제공:

Trellix ADVANCED RESEARCH CENTER

위협 보고서

2023년 2월

목차

2022년 4분기 위협 개요

위협 행위자들은 2022년 말 여전히 만만치 않은 적으로 남아 있었습니다. 이에 수백 명의 엘리트 보안 분석가 및 연구원으로 구성된 Trellix Advanced Research Center에 더 많은 위협 인텔리전스 리소스를 추가하여 대응했습니다.

"즉, 위협 인텔리전스를 한 단계 더 발전시켰습니다. 더욱 단순한 보안으로 SecOps 혼란을 진정시키십시오. 부담을 경감하고 보안 성과를 성취할 수 있습니다. 위협은 계속해서 진화하고 있습니다. 그리고 여러분도 함께 진화할 수 있습니다."

본 보고서에서는 지난 분기 어떠한 위협 행위자와 제품군, 캠페인 및 즐겨 찾는 기술이 널리 사용되었는지에 관해 업계를 선도하는 정보를 공유합니다. 그것이 전부가 아닙니다. 우리는 랜섬웨어 유출 사이트 및 보안 업계 보고서에서 데이터를 수집하기 위한 소스를 확장했습니다. Trellix의 리소스가 증가하게 되면 네트워크 보안, 클라우드 사고, 엔드포인트 사고 및 보안 운영을 다루는 새로운 콘텐츠를 포함한 위협 연구 범주 역시 증가합니다.

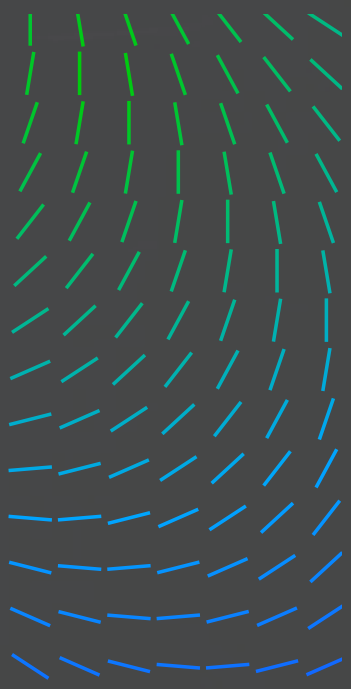
마지막 위협 보고서 이후 Trellix Advanced Research Center는 4분기에 우크라이나를 대상으로 한 사이버 공격을 크게 증가시킨 Gamaredon 링크를 포함한 전 세계의 연구 및 조사 결과에 참여했으며 61,000개의 취약한 공개 소스 프로젝트 패치를 적용하고 2023년도 위협 예측을 통해 2023년의 새로운 공격에 관한 인사이트를 제공했습니다.

다음 개요는 이러한 위협 보고서의 개선 사항에서 수집한 것으로, Trellix Advanced Research Center가 고객과 보안 업계가 위협의 결과에 대해 더 잘 이해할 수 있도록 제시하는 사례입니다.

랜섬웨어

- 4분기 가장 영향력 있는 랜섬웨어 그룹인 LockBit 3.0에 대한 브레이크아웃 연구
- 랜섬웨어는 전 세계, 특히 미국에서 지속적으로 만연
- 랜섬웨어는 공산품 및 서비스 섹터를 대상으로 함

2022년 4분기 위협 개요



국가

- 국가를 대상으로 한 섹터에는 정부, 운송 및 해운이 포함
- 미국 기업은 국가 활동에 영향을 받음

Living Off the Land(LOLBIN)

- Trellix Advanced Research Center의 헌팅 방법을 사용하여 만연한 Cobalt Strike에 대한 인사이트 확장
- Cobalt Strike 팀 서버 중 다수는 중국 클라우드 제공업체에서 호스팅
- Windows Command Shell은 보고된 캠페인에 사용된 가장 널리 사용되는 상위 10개 OS 바이너리 중 거의 절반을 차지

위협 행위자

- 중국, 북한 및 러시아가 위협 행위자가 만연한 국가 중 가장 상위에 위치

이메일 보안 경향

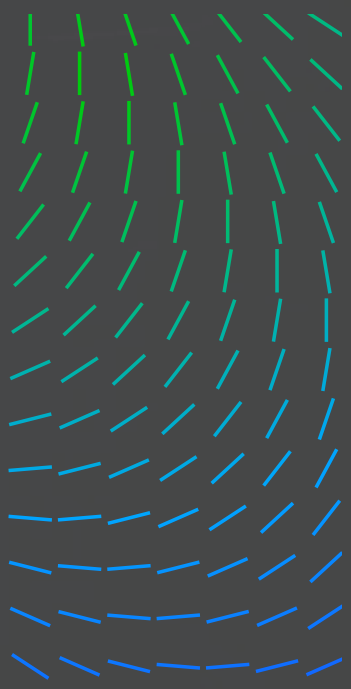
- 월드컵 기간 동안 아랍 국가들에서 악성 이메일의 양이 크게 증가
- 가장 기술을 포함한 피싱 및 보이스 피싱 캠페인에 대한 인사이트와 보이스 피싱에 사용되는 인기 있는 회사 테마

네트워크 보안

- 분기별 가장 큰 영향을 미치고, 중요하며 관련성이 높은 공격과 WebShell, 도구 및 기술

Trellix XDR에서 제공하는 보안 운영 원격 측정

- 널리 사용되는 보안 경고, 익스플로잇, 로그 소스 및 MITRE ATT&CK 기술
- 클라우드 사고
- Azure, AWS 및 GCP용 기술 및 탐지
- 최고의 기술 및 탐지

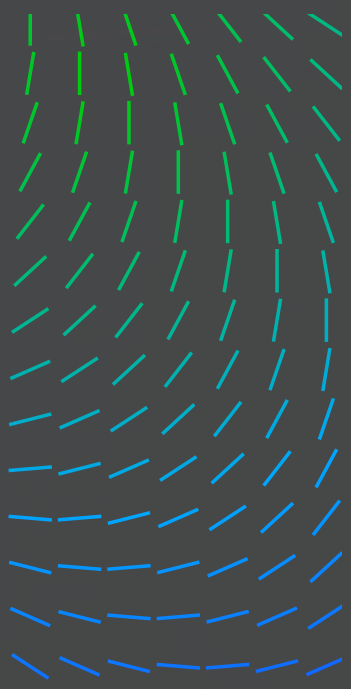


위협 인텔리전스 책임자의 편지

Trellix Advanced Research Center 팀은 한 해를 마무리하며 2022년 4분기 위협 보고서 데이터를 처음으로 공유할 수 있게 되어 기쁘게 생각합니다. 본 보고서는 랜섬웨어 유출 사이트 및 만연한 인프라 추적과 같은 기타 데이터 소스에서의 인사이트와 결합된 당사 제품 센서 배열에서의 새로운 데이터를 포함하여 계속해서 진화하고 있습니다. Trellix는 위협 행위자와 그들의 동기가 절대 멈추지 않으며, 더욱 다각적으로 나타나고 있기에, 이러한 악으로부터 당사의 고객을 보호하기 위한 임무를 계속해서 끈질기게 수행하고 있습니다. 지정학적, 경제적 전망이 더 높은 수준의 불확실성으로 인해 여전히 복잡한 상황에서 글로벌 위협 인텔리전스의 필요성이 증가하고 있습니다.

우크라이나 전쟁으로 인한 전 세계적인 경제적 불확실성은 1970년대 이후 볼 수 없었던 강력한 에너지 가격에서의 충격을 유발하였으며 이러한 상황은 세계 경제에 막대한 타격을 주고 있습니다. 유럽에서 다시 벌어진 전쟁은 특히 사이버 공간에서 EU의 보안 및 방어 접근법 및 자국 이익을 방어할 수 있는 능력에 관해 의문을 제기하는 이들에게 경종을 울렸습니다. 또한 미 행정부는 전략 지정학적 경쟁을 해결하고 중요 인프라를 보호하며 외국의 정보 조작 및 간섭에 맞서 싸워야 할 필요성을 인식했습니다. SolarWinds와 Hafnium, 우크라이나 및 기타 이벤트는 새로운 보안 표준과 국가의 책임 및 지난 미 정부의 업무를 기반으로 한 기금 조성에 관한 행정부와 의회의 초당적 조치를 촉구하는 계기가 되었습니다. 그렇다면 이러한 불확실성은 비즈니스와 공적 및 사적 기관은 물론 민주적인 가치의 사이버 보안에 어떠한 영향을 미치고 있을까요?

지난 분기에 우리 팀은 정치적, 경제적 및 영토적 야망을 위해 정탐과 전쟁 및 허위 정보 분야에서 사이버 공간의 치국책이 적극적으로 사용되고 있음을 확인했습니다. 또한 우크라이나 전쟁에서 새로운 형태의 사이버 공격의 출현 및 사이트를 훼손하고 정보를 유출하며 DDoS 공격을 실행하는 핵티비스트의 행동이 더욱 능숙하고 대담해졌음을 확인할 수 있었습니다. 한편 전통적 형태의 사이버 공격도 계속되고 있습니다. 피싱과 같이 개인을 속이고 조작하여 기밀이나 개인 정보를 누설하는 소셜 엔지니어링 술책도 여전히 널리 퍼져 있습니다.



랜섬웨어는 여전히 전 세계 많은 조직에 해를 입히고 있습니다. 코로나19의 세계적 대유행 동안 확인한 것처럼 사이버 범죄자들은 위기와 불확실성의 시기에 빠르게 수익을 얻습니다. 위협 환경이 진화함에 따라, 우리의 연구도 함께 진화할 것입니다. 우리의 임무는 항상 제품의 효율성을 개선하고 실행 가능한 인텔리전스를 투자자에게 제공하여 가장 중요한 것을 보호할 수 있도록 하는 것에 전적으로 집중하고 있습니다. 이 보고서에서 우리가 하는 일이 Trellix Advanced Research Center의 모든 구성원에게 얼마나 중요한지 확인하실 수 있을 것입니다. 우리 팀의 연구자나 전문가와 같은 모든 구성원은 모든 프로젝트에 최선을 다하고 있습니다.

확장 보고서에 관한 귀하의 의견과 더 알아보고 싶은 분야가 있으신 경우 당사 Twitter @TrellixARC를 통해 알려주시기 바랍니다. 또한 4월에 샌프란시스코에서 개최되는 RSA에서 뵐 수 있기를 고대하고 있습니다.

John Fokker
위협 인텔리전스 책임자

방법론

Trellix의 백엔드 시스템은 분기별 위협 보고서에 대한 입력으로 사용되는 원격 측정을 제공합니다. Trellix는 위협에 대한 공개 소스 인텔리전스 및 랜섬웨어, 국가 활동 등과 같은 널리 퍼진 위협에 대한 자체 조사와 원격 측정을 결합합니다.

원격 측정에 대해 이야기할 때 Trellix는 감염이 아닌 탐지에 대해 이야기합니다. 탐지는 파일, URL, IP 주소 또는 기타 표시기가 당사 제품 중 하나에서 탐지되어 당사에 다시 보고될 때 기록됩니다.

예를 들어 당사에서는 실제 맬웨어 샘플을 배포하는 효율성 테스트 프레임워크를 사용하는 조직이 점점 증가하고 있다는 사실을 알고 있습니다. 이러한 사용의 경우에는 탐지로 표시되지만, 감염은 확실히 아닙니다.

원격 측정에서 잘못된 긍정을 분석하고 필터링하는 프로세스는 지속적으로 개발이 진행되고 있으며 이를 통해 이전 버전과 비교 시 새로운 위협 범주가 생성될 수 있습니다.

본 분기별 보고서에 함께하는 Trellix 조직 팀이 점점 더 증가하고 있으므로 새로운 위협 범주도 추가될 예정입니다.

