soxy

Une suite de services pour Citrix, VMware Horizon et Windows RDP

Arnaud FONTAINE, Nicolas DEVILLERS, Jean-Romain GARNIER

SSTIC 2025

AIRBUS

Situation

Nous devons effectuer un **test d'intrusion** (par ex., un accès fournisseur au SI de l'entreprise).

Nous avons accès à une machine **uniquement via une interface de bureau virtuel** (VDI).

Toutes les **fonctionnalités de "partage" sont désactivées** (par ex., presse-papiers).

Accès via *Remote Desktop Protocol (RDP)*

- Transport de l'affichage de la VM + entrées du client (par ex., clavier, souris)
- Authentification + trafic chiffré + session unique ou sessions multiples
- Fonctionnalités avancées via les **canaux virtuels**

Solutions VDI

VMware Horizon, Citrix, XenApp, XenDesktop, . . .

- S'appuient sur l'**implémentation de RDP nativement présente** dans Windows. . .
- . . . mais avec des variations qui nécessitent des **clients RDP spécifiques**
- **Canaux virtuels propriétaires** pour les fonctionnalités supplémentaires :

  partage du presse-papiers, système de fichiers "exposé" dans la VM, périphérique USB déporté dans la VM, . . .

Ces fonctionnalités supplémentaires sont configurées côté VM

- Un utilisateur standard ne peut pas les activer/autoriser ☹

Solutions VDI

VMware Horizon, Citrix, XenApp, XenDesktop, . . .

- S'appuient sur l'**implémentation de RDP nativement présente** dans Windows. . .
- . . . mais avec des variations qui nécessitent des **clients RDP spécifiques**
- **Canaux virtuels propriétaires** pour les fonctionnalités supplémentaires :

  partage du presse-papiers, système de fichiers "exposé" dans la VM, périphérique USB déporté dans la VM, . . .

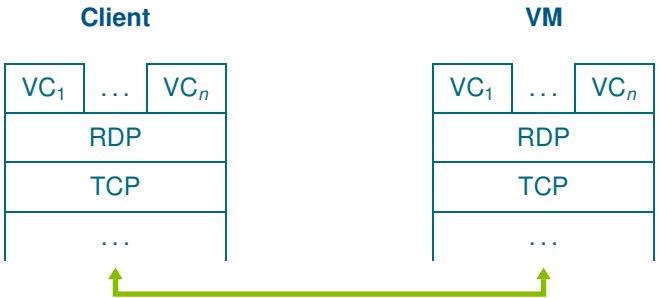
Ces fonctionnalités supplémentaires sont configurées côté VM

- Un utilisateur standard ne peut pas les activer/autoriser ☹
- **Un utilisateur standard peut créer et utiliser d'autres canaux virtuels** 😀

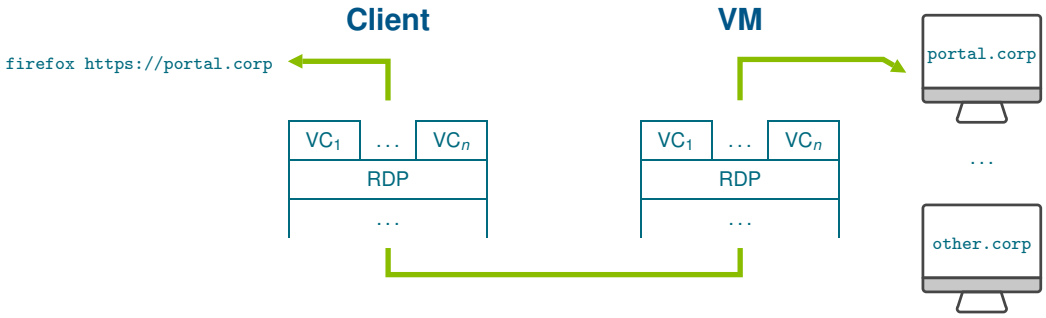
Canaux virtuels

Qu'est-ce qu'un canal virtuel (*Virtual Channel*) ?

- **Un canal de transport de données dans RDP**
- Sans perte + ordre des paquets préservé
- Chaque canal est identifié par un nom (ASCII) sur 8 octets



