최신 타겟형 공격 사례

김진국 @PLAINBIT

PLAINBIT

타겟형 공격 이란?

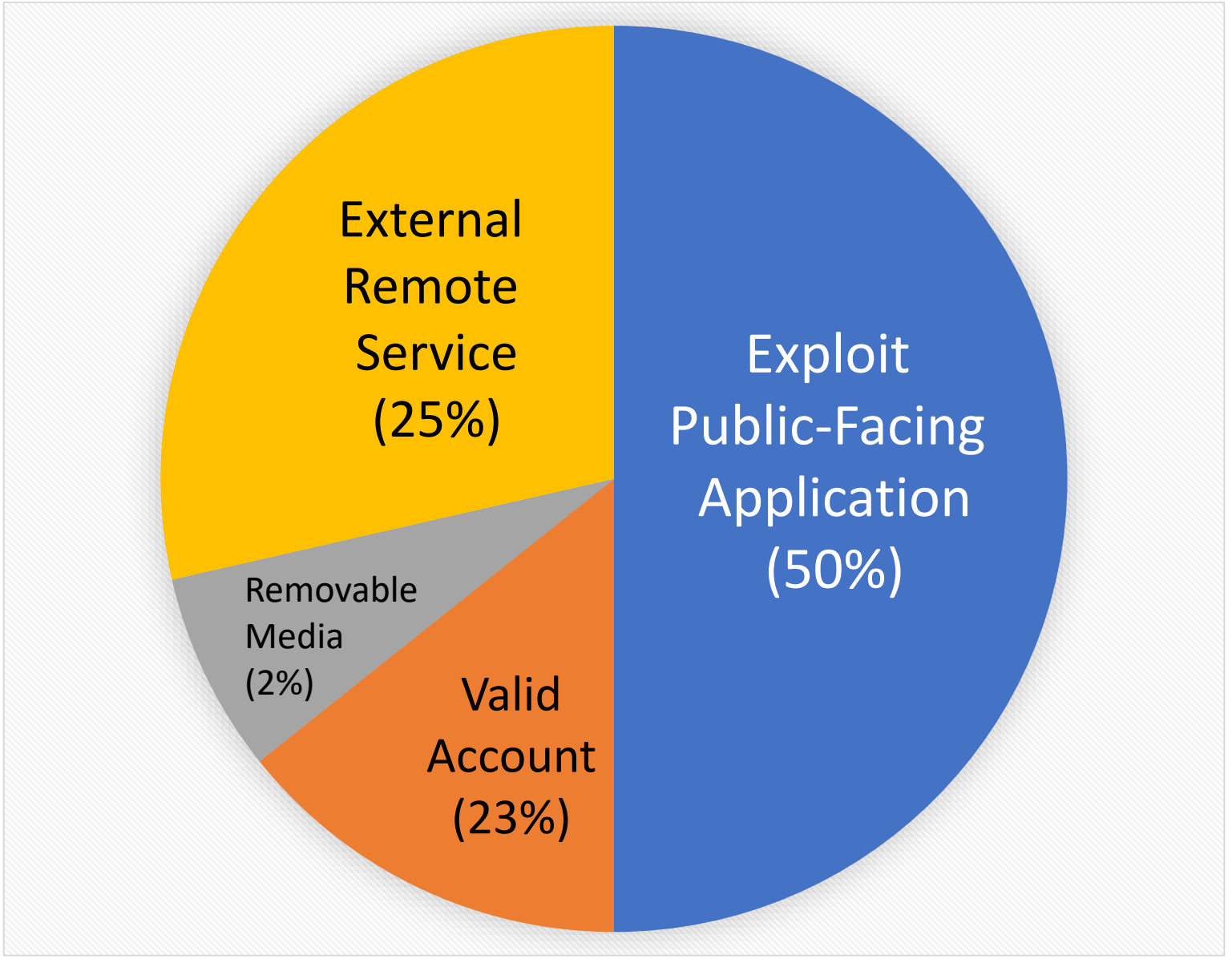
Advanced **P**ersistent **T**hreat

Targeted Attack

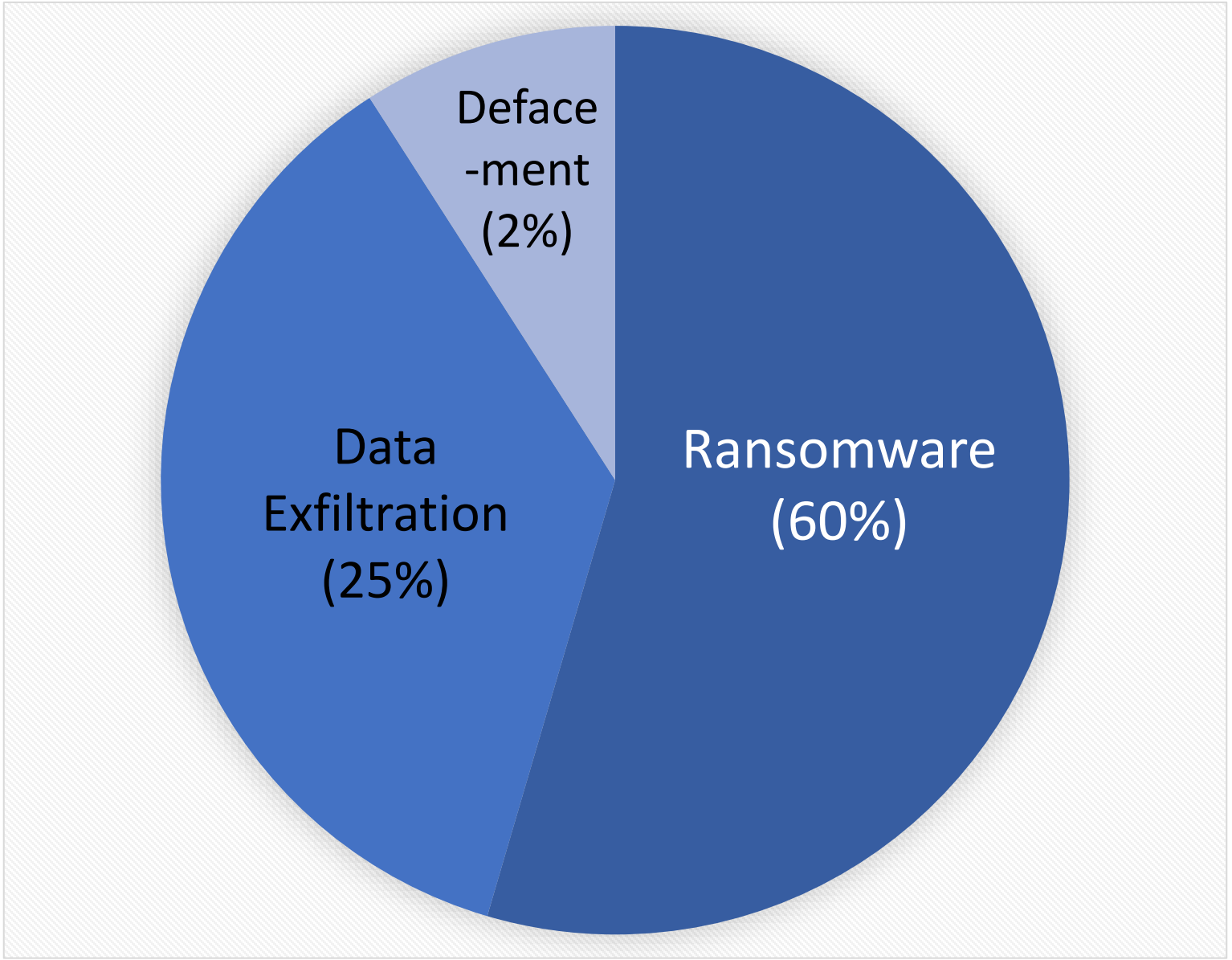
- 목표 지향성
- 정보 수집과 정밀한 계획
- 맞춤형 기술
- 은밀성과 위장
- 파괴적인 목적

타겟형 공격 통계

사고 원인



사고 영향



PLAINBIT

최근 타겟형 공격의 특징

최근 타겟형 공격의 특징

PLAINBIT

거점 폴더의 변화

- 시스템 내에서 Discovery을 위해 거점으로 사용하는 폴더
- 지속성 등록 전에 임시로 사용
- 추가 악성코드 다운로드, 임시 스크립트 저장
- 지속성 등록이나 내부 이동 후, 거점 폴더 내 파일 삭제

→ 실행 아티팩트, INDX 슬랙, 삭제된 파일 흔적으로 파악

최근에 주로 사용하는 거점 폴더

- C:\PerfLogs
- C:\ProgramData
- C:\ProgramFiles
- C:\%UserProfile%\AppData
- C:\Temp
- C:\$Recycle.Bin

최근 타겟형 공격의 특징

PLAINBIT

파일시스템 시간 조작 비율의 증가

- 거점 폴더 → 지속성 등록을 위해 시스템 폴더로 이동
  - %SystemRoot%
  - %SystemRoot%\System32
  - %SystemRoot%\...
- 시스템 폴더에 존재하는 악성코드의 대부분이 시간 조작
  - 98% : $SIA 시간만 변경
  - 2% : $SIA, $FNA 시간 모두 변경

