

剑指 工控主机安全防护 的脆弱性

文档仅限技术交流，切勿商用，违者必究

演讲者简介

ID: 一谷米粒

公司: 赛博网安

Team: 暗影安全

履历: 2018~2019年协助举办多场CTF竞赛。

2019年CSDN论坛二进制安全讲师。

2020年特聘看雪二进制安全讲师。

2021~2022年二进制漏洞挖掘至今3个CVE,若干CNVD。

暗影安全

shadowsec.org

暗刃实验室



以安全研究，先进安全技术研究为主要方向，包含应用软件漏洞挖掘、嵌入式系统漏洞挖掘、操作系统漏洞挖掘、web应用漏洞挖掘、物联网协议分析、工业系统漏洞挖掘、自动化安全检测技术、智能安全攻击源定位技术、网络攻击效能评估研究等。

影刃实验室



专注研究ATT@CK攻击模型，拥有包括但不限于ATT@CK的攻击路径复原技术，使用战争战术级攻击思维，进行安全实景渗透，以实景渗透作为蓝本，通过攻防技术培训，提升企业安全团队的攻防技术能力，建立高素质的实战团队。

议题简介

没有网络安全就没有国家安全——习近平

工业基础设施安全关系民生、教育、金融、军工等多个领域。工业战争所产生的破坏性是巨大的，本次议题针对工业当中，体量巨大的工控主机安全防护手段进行深入分析，选择一款在国内工控主机安全防护当中，应用广泛的防护软件进行实战分析。

议题简介

2022年4月8日 16:10:00

Sandworm攻击乌克兰高压变电站。

文档仅限技术交流，切勿商用，违者必究







CONTENTS



软件功能介绍

知己知彼，百战不殆。针对软件的功能做一个简单的了解。



猜想

通过了解软件，对软件的脆弱点做出一些猜想。



详细分析

在逆向分析的过程中来验证猜想。



CONTENTS



软件功能介绍

知己知彼，百战不殆。针对软件的功能做一个简单的了解。



猜想

通过了解软件，对软件的脆弱点做出一些猜想。



详细分析

在逆向分析的过程中来验证猜想。

文档仅限技术交流，切勿商用，违者必究

身份访问控制


固化


设置


主机加固


报警


用户管理

新建

删除

修改密码

重置密码

序号	用户名	类型	内置用户
1	SuperAdmin	超级管理员	是
2	Admin	管理员	是
3	Audit	审计员	是

文档仅限技术交流，切勿商用，违者必究

9

软件目录

名称	修改日期	类型	大小
skin	2021/7/21 10:55	文件夹	
x64	2021/7/21 10:55	文件夹	
 .lcs	2021/7/21 10:55	LCS 文件	1 KB
 config.dat	2021/7/21 10:55	DAT 文件	1 KB
 DuiLib_u.dll	2019/12/21 15:36	应用程序扩展	582 KB
 GdiPlus.dll	2019/6/24 10:55	应用程序扩展	1,668 KB
 Launcher.exe	2020/8/29 17:47	应用程序	376 KB
 ObCtrl.dll	2020/8/29 17:47	应用程序扩展	167 KB
 SAudit.exe	2020/8/29 17:47	应用程序	1,977 KB
 SDBCtrl.dll	2020/8/29 17:47	应用程序扩展	319 KB
 SHostSec.dll	2020/8/29 17:47	应用程序扩展	239 KB
 SLog.db	2021/7/21 10:55	Data Base File	16 KB
 SMain.exe	2020/8/29 17:47	应用程序	2,438 KB
 Solidify.exe	2020/8/29 17:47	应用程序	2,104 KB
 sqlite3.dll	2020/3/14 17:19	应用程序扩展	600 KB
 SUser.db	2021/7/21 10:57	Data Base File	8 KB