Idée/principe

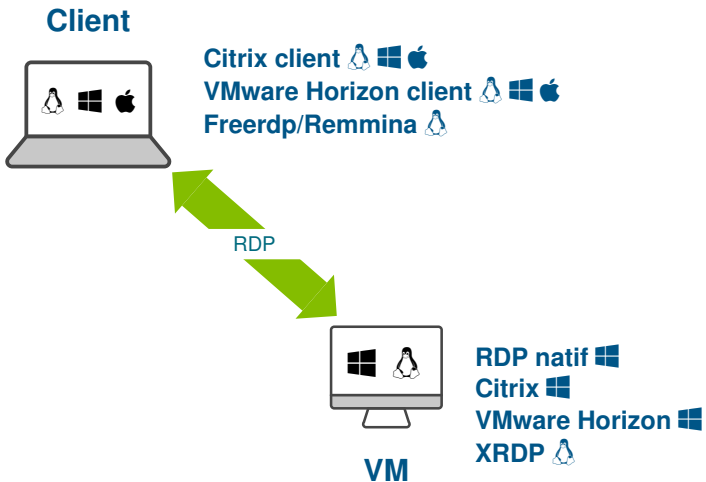


Solutions existantes qui exploitent les canaux virtuels

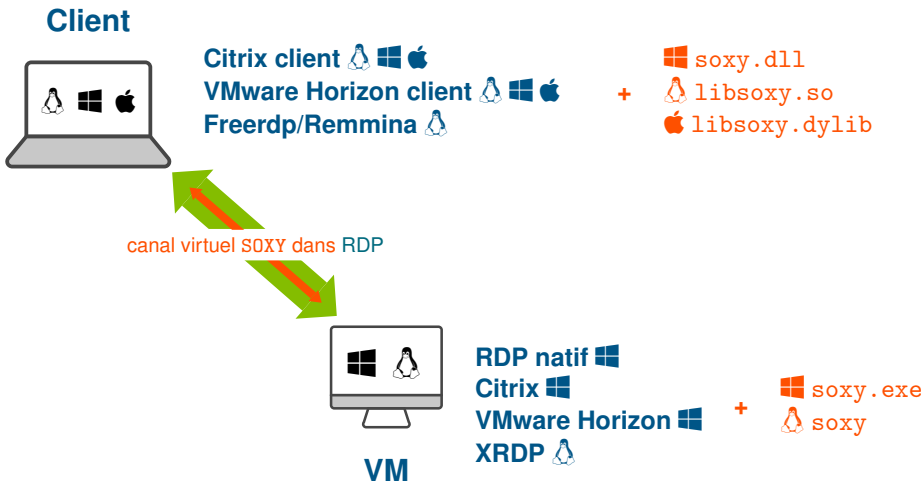
	Clients	VDI	Services	Stable	Maintenue
rdp2tcp *HSC*		RDP natif	tunnel TCP proxy SOCKS		2010-2020
SocksOverRdp *NCC group*		RDP natif Citrix Xen*	proxy SOCKS		2020-2022
ica2tcp *Synacktiv*		Citrix	proxy SOCKS		2022

AIRBUS

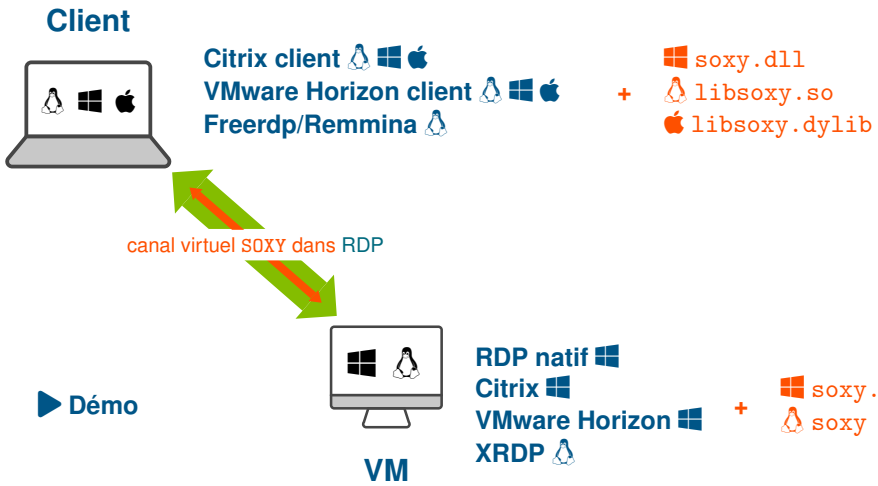
soxy


Client
Citrix client
VMware Horizon client
Freerdp/Remmina
RDP
RDP natif
Citrix
VMware Horizon
XRDP
VM

soxy


Client
Citrix client
VMware Horizon client
Freerdp/Remmina
+
soxy.dll
libsoxy.so
libsoxy.dylib
canal virtuel SOXY dans RDP
RDP natif
Citrix
VMware Horizon
XRDP
+
soxy.exe
soxy
VM

soxy


Client
Citrix client
VMware Horizon client
Freerdp/Remmina
+
soxy.dll
libsoxy.so
libsoxy.dylib
canal virtuel SOXY dans RDP
Démo
RDP natif
Citrix
VMware Horizon
XRDP
+
soxy.exe
soxy
VM

AIRBUS


La VDI bloque totalement l'accès à internet et le transfert de fichiers.
En utilisant soxy on peut accéder au réseau derrière la VDI.
Pas besoin de déployer d'outil sur la VDI, il suffit de lancer soxy !
Pas besoin de déployer d'outil sur la VDI, il suffit de lancer soxy !

