이스트시큐리티

보안 동향 보고서

No.144 2021.09

No.144 2021.09

이스트시큐리티 보안 동향 보고서

CONTENTS

01
악성코드 통계 및 분석

악성코드 동향

알약 악성코드 탐지 통계

랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1. 악성코드 동향

2021 년 8 월에는 국내외적으로 개인정보 유출 사건이 많이 발생하였으며, 유출된 개인정보들이 다크웹에서 많이 판매되는 정황이 포착되었습니다.

지난 6 월, EA 의 네트워크가 해킹되어 데이터들이 탈취되었습니다. 이렇게 탈취된 데이터들이 사이버 범죄 포럼에서 공개되었으며, 이 데이터의 사본들이 또 다른 언더그라운드 해커 포럼에서 게시되었습니다.

또한 T-Mobile 이 공격을 당해 1 억 명이 넘는 미국 고객의 개인정보가 유출되었으며, Nokia 의 자회사가 Conti 랜섬웨어의 공격을 받아 250GB 의 데이터가 유출되고 시스템이 암호화 되었습니다.

또한 Puma 에서 탈취된 것으로 추정되는 데이터가 Marketo 다크웹에서 판매 중이며, 중국의 모바일 게임회사 EskyFun 에서 데이터 유출 사고가 발생하여 100 만 명이 넘는 게임 사용자의 정보가 유출되었습니다.

넷플릭스(Netflix), 티빙(Tving), 왓챠(Whtcha) 등 OTT 서비스 계정 정보도 다크웹에서 거래되고 있어 부정 사용 우려와 함께 2 차 피해 가능성도 제기되고 있습니다.

국내에서는 샤넬코리아와 키움예스저축은행, 서울성모병원이 해킹 공격을 받아 고객정보가 유출되었으며, 에듀테크 기업회원 정보가 다크웹에서 판매되는 정황이 포착되었습니다. 뿐만 아니라 조선일보에서 직원 이메일 해킹 시도가 있었으며, 피싱 메일 및 스미싱을 통해 일반 사용자들의 개인정보를 노린 공격도 끊임없이 발생하고 있습니다.

개인정보가 유출되면, 유출된 개인정보를 악용하여 부정 결제나 대출 등의 2 차 피해를 입을 수 있으며, 유출된 개인정보들을 조합하여 더 정교한 사이버 공격을 진행할 수 있어 각별한 주의가 요구되고 있습니다.

기업들은 보유하고 있는 데이터의 식별 및 분류를 데이터의 현황을 정확히 파악하고, 개인정보와 같은 민감 데이터들은 따로 분리하여 암호화, 접근제어 등의 높은 수준의 보호 조치를 적용해야 합니다. 일반 사용자들 역시 주기적으로 비밀번호를 변경하고, 로그인 시 2 단계 인증을 사용하여 자신의 계정 정보를 보호하려는 노력을 해야합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2021 년 8 월의 감염 악성코드 Top 15 리스트에서는 지난달에 이어 Heur.BZC.ONG.Pantera.14.C76F5E25 가 1 위를 차지했다. 이번 달에는 큰 순위 변동폭을 보여준 Gen:Variant.Razy.767621 과 Gen:Variant.Doina.18540 을 제외하고는 전체적으로 지난달과 유사한 순위를 나타냈다. 또한 Gen:Variant.Cerbu.109340 을 비롯한 5 건의 악성코드가 새롭게 Top 15 에 이름을 올렸다.

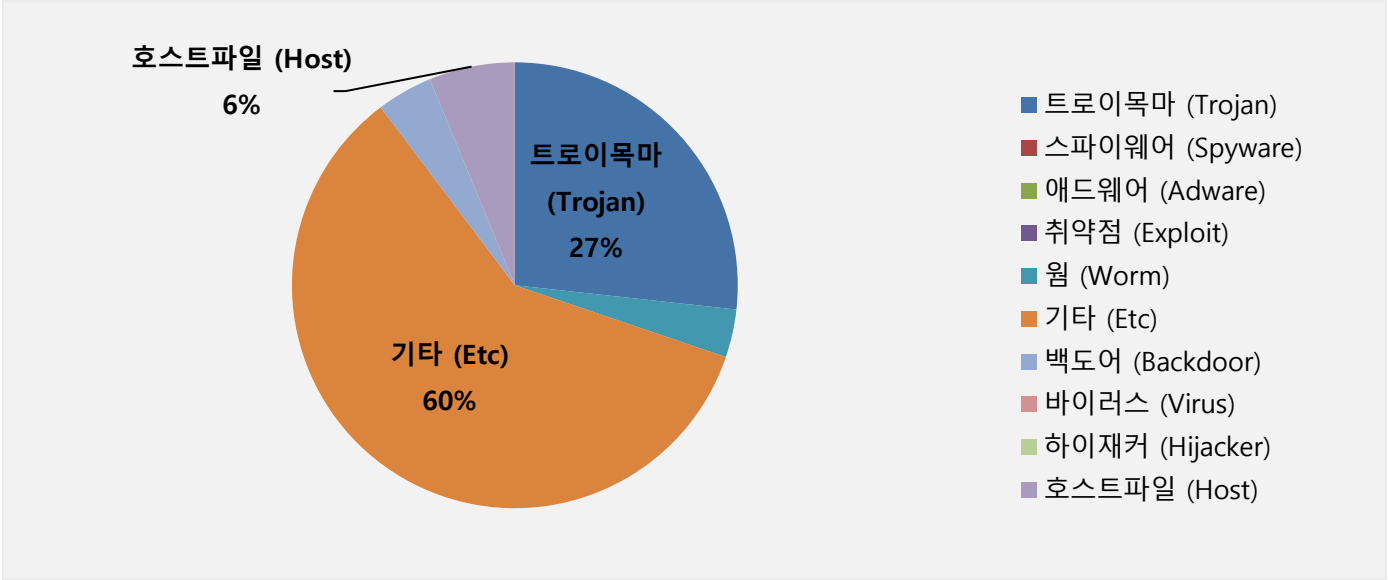
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Heur.BZC.ONG.Pantera.14.C76F5E25	ETC	1,048,538
2	New	Gen:Variant.Cerbu.109340	ETC	872,352
3	-	Trojan.GenericFCA.Agent.7232	Trojan	386,500
4	↑ 9	Gen:Variant.Razy.767621	ETC	359,599
5	↓ 1	Hosts.media.opencandy.com	Host	358,506
6	New	Trojan.GenericKD.46718480	Trojan	337,880
7	New	Trojan.ShadowBrokers.A	Trojan	333,243
8	↑ 1	Misc.Riskware.Segurazo	ETC	312,322
9	↓ 2	Misc.HackTool.AutoKMS	ETC	281,846
10	↓ 8	Gen:Variant.Doina.18540	ETC	278,440
11	↓ 6	Heur.BZC.YAX.Linx.15.05E78B67	ETC	270,994
12	-	Trojan.Agent.Injector.Gen	Trojan	243,451
13	↑ 1	Trojan.Agent.Zpevdo.A	Trojan	237,831
14	New		Backdoor.Generic.792814	Backdoor
15	New	Worm.ACAD.Bursted	Worm	200,254

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2021 년 08 월 01 일 ~ 2021 년 08 월 31 일