软件目录

```
config.dat - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

[component]
count=5
com1=SCProcess.dll
com2=SCUDisk.dll
com3=SCData.dll
com4=SCHostSec.dll
com5=SCConfig.dll
[SETTING]
CSIDL_DESKTOPDIRECTORY=C:\Users\YGML_WIN7\Desktop
CSIDL_PROGRAMS=C:\Users\YGML_WIN7\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
[server]
UserSid=
```

文档仅限技术交流，切勿商用，违者必究

LCS文件

0000h:	B0 6F 09 7B 1D E3 36 F4 0F 2D 18 07 92 77 A3 D2	°o.{.ã6ô.-...'w£Ô
0010h:	53 6F 92 FB E4 B1 0F 50 A7 AF A4 D0 D5 C1 E4 31	So'ûä±.PS¬¤ĐŌÄä1
0020h:	4D 37 DD BD 48 5B 7E D2 0F 34 73 E4 74 07 1A B5	M7Ý¾H[~ò.4sät..µ
0030h:	06 A2 37 C9 55 1E 59 56 77 B9 83 91 D1 34 62 CC	.¢7ÉU.YVw²f'Ñ4bİ
0040h:	95 9F 1D 76 F2 2F 8D 60 B2 3C 2D 90 8F B3 C9 97	•Ÿ.vò/.`²<-...³É-
0050h:		

软件目录

名称	修改日期	类型	大小
skin	2021/7/21 10:55	文件夹	
x64	2021/7/21 10:55	文件夹	
.lcs	2021/7/21 10:55	LCS 文件	1 KB
config.dat	2021/7/21 10:55	DAT 文件	1 KB
DuiLib_u.dll	2019/12/21 15:36	应用程序扩展	582 KB
GdiPlus.dll	2019/6/24 10:55	应用程序扩展	1,668 KB
Launcher.exe	2020/8/29 17:47	应用程序	276 KB
ObCtrl.dll	2020/8/29 17:47	应用程序扩展	157 KB
SAudit.exe	2020/8/29 17:47	应用程序	1,977 KB
SDBCtrl.dll	2020/8/29 17:47	应用程序扩展	319 KB
SHostSec.dll	2020/8/29 17:47	应用程序扩展	239 KB
SLog.db	2021/7/21 10:55	Data Base File	16 KB
SMain.exe	2020/8/29 17:47	应用程序	2,438 KB
Solidify.exe	2020/8/29 17:47	应用程序	2,104 KB
sqlite3.dll	2020/3/14 17:19	应用程序扩展	600 KB
SUser.db	2021/7/21 10:57	Data Base File	8 KB

名称	修改日期	类型
version.ini	2020/8/29 17:47	配置设置

version.ini - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
[[SETTING]
KEY= .lcs
1=2.0.3.46
2=
3=版权所有 (C) 2020 .
4=http://
5=主机卫士
6=版本信息: V2.0

软件目录

名称	修改日期	类型	大小
 ObCtrl.dll	2020/8/29 17:47	应用程序扩展	195 KB
 SCConfig.dll	2020/8/29 17:47	应用程序扩展	810 KB
 SCData.dll	2020/8/29 17:47	应用程序扩展	876 KB
 SCHostSec.dll	2020/8/29 17:47	应用程序扩展	394 KB
 SCProcess.dll	2020/8/29 17:47	应用程序扩展	557 KB
 SCUDisk.dll	2020/8/29 17:47	应用程序扩展	325 KB
 SDBCtrl.dll	2020/8/29 17:47	应用程序扩展	377 KB
 SHostSec.dll	2020/8/29 17:47	应用程序扩展	281 KB
 SNetComm.dll	2020/8/29 17:47	应用程序扩展	2,000 KB
 SolidifySrv.exe	2020/8/29 17:47	应用程序	672 KB
 sqlite3.dll	2020/3/14 17:19	应用程序扩展	830 KB
 UnInstall.exe	2020/8/29 17:47	应用程序	837 KB

