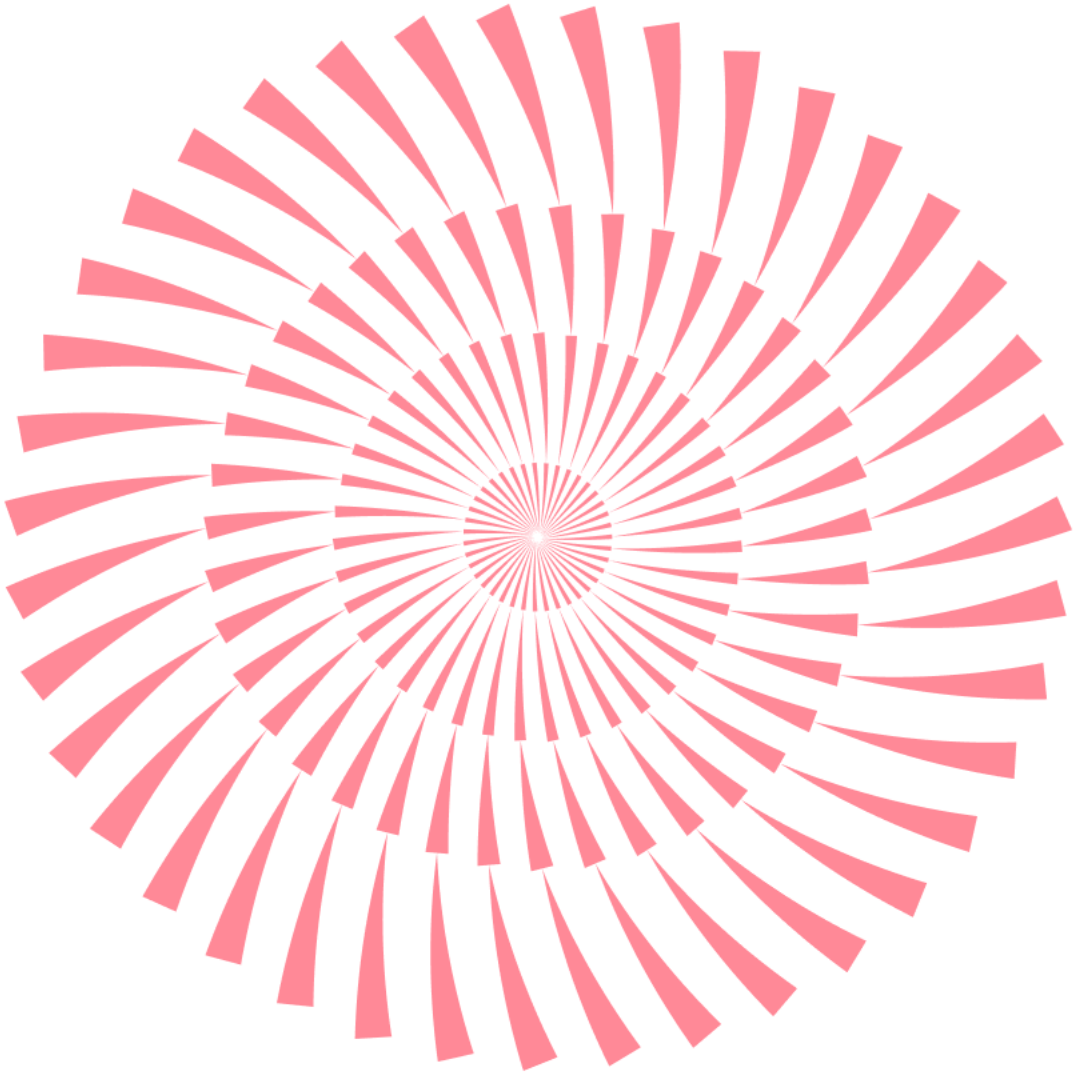
No.179 | 2024.8

ESRC 보안동향보고서

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



Copyright©2024 ESTsecurity Corp. All rights reserved.

EST SECURITY

ESRC 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 최신 보안 동향 08-10

2 분기 랜섬웨어 동향

1

악성코드 통계 및 분석

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

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

1. 악성코드 동향

사회적 이슈를 활용한 공격은 사이버 공격자들이 즐겨 사용하는 공격 방식 중 하나입니다.

