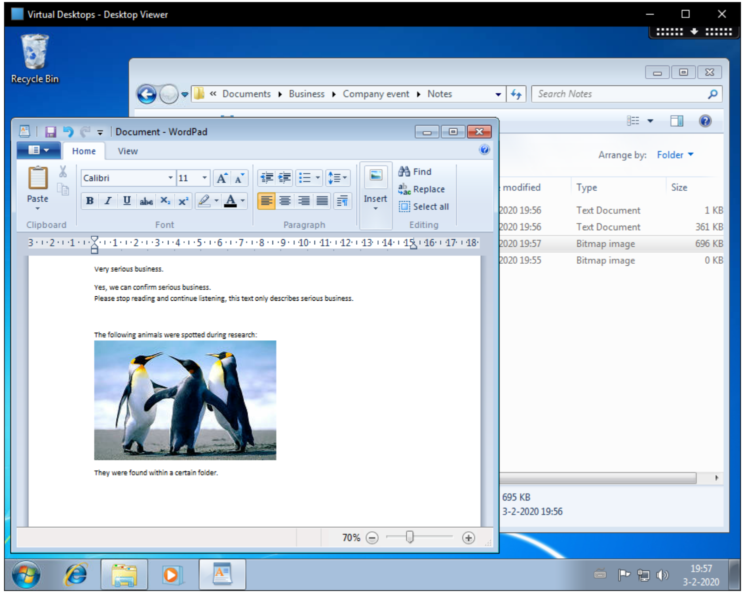
Tunneling data over a Citrix Virtual Apps and Desktops session

Ward Bakker
Niels den Otter

Security and Network Engineering
University of Amsterdam

Citrix Virtuals Apps and Desktops

- XenApp / XenDesktop
- Virtual Desktop Infrastructure
  - Employees can work anywhere, anytime
  - Employees can use any device
- IT Admins control the entire environment
- Makes use of a master VM



Very serious business.

Yes, we can confirm serious business.
Please stop reading and continue listening, this text only describes serious business.

The following animals were spotted during research:

They were found within a certain folder.

modified	Type	Size
2020 19:56	Text Document	1 KB
2020 19:56	Text Document	361 KB
2020 19:57	Bitmap image	696 KB
2020 19:55	Bitmap image	0 KB

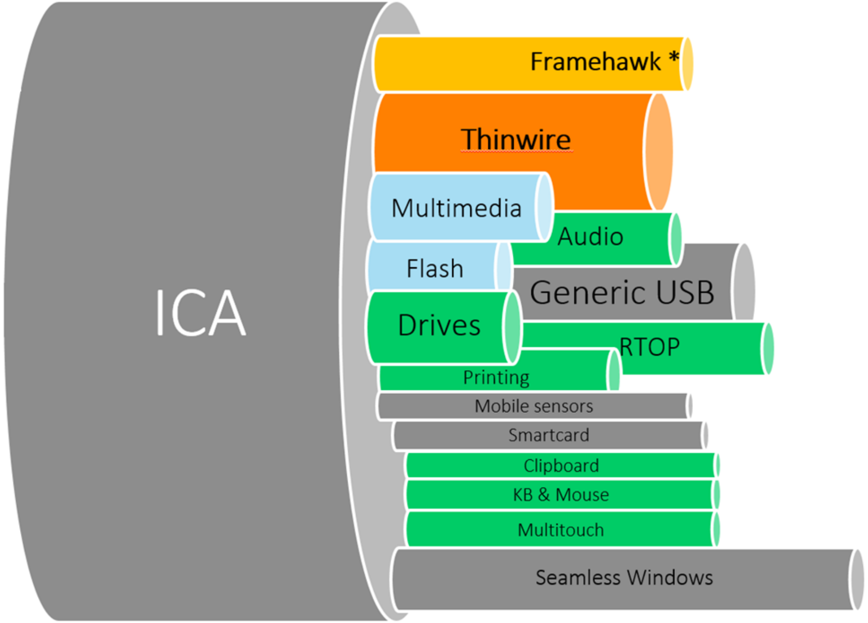
695 KB
3-2-2020 19:56

History: Citrix and Remote Desktop Protocol

- First version of RDP relied on Citrix technology
  - Citrix-provided .DLL’s still contained Citrix copyright
- Both solutions use Virtual Channels