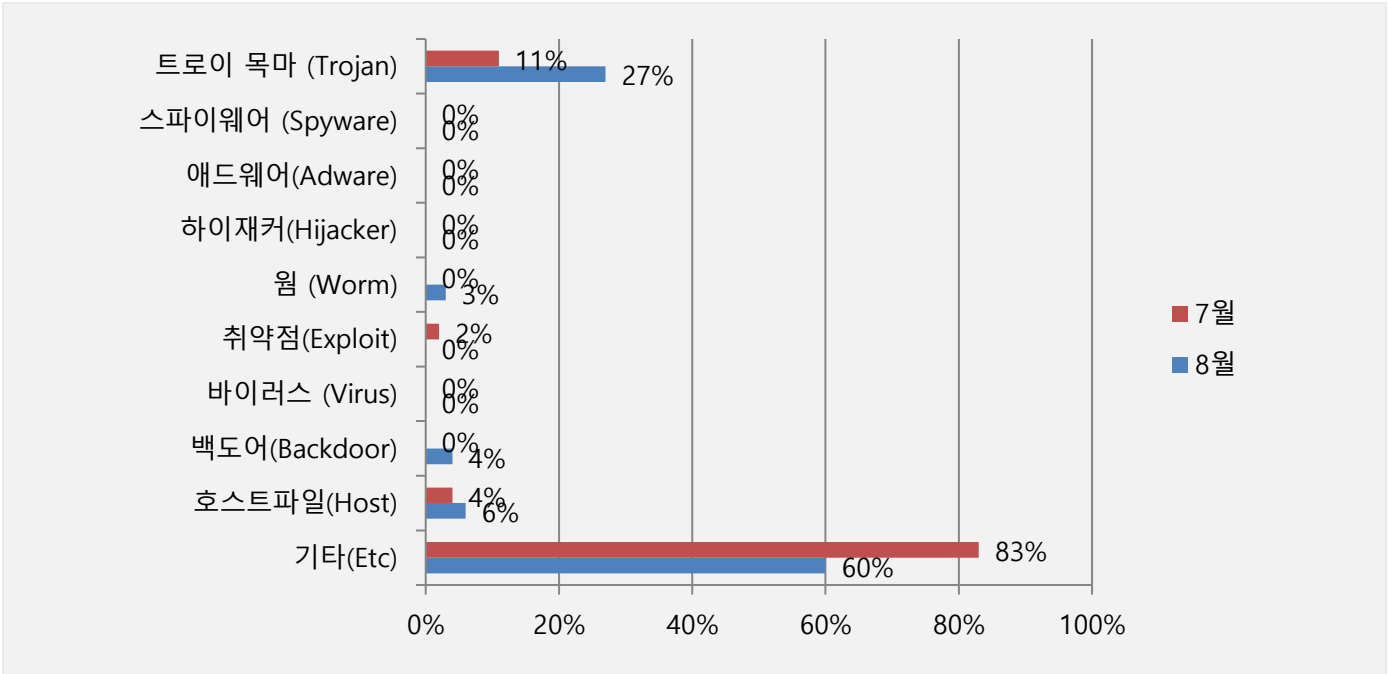
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 가장 많은 60%를 차지했으며 트로이목마(Trojan) 유형과 호스트파일(Host) 유형이 각각 27%와 6%로 그 뒤를 이었다. 지난달 낮은 탐지율을 기록했던 웜(Worm) 유형과 백도어(Backdoor) 유형이 약간 증가하여 각각 3%와 4%를 기록했다. 2021 년 7 월과 비교하여 전체 감염 건수는 약 55.45% 감소하였다.



카테고리별 악성코드 비율 전월 비교

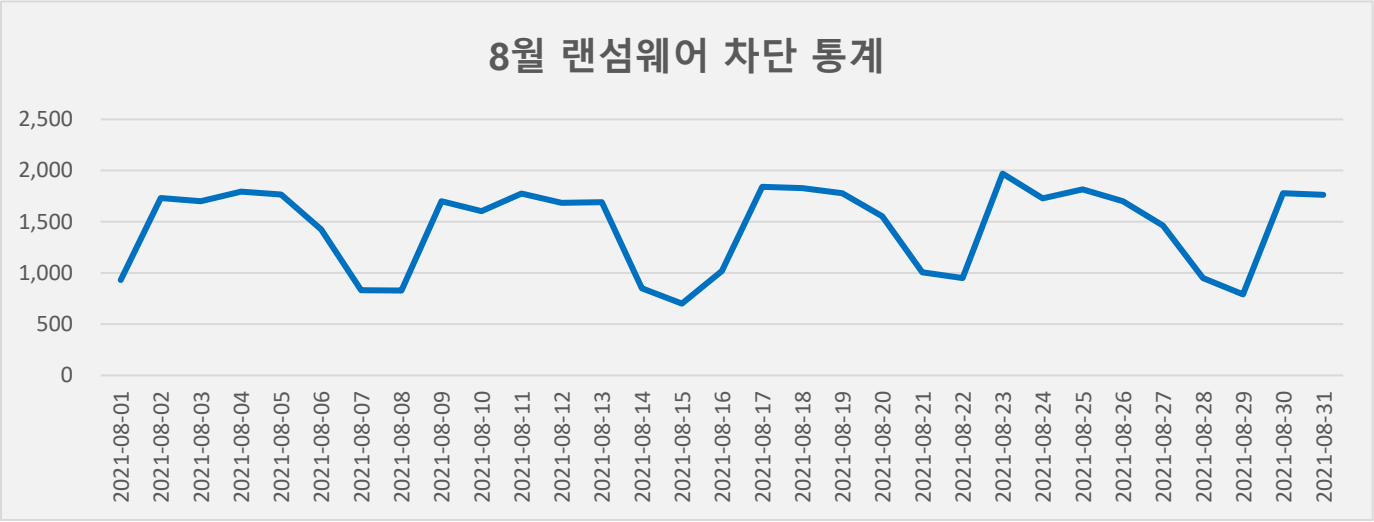
8 월에는 지난 7 월과 비교하여 트로이목마(Trojan) 유형이 16% 증가하였으며, 호스트파일(Host) 유형의 악성코드 감염 비율이 2% 증가했다. 7 월에 2%를 차지했던 취약점 익스플로잇(Exploit) 유형이 이번 달에는 낮은 탐지율을 기록하여 Top15 탐지명에 기록되지 못했다. 반면에 지난달에 낮은 탐지율을 보였던 웜(Worm) 유형과 백도어(Backdoor) 유형이 이번 달에는 다수 탐지되며 전월과 비교하여 크게 상승폭을 보였다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

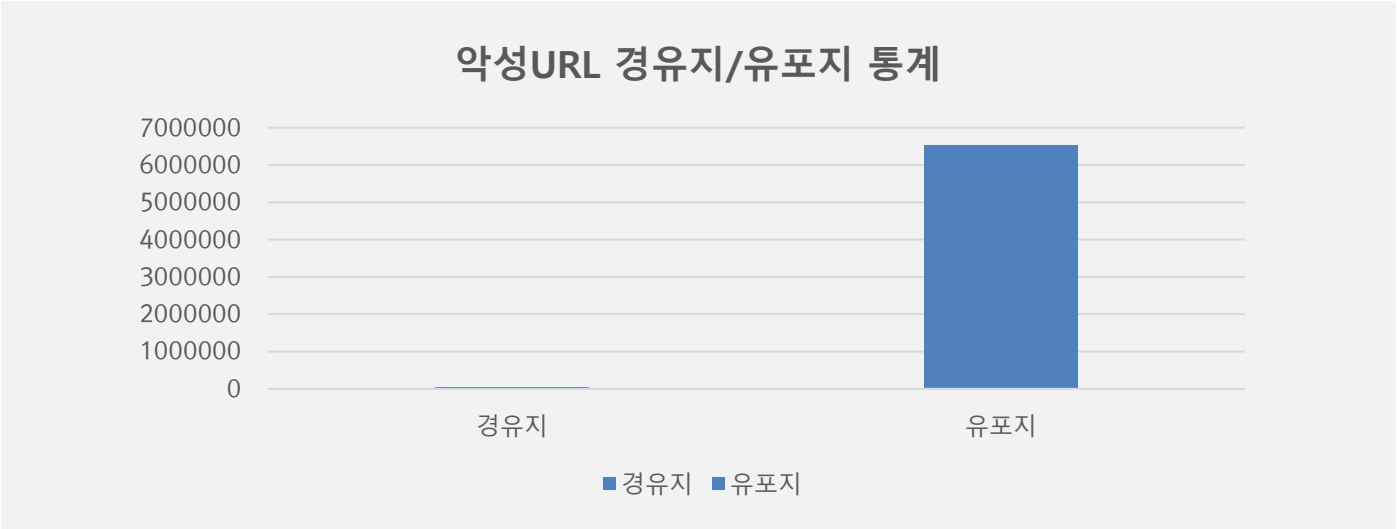
8 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않는다. 8 월 1 일부터 8 월 31 일까지 총 44,962 건의 랜섬웨어 공격 시도가 차단되었다. 7 월의 랜섬웨어 공격 건수인 52,653 건에 비해 약 14.61% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 8 월 한 달간 총 6,561,087 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 7 월 한 달간 확인되었던 6,594,647 의 악성코드 경유지/유포지 URL 수에 비해 약 0.51% 가량 감소한 수치다. 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 바란다.



