DDoS 공격, 게임계정 유출 해커, 비트코인 등 가상화폐 노린다

- '13년 10월부터 DDoS, 원격제어, 게임계정 유출하더니 최근 암호화폐 채굴 -

□ 개 요

지난 '13년 10월, Microsoft社의 인터넷 익스플로러 취약점(CVE-2013-3897)을 통해 유포되는 악성코드가 DDoS, 원격 제어, 게임계정 유출 기능을 하고 국내 감염 PC가 2만 8천여대에 이르러 KISA는 신속 대응한 바 있다. 해당 악성코드 제작자는 '14년 1월 게임계정 유출 기능을 업그레이드하여 감염 PC에서 사용 중인 비트코인 사이트 계정을 수집하였다.

※ 비트코인 : '08년 일본人 사토시 나카모토가 처음 발행한 전자화폐로 중앙 관리 기구는 존재하지 않으며 성능 좋은 컴퓨터를 활용하여 어려운 수학문제를 풀면 획득 가능

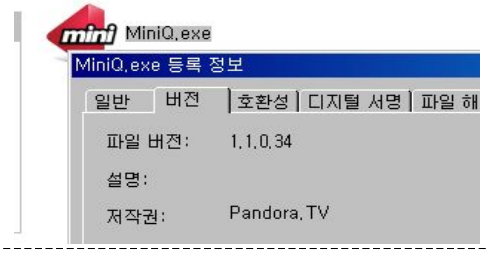
< 감염 PC에서 접속하는 비트코인 사이트 모니터링 >

.rdata:100…	0000000B	C	bitpay.com
.rdata:100…	0000000D	C	coinbase.com
.rdata:100…	0000000D	C	multibit.org
.rdata:100…	0000001B	C	bitcoindomains.blogspot.kr
.rdata:100…	00000011	C	.bitcointalk.org
.rdata:100…	0000000D	C	.bitcoin.org

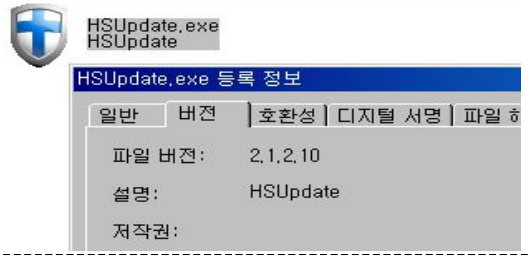
이 후 해커는 국내 동영상 스트리밍 서비스인 판도라TV 서버를 해킹하고 변조된 설치 파일을 통해 악성코드를 유포하였다. 해당 악성코드 제작 일자는 '14년 2월 3일이었으며 신속한 대응으로 3일 만에 삭제 조치되었다. 그러나 2월 16일 또다시 해커는 안랩의 게임 보안 솔루션('핵쉴드') 업데이트 파일을 가장하여 악성코드를 유포하였다. 해당 악성코드는 비트코인 계정을 탈취하던 기존 방식을 암호화폐 Protoshares(PTS, '13년 11월 5일 최초 발행)를 채굴하는 방식으로 변경하여 금전적 이득을 취했다.

※ Protoshares(PTS) 암호화폐 : '13년 11월 5일 Invictus Innovations社가 미국 아틀란타에서 최초 발행한 전자화폐로 공급량이 많아지면서 통화가치가 상승할 것으로 판단하여 채굴 대상으로 선택 추정

< 판도라 TV 설치 파일을 가장한 악성코드 >



< 안랩 핵쉴드 설치 파일을 가장한 악성코드 >



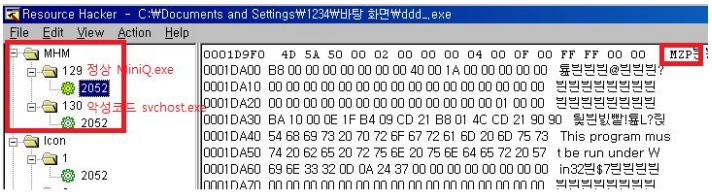
'13년 10월 30일 IE 제로데이 취약점 (CVE-2013-3897) 이용 악성코드 유포건	'14년 2월 3일 판도라 TV건	'14년 2월 16일 안랩 핵쉴드건
Description / Value Machine / IMAGE_FILE_MACHINE_I386 Number of Sections Time Date Stamp / 2006/06/13 05:49:21 UTC 제작 일시 : 2006년 6월 13일	Description / Value Machine / IMAGE_FILE_MACHINE_I386 Number of Sections Time Date Stamp / 2014/02/03 00:38:39 UTC 제작 일시 : 2014년 2월 3일	Description / Value Machine / IMAGE_FILE_MACHINE_I386 Number of Sections Time Date Stamp / 2014/02/16 05:36:33 UTC 제작 일시 : 2014년 2월 16일

□ 악성코드 다운로더 분석 결과

변조된 판도라 TV 및 핵쉴드 설치파일은 리소스 영역에 정상 설치 파일과 악성코드를 숨기는데 동일한 리소스명을 사용하였다. 리소스명은 모두 MHM/129/2052와 MHM/130/2052 이었다.