고객의 개인 정보는 매우 중요합니다. 이는 원격 측정 및 고객의 섹터 및 국가에 매핑할 때 중요합니다. 국가별로 클라이언트 기반이 다르며 숫자가 증가를 나타낼 수 있지만 그러려면 데이터를 더 자세히 살펴보아야 합니다. 예를 들어 통신 섹터는 데이터에서 높은 점수를 받는 경우가 많습니다. 이는 이 섹터가 반드시 고도로 타겟팅되어 있다는 의미는 아닙니다. 통신 섹터에는 회사가 구매할 수 있는 자체 IP 주소 공간과 ISP 공급자가 포함됩니다. 이 메시지의 의미는 무엇입니까? ISP의 IP 주소 공간에서 제출된 항목은 통신 탐지로 표시되지만 다른 섹터에서 작동하는 ISP 클라이언트에서 전송된 것일 수 있습니다.

2022년 4분기 랜섬웨어

이 섹션에서는 랜섬웨어 그룹 활동에 관해 수집한 다양한 인사이트를 제공합니다. 이 정보는 위협 환경을 더 잘 파악하고, 관찰 편향을 줄이며 어떤 랜섬웨어 제품군이 2022년 4분기에 가장 영향력이 컸는지 판단하는 데 유용하게 사용할 수 있도록 다양한 소스에서 수집되었습니다. 첫 번째는 정량적 소스로 랜섬웨어 IOC와 Trellix 고객 원격 측정의 상관 관계에서 추출한 랜섬웨어 캠페인 통계를 나타냅니다. 두 번째는 정성적 소스로 보안 업계에서 발행한 다양한 보고서에 대해 위협 인텔리전스 그룹에서 조사하고 분석하고 검토한 내용을 나타냅니다. 마지막으로 새로운 범주인 세 번째 소스는 다양한 랜섬웨어 그룹의 "유출 사이트"에서 스크랩하여 표준화와 보강 및 분석을 진행한 다음 익명 버전으로 결과를 제공한 랜섬웨어 피해자 보고서 세트로 구성되어 있습니다.

당사의 목표는 다양한 관점을 제공함으로써 현재 위협 환경을 구성하는 많은 퍼즐 조각을 제공하는 것입니다. 각기 제한 사항이 존재하므로 충분하지 않습니다. 그 누구도 인터넷에 연결된 모든 시스템의 모든 로그에 액세스할 수 없으며 모든 보안 사고가 보고되는 것도 아니며 모든 피해자가 탈취당하고 유출 사이트에 포함되는 것도 아닙니다. 그러나 서로 다른 관점의 조합은 각자의 사각지대를 줄여 다양한 위협을 더 잘 이해할 수 있습니다.

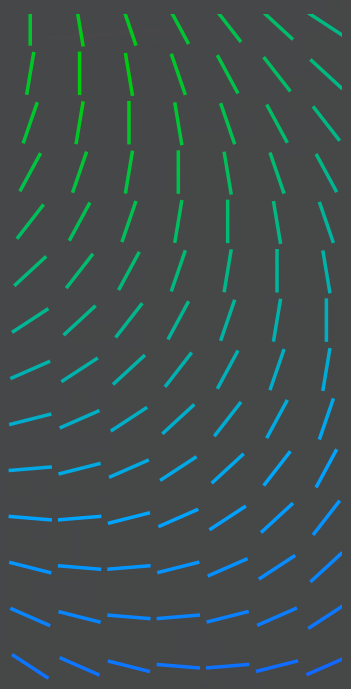
정보를 기반으로 한 판단이란 소스의 정량적 데이터와 정성적 데이터를 결합하면서 동시에 잠재적 문제점과 사각지대를 고려한 결과입니다.

2022년 4분기 랜섬웨어 주요 사항

4분기에 가장 큰 영향을 미친 랜섬웨어 그룹: LockBit 3.0

Trellix의 다양한 소스를 관찰한 결과 2022년 4분기에 가장 큰 영향을 미친 랜섬웨어 그룹이 LockBit 3.0이라는 결론을 내릴 수 있었습니다. LockBit 3.0이 선정된 이유는 다음과 같은 특징 때문입니다.

3위 Trellix의 글로벌 센서에서 수집한 랜섬웨어 원격 측정 분석에 따르면 LockBit 3.0은 해당 분기에 가장 널리 퍼져 있는 랜섬웨어 그룹 중 3위를 차지했습니다.



2위 LockBit 3.0은 위협 인텔리전스 그룹에서 수집한 다양한 캠페인에서 분석한 것과 같이 Cuba 랜섬웨어와 함께 보안 업계에서 가장 많이 보고된 랜섬웨어에서 2위를 차지했습니다.

1위 LockBit 3.0 유출 사이트에서는 해당 분기의 랜섬웨어 그룹 중 가장 많은 피해자가 보고되었습니다. LockBit은 피해자들에게 이름을 지정하고 수치심을 주어 가장 열성적으로 압박을 가합니다.

다음은 2022년 4분기 LockBit 범주 및 결과입니다.

2022년 4분기 LOCKBIT 3.0에 영향을 받은 섹터

29%

LockBit 3.0 피해자 유출 사이트에 따르면 2022년 4분기 LockBit 3.0의 영향을 가장 많이 받은 섹터는 공산품 및 서비스였습니다.

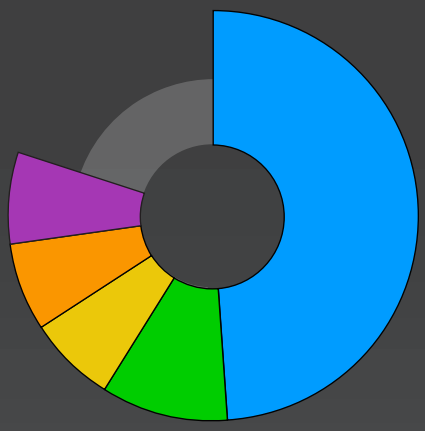
- 공산품 및 서비스
- 소매
- 기술
- 보건의료
- 건설 및 자재
- 개인 및 생활용품
- 정부

2022년 4분기 LOCKBIT 3.0에 영향을 받은 회사의 국가

49%

LockBit 3.0 피해자 유출 사이트에 따르면 2022년 4분기 LockBit 3.0의 영향을 가장 많이 받은 국가는 미국 기업(49%)이었으며, 영국 기업이 그 뒤를 이었습니다.

- 미국
- 영국
- 캐나다
- 프랑스
- 브라질



LockBit 3.0 도구 및 익스플로잇

LOCKBIT 3.0에 의해 공격을 받은 것으로 알려진 취약성

CVE-2018-13379
CVE-2020-0787
CVE-2021-20028
CVE-2021-34473
CVE-2021-34523

LOCKBIT 3.0에서 사용된 악성 도구

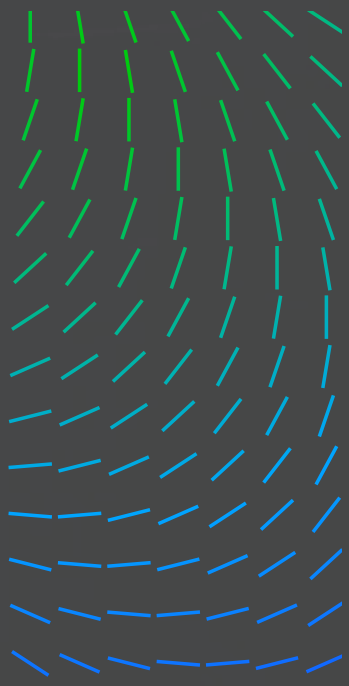
Amadey	Hakops
Blister	Neshta
BloodHound	SocGholish
Cobalt Strike	StealBit
Grabff	WinPEAS

LOCKBIT 3.0에서 사용된 비악성 도구

BCDEdit	MiniDump	NSIS	Schtasks.exe
Cmd	MpCmdRun.exe	PCHunter	VSSAdmin
Fltmc.exe	Mshta	PowerShell	wevtutil
Fsutil	Mstsc	Process Monitor	WMIC
GMER	Netsh	Rundll32	RCLONE
MEGASYNC	Nltest		

원격 측정을 통해 보는 랜섬웨어

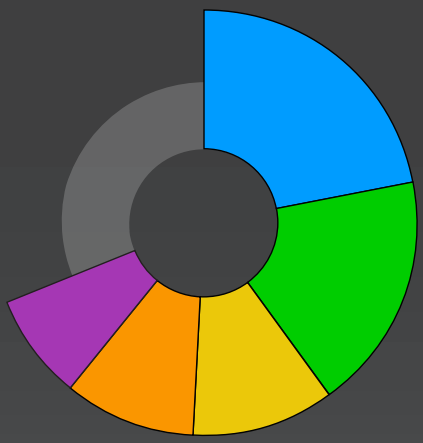
다음 통계는 당사의 원격 측정과 위협 인텔리전스 기술 자료 간 상관 관계를 기반으로 합니다. 분석 단계 다음으로 선택한 시간 동안의 데이터에서 캠페인 세트를 식별하고 해당 특성을 추출합니다. 탐지 자체가 아닌 캠페인 통계가 표시됩니다. Trellix의 글로벌 원격 측정을 통해 다양한 랜섬웨어 그룹의 여러 캠페인에 속하는 침해 지표(IoC)를 보여줍니다. 다음의 랜섬웨어 제품군은 각각의 도구 및 기술을 사용하며, 확인된 캠페인에서 가장 널리 사용되는 제품군을 나타냅니다. 마찬가지로 확인된 캠페인의 영향을 가장 많이 받은 국가, 섹터는 다음과 같습니다.



2022년 4분기 가장 널리 사용된 랜섬웨어 제품군

22%

2022년 4분기에 전 세계적으로 가장 널리 사용된 랜섬웨어 제품군은 Cuba였습니다. Zeppelin은 Vice Society에서 자주 사용되었습니다. Yanluowang의 통신 유출 자세히 알아보기



- Cuba
- Hive
- LockBit
- Zeppelin
- Yanluowang

2022년 4분기 랜섬웨어 그룹에서 가장 널리 사용된 악성 도구

41%

2022년 4분기에 랜섬웨어 그룹에서 가장 널리 사용된 악성 도구는 Cobalt Strike였습니다.

1.	Cobalt Strike	41%
2.	Mimikatz	23%
3.	BURNTCIGAR	13%
4.	VMProtect	12%
5.	POORTRY	11%

2022년 4분기 랜섬웨어 그룹에서 가장 널리 사용된 MITRE-ATT&CK 기술

1.	강력한 데이터 암호화	17%
2.	시스템 정보 검색	11%
3.	PowerShell	10%
4.	인그레스 도구 전송	10%
5.	Windows Command Shell	9%

2022년 4분기 랜섬웨어 그룹에서 가장 널리 사용된 비악성 도구

21%

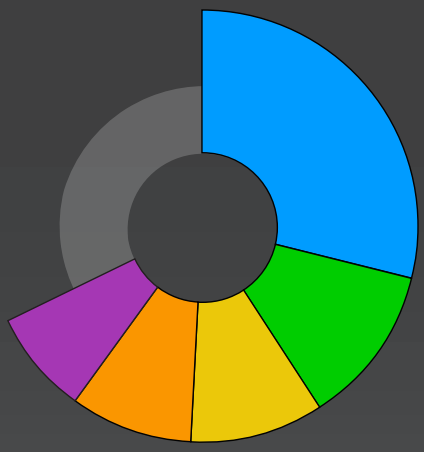
2022년 4분기에 랜섬웨어 그룹에서 가장 널리 사용된 비악성 도구는 Cmd였습니다.

