2023 Global Threat Report

주요 내용 요약

크라우드스트라이크

CROWDSTRIKE

2023 GLOBAL THREAT REPORT

다루는 내용

- Threat landscape
- 2022 테마
- 준비해야 할 5단계

CROWDSTRIKE

CROWDSTRIKE

2023 GLOBAL THREAT REPORT

Threat Landscape

- Breakout time – 초기침투에서 확산이동까지 시간
- Access broker 왕성한 활동
- 악성코드 없이 활동하는 Adversary
- Interactive intrusions

코로나시기의 원격, 하이브리드 환경과 글로벌 안보와 경제의 불확실성이 공격자들에게 활발하게 활동할 수 있는 근거와 환경을 제공하게 됨.
(Access Broker, Ransomware 서비스의 활성화)

CROWDSTRIKE

eCRIME BREAKOUT TIME

84'

Every Second Counts

비용과 피해를 최소화

위협을 억제하려면 우리는 Breakout 시간(84분) 내에 대응해야 합니다.

점점 빨라지는 Adversary

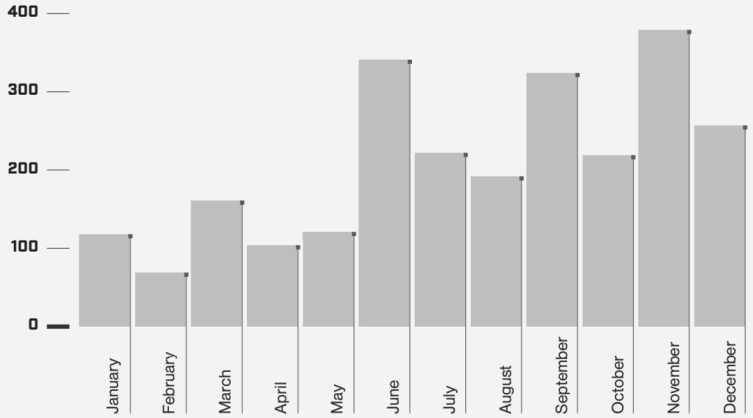
Breakout 시간은 2021년 98분에서 2022년 84분으로 감소했습니다.

1-10-60 규칙을 지키세요

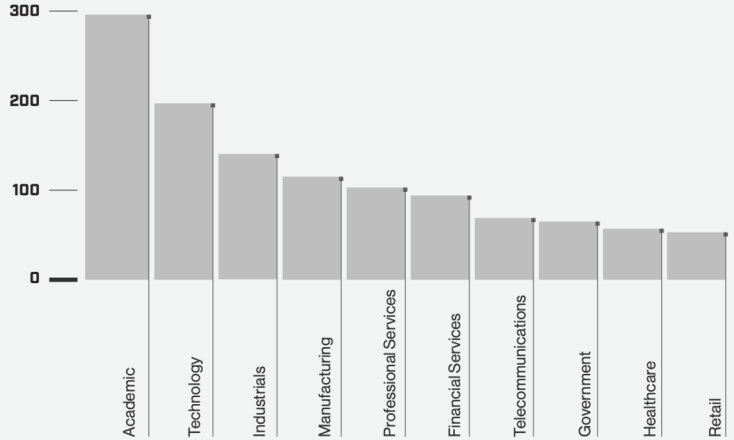
1분 안에 조사, 10분 안에 조사, 60분 안에 대응해야 합니다.

CROWDSTRIKE

ACCESS BROKER ADVERTISEMENTS BY MONTH, 2022



TOP 10 SECTORS ADVERTISED BY ACCESS BROKERS, 2022



Access Broker 왕성한 활동

수요의 가속화

2,500개 이상의 광고로 서비스 인기도 상승 – 2021년 대비 112% 증가

단품 또는 대량 구매

Access information 거래가 단건 별로도 Bulk로도 거래되고 있음

액세스 방법은 일관되게 유지됨

다크웹에서 해커들에 의해 도용되어 사용된 정보들이 판매되고 있음

"모든 침해의 80%는 탈취된 ID를 사용하고 조직의 50%는 지난 2년 동안 AD(Active Directory) 공격을 경험했습니다."

CROWDSTRIKE

공격자는 초기 액세스 및 지속성을 확보하기 위해 계속해서 맬웨어를 사용하지 않았습니다.