Independent Computing Architecture (ICA)

HDX with Enlightened Data Transport



* Framehawk actually uses its own UDP data transport layer based on gearing

Tunneling using ICA

Benefits

- Hard to detect
  - Virtual Channel data encapsulated
- Avoiding firewalls

Trade-offs

- Limited to server’s capabilities
- ICA is a proprietary protocol

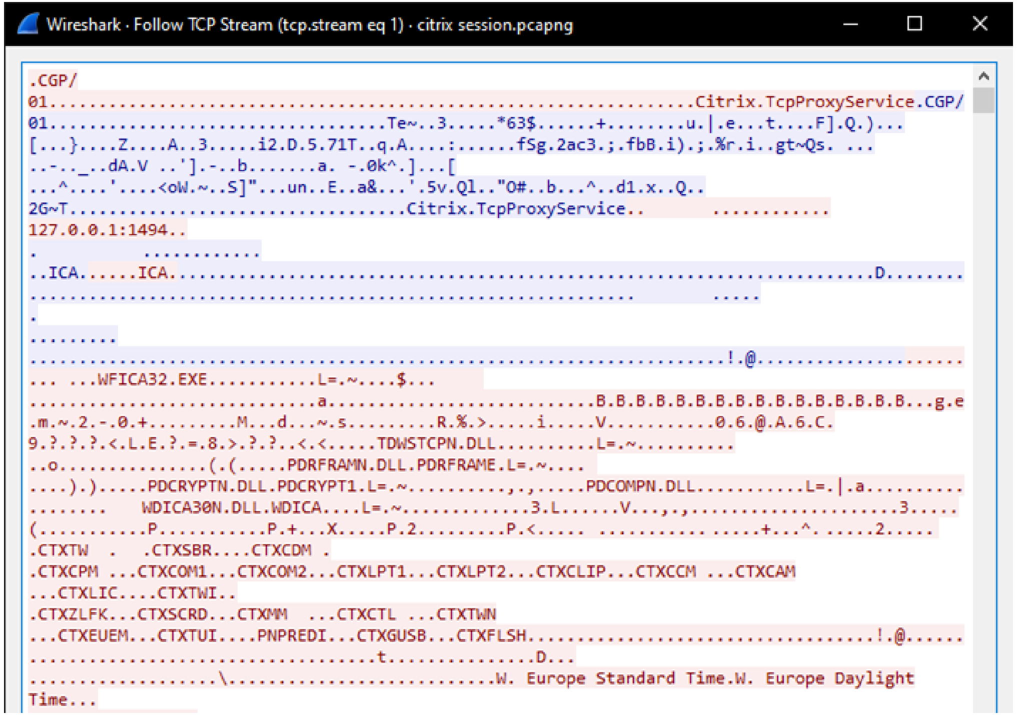
Our research

- Tunnel data through a Citrix session
  - Similar to rdp2tcp, VcCom
- Useful for intelligence gathering

How can data be sent through a Citrix Virtual Apps and Desktops session?