※ '12년 10월 30일 발생한 IE 제로데이 취약점을 통한 악성코드 유포 건에는 해당되지 않음

```
v3 = GetModuleHandleA(0);
if ( lpName == (HRSRC)129 )
{
  v4 = FindResourceA(v3, (LPCSTR)129, "MHM");
}
else if ( lpName == (HRSRC)130 )
{
  v4 = FindResourceA(v3, (LPCSTR)130, "MHM");
}
else
{
  v4 = lpName;
```



< 판도라 TV 설치파일을 가장한 악성코드 내 리소스 영역 >

< 안랩 핵쉴드 설치파일을 가장한 악성코드 내 리소스 영역 >

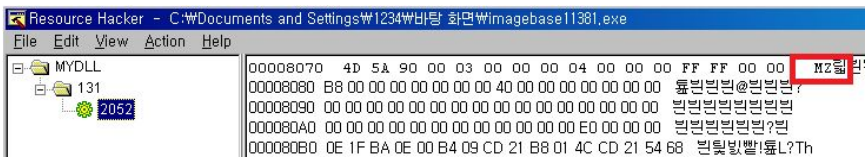
또한 16개 ~ 19개 사이트에 주기적으로 접속하여 악성코드를 추가 다운로드하려고 시도했다. 사이트 대부분이 정상 사이트이었으며 이 중 한 사이트가 특정 시점에 악성코드를 포함하고 있었다. 이는 악성코드 분석가가 진짜 다운로드 사이트를 알아채기 못하도록 혼동을 주기위한 목적으로 보인다. 16개 ~ 19개 사이트는 분석을 방해하기 위해 인코딩되어 있으며 해독하는 알고리즘은 모두 동일하였다.

'13년 10월 30일 IE 제로데이 취약점 (CVE-2013-3897) 이용 악성코드 유포건	'14년 2월 3일 판도라TV 건	'14년 2월 16일 안랩 핵쉴드건

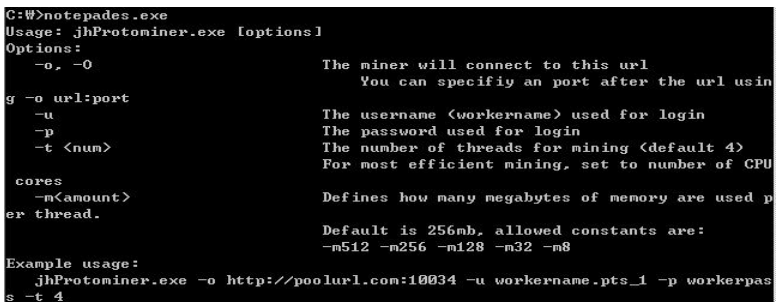
`v1 = decodedURL;`
`cnt = -2;`
`for ( result = *(_BYTE *)decodedURL; result; --cnt )`
`{`
`  *(_BYTE *)v1 = cnt ^ result;`
`  result = *(_BYTE *)(v1++ + 1);`
`}`
	`v1 = a1;`
	`v2 = -2;`
	`for ( result = *(_BYTE *)a1; result; --v2 )`
	`{`
	`  *(_BYTE *)v1 = v2 ^ result;`
	`  result = *(_BYTE *)(v1++ + 1);`
	`}`
	`return result;`
		`v1 = a1;`
		`v2 = -2;`
		`for ( result = *(_BYTE *)a1; result; --v2 )`
		`{`
		`  *(_BYTE *)v1 = v2 ^ result;`
		`  result = *(_BYTE *)(v1++ + 1);`
		`}`
		`return result;`

