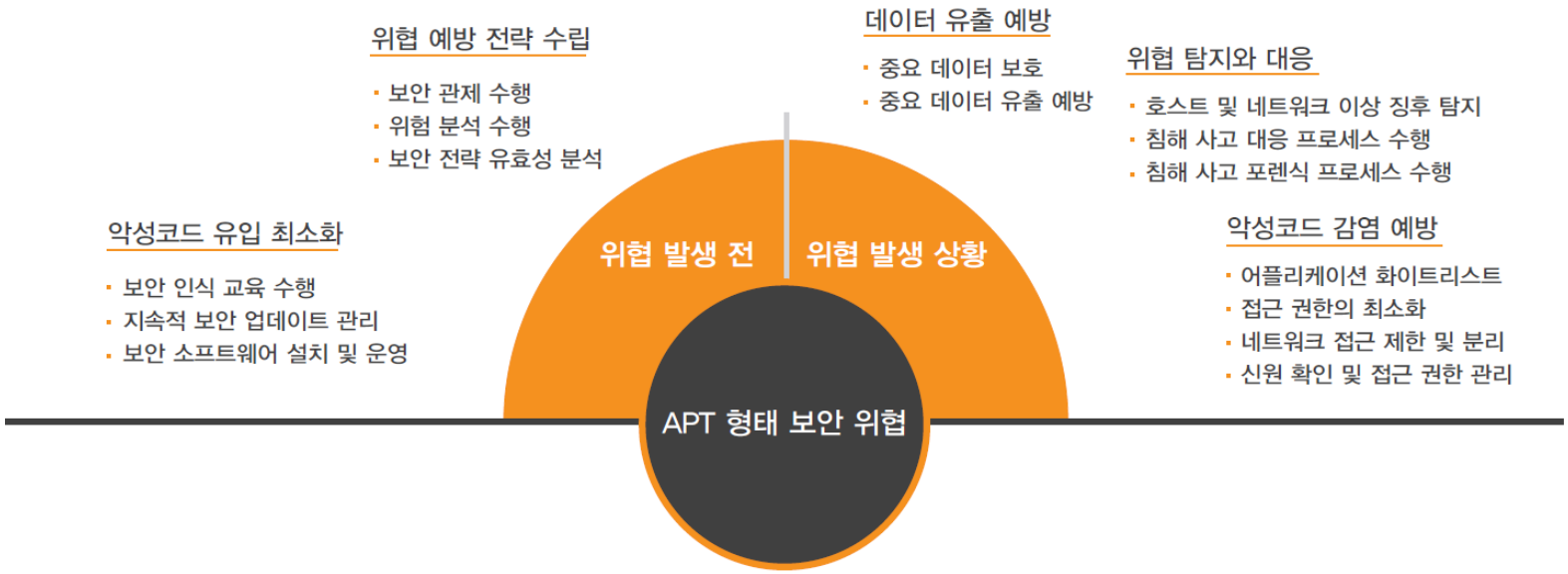
2) APT(Advanced Persistent Threat) 공격 Timeline

- 유포지 획득 - 제 3의 시스템 해킹 후 악성코드 업로드
- 악성코드 유입 및 감염 – 사회 공학 기법(Social Engineering)을 이용한 Targeted Attack 진행
- 공격자와 연결 – 역 접속(Reverse Connection)으로 C&C 서버 연결
- 공격 명령 - C&C 서버를 통해 원격 제어 및 공격 명령 지시



3) APT(Advanced Persistent Threat) 통합대응전략

- ❖ 보안 위협 대응을 위해 Risk Management 기반의 **기업 보안 정책 수립**
- ❖ Attack Surface 축소와 공격 탐지의 효율을 위해 **Defense in Depth 전략 수립**
- ❖ 새로운 보안 위협에 대한 신속한 대응을 위해 **Security Intelligence 확보**
- ❖ 보안 위협의 출발점이 내부 임직원임으로 **주기적인 보안 인식 교육 제공**



APT 공격에 대응하기 위한 보안 전략

4) APT(Advanced Persistent Threat) 공격 예방적 System Hardening

- 모든 운영체제와 Web Application 및 관련 Server는 최신 버전과 보안 패치 적용
- WSUS(Windows Server Update Services)로 최신 보안 패치 배포 및 설치
- 모든 System에는 Anti-Virus Software 설치 후 Anti-Virus Management Server에서 Monitoring
- 모든 운영체제에 존재하는 사용하지 않는 사용자 계정 비활성화 또는 삭제
- HSM(Host Security Monitoring, HIPS) 설치 후 Monitoring 및 주기적 분석
- Terminal Server에는 공용 계정 삭제 후 저장된 계정 정보 및 암호 모두 삭제
- Terminal Server에는 업무 목적 별로 개별 계정 생성 후 Login Log 생성 및 관리
- Database의 xp_cmdshell Procedure 삭제 및 관련 파일 xplog70.dll 삭제
- Database 정보는 암호화 관리하되, Web Server에서 암호화하여 Database로 전송
- Web Server에는 SSL(Secure Socket Layer) 활성화
- 윈도우 Event Log 및 IIS Web Log는 통합 후 Log Management Server에서 관리

5) APT(Advanced Persistent Threat) 공격 탐지적 Network Control

- Backbone Switch에서는 Whitelist 및 Blacklist 이중 정책 설정 및 관리
- 기업 외부 Network에서 기업 내부로 접속 시 IPSec VPN 또는 SSL VPN 이용
- IPSec VPN 또는 SSL VPN 연결 마다 발생하는 모든 VPN Log 별도 관리
- VPN 계정은 업무 목적 별로 생성하고, 권한 역시 구분하여 적용
- 기업 내부 Outbound Packet 에 대한 Filtering 적용
- 기업 내부 HTTP 통신은 모두 Web Proxy를 거치도록 운영 및 관리
- 기업 내부에서는 파일 공유 서비스 대신 SFTP 또는 SCP(Secure Copy)만 사용
- NIDS와 같은 NSM(Network Security Monitoring) 247 운영 및 관리
- NIDS Event 및 전체 Session Data와 Full Packet 저장 및 분석
- 업무 영역 별로 Network 분리 후 각 업무 영역 마다 Firewall 운영 및 관리
- System, Network 및 Database 등 IT 관리 부서는 일반 업무 영역과 별도 구분

Thank you.