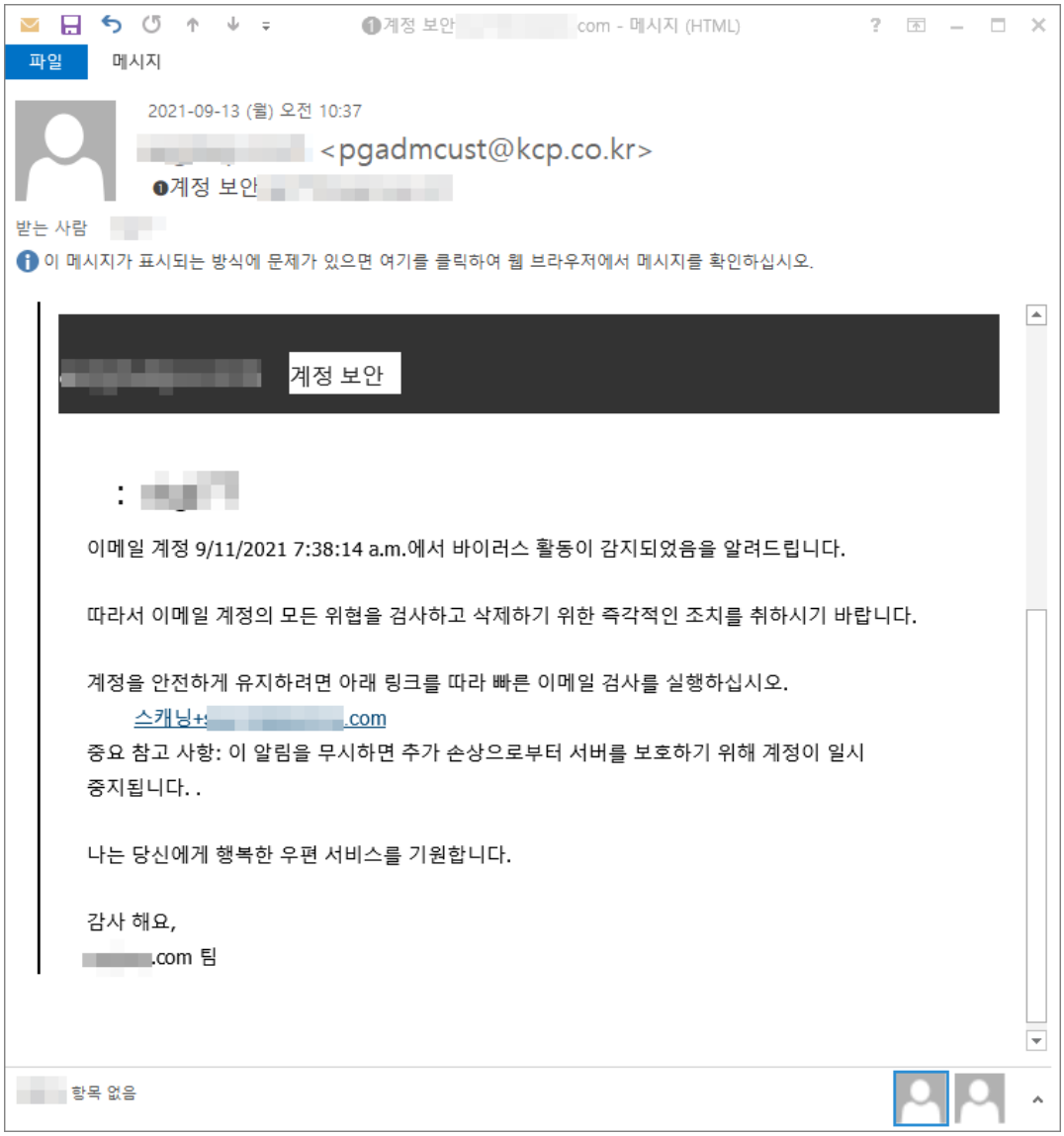
02
전문가 보안 기고

1. '이메일 바이러스 체크'로 위장한 피싱 메일 유포 주의!
2. 정상 한글 파일이 포함된 피싱 메일로 유포 중인 Lokibot 주의!

1. ‘이메일 바이러스 체크’로 위장한 피싱 메일 유포 주의!

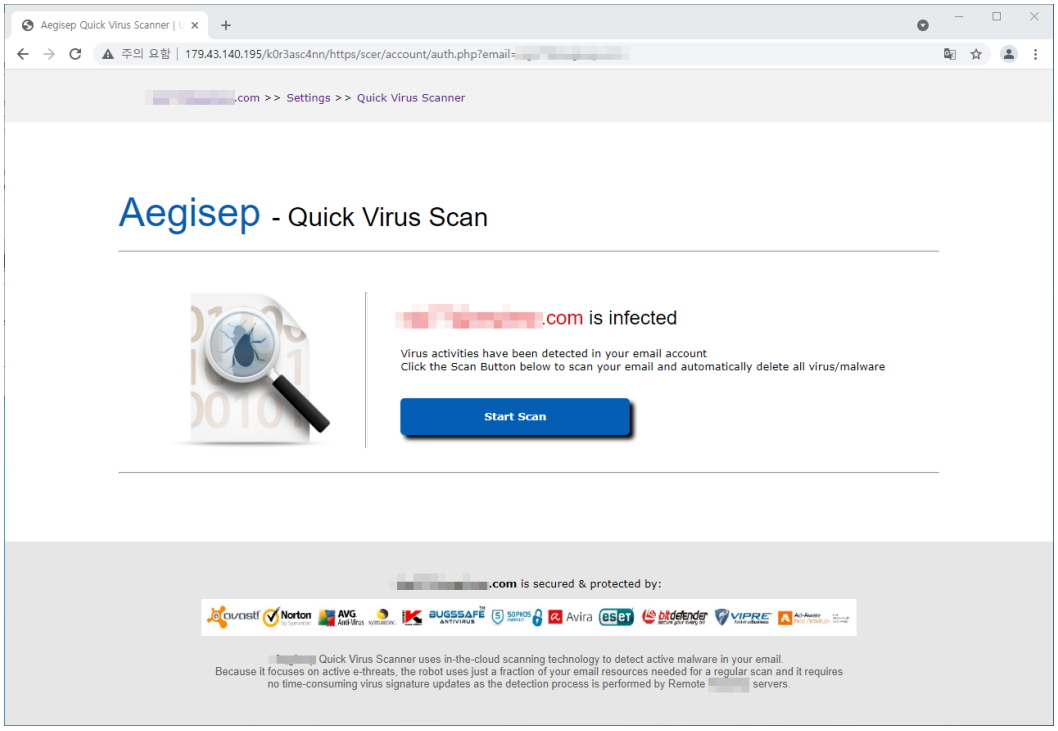
수신된 이메일에서 바이러스 활동이 감시되어 이메일 검사를 진행하라는 내용의 피싱 공격이 발견되어 사용자들의 주의가 필요합니다.