'13년 10월 30일 IE 제로데이 취약점 (CVE-2013-3897) 이용 악성코드 유포건	'14년 2월 3일 판도라TV 건	'14년 2월 16일 안랩 핵쉴드건
adw.grXXn24.XX.XX/djdjdaua.jpg	XXX.naver.com/panmenu.jpg	XXX.naver.com/panmenu.jpg
XXX.naver.com/djdjdaua.jpg	fXXXone.co.kr/bbs/data/panmenu.jpg	fXXXone.co.kr/bbs_back/data/7zone/panmenu.jpg
m.ahXXXb.com/djdjdaua.jpg	m.ahXXXb.com/panmenu.jpg	m.ahXXXb.com/panmenu.jpg
www.cXs.co.kr/djdjdaua.jpg	sXXXate.gndot.com/panmenu.jpg	sXXXate.gndot.com/panmenu.jpg
www.dXXm.net/djdjdaua.jpg	www.hXXXame.com/panmenu.jpg	www.hXXXame.com/panmenu.jpg
www.hXXXame.com/djdjdaua.jpg	www.hXXXan.co.kr/panmenu.jpg	www.hXXXan.co.kr/panmenu.jpg
www.hXXXan.co.kr/djdjdaua.jpg	www.jXXXsmsn.com/panmenu.jpg	www.jXXXsmsn.com/panmenu.jpg
www.jXXXsmsn.com/djdjdaua.jpg	www.mXXXuc.com/panmenu.jpg	www.mXXXuc.com/panmenu.jpg
www.lXXXoul.co.kr/djdjdaua.jpg	www.mXn.com/panmenu.jpg	www.mXn.com/panmenu.jpg
www.mXn.com/djdjdaua.jpg	www.nXXe.com/panmenu.jpg	www.nXXe.com/panmenu.jpg
www.nXXe.com/djdjdaua.jpg	www.nXXXarble.net/panmenu.jpg	www.nXXXarble.net/panmenu.jpg
www.nXXXarble.net/djdjdaua.jpg	www.nXXXn.com/panmenu.jpg	www.nXXXn.com/panmenu.jpg
www.nXXXn.com/djdjdaua.jpg	www.sXXXtkorea.com/bbs2/panmenu.jpg	www.sXXXtkorea.com/bbs2/panmenu.jpg
www.tXXXory.com/djdjdaua.jpg	www.sXXr.co.kr/bbs2/data/panmenu.jpg	www.sXXr.co.kr/bbs2/data/panmenu.jpg
www.tXXXni.com/djdjdaua.jpg	www.tXXXory.com/start/panmenu.jpg	www.tXXXory.com/start/panmenu.jpg
www.vXXXte.com/djdjdaua.jpg	www.tXXXni.com/panmenu.jpg	www.tXXXni.com/panmenu.jpg
	www.vXXXte.com/panmenu.jpg	www.vXXXte.com/panmenu.jpg
	www1.nXXXk.net/panmenu.jpg	www1.nXXXk.net/panmenu.jpg
	fXXt.co.kr/board/data/media/panmenu.jpg	fXXt.co.kr/board/data/media/panmenu.jpg
	fXXt.co.kr/board/data/qna/count.php	fXXt.co.kr/board/data/qna/XXXme.php

반면 유포지에 접속하는 주기는 사건별로 달랐으며 작년 10월 발생한 악성코드 유포건의 경우 1초였으나 판도라TV 건과 핵쉴드 건의 경우 10분이었다. 해커는 탐지 및 삭제 등을 우회하기 위해 원하는 시점에 악성코드를 16 ~ 19개 사이트 중 한 곳에 설치하였다. 다운로드된 악성코드에는 MYDLL\131\2052 리소스 영역이 존재하며 해당 영역에 jhProtomine이라는 공개된 암호화폐 채굴 프로그램을 저장하고 실행시켰다.



< 다운로드된 악성코드 내 리소스 영역 >



< 리소스 영역에 저장된 PTS 암호채굴 프로그램 >

□ Protoshares(PTS) 암호화폐 채굴 악성코드 분석 결과

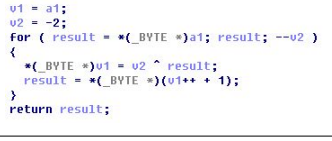
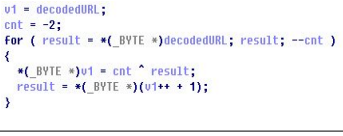
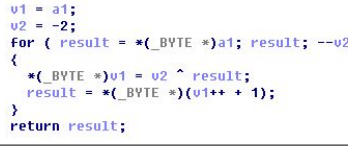
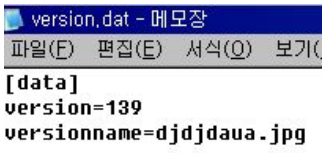
악성코드는 CPU를 최대한 사용하기 위해 다른 비트코인 채굴 프로그램(minerd.exe)이 있을 시 종료시키고 PTS 암호 화폐 채굴 프로그램을 실행시켰다. 실행 옵션으로 채굴 사이트 아이디 및 패스워드를 입력하는데 국내 홈페이지에서 유포된 악성코드를 분석한 결과 아이디가 모두 유사하였다. 아래 표는 유포지에서 발견된 악성코드별 아이디, 패스워드, C&C이며 버전별로 아이디가 관리되고 있는 것으로 보인다. 악성코드 다운로더와 다운로드된 암호화폐 채굴 악성코드에서 명령조정지 fXXt.co.kr가 동시에 발견된 점으로 미루어 볼 때 해커가 애용하는 사이트로 보인다.

