이스트시큐리티

보안 동향 보고서

No.143 2021.08

No.143 2021.08

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 7 월에는 대규모 랜섬웨어 해킹사건이 발생하였으며, 새로운 랜섬웨어도 발견되었습니다.

7 월 2 일, Sodinokibi 랜섬웨어 그룹 공격자들이 Kaseya IT 관리 소프트웨어 업데이트를 통해 전 세계 약 40 여 곳에 랜섬웨어 공격을 진행하였습니다. 이번 공격은 Kaseya VSA 를 활용하여 피해자의 환경에 Sodinokibi 랜섬웨어 변종을 유포하고, 바이너리는 가짜 윈도우 디펜더(Windows Defender) 앱을 통해 사이드로드 된 것으로 확인되었습니다. 이번 사건으로 인해 전 세계의 최소 1500 개의 기업이 피해를 받은 것으로 밝혀졌습니다.

하지만 13 일, Sodinokibi 랜섬웨어 공격그룹이 운영하는 웹사이트가 갑작스럽게 폐쇄되었습니다. 이와 관해 법 집행기관의 압력에 의해 운영자가 작업을 중단한 것인지, 법 집행기관에 의해 압수된 것인지는 확인이 되지 않습니다.

7 월 말, Darkside 와 Sodinokibi 등 유명 랜섬웨어의 기능들을 포함한 BlackMatter 랜섬웨어가 등장하였습니다.

국내에서는 유출된 정보들이 해외 다크웹에서 판매되고 있는 사실이 확인되었습니다. 딥웹에서 매출 약 1 조 1000 억원 규모의 한국 자동차 관련 기업의 네트워크 관리자 접근권한을 판매하는 글이 올라왔으며, 연 50 조 한국 대기업의 내부 접근권한도 판매한다는 글이 확인되었습니다.

실제로 최근 재택 근무가 증가하면서 가상 데스크톱 인프라(VDI)나 가상 사설망(VPN)의 계정 탈취를 노린 공격이 자주 발생하고 있습니다.

국내 기업들은 해외 해커들의 다크웹, 딥웹 활동을 주기적으로 모니터링하여 국내 기업들의 정보유출 여부를 신속히 찾아내고 조치하여 추가적인 피해를 막는데 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 7 월의 감염 악성코드 Top 15 리스트에서는 지난달에 Heur.BZC.ONG.Pantera.14.C76F5E25 가 1 위를 차지했다. 이번 달에는 전체적으로 큰 순위 변동은 없었으며, Gen:Variant.Doina.18540 을 비롯한 5 건의 악성코드가 새롭게 Top 15 에 이름을 올렸다. 그 외에 눈에 띄는 부분으로는 Heur.BZC.YAX.Linx.15.05E78B67 이 지난달 순위에서 5 계단 상승하여 5 위를 차지했다.

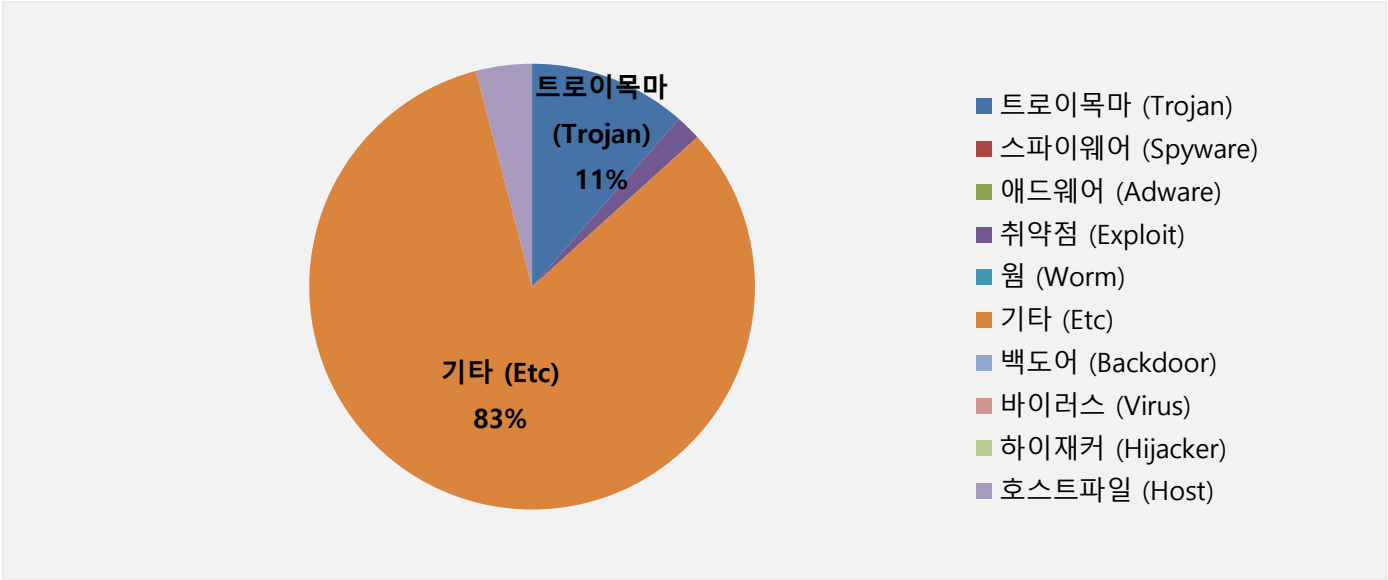
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Heur.BZC.ONG.Pantera.14.C76F5E25	ETC	7,759,715
2	New	Gen:Variant.Doina.18540	ETC	864,131
3	-	Trojan.GenericFCA.Agent.7232	Trojan	563,665
4	↓2	Hosts.media.opencandy.com	Host	524,015
5	↑5	Heur.BZC.YAX.Linx.15.05E78B67	ETC	516,946
6	New	Trojan.Downloader.Script.gen	Trojan	474,942
7	↓2	Misc.HackTool.AutoKMS	ETC	304,595
8	↓4	Misc.Riskware.BitCoinMiner	ETC	276,101
9	New	Misc.Riskware.Segurazo	ETC	272,688
10	New	Gen:Variant.Fugrafa.84058	ETC	256,271
11	↓4	Exploit.CVE-2010-2568.Gen	Exploit	237,962
12	↓3	Trojan.Agent.Injector.Gen	Trojan	228,455
13	-	Gen:Variant.Razy.767621	ETC	218,919
14	New	Trojan.Agent.Zpevdo.A	Trojan	212,705
15	-	Gen:Variant.Application.Keygen.16	ETC	207,629

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2021 년 07 월 01 일 ~ 2021 년 07 월 31 일

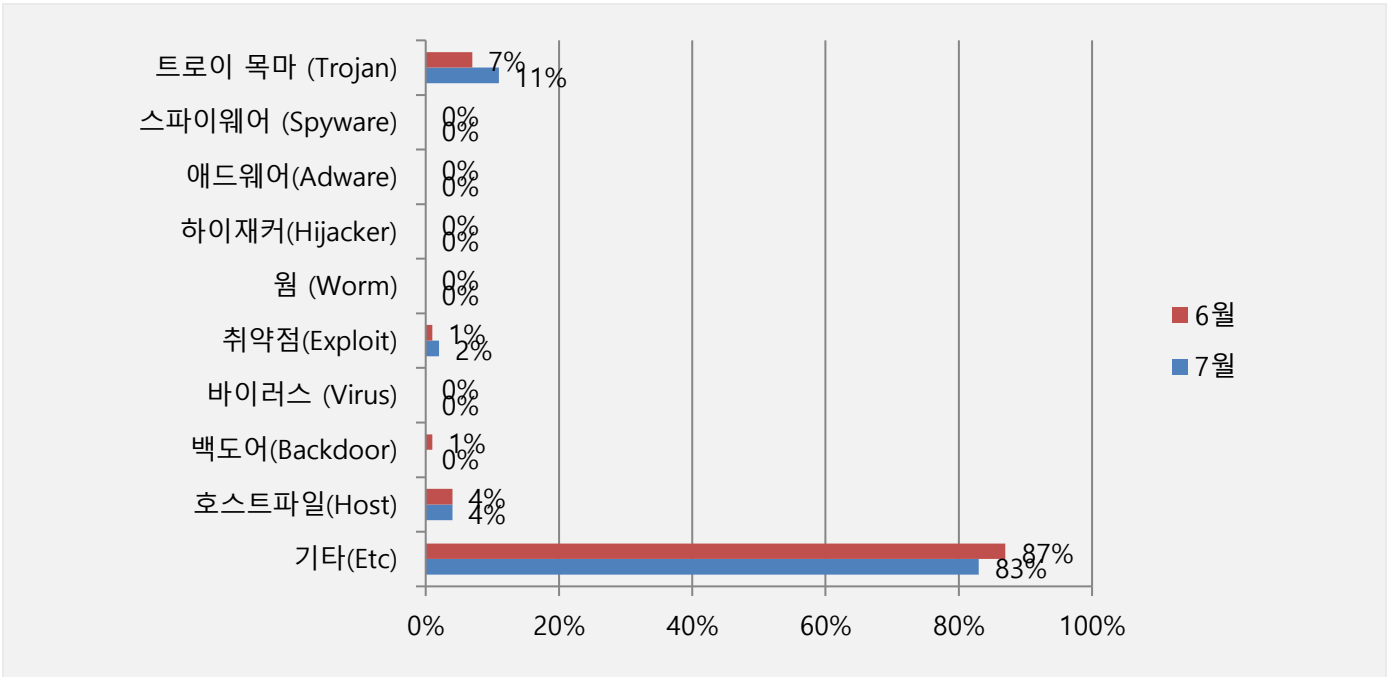
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 가장 많은 83%를 차지했으며 트로이목마(Trojan) 유형과 호스트 파일(Host) 유형이 각각 11%와 4%로 그 뒤를 이었다. 지난달 1%를 차지했던 취약점 익스플로잇(Exploit) 유형이 약간 증가하여 2% 를 기록했다. 2021 년 6 월과 비교하여 전체 감염 건수는 약 16.75% 감소하였다.



