Trellix

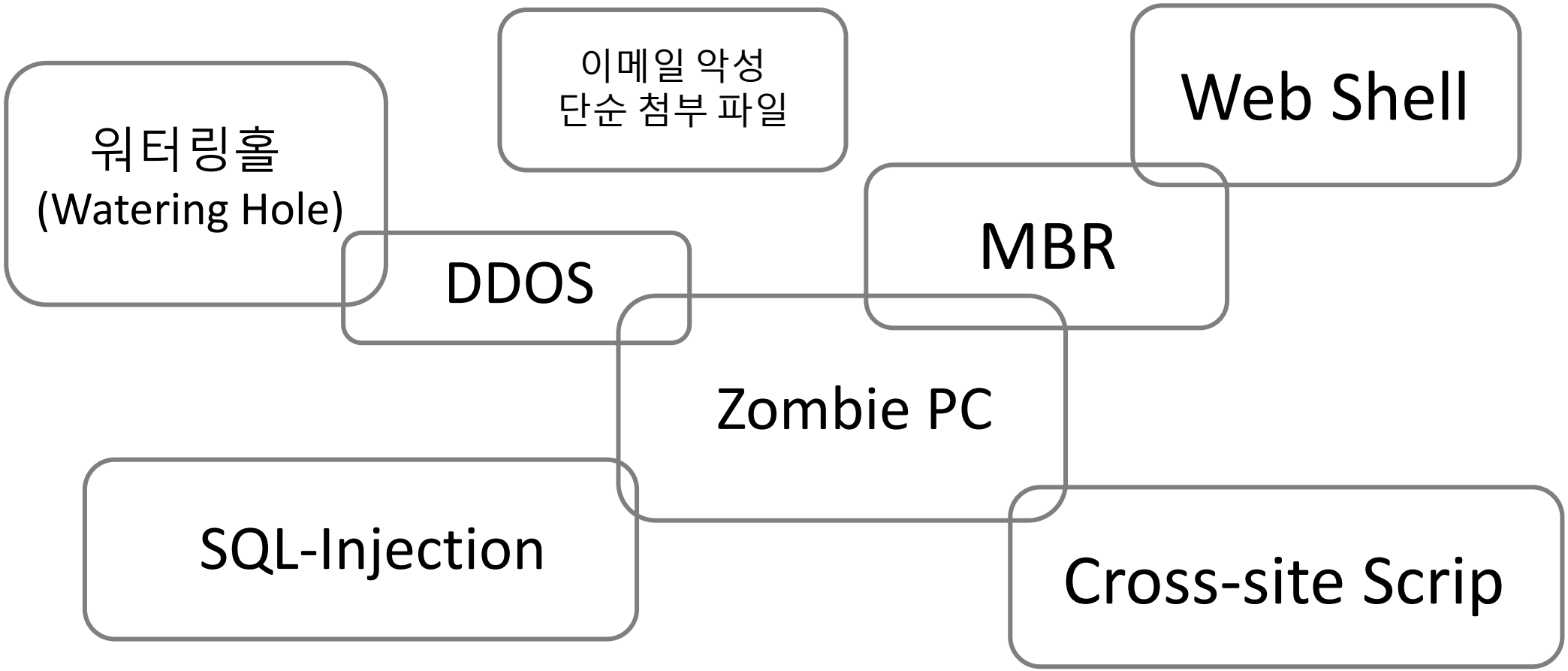
최신 위협(Threat)대응

그들은 무엇에 진심인가...