Background

- Transport protocol
- Session establishment
- Encryption


Wireshark · Follow TCP Stream (tcp.stream eq 1) · citrix session.pcapng

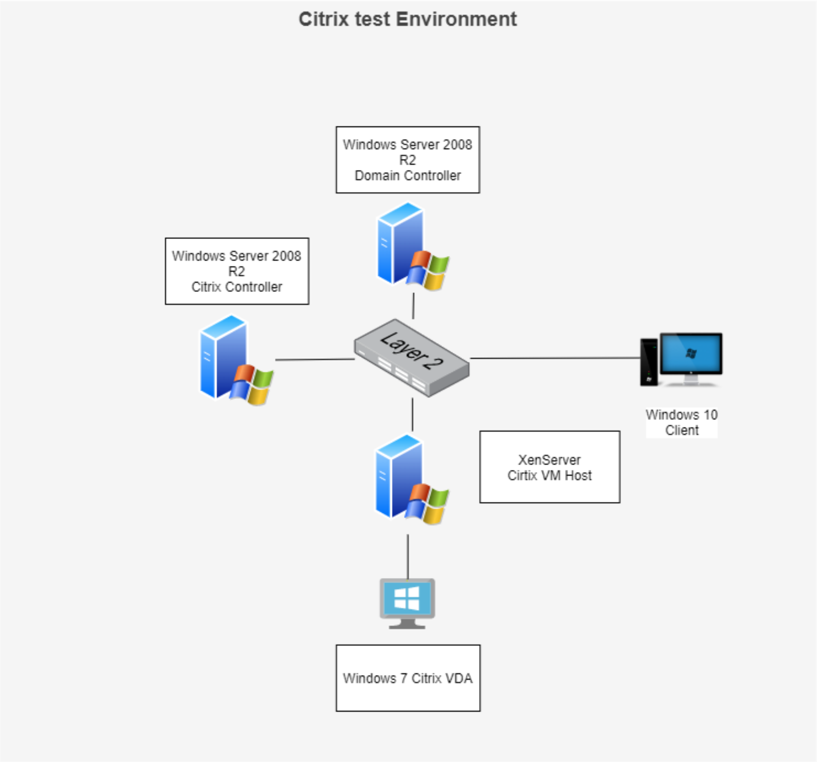
```
.CGP/
01..............................................................Citrix.TcpProxyService.CGP/
01................................Te~..3.....*63$......+........u.|.e...t....F].Q.)...
[...}....Z....A..3.....i2.D.5.71T..q.A....:......fSg.2ac3.;.fbB.i).;.%r.i..gt~Qs. ...
..-.._..dA.V ..'].-..b.......a. -.0k^.]...[
...^....'....<oW.~..S]"...un..E..a&...'.5v.Ql.."O#..b...^..d1.x..Q..
2G~T................................Citrix.TcpProxyService..      ............
127.0.0.1:1494..
.           ............
..ICA......ICA...........................................................D........
.............................................................       .....
.
.........
.......................................................................!.@...................
... ...WFICA32.EXE...........L=.~....$...
..............................a..............................B.B.B.B.B.B.B.B.B.B.B.B.B.B.B.B...g.e
.m.~.2.-.0.+.........M...d...~.s.........R.%.>.....i.....V...........0.6.@.A.6.C.
9.?.?.?.<.L.E.?.=.8.>.?.?..<.<.....TDWSTCPN.DLL..........L=.~..........
..o...............(.(.....PDRFRAMN.DLL.PDRFRAME.L=.~....
....).).....PDCRYPTN.DLL.PDCRYPT1.L=.~..........,.,.....PDCOMPN.DLL...........L=.|.a..........
........   WDICA30N.DLL.WDICA....L=.~.............3.L......V...,.,......................3.....
(...........P...........P.+...X.....P.2.........P.<..... ............ .....+...^. .....2.....
.CTXTW  .   .CTXSBR....CTXCDM .
.CTXCPM ...CTXCOM1...CTXCOM2...CTXLPT1...CTXLPT2...CTXCLIP...CTXCCM ...CTXCAM
...CTXLIC....CTXTWI..
.CTXZLFK...CTXSCRD...CTXMM  ...CTXCTL ...CTXTWN
...CTXEUEM...CTXTUI....PNPREDI...CTXGUSB...CTXFLSH.................................!.@......
...................................t...............D...
...................\...........................W. Europe Standard Time.W. Europe Daylight
Time...
```

Methodology

How do we get information from and to client?