2022년에는 **맬웨어 없는** 활동이 모든 탐지의 71%를 차지하면서 **맬웨어 사용**에서 지속적으로 변화했습니다(2021년 62%에서 증가). 이것은 부분적으로 공격자가 피해자 환경에서 액세스 및 지속성을 촉진하기 위해 **유효한 자격 증명을 많이 남용**하는 것과 관련이 있습니다. 또 다른 요인은 새로운 취약점이 공개되는 속도와 공격자가 익스플로잇을 활용할 수 있는 속도였습니다.

ADVERSARY TACTICS Malware-Free

71%	**2022**
62%	2021
51%	2020
40%	2019
39%	2018

50%

increase in interactive intrusion campaigns

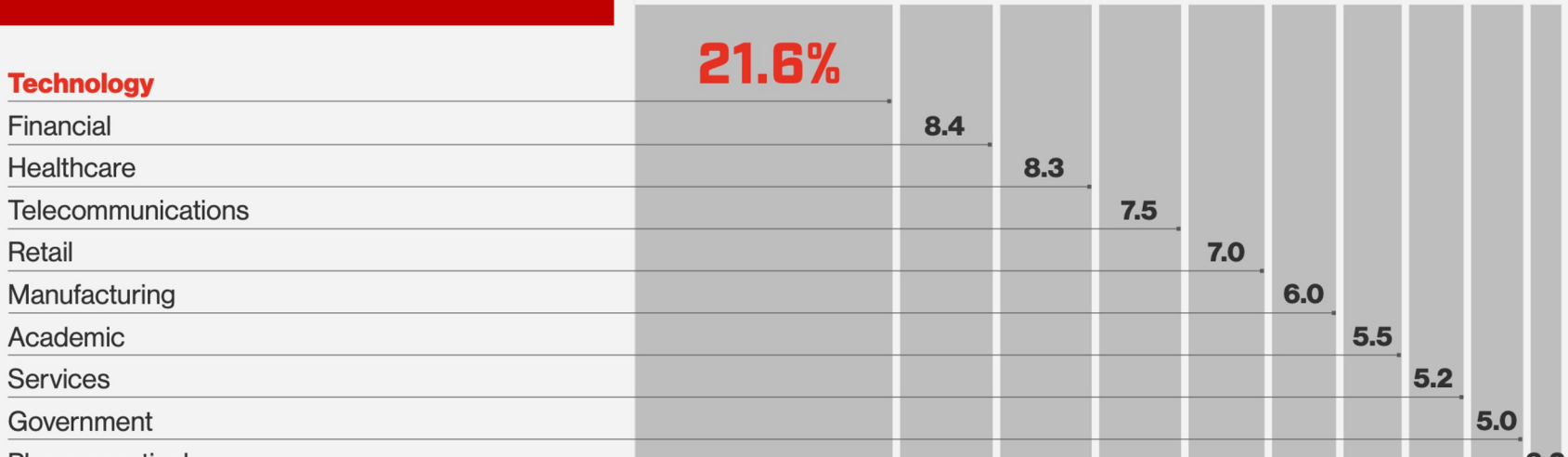
Tech 산업군에 공격이 증가하는 이유는

High Tech Intellective Property가 고가 판매 가능하고, Ransom을 받을 수도 있고 국가보안 기술(Supply Chain)로 거래될 수 도 있기에 해커과 국가 배후 해커들이 적극 공격함

속도와 추진력을 얻은 대화형 침입 공격
Interactive intrusions

크라우드스트라이크는 2021년에 비해 4분기 활동이 가속화되면서 반복적인 침입 캠페인 수가 50% 증가한 것을 관찰했습니다.
또한 Falcon Overwatch가 2022년에 대화형 침입 활동을 발견한 가장 자주 표적이 된 산업군은 아래와 같습니다.
이를 보면 지난 12개월 동안 상위 10개 산업군의 상대적 침입 빈도와 비교하여 증가한 수치입니다.