카테고리별 악성코드 비율 전월 비교

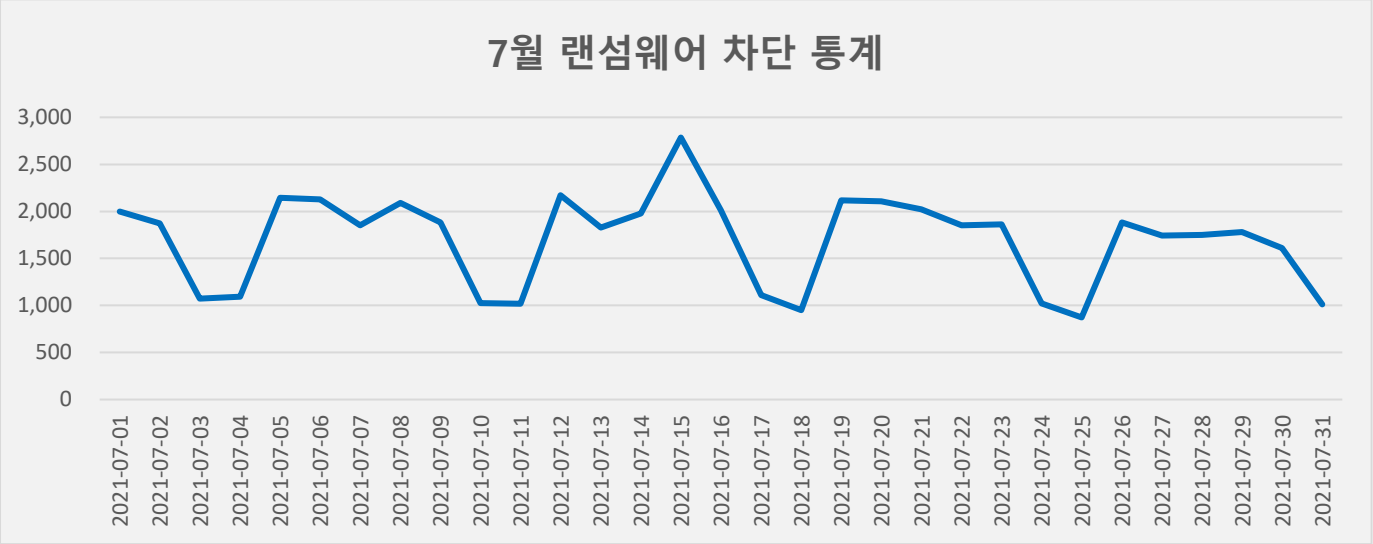
7 월에는 지난 6 월과 비교하여 트로이목마(Trojan) 유형이 4% 증가하였으며, 호스트파일(Host) 유형의 악성코드 감염 비율은 지난달과 동일하게 4%를 기록했다. 6 월에 1%를 차지했던 취약점 익스플로잇(Exploit) 유형이 소폭 증가하여 2%를 기록했다. 지난달에 적은 비율이지만 1%를 차지했던 백도어(Backdoor) 악성코드 유형은 이번 달에는 큰 탐지율을 보이지 못했다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

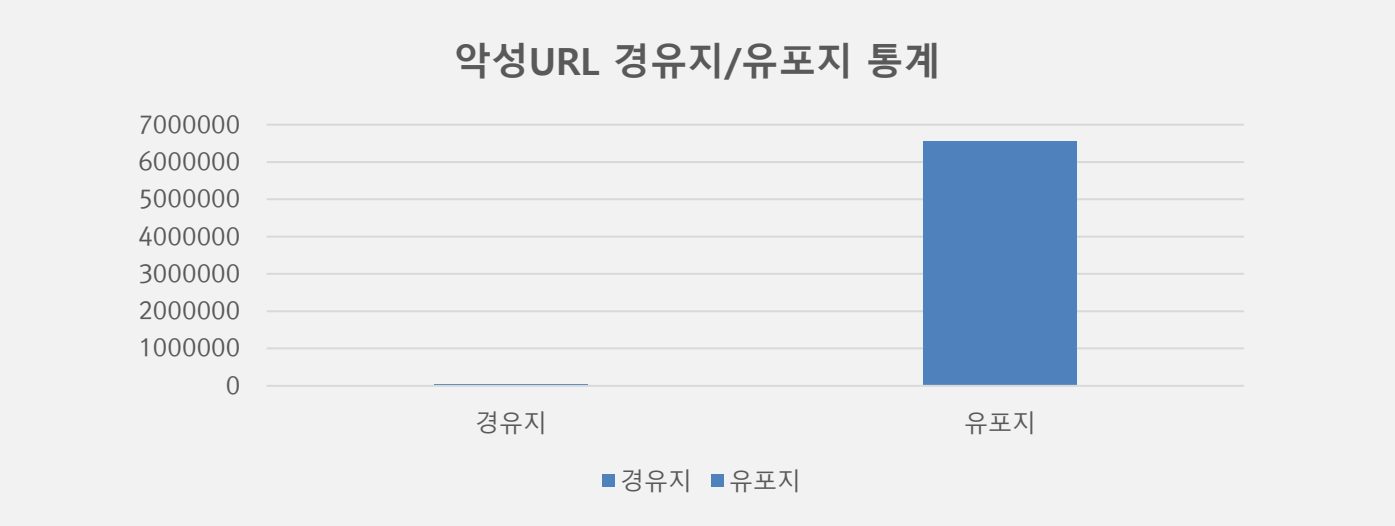
7 월 랜섬웨어 차단 통계

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 52,653 건의 랜섬웨어 공격 시도가 차단되었다. 5 월의 랜섬웨어 공격 건수인 53,704 건에 비해 약 1.96% 가량 감소하였다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 7 월 한 달간 총 6,594,647 건의 악성코드 경유지/유포지 URL 이 확인되었다. 이 수치는 6 월 한 달간 확인되었던 6,822,860 건의 악성코드 경유지/유포지 URL 수에 비해 약 3.34% 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. 랜섬웨어 대유행 '랜데믹 시대', 이젠 안보 위협

2. 통일부 사칭, 北 연계 APT 공격 등장… ‘사이버 공격 주의 업무로 둔갑’

1. 랜섬웨어 대유행 '랜데믹 시대', 이젠 안보 위협

지금 사이버 공간은 마치 '랜데믹(랜섬웨어+팬데믹)'이라는 표현을 써도 과언이 아닐 정도로 수년 동안 글로벌 랜섬웨어 위협이 대유행 중입니다.

2017 년 국내 웹 호스팅 전문업체 '인터넷나야나'가 운영하던 리눅스 웹 서버 300 여대 가운데 153 대가 일명 '에레버스(Erebus)' 랜섬웨어에 감염되는 사태가 발생했습니다. 해커는 암호화한 데이터를 볼모로 협박을 했고, 회사 측은 고객 데이터 복구를 위해 해커에게 약 13 억원 상당의 비트코인을 협상대금과 복호화 비용 명목으로 건네기로 합의했습니다. 이 소식이 알려지자 업계 안팎에서 대응방식을 두고 많은 논란이 일었습니다.

※ 관련 글 보기 : 국내 특정 웹호스팅 서비스를 사용하는 사이트를 공격한 Erebus 랜섬웨어

이스트시큐리티 시큐리티대응센터(ESRC) 문종현 센터장은 당시 랜섬웨어 대응에 나쁜 선례를 남겼다고 지적했습니다. 랜섬웨어를 이용해 주요 기업의 데이터를 암호화해 협박하면 거액의 비용을 비트코인으로 받아낼 수 있다는 고수익 랜섬웨어 시장의 가능성을 전 세계 해커들에게 증명해 준 사례로 앞으로 이와 유사한 공격들이 되풀이될 가능성이 커졌기 때문입니다.