이번에 발견된 메일은 "계정 보안 [이메일주소]” 라는 제목이 사용되었으며, 사용 중인 이메일 계정에서 바이러스 활동이 감지되어 계정 안전을 위해 본문에 표기된 링크를 클릭하여 이메일 검사를 유도하고 있습니다. 특히 발신자 주소가 한국 사이버결제사에서 보낸 것처럼 위장하여 사용자의 의심을 피하려 했습니다.



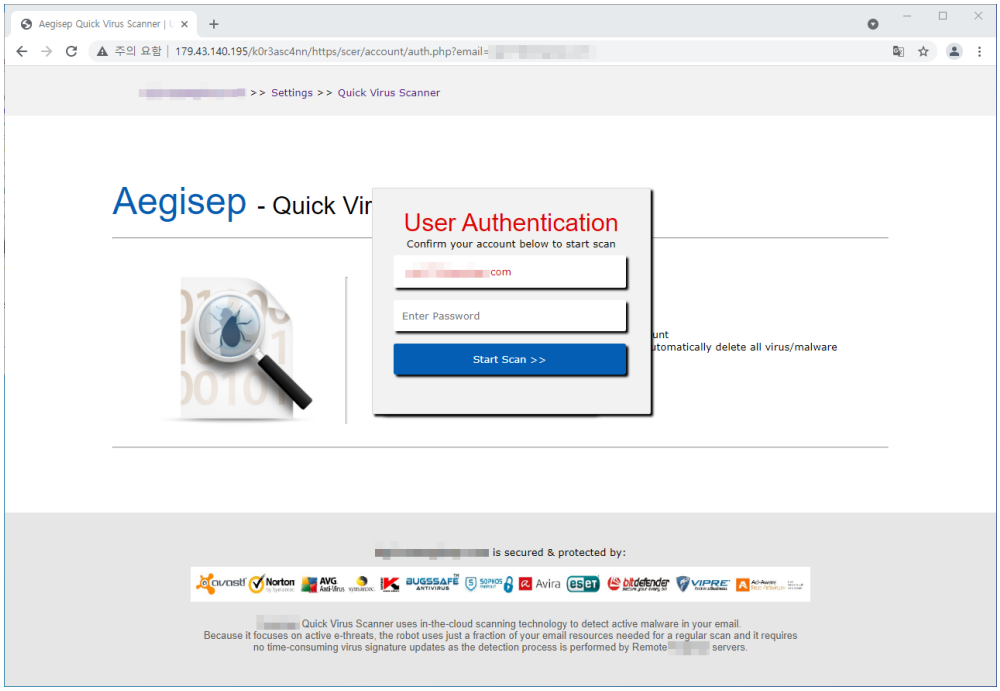
[그림 1] 이메일 바이러스 검사 요청 관련 피싱메일 화면

사용자가 이메일 바이러스 검사를 위해 본문에 기재 된 스캐닝 주소를 클릭하면 로그인 계정과 패스워드를 탈취하는 피싱 사이트로 이동하게 됩니다.



[그림 2] 사용자 이메일의 감염을 알리는 피싱사이트 초기 화면

피싱사이트에 접속되면 사용자의 이메일이 감염되었다는 문구가 표시되며, 정상적인 바이러스 스캔 사이트인 것처럼 정교하게 제작되어 있습니다.



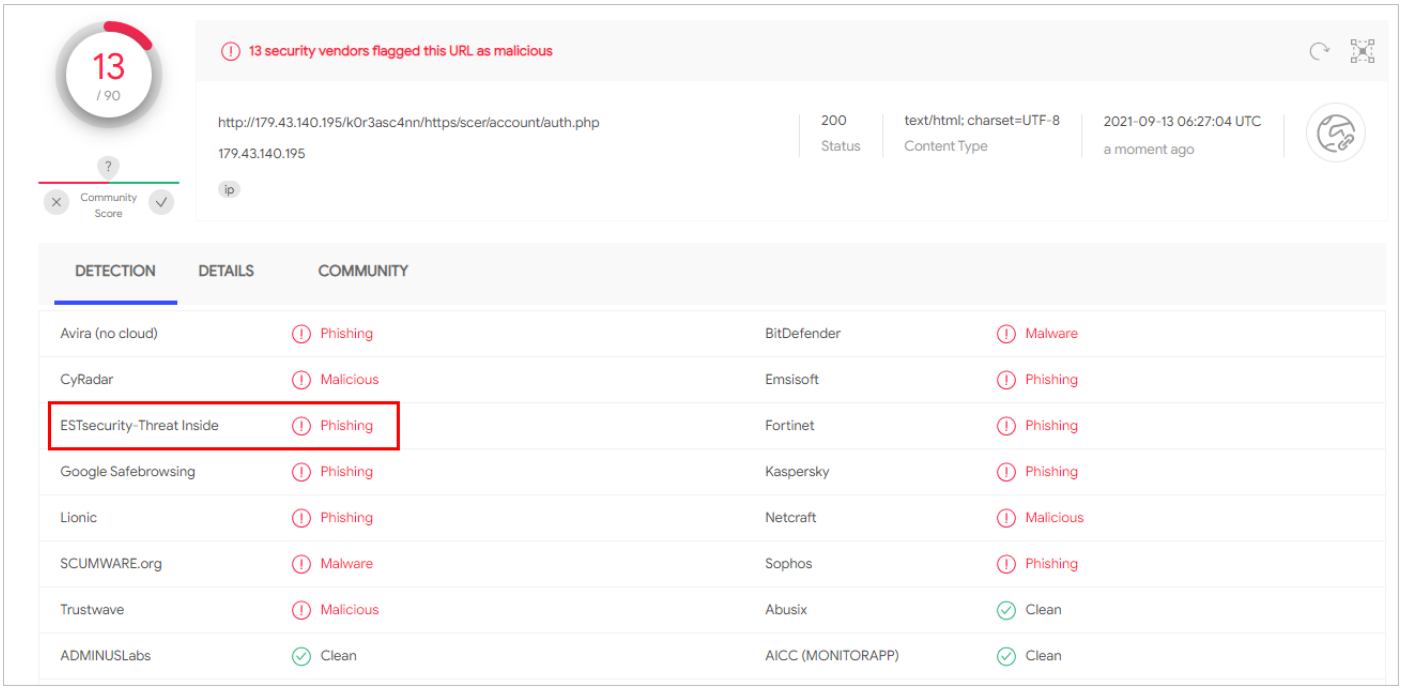
[그림 3] 사용자의 개인정보를 탈취하기 위한 피싱사이트 화면

02 전문가 기고

피싱 사이트에 입력한 사용자의 계정 / 패스워드는 아래 공격자 서버로 전달됩니다.

- 개인정보 피싱 및 수집 사이트
hxxp://179.43.140[.]195/k0r3asc4nn/https/scer/account/auth.php
hxxp://179.43.140[.]195/k0r3asc4nn/https/scer/account/ray.php

현재 이스트시큐리티 '쓰렛 인사이드(Threat Inside)'에서는 해당 피싱 사이트를 아래와 같이 탐지하고 있습니다.



[그림 4] ESTSecurity-Threat Inside 개인정보 수집 사이트 탐지 화면

2. 정상 한글파일이 포함된 피싱 메일로 유포중인 Lokibot 주의!