파리 올림픽이 개막한 7 월에는 올림픽 티켓 구매페이지, 올림픽 코인 ico 페이지 등 다양한 피싱 페이지가 발견되었으며, 올림픽 투자사기 관련 악성앱 등 올림픽 이슈를 활용한 다양한 사이버 공격이 발견되었습니다.

국내에서는 대형 이커머스들이 판매자들에게 판매 대금을 지급하지 않으면서, 판매자 및 소비자들의 큰 피해가 발생했는데, 이 틈을 타 공격자들은 이커머스 환불 사태 키워드를 이용한 스미싱을 유포하여 사용자들의 개인정보 탈취를 시도하는 공격이 확인되었습니다.

2 개의 새로운 APT 조직이 공개되었습니다.

인포블록스(Infoblox)라는 보안업체는 비고리시바이퍼(Vigorish Viper)라는 APT 조직을 공개하였습니다.

인포블록스는 비고리시바이퍼는 2018 년부터 운영된 중국의 사이버 범죄 조직으로 세계 불법 스포츠 도박 경제에 깊숙히 연루되어 있으며, 규모가 약 1 조 7000 억 달러에 해당한다고 밝혔습니다. 이 그룹은 맨체스터 유나이티드를 포함한 여러 유러 축구 클럽과의 파트너십을 맺고 있는 야보그룹(Yabo Group)과 연관이 있는 것으로 밝혀졌습니다.

또한 클라우드소서러(CloudSorcerer)라고 명명된 APT 그룹이 공개되었는데, 이 조직은 주로 러시아 단체를 타깃으로 공격을 진행하고 있는 것으로 확인되었습니다. 이 그룹은 클라우드위자드(CloudWizard)라는 공격 조직과 많은 부분이 비슷하지만, 사용되는 악성코드의 소스코드는 큰 차이가 있어 같은 그룹은 아닌 것으로 추정되고 있습니다.

사이버 공격이 심화됨에 따라, 여러건의 합동 경고문도 공개되었습니다.

호주, 캐나다, 독일, 일본, 뉴질랜드, 한국, 영국, 미국이 합동으로 APT40 조직에 대한 보안권고문을 발표하였습니다.

APT40 은 중국정부의 후원을 받고 있는 APT 조직으로 최근 취약점 정보나 개념증명용 익스플로잇이 공개되면 수 시간만에 해당 정보를 공격에 사용하며 높은 공격 성공률을 보인다고 밝혔습니다. 공격 목적은 정보수집으로 기업과 기관을 가리지 않고 공격 대상으로 삼는다며 각별한 주의를 당부하였습니다.

또한 한국, 영국, 미국은 북한의 후원을 받고 있는 안다리엘 해킹 조직에 대한 보안권고문을 발표하였습니다.

안다리엘(Onyx Sleet, 구 PLUTONIUM, DarkSeoul, Silent Chollima, Stonefly/Clasiopa 등으로 알려져 있음)은 평양과 신의주에 기반을 두고 있는 북한 정찰총국 3 국 산하 국가배후 해킹조직으로, 미국과 한국을 겨냥하여 파괴적 공격에서 전문화된 사이버 첩보활동과 랜섬웨어 활동으로 진화했으며 주로 방산, 항공우주, 핵, 공학 단체 및 에너지 산업을 주요 공격 타깃으로 합니다. 안다리엘 조직 역시 Log4j 를 포함한 다수의 알려진 취약점을 공격 초기벡터로 사용하는 만큼 기업 및 기관들의 취약점 관리에 각별한 주의가 요구되고 있습니다.

이 밖에도 국내 해외 정보 업무를 담당하는 전문 정보기관인 국군정보사령부의 해외 주재 첩보요원들 신상정보가 외부 유출되었는데, 해당 정보들은 망분리된 내부망에 존재하던 파일이었으나 외부(특정 개인 PC)로 유출이 되었으며, 이 정보에는 외교관 등 공식적인 신분을 가진 '화이트요원'의 정보와 함께 한국과는 전혀 관계없는 인물로 신분을 위장해 활동하는 '블랙요원'의 정보가 함께 포함되어 있어 큰 파장을 일으키고 있습니다.

