Author:重剑无锋@Tide安全团队

Tide安全团队：

Tide安全团队致力于分享高质量原创文章，研究方向覆盖网络攻防、Web安全、移动终端、安全开发、IoT/物联网/工控安全等多个领域，对安全感兴趣的小伙伴可以关注或加入我们。

Tide安全团队自研开源多套安全平台，如Tide(潮汐)网络空间搜索平台、潮启移动端安全管控平台、分布式web扫描平台WDScanner、Mars网络威胁监测平台、潮汐指纹识别系统、潮巡自动化漏洞挖掘平台、工业互联网安全监测平台、漏洞知识库、代理资源池、字典权重库、内部培训系统等等。

Tide安全团队自建立之初持续向CNCERT、CNVD、漏洞盒子、补天、各大SRC等漏洞提交平台提交漏洞，在漏洞盒子先后组建的两支漏洞挖掘团队在全国300多个安全团队中均拥有排名前十的成绩。团队成员在FreeBuf、安全客、安全脉搏、t00ls、简书、CSDN、51CTO、CnBlogs等网站开设专栏或博客，研究安全技术、分享经验技能。

对安全感兴趣的小伙伴可以关注Tide安全团队Wiki：http://paper.TideSec.com 或团队公众号。

声明：文中所涉及的技术、思路和工具仅供以安全为目的的学习交流使用，任何人不得将其用于非法用途以及盈利等目的，否则后果自行承担！

文章打包下载及相关软件下载： `https://github.com/TideSec/BypassAntiVirus`

- 前言
- 文章概览
- 免杀能力一览
- 文章导航汇总
- 参考资料
- 完结

前言

本系列文章从2019年12月底开始，原计划就是用大约一个月时间把各种常见免杀工具分析一下，也就是现在的工具篇部分。后来在学习过程中发现使用C、C++、Go语言对shellcode进行人工编译处理免杀效果也不错，于是把这类单独拿出来写成了第二部分代码篇，涉及7种常见编程语言对shellcode的免杀处理。再之后，为了让免杀能更完善，又把白名单程序梳理了一便，通过这个过程对很多白名单程序的原理和使用也有了一定的理解。

因为额外加了很多内容，这也导致免杀系列文章絮絮叨叨写了68篇，也从2019年12月一直更新到2020年4月，在梳理白名单篇时因为当时春节后刚复工时间和精力都比较有限，Tide安全团队的小伙伴 `nuoyan` 、 `CSeroad` 、 `VllTomFord` 、 `雨夜RainyNight` 、 `zhangyida` 帮助写了一部分白名单程序， `雨夜RainyNight` 大佬还另外写了两篇免杀的实践文章，非常感谢小伙伴们的鼎力相助。

在免杀学习过程中也得到了很多大佬的指导，比如 `Green_m` 大佬、 `haya` 大佬，也参考了 `klion` 、 `shiying` 、 `-卿-` 等众大佬的博客，在此一并表示感谢。在整个免杀文章编写过程中生成了大约800多个远程样本、查阅了不下于几百篇文章，大部分链接我都放在了最后的参考资料，里面每一篇都比我写的这些要好很多。

本文只是把文章汇总一下方便查阅，没有实质技术内容，唯一有价值的可能就是最后的参考资料，这是免杀系列文章的源泉，大家可以收藏后多多揣摩。免杀系列文章虽然暂时告一段落，但后续还会有一些实战型的免杀技巧陆续更新，感兴趣的小伙伴可以多多交流。

文章概览

- **工具篇内容** 从专题2到专题25，共涉及21款较为常见的免杀工具。msf自免杀、Veil、Venom、Shellter、BackDoor-Factory、Avet、TheFatRat、Avoidz、Green-Hat-Suite、zirikatu、AVIator、DKMC、Unicorn、Python-Rootkit、DKMC、Unicorn、Python-Rootkit、ASWCrypter、nps_payload、GreatSCT、HERCULES、SpookFlare、SharpShooter、CACTUSTORCH、Winpayload等。

- **代码篇内容**：从专题26到专题33，涉及7种编程语言对shellcode的免杀处理。C/C++、C#、python、powershell、ruby、go等。

