

Forum: [Hack Forums](#)

Thread: [Free Pentest tool malware](#)

BlackHatFrench - August 30, 2024, 6:51 am

#malware #builder #rat #crackedsoftware #crypter #binder #proxy
[deleted] [warn]

Reviewed by staff : Programs Backdoored

Bastille - August 31, 2024, 1:21 am

OP shared a website where hacking tools are proposed for free, and where he sells RDP access and a Ransomware.

The tools are shared via monetized link shorteners, there is a timer, you must wait, and the more people wait, the more OP earns money.

All tools proposed are RAR files and password protected. The objective is to bypass Virustotal scans. There are other techniques, such as increasing the size of the file (more than 700MB, which is the limit of Virustotal) so victims are less likely to upload it and scan it.

("Mot de passe" = "Password" in french)

Analysis : 1/10 - "UnamBinder.exe"

Official Github Repo : <https://github.com/UnamSanctam/UnamBinder>

Official version VT scan :

<https://www.virustotal.com/gui/file/a90ba5a56422c0d2a41f28da056affd69cc8929e14dcdab1583ec96b50b8e28d>

MD5 : 70565dbd654937df2eaefc7c79941169

SHA-1 : 5cb8daf1185704a9772f07dcec2e499149517715

[BlackHatFrench](#) version :

RAR file and password protected : Virustotal is not able to scan the file

Extracted file :

MD5 : e28b353cdd171bebc92bfba22df84e55

SHA-1 : def28d38a81339318da908c50f32c840903d3270

I. COMPARISON

OP's version has been modified compared to the "Official" version available on Github. Different IP addresses are contacted, different files are dropped, executed and deleted, TTPs are different too.

a. IP addresses and Domain names

UB (UnamBinder) version shared by OP contacts a Domain name flagged as malicious : jajaovh.duckdns.org (<https://www.duckdns.org/> is a Dynamic DNS service provider) either OP is often changing his IP address (VPN, VPS), or he's hosting his C2 server at home because of a dynamic IP address provided by his ISP.

b. Notable files

crack.exesha256 010b8db19ead1ba157738c6da0d1e5ae38f611aac56de325e872e1dc61229cf2
type PE_EXE

Identification : family_xworm (YaraRule)

Windows Driver Fondation.exesha256

010b8db19ead1ba157738c6da0d1e5ae38f611aac56de325e872e1dc61229cf2

type PE_EXE

Identification : family_xworm (YaraRule)

VT :

<https://www.virustotal.com/gui/file/010b8db19ead1ba157738c6da0d1e5ae38f611aac56de325e872e1dc61229cf2/behavior>

Quote:"C:\Windows\System32\schtasks.exe" /create /f /sc minute /mo 1 /tn "Windows Driver Fondation" /tr "C:\Users\admin\AppData\Local\Temp\Windows Driver Fondation"

ANY.RUN link :

<https://any.run/report/dbf2cb7da5398a29caf5d636a76c716801d6562646edc694b2c9f2ae6289642c/48d052a0-9e32-4b90-9c0f-30f2c891e13e>

c. TTPs

Here are the additional TTPs (Tactics, Techniques, Procedures) that are not present in the "Official" version available on Github, which tells us that this version has been backdoored :

Persistence [[TA0003](#)]Scheduled Task/Job - T1053

Boot or Logon Autostart Execution - T1547

Privilege Escalation [[TA0004](#)]Process Injection - T1055

Access Token Manipulation - T1134

Credential Access [[TA0006](#)]Input Capture - T1056 > (Process #2) crack.exe logs keys and potentially exfiltrates data.

Steal Web Session Cookie - T1539

Decoded text

```
{'XWorm': {'C2': ['jajaovh.duckdns.org'], 'Port': ['1605'], 'AES Key (connections)': ['123456789'],  
'SPL': ['Xwormmm'], 'AES Key (configs)':  
['a525f59160cfea3aa19835326ca80fa525f59160cfea3aa19835326ca80fbd00'], 'Mutex':  
['ULGFpUS9mj98magF'], 'InstallDir': ['Temp'], 'InstallBinName': ['WindowsDriverFondation']}}
```

I'm also providing here the TRIA.GE report : <https://tria.ge/240831-hgsdfa1all/behavioral1>

Another tool shared on his website is WH-ApkCrypter-V2.1.sfx.exe, has also been flagged by VT <https://www.virustotal.com/gui/file/f50db29597d991131fcb17ca02262ea1e3b8605555c7b70bef4ce04f93d00fb5/behavior> , what I want to emphasize here are the similarities with UB :

There is like a dozen different tools proposed for free (cracked), I might take a look at all of them but I think they are all backdoored the same way.

Stay safe guys ?

DramaKing - August 31, 2024, 5:14 am

(Aug 31, 2024 01:21 AM) Bastille Wrote: [\[CITE\]](#) OP shared a website where hacking tools are proposed for free, and where he sells RDP access and a Ransomware.