4 년이 지난 현재 꾸준히 진화를 거듭한 랜섬웨어 위협은 기업활동을 방해해 막대한 재산상 피해를 입히는 것을 넘어 국가 사이버 안보를 위협하는 수준까지 심각성이 확대되고 있습니다. 그러나 위협 행위자는 여전히 자유롭게 전 세계를 넘나들며 활보하고 있는 게 현실입니다. 또한 정부 차원의 사이버 첩보 활동과 사보타주의 경우 금전적 수익 목적과 별개로 침투 증거 은닉을 목적으로 한 랜섬웨어 감염 위장 사례도 존재해 강대국 간의 사이버 무기 전략은 갈수록 경쟁이 치열해질 것이 분명합니다.

따라서 국제사회가 힘을 모아 중대 사이버 위협을 테러리즘에 가까운 강력 범죄 행위로 규정하고 각국 사법기관들 간의 긴밀한 연대와 협력을 도모해 지금보다 적극적으로 사이버 위협 행위에 대한 처벌 강화 및 검거 활동에 나서야 합니다.

사이버 공간에서 발생하는 다양한 위협들은 독립된 위협 행위자에 의해 관리되는 것도 존재하지만 대규모의 조직적 위협활동은 정부 차원의 지원 또는 무관심, 인터넷 익명성 보장이 주요 원인이기 때문에 사이버 범죄활동을 위축시키고 예방하기 위해선 국가차원에서 적극적인 관심과 사이버 위협 예방을 위한 단호하고 일관된 정책 입장 표명이 중요합니다.

마치 핵확산방지조약(NPT)처럼 이제는 사이버 위협 확산 방지를 위한 각국 정상 간의 긴밀한 논의와 국제상호협약이 필요한 시점이며, 나날이 심각성이 커지는 국가 간 사이버 위협을 축소·제거하기 위해 주요 사이버 위협 쟁점에 대한 규범과 제도 구축을 위한 노력이 필요합니다. 이는 사이버 위협 행위자를 끝까지 추적 검거해 법적 책임을 묻고 향후 재발 방지를 위한 발판까지 만들어 줄 수 있는 선결 과제 중 하나입니다.

02 전문가 기고

국민의 생명을 위협하는 코로나 19 대유행 팬데믹 시대가 이어지고 있듯 랜섬웨어를 포함한 다양한 사이버 위협 역시 호시탐탐 우리의 정보를 노리고 있습니다. 총성 없는 전쟁터를 방불케 하는 사이버 공간의 안보 상황을 상시로 면밀히 점검하고, 피해를 예방하는데 더 많은 관심과 투자가 필요할 때입니다.

이스트시큐리티는 외부 보안 위협에 신속하게 대응하고 발견된 보안 위협에 대해 백신 긴급 업데이트 및 보안 공지를 통해 사용자들에게 알리고, 정부 기관에도 위협정보를 공유해 빠른 선제 조치를 할 수 있도록 지속적으로 최선을 다할 예정입니다.

2. 통일부 사칭, 北 연계 APT 공격 등장… '사이버 공격 주의 업무로 둔갑'

최근 통일부 정착지원과의 모 사무관이 발송한 업무 내용처럼 위장한 해킹 이메일 공격이 등장해 각별한 주의가 필요합니다.

210812_업무연락(사이버안전) 2021-08-12 (목)

보낸사람 하나센터

대용량파일 1개 (561.5KB) ~ 2021.09.10 (30일 보관, 100회 다운로드 가능)

210811_업무연락(사이버안전).doc (561.5KB)

안녕하세요, 통일부 정착지원과 [redacted] 사무관입니다.

최근 유명인사를 노린 사이버공격이 전방위로 진행되고 있어 각별한 주의가 필요합니다.
사이버 안전에 항상 유의하여 주시기를 부탁드립니다^^

자세한 조치는 아래 첨부해드린 내용을 확인하시면 됩니다.

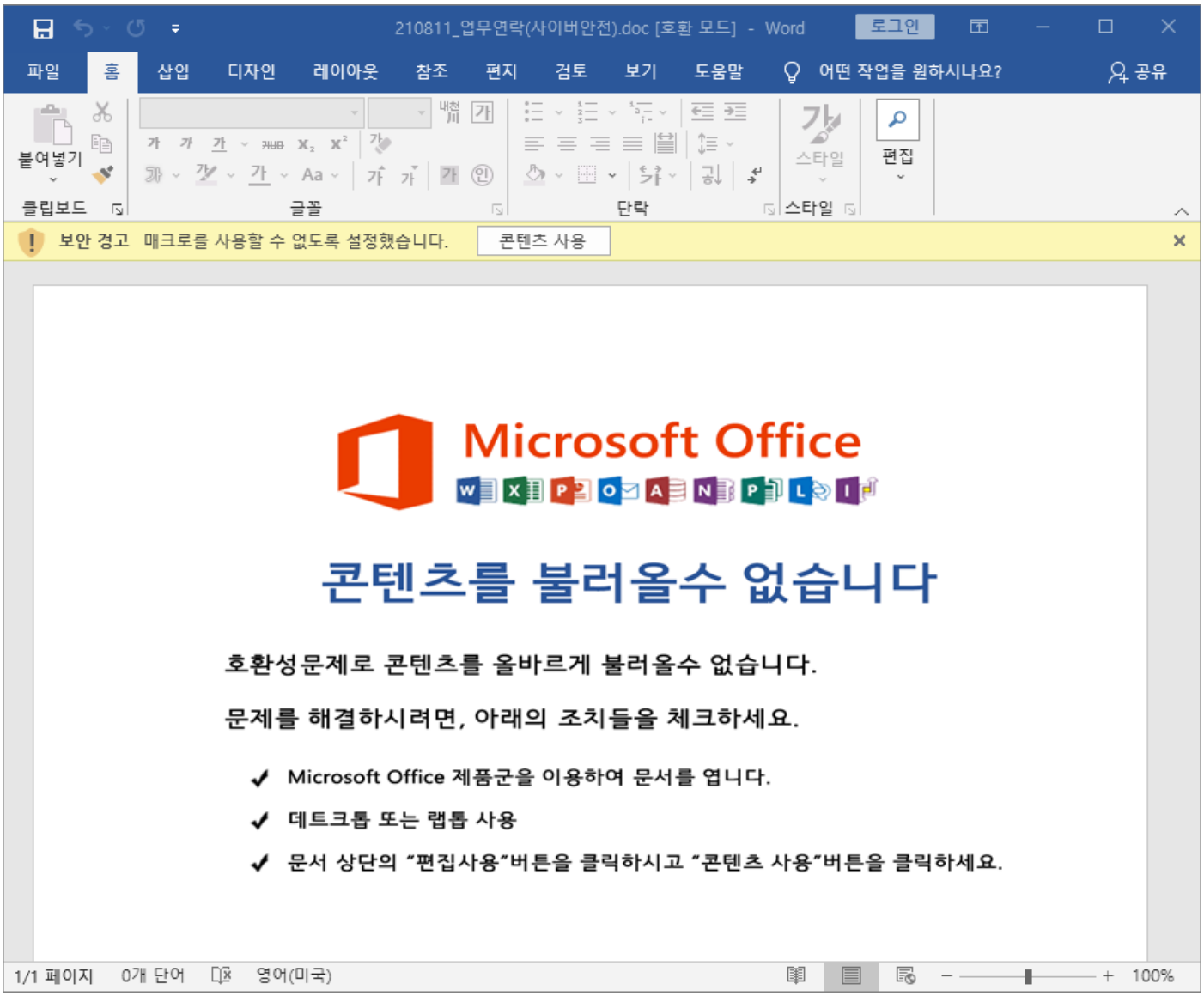
코로나위험속에 건강 관리 잘 하시길 바랍니다^^

감사합니다.

[그림 1] 통일부 하나센터 발신처럼 사칭한 해킹 이메일 본문

이번 스피어 피싱 공격은 08 월 12 일 한국의 대북 분야 종사자를 상대로 진행됐고, 이메일에는 "최근 유명인사를 노린 사이버 공격이 전방위로 진행되고 있어 사이버 안전에 유의를 부탁한다"는 본문과 함께 첨부된 '210811_업무연락(사이버안전).doc' 악성 문서 파일을 열어 보도록 유인하는 특징이 있습니다.

최근 국내 사이버 보안 위협이 가중되고, 민관 사이버 위기 경보가 '정상'에서 '관심' 단계로 격상 됨에 따라 공격자가 이 점을 노린 것으로 파악되며, 분석 결과 이번 통일부 사칭으로 유포된 DOC 문서 파일 내부에 악성 매크로 코드가 숨겨진 것이 발견됐고, 국내 특정 고시학원 사이트를 침투 해 추가 명령 제어(C2) 거점으로 활용한 사실이 드러났습니다.