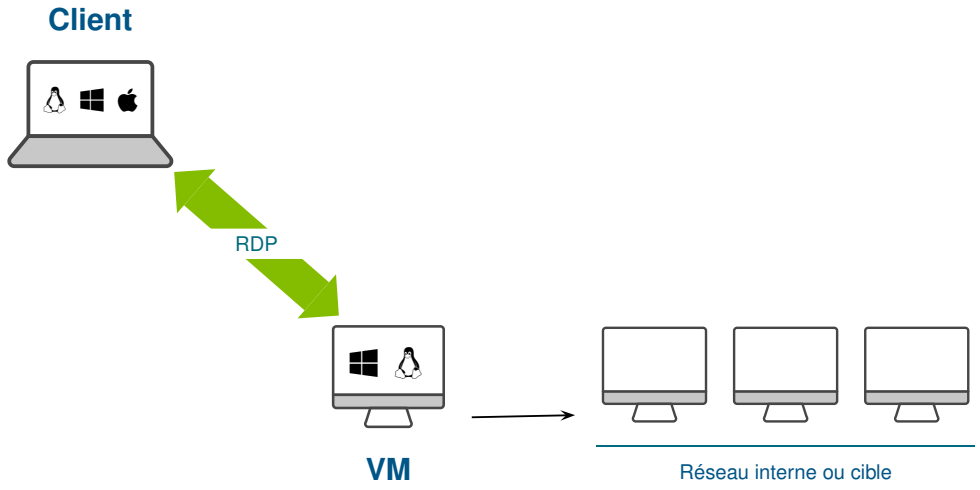
Démo

Point de vue Red Team

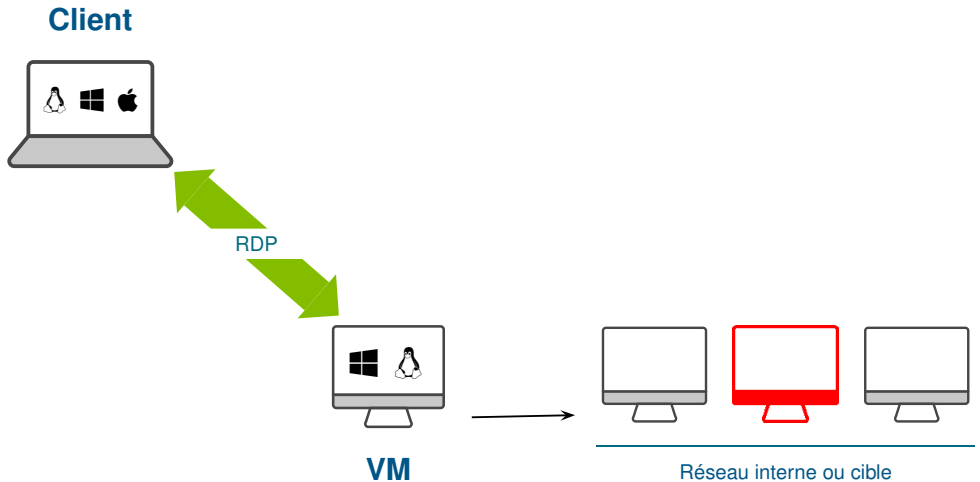
Une fois `soxy` executé, depuis notre client, on peut désormais :

- ✓ Accéder en lecture/écriture au système de fichiers de la VM
- ✓ Accéder au réseau derrière le VDI
- ✓ Accéder au presse-papiers de la VM

Point de vue Red Team



Point de vue Red Team



Point de vue Blue Team

Détection de canaux virtuels : source

Stratégie de surveillance

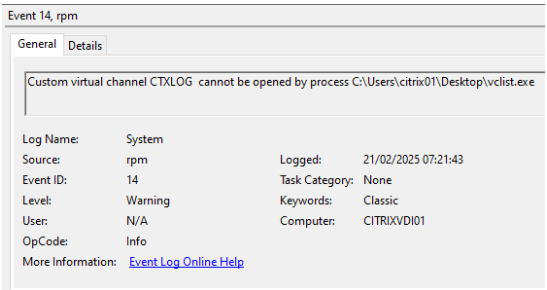
- Identifier l'utilisation de canaux virtuels par l'analyse des journaux d'événements
- S'appuyer sur les événements propres à chaque technologie pour détecter les usages suspects ou non autorisés

Type d'événement	RDP	Citrix	VMware Horizon
Création	Event ID 132	Event ID 13	Log RDPVCBridge
Échec	Event ID 131	Event ID 14	–
Fermeture	Event ID 140	Event ID 15/16	Log RDPVCBridge

