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
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
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
[CL INIT] Initialized console
[CL INIT] Virtual Channel handle name is CTXOVER
[CL INIT] Running as HPC client
[CL INIT] Virtual Channel has successfully been opened
[CL INIT] NOTICE: CLOSE CTXOVER WHEN DONE
[CL INIT] NOTICE: OR YOUR CITRIX SESSION WILL FREEZE AFTER SOME TIME
[CL INIT] Type 2 for a small help menu
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
5 net [213.51.158.12]
6 * 15 ms 14 ms nl-ams02a-rc2-lag60-2.core.as33915.net
7 [213.51.64.134]
8 63 ms 31 ms 34 ms ie-dub02a-rcl-ae-1-0.aorta.net [84.11
9 6.130.34]
10 73 ms 32 ms 32 ms ie-dub02a-ri1-ae-74-0.aorta.net [84.1
11 16.134.38]
12 83 ms 34 ms 35 ms 99.82.176.230
13 93 ms 36 ms 33 ms 52.93.100.179
14 104 ms 34 ms 33 ms 52.93.101.141
15 * * * Request timed out.
16 11 * * * Request timed out.
17 12 * * * Request timed out.
18 13 * * * Request timed out.
19 14 * * * Request timed out.
20 15 * * * Request timed out.
21 16 34 ms 33 ms 39 ms server-99-86-122-16.dub2.r.cloudfront.
22 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!
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