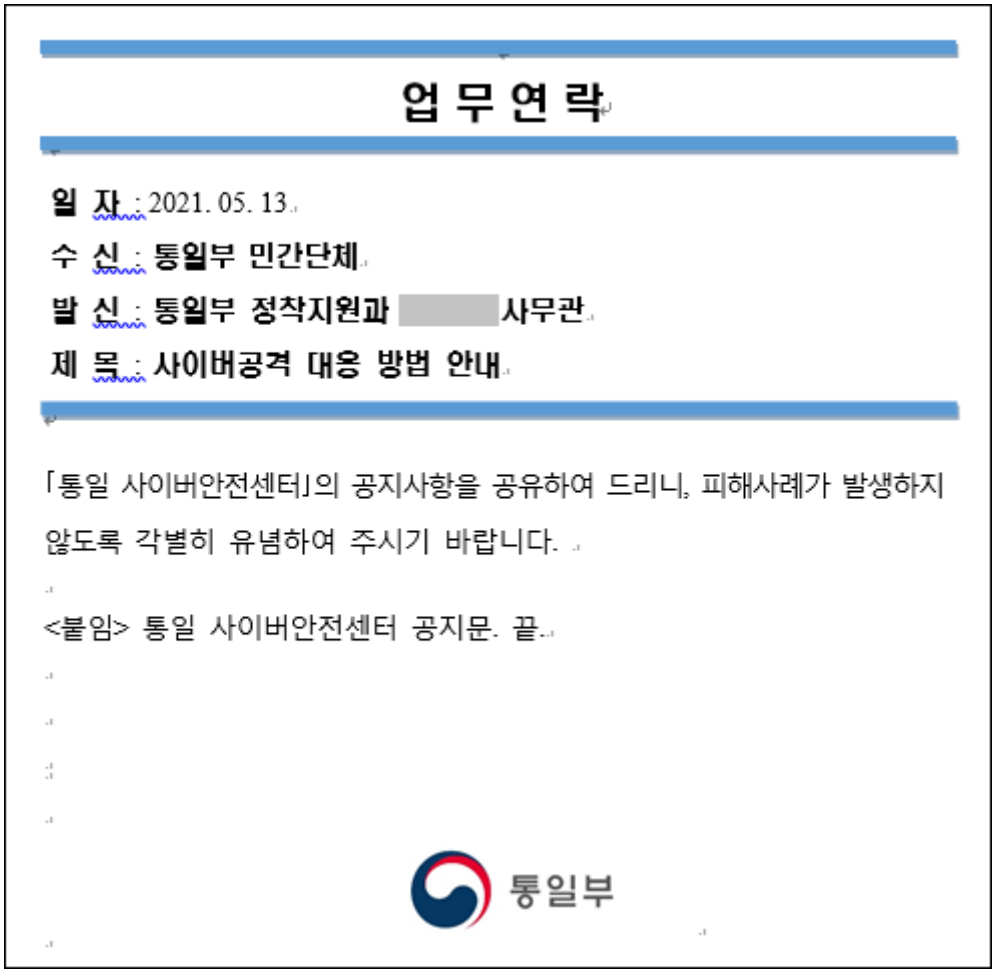
[그림 2] 악성 DOC 문서가 실행된 후 보여지는 [콘텐츠 사용] 유도 화면

이메일에서 내려 받은 DOC 문서를 열면, 악성 매크로 명령 수행을 위해 공격자가 허위로 만들어 삽입한 가짜 MS 오피스 호환성 문제 화면이 나옵니다. 그리고 실제 MS 오피스 보안 기능으로 사전 중지된 [콘텐츠 사용] 버튼을 클릭해야만 정상적인 콘텐츠를 볼 수 있다고 유도합니다.

이때 만약 사용자가 [콘텐츠 사용] 버튼을 누르면 해킹 명령이 은밀하게 작동하기 때문에 보안 경고 타이틀에 있는 [콘텐츠 사용] 버튼을 절대로 클릭하지 않는 보안 습관이 무엇보다 중요합니다.

유사한 공격이 지난 5 월에도 발생했으며, 당시 사용된 일명 '사이버 스톰 작전'과 동일한 계열의 코드 분석 결과 북한 연계 해킹 조직 '탈륨'이 위협 배후로 최종 지목된 바 있습니다.

또한, 이번 위협은 '탈륨'의 대표적인 3 대 위협 중 하나인 '스모크 스크린' 캠페인의 연장선으로, 이들 조직은 최근 PDF 취약점 공격과 함께 DOC 악성 문서 공격까지 갈수록 사이버 위협이 거세지고 있습니다.



업 무 연 락

일 자 : 2021. 05. 13.

수 신 : 통일부 민간단체.

발 신 : 통일부 정착지원과 [redacted] 사무관.

제 목 : 사이버공격 대응 방법 안내.

「통일 사이버안전센터」의 공지사항을 공유하여 드리니, 피해사례가 발생하지 않도록 각별히 유념하여 주시기 바랍니다.

<붙임> 통일 사이버안전센터 공지문. 끝.

통일부

[그림 3] 지난 05 월 발견된 통일부 사칭 유사 변종 공격 화면

국내에서 암약하는 대표적인 사이버 위협 조직 '탈륨'은 최근까지 국내 전·현직 고위 정부 인사 등을 상대로 해킹 공격을 시도해왔고, 얼마 전에는 국내 유명 방송 및 언론사의 주요 간부나 국장급을 상대로 PDF 취약점 (CVE-2020-9715) 공격을 수행했습니다.

아직도 PDF 유형의 공문서 파일은 보안상 안전하다는 인식이 있어, 더욱 더 세심한 주의가 필요하며 항시 최신 버전으로 업데이트를 유지해 유사한 보안 위협에 노출되지 않도록 철저한 대비가 필요한 상황입니다.

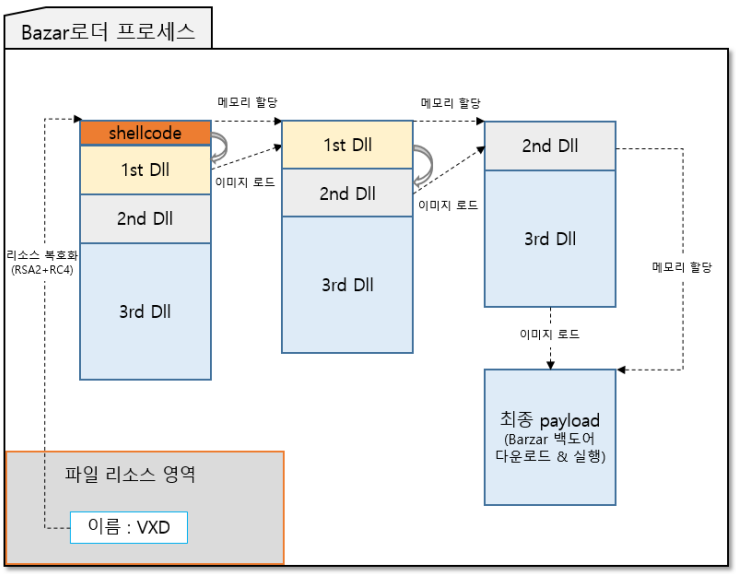
현재 알약에서는 해당 악성코드를 Trojan.DOC.574976A 탐지 명으로 진단하고 있으며, 관련 상세 분석 보고서는 Threat Inside 웹서비스 구독을 통해 확인하실 수 있습니다.

03
악성코드 분석 보고

[Bazar loader] 악성코드 분석 보고서

2020 년 4 월에 처음 등장한 Bazar 악성코드는 미국 및 유럽 전역의 전문 서비스, 의료, 제조, IT, 물류 및 여행 회사를 공격 대상으로 하고 있으며, 주로 피싱 이메일을 통하여 공격이 이루어 지고 지속적으로 진화를 거듭해 오고 있다.

Bazar 로더는 Trickbot 로더와 마찬가지로 해킹된 유효한 디지털 인증서를 이용하여 탐지를 회피한다. 그리고 Bazar 로더는 명령 및 제어를 위해 EmerDNS(.bazar) 블록체인 도메인(도메인 차단 방지용)을 사용하여 C2 서버와 통신하며, 필요한 API 및 문자열 등이 난독화 되어 있어 자동 및 수동 분석을 방해하고 암호화된 백도어를 메모리에만 로드하여 실행 한다.



[그림] 동작 흐름도

Bazar 악성코드는 탐지 회피 및 은폐에 중점을 두고 있으며. 2020 년 4 월에 등장한 이후 계속적인 프로그램 업데이트가 이루어 지고 있음이 확인되고 있어 앞으로도 큰 위협이 될 것임은 분명하다.

따라서, 악성코드 감염을 방지하기 위해 출처가 불분명한 이메일의 첨부 파일 혹은 URL 클릭을 삼가야 하며, 백신의 최신화 및 정기적인 검사를 습관화하여야 한다.

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

[Trojan.Android.Banker] 악성코드 분석 보고서

고전적인 수법의 피싱 사기는 현재까지도 지속해서 발생하고 있다. 공격자들은 유형만 조금씩 바꿔서 진행하는데, 여러 가지 버전의 앱들을 만들고 배포하며 체계적으로 관리한다. 최근에도 SNS 를 통해 본인이 필라테스 강사임을 밝히며 접근해오는 수법으로 피해자를 물색하고 있다. 공격자들이 유포하고 있는 앱을 보면 갤러리, 동영상, 보안카메라 등등 사진 관련 앱들로 구성되어 있고 주로 영상을 보여주는 것처럼 위장하고 있다.