软件目录

名称	修改日期	类型	大小
ObCtrl.dll	2020/8/29 17:47	应用程序扩展	195 KB
SCConfig.dll	2020/8/29 17:47	应用程序扩展	819 KB
SCData.dll	2020/8/29 17:47	应用程序扩展	376 KB
SCHostSec.dll	2020/8/29 17:47	应用程序扩展	394 KB
SCProcess.dll	2020/8/29 17:47	应用程序扩展	557 KB
SCUDisk.dll	2020/8/29 17:47	应用程序扩展	325 KB
SDBCtrl.dll	2020/8/29 17:47	应用程序扩展	377 KB
SHostSec.dll	2020/8/29 17:47	应用程序扩展	281 KB
SNetComm.dll	2020/8/29 17:47	应用程序扩展	2,000 KB
SolidifySrv.exe	2020/8/29 17:47	应用程序	672 KB
sqlite3.dll	2020/3/14 17:19	应用程序扩展	830 KB
UnInstall.exe	2020/8/29 17:47	应用程序	837 KB

身份验证

用户名: SuperAdmin

密码:

验证取消



CONTENTS



软件功能介绍

知己知彼，百战不殆，针对软件的功能做一个简单的了解。



猜想

通过了解软件，对软件的脆弱点做出一些猜想。



详细分析

在逆向分析的过程中来验证猜想。

文档仅限技术交流

切勿商用，违者必究

猜想

1.绕过白名单进程防护

2.运行软件获取数据库信息

3.绕过身份验证

4.卸载安全防护

文档仅限技术交流，切勿商用，违者必究



CONTENTS



软件功能介绍

知己知彼，百战不殆。针对软件的功能做一个简单的了解。



猜想

通过了解软件，对软件的脆弱点做出一些猜想。




详细分析

在逆向分析的过程中来验证猜想。

文档仅限技术交流，切勿商用，违者必究



CONTENTS



安装软件

需要注册码验证。



二进制文件分析

分析文件结构找到文件脆弱点。



推演及验证

验证分析结果。



Show!

视频展示。

文档仅限技术交流，切勿商用！违者必究

CONTENTS

安装软件

需要注册码验证。

二进制文件分析

分析文件结构找到文件脆弱点。

推演及验证

验证分析结果。

Show!

视频展示。

文档仅限技术交流，切勿商用！违者必究

安装软件

安装向导

软件注册

请将申请码发给软件厂商以获取注册码，请妥善保管申请码和注册码以备再次安装时使用。

申请码：

注册码：

AA1Aa

< 上一步 (B)

注册

取消

安装软件

定位程序关键点方法:

1.通过API定位

2.通过消息断点定位

3.通过内存读取断点定位

文档仅限技术交流，切勿商用，违者必究

安装软件

IP	Address	Disassembly
●	00446910	55
●	00446911	8BEC
●	00446913	6A FF
●	00446915	68 4B4D4800
●	0044691A	64:A1 00000000
●	00446920	50
●	00446921	83EC 70
●	00446924	A1 F09E4A00
●	00446929	33C5
●	0044692B	8945 E8
●	0044692E	50
●	0044692F	8D45 F4
●	00446932	64:A3 00000000
●	00446938	894D 8C
●	0044693B	C745 F0 FFFFFFFF
●	00446942	8B4D 8C
●	00446945	81C1 94000000
●	0044694B	E8 70F1FFFF
●	00446950	8945 EC
●	00446953	837D EC 00
●	00446957	75 29
●	00446959	68 39D64800
●	0044695E	68 8DD1FDFF
●	00446963	83C4 04
●	00446966	50
●	00446967	68 40D64800
●	0044696C	E8 7FD1FDFF
●	00446971	83C4 04
●	00446974	50
●	00446975	8B4D 8C
●	00446978	E8 13FFFFFF
●	0044697D	✓ E9 FB010000
●	00446982	837D EC 1D
●	00446986	✓ 74 29