Sept 2022

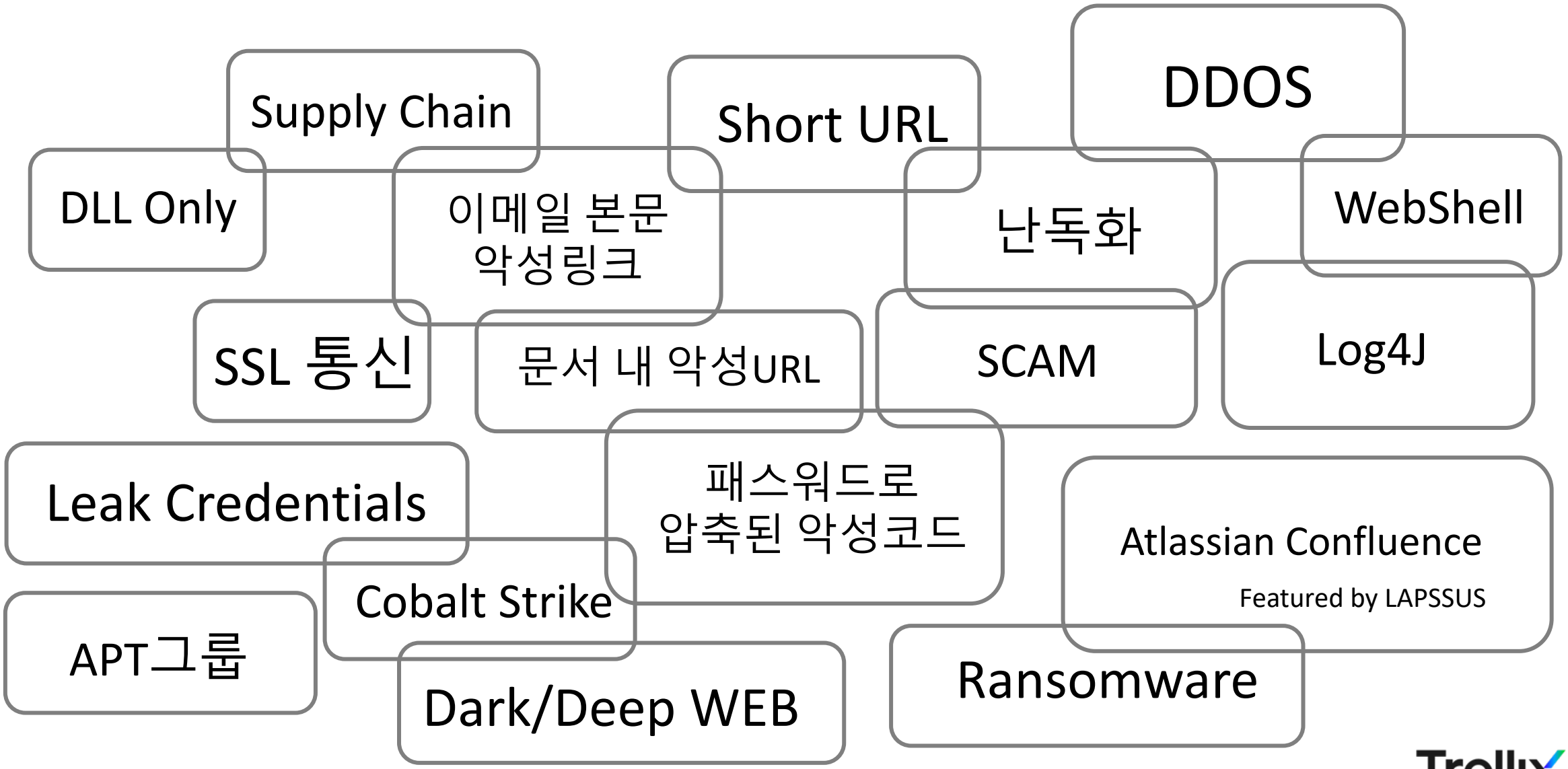
Living Security

10 Years Ago...



Trellix

Now…


Supply Chain
Short URL
DDOS
DLL Only
이메일 본문
악성링크
난독화
WebShell
SSL 통신
문서 내 악성URL
SCAM
Log4J
Leak Credentials
패스워드로
압축된 악성코드
Atlassian Confluence
Featured by LAPSSUS
Cobalt Strike
APT그룹
Dark/Deep WEB
Ransomware

Trellix

어떻게 변화하고 있는가..

Targeting 공격의 증가 ✓

인프라 환경의 변화에 따른 공격 표면(Surface) 증가 ✓

Business Hacking ✓

Hacker → Hacking Group (APTs) / Hacking Group의 리소스 증가 ✓

새로운 Zero Day 취약점/Exploit의 지속적인 증가?

새로운 공격 도구의 증가?

Email Security Trends: Q1 2022.