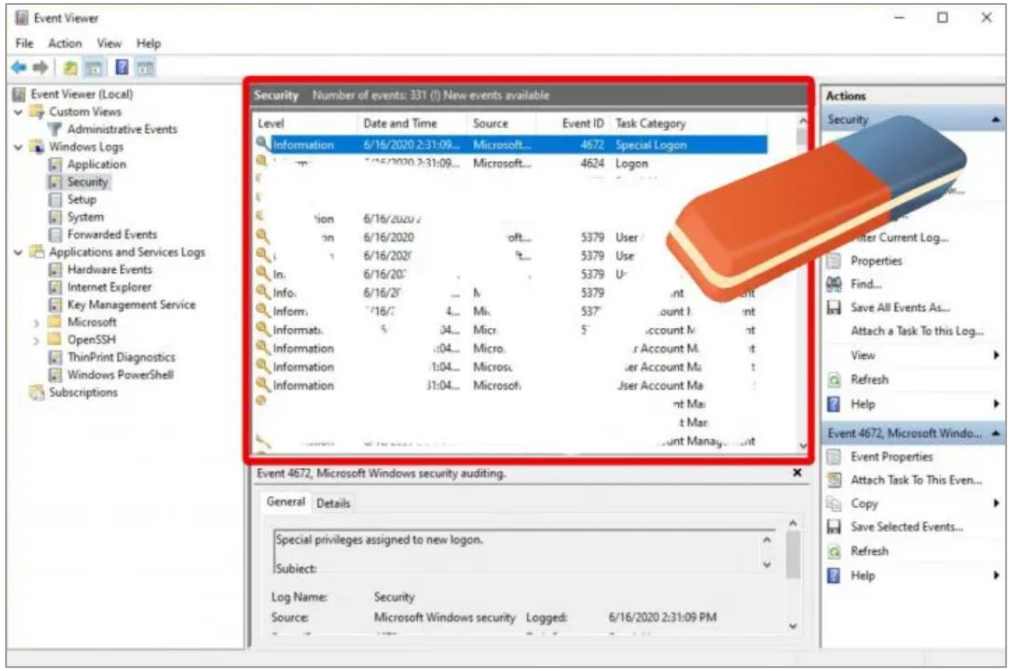
시간 조작된 파일 식별 방안

- *$FNA 시간을 기준으로 타임라인 분석*
- *$SIA Created < $FNA Created*
- *시간 정보가 동일한 파일(동기화)*
- *나노초 이하 정밀도가 '0' 인 파일*
- *주요 폴더의 MFT Sequence 증가 패턴*

최근 타겟형 공격의 특징

PLAINBIT

이벤트 로그 삭제 비율의 증가



- 타겟형이 아닌 랜섬웨어 공격도 이벤트 로그 삭제
  - wevtutil, Remove-EventLog(PowerShell)

- 이벤트 로그 삭제는 Default → 호스트 침해 탐지 규칙으로 활용
  - Security.evtx
  - System.evtx
  - Application.evtx
  - Windows PowerShell.evtx
  - Microsoft-Windows-TerminalServices-*.evtx
  - Microsoft-Windows-Sysmon%4Operational.evtx

최근 타겟형 공격의 특징

PLAINBIT

주요 악성파일의 치밀한(?) 은닉

- 공격에 사용하는 공격자 핵심 파일의 경우 → 정교하게 은닉
  - 0-day 취약점 코드
  - 인프라 유지/관리를 위한 웹셸
  - 중요 악성코드 (내부망 스캔, 취약점 공격 코드 등)

- 지속 매커니즘을 사용하지 않고, 임시 실행을 통해 노출 최소화

- 공격 간 혹은 마무리에 핵심 파일만 완전 삭제(Wipe)

최근 타겟형 공격의 특징

PLAINBIT

악성코드 형식의 변화

- LotL(Living off the Land) 공격의 증가
  - 파일리스(Fileless) 형식의 악성코드 사용(전체 악성코드의 60% 이상)
    - ✓ PowerShell
    - ✓ Windows Command Shell
    - ✓ Visual Basic, Python, JavaScript
  - 시스템의 기본으로 존재하고 합법적인 도구를 사용 → 추가 파일이나 서명이 필요 없음
    - ✓ wmic.exe, PsExec.exe
    - ✓ reg.exe, regsvr32.exe, mshta.exe, rundll32.exe, certutil.exe
    - ✓ WScript.exe, CScript.exe, mimikatz.exe, CobaltStrike
    - ✓ Schtasks.exe, sc.exe, findstr.exe, whoami.exe

정교한 공격자도

안전이 보장되면 더 이상 정교하지 않다.

PLAINBIT