Assembly
push ebp
mov ebp,esp
push FFFFFFFF
push setup.484D48
mov eax,dword ptr fs:[0]
push eax
sub esp,70
mov eax,dword ptr ds:[4A9EF0]
xor eax,ebp
mov dword ptr ss:[ebp-18],eax
push eax
lea eax,dword ptr ss:[ebp-c]
mov dword ptr fs:[0],eax
mov dword ptr ss:[ebp-74],ecx
mov dword ptr ss:[ebp-10],FFFFFFFF
mov ecx,dword ptr ss:[ebp-74]
add ecx,94
call <setup.My_GetWindowText>
mov dword ptr ss:[ebp-14],eax
cmp dword ptr ss:[ebp-14],0
jne setup.446982
push setup.48D634
call setup.423AF0
add esp,4
push eax
push setup.48D640
call setup.423AF0
add esp,4
push eax
mov ecx,dword ptr ss:[ebp-74]
call setup.446890
jmp setup.44687D
cmp dword ptr ss:[ebp-14],1D
je setup.446981

安装软件

```
v23 = sub_42E060(v15, &String);           // 返回0为正确
memset(&String, 0, 0x3Cu);
if ( v23 )
{
    v19 = dword_4AC4E4;
    v20 = dword_4AC4E4;
    if ( dword_4AC4E4 )
        sub_446D30(1);
    dword_4AC4E4 = 0;
    if ( v23 == 1 )
    {
        v6 = (const WCHAR *)sub_423AF0(L"1000");
        v7 = (const WCHAR *)sub_423AF0(L"1134"); // 安装失败
        sub_446890(v7, v6);
    }
    else if ( v23 == 2 )
    {
        v8 = (const WCHAR *)sub_423AF0(L"1000");
        v9 = (const WCHAR *)sub_423AF0(L"1135"); // 安装失败
        sub_446890(v9, v8);
    }
}
```


安装软件

```
1 int __thiscall sub_42E060(void *this, wchar_t *My_input)
2 {
3     HMODULE v2; // eax@2
4     int v4; // [sp+4h] [bp-24h]@2
5     void *v5; // [sp+8h] [bp-20h]@1
6     void *v6; // [sp+10h] [bp-18h]@1
7     signed int v7; // [sp+18h] [bp-10h]@1
8
9     v5 = this;
10    v7 = -1;
11    v6 = operator new(0x170u);
12    if ( v6 )
13    {
14        v2 = GetModuleHandleW(0);
15        v4 = sub_402A70((int)v6, (int)v2, 14);
16    }
17    else
18    {
19        v4 = 0;
20    }
21    *(_DWORD *)v5 = v4;
22    if ( !sub_402F40(*(_DWORD *)v5) )
23    {
24        sub_4038A0(*(_DWORD *)v5); // 反调试函数
25        *((_DWORD *)v5 + 1) = unknown_libname_160(0xDu);
26        memset(*(_DWORD **)v5 + 1, 0, 0xDu);
27        sub_42D184(*((char **)v5 + 1), 13);
28        if ( sub_42DED0(v5, My_input) ) // 关键算法函数
29        {
30            if ( sub_42E190((int)v5) ) // 进一步对算法进行验证
31                v7 = 0; // 返回0成功安装
32            else
33                v7 = 2;
34        }
35        else
36        {
37            v7 = 1; // 返回1 注册码格式错误
38        }
39    }
40    return v7;
41 }
```


安装软件

反调试方法：

1.使用系统API

2.系统检测

3.调试器断点检测

文档仅限技术交流，切勿商用，违者必究

安装软件

1.使用系统API:

