

Internal Memorandum

**To:** CIO

**CC:**

**From:** Michael Ibeh

**Date:**

**Memo #:**

**Re:** Security Update

Greetings,

Over the course of today, HAL Corp’s internal security team found several concerning items we had to address. Using the Sysinternals tool Autoruns, we found a malicious DLL named “JoshFinish” and a malicious VBS script, both of which were removed. In the Windows Event Log under the security tab, Several failed logon attempts were noticed with usernames such as “metasploit” and random alphanumeric strings. Using netstat, several TCP connections to external IP addresses were observed using svchost processes which was highly suspicious. These IP address were added to firewall rules to block all inbound and outbound traffic to them. Microsoft Security Essentials was installed to increase our defensive posture and a scan found two malicious files, which were then removed from the system. These were a Meterpreter shell and a Visual Basic script.

Regards,

Michael Ibeh