

Internal Memorandum

**To:** CIO

**CC: n/a**

**From: Aiden Durand**

**Date:** 10/21/2018

**Memo #:** 7

**Re:** Special Inject 007

CIO;

Today I discovered many malicious files and configurations on the machine I was working on, and took the required countermeasures to reduce risk.

First, I discovered that there were many unaccounted users with permissions to login to this machine. I disabled all non-required user accounts and changed the passwords for all the accounts to secure alternatives.

Then, it came to my attention that the firewall was disabled. I remediated this by turning on the firewall, creating new rules to allow the required services through, and deleting all the malicious rules that were in effect already (there was a rule named “bad” that allowed all).

After that, I went into task scheduler and discovered that a Netcat backdoor was running every fifteen minutes. I deleted the task scheduler rule and then found the backdoor and deleted it.

Then, I used the Sysinternals suite to discover a malicious DLL called “ColinFinished.dll”. I deleted its autorun entry then deleted the file itself.

I also discovered that the “sethc.exe” file had been replaced with a system-level cmd prompt, and removed to mitigate the risk of a hacker using that to access our system.

I found that the XAMPP web server was configured to allow anyone to edit the server’s settings, and that it was full of suspicious files. I password protected the administration pages and added a new home page to the webserver, proclaiming that there were no anime girls or traps on this machine. I also removed anything that looked even remotely like a webshell.

There was a malicious share running on the machine that gave anyone access to the entire C drive. I went into the shares utility and removed it, reducing the amount of entry points to the machine.

I hope you are satisfied with the security configurations I made to the machine.

Regards;

Aiden Durand

*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.*