IsDebuggerPresent

IsDebuggerPresent 查询进程环境块(PEB)中的IsDebugged标志。

CheckRemoteDebuggerPresent

CheckRemoteDebuggerPresent 通过传递自己的进程句柄来判断自己是否被调试

3.调试器断点检测:

a.软件断点

在自己的代码中查找机器码0xCC。

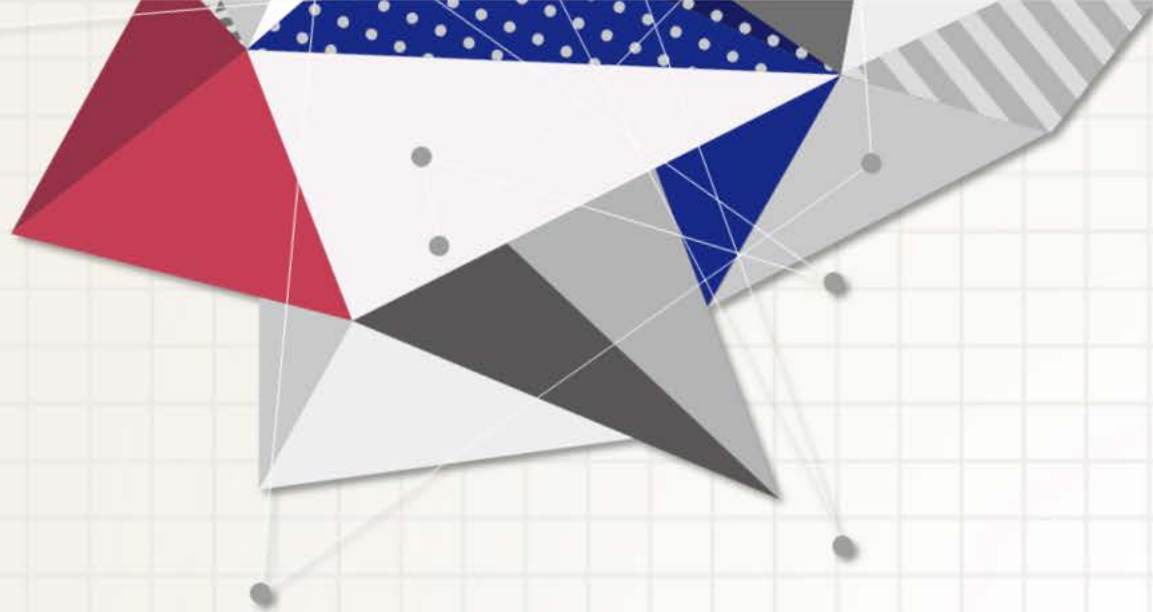
b.硬件断点

DR0、 DR1、 DR2、 DR3这四个寄存器值是否为0。

文档仅限技术交流，切勿商用，违者必究

二进制文件分析

```
do
{
    if ( !v10 )
        break;
    v9 = *(_WORD *)v11 == 0;
    v11 += 2;
    --v10;
}
while ( !v9 );
sub_7FEF45079F0(&v20, my_username, -v10 - 2);
result = sub_7FEF44F6760(a1 + 8, &v20, &v16); // 返回0验证失败, 返回1验证成功
if ( !(_DWORD)result )
{
    Sleep(0x1F4u);
    v19 = 7i64;
    v18 = 0i64;
    v17 = 0;
    v12 = -1i64;
    v13 = input_password;
```

