당신의 보안프로그램은 안녕하십니까?

이 강 혁

그 파일은.. 알고 보니 악성코드였다…

[주간 악성링크] 새해 벽두 교통관련 사이트 노리는 해커들 外

새해 초 교통관련 사이트를 노린 악성코드가 기승을 부린 데다가 자바 스크립트로 개발된 랜섬웨어 변종인 Ransom32까지 발견돼 이용자들의 주의가 요구된다. 지난 4일에는 XX시 버스 정보시스템, XX고속, 코레일 XX 등 교통관련 사이트에서 악성링크가 줄줄이 포착됐다... 김경애 기자 | 2016.01.06 17:05

[긴급] 감염시 PC 부팅 불가능한 MBR 악성코드 국내 유포!

국내에서 MBR(Master Boot Record) 부트킷(bootkit) 악성코드가 발견돼 이용자들의 주의가 요구된다. 해당 악성코드에 감염되면 PC 시스템 부팅이나 재부팅이 불가능하다. 김경애 기자 | 2016.01.08 11:45

[긴급] 국내 전력기관, 랜섬웨어 포함한 매크로 악성코드 발견

국내 전력기관에도 이메일로 유입되는 매크로 악성코드가 발견된 것으로 드러났다. 최근 이스라엘 전력시설이 이메일로 유입된 랜섬웨어 감염으로 일부 시설에 장애가 발생한 바 있다. 이러한 가운데 국내 전력기관에도 유사한 이메일 악성코드가 지속적으로 유입되는 게 포착된 것. ... 김경애 기자 | 2016.01.29 11:15

[긴급] 벌금·매크로·파워쉘, 랜섬웨어 3종 세트 국내 공략

랜섬웨어가 갈수록 지능화되고 있다. 다양한 프로그램을 악용하는 등 랜섬웨어 감염경로가 확대되고 있는 것. 영문이력서를 위장한 매크로 실행을 유도해 랜섬웨어 감염을 유도하고, 익스플로잇 킷(Exploit Kit)을 통해 랜섬웨어 악성코드를 파워쉘로 다운로드해 실행하기도 ... 김경애 기자 | 2016.02.04 18:10

'꿀뷰' 다운로드 받으려다 200여명 악성코드 감염

반디소프트의 이미지 뷰어 프로그램인 '꿀뷰'를 다운로드 받은 200여명의 사용자들이 꿀뷰 설치 파일 대신 악성코드를 다운로드 받은 것으로 드러났다. 26일 오후 2시부터 4시까지 약 두 시간 동안, 반디소프트 홈페이지(www.bandisoft.co.kr)가 외부로부터 ... 권준 기자 | 2016.03.27 23:50

말하는 랜섬웨어 'Cerber' 국내 유포 확산으로 피해 증가

최근 말하는 랜섬웨어 'Cerber'가 웹에서 플래시 제로데이 취약점을 통해 유포되며 기승을 부리고 있다. 이로 인해 국내에 피해자들이 급증해 이용자들의 각별한 주의가 요구된다. 김경애 기자 | 2016.04.08 12:23

출처 : www.boannews.com

북한… 해킹 배우러 유학 갈까?

북한 제작 추정 악성프로그램 변종 발견

북한 추정의 사이버 공격이 지난 1월 29일에도 포착됐다. 북한의 핵실험 발표 이후 특정기관을 노리는 사이버공격이 포착된 이후에도 청와대와 공공기관을 사칭한 악성메일 유포로 정보 유출을 노리는 공격이 감행됐다. 김경애 기자 | 2016.02.01 20:55

기반시설 이어 금융권까지…北 해킹 공격 전방위 확대되나?