Source : FY22 Trellix Threat Insight Report

Email 유형

Phising URLs, 문서 내 URL, 패스워드를 포함한 압축파일, 매크로가 포함된 악성 문서형태를 전달하는 공격의 지속적인 증가가 발견되었습니다.

Exploit

사용된 Exploit에 초점을 맞추면 대부분이 악성 RTF 파일, 무기화된 OLE 개체가 있는 MS Office 문서, Adobe Reader Exploit 또는 악성 JS 스크립트에 감염된 PDF로 포장되어 있음을 알게 됩니다. 다음 그림에서 상위 3개 파일 형식이 Windows RTF 이고 그 다음이 최신 Office 형식이며 마지막으로 레거시 역할을 하는 Office 문서형태가 가장 많이 발견 되었습니다.

RTF	50.76%
CVE-2017-11882	15.7%
CVE-2012-0158	12.84%
CVE-2017-0199	17.94%
CVE-2014-1761	5.8%
CVE-2017-8759	4.41%

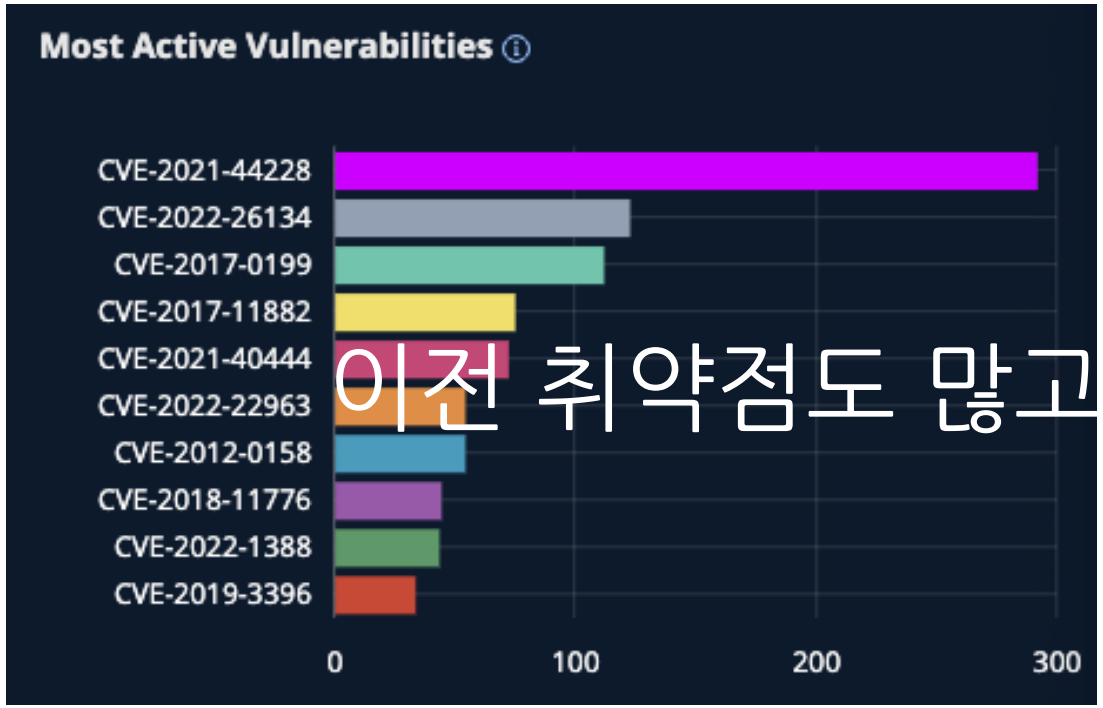
Office	31.25%
CVE-2017-11882	23.84%
CVE-2017-0199	3.05%
CVE-2017-8570	1.7%