CONTENTS

漏洞挖掘过程

安装软件

需要注册码验证。

二进制文件分析

分析文件结构找到文件脆弱点。

推演及验证

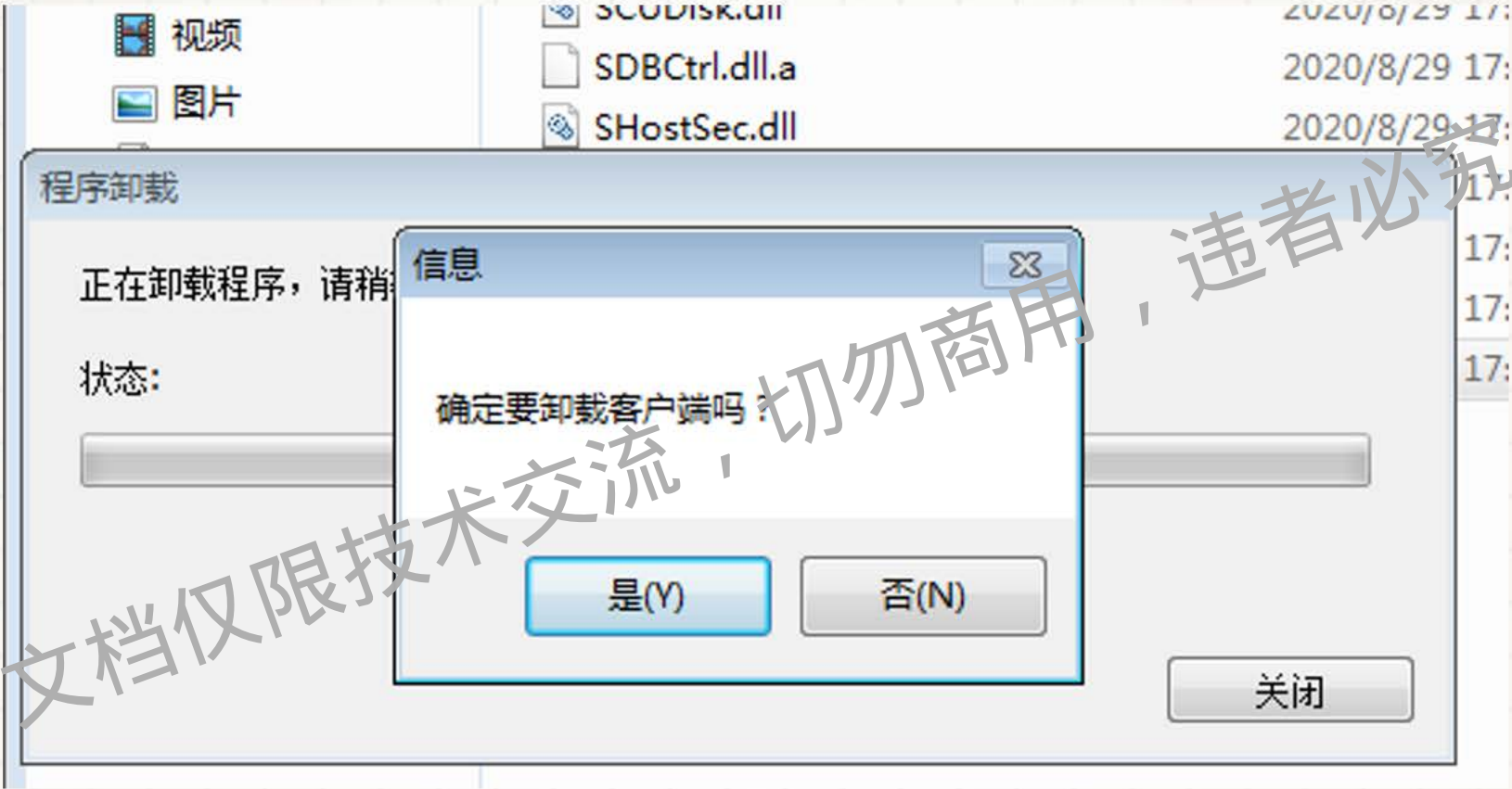
验证分析结果。

Show!