ESTSECURITY Copyright©2024 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.

2024 년 7 월에는 Gen:Variant.TDss.49,Exploit.CVE-2010-2568.Gen, Trojan.Meredrop.AF, Trojan.Acad.Bursted.AK, Gen:Variant.Fragtor.567760 의 새로운 탐지명이 순위권에 자리하였습니다.

순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	NEW	Gen:Variant.TDss.49	ETC	155,147
2	↓1	Gen:Variant.Lazy.266772	ETC	114,180
3	NEW	Exploit.CVE-2010-2568.Gen	Exploit	84,439
4	↑3	Gen:Variant.Lazy.540900	ETC	81,673
5	NEW	Trojan.Meredrop.AF	Trojan	78,139
6	↓3	Trojan.GenericKD.72973671	Trojan	72,218
7	↓5	Trojan.Downloader.MSIL	Trojan	50,472
8	↓2	Backdoor.Generic.792814	Backdoor	39,368
9	↓5	Trojan.DDoS.Nitol.gen	Trojan	33,868
10	↓5	Misc.HackTool.AutoKMS	ETC	31,804
11	↓2	Gen:Variant.Lazy.20522	ETC	25,348
12	↓1	Gen:Variant.Ulise.144799	ETC	22,254
13	-	Application.Hacktool.BBJ	ETC	22,061
14	NEW	Trojan.Acad.Bursted.AK	Trojan	20,869
15	NEW	Gen:Variant.Fragtor.567760	ETC	19,994

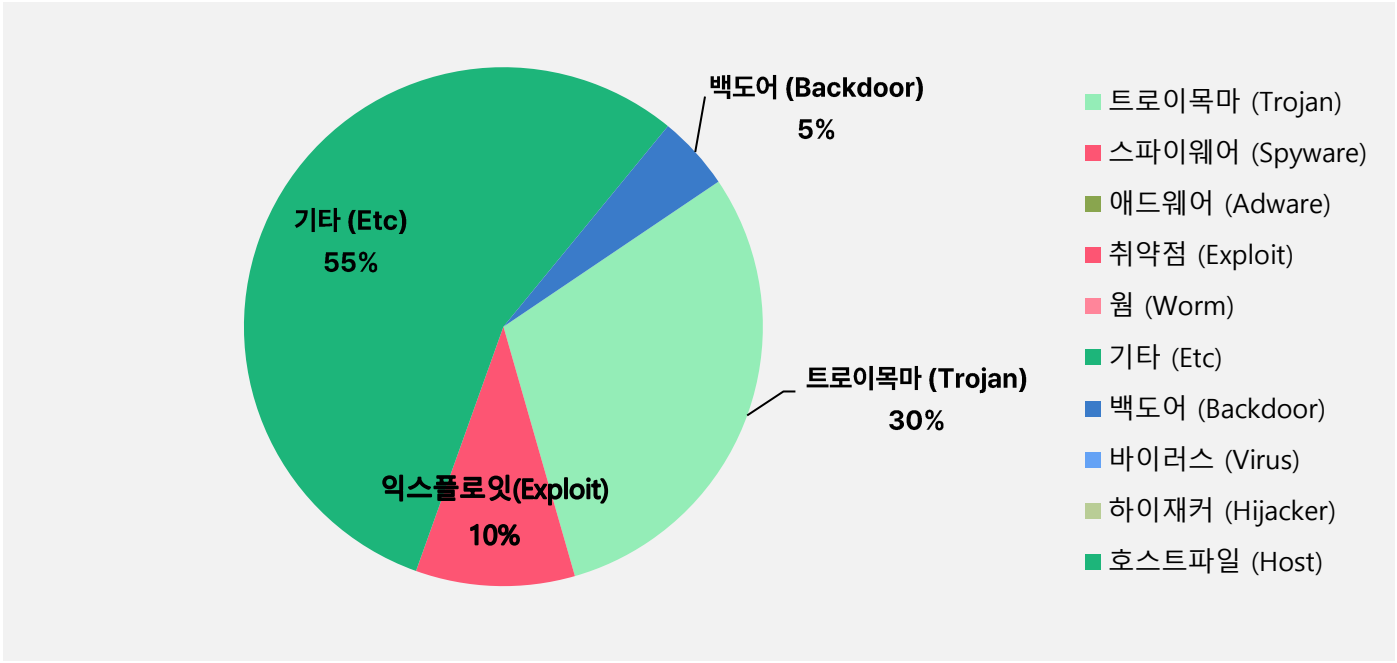
*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2024 년 7 월 1 일 ~ 2024 년 7 월 31 일

ESTsecurity Copyright©2024 ESTsecurity Corp. All rights reserved.