OLE	17.99%
CVE-2017-11882	12.74%
CVE-0201-20158	4.16%

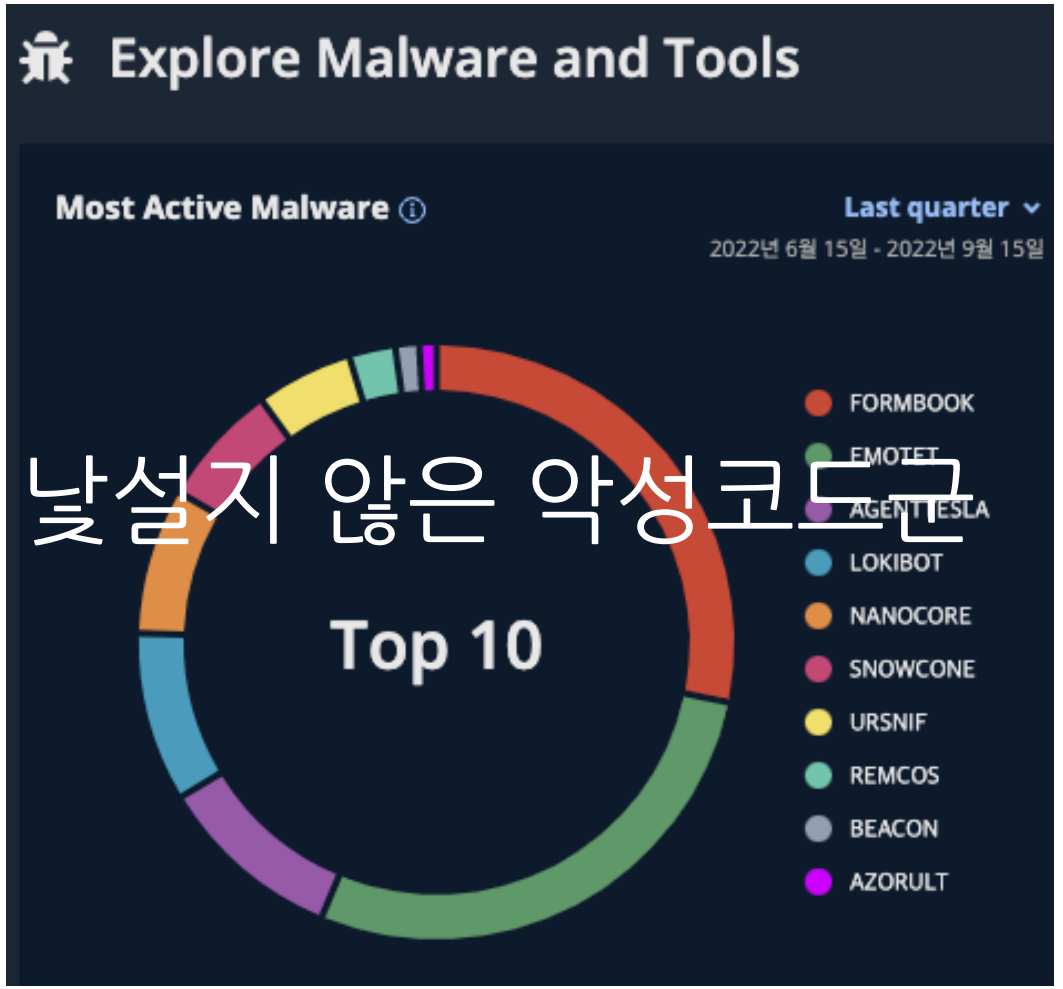
Trellix

최근 위협에 가장 많이 사용된 취약점 / Malware Family(악성코드군)