The tools are shared via monetized link shorteners, there is a timer, you must wait, and the more people wait, the more OP earns money.

All tools proposed are RAR files and password protected. The objective is to bypass Virustotal scans. There are other techniques, such as increasing the size of the file (more than 700MB, which is the limit of Virustotal) so victims are less likely to upload it and scan it.

("Mot de passe" = "Password" in french)

Analysis : 1/10 - "UnamBinder.exe"

Official Github Repo : <https://github.com/UnamSanctam/UnamBinder>

Official version VT scan :

<https://www.virustotal.com/gui/file/a90ba5a56422c0d2a41f28da056affd69cc8929e14dcdab1583ec96b50b8e28d>

MD5 : 70565dbd654937df2eaefc7c79941169

SHA-1 : 5cb8daf1185704a9772f07dcec2e499149517715

[BlackHatFrench](#) version :

RAR file and password protected : Virustotal is not able to scan the file

Extracted file :

MD5 : e28b353cdd171bebc92bfba22df84e55

SHA-1 : def28d38a81339318da908c50f32c840903d3270

I. COMPARISON

OP's version has been modified compared to the "Official" version available on Github. Different IP addresses are contacted, different files are dropped, executed and deleted, TTPs are different too.

a. IP addresses and Domain names

UB (UnamBinder) version shared by OP contacts a Domain name flagged as malicious : [jajaovh.duckdns.org](https://www.duckdns.org/) (<https://www.duckdns.org/> is a Dynamic DNS service provider) either OP is often changing his IP address (VPN, VPS), or he's hosting his C2 server at home because of a

dynamic IP address provided by his ISP.

b. Notable files

crack.exesha256 010b8db19ead1ba157738c6da0d1e5ae38f611aac56de325e872e1dc61229cf2
type PE_EXE

Identification : family_xworm (YaraRule)

Windows Driver Fondation.exesha256

010b8db19ead1ba157738c6da0d1e5ae38f611aac56de325e872e1dc61229cf2

type PE_EXE

Identification : family_xworm (YaraRule)

VT :

<https://www.virustotal.com/gui/file/010b8db19ead1ba157738c6da0d1e5ae38f611aac56de325e872e1dc61229cf2/behavior>

ANY.RUN link :

<https://any.run/report/dbf2cb7da5398a29caf5d636a76c716801d6562646edc694b2c9f2ae6289642c/48d052a0-9e32-4b90-9c0f-30f2c891e13e>

c. TTPs

Here are the additional TTPs (Tactics, Techniques, Procedures) that are not present in the "Official" version available on Github, which tells us that this version has been backdoored :

Persistence [TA0003]Scheduled Task/Job - T1053

Boot or Logon Autostart Execution - T1547

Privilege Escalation [TA0004]Process Injection - T1055

Access Token Manipulation - T1134

Credential Access [TA0006]Input Capture - T1056 > (Process #2) crack.exe logs keys and potentially exfiltrates data.

Steal Web Session Cookie - T1539

Decoded text

```
{'XWorm': {'C2': ['jajaovh.duckdns.org'], 'Port': ['1605'], 'AES Key (connections)': ['123456789'],  
'SPL': ['Xwormmm'], 'AES Key (configs)':  
['a525f59160cfea3aa19835326ca80fa525f59160cfea3aa19835326ca80fbd00'], 'Mutex':  
['ULGFpUS9mj98magF'], 'InstallDir': ['Temp'], 'InstallBinName': ['WindowsDriverFondation']}}
```

I'm also providing here the TRIA.GE report : <https://tria.ge/240831-hgsdfa1all/behavioral1>

Another tool shared on his website is WH-ApkCrypter-V2.1.sfx.exe, has also been flagged by VT <https://www.virustotal.com/gui/file/f50db29597d991131fcb17ca02262ea1e3b8605555c7b70bef4ce04f93d00fb5/behavior> , what I want to emphasize here are the similarities with UB :

There is like a dozen different tools proposed for free (cracked), I might take a look at all of them but I think they are all backdoored the same way.

Stay safe guys ?

Weirdly, jajaovh.duckdns.org returns 8.8.8.8.