[그림] 유사 앱 목록

분석 내용을 살펴보면 'Trojan.Android.Banker'는 돈을 목적으로 사용자의 정보를 탈취한다. 현재 감염자는 대략 1,000 명이며 지금, 이 순간에도 지속해서 늘어나고 있다. 보이스 피싱으로 인해 금전적인 피해도 발생하지만, 문자를 확인하여 다른 사이트나 플랫폼에 계정을 추가로 만들 수 있고 이를 다시 범죄에 악용할 수도 있으니 앱을 설치하지 않도록 사용자의 각별한 주의가 필요하다.

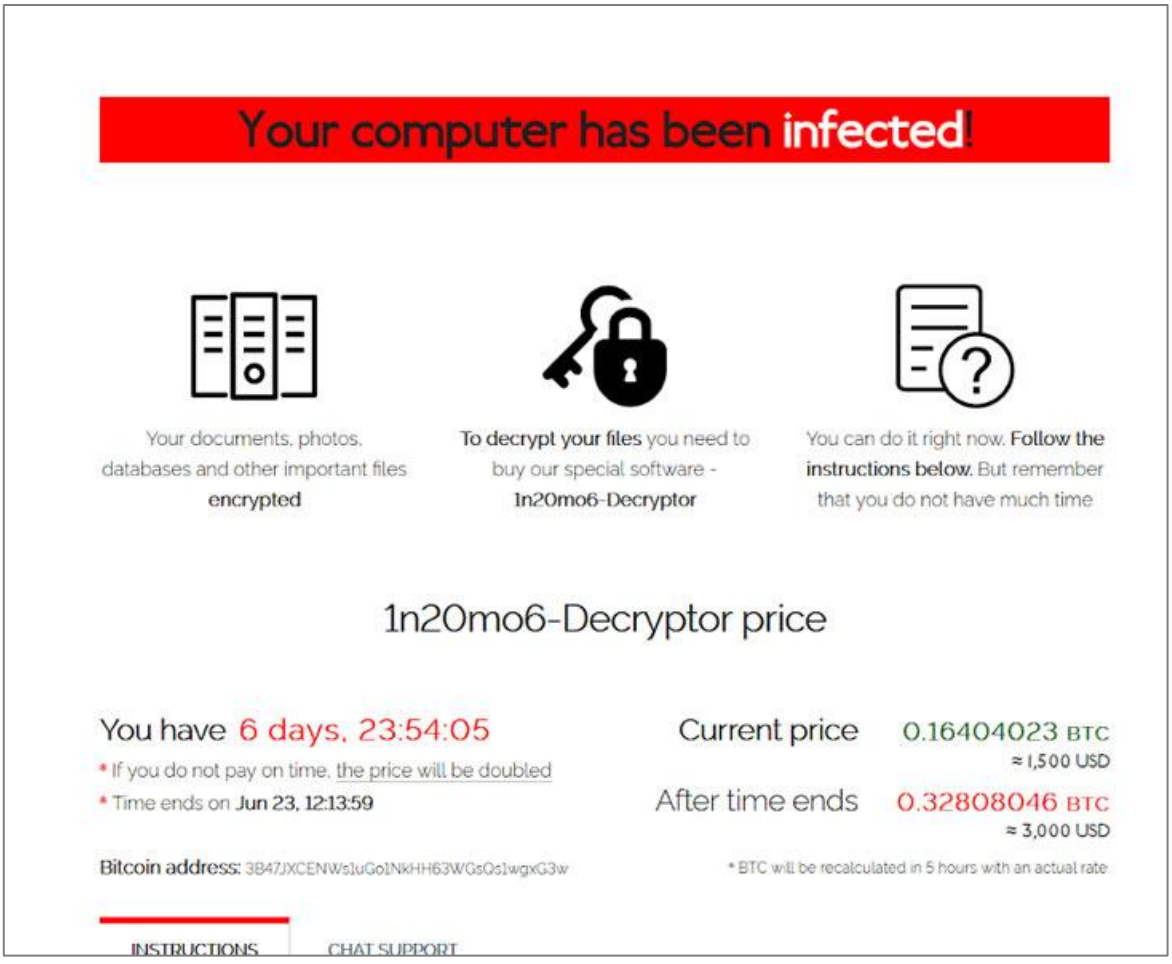
현재 알약 M 에서는 해당 앱을 ′Trojan.Android.Banker' 탐지 명으로 진단하고 있으며, 관련 상세 분석 보고서는 Threat Inside 웹서비스 구독을 통해 확인이 가능하다.

04
글로벌 보안 동향

Kaseya 공급망 공격, Sodinokibi 랜섬웨어 통해 서비스 제공 업체 약 40 곳 공격해

Kaseya Supply-Chain Attack Hits Nearly 40 Service Providers With REvil Ransomware

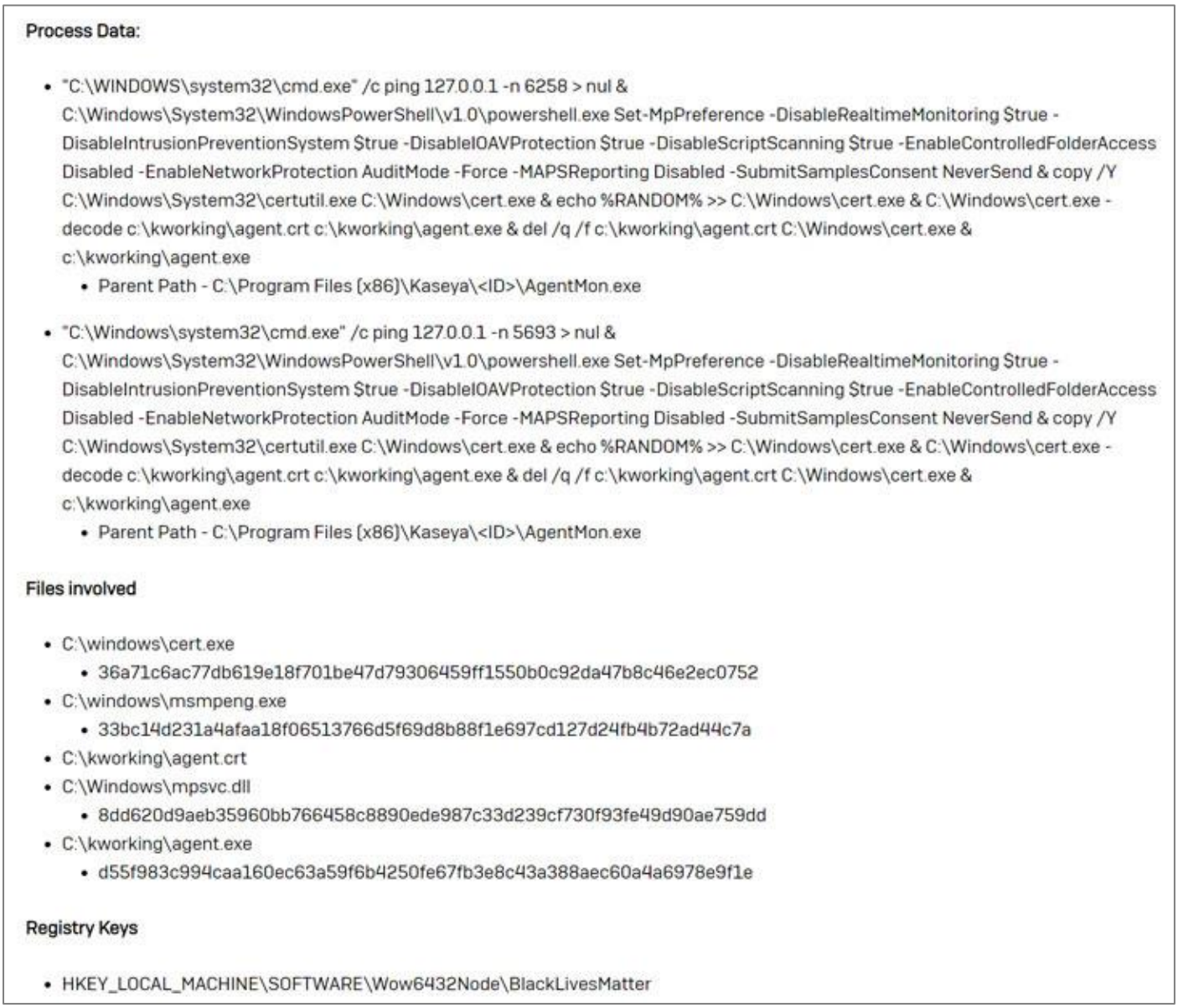
악명 높은 Sodinokibi 랜섬웨어 그룹 공격자들이 Kaseya IT 관리 소프트웨어 업데이트를 통해 랜섬웨어를 유포한 것으로 나타났다. 이들은 광범위한 랜섬웨어 공격을 통해 전 세계의 고객 약 40 곳을 공격했다. 지난 금요일 회사의 CEO 인 Fred Voccola 는 성명문을 통해 다음과 같이 밝혔다. "Kaseya 의 사고대응팀은 2021 년 7 월 2 일 금요일 정오(EST)에 VSA 소프트웨어와 관련된 잠재적 보안 사고에 대해 알게 되었다." 사고 이후, 해당 회사는 사전 예방 조치로 SaaS 서버를 종료시켰으며, 온-프레미스 고객에게 VSA 서버가 해킹되지 않도록 이를 종료하도록 알렸다.