1.	Cmd	21%
2.	PowerShell	14%
3.	Net	10%
4.	Reg	8%
5.	PsExec	8%

2022년 4분기 랜섬웨어 그룹의 영향을 가장 많이 받은 국가

29%

Trellix의 원격 측정에 따르면 2022년 4분기 랜섬웨어 그룹의 영향을 가장 많이 받은 국가는 미국이었습니다.

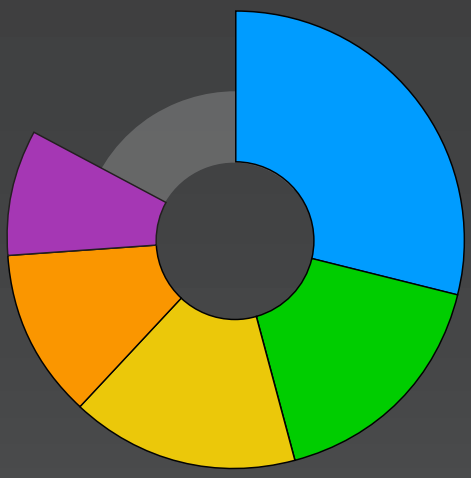


- 미국
- 중국
- 카타르
- 일본
- 인도네시아

2022년 4분기 랜섬웨어 그룹의 영향을 가장 많이 받은 섹터

29%

Trellix의 원격 측정에 따르면 2022년 4분기 랜섬웨어 그룹의 영향을 가장 많이 받은 섹터는 아웃소싱 및 호스팅이었습니다. 랜섬웨어 유출 사이트에 나열된 피해자의 평균 조직 크기와 상관 관계가 있는 것이며 해당 조직에는 자체적으로 할당된 IP 블록이 없고, 타사 호스팅 제공업체에게 의존하고 있습니다.



- 아웃소싱 및 호스팅
- 은행/금융/자산 관리
- 정부
- 도매
- 제약

보안 업계에서 보고된 랜섬웨어

다음 통계는 공개 보고서 및 사내 연구를 기반으로 합니다. 모든 랜섬웨어 사고가 보고된 것은 아닙니다. 많은 랜섬웨어 제품군이 한동안 활발한 활동을 펼쳤으며, 자연스럽게 특정 분기 동안에는 신종 제품군보다는 주목을 받지 못합니다. 이러한 기준에 따라 해당 메트릭은 보안 업계가 분기에 가장 영향력 있고 관련성이 높다고 확인한 랜섬웨어 제품군을 나타내는 지표입니다.

2022년 4분기 가장 많이 보고된 랜섬웨어 제품군

15%

보안 업계 보고서에 따르면 2022년 4분기에 가장 많이 보고된 랜섬웨어 제품군은 Black Basta 랜섬웨어와 Magniber 랜섬웨어였습니다.

2022년 4분기 가장 많이 사용된 랜섬웨어 제품군 공격 기술

19%

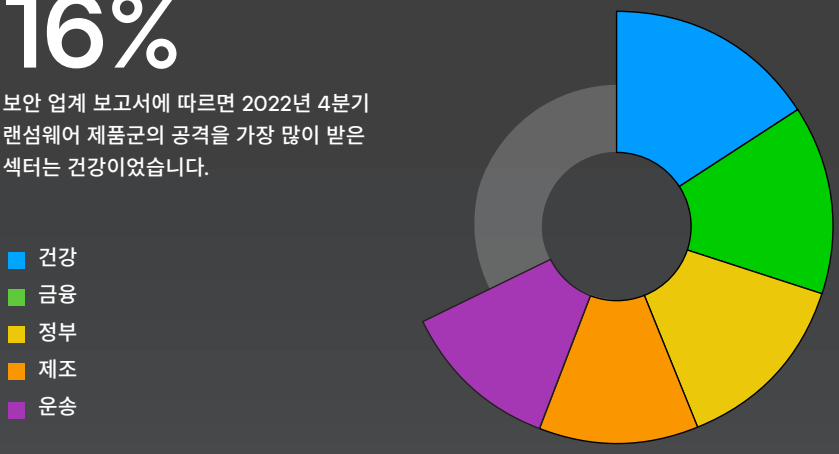
보안 업계 보고서에 따르면 2022년 4분기에 가장 많이 보고된 랜섬웨어 제품군 공격 기술은 강력한 데이터 암호화였습니다.

1.	강력한 데이터 암호화	19%
2.	Windows Command Shell	11%
3.	시스템 정보 검색	10%
4.	인그레스 도구 전송	10%
5.	PowerShell	10%

2022년 4분기 랜섬웨어 제품군의 공격을 가장 많이 받은 섹터

16%

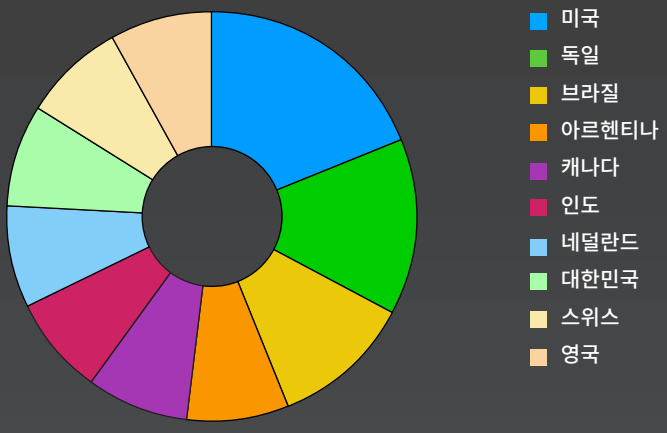
보안 업계 보고서에 따르면 2022년 4분기 랜섬웨어 제품군의 공격을 가장 많이 받은 섹터는 건강이었습니다.



2022년 4분기 랜섬웨어 제품군의 공격을 가장 많이 받은 국가

19%

보안 업계 보고서에 따르면 2022년 4분기 랜섬웨어 제품군의 공격을 가장 많이 받은 국가는 미국이었습니다.



2022년 4분기 랜섬웨어 제품군에서 사용된 CVE

1.	CVE-2021-31207	16%
	CVE-2021-34474	16%
	CVE-2021-34523	16%
2.	CVE-2021-34527	13%
3.	CVE-2021-26855	9%
	CVE-2021-27065	9%

2022년 4분기 랜섬웨어 제품군에서 사용된 악성 도구

44%

보안 업계 보고서에 따르면 2022년 4분기 랜섬웨어 제품군에서 가장 많이 사용된 악성 도구는 Cobalt Strike였습니다.

1.	Cobalt Strike	44%
2.	QakBot	13%
3.	IcedID	9%
4.	BURNTCIGAR	7%
5.	Carbanak SystemBC	7% 7%

2022년 4분기 랜섬웨어 제품군에서 사용된 비악성 도구

21%

보안 업계 보고서에 따르면 2022년 4분기 랜섬웨어 제품군에서 가장 많이 사용된 비악성 도구는 PowerShell이었습니다.

1.	PowerShell	21%
2.	Cmd	18%
3.	Rundll32	11%
4.	VSSAdmin	10%
5.	WMIC	9%

2022년 4분기 랜섬웨어 "유출 사이트" 피해자 보고서

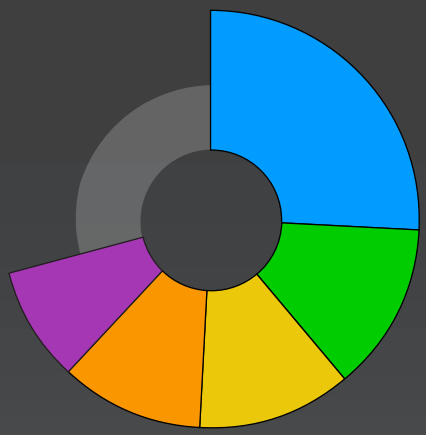
이 섹션의 데이터는 다양한 랜섬웨어 그룹의 "유출 사이트"를 스크랩하여 컴파일한 것입니다. 랜섬웨어 그룹은 이러한 웹사이트에 피해자에 관한 정보를 게시하여 피해자를 갈취합니다. 협상이 지연되거나, 피해자들이 랜섬웨어 그룹의 기한까지 몸값 지불을 거부하면 랜섬웨어 그룹은 피해자로부터 훔친 정보를 공개합니다. 당사는 오픈 소스 도구인 RansomLook을 사용해 다양한 게시글을 수집하고 해당 데이터를 내부 프로세스를 거쳐 결과를 정규화 및 강화하여 익명화된 버전의 피해자 연구 분석을 제공합니다.

여기서 중요한 점은 모든 랜섬웨어 피해자가 각 유출 사이트에 보고되는 것이 아니라는 사실입니다. 많은 피해자가 몸값을 지불하여 사이트에 보고되지 않습니다. 이러한 메트릭은 랜섬웨어 그룹이 갈취하거나 보복한 피해자 지표이며, 이는 총피해자 수와 혼동해서는 안 됩니다.

2022년 4분기 가장 많은 피해자가 보고된 랜섬웨어 그룹

26%

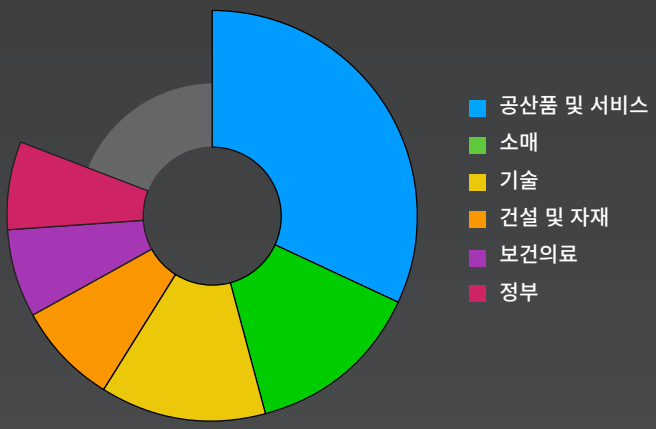
LockBit 3.0은 2022년 4분기에 각 유출 사이트에서 가장 많은 피해자가 보고된 상위 10개 랜섬웨어 그룹 중 26%를 차지했습니다.



2022년 4분기 유출 사이트별 랜섬웨어 그룹의 영향을 받는 섹터

32%

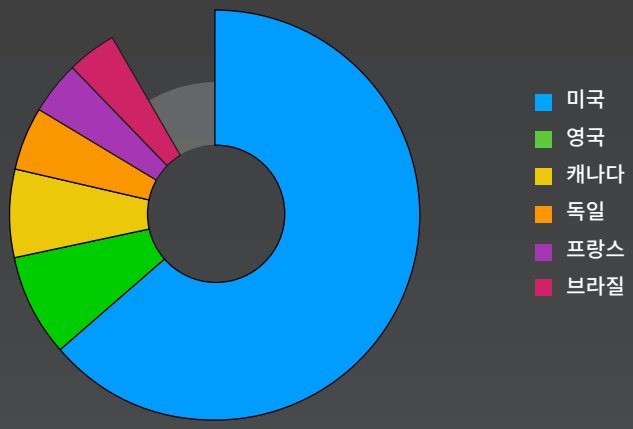
2022년 4분기에 유출 사이트별 랜섬웨어 그룹의 영향을 가장 많이 받은 산업은 공산품 및 서비스였습니다. 공산품 및 서비스는 주로 건설 및 제조에 사용되는 모든 자제 및 무형의 서비스를 포함하는 산업입니다.



2022년 4분기 유출 사이트별 랜섬웨어 그룹의 영향을 받는 기업의 국가

63%

2022년 4분기 유출 사이트별 다양한 랜섬웨어 그룹에서 보고한 상위 10개 기업 중에서 63%가 미국 기업이었으며, 영국(8%)과 캐나다(7%)가 그 뒤를 이었습니다.