북한의 4차 핵실험 이후 남북간의 긴장감이 최고조에 달하고 있는 가운데 북한에서 제작된 것으로 추정되는 금융관련 악성프로그램이 발견돼 금융보안에도 경고등이 켜졌다. 지난 15일 발견된 악성프로그램은 금융관련 모듈과 DRM 관련 모듈 프로그램으로, 공격에 이용된 변종도 … 김경애 기자 | 2016.02.16 19:25

국정원 "북한 김정은이 대남 사이버테러 지시"

북한이 4차 핵실험 이후 우리나라를 타깃으로 한 사이버공격을 강화하고 있다는 보고서가 나와 이목이 집중되고 있다. 김경애 기자 | 2016.02.18 11:50

철도운영기관 노린 북한 해킹 공격, 피해 및 대응현황은?

북한이 지난 1~2월 2개 지방의 철도운영기관 직원들을 대상으로 피싱 메일을 유포해 직원들의 메일 계정과 패스워드 탈취를 시도한 것으로 드러났다. 이는 철도교통관제 시스템을 대상으로 한 사이버테러 준비단계로, 국정원은 지난 2월 해킹징후를 감지하고, 주요 기관들의 트래… 김경애 기자 | 2016.03.08 14:55

3.20은 지났지만…北 사이버테러는 현재진행형

북한이 무력 도발과 사이버공격 위협은 물론 박근혜 대통령 제거까지 거론하는 등 우리나라에 대한 총공세에 나서고 있다. 지난 23일 북한은 중대보도를 통해 박근혜 대통령 제거를 거론하고 정규부대와 특수부대 투입까지 암시하며 위협하고 있다. 청와대를 비롯한 주요 대상들을 … 김경애 기자 | 2016.03.24 16:40

출처 : www.boannews.com

기업은 언제나 꾸준히…

[웹사이트 경보] 대형 치과병원 사내 사이트 해킹 外

한 주간 전국 9개 지점을 보유한 치과병원 사내 사이트가 해킹됐으며, 네이버를 사칭한 악성사이트도 발견됐다. 또한, XX설계용역업무 지원시스템 사이트에 업로드된 엑셀 파일에서는 매크로용 바이러스가 탐지됐으며, 배송과 구매대행 사이트에서는 랜섬웨어가 탐지됐다. 다음은 악… 김경애 기자 | 2016.02.23 17:40

[주간 악성링크] 디페이스 해킹에 파워셀 이용 악성코드 유포까지

한 주간 보안이 취약한 국내 웹사이트가 대거 디페이스 해킹을 당한 것으로 드러났다. 국내 29개 사이트가 한 공격자로부터 디페이스 해킹을 당한 정황이 포착됐으며, 해운 사이트, 홈페이지 제작 사이트 등도 디페이스 해킹을 당한 것으로 드러났다. 뿐만 아니라 한 주간 파워… 김경애 기자 | 2016.02.24 18:55

영국거주 한국계 해커, 국내 포털 이메일 계정 대거 공개

지난해 10월 국내 K은행 창작동화제 작품공모전 웹사이트와 H은행 웹사이트를 해킹해온 영국거주 한국계 혼혈 해커가 국내 유명 포털사이트 이메일 계정정보까지 대거 공개한 것으로 알려져 파문이 확대되고 있다. 민세아 기자 | 2016.03.02 14:55

한국계 혼혈해커, 국내 기업 그룹웨어 서버 해킹

지난 18일, 국내 기업 두 곳의 그룹웨어 웹사이트가 해킹당한 사실이 뒤늦게 밝혀졌다. 해당 웹사이트를 해킹한 이 해커는 트위터를 통해 자신을 지난해 10월 국내 K은행 창작동화제 작품공모전 웹사이트와 H은행 웹사이트를 해킹한 영국거주 한국계 혼혈해커라고 소개했다. 민세아 기자 | 2016.03.22 18:51

출처 : www.boannews.com

2016년은 한해 공격은..?

출처 : KISA Facebook

사이버 공격 형태

알면 차단하였다고 보고하고, 모르면 이상 없다고 지나갑니다.