- **白名单内容**：从专题34到专题63，总计涉及113个白名单程序，包括Rundll32.exe、Msiexec.exe、MSBuild.exe、InstallUtil.exe、Mshta.exe、Regsvr32.exe、Cmstp.exe、CScript.exe、WScript.exe、Forfiles.exe、te.exe、Odbcconf.exe、InfDefaultInstall.exe、Diskshadow.exe、PsExec.exe、Msdeploy.exe、Winword.exe、Regasm.exe、Regsvcs.exe、Ftp.exe、pubprn.vbs、winrm.vbs、slmgr.vbs、Xwizard.exe、Compiler.exe、IEExec.exe、MavInject32、Presentationhost.exe、Wmic.exe、Pcalua.exe、Url.dll、zipfldr.dll、Syncappvpublishingserver.vbs等，在专题67中介绍了其他的80个不太常见的白名单程序。

免杀能力一览

1、表中标识 √ 说明相应杀毒软件未检测出病毒，也就是代表了Bypass。

2、为了更好的对比效果，大部分测试payload均使用msf的 `windows/meterperter/reverse_tcp` 模块生成。

3、由于本机测试时只是安装了360全家桶和火绒，所以默认情况下360和火绒杀毒情况指的是静态+动态查杀。360杀毒版本 `5.0.0.8160` (2020.01.01)，火绒版本 `5.0.34.16` (2020.01.01)，360安全卫士 `12.0.0.2002` (2020.01.01)。

4、其他杀软的检测指标是在 `virustotal.com` （简称VT）上在线查杀，所以可能只是代表了静态查杀能力，数据仅供参考，不足以作为杀软查杀能力或免杀能力的判断指标。

5、完全不必要苛求一种免杀技术能bypass所有杀软，这样的技术肯定是有的，只是没被公开，一旦公开第二天就能被杀了，其实我们只要能bypass目标主机上的杀软就足够了。

6、由于白名单程序加载payload的免杀测试需要杀软的行为检测才合理，静态查杀payload或者查杀白名单程序都没有任何意义，所以这里对白名单程序的免杀效果不做评判。

文章导航汇总

1.远控免杀专题(1)-基础篇：https://mp.weixin.qq.com/s/3LZ_cj2gDC1bQATxqBfweg

2.远控免杀专题(2)-msfvenom隐藏的参数：https://mp.weixin.qq.com/s/1r0iakLpnLrjCrOp2gT10w

3.远控免杀专题(3)-msf自带免杀(VT免杀率35/69)：https://mp.weixin.qq.com/s/A0CZslLhCLOK_HgkHGcpEA

4.远控免杀专题(4)-Evasion模块(VT免杀率12/71)：https://mp.weixin.qq.com/s/YnnCM7W20xScv52k_ubxYQ

5.远控免杀专题(5)-Veil免杀(VT免杀率23/71):https://mp.weixin.qq.com/s/-PHVIAQVyU8QIpHwcpN4yw

6.远控免杀专题(6)-Venom免杀(VT免杀率11/71):https://mp.weixin.qq.com/s/CbfxupSWEPB86tBZsmxNCQ

7.远控免杀专题(7)-Shellter免杀(VT免杀率7/69)：https://mp.weixin.qq.com/s/ASnldn6nk68D4bwkfYm3Gg

8.远控免杀专题(8)-BackDoor-Factory免杀(VT免杀率13/71)：https://mp.weixin.qq.com/s/A30JHhXhwe45xV7hv8jvVQ

9.远控免杀专题(9)-Avet免杀(VT免杀率14/71)：https://mp.weixin.qq.com/s/EIfqAbMC8HoC6xcZP9SXpA

10.远控免杀专题(10)-TheFatRat免杀(VT免杀率22/70)：https://mp.weixin.qq.com/s/zOvwfmEtbkpGWWBn642ICA

11.远控免杀专题(11)-Avoidz免杀(VT免杀率23/71)：https://mp.weixin.qq.com/s/TnfTXihlyv696uCiv3aWfg

12.远控免杀专题(12)-Green-Hat-Suite免杀(VT免杀率23/70)：https://mp.weixin.qq.com/s/MVJTXOIqjgL7iEHrnq6OJg

13.远控免杀专题(13)-zirikatu免杀(VT免杀率39/71)：https://mp.weixin.qq.com/s/5xLuu5UfF4cQbCq_6JeqyA

14.远控免杀专题(14)-AVIator免杀(VT免杀率25/69)：https://mp.weixin.qq.com/s/JYMq_qHvnsIVlqijHNny8Q

