

Forum:[Hack Forums](#)

Thread: [Generating an undetectable backdoor in 2019?](#)

bexpr9 - August 20, 2019, 12:53 am

I know that bypassing AV programs is like a game of cat and mouse, so backdoors might start getting detected at some stage, then the developers release an update, this will allow us to generate undetectable backdoors, then AV programs release an update which will make backdoors detectable...

The problem is I have tried almost every payload in Veil Framework, Empire and Phantom Evasion but all of them are detected. Are there any tools that are working in 2019?

One - August 20, 2019, 2:09 am

(Aug 20, 2019 12:53 AM)bexpr9 Wrote: [\[CITE\]](#) I know that bypassing AV programs is like a game of cat and mouse, so backdoors might start getting detected at some stage, then the developers release an update, this will allow us to generate undetectable backdoors, then AV programs release an update which will make backdoors detectable...

The problem is I have tried almost every payload in Veil Framework, Empire and Phantom Evasion but all of them are detected. Are there any tools that are working in 2019?
get a Rat and a Crypter

bexpr9 - August 20, 2019, 6:40 am

(Aug 20, 2019 02:09 AM)Tygaking Wrote: [\[CITE\]](#) get a Rat and a Crypter

I've had some Rat and crypter, but I'm not sure about them.
Would you tell me what is the best Rat and Crypter?
Thank you for your attention.

CyberStrike - August 20, 2019, 10:35 am

(Aug 20, 2019 12:53 AM)bexpr9 Wrote: [\[CITE\]](#) I know that bypassing AV programs is like a game of cat and mouse, so backdoors might start getting detected at some stage, then the developers release an update, this will allow us to generate undetectable backdoors, then AV programs release an update which will make backdoors detectable...

The problem is I have tried almost every payload in Veil Framework, Empire and Phantom Evasion but all of them are detected. Are there any tools that are working in 2019?

Veil/Empire .. most of these really are "canned" solutions and well researched, you want to bypass AV start coding your own reverse shells or shellcode loaders generally reverse shells are quick and are a great way for that initial access. You gotta remember that many of these tools use what? You guessed it msfvenom it's actually not hard to go in check out the templates that are built and modify those.. also editing the templates in Metasploit is not impossible in fact if you know some asm you probably can get metersrv.dll to be rather undetectable for a while at least .. if you want all the options of meterpreter.. although that might be a better option for after priv esc and knocking out defenses.

bexpr9 - August 21, 2019, 5:08 pm

(Aug 20, 2019 10:35 AM)CyberStrike Wrote: [\[CITE\]](#) Veil/Empire .. most of these really are "canned" solutions and well researched, you want to bypass AV start coding your own reverse shells or shellcode loaders generally reverse shells are quick and are a great way for that initial access. You

gotta remember that many of these tools use what? You guessed it msfvenom it's actually not hard to go in check out the templates that are built and modify those.. also editing the templates in Metasploit is not impossible in fact if you know some asm you probably can get metsrv.dll to be rather undetectable for a while at least .. if you want all the options of meterpreter.. although that might be a better option for after priv esc and knocking out defenses.
thank you for your advice.

Silkroad - August 21, 2019, 5:25 pm

(Aug 20, 2019 10:35 AM)CyberStrike Wrote: [\[CITE\]](#) Veil/Empire .. most of these really are "canned" solutions and well researched, you want to bypass AV start coding your own reverse shells or shellcode loaders generally reverse shells are quick and are a great way for that initial access. You gotta remember that many of these tools use what? You guessed it msfvenom it's actually not hard to go in check out the templates that are built and modify those.. also editing the templates in Metasploit is not impossible in fact if you know some asm you probably can get metsrv.dll to be rather undetectable for a while at least .. if you want all the options of meterpreter.. although that might be a better option for after priv esc and knocking out defenses.

Great advice, also there's a couple of good crypters on here. Dunno if you'll get 0 detections with them though.

BestHackTools - August 22, 2019, 4:17 am

(Aug 20, 2019 12:53 AM)bexpr9 Wrote: [\[CITE\]](#) I know that bypassing AV programs is like a game of cat and mouse, so backdoors might start getting detected at some stage, then the developers release an update, this will allow us to generate undetectable backdoors, then AV programs release an update which will make backdoors detectable...

The problem is I have tried almost every payload in Veil Framework, Empire and Phantom Evasion but all of them are detected. Are there any tools that are working in 2019?

have you checked [UnknownCRYPTER v2.0 - JAVA CRYPTER::JS CRYPTER - AUTO-INSTALL JRE :: 100% FUD](#)

CyberStrike - August 23, 2019, 5:34 am

(Aug 21, 2019 05:25 PM)Nozorhan Wrote: [\[CITE\]](#) Great advice, also there's a couple of good crypters on here. Dunno if you'll get 0 detections with them though.

When you code your own though you can have code that is compiled with encryption, string obfuscation and anti-analysis or anti-vm all in one solution. It honestly works rather well.

equity - August 23, 2019, 5:40 am

(Aug 22, 2019 04:17 AM)BestHackTools Wrote: [\[CITE\]](#) have you checked [UnknownCRYPTER v2.0 - JAVA CRYPTER::JS CRYPTER - AUTO-INSTALL JRE :: 100% FUD](#)

Shameless promotion xD

Silkroad - August 24, 2019, 10:32 am

(Aug 23, 2019 05:34 AM)CyberStrike Wrote: [\[CITE\]](#) When you code your own though you can have code that is compiled with encryption, string obfuscation and anti-analysis or anti-vm all in one solution. It honestly works rather well.

True but with my experience, having high levels of obfuscation and encryption can some times mess with the stub's code. Depending on what your original stub is and how big it is, there's so much you can do.