

Reported by: Martin Guzman

Incident Description

Time of First Attack: 10:39:00 AM Time of Attack Detection: 11:00:00 AM  
Estimated Recovery Time: 00:00 Duration of Attack: 00:21  
Has the Attack Ended?: Yes Estimated Damage Account: Damage is too much to account for.   
Number of Hosts Affected: 40 Number of Users Affected: 35  
Severity of Attack: Severe Attack Category: File Server  
Type of Incident: Active Reconnaissance  
How Did You Become Initially Aware of the Attack?  
Derick told me that I needed to check the PC, I dunno.

Impact of Attack

Primary Purpose of Host: HMI/ICS System  
Host Name: HELIOS-WIN IP Address: 10.0.4.10  
Operating System: Ubuntu 16.04  
Applications Affected: MySQL

Data Loss/Compromise

Was there any loss or compromise of sensitive data?:  
There was no loss to anything except for my pride and dignity.   
Was there any change to the afflicted system?:  
The only change was that of kicking Derick off the damn team.   
Was the HMI/ICS affected?:  
Yes  
Corrective measures enacted:  
I took it upon myself to officially hack the mainframe. It was time that I showed my true colors in the best fashion that I could. I don't want to go into much detail, but let's just say that I'm gonna kill Martin Guzman.