2022년 4분기 국가 통계

이 섹션에서는 국가 그룹 활동에 관해 수집한 인사이트를 제공합니다. 이 정보는 위협 환경을 더 잘 파악하고, 관찰 편향을 줄일 수 있도록 다양한 소스에서 수집되었습니다. 먼저, 국가 그룹 IOC와 Trellix 고객 원격 측정의 상관 관계에서 추출한 통계를 나타냅니다. 두 번째로 보안 업계에서 발행한 다양한 보고서에 대해 위협 인텔리전스 그룹에서 조사, 분석 및 검토한 내용에 대한 인사이트를 제공합니다.

2022년 4분기 국가 주요 사항

· 미국과 독일에서 국가 공격이 크게 증가했습니다.
· 중국과 베트남에서 4분기 국가 공격이 생겼습니다.

글로벌 원격 측정을 통해 보는 국가 통계

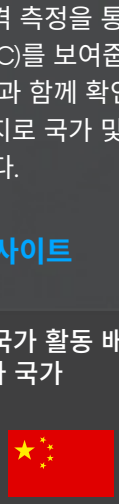
이 통계는 당사의 원격 측정과 위협 인텔리전스 기술 자료 간 상관 관계를 기반으로 합니다. 분석 단계 다음에는, 선택한 기간의 데이터에서 캠페인 세트를 식별하고 해당 특성을 추출합니다. 탐지 자체가 아닌 캠페인 통계가 표시됩니다. 다양한 로그 집계, 고객의 위협 시뮬레이션 프레임워크 사용, 위협 인텔리전스 기술 자료와의 높은 수준의 상관 관계로 인해 데이터가 원하는 기준을 충족하도록 수동 필터링됩니다.

Trellix의 글로벌 원격 측정을 통해 지능형 지속 공격 그룹(APT)의 여러 캠페인과 관련된 침해 지표(IoC)를 보여줍니다. 다음 위협 행위자의 국가 및 위협 행위자는 각각의 도구 및 기술과 함께 확인된 캠페인에서 가장 널리 퍼져 있는 것을 나타냅니다. 마찬가지로 국가 및 섹터에 대한 데이터가 확인된 캠페인의 영향을 가장 많이 받았습니다.

국가 원격 측정 인사이트

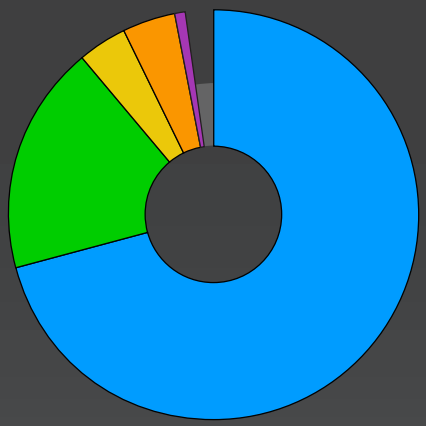
2022년 4분기 국가 활동 배후에 가장 널리 퍼져 있는 위협 행위자 국가

71%



2022년 4분기 국가 활동 배후에 가장 널리 퍼져 있는 위협 행위자 국가는 중국이었습니다.

- 중국
- 북한
- 러시아
- 이란
- 레바논

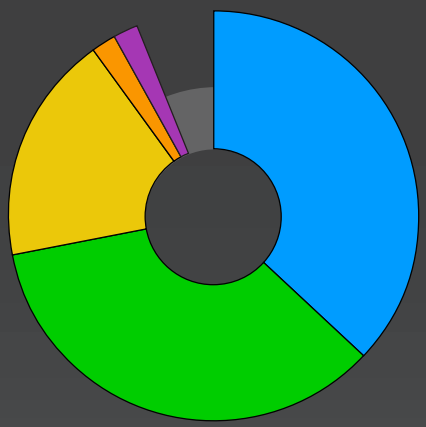


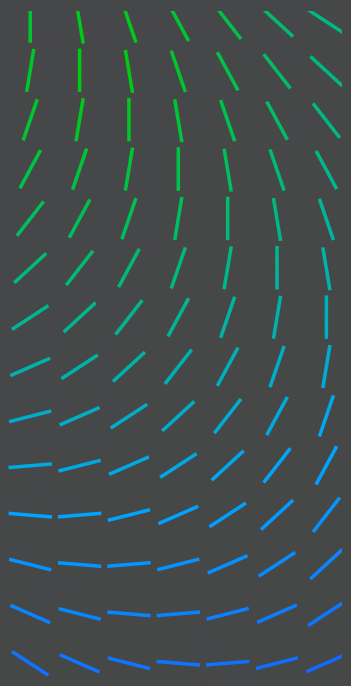
2022년 4분기 가장 널리 퍼져 있는 위협 행위자 그룹

37%

국가 원격 측정에 따르면 2022년 4분기 가장 널리 퍼져 있는 위협 행위자 그룹은 Mustang Panda였습니다.

- Mustang Panda
- UNC4191
- Lazarus
- MuddyWater
- Kimsuky





2022년 4분기 국가 활동에서 가장 널리 사용된 MITRE ATT&CK 기술

1.	DLL 사이드 로딩	14%
2.	Rundll32	13%
3.	파일 또는 정보 난독화	12%
4.	Windows Command Shell	11%
5.	레지스트리 실행 키/시작 폴더	10%

2022년 4분기 국가 활동에서 가장 널리 사용된 악성 도구

1.	PlugX	24%
2.	BLUEHAZE	23%
3.	DARKDEW	23%
4.	MISTCLOAK	23%
5.	JSX 원격 액세스 트로이 목마	2%

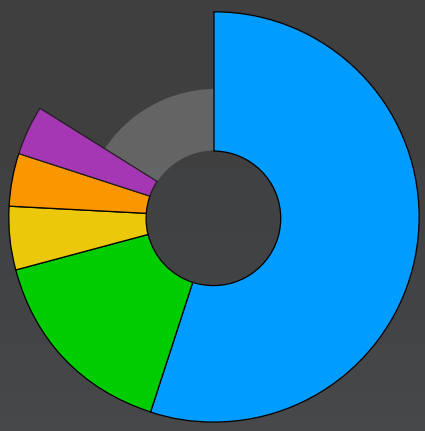
2022년 4분기 국가 활동에서 가장 널리 사용된 비악성 도구

1.	Rundll32	22%
2.	Cmd	19%
3.	Reg	17%
4.	Ncat	12%
5.	Regsvr32	6%

2022년 4분기 국가 활동에 가장 많은 영향을 받은 국가

55%

2022년 4분기 국가 활동에 가장 많은 영향을 받은 국가는 미국이었습니다.

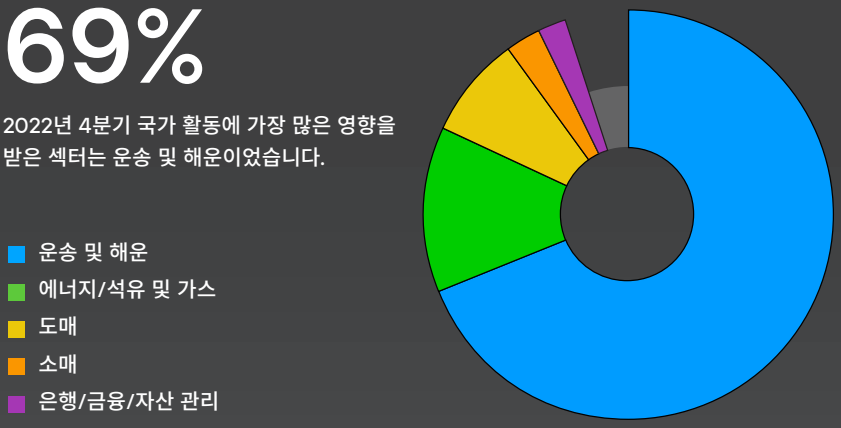


- 미국
- 베트남
- 인도
- 독일
- 중국

2022년 4분기 국가 활동에 가장 많은 영향을 받은 섹터

69%

2022년 4분기 국가 활동에 가장 많은 영향을 받은 섹터는 운송 및 해운이었습니다.



2022년 4분기 공개 보고서에 따른 국가 사고

이러한 통계는 고객 로그를 통한 원격 측정이 아닌 공개 보고서 및 사내 연구를 기반으로 합니다. 모든 국가 사고가 보고된 것은 아닙니다. 많은 캠페인은 이미 알려져 있고, 보고하기에 덜 매력적이기도 한 동일한 TTP를 따릅니다. 업계에서는 행위자가 새로운 것을 시도했거나 실수를 한 신종 캠페인을 선택하는 경향이 있습니다. 이러한 메트릭은 2022년 4분기 동안 업계에서 인사이트와 관련성이 있다고 판단한 지표입니다.

2022년 4분기 국가 캠페인에 가장 많이 보고된 위협 행위자 국가

37%

2022년 4분기에 공개적으로 보고된 국가 캠페인의 37%는 중국에서 발생했습니다.

1.	중국	37%
2.	북한	24%
3.	이란	1%
4.	러시아	1%
5.	인도	1%

2022년 4분기 국가 활동에 보고된 가장 널리 퍼져 있는 위협 행위자

33%

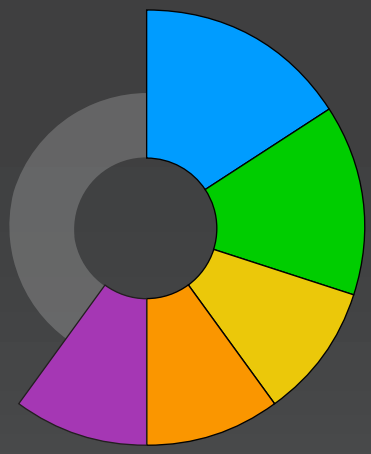
2022년 4분기 국가 활동에 보고된 가장 널리 퍼져 있는 위협 행위자는 Lazarus였습니다.

1.	Lazarus	33%
2.	Mustang Panda	17%
3.	APT34 APT37 APT41 COLDRIVER Patchwork Polonium SideWinder Winnti Group	각 1%

2022년 4분기 국가 캠페인에 보고된 가장 많이 표적이 된 국가

16%

2022년 4분기 국가 캠페인에 보고된 가장 많이 표적이 된 국가는 미국이었습니다.

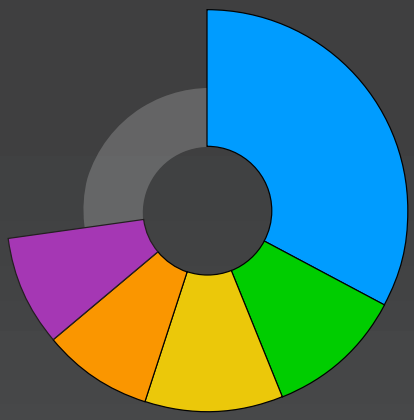


- 미국
- 영국
- 파키스탄
- 러시아
- 우크라이나

2022년 4분기 국가 캠페인에 보고된 가장 많이 표적이 된 섹터

33%

2022년 4분기 국가 캠페인에 보고된 가장 많이 표적이 된 섹터는 정부였으며, 군대(11%)와 통신(11%)이 그 뒤를 이었습니다.