TOP 10 VERTICALS BY INTRUSION FREQUENCY



CROWDSTRIKE

2023 GLOBAL THREAT REPORT

2022 테마

- eCrime 액터는 세간의 이목을 끄는 공격으로 악명을 얻음
- 클라우드 취약점 이용의 지속적인 증가
- 검색, 재발견 및 우회: 2022년 취약성 인텔리전스 환경
- 많은 노력과 제한된 수익: 러시아 사이버 작전이 우크라이나 전쟁을 지원하고 있습니다.
- 스파이 환경 지배: 중국과 연계된 적대 세력이 2022년 작전 규모를 크게 늘림

CROWDSTRIKE

eCrime 액터는 세간의 이목을 끄는 공격으로 악명을 얻음

"이중 갈취" 모델 증가

랜섬웨어를 배포하지 않고 데이터 절도 및 갈취를 수행하는 공격자의 수 20% 증가

SLIPPY SPIDER

Microsoft, Nvidia, Okta와 같은 다양한 유명 다국적 기술 회사를 대상으로 데이터 갈취 캠페인을 진행

SCATTERED SPIDER

다단계 인증을 우회하기 위해 사회 공학 사용

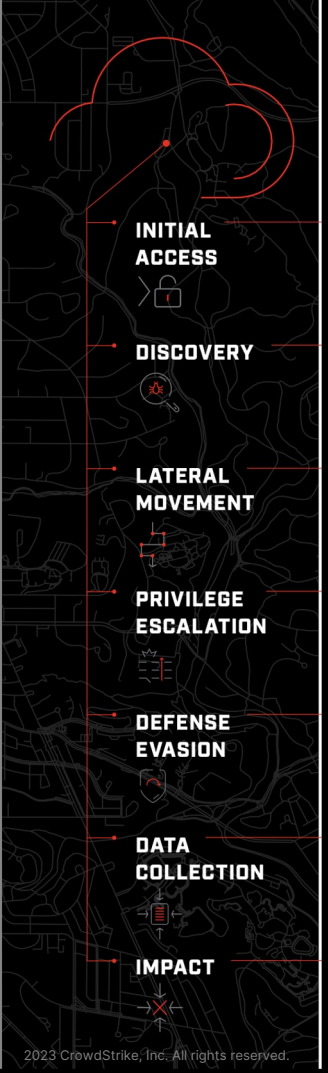
CROWDSTRIKE INTELLIGENCE BEGAN TRACKING

33

NEW ADVERSARIES, RAISING THE TOTAL NUMBER OF ACTORS TRACKED TO

200+

CROWDSTRIKE



클라우드 취약점 이용의 지속적인 증가

취약점 증가

클라우드 악용 사례는 95% 증가했습니다. 2021년보다 클라우드에 민감한 행위자가 관련된 사례가 거의 3배 증가했습니다.

클라우드 TTPs

TTP 레퍼토리 확장에는 클라우드 계정 검색, 초기 액세스를 위한 공개 앱, 에스컬레이션을 위한 더 높은 권한의 계정 사용이 포함됩니다.

클라우드 TTP 사용 의심되는 PANDA 조직

기존 엔드포인트를 활용하여 클라우드로 피벗(또는 그 반대로)하는 공격자가 더욱 자신감을 갖게 됨

"CrowdStrike Intelligence는 공격자가 침투 로그 변조 노력뿐만 아니라 백신 및 방화벽 기술의 비활성화하려는 기술에서 벗어나는 것을 보았습니다. 대신 인증 프로세스를 수정하고 ID를 공격하는 방법을 찾는 것이 관찰되었습니다."

"클라우드 침해를 막으려면 잘못된 구성 및 컨트롤 플레인 공격으로부터 보호하는 에이전트 LESS 기능과 클라우드 워크로드를 보호하는 에이전트 기반 런타임 보안의 조합이 필요합니다."

CROWDSTRIKE

DISCOVERY, REDISCOVERY AND CIRCUMVENTION

The 2022 Vulnerability Intelligence Landscape

취약점 발견 및 재발견

공격자는 유사하게 취약한 제품을 대상으로 동일한 익스플로잇을 수정하거나 심지어 재적용합니다.

이전 패치 우회

2022년에 관찰된 제로데이 및 N데이 취약점은 공격자가 전문 지식을 활용하여 이전 패치의 완화 조치를 우회하여 동일한 취약한 구성 요소를 표적으로 삼을 수 있는 능력을 보여주었습니다.