Known Attack

공격패턴 파악 완료

- **방화벽**, IPC, NAC **등의 패턴기반의 보안 장비로 보안**

취약점 Attack

Zero-Day, **악성코드**

- **접근통제**, SSO **등의 보안장비로 인증 강화**

Unknown Attack

정상활동(?)

- DRM, DLP **등으로 데이터 암호화 및 접근 통제**

일반 회사의 보안 현황

우리회사만은 해킹 당하지 않게 해주세요. 안 그러면 저 잘려요.

이제 메신저도?

사내 모든 프로그램을 사칭할 기세...

인터넷 | **삼성 메신저 '마이싱글' 사칭 악성코드 유포**

손경호 기자 | 입력 : 2016.01.25. 19:36 | 수정 : 2016.01.26. 07:53

삼성그룹 내부에서 베타테스트 버전으로만 개발한 사내 메신저인 '마이싱글'의 설치파일(mySingleMessenger.exe)과 같은 이름을 가진 악성코드가 발견됐다.

현재 삼성그룹은 사내 인트라넷인 '마이싱글'에 접속하면 임직원 인증을 거쳐 사내 PC, 모바일 버전용 메신저인 '스퀘어 포 마이싱글(Square for mySingle)'이 푸시형태로 자동설치된다.

이 메신저를 개발한 삼성SDS측 관계자는 "마이싱글이라는 설치파일은 현재 사용되고 있는 스퀘어와는 전혀 다른 것으로 사내 베타테스트 용도로만 썼던 것"이라며 "이와 관련해 내부에 악성코드가 유입된 흔적은 찾지 못했으며, 추가로 분석을 진행 중"이라고 밝혔다. 마이싱글을 사칭한 악성코드는 개발자들이 내부에서 개발 중 테스트했던 버전이었다는 설명이다.

이 관계자는 "지난해 말 부터 삼성그룹 사내 메신저로 도입된 스퀘어 포 마이싱글은 마이싱글을 사칭한 악성코드와는 별개"라고 덧붙였다.

출처 : www.zdnet.co.kr

디지털 서명도..

어디 회사인지 저는 알아도 알지 못한다고 합니다..

[단독]제2의 3·20 재현 우려…금융권 보안솔루션 공급사 디지털서명 해킹

금융권과 공공기관에 보안솔루션을 제공하는 한 보안업체의 최신 디지털서명(코드사인)이 해킹됐다. 이 회사 고객인 금융권이나 공공기관, 기업에 대규모 사이버 장애를 일으킬 수 있는 악성코드가 잠복했을 가능성이 높다. 보안 전문가들은 2013년에 금융 및 방송망을 마비시킨 3·20사이버테러와 유사한 공격이 발생할 수 있는 심각한 사안으로 보고 있다.