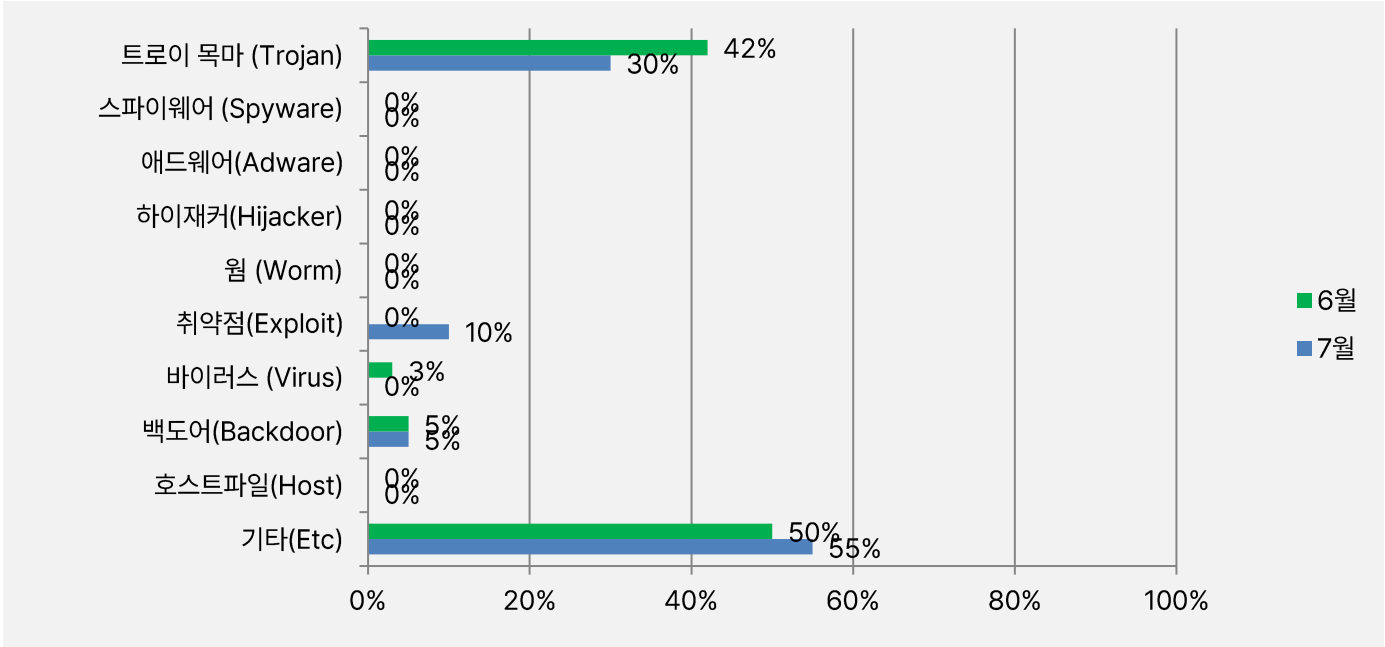
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 55%로 가장 높은 비율로 탐지되었으며, 그 다음으로 트로이목마 (Trojan) 유형이 30%, 취약점(Exploit) 10%, 백도어(Backdoor) 5%로 확인되었습니다.



카테고리별 악성코드 비율 전월 비교

2024 년 7 월에는 지난 6 월과 비교하였을 때 트로이목마(Trojan) 유형이 12% 감소하였고, 바이러스(Virus) 유형이 3% 감소하였습니다. 반면, 기타(ETC) 유형이 5% 증가하였으며 취약점(Exploit) 유형이 10%로 등장하였습니다.