- 정부
- 군대
- 통신
- 에너지
- 금융

2022년 4분기 국가 캠페인에 보고된 가장 인기 있는 악성 도구

1.	PlugX	22%
2.	Cobalt Strike	17%
3.	Metasploit	13%
4.	BlindingCan	9%
5.	Scanbox ShadowPad ZeroCleare	각 9%

2022년 4분기 국가 캠페인에서 사용된 가장 인기 있는 비악성 도구

1.	Cmd	32%
2.	Rundl132	20%
3.	PowerShell	14%
4.	Reg	8%
5.	Schtasks.exe	7%

2022년 4분기에 보고된 국가 캠페인에서 사용된 가장 인기 있는 MITRE ATT&CK 기술

1.	인그레스 도구 전송	13%
2.	시스템 정보 검색	13%
3.	파일 또는 정보 난독화	12%
4.	웹 프로토콜	11%
5.	파일 또는 정보 정체 밝히기/디코드	11%

2022년 4분기 국가 캠페인에 보고된 취약성 공격 관찰

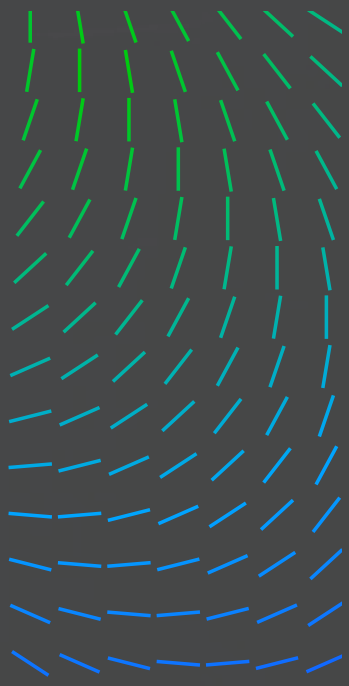
CVE-2017-11882
CVE-2021-44228
CVE-2018-0802
CVE-2021-26855
CVE-2021-27065
CVE-2021-34473
CVE-2021-34523
CVE-2015-2545
CVE-2017-0144
CVE-2018-0798
CVE-2018-8581
CVE-2019-0604
CVE-2019-0708
CVE-2019-16098
CVE-2020-0688
CVE-2020-1380
CVE-2020-1472
CVE-2020-17141
CVE-2020-17143
CVE-2021-21551
CVE-2021-26606
CVE-2021-26857
CVE-2021-26858
CVE-2021-28480
CVE-2021-28481
CVE-2021-28482
CVE-2021-28483
CVE-2021-31196
CVE-2021-31207
CVE-2021-40444
CVE-2021-45046
CVE-2021-45105
CVE-2022-1040
CVE-2022-30190
CVE-2022-41128

2022년 4분기 LIVING OFF THE LAND(LOLBIN) 및 타사 도구

Trellix Insights Global Threat Intelligence 플랫폼을 통한 관찰 및 추적으로 2022년 4분기 위협 환경에 관한 다음과 같은 인텔리전스 및 가시성을 확보했습니다.

2022년 4분기 LOLBIN 주요 사항

- Living Off the Land(LOLBIN)는 초기 액세스, 실행, 검색, 지속성과 영향 측면에서 계속 역할을 수행하고 있습니다.
- 2022년 4분기 데이터는 가장 일반적으로 사용/남용되는 기술인 Windows Command Shell 또는 PowerShell을 통해 실행되는 명령 및 스크립팅 기술의 지속적인 추세를 보여줍니다.



- 사이버 범죄자의 사용은 경험이 많은 APT, 핵티비스트와 같이 금전적 동기가 있는 그룹을 포함한 위협 행위자들 사이에 널리 퍼져 있습니다.

위협 환경에서 발견되는 신규 사용자, 일회성 사용자 및 스크립트 키디들은 유명한 공격 프레임워크에 통합된 기존에 존재하는 바이너리를 사용하여 눈에 잘 띄지 않게 깁슨을 해킹하거나 취약성을 공격하려 시도합니다.

Living off the Land(LOLBIN) 기술은 계속해서 초기 액세스, 실행, 검색, 지속성과 영향을 악의적인 작업을 위해 사용/남용하고 있습니다. 2022년 4분기에 수집한 데이터에 따르면 가장 일반적으로 사용/남용되는 기술인 Windows Command Shell 및 PowerShell을 통해 실행되는 명령 및 스크립팅 기술의 지속적인 추세를 확인할 수 있습니다.

2022년 4분기 가장 널리 사용된 OS 바이너리

47%

2022년 4분기에 가장 널리 퍼진 10개의 OS 바이너리 중 Windows Command Shell은 절반에 가까운 47%를 차지했으며, PowerShell(32%)과 Rundl32(27%)가 그 뒤를 이었습니다.

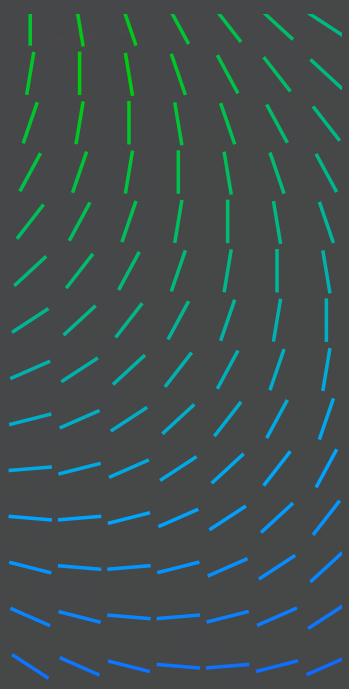
1.	Windows Command Shell	47%
2.	PowerShell	32%
3.	Rundl32	27%
4.	Schtasks	23%
5.	WMI	21%

사이버 범죄자의 사용은 경험이 많은 APT, 각성한 상태의 핵티비스트와 같이 금전적 동기가 있는 그룹을 포함한 위협 행위자들 사이에 널리 퍼져 있습니다.

위협 행위자가 Windows 바이너리를 사용하는 Trellix Insights 플랫폼을 통해 처리된 이벤트는 정보 도용자, 원격 액세스 트로이 목마 또는 랜섬웨어와 같은 맬웨어의 추가 배포로 이어졌습니다. 공격자가 제어하는 리소스에서 추가적인 페이로드 검색을 위해 MSHTA, WMI 또는 WScript와 같은 바이너리가 실행되었을 수도 있습니다.

2022년 4분기 상위 타사 도구

1.	원격 액세스 도구	58%
2.	파일 전송	22%
3.	후속 익스플로잇 도구	20%
4.	네트워크 검색	16%
5.	AD 검색	10%



원격 액세스 및 제어 도구는 여전히 위협 행위자가 많이 남용하는 도구 중 하나이지만, 보안 담당자가 사용하는 도구는 악의적인 의도로 계속해서 악용되고 있습니다. 위협 행위자는 해당 도구를 사용하여 비콘을 계속 켜두거나, 반출을 자동화하거나 또는 목표 정보를 수집하고 압축할 수 있습니다.

무료 및 공개 소스 도구 중에서 소프트웨어 패커는 위협 행위자가 악의적인 콘텐츠를 포함하여 합법적인 소프트웨어를 리패키지하거나 탐지를 바이패스하고 분석을 방해하기 위해 맬웨어를 패킹하는 용도로 남용되고 있습니다.

2022년 4분기 COBALT STRIKE 인사이트

Advanced Research Center의 위협 인텔리전스 그룹은 페이로드를 결합하고 인프라 헌팅 방법론을 사용하여 만연한 Cobalt Strike 팀 서버 (Cobalt Strike C2s) 사용을 모니터링합니다. 수집된 Cobalt Strike 비콘을 분석하는 동안 확인된 주요 인사이트는 여기에서 확인하실 수 있습니다.

15%
COBALT STRIKE 체험판 라이선스

만연하게 관찰되는 Cobalt Strike 비콘의 15%만이 Cobalt Strike 체험판 라이선스를 보유하고 있었습니다. 해당 버전의 Cobalt Strike에는 후속 익스플로잇 프레임워크의 알려진 기능 대부분이 포함되어 있습니다. 그러나 보안 제품에서 페이로드를 간편하게 탐지할 수 있도록 전송 중 암호화를 제거하고 "말"을 추가합니다.

5% HOST HTTP 헤더

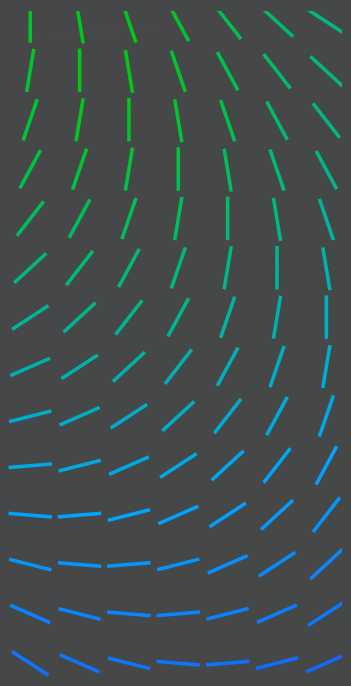
관찰된 Cobalt Strike 비콘의 최소 5%는 Cobalt Strike로 도메인 프론팅을 용이하게 하는 옵션인 Host HTTP 헤더를 사용했습니다. 도메인 프론팅은 다양한 도메인을 호스팅하는 콘텐츠 전송 네트워크 (CDN)를 남용하는 기술입니다. 공격자는 합법적인 웹 사이트에 대한 TLS 연결에서 악의적인 웹 사이트에 대한 HTTPS 요청을 숨깁니다.

87%
RUNDLL32.EXE

세션 생성 및 후속 익스플로잇 작업 실행 시 사용되는 기본 프로세스인 Rundll32.exe는 확인된 비콘 중 87%에서 발견되었습니다.

22% DNS 비콘

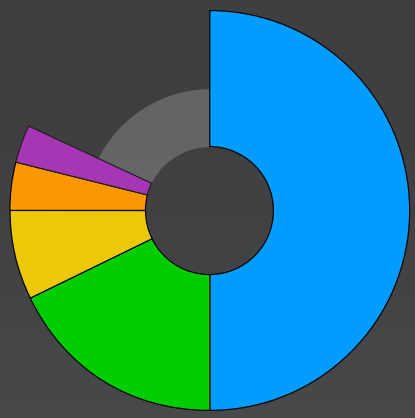
DNS 비콘은 확인된 Cobalt Strike 비콘 중 22%를 차지했습니다. 이 페이로드 유형은 DNS 쿼리를 통해 도메인의 신뢰할 수 있는 서버인 공격자의 Cobalt Strike 팀 서버와 통신하여 활동을 숨깁니다.



2022년 4분기 COBALT STRIKE 팀 서버를 호스팅하는 상위 국가

50%

2022년 4분기에 탐지된 Cobalt Strike 팀 서버의 절반은 중국에서 사용 가능한 클라우드 호스팅의 규모 때문에 중국에서 호스팅되었습니다



2022년 4분기 GOOTLOADER

Gootloader는 모듈식 맬웨어로 "GootKit" 또는 "GootKit Loader"로 확인된 다른 맬웨어로 바꿔 쓸 수 있습니다. 현재 Gootloader 맬웨어의 모듈식 기능은 REvil, Kronos, Cobalt Strike 및 Icedid를 포함하는 추가 맬웨어 페이로드를 배포하는 데 사용되고 있습니다.

최근 이벤트에서 Gootloader는 JS(JavaScript) 파일 페이로드를 포함한 보관 파일을 호스팅하기 위해 사용되는 손상된 사이트 또는 가짜 사이트로 순진한 사용자를 유도하기 위해 검색 엔진 최적화(SEO)를 사용하고 있음이 확인되었습니다. 그렇지만 이 기술을 사용하려면 순진한 사용자가 보관 파일을 열고 콘텐츠를 실행해야 하며, 이 콘텐츠를 실행할 경우 Windows Scripting Host를 통해 악성 JS 코드가 실행됩니다. 실행되면 Gootloader는 C2 통신을 시작하고 추가 맬웨어를 검색합니다.