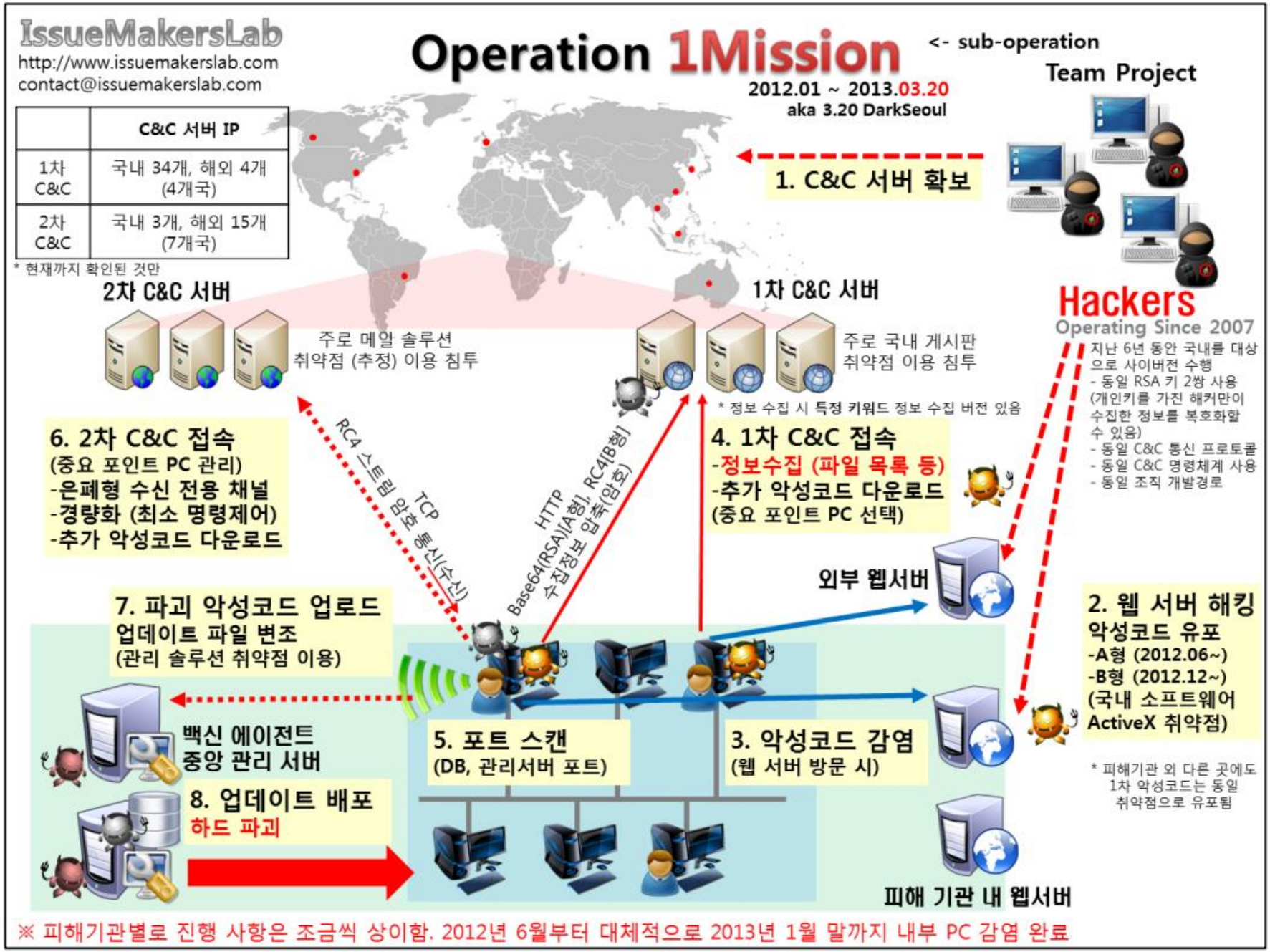
금융보안원(원장 허창언)은 최근 이 회사 코드사인이 해킹되고 이를 이용한 악성코드가 발견돼 금융권에 비상대응령을 내렸다. 북한 4차 핵실험 후 남북 사이버 긴장감이 최고조다. 보안 전문가는 이 기업 이외에 국내에서 많이 사용하고 있는 보안이나 소프트웨어 프로그램의 취약점 점검과 코드사인 관리 강화를 주문했다.

코드사인은 프로그램 신뢰와 안정성을 입증하는 역할이다. 특정 프로그램을 사용자 PC에 설치할 때 해당 제품이 변조되지 않고 안전하며 신뢰할 수 있다는 것을 공인된 인증기관이 입증한 디지털 서명이다.

금융 업무나 전자민원 서비스를 할 때 각종 보안 프로그램을 내려받는다. 이때 어떤 회사에서 만든 프로그램인지 알려준 후 신뢰하면 내려받으라는 문구를 보여 준다.