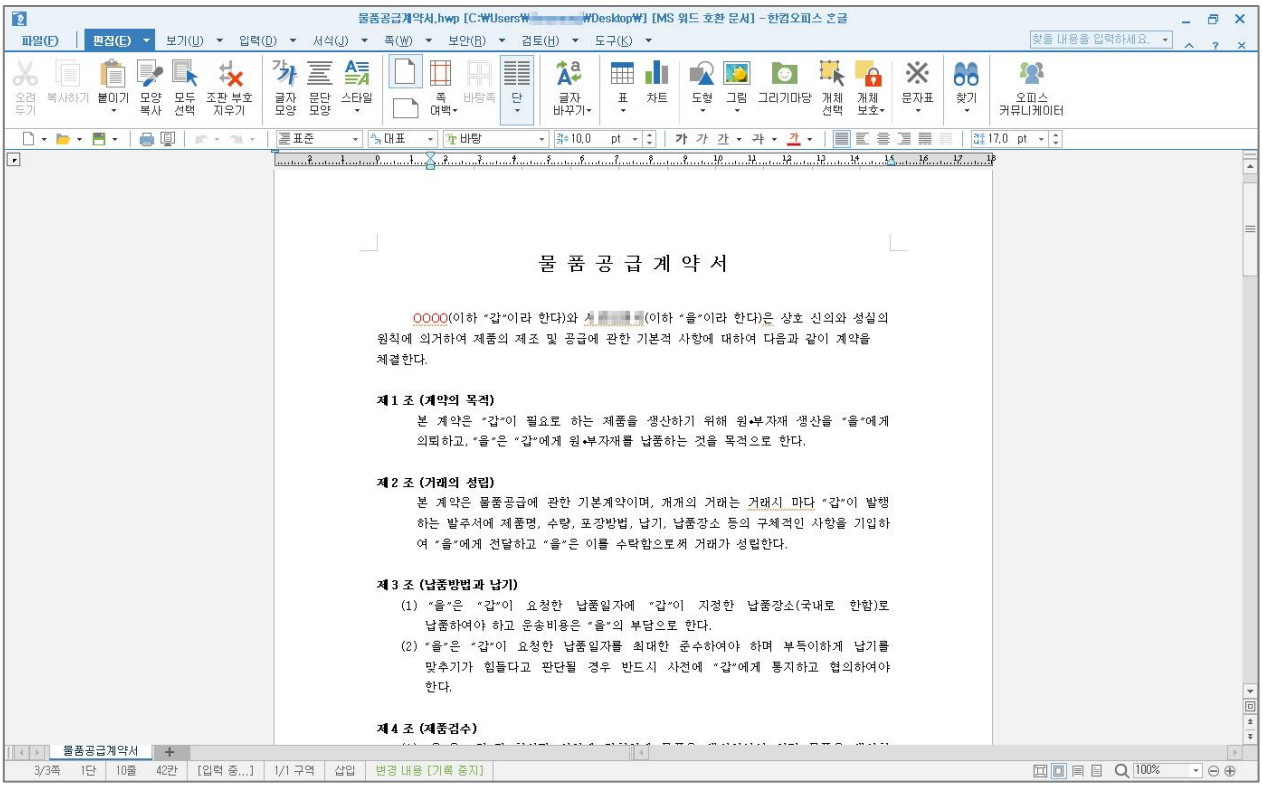
피싱 메일을 통해 꾸준히 유포되고 있는 Lokibot 이 피싱 메일의 형태를 변경하여 유포중에 있습니다.

이번에 발견된 피싱 메일은 물품공급계약서를 위장하고 있으며 2 개 파일이 첨부되어 있습니다.

[그림 1] 물품공급계약서를 위장한 피싱 메일

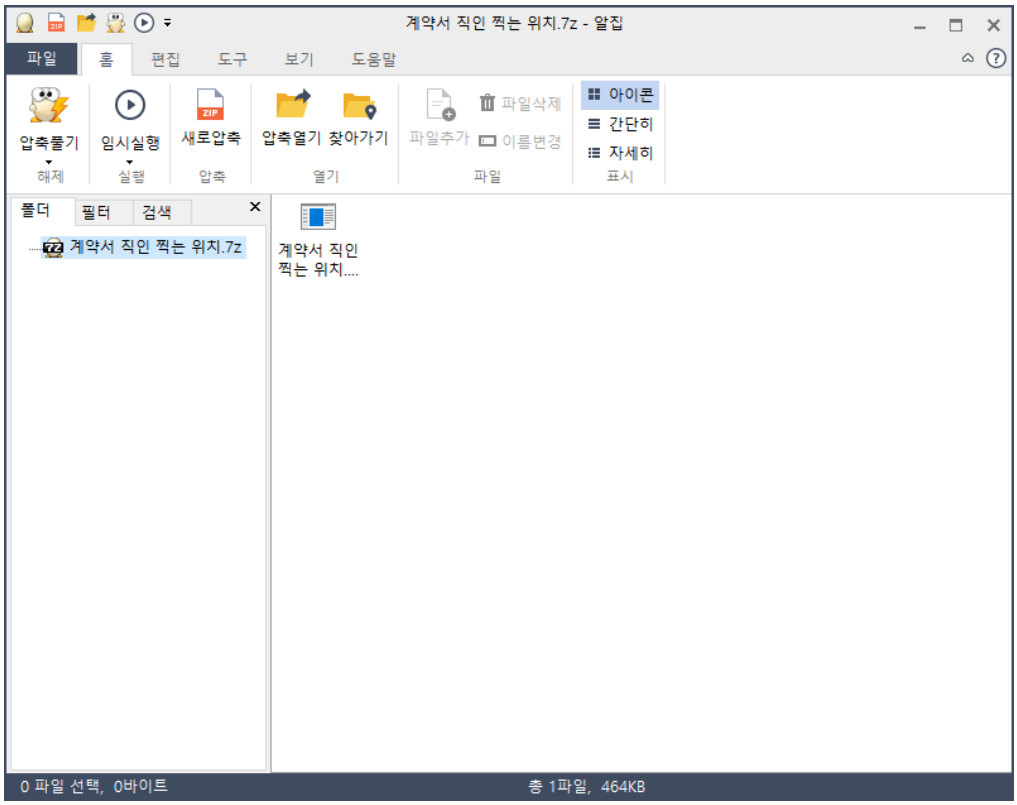
이메일 내용은 거래를 위하여 물품공급계약서를 받고 있다며, 첨부되어있는 '물품공급계약서' 파일명의 한글 파일을 실행하도록 유도합니다. 또한 직인 찍는 메뉴얼이라면서 '계약서 직인 찍는 위치.7z' 압축파일을 실행하도록 유도합니다.

한글 파일은 정상 파일로, 내부에는 일반적인 계약서 내용이 작성되어 있습니다.



[그림 2] 피싱 메일에 포함되어 있는 정상 한글 파일

압축파일 내에는 정상파일을 위장한 .exe 파일이 포함되어 있으며, 만약 사용자가 해당 파일의 압축을 해제한 후 클릭하면 Lokibot 악성코드가 실행되게 됩니다.