- Choices
    - Modifying virtual channel
    - Manipulating virtual channel
    - Creating our own virtual channel

Test environment



Virtual channel setup

Client

- Required to modify registry
  - Loading custom .DLL
  - Admin privileges necessary

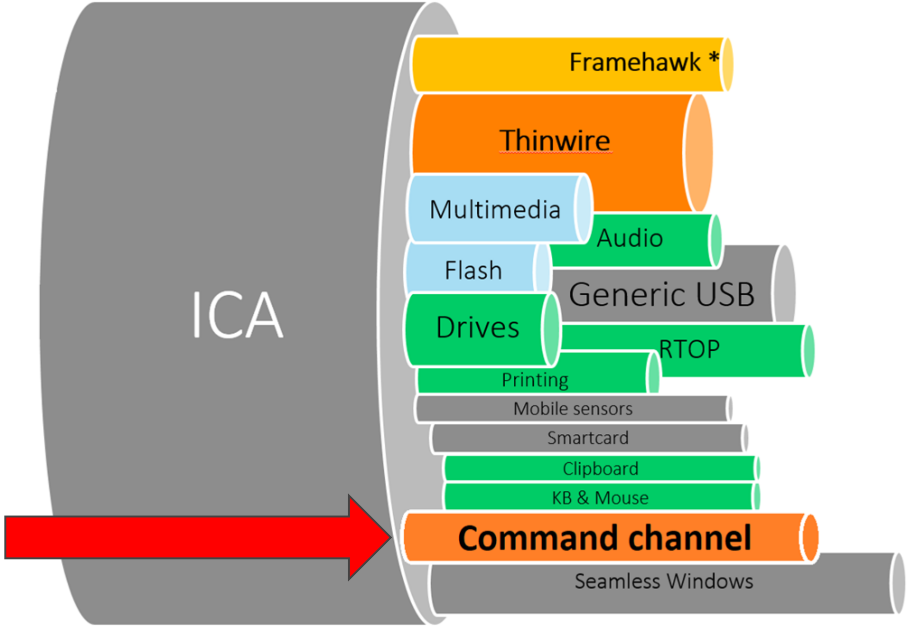
VDI

- Required to launch application
  - Application will use the Virtual Channel
  - No admin privileges necessary