15.远控免杀专题(15)-DKMC免杀(VT免杀率8/55)：https://mp.weixin.qq.com/s/UZqOBQKEMcXtF5ZU7E55Fg

16.远控免杀专题(16)-Unicorn免杀(VT免杀率29/56)：https://mp.weixin.qq.com/s/y7P6bvHRFes854EAHAPOzw

17.远控免杀专题(17)-Python-Rootkit免杀(VT免杀率7/69)：https://mp.weixin.qq.com/s/OzO8hv0pTX54ex98k96tjQ

18.远控免杀专题(18)-ASWCrypter免杀(VT免杀率19/57)：https://mp.weixin.qq.com/s/tT1i55swRWIYiEdxEWElSQ

19.远控免杀专题(19)-nps_payload免杀(VT免杀率3/57)：https://mp.weixin.qq.com/s/XmSRgRUftMV3nmD1Gk0mvA

20.远控免杀专题(20)-GreatSCT免杀(VT免杀率14/56)：https://mp.weixin.qq.com/s/s9DFRIgpvpE-_MneO0B_FQ

21.远控免杀专题(21)-HERCULES免杀(VT免杀率29/70)：https://mp.weixin.qq.com/s/Rkr9lixzL4tiL89r10ndig

22.远控免杀专题(22)-SpookFlare免杀(VT免杀率16/67)：https://mp.weixin.qq.com/s/LfuQ2XuD7YHUWJqMRUmNVA

23.远控免杀专题(23)-SharpShooter免杀(VT免杀率22/57)：https://mp.weixin.qq.com/s/EyvGfWXLbxkHe7liaNFhGg

24.远控免杀专题(24)-CACTUSTORCH免杀(VT免杀率23/57)：https://mp.weixin.qq.com/s/g0CYvFMsrV7bHlfTnSUJBw

25.远控免杀专题(25)-Winpayloads免杀(VT免杀率18/70)：https://mp.weixin.qq.com/s/YTXT31mCOWhMZEbCg4Jt0w

26.远控免杀专题(26)-C、C++加载shellcode免杀(上)(VT免杀率9-70)：https://mp.weixin.qq.com/s/LftwV4bpuikDkIljuRw2LQ

27.远控免杀专题(27)-C、C++加载shellcode免杀(中)(VT免杀率8-70)：https://mp.weixin.qq.com/s/McVWP386q5in6cQ8hRxwdA

28.远控免杀专题(28)-C、C++加载shellcode免杀(下)(VT免杀率3-71)：https://mp.weixin.qq.com/s/Kw3-fdyHyiettYn44WNZQw

29.远控免杀专题(29)-C#加载shellcode免杀-5种方式(VT免杀率8-70)：https://mp.weixin.qq.com/s/Kvhfb13d2_D6m-Bu9Darog

30.远控免杀专题(30)-Python加载shellcode免杀-8种方式(VT免杀率10-69)：https://mp.weixin.qq.com/s/HyBSqrF_kl2ARaCYAMefgA

31.远控免杀专题(31)-powershell加载shellcode免杀-4种方式(VT免杀率5-58)：https://mp.weixin.qq.com/s/Tw-FAduHMVzek_YxIErQDQ

32.远控免杀专题(32)-Go加载shellcode免杀-3种方式(VT免杀率7-70)：https://mp.weixin.qq.com/s/TmfDQgRfEp2qg9SKbD0Quw

33.远控免杀专题(33)-Ruby加载shellcode免杀(VT免杀率0-58)：https://mp.weixin.qq.com/s/2eF6LklvdGetgbhYWdaFIg

34.远控免杀专题(34)-白名单MSBuild.exe执行payload(VT免杀率4-57)：https://mp.weixin.qq.com/s/1WEglPXm1Q5n6T-c4OhhXA

35.远控免杀专题(35)-白名单Msiexec.exe执行payload(VT免杀率27-60)：https://mp.weixin.qq.com/s/XPrBK1Yh5ggO-PeK85mqcg

36.远控免杀专题(36)-白名单InstallUtil.exe执行payload(VT免杀率3-68)：https://mp.weixin.qq.com/s/gN2p3ZHODZFia2761BVSzg

37.远控免杀专题(37)-白名单Mshta.exe执行payload(VT免杀率26-58)：https://mp.weixin.qq.com/s/oBr-syv2ef5IjeGFrs7sHg

38.远控免杀专题(38)-白名单Rundll32.exe执行payload(VT免杀率22-58)：https://mp.weixin.qq.com/s/rmC4AWC6HmcphozfEZhRGA