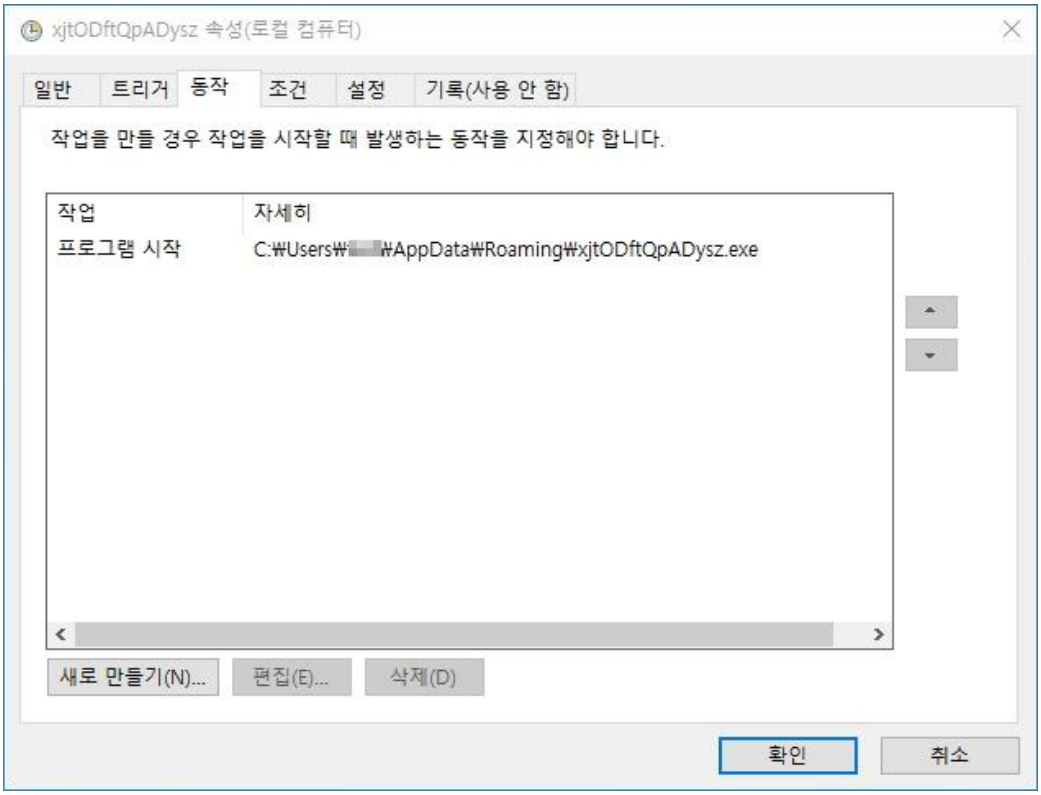
[그림 3] 피싱 메일에 포함되어 있는 악성 파일

02 전문가 기고

Lokibot 이 실행되면 사용자 PC 정보와 함께 웹 브라우저, 메일 클라이언트, FTP 프로그램 등에 저장해 놓은 계정 비밀번호를 탈취하여 공격자의 C&C 서버로 전송합니다.

C&C 서버 정보
hxxp://23[.]254.225.235/ogaa/fre.php

또한 사용자 PC 에서 오랫동안 살아남기 위하여 스케줄러에 자신을 등록하여 사용자 PC 실행 시 자동으로 실행되도록 합니다.



[그림 4] 스케줄러 등록

이번에 발견된 피싱 메일의 경우, 기존 피싱 메일과 다르게 정상 한글파일을 함께 첨부하여 사용자들의 의심을 피하고자 했습니다.

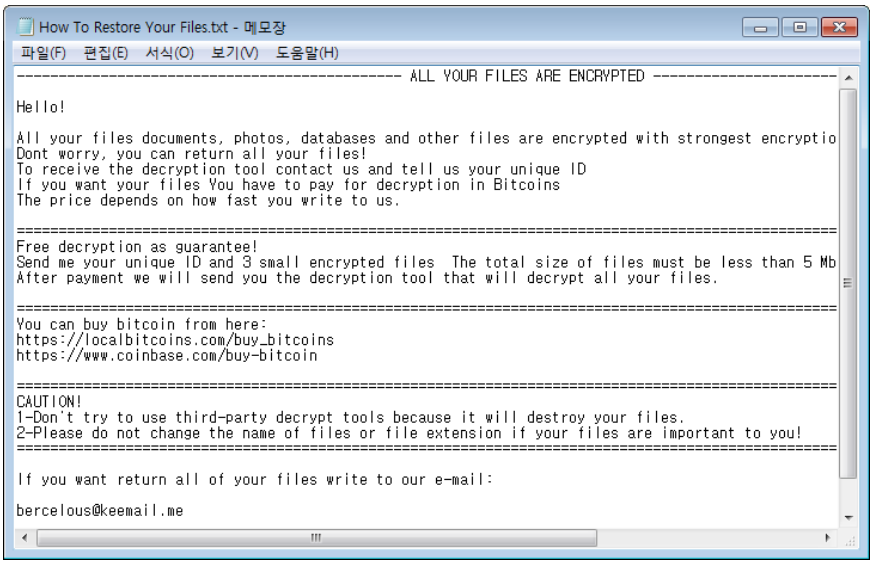
사용자 여러분들은 출처가 불분명한 사용자에게서 온 메일에 포함된 링크 클릭이나 첨부파일 실행을 지양해 주시기 바라며, 링크 클릭 혹은 첨부파일 실행 전 미리보기를 통해 링크 주소 및 파일 확장자를 확인해야 합니다. 현재 알약에서는 해당 악성코드에 대해 Spyware.Lokibot 으로 탐지중에 있습니다.

03
악성코드 분석 보고

[Trojan.Ransom.Babuk] 악성코드 분석 보고서

2021 년 올해 첫 새로운 랜섬웨어 패밀리가 발견되었다. 이름은 바북 락커(Babuk Locker)이고 지난 4 월 워싱턴 DC 경찰서에 침투해 파일을 암호화하고 협박 한 것으로 유명하다.

그러나 얼마 지나지 않아 운영을 중단한 후 5 월 말 PayloadBin 으로 리브랜딩한 Babuk 랜섬웨어의 소스코드가 한 러시아 해킹 포럼에 게시되었다.



[그림] 랜섬노트 화면

Babuk 랜섬웨어는 사용자 PC 의 데이터를 암호화하여 금전을 요구하는 악성코드이다. 서비스형 랜섬웨어(RaaS)로 암호화 대상 파일 크기에 따라 암호화 파일 구조가 달라지는 점이 특징이다.

또한 로컬 드라이브와 네트워크 드라이브로 연결된 모든 파일을 암호화 대상에 포함하고 C&C 연결을 하지 않아도 암호화되기 때문에 보안을 위해 폐쇄망을 사용하는 기업들도 랜섬웨어 공격에 더 큰 주의를 기울여야 한다.

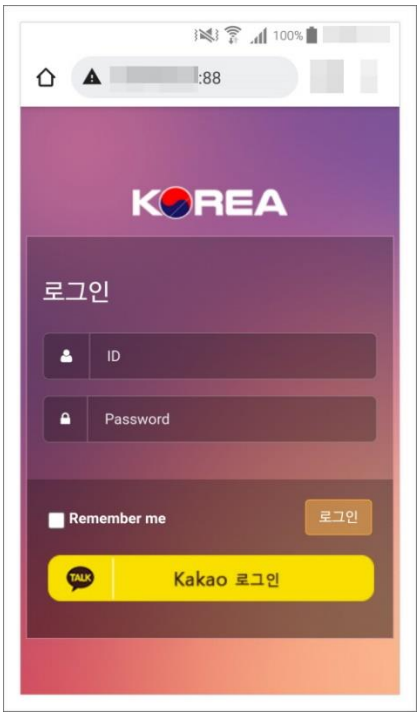
따라서 랜섬웨어를 예방하기 위해서는 기본 보안 수칙을 준수하고, 윈도우, 애플리케이션을 최신으로 업데이트 해야 한다. 또한 중요한 자료는 정기적으로 외장 매체나 클라우드 서비스 등에 백업해서 피해를 최소화할 수 있도록 해야 한다.