Point de vue Blue Team

Détection de canaux virtuels : informations obtenues

- **RDP**
  - Nom du canal virtuel
- **Citrix**
  - Nom du canal et chemin complet du binaire appelant
  - Utilisateur en cas de création
- **VMware Horizon**
  - non identifié



Point de vue Blue Team

Détection de canaux virtuels

File: ../common/src/lib.rs

```rust
use std::ffi;
#[cfg(feature = "log")]
use std::fs;

pub mod api;
pub mod service;

mod clipboard;
mod command;
mod ftp;
mod socks5;
mod stage0;

mod log;
#[cfg(feature = "backend")]
mod util;

pub const VIRTUAL_CHANNEL_NAME: &ffi::CStr = c"SOXY";
```

Point de vue Blue Team

Blocage : Liste d'autorisations de canaux virtuels

VDI	Liste d'autorisations	Version	Activée par défaut
RDP natif	✗	–	✗
Citrix	✓	CVAD 2006 (Juin 2020)	✓[1]
VMware Horizon	✓	Horizon 8 - 2106 (Juillet 2021)	✗[2]

1. https://docs.citrix.com/fr-fr/citrix-virtual-apps-desktops/secure/virtual-channel-security.html
2. https://kb.omnissa.com/s/article/84156

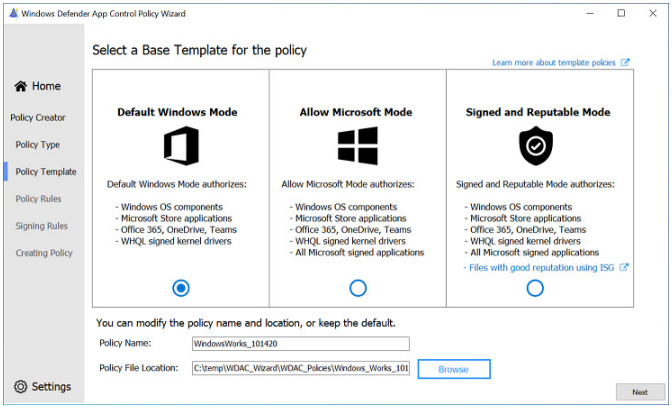
Point de vue Blue Team

Blocage : Liste d'autorisations de canaux virtuels

```
.data:0000000180228C48                 dq offset aWindowsSystem3 ; "\\Windows\\System32\\net.exe"
.data:0000000180228C50                 dq offset aCtxlpt1        ; "CTXLPT1"
.data:0000000180228C58                 db    1
.data:0000000180228C59                 db    0
.data:0000000180228C5A                 db    0
.data:0000000180228C5B                 db    0
.data:0000000180228C5C                 db    2
.data:0000000180228C5D                 db    0
.data:0000000180228C5E                 db    0
.data:0000000180228C5F                 db    0
.data:0000000180228C60                 dq offset aWindowsSyswow6 ; "\\Windows\\SysWOW64\\net.exe"
.data:0000000180228C68                 dq offset aCtxlpt1        ; "CTXLPT1"
.data:0000000180228C70                 db    1
.data:0000000180228C71                 db    0
.data:0000000180228C72                 db    0
.data:0000000180228C73                 db    0
.data:0000000180228C74                 db    2
.data:0000000180228C75                 db    0
.data:0000000180228C76                 db    0
.data:0000000180228C77                 db    0
.data:0000000180228C78                 dq offset aWindowsSystem3_0 ; "\\Windows\\System32\\cmd.exe"
.data:0000000180228C80                 dq offset aCtxlpt1          ; "CTXLPT1"
.data:0000000180228C88                 db    1
.data:0000000180228C89                 db    0
.data:0000000180228C8A                 db    0
.data:0000000180228C8B                 db    0
.data:0000000180228C8C                 db    2
.data:0000000180228C8D                 db    0
.data:0000000180228C8E                 db    0
.data:0000000180228C8F                 db    0
.data:0000000180228C90                 dq offset aWindowsSyswow6_0 ; "\\Windows\\SysWOW64\\cmd.exe"
.data:0000000180228C98                 dq offset aCtxlpt2          ; "CTXLPT2"
.data:0000000180228CA0                 db    2
```

Blocage indépendant – Contrôle des applications

- AppLocker (depuis Windows 7+)
- WDAC (Windows 10+)



Et maintenant ?

Évolutions à venir

- Service de **scan réseau efficace**
- Amélioration de la **furtivité du binaire** côté VM
- Compilation dans docker/podman (pour le gérer les dépendances système)
- [à confirmer] Intégration d'une **VM Python pour exécuter du code arbitraire** côté VM

D'autres idées ?

- Faites le nous savoir en postant une *issue* voire une *pull request* 🥹

Merci !

https://github.com/airbus-seclab/soxy

@AirbusSecLab – https://airbus-seclab.github.io