Results

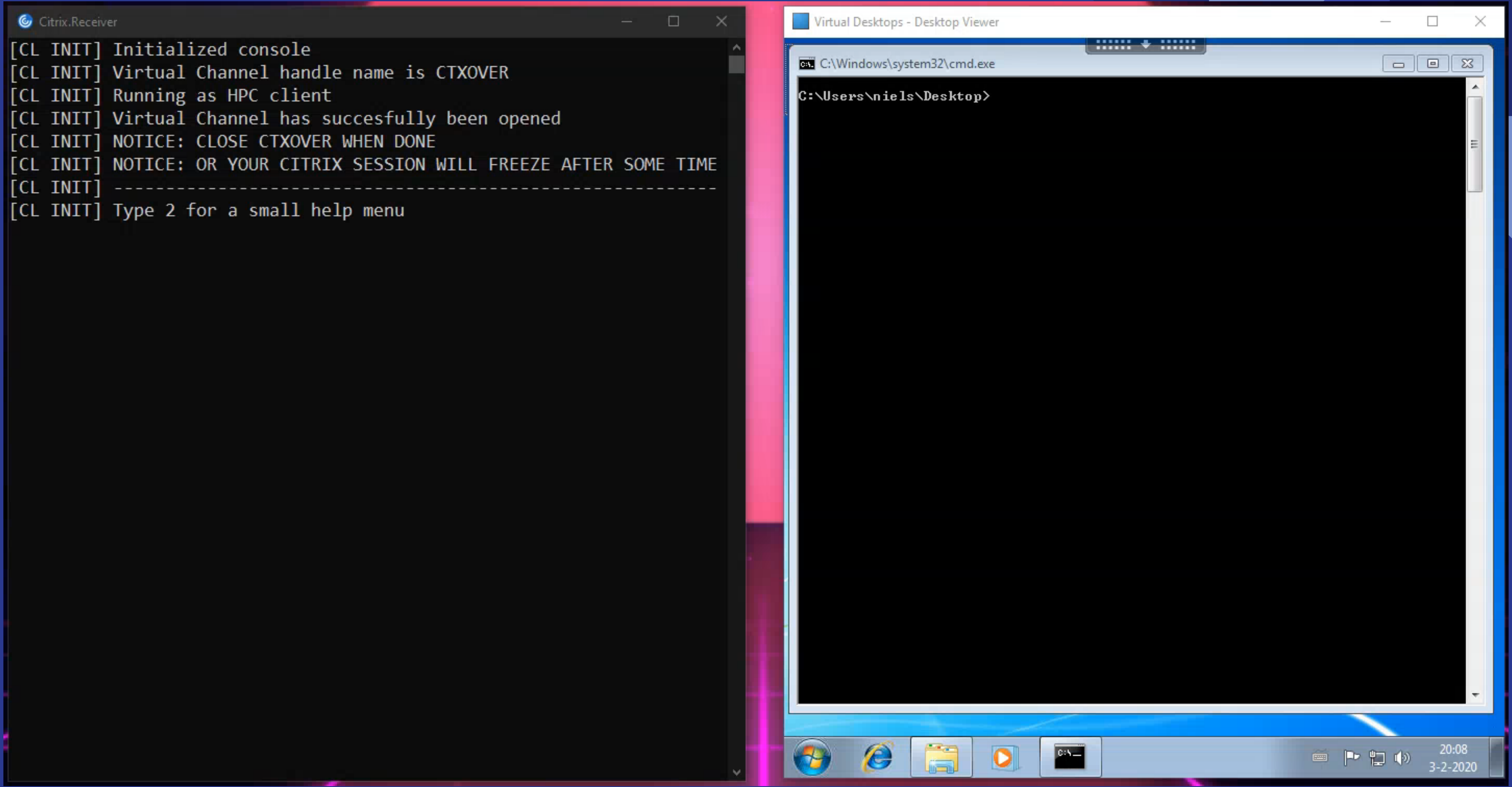
Added virtual channel

HDX with Enlightened Data Transport



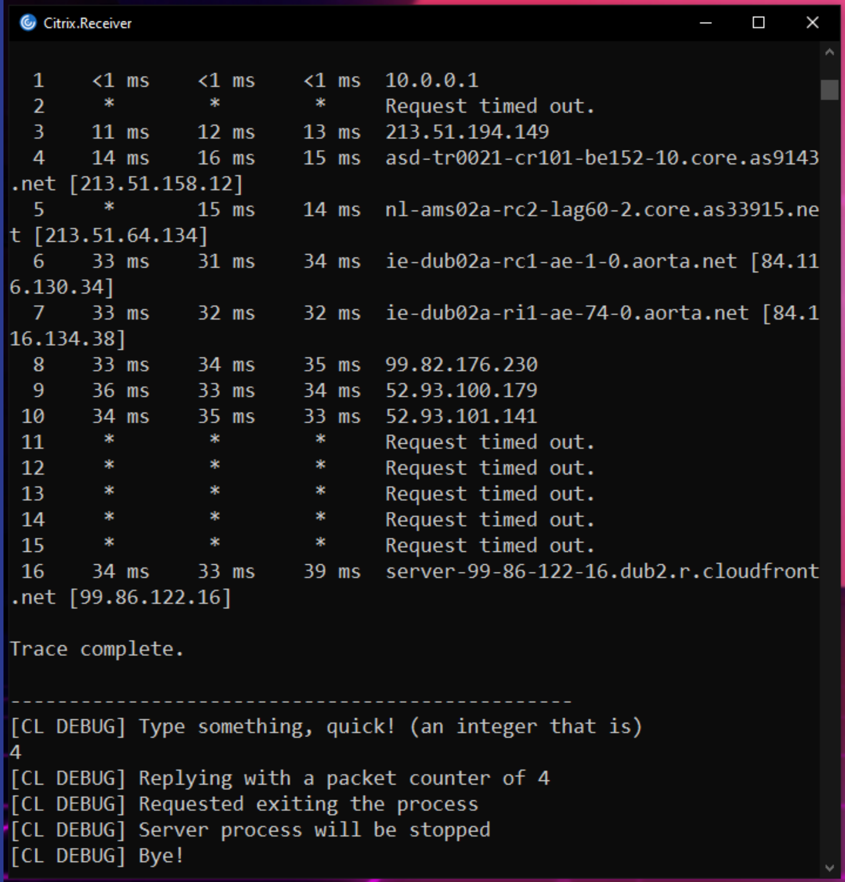
* Framehawk actually uses its own UDP data transport layer based on gearing