Microsoft's 신뢰의 위기

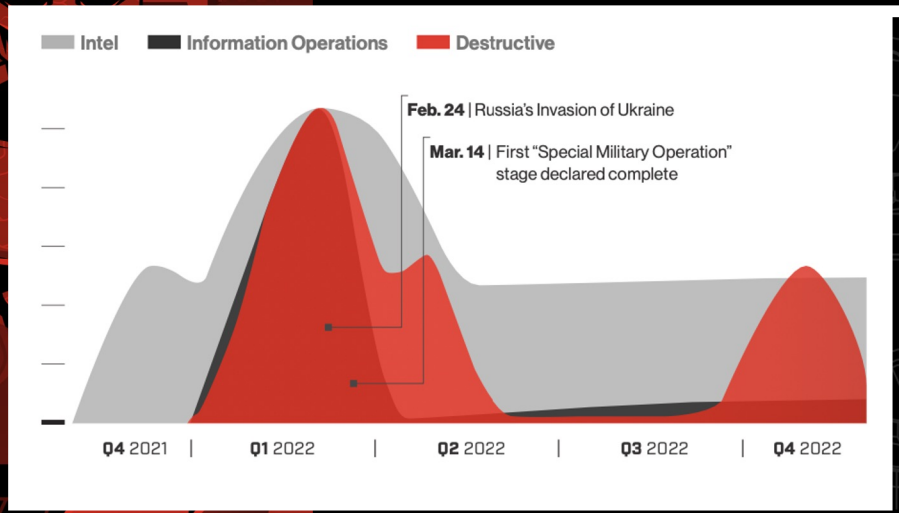
MSFT 는 2022년에 28개의 제로 데이를 포함하여 1200개 이상의 패치를 발표했습니다.

"패치 관리는 설정하고 잊어버리는 것이 아닙니다. 적의 정교화를 위해서는 중요한 패치의 우선 순위를 지정하고 적의 활동을 즉시 식별할 수 있는 심층 방어가 필요합니다."

CROWDSTRIKE

High Effort, Limited Return

우크라이나 전쟁을 지원하는 러시아 사이버 작전



에너지, 통신, 운송 및 미디어와 같은 핵심 부문에 대한 공격은 예상만큼 광범위하지 않았으며, 이는 크렘린이 우크라이나에 대한 신속하고 결정적인 승리를 기대하고 이러한 기능 자원을 사용하여 우크라이나를 새로운 체제 하에서 계속 운영할 계획임을 나타내는 것으로 보입니다.

우크라이나 전쟁에서 중국이 얻은 교훈
- 사이버보안관점

러시아의 사이버 공격이 신속/충분하지/성공적이지 못했다 공격의 대상은 우크라이나 한곳, 대응은 우방 전체 (ex: Starlink) 사이버 역량에 대한 재평가와 대규모 투자 통해 사이버 공격 역량이 더욱 증대될 것이며 그 대상이 미국과 더불어 지리적 우방 (대만,한국,일본)에 대한 정보 수집과 공격 역량을 더욱 강화 시킬 것으로 예상됨

"침해를 막으려면 공격자의 동기, 기술, 조직을 표적으로 삼는 방법을 포함하여 적에 대한 이해가 필요합니다."

CROWDSTRIKE

DOMINATING THE ESPIONAGE LANDSCAPE

China-nexus adversaries, 2022년 작전 규모 대폭 증가

초기 액세스 권한을 얻기 위한 Exploit

China-Nexus 적들은 계속해서 공개 웹 서비스를 Exploit하는 방향으로 공격

제로데이 익스플로잇 사용 증가

엔터프라이즈 소프트웨어는 계속해서 우선 순위가 높은 타깃 대상이었습니다. 추가적인 제로데이 익스플로잇에는 무기화된 MSFT Office 문서가 포함됩니다.

대만을 타깃으로 한 공격 증가

기존 엔드포인트를 활용하여 클라우드로 피벗(또는 그 반대로)하는 공격자가 더욱 자신감을 갖고 공격을 수행

"거의 모든 39개 글로벌 산업 부문과 20개 지역을 노리는 중국 넥서스 적들이 관찰되었습니다."

제로데이 익스플로잇은 2022년 북미 조직을 대상으로 한 침입에서 가장 일반적으로 관찰되었습니다. 중국과 연계된 적들은 제로데이 익스플로잇을 사용하여 항공 우주, 법률 및 학술 부문의 기업을 손상시켰습니다.