39.远控免杀专题(39)-白名单Regsvr32.exe执行payload(VT免杀率18-58)：https://mp.weixin.qq.com/s/6v8w2YZLxHJFnXb-IbnYAA

40.远控免杀专题(40)-白名单Cmstp.exe执行payload(VT查杀率为21-57)：https://mp.weixin.qq.com/s/tgtvOMDGlKFwdRQEnKJf5Q

41.远控免杀专题(41)-白名单Ftp.exe执行
payload：https://mp.weixin.qq.com/s/rnmCIx5oxA9z-0OfjoUAVw

42.远控免杀专题(42)-白名单Regasm.exe-Regsvcs.exe执行
payload：https://mp.weixin.qq.com/s/MCMjxPdUNdwV8is04AklLA

43.远控免杀专题(43)-白名单Compiler.exe执行
payload：https://mp.weixin.qq.com/s/Sm_3cJlSk6Pud1CLp-eAEQ

44.远控免杀专题(44)-白名单MavInject.exe执行
payload：https://mp.weixin.qq.com/s/dPOGj1VLhqwxJ0e-gOs8vA

45.远控免杀专题(45)-白名单presentationhost.exe执行
payload：https://mp.weixin.qq.com/s/r9l5Lh6MHv-Ece2DFr3EsA

46.远控免杀专题(46)-白名单IEexec.exe执行
payload：https://mp.weixin.qq.com/s/wVbFrU9cE3hCYAENjmnSUQ

47.远控免杀专题(47)-白名单winrm.vbs、slmgr.vbs执行
payload：https://mp.weixin.qq.com/s/B3oiMrEB98jtm4DvD2t2tQ

48.远控免杀专题(48)-白名单pubprn.vbs执行
payload：https://mp.weixin.qq.com/s/btiaVMBPxfxG4oXPa7__kw

49.远控免杀专题(49)-白名单Xwizard.exe执行
payload：https://mp.weixin.qq.com/s/8gaweOqkOrT77riaevvFUg

50.远控免杀专题(50)-白名单winword.exe执行
payload：https://mp.weixin.qq.com/s/qXWK5i2cDaletSzkAEzL3w

51.远控免杀专题(51)-白名单msdeloy.exe执行
payload：https://mp.weixin.qq.com/s/1oEzadXZxd3JukrBhNxxyw

52.远控免杀专题(52)-白名单psexec.exe执行
payload：https://mp.weixin.qq.com/s/JdOmlqif67GcSqZuuGPz0Q

53.远控免杀专题(53)-白名单WMIC.exe执行
payload：https://mp.weixin.qq.com/s/QNqM8Vdlu-SOP7ZqnRWY3w

54.远控免杀专题(54)-白名单SyncAppvPublishingServer.vbs执行
payload：https://mp.weixin.qq.com/s/Ud7TbeMJb8fsRlaGHWhBww

55.远控免杀专题(55)-白名单Pcalua.exe执行
payload：https://mp.weixin.qq.com/s/Aj9A5_LRS_uX8XN1rdUobQ

56.远控免杀专题(56)-白名单zipfldr.dll执行payload：https://mp.weixin.qq.com/s/-qPVenl_lk-ZnMA4j9XNRQ

57.远控免杀专题(57)-白名单Url.dll执行
payload：https://mp.weixin.qq.com/s/GzoYvfj7NkXe_nc8eOVEBQ

58.远控免杀专题(58)-白名单DiskShadow.exe执行
payload：https://mp.weixin.qq.com/s/pr0KYjk80YIk4qJO5h3Yaw

59.远控免杀专题(59)-白名单Odbcconf.exe执行
payload：https://mp.weixin.qq.com/s/uOwqbW0nkG776zZz6O_WFA

60.远控免杀专题(60)-白名单Forfiles.exe执行
payload：https://mp.weixin.qq.com/s/1-HyeNrd4IXQYsyG6dHQkw

61.远控免杀专题(61)-白名单Te.exe执行
payload：https://mp.weixin.qq.com/s/m37wm620qQ1xw4BN2hGOpg

62.远控免杀专题(62)-白名单CScript.exe-WScript.exe执行
payload：https://mp.weixin.qq.com/s/jzWHq7Yc1UjOwnXuIlAPKQ