Demo


Citrix.Receiver
Virtual Desktops - Desktop Viewer
C:\Windows\system32\cmd.exe
20:08
3-2-2020

```
[CL INIT] Initialized console
[CL INIT] Virtual Channel handle name is CTXOVER
[CL INIT] Running as HPC client
[CL INIT] Virtual Channel has succesfully been opened
[CL INIT] NOTICE: CLOSE CTXOVER WHEN DONE
[CL INIT] NOTICE: OR YOUR CITRIX SESSION WILL FREEZE AFTER SOME TIME
[CL INIT] ----------------------------------------------------------
[CL INIT] Type 2 for a small help menu
```

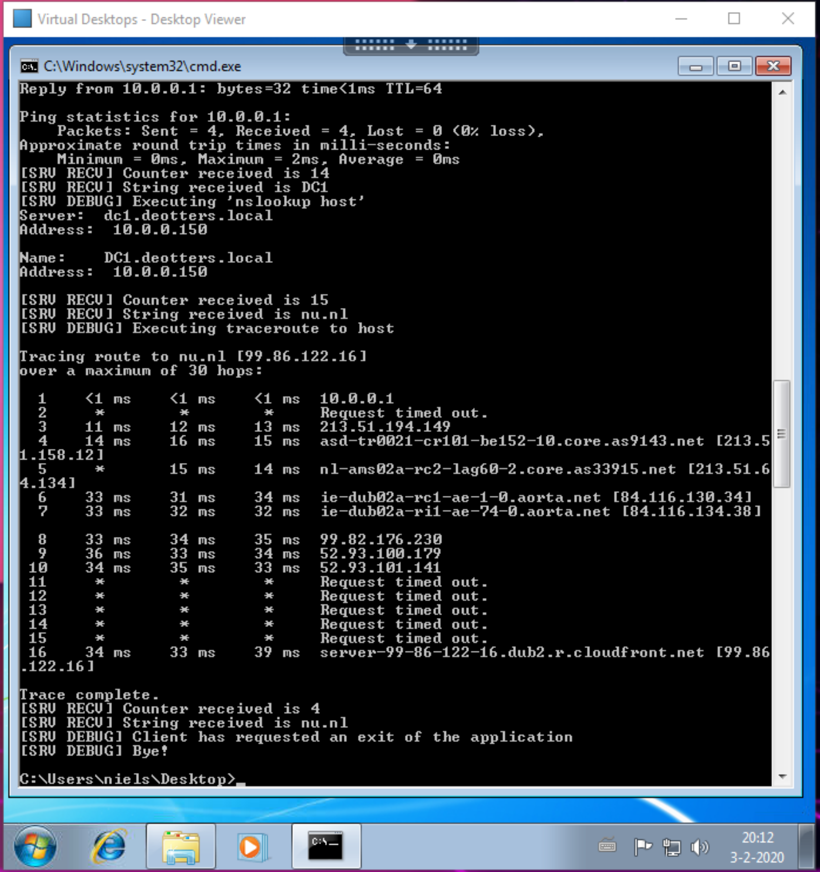
```
C:\Users\niels\Desktop>
```



```
  1    <1 ms    <1 ms    <1 ms  10.0.0.1
  2     *        *        *     Request timed out.
  3    11 ms    12 ms    13 ms  213.51.194.149
  4    14 ms    16 ms    15 ms  asd-tr0021-cr101-be152-10.core.as9143
.net [213.51.158.12]
  5     *       15 ms    14 ms  nl-ams02a-rc2-lag60-2.core.as33915.ne
t [213.51.64.134]
  6    33 ms    31 ms    34 ms  ie-dub02a-rc1-ae-1-0.aorta.net [84.11
6.130.34]
  7    33 ms    32 ms    32 ms  ie-dub02a-ri1-ae-74-0.aorta.net [84.1
16.134.38]
  8    33 ms    34 ms    35 ms  99.82.176.230
  9    36 ms    33 ms    34 ms  52.93.100.179
 10    34 ms    35 ms    33 ms  52.93.101.141
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16    34 ms    33 ms    39 ms  server-99-86-122-16.dub2.r.cloudfront
.net [99.86.122.16]

Trace complete.

---------------------------------------------
[CL DEBUG] Type something, quick! (an integer that is)
4
[CL DEBUG] Replying with a packet counter of 4
[CL DEBUG] Requested exiting the process
[CL DEBUG] Server process will be stopped
[CL DEBUG] Bye!
```