CROWDSTRIKE

DOMINATING THE ESPIONAGE LANDSCAPE

China-nexus adversaries, 2022년 작전 규모 대폭 증가

- 대만에 대한 중국의 공격은 한국에 대한 공격의 아주 유사한 Case Study 형태를 가짐
- 미국의 중국에 대한 다양한 제제는 중국이 대만과 한국이 보유한 첨단 기술 유출을 목적으로 함.
- 중국이 미국 기업에 대한 직접적인 공격없이 필요한 기술, 정보 탈취가능하기 때문
- 정부 기관 및 첨단기술기업 (Supply Chain관련)들의 각별한 관심이 필요한 영역임

" CCP(Chinese Communist Party) Intel Goal is Tech Independence & Dominance"

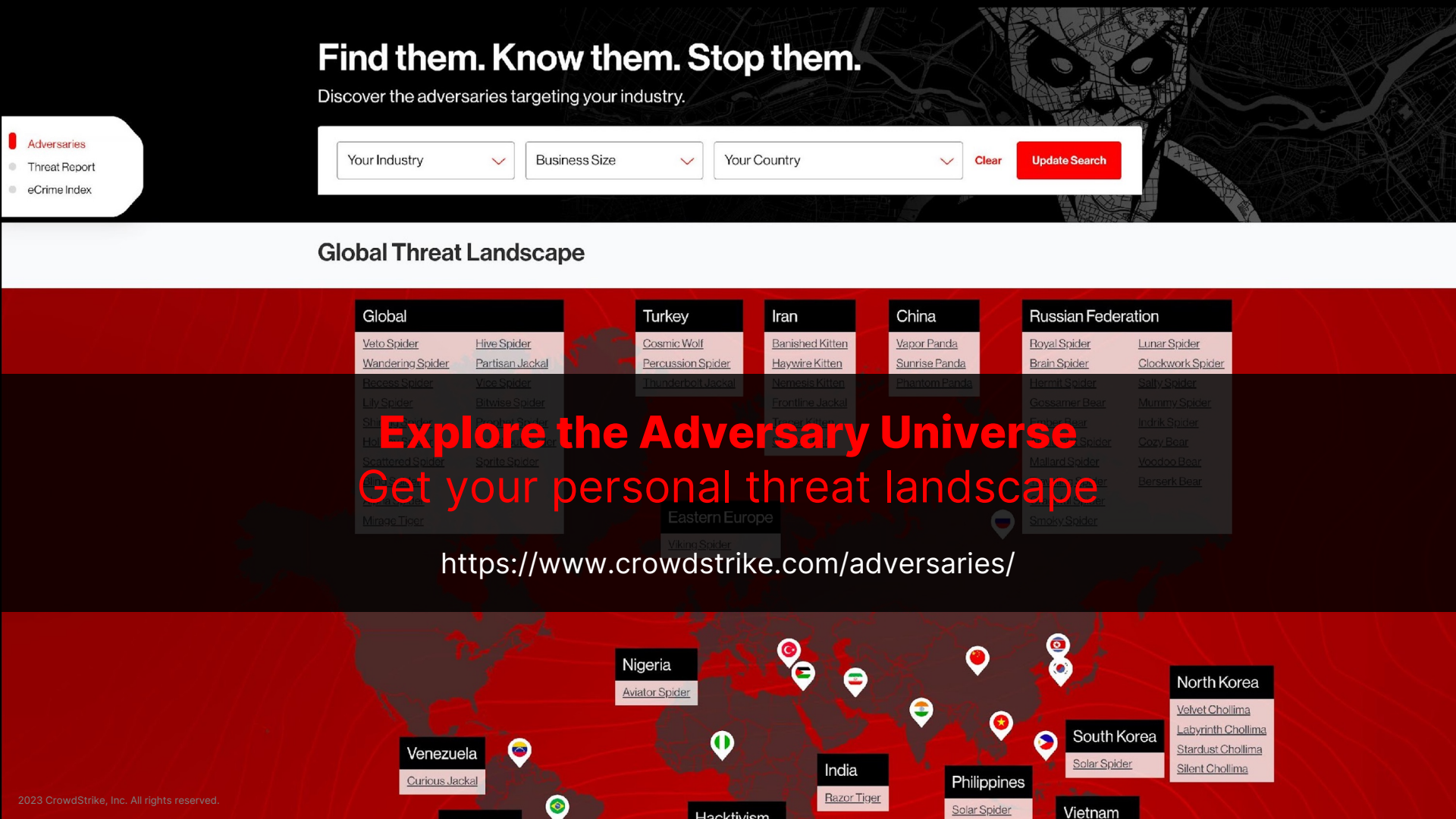
대만을 타깃으로 한 공격 증가

기존 엔드포인트를 활용하여 클라우드로 피벗(또는 그 반대로)하는 공격자가 더욱 자신감을 갖고 공격을 수행

CROWDSTRIKE

준비해야 할 5단계

1. **Gain visibility into your security gaps**
   진화하는 공격기술과 툴을 탐지할 수 있는 기술과 역량을 육성 또는 서비스
2. **Prioritize identity protection**
   AD취약성 보완을 위한 기술, Access Broker에 대응할 수 있는 인텔리젼스
3. **Prioritize cloud protection**
   증가하는 Risk/Attk Surface에 대한 대응
4. **Know your adversary**
   Real Threat Intelligence , IOA beyond IOC
5. **Practice makes perfect**
   Red/Blue Team 의 상시화, Gap,취약점의 상시 감지 및 보완


Find them. Know them. Stop them.
Discover the adversaries targeting your industry.
Adversaries
Threat Report
eCrime Index
Your Industry
Business Size
Your Country
Clear
Update Search
Global Threat Landscape
Global
Veto Spider
Hive Spider
Wandering Spider
Partisan Jackal
Recess Spider
Vice Spider
Lily Spider
Bitwise Spider
Scattered Spider
Sprite Spider
Mirage Tiger
Turkey
Cosmic Wolf
Percussion Spider
Thunderbolt Jackal
Iran
Banished Kitten
Haywire Kitten
Nemesis Kitten
Frontline Jackal
China
Vapor Panda
Sunrise Panda
Phantom Panda
Russian Federation
Royal Spider
Lunar Spider