[이미지 출처] https://thehackernews.com/2021/07/kaseya-revil-ransomware-attack.html

Voccola 는 회사가 취약점의 출처를 확인했으며, 현재 이를 완화하기 위한 패치를 준비 중이라 밝혔다. 또한 안전해지기 전까지 모든 온-프레미스 VSA 서버, SaaS, 호스팅되는 VSA 서버를 중단할 계획이라고도 밝혔다. Sophos 의 악성코드 분석가인 Mark Loman 에 따르면, 업계 전반에 걸쳐진 이 공급망 공격은 Kaseya VSA 를 활용하여 피해자의 환경에 Sodinokibi 랜섬웨어 변종을 배포하고, Sodinokibi 바이너리는 가짜 윈도우 디펜더 앱을 통해 사이드로드된 것으로 나타났다. 또한 공격 체인은 PowerShell 을 통해 마이크로소프트 디펜더의 실시간 모니터링을 비

활성화하려 시도한다고 밝혔다. Huntress Labs 는 레딧 게시물을 통해 트로이목마가 포함된 이 소프트웨어가 "Kaseya VSA 에이전트 핫픽스"의 형태로 배포되고 있다고 밝혔다.



Process Data:

- "C:\WINDOWS\system32\cmd.exe" /c ping 127.0.0.1 -n 6258 > nul & C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend & copy /Y C:\Windows\System32\certutil.exe C:\Windows\cert.exe & echo %RANDOM% >> C:\Windows\cert.exe & C:\Windows\cert.exe -decode c:\kworking\agent.crt c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt C:\Windows\cert.exe & c:\kworking\agent.exe
  - Parent Path - C:\Program Files (x86)\Kaseya\<ID>\AgentMon.exe
- "C:\Windows\system32\cmd.exe" /c ping 127.0.0.1 -n 5693 > nul & C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend & copy /Y C:\Windows\System32\certutil.exe C:\Windows\cert.exe & echo %RANDOM% >> C:\Windows\cert.exe & C:\Windows\cert.exe -decode c:\kworking\agent.crt c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt C:\Windows\cert.exe & c:\kworking\agent.exe
  - Parent Path - C:\Program Files (x86)\Kaseya\<ID>\AgentMon.exe

Files involved

- C:\windows\cert.exe
  - 36a71c6ac77db619e18f701be47d79306459ff1550b0c92da47b8c46e2ec0752
- C:\windows\msmpeng.exe
  - 33bc14d231a4afaa18f06513766d5f69d8b88f1e697cd127d24fb4b72ad44c7a
- C:\kworking\agent.crt
- C:\Windows\mpsvc.dll
  - 8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd
- C:\kworking\agent.exe
  - d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e

Registry Keys

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BlackLivesMatter

[이미지 출처] https://thehackernews.com/2021/07/kaseya-revil-ransomware-attack.html

연구원들은 이 공격에 피해를 입은 기업 중 다른 회사에 IT 서비스를 제공하는 '관리 서비스 제공 업체(MSP)' 8 곳을 발견했다고 밝혔다. Huntress Labs 은 해당 MSP 업체에서 관리 중인 기업 200 곳의 네트워크가 감염되었다고 밝혔다. MSP 침투에 성공하면 여러 고객에 접근할 수 있게 되기 때문에, 이는 랜섬웨어의 수익성 있는 타깃으로 급부상했다. 지난 토요일, Kaseya 는 "정교한 사이버 공격에 피해를 입었다"고 밝히며 고객들에게 랜섬웨어 운영자가 전송하는 어떠한 링크도 클릭하지 말 것을 당부했다. 연구원들은 Sodinokibi 랜섬웨어가 Kaseya VSA 소프트웨어의 제로데이 취약점을 악용한 것으로 추측했다. Kaseya 는 공격 벡터를 격리 및 제거했으며, 해당 취약점을 수정하기 위한 소프트웨어 패치를 준비하고 있다고 밝혔다.

[출처]

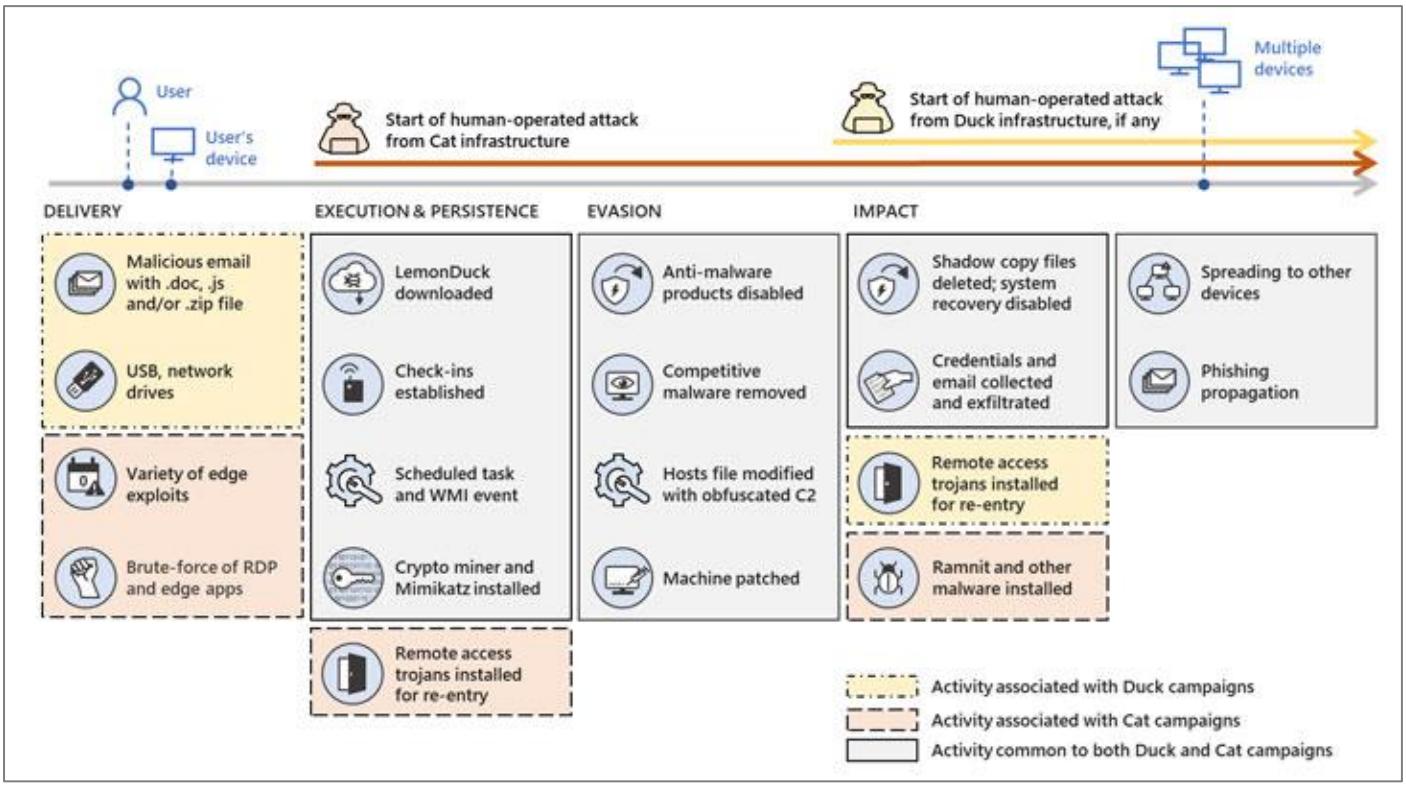
https://thehackernews.com/2021/07/kaseya-revil-ransomware-attack.html