Source : Mandiant Advantage



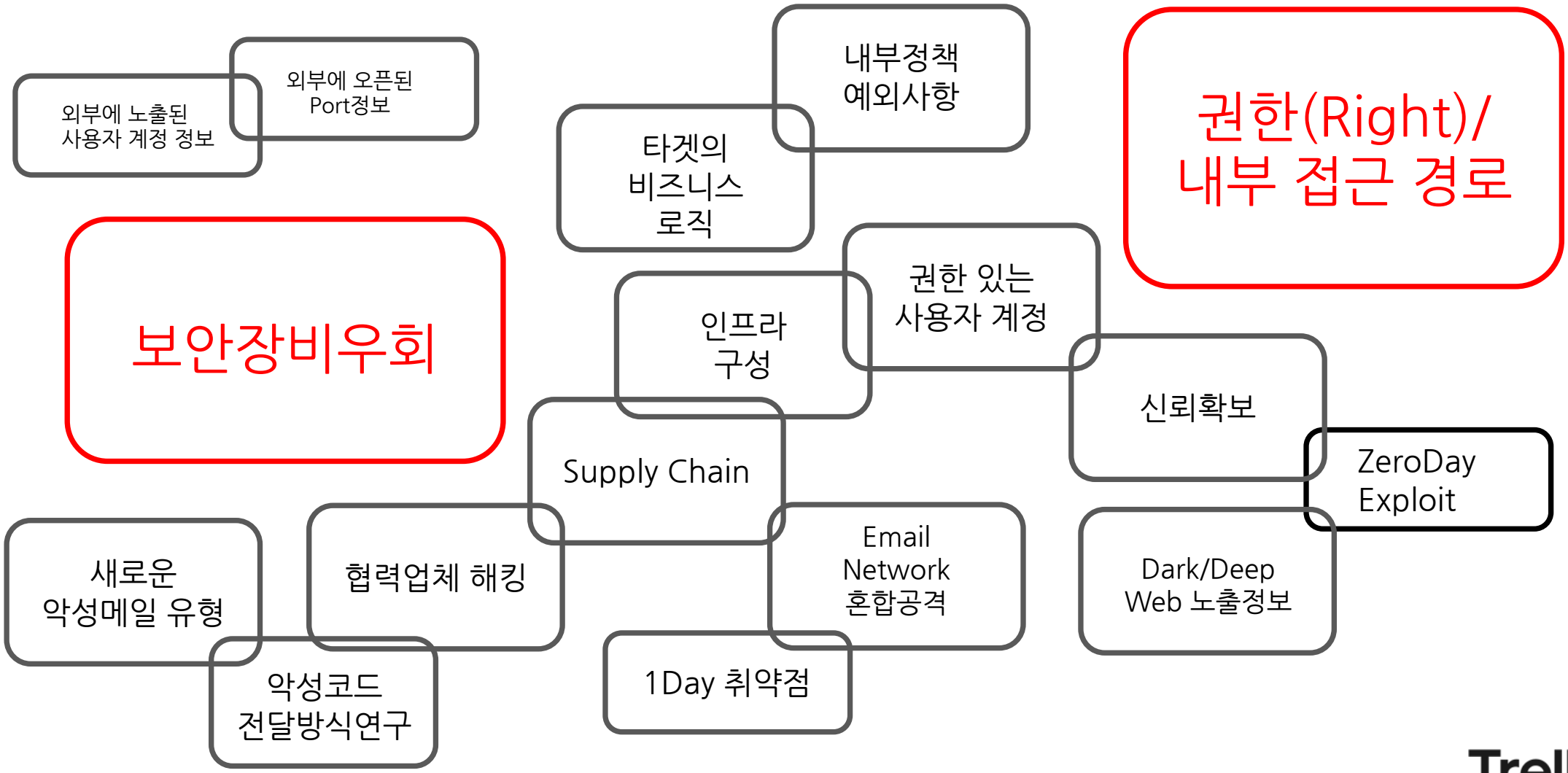
이전 취약점도 많고



낯설지 않은 악성코드군

Trellix

공격자는 어디에 노력을 기울이고 있을까 ?



Trellix

NIST Cyber Security Framework

IDENTIFY

What processes and assets need protection?

PROTECT

Implement appropriate safeguards to ensure the protection of assets of enterprises

DETECT

Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents

RESPOND

Develop techniques to contain the impacts of cybersecurity events

RECOVER

Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events

최신 위협 대응 (Threat Response)에 무엇이 더 필요할까?

Basic

내 외부 권한 관리 (Right Management)

Network Segmentation

Multi-Factor Authentication

보안 EVENT 대응

Advance

Multi-flow 분석 능력 향상

Threat 중심 대응

Trellix

악성코드에만 집중하지 마세요

공격자의 공격 전달 방법/ 공격 유형을 이해하지 못하면 알려진 공격도 방어 할 수 없습니다

보이지 않는 위협(Threat)은 막을 수 없습니다

Trellix

우리가 대응해야 하는 것은

하나 하나의 이벤트(Alert)가 아닌

위협(Threat)입니다

Trellix

감사합니다