Virtual Desktops - Desktop Viewer
C:\Windows\system32\cmd.exe
20:12
3-2-2020

```
Reply from 10.0.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
[SRV RECV] Counter received is 14
[SRV RECV] String received is DC1
[SRV DEBUG] Executing 'nslookup host'
Server:  dc1.deotters.local
Address:  10.0.0.150

Name:    DC1.deotters.local
Address:  10.0.0.150

[SRV RECV] Counter received is 15
[SRV RECV] String received is nu.nl
[SRV DEBUG] Executing traceroute to host

Tracing route to nu.nl [99.86.122.16]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.0.0.1
  2     *        *        *     Request timed out.
  3    11 ms    12 ms    13 ms  213.51.194.149
  4    14 ms    16 ms    15 ms  asd-tr0021-cr101-be152-10.core.as9143.net [213.5
1.158.12]
  5     *       15 ms    14 ms  nl-ams02a-rc2-lag60-2.core.as33915.net [213.51.6
4.134]
  6    33 ms    31 ms    34 ms  ie-dub02a-rc1-ae-1-0.aorta.net [84.116.130.34]
  7    33 ms    32 ms    32 ms  ie-dub02a-ri1-ae-74-0.aorta.net [84.116.134.38]

  8    33 ms    34 ms    35 ms  99.82.176.230
  9    36 ms    33 ms    34 ms  52.93.100.179
 10    34 ms    35 ms    33 ms  52.93.101.141
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16    34 ms    33 ms    39 ms  server-99-86-122-16.dub2.r.cloudfront.net [99.86
.122.16]

Trace complete.
[SRV RECV] Counter received is 4
[SRV RECV] String received is nu.nl
[SRV DEBUG] Client has requested an exit of the application
[SRV DEBUG] Bye!

C:\Users\niels\Desktop>_
```

Conclusion

How can data be sent through a Citrix Virtual Apps and Desktops session?

- Virtual Channels
  - Tunneling is possible
  - Lots of possibilities

Discussion

- Set up as unprivileged user
- Virtual channel data encapsulated or encrypted
- Commands executed as current user

Future work

- (Reflective) DLL injection on the mandatory virtual channels
- Research ICA protocol
- Expand code for usage of custom applications

Thanks for listening!

How can data be sent through a Citrix Virtual Apps and Desktops session?

- Virtual Channels
  - Tunneling is possible
  - Lots of possibilities