마이크로소프트, 윈도우 및 리눅스 시스템을 노리는 LemonDuck 악성코드 경고

Microsoft Warns of LemonDuck Malware Targeting Windows and Linux Systems

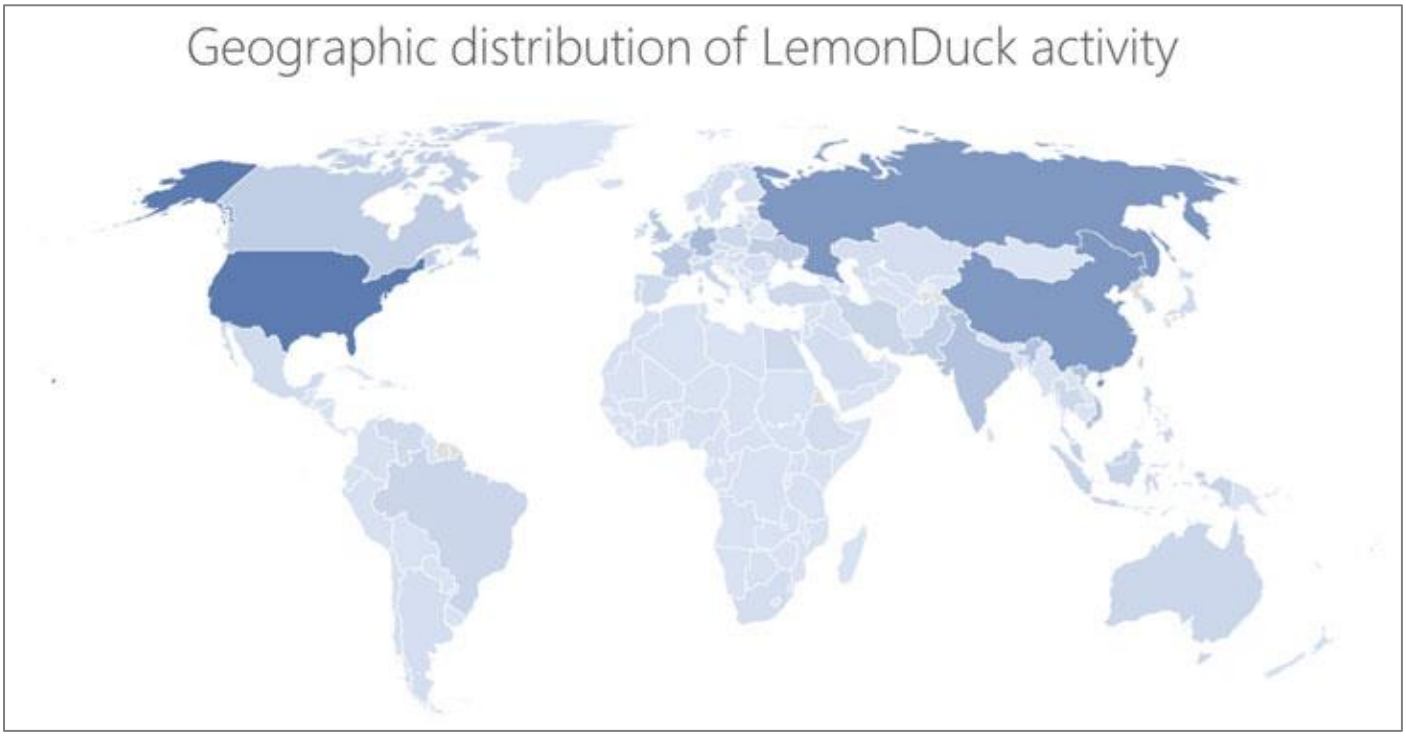
악명 높은 크로스 플랫폼 크립토마이닝 악성코드가 오래된 취약점을 노리며 Windows 및 Linux OS 를 공격하는 기술을 끊임없이 개선하고, 다양한 확산 메커니즘을 활용하여 캠페인의 효율성을 극대화하고 있는 것으로 나타났다. 마이크로소프트는 지난주 발행한 기술 문서에서 다음과 같이 밝혔다. “LemonDuck 은 봇넷 및 가상화폐 채굴기로 알려졌으며 활발히 업데이트되는 강력한 악성코드이다. 이 악성코드는 더욱 정교한 행동을 채택했으며, 그들의 작전을 더욱 확장시켰다. LemonDuck 은 기존에 봇 및 마이닝 활동에 리소스를 사용하는 것을 넘어 크리덴셜을 훔치고, 보안 장치를 제거하고, 이메일을 통해 확산되고, 측면 이동하고, 결국 인간 개입 공격을 위한 더 많은 툴을 드롭한다.”

LemonDuck 악성코드는 감염된 네트워크 전체에 빠르게 확산되어 정보 탈취를 용이하게 하고, 가상화폐를 불법적으로 채굴하기 위해 컴퓨터 리소스를 사용함으로써 컴퓨터를 가상화폐 채굴 봇으로 사용하는 것으로 알려져 있다. 또한 크리덴셜 탈취 및 랜섬웨어를 포함한 다양한 악성 위협을 실행할 수 있는 게이트웨이 역할을 하는 차세대 임플란트를 설치하고, 관련 후속 공격을 진행하는 로더 역할을 한다.



[이미지 출처] https://www.microsoft.com/security/blog/2021/07/22/when-coin-miners-evolve-part-1-exposing-lemonduck-and-lemoncat-modern-mining-malware-infrastructure/

LemonDuck 활동은 2019 년 5 월 중국에서 처음 발견되었으며, 2020 년 COVID-19 를 주제로 사용하는 이메일 공격을 사용하기 시작했다. 최근에는 패치되지 않은 시스템에 접근하기 위해 "ProxyLogon" 익스체인지 서버 취약점을 악용했다. 주목할만한 또 다른 전략은 “경쟁 악성코드를 제거하고, 접근 권한을 얻는데 악용한 동일한 취약점을 패치함으로써 새로운 감염을 막아 다른 공격자를 막는다”는 것이다. LemonDuck 악성코드를 사용한 공격은 주로 제조 및 IoT 부문에 집중되어 있으며 미국, 러시아, 중국, 독일, 영국, 인도, 한국, 캐나다, 프랑스, 베트남에서 가장 많이 발생했다.



[이미지 출처] https://www.microsoft.com/security/blog/2021/07/22/when-coin-miners-evolve-part-1-exposing-lemonduck-and-lemoncat-modern-mining-malware-infrastructure/

또한 마이크로소프트는 “또 다른 목표”를 달성하기 위해 LemonDuck 에 의존하는 “LemonCat”이라는 두 번째 작전에 대해 공개했다. “CAT” 변종과 관련된 해당 공격 인프라는 2021 년 1 월 등장해 마이크로소프트 익스체인지 서버를 노린 취약점을 악용하는 공격에 사용되었다. Cat 도메인을 이용하는 후속 침입을 통해 백도어 설치, 크리덴셜 및 데이터 탈취, Ramnit 윈도우 트로이목마를 포함한 악성코드 전달 등과 같은 공격이 발생했다.

마이크로소프트는 다음과 같이 밝혔다. “Cat 인프라가 더 위험한 캠페인에 사용된다고 해서 Duck 인프라에서 발생하는 악성코드 감염이 중요하지 않다는 것은 아니다. 대신 이 인텔리전스는 해당 위협을 이해하는데 중요한 컨텍스트를 추가한다. 더욱 큰 효과를 위해 동적 간격으로 동일한 도구 세트, 접근, 방식이 재사용될 수 있다는 것이다.”

[출처]

https://thehackernews.com/2021/07/microsoft-warns-of-lemonduck-malware.html

새로운 윈도우 프린트 스풀러 내 제로데이 취약점 발견

New Windows print spooler zero day exploitable via remote print servers

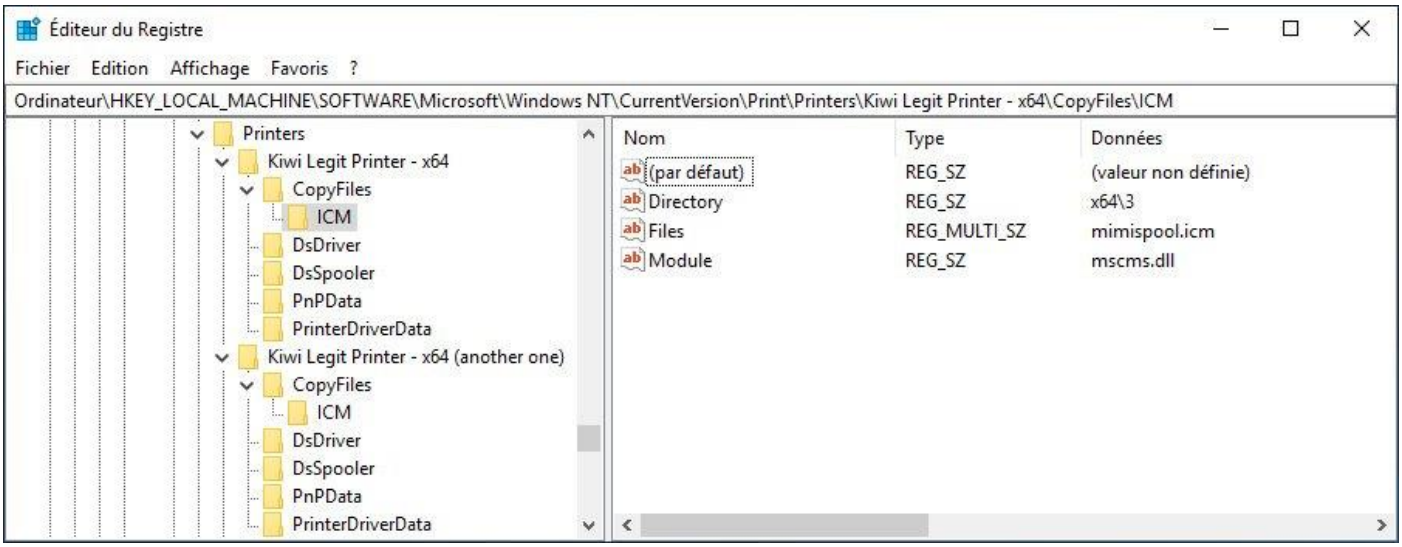
윈도우 프린트 스풀러에서 또 다른 제로데이 취약점이 발견되었다. 이를 악용한 공격자는 공격자가 제어하는 원격 서버와 '대기열 별 파일(Queue-Specific Files)' 기능을 통해 윈도우 기기에서 관리자 권한을 얻어낼 수 있다. 지난달, 한 보안 전문가는 의도치 않게 윈도우 프린트 스풀러에 존재하는 제로데이인 PrintNightmare(CVE-2021-34527)를 공개했다. 공격자가 이 취약점을 악용할 경우 시스템 내에서 권한을 상승시키거나 원격으로 코드를 실행할 수 있다. 마이크로소프트는 이 취약점을 수정하는 보안 업데이트를 공개했지만, 연구원들은 해당 패치가 특정 조건에서 우회 가능하다고 판단했다. 이후 연구원들은 윈도우의 프린팅 API 를 자세히 조사했으며, 윈도우 프린트 스풀러에 존재하는 취약점을 추가로 발견할 수 있었다.