Gootloader는 위협 행위자가 다양한 페이로드를 추가로 로드할 수 있도록 구독자에게 제공되는 서비스형 맬웨어(MaaS)로 의심되는 서비스이며, 기업 환경에 중대한 위협이 됩니다.

당사의 내부 Gootloader 추적기를 통해 2022년 11월 18일 기준으로 만연한 최신 변형을 확인했으며, 2022년 11월 13일 기준으로 구형 변형이 실행되지 않는 것을 확인했습니다. 최신 변형에 관한 수정 내용은 다음과 같습니다.

- 레지스트리 조작 기능 제거
- 원격 네트워크 요청이 3개가 아닌 10개의 URL로 증가
- CScript를 통한 PowerShell 스크립트 직접 호출 기능
- 모든 사용자 로그온 지속성

당사의 Gootloader 추적 프로세스

Gootloader의 새로운 변형은 여러 난독화 계층을 사용하여 진화했습니다. 압축을 푼 후 각각의 중첩된 단계는 이전 단계에서 로드된 변수를 사용하여 분석이 더욱 어렵습니다. YARA 헌팅으로 수집된 샘플은 정적 JavaScript 및 PowerShell 분석기에 제공되어 원격 명령 및 제어(C&C, C2) 서버 및 고유 ID 서명과 같은 IOC를 추출합니다. 이러한 IOC는 Gootloader의 만연한 특정 인스턴스를 확인하고 추적하는 데 사용할 수 있습니다.

추출된 Gootloader IOC는 다음으로 Trellix URL 평판 팀의 데이터베이스를 쿼리하여 어떤 것이 악성인지, 잠재적으로 손상된 합법 도메인 및 분석을 손상시킬 수 있는 미끼로 사용되는 합법 도메인을 확인하는 것으로 처리됩니다.

Gootloader 원격 측정 인사이트

탐지 자체가 아닌 추출된 IOC와 고객 로그 간 상관 관계에서 확인된 캠페인 통계가 표시됩니다. Gootloader의 경우 대부분의 탐지는 도메인 조회수를 기반으로 합니다. Gootloader의 경우 미끼 도메인을 사용하므로 표시되는 통계는 중간 수준 신뢰도의 악의적인 것으로 해석되어야 합니다.

2022년 4분기 GOOTLOADER의 가장 많은 피해자가 발생한 국가

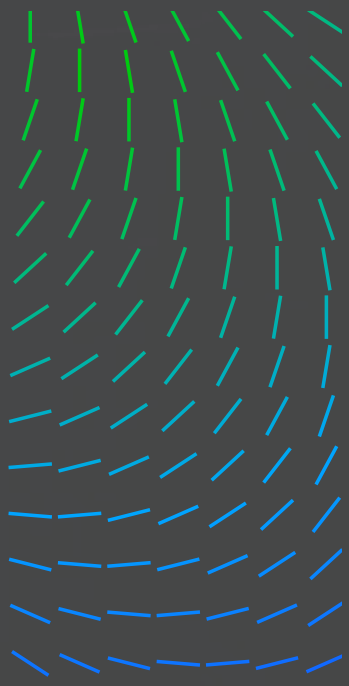
37%

2022년 4분기 Gootloader의 가장 많은 피해자가 발생한 국가는 미국이었습니다.

1.	미국	37%
2.	이탈리아	19%
3.	인도	11%
4.	인도네시아	9%
5.	프랑스	5%

2022년 4분기 GOOTLOADER에서 사용되는 가장 인기 있는 MITRE ATT&CK 기술

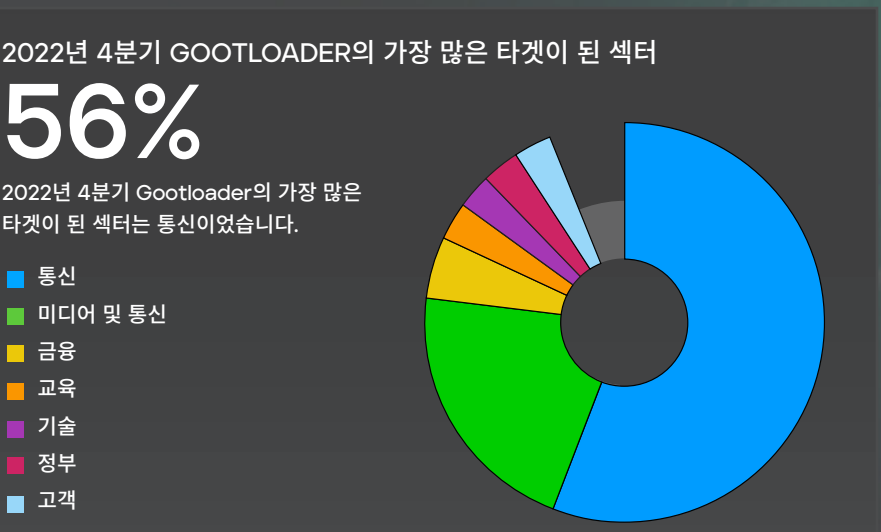
1. 파일 또는 정보 정체 밝히기/디코드
2. JavaScript
3. 파일 또는 정보 난독화
4. PowerShell
5. 프로세스 할로잉



2022년 4분기 GOOTLOADER의 가장 많은 타겟이 된 섹터

56%

2022년 4분기 Gootloader의 가장 많은 타겟이 된 섹터는 통신이었습니다.



2022년 4분기 Gootloader에서 사용되는 가장 인기 있는 MITRE ATT&CK 기술

파일 또는 정보 정체 밝히기/디코드

JavaScript

파일 또는 정보 난독화

PowerShell

프로세스 할로잉

반사 코드 로딩

레지스트리 실행 키 / 시작 폴더

Rundll32

예약된 작업

2022년 4분기 취약성 인텔리전스

당사의 취약성 대시보드에서는 영향력이 큰 최신 취약성 분석을 수집합니다. 분석 및 분류는 Trellix Advanced Research Center의 업계 취약성 전문가가 수행합니다. 해당 연구자들은 역설계 및 취약성 분석을 전문으로 하고 있으며, 최신 취약성과 위협 행위자들이 이러한 취약성을 공격에 활용하는 방법에 관해 지속적으로 모니터링을 진행하고, 복원 지침을 제공합니다. 이 간결하고 전문적인 전문가 조언을 통해 노이즈에서 신호를 필터링하고 조직에 영향을 미칠 수 있는 가장 영향력이 큰 취약성에 집중하여, 빠른 대응이 가능합니다.

2022년 4분기 취약성 인텔리전스 주요 사항

41% Lanner는 2022년 4분기에 고유 CVE의 영향을 받은 취약 제품 및 공급업체 중 41%를 차지했습니다.

29% IAC-AST2500A 펌웨어 버전 1.10.0은 2022년 4분기에 제품에서 가장 많이 보고된 CVE였습니다.

2022년 4분기 가장 큰 영향을 미친 취약 제품, 공급업체 및 CVE

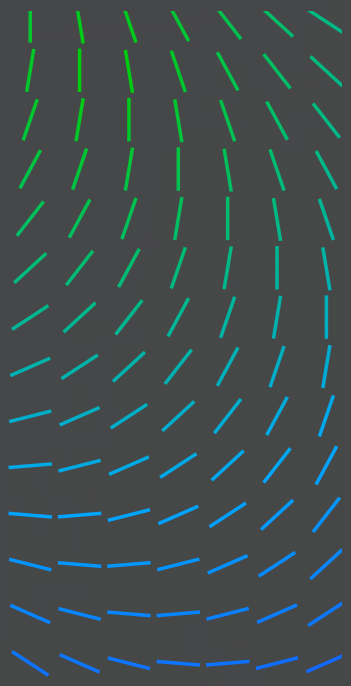
1.	Lanner	41%
2.	Microsoft	19%
3.	BOA	15%
4.	Oracle	8%
5.	Apple Chrome Citrix Fortinet Linux	각 5%

2022년 4분기 제품별 보고된 CVE

29%

IAC-AST2500A 펌웨어 버전 1.10.0은 2022년 4분기에 제품에서 가장 많이 보고된 CVE였습니다. BOA 서버(10%)와 IAC-AST2500A(6%) 및 Exchange(6%)가 뒤를 이었습니다.

보고된 CVE 제품	고유 CVE
IAC-AST2500A, 펌웨어 버전 1.10.0	9
BOA 서버	3
Exchange	3
IAC-AST2500A	2
tvOS	1
iPadOS	1
iOS	1
Windows	1
Safari	1
SQLite 3.40.0 이하	1
Oracle Access Manager, 11.1.2.3.0, 12.2.1.3.0, 12.2.1.4.0	1
MacOS	1
Linux 커널 5.15.61 이하	1
Internet Explorer	1



보고된 CVE 제품	고유 CVE
FortiOS(sslvpnd)	1
Citrix ADC/Citrix 게이트웨이	1
Chrome, 108.0.5359.94/.95 버전 이하	1
BOA 서버, Boa 0.94.13	1

2022년 4분기 보고된 CVE

CVE-2022-1786
CVE-2022-26134
CVE-2022-27510
CVE-2022-27518
CVE-2022-31685
CVE-2022-32917
CVE-2022-32932
CVE-2022-33679
CVE-2022-34718
CVE-2022-35737
CVE-2022-3602
CVE-2022-3786
CVE-2022-37958
CVE-2022-40684
CVE-2022-41040
CVE-2022-41080
CVE-2022-41082
CVE-2022-41128
CVE-2022-41352
CVE-2022-42468
CVE-2022-42475
CVE-2022-4262
CVE-2022-42856
CVE-2022-42889
CVE-2022-43995
CVE-2022-46908
CVE-2022-47939

2022년 4분기 이메일 보안 동향

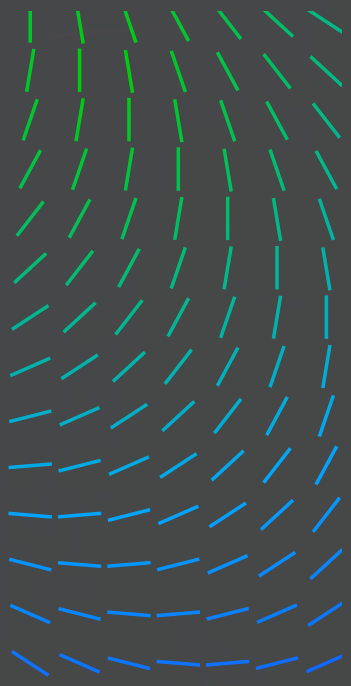
이메일 보안 통계는 전 세계 고객 네트워크에 배포된 여러 이메일 보안 어플라이언스에서 생성된 원격 측정을 기반으로 합니다. 탐지 로그를 집계 및 분석하여 다음 결과를 생성합니다.

2022년 4분기 이메일 보안 동향 주요 사항

100% 아랍 국가들의 악성 이메일 양이 8월과 9월 대비 10월에는 100% 증가한 것으로 확인되었습니다.

40% Qakbot은 가장 많이 사용된 맬웨어 전술로, 아랍 국가를 대상으로 한 캠페인의 40%를 차지했습니다.

42% 통신은 2022년 4분기 악성 이메일의 영향을 가장 많이 받은 섹터로, 업계를 대상으로 한 악성 이메일 캠페인의 42%를 차지했습니다.



87% 2022년 4분기 가장 널리 퍼진 공격 벡터는 악성 URL을 이용한 피싱 이메일이었습니다.

64% 가장의 성공률이 2022년 3분기부터 4분기까지 64% 증가했습니다.

82% 전체 CEO 사기 이메일의 82%가 무료 이메일 서비스를 통해 전송되었습니다.