Bastille - August 31, 2024, 5:50 am

(Aug 31, 2024 05:14 AM)DramaKing Wrote: [\[CITE\]](#) Weirdly, jajaovh.duckdns.org returns 8.8.8.8. I thought that the Dyn DNS would hide the IP address, and act as a mandatory server, but when I make a NSLOOKUP on jajaovh.duckdns.com it I have the following IP address : 95.211.189.138 which is related to <https://www.leaseweb.com>, and doesn't seem related to duckdns.org

His website seems protected or hosted by CloudFlare tho, not the same IP

EDIT : sometimes I also get this IP with a NSLOOKUP on jajaovh.duckdns.com : 192.198.80.148, I'm using this tool : <https://www.nslookup.io/>

Just used another tool that confirmed this :

DramaKing - August 31, 2024, 5:58 am

(Aug 31, 2024 05:50 AM)Bastille Wrote: [\[CITE\]](#) I thought that the Dyn DNS would hide the IP address, and acting as a mandatory server, but when I make a NSLOOKUP on jajaovh.duckdns.com it I have the following IP address : 95.211.189.138 which is related to <https://www.leaseweb.com>, and doesn't seem related to duckdns.org

His website seems protected or hosted by CloudFlare tho, not the same IP

EDIT : sometimes I also get this IP with a NSLOOKUP on jajaovh.duckdns.com : 192.198.80.148, I'm using this tool : <https://www.nslookup.io/>

Just used another tool that confirmed this :

How are you getting that? I even used the tool that you mentioned.

EDIT: I know how. I was using duckdns.org, and you were using duckdns.com.

Bastille - August 31, 2024, 9:17 am

(Aug 31, 2024 05:58 AM)DramaKing Wrote: [\[CITE\]](#) How are you getting that? I even used the tool that you mentioned.

EDIT: I know how. I was using duckdns.org, and you were using duckdns.com.
Holy ...

Weird that 8.8.8.8 is returned so, I'll take a look at duckdns to see how it works

Ivanov_1 - September 1, 2024, 7:23 am

Bastille thank you for looking out for other members, if he was intentionally trying to infect members he should be banned.

Bastille - September 1, 2024, 7:52 am

(Sep 1, 2024 07:23 AM)Ivanov_1 Wrote: [\[CITE\]](#) Bastille thank you for looking out for other members, if he was intentionally trying to infect members he should be banned.

Thanks man ! Don't forget to quote or to use the mention feature when you type someone's username otherwise the member will not get notified (@ username@ without the space after the first @).

If you're interested in this kind of content, take a look at this thread, it's a collection of spotted

malicious programs <https://hackforums.net/showthread.php?tid=6276795>

And OP has been banned, that's why his username is black. Of course it was intentional, no place for people trying to infect HF members ?

InspectorGadget - September 1, 2024, 9:25 am

(Aug 31, 2024 01:21 AM)Bastille Wrote: [\[CITE\]](#) ...

(Aug 31, 2024 05:14 AM)DramaKing Wrote: [\[CITE\]](#) ...

Great work both of you :)

Ivanov_1 - September 1, 2024, 9:30 am

(Sep 1, 2024 07:52 AM)Bastille Wrote: [\[CITE\]](#) Thanks man ! Don't forget to quote or to use the mention feature when you type someone's username otherwise the member will not get notified (@username@ without the space after the first @).

If you're interested in this kind of content, take a look at this thread, it's a collection of spotted malicious programs <https://hackforums.net/showthread.php?tid=6276795>

And OP has been banned, that's why his username is black. Of course it was intentional, no place for people trying to infect HF members ?

My bad Bastille,i will keep it in mind. I will take a look at the sources you wrote,thank you.

Novo - January 14, 2025, 8:14 am

(Aug 31, 2024 05:14 AM)DramaKing Wrote: [\[CITE\]](#) Weirdly, jajaovh.duckdns.org returns 8.8.8.8.

(Aug 31, 2024 09:17 AM)Bastille Wrote: [\[CITE\]](#) Holy ...

Weird that 8.8.8.8 is returned so, I'll take a look at duckdns to see how it works
DuckDNS voids all subdomains when they get reported from <https://urlhaus.abuse.ch/> to local ip addresses, 8.8.8.8, etc

EDIT: not urlhaus, but abuse.ch or one of its websites or it just mainly it got reported. but yeah, duckdns voids subdomains when they link to malware

Bastille - January 15, 2025, 1:03 am

(Jan 14, 2025 09:14 AM)NovoDev Wrote: [\[CITE\]](#) DuckDNS voids all subdomains when they get reported from <https://urlhaus.abuse.ch/> to local ip addresses, 8.8.8.8, etc

EDIT: not urlhaus, but abuse.ch or one of its websites or it just mainly it got reported. but yeah, duckdns voids subdomains when they link to malware

Really interesting info thanks ! But now the domain name returns : 192.169.69.26

Browsing this IP through a browser I've got the following message :
read tcp 193.176.84.3:44328->192.169.69.26:80: read: connection reset by peer

Both of these IP have been reported as malicious

Wondering if I should dig

Novo - January 15, 2025, 3:47 am

(Jan 15, 2025 02:07 AM)m0hx Wrote: [\[CITE\]](#) could be a fake ip / used only when active kinda thing...and he changes it back to 8.8.8.8 to prevent suspicion.

never trust anything links to cf if its not their domains lol.

Nah, they do actually do that, once he does it

DuckDNS locks his dns, he cannot delete his account, delete the domain, changing the dns will not do anything