코드사인이 없는 프로그램이 PC나 서버에 설치되면 '게시자를 확인할 수 없어서 소프트웨어를 차단했습니다'란 경고창이 뜬다. 프로그램 설치 화면에 '알 수 없는 게시자'라는 경고가 나타난다. 악성코드 등 악의성 프로그램 설치를 막는 기능이다.

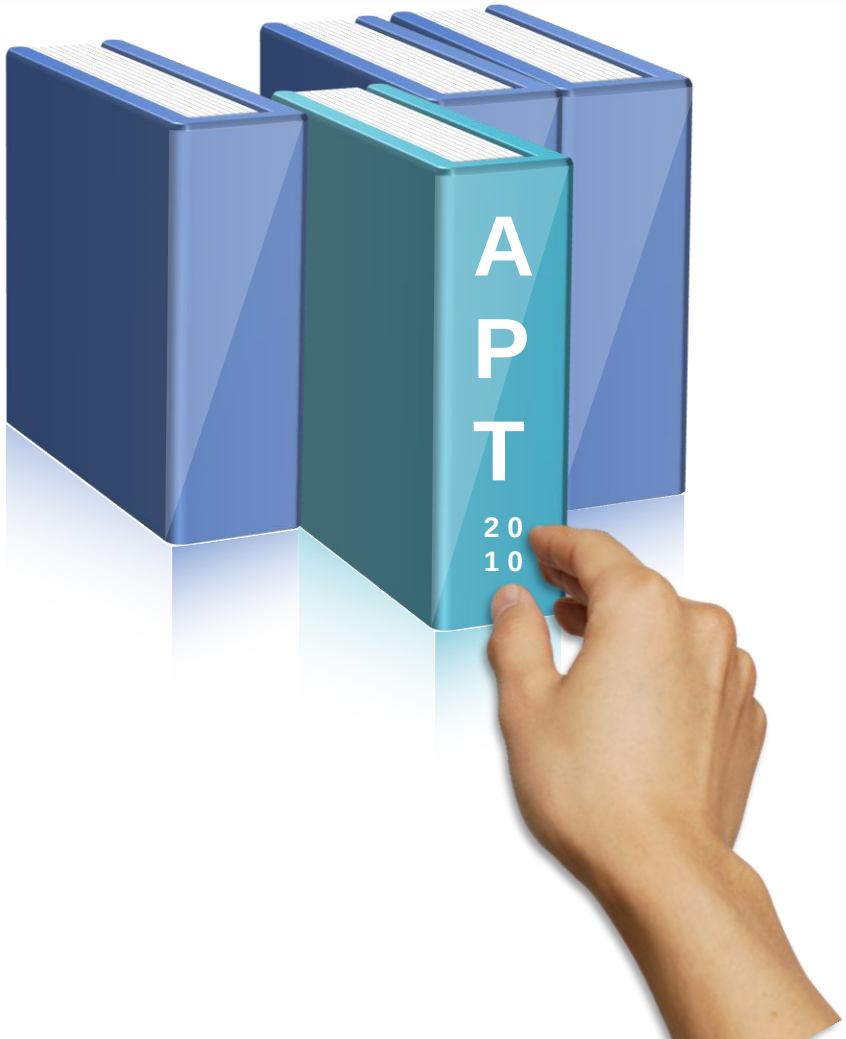
출처 : www.etnews.com


IssueMakersLab
http://www.issuemakerslab.com
contact@issuemakerslab.com
Operation 1Mission
<- sub-operation
Team Project
2012.01 ~ 2013.03.20
aka 3.20 DarkSeoul
C&C 서버 IP
1차 C&C
국내 34개, 해외 4개 (4개국)
2차 C&C
국내 3개, 해외 15개 (7개국)
* 현재까지 확인된 것만
1. C&C 서버 확보
2차 C&C 서버
주로 메일 솔루션 취약점 (추정) 이용 침투
1차 C&C 서버
주로 국내 게시판 취약점 이용 침투
* 정보 수집 시 특정 키워드 정보 수집 버전 있음
Hackers
Operating Since 2007
지난 6년 동안 국내를 대상으로 사이버전 수행
- 동일 RSA 키 2쌍 사용 (개인키를 가진 해커만이 수집한 정보를 복호화할 수 있음)
- 동일 C&C 통신 프로토콜
- 동일 C&C 명령체계 사용
- 동일 조직 개발경로
6. 2차 C&C 접속
(중요 포인트 PC 관리)
-은폐형 수신 전용 채널
-경량화 (최소 명령제어)
-추가 악성코드 다운로드