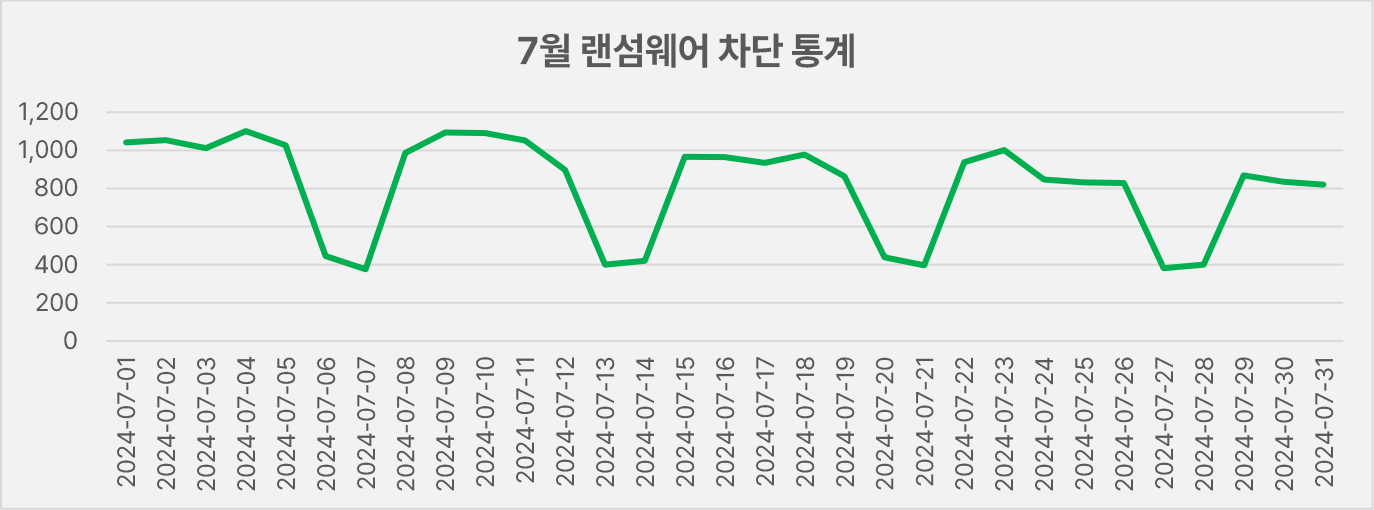


 Copyright©2024 ESTsecurity Corp. All rights reserved.

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 않습니다. 7 월 1 일부터 7 월 31 일까지 25,297 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 8,171,189 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 6 월 한 달간 확인되었던 7,803,314 건의 악성코드 경유지/유포지 URL 수에 비해 약 4.7%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.



ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

2

최신 보안 동향

ESTsecurity Copyright©2024 ESTsecurity Corp. All rights reserved.

2 분기 랜섬웨어 동향

1 분기, 전 세계적으로 악명을 떨친 락빗(LockBit) 랜섬웨어 조직과 블랙캣(Black Cat) 랜섬웨어 조직이 국제 사법기관들의 공조, 파트너들사 신뢰를 저버리는 행위 등의 이유로 영향력이 크게 약화되었습니다.

이 두 조직은 RaaS(Ransomware as a Service) 산업에서 가장 큰 영향력을 발휘하던 그룹으로 랜섬웨어의 기세가 꺾일 것으로 기대하였습니다. 하지만 기대와 다르게 이 틈을 타 랜섬허브(RansomHub), 킬섹(KillSec), 캐시(Cash) 랜섬웨어, 엘도라도(Eldorado) 등 다양한 RaaS 들이 우후죽순 등장하였습니다.

새로 등장한 RaaS 서비스 중 랜섬허브(RansomHub) RaaS 는 Go 언어와 C++언어로 제작된 멀티플랫폼(윈도우, 리눅스, ESXi) 서비스입니다. 랜섬허브 RaaS 는 파트너사에게 많은 제휴사 유치를 위해 높은 커미션을 제시하고, 실제로 매우 빠른 속도로 성장하고 있습니다. 일각에서는 코드 및 난독화 기술 등의 유사성을 언급하며 랜섬허브가 나이트(Knight) 랜섬웨어의 리브랜딩 버전이라는 의견도 있습니다.