78% 전체 비즈니스 이메일 손상(BEC) 공격의 78%는 일반적인 CEO 문구를 사용했습니다.

142% 보이스 피싱 공격은 2022년 4분기에 두드러지게 나타난 공격으로, 3분기에 비해 142% 증가했습니다.

2022년 4분기 가장 널리 퍼진 이메일 맬웨어 전술

40%

2022년 4분기에 가장 널리 사용된 이메일 맬웨어 전술은 Qakbot이었습니다.

1.	Qakbot	40%
2.	Emotet	26%
3.	Formbook	26%
4.	Remcos	4%
5.	QuadAgent	4%

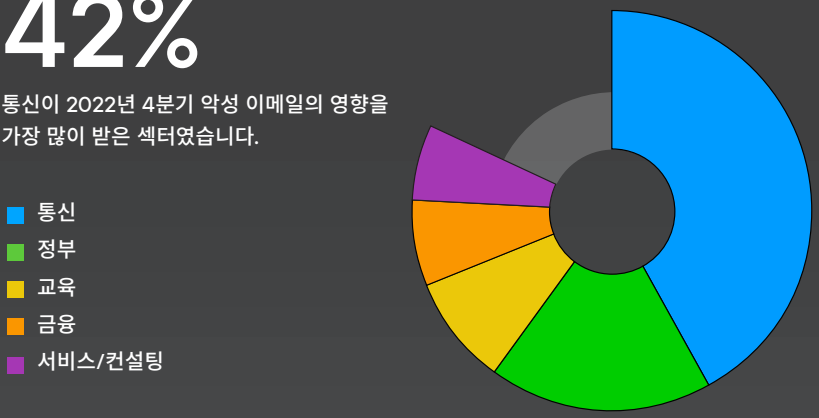
2022년 4분기 이메일 피싱의 가장 많은 표적이 된 제품 및 브랜드

1.	일반	62%
2.	Outlook	13%
3.	Microsoft	11%
4.	Ekinet	8%
5.	Cloudfare	3%

2022년 4분기 악성 이메일의 영향을 가장 많이 받은 섹터

42%

통신이 2022년 4분기 악성 이메일의 영향을 가장 많이 받은 섹터였습니다.



2022년 4분기 이메일 가장 동향 주요 사항

82% 전체 CEO 사기 이메일의 82%가 무료 이메일 서비스를 통해 전송되었습니다.

78% 전체 비즈니스 이메일 손상(BEC) 공격의 78%는 일반적인 CEO 문구를 사용했습니다.

64% 2022년 3분기부터 4분기까지 CEO 및 기타 비즈니스 리더를 가장하는 악성 이메일이 64% 증가했습니다.

2022년 4분기 BEC 공격에서 사용된 상위 CEO 문구:

"해당 작업 즉시 진행 부탁드립니다."

"작업 완료를 위해 휴대폰 번호를 알려주시기 바랍니다."

"전화번호를 보내주시기 바랍니다. 지금 당장 처리할 일이 있습니다."

"휴대폰 번호를 보내주시고, 제 문자 메시지를 잘 살펴보시기 바랍니다. 완료할 작업이 있습니다."

"휴대폰 번호를 검토 및 확인 부탁드리며, 지시 사항을 위해 제 문자 메시지를 잘 살펴보시기 바랍니다."

"이전 메일을 받으셨나요? 당신에게 이익이 되는 거래가 있습니다."

2022년 4분기 가장 비교

64% 가장의 성공률이 2022년 3분기부터 4분기까지 64% 증가했습니다.

2022년 4분기 피싱 캠페인 인사이트

스캠 및 도용에의 사례가 증가하는 웹 호스팅 제공업체

4분기에는 사용자 스캠 및 자격 증명을 도용하기 위해 합법적인 웹 호스팅 제공업체를 사용하는 사례가 증가함을 확인했습니다. 주로 남용된 서비스 공급자는 세 곳으로, dweb.link, ipfs.link, translate.goog입니다. 당사에서는 또한 ekinet, storageapi_fleek, and selcdn.ru와 같은 다른 서비스 공급자 도메인에서도 상당한 양을 확인했습니다. 공격자는 피싱 페이지를 호스팅하고 안티피싱 엔진을 바이패스하기 위하여 새롭고 인기 있는 호스팅 서비스를 지속적으로 사용하고 있습니다. 합법적인 웹 호스팅 제공업체에 대한 공격자의 관심이 증가한 한 가지 이유는 이러한 서비스의 주요 목표가 합법적인 파일을 호스팅하고 콘텐츠 공유를 위한 것이기 때문입니다. 이러한 이유로 해당 사이트를 어떤 탐지 시스템에서도 블랙리스트에 올릴 수 없습니다.

피싱 이메일에서 가장 많이 사용되는 공격 벡터

87%

2022년 4분기 가장 널리 사용된 공격 벡터는 악성 URL을 이용한 피싱 이메일이었습니다.

1.	URL	87%
2.	첨부 파일	7%
3.	헤더	6%

2022년 4분기 가장 많이 남용된 웹 호스팅 제공업체

154%

2022년 4분기에 가장 많이 남용된 웹 호스팅 제공업체는 Dweb인 반면, 3분기에서 4분기까지 가장 크게 증가한 것은 Google Translate(154%)였습니다.

1.	Dweb	81%
2.	Ipfs	17%
3.	Google Translate	10%

2022년 4분기 피싱 공격에 가장 많이 사용되는 우회 공격 기술

63%

2022년 4분기에 302 리디렉션 기반 우회가 가장 두드러졌습니다.

- 지역 기반 우회 피싱 공격이 4분기에 크게 증가했습니다.
- Captcha 기반 공격도 4분기에 증가했습니다.

2022년 4분기 보이스 피싱 인사이트

보이스 피싱은 피싱의 또 다른 형태로, 주로 문자 메시지, 전화 통화 또는 다이렉트 채팅 메시지를 통해 공격자와 연결되게끔 피해자를 유인하도록 설계되었습니다.

142% 보이스 피싱 공격은 2022년 4분기에 두드러지게 나타난 공격으로, 3분기에 비해 142% 증가했습니다.

85% 무료 이메일 서비스는 보이스 피싱을 사용하는 악의적 행위자들이 가장 즐겨 찾는 서비스입니다. 당사에서 탐지한 2022년 4분기 보이스 피싱 공격의 대부분(85%)은 무료 이메일 서비스를 통해 전송된 것이었습니다.

4분기 보이스 피싱 캠페인에 사용된 가장 인기 있는 테마는 **Norton, McAfee, Geek Squad, Amazon 및 PayPal 이었습니다.**

2022년 4분기 네트워크 보안

Trellix ARC 네트워크 연구팀은 고객을 위협하는 네트워크 기반 공격을 탐지하고 차단하는 데 집중하고 있습니다. 당사에서는 정찰과 초기 손상, C2 통신 및 내부 확산 TTP에서 킬 체인의 다양한 영역을 검사합니다. 당사의 결합된 기술의 강점을 활용하는 능력을 바탕으로 알려지지 않은 위협을 더 잘 탐지할 수 있는 가시성을 가질 수 있습니다.

2022년 4분기 네트워크 보안에 사용되는 가장 인기 있는 MITRE ATT&CK 기술

- T1083 - 파일 및 디렉터리 검색
- T1573 - 암호화된 채널
- T1020 - 자동 반출
- T1210 - 원격 서비스 익스플로잇
- T1569 - 시스템 서비스
- T1059 - 명령 및 스크립팅 인터프리터: Windows Command Shell
- T1047 - WMI(Windows 관리 도구)
- T1087 - 계정 검색
- T1059 - 명령 및 스크립팅 인터프리터
- T1190 - 공용 응용프로그램 익스플로잇

2022년 4분기 외부 서비스에 대한 가장 영향력 있는 공격

고객 환경에 대한 잠재적인 임계값을 찾기 위해, 외부 시스템 조사를 위해 매일 수행되는 다양한 네트워크 검색이 존재합니다. 기존 익스플로잇은 패치되지 않은 시스템을 계속 찾습니다.

- 파일 /etc/passwd 액세스 시도 탐지
- 사이트 간 스크립팅 공격 가능성
- SIPVicious 보안 스캐너
- Nmap 스캐너 트래픽 탐지
- 검색 활동 - Shellshock, 웹 서버 프로브
- Bash 원격 코드 실행(Shellshock) HTTP CGI(CVE-2014-6278)
- Oracle WebLogic CVE-2020-14882 원격 코드 실행 취약성
- 디렉터리 이동 시도
- Apache Struts 2 ConversionErrorInterceptor OGNL 스크립트 주입
- Apache Log4j CVE-2021-44228 원격 코드 실행

2022년 4분기 초기 네트워크 침투 발판으로 사용된 가장 중요한 WebShell

일반적으로 취약한 웹 서버 제어에 사용되는 WebShell는 다음과 같습니다.

- China Chopper WebShell
- JFolder WebShell
- ASPXSpy WebShell
- C99 WebShell
- Tux WebShell
- B374K WebShell / RootShell Family

2022년 4분기 네트워크 내부 침입과 가장 관련성이 높은 도구, 기술 및 절차

일반적으로 취약한 웹 서버 제어에 사용되는 WebShell는 다음과 같습니다.

당사에서는 SCShell 및 PSExec과 같은 기존 취약성 및 도구의 사용을 포함하여 내부 확산 중 공격자가 사용하는 많은 양의 TTP를 확인했습니다.

- SCshell: 서비스 관리자를 이용한 파일리스 내부 확산
- Windows WMI 원격 프로세스 호출
- SMB WMIEXEC를 통한 CMD Shell 호출
- EternalBlue 익스플로잇 탐지
- Microsoft SMBv3 CVE-2020-0796 시도
- Apache Log4j CVE-2021-44228 RCE
- 원격 도메인/기업 관리자 계정 열거
- 의심스러운 PowerShell 원격
- WMIC를 사용하여 의심스러운 네트워크 정찰
- 배치 파일에서 열거 명령 탐지
- SMB PSEXEC 작업

TRELLIX XDR에서 제공하는 보안 운영 원격 측정

이 통계는 고객 기반의 다양한 센서에서 생성된 원격 측정을 기반으로 합니다. 탐지 로그는 집계되고 분석되어 다음 섹션을 생성합니다.

2022년 4분기 가장 영향력 있는 보안 사고

2022년 4분기에 가장 널리 사용되는 보안 경고를 아래 섹션에서 확인하실 수 있습니다.