63.远控免杀专题(63)-白名单InfDefaultInstall.exe执行
payload：https://mp.weixin.qq.com/s/mrtX4ayCXJJ1LPfBlSuvHw

64.远控免杀专题(64)-Msf自编译免杀补充：https://mp.weixin.qq.com/s/HsIqUKl7j1WJ4yyYzXdPZg

65.远控免杀专题(65)-shellcode免杀实践补充：https://mp.weixin.qq.com/s/J78CPtHJX5ouN6fxVxMFgg

66.远控免杀专题(66)-工具篇总结：https://mp.weixin.qq.com/s/WdErH1AOaI3B5Kptu7DK5Q

67.远控免杀专题(67)-白名单篇总结：https://mp.weixin.qq.com/s/2bC5otYgIgGnod-cXwkfqw

68.远控免杀专题(68)-Mimikatz免杀实践(上)：https://mp.weixin.qq.com/s/CiOaMnJBcEQfZXV_hopzLw

69.远控免杀专题(69)-Mimikatz免杀实践(下)：https://mp.weixin.qq.com/s/0p88rj-tWClLa_geKMkPgw

70.远控免杀专题(70)-终结篇：本文

参考资料

绕过应用程序白名单技巧：https://mp.weixin.qq.com/s/NGYhrK4dH-ikfdkIEA4nUQ

shellcode加载总结：https://uknowsec.cn/posts/notes/shellcode加载总结.html

多种白名单：https://www.cnblogs.com/backlion/category/1181220.html

后渗透详解: https://wh0ale.github.io/2019/01/23/2019-1-23-后渗透详解/

免杀方法集合：https://anhkgg.com/aanti-virus/

使用Meterpreter的多种姿势：https://wh0ale.github.io/2019/01/05/2019-1-4-使用Meterpreter的多种姿势/

Micro8:https://micro8.gitbook.io/micro8/

Windows上传并执行恶意代码的N种姿势:https://cloud.tencent.com/developer/article/1141143

https://github.com/api0cradle/UltimateAppLockerByPassList/

https://github.com/api0cradle/LOLBAS

https://www.shellterproject.com 杀毒软件绕过

https://github.com/trustedsec/unicorn py，一键生成多种后门

https://github.com/islamTaha12/Python-Rootkit windows 下 rootkit，反弹 meterpreter

https://github.com/n00py/Hwacha linux 下快速生成 metepreter 等多种 payload

https://github.com/Screetsec/Vegile msf 免杀，程序注入

https://github.com/MohamedNourTN/Terminator py2，msf 免杀

https://github.com/Veil-Framework/Veil msf 免杀

https://github.com/abedalqaderswedan1/aswcrypter py、bash，msf 免杀

https://github.com/Screetsec/TheFatRat java，msf 免杀，利用 searchsploit 快速搜索

https://github.com/pasahitz/zirikatu msf 免杀

https://github.com/govolution/avet msf 免杀

https://github.com/GreatSCT/GreatSCT msf 免杀

https://github.com/EgeBalci/HERCULES msf 免杀

https://github.com/trustedsec/nps_payload msf 免杀

https://github.com/4w4k3/Insanity-Framework py，payload 生成，过杀软，识别虚拟机，钓鱼，内存注入等

https://github.com/hlldz/SpookFlare Meterpreter，Empire，Koadic 等 loader/dropper 的生成器，可以绕过客户端检测和网络端检测的端点策略

https://github.com/pasahitz/regsvr32 使用 C#+Empire 实现最小体积免杀后门

https://github.com/malcomvetter/UnstoppableService 将自身安装为 Windows 服务且管理员无法停止/暂停服务的程序. C#编写

https://github.com/Cn33liz/StarFighters 基于 DotNetToJScript，利用 JavaScript 和 VBScript 执行 Empire Launcher

https://github.com/mdsecactivebreach/SharpShooter 基于 DotNetToJScript 使用 js、vbs，用于检索和执行任意 CSharp 源码的 payload 创建框架

https://github.com/mdsecactivebreach/CACTUSTORCH 基于 DotNetToJScript 使用 js、vbs 生成恶意 payload

https://github.com/OmerYa/Invisi-Shell 对 powershell 文件进行混淆

https://github.com/danielbohannon/Invoke-DOSfuscation 对 powershell 文件进行混淆，加密操作以及重新编码

https://github.com/danielbohannon/Invoke-Obfuscation 对 powershell 文件进行混淆，加密操作以及重新编码