- 원격 프린트 서버, 공격에 악용돼

보안 연구원이자 Mimikatz 제작자인 Benjamin Delpy 는 공격자가 제어하는 원격 프린트 서버를 통해 윈도우 기기에서 SYSTEM 권한을 쉽게 얻어낼 수 있는 새로운 제로데이 취약점을 공개했다.

[이미지 출처] https://twitter.com/gentilkiwi/status/1416079316673339392

Delpy 는 Bleeping Computer 과의 인터뷰에서 그의 익스플로잇이 클라이언트가 공격자가 제어하는 프린트 서버에 연결하면 Windows Point and Print 의 '대기열 별 파일' 기능을 통해 악성 DLL 을 자동으로 다운로드 및 실행한다고 밝혔다. 마이크로소프트의 대기열 별 파일 문서에서는 해당 기능에 대해 다음과 같이 설명했다. "프린트 설치 시, 공급업체가 제공한 설치 어플리케이션은 특정 인쇄 대기열과 연결될 모든 파일 유형 세트를 지정할 수 있다. 파일은 프린트 서버에 연결하는 각 클라이언트에 다운로드된다." 연구원들은 이 취약점 악용을 위해 '대기열 별 파일' 기능을 사용하는 공유 프린터 두 대로 인터넷에서 접근이 가능한 프린트 서버를 생성했다.



[이미지] 대기열 별 파일 레지스트리 구성

[이미지 출처] Delpy

악성 DLL 이 SYSTEM 권한으로 실행되면, 컴퓨터에서 모든 명령을 실행하는데 악용될 수 있다. CERT/CC 의 취약점 분석가인 Will Dormann 은 이 취약점에 대한 추가 정보를 제공하는 권고를 발표했다. 이 취약점이 더욱 위험한 이유는 모든 윈도우 버전에 영향을 미치고, 공격자가 네트워크에서 제한된 접근 권한을 얻고 취약한 기기에서 SYSTEM 권한을 즉시 획득할 수 있기 때문이다. 공격자는 이 접근 권한을 통해 도메인 컨트롤러에 접근할 수 있을 때까지 네트워크를 통해 측면 이동이 가능하다. Bleeping Computer 는 이 공격을 시연한 영상을 공개했다.

- 새로운 프린터 취약점 완화하기

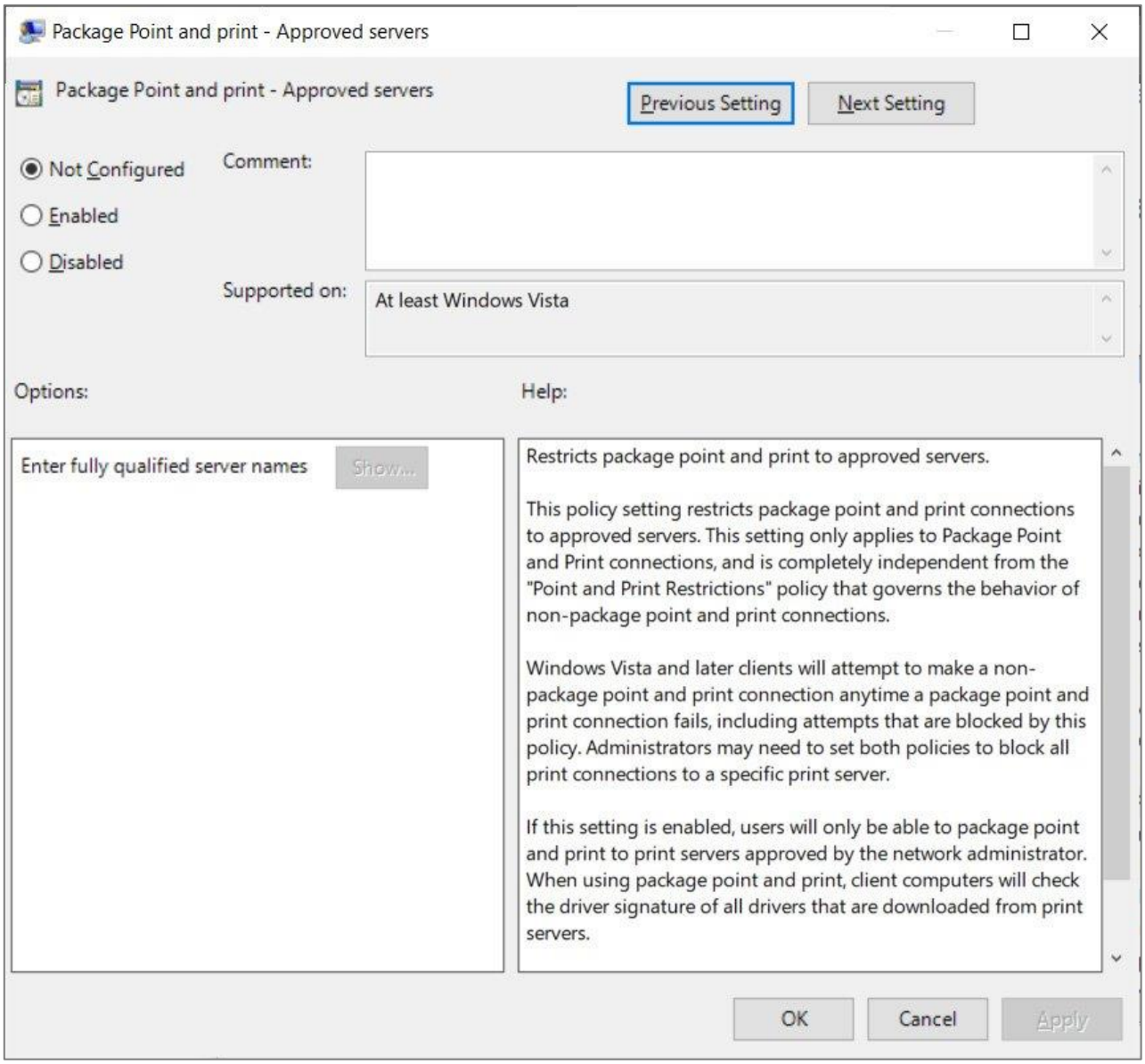
다행히도 Delpy 와 Dormann 이 이 새로운 '대기열 별 파일' 취약점을 완화할 수 있는 방법 2 가지를 공유했으며, 이 두 방법 모두 CERT 의 권고에 요약되어 있다.

<방법 1. 네트워크 경계에서 아웃바운드 SMB 트래픽 차단>

Delpy 의 공개 익스플로잇은 원격 인쇄 서버를 사용하기 때문에 아웃바운드 SMB 트래픽을 차단해 원격 컴퓨터에 대한 접근을 방지할 수 있다. 하지만 Dormann 은 MS-WPRN 을 사용하여 SMB 를 사용하지 않고 드라이버를 설치하는 것이 가능하며, 공격자는 로컬 프린터 서버에서 이 기술을 계속해서 사용할 수 있다고 밝혔다.

<방법 2. PackagePointAndPrintServerList 구성하기>

이 익스플로잇을 예방할 수 있는 더 나은 방법은 'Package Point and print - Approved servers' 그룹 정책을 사용하여 Point and Print 를 승인된 서버 목록으로 제한하는 것이다.



[이미지] 'Package Point and print – Approved servers' 정책

[이미지 출처] https://www.bleepingcomputer.com/news/microsoft/new-windows-print-spooler-zero-day-exploitable-via-remote-print-servers/

이 정책은 관리자가 아닌 사용자가 승인된 목록에 프린트 서버가 없는 경우 이를 지정하여 프린트 드라이버를 설치하는 것을 방지한다. 이 그룹 정책은 현재까지 알려진 익스플로잇을 예방할 수 있는 최선의 방법이며, 마이크로소프트는 아직까지 이 문제와 관련하여 답변을 하지 않은 상태다.

[출처]

https://www.bleepingcomputer.com/news/microsoft/new-windows-print-spooler-zero-day-exploitable-via-remote-print-servers/

(주)이스트시큐리티

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