해커그룹 킬섹(KillSec)이 KillSec RaaS 를 공개했습니다.

이 서비스는 Tor 네트워크를 사용하며 통계, 채팅, 빌드 기능 등 사용자들을 위해 다양한 편의성을 제공한다고 홍보하고 있습니다. 뿐만 아니라 향후 DDoS, 통화기능, 정보탈취 기능 등이 업데이트 될 예정이라고 밝혔습니다.

보안업체 소포스(Sophos)는 가격이 저렴하고 낮은 수준의 '정크건'(Junk Gun) 랜섬웨어에 대해 공개하였습니다.

이 랜섬웨어들은 기존의 파트너 기반의 구독형 RaaS 와는 다르게 독자적으로 운영되며 저렴한 가격이 특징입니다. 보고서에서 23 년 6 월부터 24 년 2 월 동안 수집한 19 가지 종류의 정크건 랜섬웨어 정보를 공개하였으며, 기존의 RaaS 들과 비교하였을 때 정교함과 기술력이 뒤떨어지지만 그에 반해 평균 가격이 400 달러로, 공격에 성공하면 얻은 수익의 전부를 가져간다는 점에서 많은 초보 해커들의 환영을 받고 있다고 밝혔습니다.

정크건 랜섬웨어들이 랜섬웨어 시장에 새로운 유형으로 자리 잡을지는 좀 더 지켜봐야겠습니다.

랜섬웨어 공격은 여전히 지속되었습니다.

케르베르(Cerber) 랜섬웨어 리눅스 변종이 CVE-2023-22518 취약점을 악용해 유포되는 것이 확인되었습니다.

CVE-2023-22518 는 아틀라시안 컨플루언스 데이터센터(Atlassian Confluence Data Center) 및 서버에 존재하는 취약점으로, 공격자들은 해당 취약점을 악용하여 관리자 계정을 생성하고 웹 셸을 통해 Cerber 랜섬웨어 리눅스 변종을 내려받은 후 실행합니다.

CVE-2023-22518 취약점 패치가 공개되었지만, 여전히 패치되지 않은 취약한 시스템을 타깃으로 공격이 지속되고 있는 만큼 보안담당자들의 빠른 패치가 필요합니다.

사용자들이 가짜 소프트웨어를 내려받도록 유도하는 캠페인도 발견되었습니다.

공격자들은 검색엔진에서 특정 소프트웨어를 검색할 때, 정상 Putty 및 WinSCP 프로그램 다운로드 페이지처럼 위장한 광고 페이지를 띄워 사용자로 하여금 가짜 소프트웨어를 내려받도록 유도합니다.

이 설치 패키지 내부에는 정상 exe 파일과 함께 악성 python311.dll 이 포함되어 있으며, 사용자가 셋업 파일 실행 시 DLL 사이드로딩(DLL Sideloading)을 통해 악성 dll 이 실행되고 최종적으로 랜섬웨어 배포를 시도합니다. 이런

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

공격방식은 블랙캣/알프브이(BlackCat/ALPHV) 랜섬웨어를 배포한 공격 캠페인과 유사하지만 랜섬웨어와 관련된 자세한 정보는 공개되지 않았습니다.

VMware ESXi 시스템을 타깃으로 하는 랜섬웨어 공격이 지속되고 있는 가운데, 보안전문가들이 ESXi 시스템을 타깃으로 하는 랜섬웨어 공격 패턴에 대해 공개하였습니다.

주로 피싱, 악성파일 다운로드, 취약점 등을 통해 최초 공격이 시도되며, 최초 공격이 성공하면 부르트 포스(brute force) 공격이나 기타 방식을 이용하여 ESXi 호스트 또는 vCenter 에 접근을 위한 권한상승을 시도 후 백업 시스템을 파괴하거나 암호화하고 데이터를 탈취합니다.

데이터 탈취 후에는 랜섬웨어를 실행시켜 ESXi 파일 시스템의 "/vmfs/volumes" 하위 디렉토리를 암호화하고, 가상화 되지 않은 워크스테이션과 서버에 랜섬웨어를 확산시킨다고 밝혔습니다.

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

㈜이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616

www.estsecurity.com