RC4 스트림 암호 통신(수신)
TCP
HTTP
Base64(RSA)[A형], RC4[B형]
수집정보 압축(암호)
4. 1차 C&C 접속
-정보수집 (파일 목록 등)
-추가 악성코드 다운로드
(중요 포인트 PC 선택)
외부 웹서버
2. 웹 서버 해킹
악성코드 유포
-A형 (2012.06~)
-B형 (2012.12~)
(국내 소프트웨어 ActiveX 취약점)
* 피해기관 외 다른 곳에도 1차 악성코드는 동일 취약점으로 유포됨
7. 파괴 악성코드 업로드
업데이트 파일 변조
(관리 솔루션 취약점 이용)
백신 에이전트 중앙 관리 서버
5. 포트 스캔
(DB, 관리서버 포트)
3. 악성코드 감염
(웹 서버 방문 시)
8. 업데이트 배포
하드 파괴
피해 기관 내 웹서버
※ 피해기관별로 진행 사항은 조금씩 상이함. 2012년 6월부터 대체적으로 2013년 1월 말까지 내부 PC 감염 완료

출처 : NSHC

What?

Advanced Persistent Treat (지능형 지속 공격)



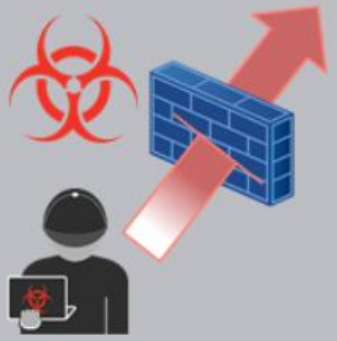
DieHard 4.0(2007)

정부의 네트워크 전산망을 파괴해 미국을 장악 - 미국의 교통,통신,금융,전기 등 모든 네트워크가 테러리스트의 손아귀

APT는 Stuxnet(2010)에서 부터…

출처 : DieHard4.0 한 장면(발전소)

1



침투

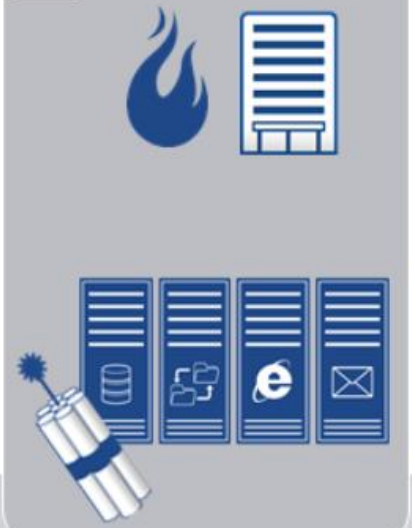
목표 대상을 정해 관련 정보 수집 후, 취약점을 찾아내 제로데이 익스플로잇을 통해 침투 시도