현재 알약에서는 해당 악성코드를 'Trojan.Ransom.Babuk' 탐지 명으로 진단하고 있으며, 관련 상세 분석 보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

[Spyware.Android.Agent] 악성코드 분석 보고서

몸캠 피싱 공격은 스미싱과 같은 다른 공격들에 비해 공격 빈도가 낮은 편이지만 지속적으로 공격이 이루어지고 있으며 최근까지도 변종이 꾸준히 발견되고 있다.

몸캠 피싱은 스마트폰 채팅 앱(랜덤채팅)을 통해 피해자를 찾으며 음란 화상 채팅을 유도하여 피해자의 음란 행위를 녹화한다. 그리고 피해자의 스마트폰에 악성 앱 설치를 유도하여 피해자의 연락처를 탈취한다. 이후 음란 행위 영상을 지인들에게 유포하겠다는 협박을 통해 금전을 갈취한다.



[그림] 악성 앱 실행 시 화면

몸캠 피싱은 피해자의 음란 영상과 함께 피해자의 지인 연락처가 있어야 협박이 가능하기에 악성앱을 설치하지 않는다면 공격자의 협박을 막을 수 있다. 따라서, 출처가 불명확한 URL 과 파일은 실행하지 않아야 하며 주변 기기의 비밀번호를 자주 변경하고 백신 애플리케이션을 설치하여 항상 최신 업데이트 버전으로 유지하는 것이 위협으로부터 자신을 지키는 첫 걸음이라 할 수 있을 것이다.

현재 알약 M 에서는 해당 앱을 'Spyware.Android.Agent' 탐지 명으로 진단하고 있으며, 관련 상세 분석 보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

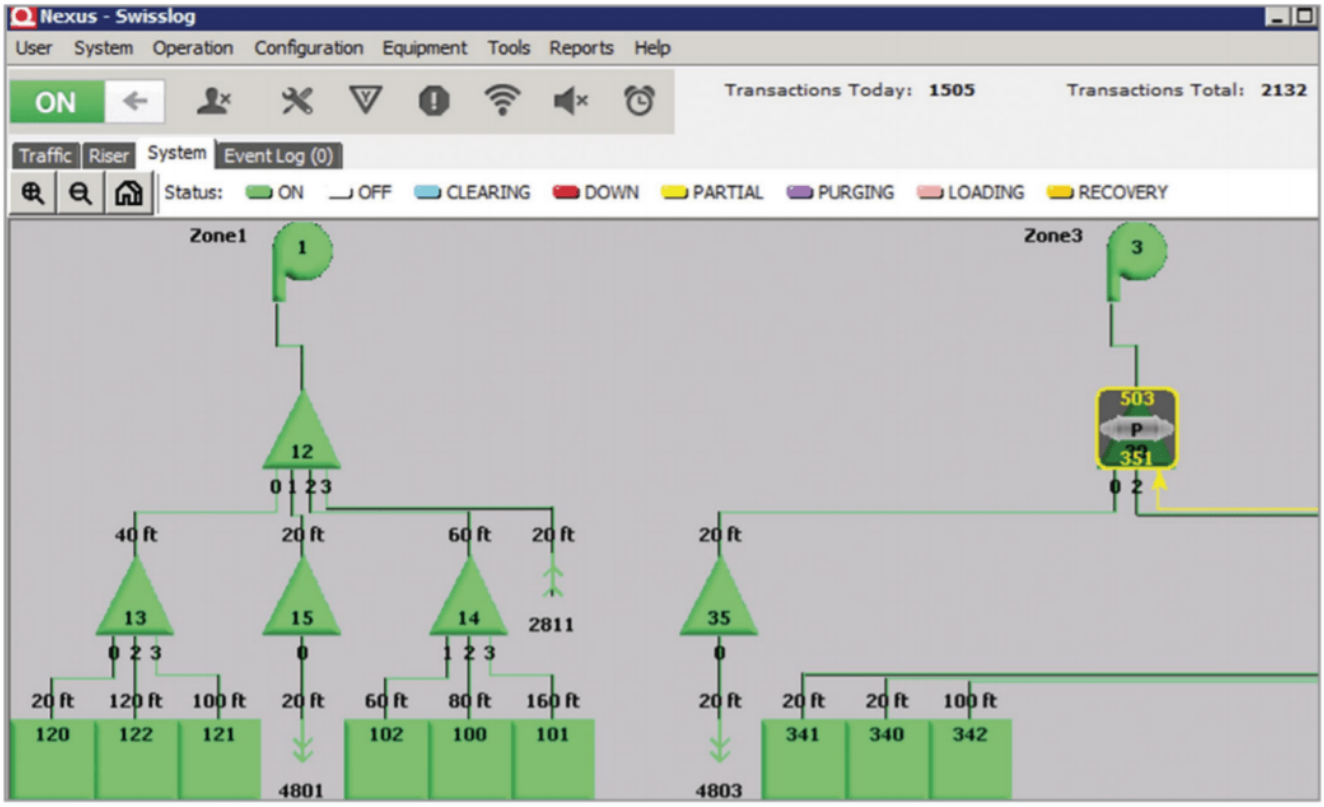
04
글로벌 보안 동향

PTS 시스템의 PwnedPiper 취약점, 미 주요 병원 80%에 영향 미쳐

PwnedPiper flaws in PTS systems affect 80% of major US hospitals

사이버 보안 회사인 Armis 의 연구원들이 널리 사용되는 PTS(Pneumatic Tube System, 기송관)에 다양한 공격을 실행하는데 악용될 수 있는 PwnedPiper 라 명명된 취약점 9 개를 발견했다. Swisslog PTS 시스템은 병원에서 공압 튜브 네트워크를 통해 건물 전체에 물류 및 자재 운송을 자동화하는데 사용된다. 이 취약점은 북미 주요 병원의 약 80%, 전 세계 병원 수천 곳에 설치된 Swisslog Healthcare 의 Translogic PTS 시스템에 영향을 미친다.

공격자는 PwnedPiper 취약점을 악용해 Translogic PTS 의 최신 모델에 전원을 공급하는 Translogic Nexus Control Panel 의 제어권을 완전히 탈취할 수 있었다. 공격자는 이 취약점을 악용해 중간자 공격을 실행해 시스템을 변경하거나, 랜섬웨어를 배포하는 등 다양한 공격을 실행할 수 있다. “이러한 취약점을 통해 인증되지 않은 공격자가 Translogic PTS 스테이션을 점령해 타깃 병원의 PTS 네트워크를 완전히 제어할 수 있다. 이러한 제어권을 얻을 경우 교묘한 랜섬웨어 공격을 실행할 뿐 아니라 병원의 민감 정보를 유출하는 것도 가능하다.”



[이미지 출처] https://www.armis.com/research/pwnedpiper

이 취약점은 권한 상승, 메모리 충돌, 원격 코드 실행, 서비스 거부 이슈를 포함하고 있다. 공격자는 안전하지 않은 펌웨어 업그레이드를 푸시해 기기를 완전히 해킹할 수도 있다. 연구원들이 발견한 취약점 9 가지는 아래와 같다.