https://github.com/Mr-Un1k0d3r/SCT-obfuscator Cobalt Strike SCT 有效载荷混淆器

https://github.com/tokyoneon/Armor bash，生成加密 Payload 在 macOS 上反弹 Shell

https://github.com/Mr-Un1k0d3r/MaliciousMacroGenerator 宏混淆，其中还包括 AV/Sandboxes 逃避机制

https://github.com/Kkevsterrr/backdoorme py3、py2 多种类型的后门、shell 生成工具，可以自动维持权限

https://github.com/TestingPens/MalwarePersistenceScripts win 下权限维持脚本

https://github.com/mhaskar/Linux-Root-Kit py，simple，linux 下 rootkit

https://github.com/PinkP4nther/Sutekh simple，rootkit，使普通用户获取 root shell

https://github.com/threatexpress/metatwin 从一个文件中提取元数据，包括数字签名，并注入到另一个文件中

https://github.com/Mr-Un1k0d3r/Windows-SignedBinary 可以修改二进制文件的 HASH，同时保留微软 windows 的签名

https://github.com/secretsquirrel/SigThief py，用于劫持合法的数字签名并绕过 Windows 的哈希验证机制的脚本工具

https://github.com/9aylas/Shortcut-Payload-Generator 快捷方式(.lnk)文件 Payload 生成器.AutoIt 编写

https://github.com/GuestGuri/Rootkit 反弹一个 tcp 连接，将进程 id 绑定到一个空文件夹

https://github.com/secretsquirrel/the-backdoor-factory 可以生成 win32PE 后门测试程序,ELF 文件后门程序等

https://github.com/islamadel/bat2exe 将 bat 文件转换为 exe 二进制文件

https://github.com/tywali/Bat2ExeConverter 将 bat 文件转换为 exe 二进制文件

https://github.com/Juntalis/win32-bat2exe 将 bat 文件转换为 exe 二进制文件
http://www.f2ko.de/downloads/Bat_To_Exe_Converter.zip 将 bat 文件转换为 exe 二进制文件，可以隐藏窗口。

https://github.com/r00t-3xp10it/trojanizer 将两个可执行文件打包为自解压文件，自解压文件在执行时会执行可执行文件

https://github.com/r00t-3xp10it/backdoorppt 将 payload 更换图标

https://github.com/r00t-3xp10it/FakeImageExploiter 将 payload 更换图标。需要 wine 与 resourcehacker 环境

https://github.com/DamonMohammadbagher/FakeFileMaker 更换图标和名称

https://github.com/peewpw/Invoke-PSImage 将 PS 脚本隐藏进 PNG 像素中并用一行指令去执行它

https://github.com/Mr-Un1k0d3r/DKMC Don't kill my cat 生成混淆的 shellcode，将 shellcode 存储在多语言图像中

https://github.com/deepzec/Bad-Pdf 生成一个 pdf 文件，内含 payload 来窃取 win 上的 Net-NTLM 哈希

https://github.com/3gstudent/Worse-PDF 向 PDF 文件中插入恶意代码，来窃取 win 上的 Net-NTLM 哈希

https://github.com/TideSec/BypassAntiVirus //远控免杀系列

https://github.com/Veil-Framework/Veil //PY.Msf免杀。1.5K。

https://github.com/Screetsec/TheFatRat //JAVA.msf免杀，利用searchsploit快速搜索

https://github.com/Screetsec/Vegile //SHELL/C.msf免杀，程序注入

https://github.com/MohamedNourTN/Terminator //PY2.msf免杀

https://github.com/abedalqaderswedan1/aswcrypter //py,bash.msf免杀

https://github.com/pasahitz/zirikatu //msf免杀

https://github.com/govolution/avet //msf免杀

https://github.com/GreatSCT/GreatSCT //msf免杀

https://github.com/EgeBalci/HERCULES //msf免杀

https://github.com/trustedsec/nps_payload //msf免杀

https://github.com/hlldz/SpookFlare //PY.客户端与网络端策略绕过，msf/empire/koadic生成加载混淆免杀。goodjob。

https://github.com/n00py/Hwacha //linux下快速生成metepreter等多种payload

https://github.com/4w4k3/Insanity-Framework //PY.生成免杀payload，识别虚拟机，钓鱼，内存注入等

https://github.com/trustedsec/unicorn //PY.一键生成多种后门

https://github.com/Kkevsterrr/backdoorme //py3、py2。多种类型的后门、shell生成工具，可以自动维持权限

https://github.com/pasahitz/regsvr32 //C#.使用C#+Empire实现最小体积免杀后门

https://github.com/Cn33liz/StarFighters //基于DotNetToJScript，利用JavaScript和VBScript执行Empire Launcher