2

검색

침투한 내부 시스템 및 인프라 구조에 대한 정보를 수집한 후 다음 단계 계획

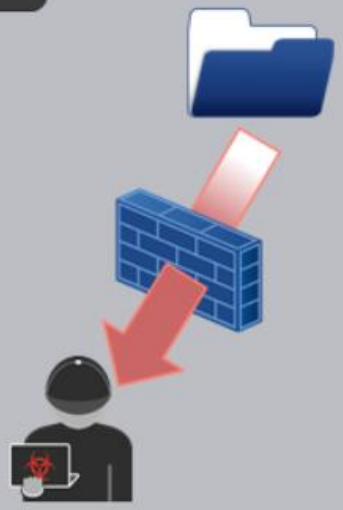
3



수집

중요 서버 점령, 제어권 획득 후 무력화된 시스템 상의 데이터 수집

4



유출

공격자의 근거지로 데이터 전송 혹은 시스템 운영 방해 또는 장비 파괴

출처 : belldoor.tistory.com


1
Firewall
2
TMS
3
AV
4
IPS, IDS
5
EMS
6
DLP
7
UTM
8
RMS
9
DRM
10
NAC
11
NMS
12
PMS
13
VPN
14
MMS
15
VDI

3
AV

6
DLP

9
DRM

12
PMS

10
NAC

13
VPN

이 파일의 정체는..

보안프로그램은 모두 정상인가?

YES or No

보안프로그램으로 가장한 악성코드를 구분할 수 있는가?