CVE-2021-37161 – udpRXThread 내 언더플로우
CVE-2021-37162 – sccProcessMsg 내 오버플로우
CVE-2021-37163 – Telnet 서버를 통해 접근 가능한 하드코딩된 비밀번호 2 개
CVE-2021-37164 – tcpTxThread 내 Off-by-3 스택 오버플로우
CVE-2021-37165 – hmiProcessMsg 내 오버플로우
CVE-2021-37166 – GUI 소켓 서비스 거부
CVE-2021-37167 – 루트로 실행되는 사용자 스크립트를 PE 에 사용할 수 있는 오류
CVE-2021-37160 – 인증되지 않고, 암호화되지 않고, 서명되지 않은 펌웨어 업그레이드

[출처]
https://securityaffairs.co/wordpress/120741/hacking/pwnedpiper-flaws-pts-systems.html

BlackMatter 의 리눅스 버전, VMware ESXi 서버 노려

Linux version of BlackMatter ransomware targets VMware ESXi servers

BlackMatter 랜섬웨어 공격 그룹이 VMware 의 ESXi 가상 머신 플랫폼을 노리는 리눅스용 암호화 툴을 개발하기 위한 대열에 들어선 것으로 나타났다. 기업은 더 나은 리소스 관리 및 재해 복구를 위해 서버용 가상 머신을 점점 더 많이 사용하고 있다. 이 중 VMware ESXi 가 가장 인기 있는 가상 머신 플랫폼이기 때문에, 기업을 노리는 거의 모든 랜섬웨어들이 가상 머신을 노리는 암호화 툴을 개발하기 시작했다.

- VMware ESXi 를 노리는 BlackMatter

8 월 4 일, MalwareHunterTeam 의 보안 연구원이 BlackMatter 랜섬웨어 그룹의 리눅스 ELF64 암호화 툴을 발견했다. 기능을 살펴본 결과, 이는 VMware ESXi 서버를 노리도록 설계되었다. BlackMatter 는 지난달 활동을 시작한 비교적 새로운 랜섬웨어로 DarkSide 가 리브랜딩한 것으로 추측된다. 샘플 분석 결과, 해당 랜섬웨어가 사용하는 암호화 루틴이 DarkSide 에서 사용하는 것과 동일한 것으로 확인되었다. DarkSide 는 Colonial Pipeline 을 공격 및 폐쇄시킨 후 국제 집행 기관과 미국 정부의 총체적인 압력을 받은 후 활동을 중단했다.

Bleeping Computer 와 공유된 BlackMatter 의 리눅스 암호화 툴 샘플을 분석한 결과, VMWare ESXi 서버만을

노리도록 설계되었음을 확인했다. Advanced Intel 의 Vitali Kremez 는 샘플을 리버스 엔지니어링한 결과, 공격자가 VMware ESXi 서버에서 다양한 작업을 수행하는 데 사용되는 'esxi_utils' 라이브러리를 생성했다고 설명했다.

/sbin/esxcli
bool app::esxi_utils::get_domain_name(std::vector)&)
bool app::esxi_utils::get_running_vms(std::vector)&)
bool app::esxi_utils::get_process_list(std::vector)&)
bool app::esxi_utils::get_os_version(std::vector)&)
bool app::esxi_utils::get_storage_list(std::vector)&)
std::string app::esxi_utils::get_machine_uuid()
bool app::esxi_utils::stop_firewall()
bool app::esxi_utils::stop_vm(const string&)

Kremez 는 각 기능이 esxcli 커맨드라인 관리 도구를 사용해 VM 나열, 방화벽 중지, VM 중지와 같은 다른 명령을 실행할 것이라고 말했다. 예를 들어, stop_firewall() 함수는 다음의 명령을 실행한다.

esxcli network firewall set --enabled false

stop_vm()은 다음의 esxcli 명령을 실행한다.

esxcli vm process kill --type=force --world-id [ID]

ESXi 서버를 노리는 모든 랜섬웨어는 드라이브를 암호화하기 전 가상 머신을 먼저 종료하려고 시도한다. 이는 데이터가 암호화되는 동안 데이터 손상을 방지하기 위함이다. 모든 VM 이 종료된 후에는 랜섬웨어에 포함된 구성을 기반으로 특정 파일 확장자와 일치하는 파일을 암호화한다.

공격자가 단일 명령으로 여러 서버를 한 번에 암호화할 수 있기 때문에 ESXi 서버를 노리는 것은 랜섬웨어 공격에 매우 효율적이다. 더 많은 기업이 서버용으로 이러한 유형의 플랫폼으로 변경함에 따라, 랜섬웨어 개발자는 ESXi 를 대상으로 하는 전용 리눅스 암호화 툴을 계속해서 개발할 것이다.

[출처]
https://www.bleepingcomputer.com/news/security/linux-version-of-blackmatter-ransomware-targets-vmware-esxi-servers/

LockFile 랜섬웨어, 간헐적 파일 암호화 통해 탐지 우회해

LockFile Ransomware Bypasses Protection Using Intermittent File Encryption

지난달 새롭게 등장한 랜섬웨어 패밀리가 새로운 기술인 “부분 암호화”를 통해 랜섬웨어 탐지 기술을 우회하는 것으로 나타났다. LockFile 이라 명명된 이 랜섬웨어는 최근 공개된 취약점인 ProxyShell 과 PetitPotam 을 악용하여 윈도우 서버를 해킹하고 랜섬웨어를 배포한다. 이 랜섬웨어는 파일의 16 바이트만 암호화하여 랜섬웨어 탐지 기술을 우회한다. Sophos 의 기술 이사인 Mark Loman 은 이에 대해 다음과 같이 설명했다. “부분 암호화 기술은 일반적으로 랜섬웨어에서 암호화 프로세스의 속도를 높이기 위해 사용하며 BlackMatter, DarkSide, LockBit 2.0 에서 찾아볼 수 있었다. LockFile 의 차별화된 점은 다른 랜섬웨어와는 달리 처음 블록 일부를 암호화하지 않는다는 것이다. 대신 이는 문서의 다른 부분의 16 바이트를 암호화한다. 이를 통해 텍스트 문서와 같은 파일 종류는 부분적으로 읽을 수 있으며, 통계적으로 원본과 유사해 보일 수 있다. 이 전략은 통계 분석을 통해 콘텐츠를 검사하는 랜섬웨어 탐지 소프트웨어를 우회할 수 있다.”

Sophos 는 2021 년 8 월 22 일 VirusTotal 에 업로드된 LockFile 의 구조를 분석했다. 이 악성코드는 일단 설치되면 WMI(Windows Management Interface)를 통해 가상화 소프트웨어 및 데이터베이스와 관련된 중요한 프로세스를 종료하고 중요한 파일 및 개체를 암호화한 후 LockBit 2.0 과 문체가 유사한 랜섬노트를 표시한다.

```
267       uVar8 = uVar18;
268       lVar15 = lVar17;
269       do {
270         local_13e8 = ZEXT816(0);
271         EncryptBuffer_0002cbf4(local_13c0,lVar15,local_13e8,lVar15);
272         lVar15 = lVar15 + 0x20;
273         uVar8 = uVar8 + 1;
274         *(ulonglong *)(lVar16 + 0x208 + lVar17) = uVar8;
275         if (0x4e1fffff < uVar8) break;
276         uVar14 = uVar14 - 1;
277       } while (uVar14 != 0);
278       FUN_00002a30(&local_13c8);
279       (*_UnmapViewOfFileStub_00062040)(lVar17);
280       (*_CloseHandle_00062058)(local_res20);
281       (*_CloseHandle_00062058)(lVar12);
```

[이미지 출처] https://news.sophos.com/en-us/2021/08/27/lockfile-ransomwares-box-of-tricks-intermittent-encryption-and-evasion/

랜섬노트는 사용자에게 "contact@contipauper[.]com" 이메일 주소로 연락할 것을 안내한다. Sophos 는 이에 대해 경쟁 랜섬웨어 그룹인 Conti 를 언급한 것으로 추측했다. 또한 랜섬웨어는 시스템의 모든 문서의 암호화를 마친 후 시스템에서 자체적으로 삭제됩니다. 따라서 사고 대응자나 바이러스 백신 소프트웨어가 찾아 삭제할 랜섬웨어 바이너리가 남아있지 않는다.

[출처]

https://thehackernews.com/2021/08/lockfile-ransomware-bypasses-protection.html

(주)이스트시큐리티

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