视频展示。


文档仅限技术交流，切勿商用！违者必究

二进制文件分析





CONTENTS



安装软件

需要注册码验证。



二进制文件分析

分析文件结构找到文件脆弱点。



推演及验证

验证分析结果。

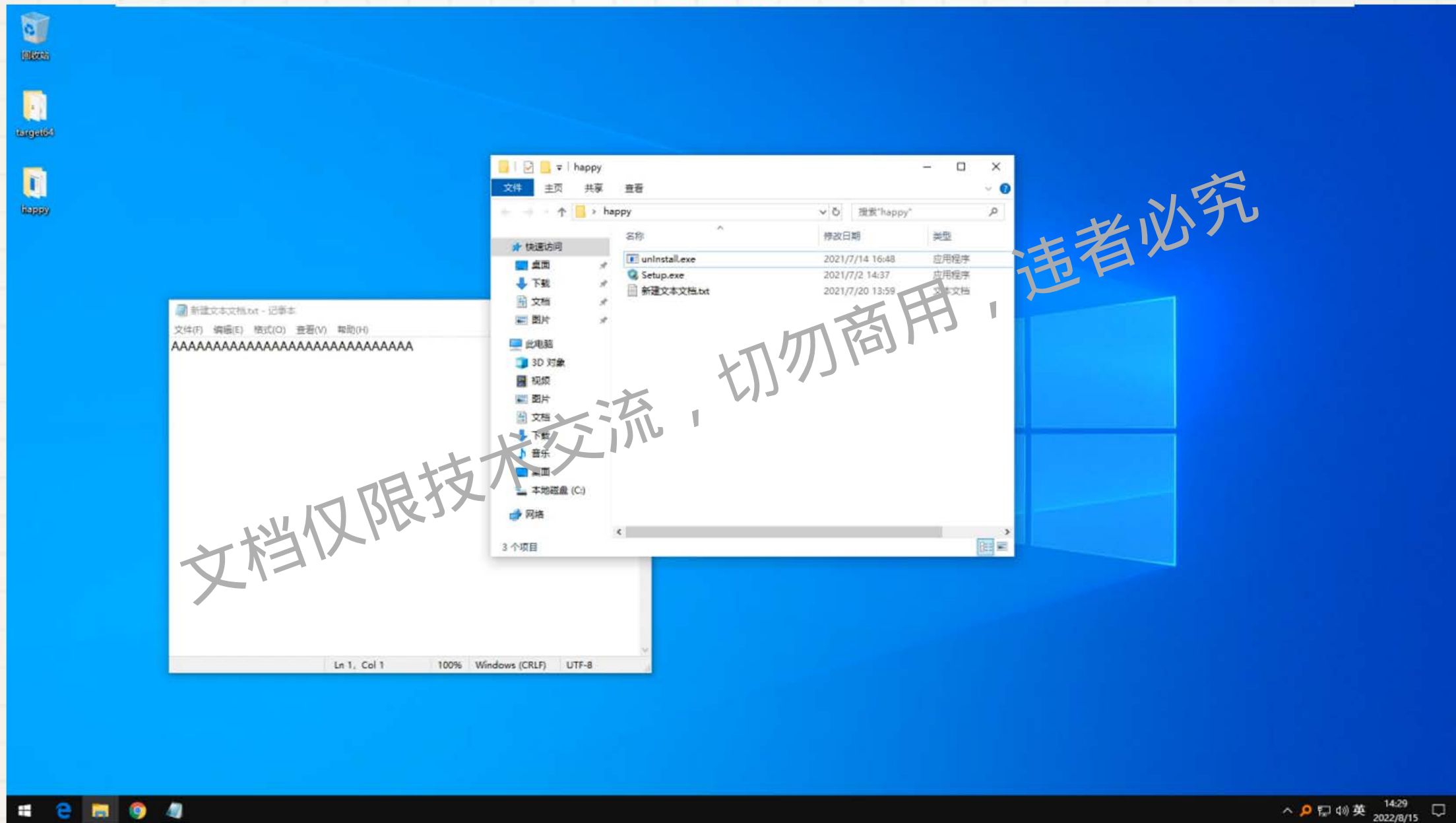


Show!

视频展示。

文档仅限技术交流，切勿商用！违者必究

Show!





THANKS FOR YOUR ATTENTION

● 暗影安全

● 一谷米粒