https://github.com/mdsecactivebreach/SharpShooter //基于DotNetToJScript使用js、vbs，用于检索和执行任意CSharp源码的payload创建框架

https://github.com/mdsecactivebreach/CACTUSTORCH //基于DotNetToJScript使用js、vbs生成恶意payload

https://github.com/OmerYa/Invisi-Shell //对powershell文件进行混淆

https://github.com/danielbohannon/Invoke-DOSfuscation //对powershell文件进行混淆，加密操作以及重新编码

https://github.com/danielbohannon/Invoke-Obfuscation //对powershell文件进行混淆，加密操作以及重新编码

https://github.com/Mr-Un1k0d3r/MaliciousMacroGenerator //VBA.宏混淆，其中还包括AV/Sandboxes逃避机制

https://github.com/9aylas/Shortcut-Payload-Generator 快捷方式(.lnk)文件Payload生成器.AutoIt编写

Composite Moniker：CVE-2017-8570 PoC。https://github.com/rxwx/CVE-2017-8570

Exploit toolkit CVE-2017-8759：一个方便的python脚本，它为测试者和安全研究人员提供了一种快速有效的方式来测试Microsoft .NET Framework RCE。https://github.com/bhdresh/CVE-2017-8759

CVE-2017-11882 Exploit：最多接受超过17k字节长度的命令/代码。https://github.com/unamer/CVE-2017-11882

Adobe Flash Exploit：CVE-2018-4878。https://github.com/anbai-inc/CVE-2018-4878

Exploit toolkit CVE-2017-0199：一个方便的python脚本，它为测试人员和安全研究人员提供了一种快速有效的方式来测试Microsoft Office RCE。https://github.com/bhdresh/CVE-2017-0199

demiguise：HTA加密工具。https://github.com/nccgroup/demiguise

Office-DDE-Payloads：收集脚本和模板以生成嵌入DDE的Office文档，无宏命令执行技术。https://github.com/0xdeadbeefJERKY/Office-DDE-Payloads

CACTUSTORCH：是一个生成payload的框架,可用于基于James Forshaw的DotNetToJScript工具的攻防对抗。https://github.com/mdsecactivebreach/CACTUSTORCH

SharpShooter：用于检索和执行任意CSharp源码的payload创建框架。https://github.com/mdsecactivebreach/SharpShooter

Don’t kill my cat：用于生成被存储在polyglot图像中的混淆shellcode。https://github.com/Mr-Un1k0d3r/DKMC

Malicious Macro Generator Utility：生成混淆宏，其中还包括AV/Sandboxes逃避机制。https://github.com/Mr-Un1k0d3r/MaliciousMacroGenerator

SCT Obfuscator：Cobalt Strike SCT有效载荷混淆器。https://github.com/Mr-Un1k0d3r/SCT-obfuscator

Invoke-Obfuscation：PowerShell混淆器。https://github.com/danielbohannon/Invoke-Obfuscation

Invoke-DOSfuscation：powershell混淆编码框架。https://github.com/danielbohannon/Invoke-DOSfuscation

Unicorn：使用PowerShell降级攻击并将shellcode直接注入内存的工具。https://github.com/trustedsec/unicorn

Shellter：一个动态的shellcode注入工具，也是有史以来第一个真正动态的PE注入工具。https://www.shellterproject.com/

SigThief：是一个由python编写的,可以用于劫持合法的数字签名并绕过Windows的哈希验证机制的脚本工具。https://github.com/secretsquirrel/SigThief

Veil：用于生成绕过常用AV的metasploit有效载荷的工具。https://github.com/Veil-Framework/Veil

CheckPlease：用PowerShell，Python，Go，Ruby，C，C＃，Perl和Rust编写的CheckPlease Sandbox evasion模块。https://github.com/Arvanaghi/CheckPlease

Invoke-PSImage：将目标PS脚本嵌入到一个PNG图片文件的像素点中，并允许我们使用一行指令来执行该脚本。https://github.com/peewpw/Invoke-PSImage

LuckyStrike：基于PowerShell的实用程序，用于创建恶意的Office宏文档。仅用于渗透测试或教育目的。https://github.com/curi0usJack/luckystrike