Brain Spider
Clockwork Spider
Hermit Spider
Sally Spider
Gossamer Bear
Mummy Spider
Indrik Spider
Cozy Bear
Mallard Spider
Voodoo Bear
Berserk Bear
Smoky Spider
Eastern Europe
Viking Spider
Explore the Adversary Universe
Get your personal threat landscape
https://www.crowdstrike.com/adversaries/
Nigeria
Aviator Spider
North Korea
Velvet Chollima
Labyrinth Chollima
Stardust Chollima
Silent Chollima
South Korea
Solar Spider
Venezuela
Curious Jackal
India
Razor Tiger
Philippines
Solar Spider
Vietnam
Hacktivism
2023 CrowdStrike, Inc. All rights reserved.

CrowdStrike Falcon 플랫폼에서 제공되는 서비스

Endpoint Security & XDR

Cloud Security

Threat Intelligence

Identity Protection

Security & IT ops

Observability

Managed Threat Hunting | **Managed Detection & Response** | **Incident Response** | **Proactive Services**

Automation & Orchestration

Data Fabric

Threat Graph | **Asset Graph** | **Intel Graph** | **APIs & Ecosystem**

Unified Agent | Agentless

CROWDSTRIKE

Pioneering Adversary Intelligence Keeps You Ahead of Attackers

업계에서 리딩 위협 인텔리전스 팀: 크라우드스트라이크의 기반

200+	200K	7+ Trillion	1.2+ Million
추적하는 공격그룹/일간	새로 발간되는 IOC/일간	실시간 수집 텔레메트리/주간	악성코드 수집/일간

FORRESTER®

#1 in Intelligence Collection

The Forrester Wave™ External Threat Intelligence Services, Q1 2021

CROWDSTRIKE

왜 CrowdStrike 인가

검증된 보안 테스트에서 우수한 결과

MITRE
동종 경쟁 대비 높은 탐지율

SE Labs
100% 랜섬웨어 차단

비용 감소

손쉬운 배포와 관리
Zero 리부팅, no downtime,
& no manual tuning

제품 통합

불필요한 에이전트 제거
독립 실행형 도구를 통합하여
복잡성 제거

CROWDSTRIKE


감사합니다