

Internal Memorandum

**To: Paula Alexander**

**CC:**

**From:** Collin Johnson, Team A

**Date:** October 21, 2018

**Memo #:** 7

**Re:** Inject 7 and found issues

Good afternoon,

With today’s adventure many things were discovered including:

Users:

‘IUSR\_ADURAND2008’

‘NOTAGUEST’

Both of these users were unknown and disabled.

Tasks:

Disabled Tasks in Task scheduler

Disabled services that could be used to penetrate the system

While it did not appear to be used, Task scheduler could be used once a backdoor is created to control system processes.

Windows Firewall:

Enabled Firewall from *regedit*

Enabled Firewall *Services* from Services tab

Set Firewall to enabled and added input and output.

I found and showed each of the windows systems how to do this. Enabling the firewall service is not possible unless you change the reg key to enable the service.

Programs:

TigerVNC was installed and used as a backdoor

Sticky keys was changed to be CMD to login from the lockscreen

Network level authentication

TigerVNC needed to be uninstalled after being found as a backdoor. The Sticky Keys binary needed to be changed.

Unfound issues:

Mouse disabled

Opened external web addresses (Youtube videos)

I believe these two issues were caused by the TigerVNC backdoor. Due to this, it never happened again after the removal of TigerVNC.

Injects:

I took control of most injects and pushed the group to complete them in a timely manner.

These are just the ones that I remember from the chaotic situation. I am impressed with the uptime that the Windows side of the Wiki held through all of the attacks. My security could have been better and helping my team is always something to improve on.

Thank you for understanding,

Collin Johnson

*In accordance with HAL Memorandum policy, the entire header must be completed or the recipient may not acknowledge this as an official memorandum. Professional communications methods and decorum must be observed at all times.*