ClickOnceGenerator：适用于红队的快速恶意ClickOnce生成器。https://github.com/Mr-Un1k0d3r/ClickOnceGenerator

macro_pack：一个用于自动生成混淆过的MS Office文档、VB脚本等其他格式的工具,其主要目的是用于渗透测试、demo以及社会工程学的评估。https://github.com/sevagas/macro_pack

StarFighters：基于JavaScript和VBScript的Empire启动器。https://github.com/Cn33liz/StarFighters

nps_payload：专为逃避入侵检测而生成Payload的工具。https://github.com/trustedsec/nps_payload

SocialEngineering：负责收集用于证书盗窃和鱼叉式网络钓鱼攻击的社交工程技巧和payloads。https://github.com/bhdresh/SocialEngineeringPayloads

Social-Engineer Toolkit：一款专为社交工程设计的开源渗透测试框架。https://github.com/trustedsec/social-engineer-toolkit

Phishery：一个支持SSL简单的HTTP服务器。https://github.com/ryhanson/phishery

PowerShdll：使用rundll32运行PowerShell。绕过软件限制。https://github.com/p3nt4/PowerShdll

Ultimate AppLocker ByPass List：常用AppLocker绕过技术存储库。https://github.com/api0cradle/UltimateAppLockerByPassList

Ruler：是一款能够通过MAPI/HTTP协议与Exchange服务器交互的工具。https://github.com/sensepost/ruler

Generate-Macro：一个独立的PowerShell脚本，它将生成具有指定有效负载和持久性方法的恶意Microsoft Office文档。https://github.com/enigma0x3/Generate-Macro

Malicious Macro MSBuild Generator：生成恶意宏并通过MSBuild应用程序白名单绕过执行Powershell或Shellcode。https://github.com/infosecn1nja/MaliciousMacroMSBuild

Meta Twin：一个文件资源克隆器。从一个文件中提取元数据，包括数字签名，并注入到另一个文件中。https://github.com/threatexpress/metatwin

WePWNise：生成独立于体系结构的VBA代码，用于Office文档或模板，并自动绕过应用程序控制。https://github.com/mwrlabs/wePWNise

DotNetToJScript：能够利用JS/Vbs脚本加载.Net程序的工具。https://github.com/tyranid/DotNetToJScript

PSAmsi：一个审计和攻击 AMSI 签名的工具。https://github.com/cobbr/PSAmsi

Reflective DLL injection：是一种库注入技术，让DLL自身不使用LoadLibraryA函数,将自身映射到目标进程内存中。https://github.com/stephenfewer/ReflectiveDLLInjection

ps1encode：用于生成和编码基于powershell的metasploit有效载荷。https://github.com/CroweCybersecurity/ps1encode

Worse PDF：将一个普通的PDF文件变成恶意文件。用于从Windows机器上窃取Net-NTLM哈希。https://github.com/3gstudent/Worse-PDF

SpookFlare：一款可帮助你有机会绕过各种安全措施的工具，例如客户端检测和网络端检测的端点策略。SpookFlare还是Meterpreter，Empire，Koadic等的loader/dropper生成器。https://github.com/hlldz/SpookFlare

GreatEST：是一个生成应用程序白名单绕过的开源项目。此工具适用于红蓝对抗。https://github.com/GreatSCT/GreatSCT

nps：运行没有PowerShell的PowerShell。https://github.com/Ben0xA/nps

Meterpreter_Paranoid_Mode.sh：一个可以创建SSL/TLS shell连接的脚本。https://github.com/r00t-3xp10it/Meterpreter_Paranoid_Mode-SSL

The Backdoor Factory：一款安全测试工具,可以轻松的生成win32PE后门测试程序,ELF文件后门程序等。https://github.com/secretsquirrel/the-backdoor-factory

MacroShop：一组脚本，通过Office宏传递有效载荷。https://github.com/khr0x40sh/MacroShop

UnmanagedPowerShell：可以从一个非托管程序来执行PowerShell , 经过一些修改后也可以被用来注入到其他进程。https://github.com/leechristensen/UnmanagedPowerShell

完结

我是`Tide安全团队`的重剑无锋，对远程免杀、安全开发、红蓝对抗感兴趣的小伙伴可以一起多交流，我的wx：`base64_decode(UmVsYXhfdmlw)`。

完结撒花~！Bye!