순번	유포지	리소스 이름	아이디	패스워드	명령조정지
1	변조된 '핵쉴드' 설치파일 <제작일시 : 2014/02/17 05:51:10>	MYDLL₩131₩2052	cheon23.PTS_7 cheon23.PTS_8	123456	hxxp://fXXt.co.kr/board/data/count10.php hxxp://fXXt.co.kr/board/data/count11.php
3	hxxp://gamefocus.co.kr/wys2/swf_upload/2010/06/01/12753477929868.jpg <제작일시 : 2013/12/13 06:37:04>	MYDLL₩131₩2052	cheon21.PTS_1	123456	hxxp://fXXt.co.kr/board/data/count6.php
4	hxxp://112.175.88.165/bbs/menu.gif <제작일시 : 손상되어 해당사항 없음>	MYDLL₩131₩2052	cheon22.PTS	123456	hxxp://fXXt.co.kr/board/data/count10.php hxxp://fXXt.co.kr/board/data/count11.php
5	hxxp://image.danimgaon.com/bbs/image.jpg <제작일시 : 2013/12/23 05:05:26>	MYDLL₩131₩2052	cheon21.PTS_7	123456	hxxp://fXXt.co.kr/board/data/count8.php
6	hxxp://www.dompage.co.kr/bbs/auto.gif <제작일시 : 손상되어 해당사항 없음>	MYDLL₩131₩2052	cheon22.PTS_19 cheon22.PTS_20	123456	hxxp://fXXt.co.kr/board/data/count10.php hxxp://fXXt.co.kr/board/data/count11.php
7	hxxp://news.dompage.co.kr/bbs/ads.gif <제작일시 : 2014/01/05 03:56:46>	MYDLL₩131₩2052	cheon23.PTS_1 cheon23.PTS_3	123456	hxxp://fXXt.co.kr/board/data/count12.php hxxp://fXXt.co.kr/board/data/count13.php hxxp://fXXt.co.kr/board/data/count15.php

□ 악성코드 감염 예방 방법

이와 같이 악성코드를 통해 게임 계정, 비트코인 계정, 인터넷 뱅킹 정보 등을 유출하여 사이버 머니 등 금전적 이득을 취하는 해커가 증가하고 있다. 암호 화폐 채굴은 다른 방식에 비해 금전적 피해는 적으나 높은 CPU 점유율으로 인해 사용자 불편을 초래할 수 있다. 사용자는 백신을 최신 버전으로 업데이트하고 주기적으로 검사하여 악성코드 감염을 예방해야 한다. 또한 특정 프로그램이 CPU를 필요 이상으로 많이 사용하고 성능이 현격히 저하되었다면 일단 의심하고 백신으로 검사한 후 118센터 등에 신고하는 것이 필요하다.

[첨부 1] 사고별 유사성 분석 결과

구분	'13년 10월 30일 안랩, 16개 웹사이트 대상 대규모 디도스 공격 경보	'14년 2월 6일 판도라TV 건	'14년 2월 16일 안랩 핵쉴드건	유사도
타임 스탬프	Description / Value Machine / IMAGE_FILE_MACHIN Number of Sections Time Date Stamp / 2006/06/13 05:49:21 2006년 6월 13일	Description / Value Machine / IMAGE_FILE_MACHINE_I Number of Sections Time Date Stamp / 2014/02/03 00:38:39 UTC 2014년 2월 3일	Description / Value Machine / IMAGE_FILE_MACHINE_I3 Number of Sections Time Date Stamp / 2014/02/16 05:36:33 UTC 2014년 2월 16일	-
서비스명	WinLogon	WinLogon	WinLogon	높음
서비스 설명	Provides automatic configuration for the 802.11 adapters	Provides automatic configuration for the 802.11 adapters	Provides automatic configuration for the 802.11 adapters	높음
파일 위치	C:₩WINDOWS₩svchost.exe	C:₩Documents and Settings₩1234₩Local Settings₩Temp₩svchostexe	C:₩Documents and Settings₩1234₩Local Settings₩Temp₩svchostexe	-
접속 주기	1초(6000ms)	10분 (600,000ms)	10분 (600,000ms)	-
인코딩된 URL 모듈				높음
URL 디코딩 모듈				높음 (동일)
데이터 파일	 version.dat	 version.dat	 version.dat	높음
다운로드 파일	hxxp://[URL]/djdjdaua.jpg	hxxp://[URL]/panmenu.jpg	hxxp://[URL]/panmenu.jpg	높음
설치 파일	C:₩WINDOWS₩image.jpg	C:₩WINDOWS₩image.jpg	C:₩WINDOWS₩image.jpg	높음
접속 사이트 수	16개 사이트	19개 사이트	19개 사이트	-