EXPLOIT - LOG4J [CVE-2021-44228]

OFFICE 365 ANALYTICS [비정상적 로그온]

OFFICE 365 [피싱 허용됨]

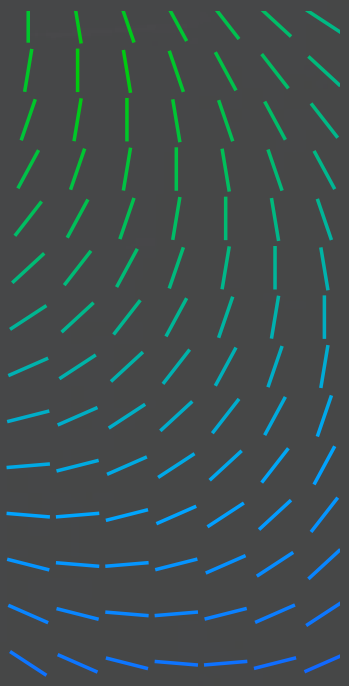
EXPLOIT - FORTINET [CVE-2022-40684]

EXPLOIT - APACHE SERVER [CVE-2021-41773 - 시도]

WINDOWS ANALYTICS [무차별 대입 성공]

EXPLOIT - ATLASSIAN CONFLUENCE [CVE-2022-26134]

EXPLOIT - F5 BIG-IP [CVE-2022-1388 시도]



2022년 4분기 가장 많이 사용된 MITRE ATT&CK 기술

1.	공용 응용프로그램 익스플로잇(T1190)	29%
2.	응용프로그램 계층 프로토콜: DNS(T1071.004) 피싱(T1566)	14% 14%
3.	계정 조작(T1098.001) 무차별 대입(T1110) 드라이브 바이 손상(T1189) 사용자 실행: 악성 파일(T1204.002) 유효한 계정: 로컬 계정 T1078,003)	각 7%

2022년 4분기 상위 로그 소스 배포

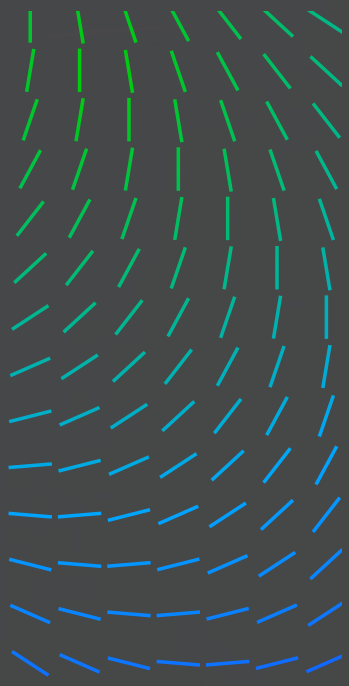
1.	네트워크	40%
2.	이메일	27%
3.	엔드포인트	27%
4.	방화벽	6%

2022년 4분기에 관찰된 익스플로잇

2022년 4분기 가장 많이 관찰된 익스플로잇

30% 2022년 4분기에 가장 널리 사용된 익스플로잇은 Log4j였습니다.

1.	Log4j(CVE-2021-44228)	30%
2.	Fortinet(CVE-2022-40684)	16%
3.	Apache 서버(CVE-2021-41773)	15%
4.	Atlassian Confluence(CVE-2022-26134)	14%
5.	F5 Big-IP(CVE-2022-1388 시도)	13%
6.	Microsoft Exchange(ProxyShell 익스플로잇 시도)	11%



2022년 4분기 클라우드 사고

많은 기업이 온프레미스 인프라에서 전환하였으므로 클라우드 인프라에 대한 공격은 항상 증가하고 있습니다. Gartner 분석가는 2025년까지 조직의 85% 이상이 클라우드 우선 원칙을 수용할 것으로 예측합니다.

2022년 4분기 원격 측정 분석을 통해 다음 내용을 확인했습니다.

- AWS와 관련된 탐지는 AWS가 인터넷 환경에서 주요 리더 지위를 차지하고 있기 때문일 수 있습니다.
- 대부분의 공격은 클라우드 공격 표면의 초기 감염 벡터를 가리키는 유효한 계정에 대한 무차별 대입 공격/Passwordspray 공격의 초기 액세스 권한을 얻는 데 초점이 맞춰져 있었습니다.
- 대부분의 기업 계정이 다단계 인증을 활성화한 상태에서 무차별 대입 공격이 성공하면 공격자가 MFA 플랫폼에 침입하여 MFA 관련 탐지가 급증합니다.

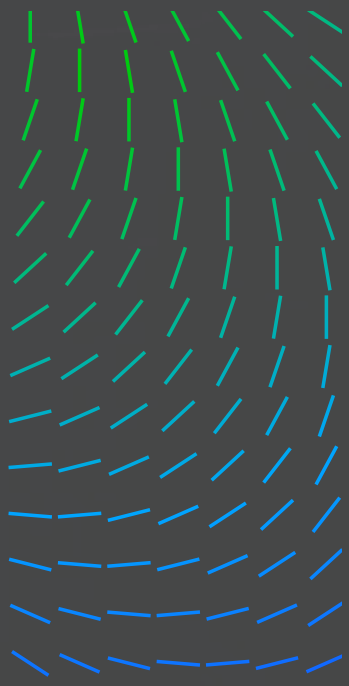
아래 섹션은 다양한 클라우드 공급자에 따른 고객 기반 내역 전체에서 클라우드 기반 공격 텔레메트리 데이터를 간략하게 설명합니다.

2022년 4분기 AWS용 MITRE ATT&CK 기술 배포

1.	유효한 계정(T1078)	18%
2.	클라우드 컴퓨팅 인프라 수정(T1578)	12%
3.	계정 조작(T1098)	9%
4.	클라우드 계정(T1078.004)	8%
5.	무차별 대입(T1110) 방어 손상(T1562)	각 6%

2022년 4분기 AZURE용 상위 MITRE ATT&CK 기술

1.	유효한 계정(T1078)	23%
2.	다단계 인증(T1111)	19%
3.	무차별 대입(T1110)	14%
4.	프록시(T1090)	14%
5.	계정 조작(T1098)	5%



2022년 4분기 MITRE ATT&CK 기술을 통한 상위 AWS 탐지

MITRE 기술	규칙
계정 조작(T1098)	IAM ID에 연결된 AWS 권한 정책 AWS S3 - 버킷 삭제 정책
유효한 계정(T1078)	AWS Analytics 비정상적 콘솔 로그인 AWS Analytics 비정상적 API 키 사용 AWS GuardDuty 비정상적 사용자 행동 AWS GuardDuty 익명 액세스 허용
방어 손상(T1562)	AWS CloudTrail 정책이 CloudTrail로 변경 AWS CloudTrail 추적 삭제
파일의 자격 증명(T1552.001)	AWS 비밀 키 도용 가능성 경고
클라우드 컴퓨팅 인프라 수정(T1578)	AWS CloudTrail S3 버킷 삭제 AWS CloudTrail S3 버킷 업로드 ACL AWS CloudTrail 개체 업로드 ACL

2022년 4분기 MITRE ATT&CK 기술을 통한 상위 AZURE 탐지

MITRE ATT&CK 기술	규칙
유효한 계정(T1078)	Azure AD 위험한 로그인 비정상적인 위치에서 Azure 로그인 계정별 Azure 로그인이 60일 동안 표시되지 않음
무차별 대입(T1110)	Azure 다단계 인증 실패 Azure 포털에 대한 Graph 무차별 대입 공격 Graph 분산 암호 크래킹 시도
다단계 인증(T1111)	사기 경고로 인해 Azure MFA 거부됨 사용자 차단으로 인해 Azure MFA 거부됨 사기 코드로 인해 Azure MFA 거부됨 사기 앱으로 인해 Azure MFA 거부됨
외부 원격 서비스(T1133)	Tor 네트워크에서 Azure 로그인
계정 조작(T1098)	Azure 비정상적 사용자 암호 재설정

2022년 4분기 GCP용 MITRE ATT&CK 기술 배포

1.	유효한 계정(T1078)	36%
2.	API를 통한 실행(T0871)	18%
3.	계정 검색(T1087.001) 계정 조작(T1098) 방어 손상(T1562) 클라우드 컴퓨팅 인프라 수정(T1578) 원격 서비스(T1021.004)	각 9%

2022년 4분기 MITRE ATT&CK 기술을 통한 상위 GCP 탐지

MITRE ATT&CK 기술	규칙
유효한 계정(T1078)	GCP 서비스 계정 생성 GCP Analytics 비정상적 활동 서비스 계정 키 GCP 생성
원격 서비스(T1021.004)	GCP 방화벽 규칙은 ssh 포트의 모든 트래픽 허용
계정 조작(T1098)	GCP 조직 IAM 정책 변경됨
계정 검색(T1087.001)	[“gcps net user”] 경고
클라우드 계정으로 데이터 전송 (T1527)	GCP 로깅 싱크 수정됨
클라우드 컴퓨팅 인프라 수정(T1578)	GCP 보호 사용 안 함

저술 및 연구

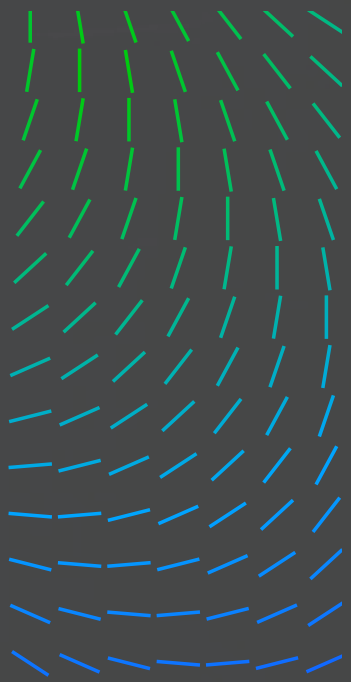
Alfred Alvarado
Henry Bernabe
Adithya Chandra
Phuc Duy Pham 박사
Sarah Erman
John Fokker
Lennard Galang
Sparsh Jain
Daksh Kapoor
Maulik Maheta
João Marques
Tim Polzer
Srini Seethapathy
Rohan Shah
Vihar Shah
Swapnil Shashikantpa
Shyava Tripathi
Leandro Velasco

리소스

Trellix Advanced Research Center에서 식별한 최신 위협과 가장 영향력 있는 위협을 추적하려면 다음 리소스를 확인하십시오.

TWITTER

Trellix ARC

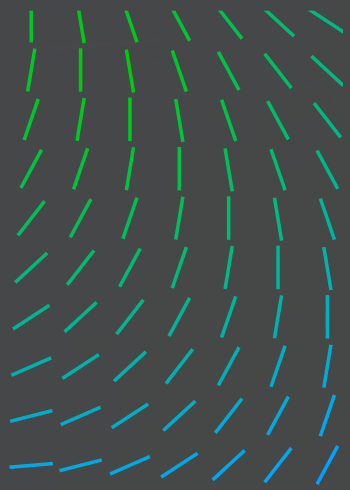


TRELLIX ADVANCED RESEARCH CENTER 정보

Trellix Advanced Research Center는 사이버 보안 업계에서 가장 포괄적인 현장을 보유하고 있으며, 위협 환경 전반에서 새롭게 부상하는 방법, 동향 및 행위자의 최전선에 있습니다. 전 세계 보안 운영팀의 최고의 파트너인 Trellix Advanced Research Center는 보안 분석가에게 인텔리전스와 최신 콘텐츠를 제공하는 동시에 최고의 XDR 플랫폼을 지원합니다.

TRELLIX 소개

Trellix는 사이버 보안과 세상을 바꾸는 기술의 미래를 혁신하는 글로벌 기업입니다. 회사의 개방형 eXtended Detection and Response(XDR) 플랫폼은 오늘날 가장 지능적인 위협에 직면한 조직이 운영의 보호 및 복원력에 대한 확신을 가질 수 있도록 지원합니다. Trellix는 광범위한 파트너 에코시스템과 함께 머신 러닝 및 자동화를 통한 기술 혁신을 가속하여 40,000개 이상의 기업 및 정부 고객에게 생활 보안을 제공합니다. www.trellix.com/ko-kr에서 자세히 살펴보십시오.



자세한 내용을 알아보려면 Trellix.com을 방문하세요.

Trellix

Trellix 소개

Trellix는 사이버 보안의 미래를 혁신하는 글로벌 기업입니다. 오늘날 최첨단 위협에 직면한 조직은 Trellix가 보유한 개방형 eXtended Detection and Response(XDR) 플랫폼을 통해 확실히 운영을 보호하고 복원할 수 있습니다. Trellix의 보안 전문가는 광범위한 파트너 에코시스템과 더불어 머신 러닝 및 자동화를 통해 기술 혁신을 가속함으로써 40,000곳 이상의 기업 및 정부 고객을 지원하고 있습니다.

072022-05