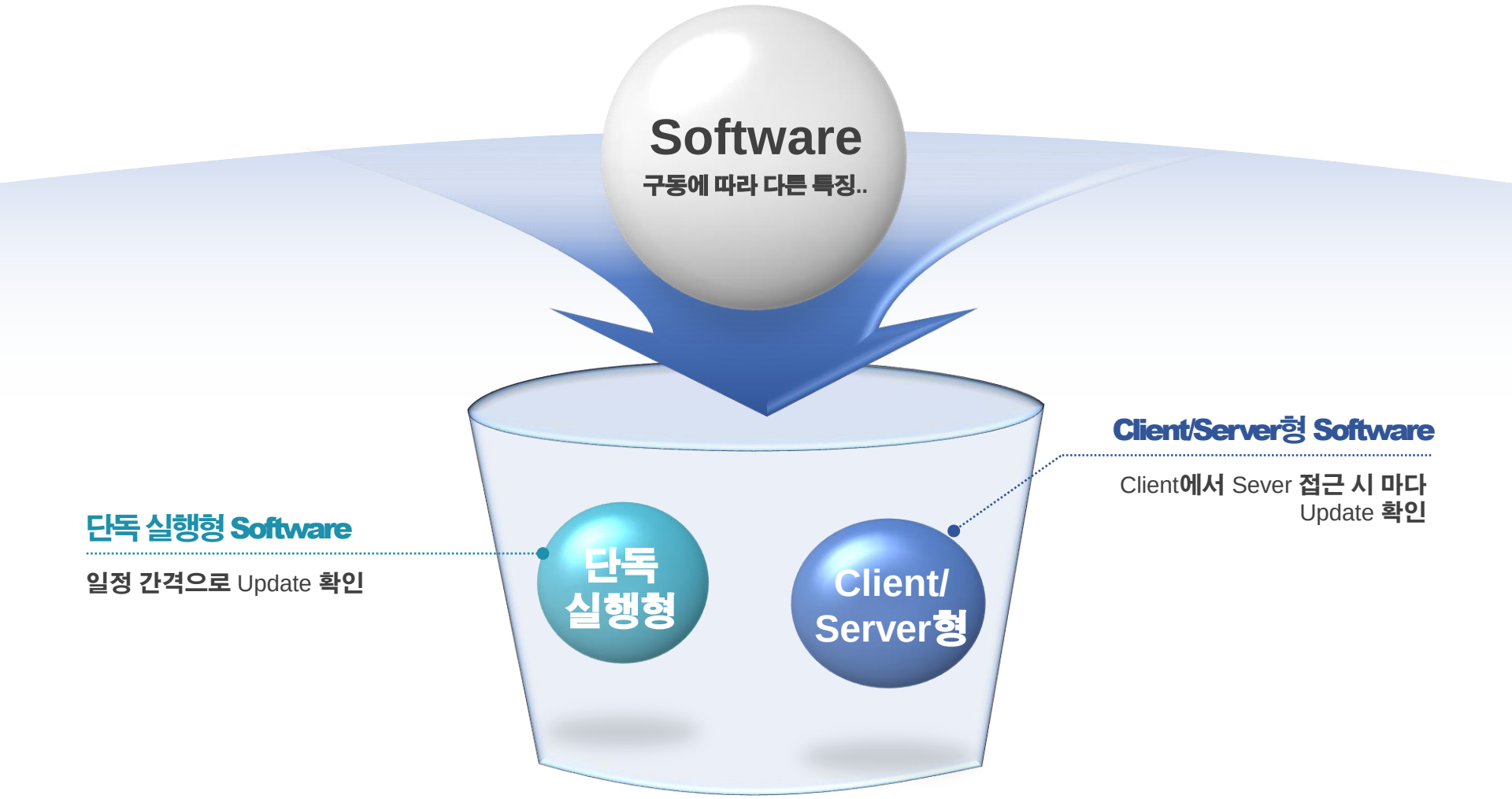
YES or No

악성코드의 목적은?

정보유출? 시스템 파괴? 보안담당자 실직?

Security Program..

Software Update



단독 실행형 Software

일정 간격으로 Update 확인

Client/Server형 Software

Client에서 Sever 접근 시 마다 Update 확인

Software Update

흠...어디서 해야 하지...

서버의 경우는...?

Update version **관리는**...?

우리회사 보안 프로그램?

우리는 보안 프로그램을 얼마나 알고 있을까요? 과연 우리 회사에 꼭 필요한 보안 프로그램들을 사용하고 있을까요?

우리 회사에는 어떤
보안 프로그램이 있는지 안다.

유지보수는 협력업체에
맡기고 운용에 필요한
기능만 안다.

동작 방법을 알고 있어 필요 시 협력업체와
기술에 대해 논할 수 있다.

누가 관리할까?

보안 프로그램의 취약점 관리 주체는?

관련 문제입니다..

"외부 기관에서 기업 내 임직원 PC들이 1111번 포트를 이용하여 악성 C&C서버와 통신되고 있다고 알려왔다. 사고 분석과정에서 임직원 PC가 있는 사무실에는 방화벽이 설치되어 있어 접근통제가 되고 있으며, 임직원 PC는 악성코드가 발견되지 않았고 특별한 이상징후도 없었다. 외부 기관에서 알려준 1111번 포트는 내부 보안프로그램에서 사용되고 있어 정상으로 판단하였다."
이러한 경우 생각해보아야 하는 방향은?

1. 임직원PC에서 이상징후가 발견되지 않았으므로 잘못된 신고로 판단한다.

2. 1111번 포트를 이용하는 프로세스를 다시 분석해보고 악성코드가 확인되지 않을 경우 보안 프로그램을 의심한다.

그럼..어떻게?

출처 : pixabay.com

보안 프로그램 자세히 알자.

사고 발생 시 “여기 좀 이상한데?”, “원래 이러지 않는데?” 라는 정보를 제공할 수 있도록…

1. 동작 확인

• 평상시 보안 프로그램의 동작을 파악해두고 주기적인 이상여부 확인

2. 무결성 검증

보안 프로그램 및 Update 파일이나 배포 파일에 대한
무결성 확보 및 **이력 관리**

정보를 제공하자

수다스런 옆집 아줌마처럼 침해분석 중 추적이 용이하도록...

꼼꼼한 운영관리

1. **회사 보안프로그램 운영 정보는 나에게!!**
2. Vender**와의 통역은 나에게!!**

꼼꼼한 이력관리

1. **사내 프로그램의** Version History**도 관리 착착!**
2. **불필요한** Update**는** No.

.

내가 보안 담당자라면?

살펴 보아야 될 관점이 늘었다... 봐도 보이지 않아.

THANK YOU

이 강 혁