

Reported by: Isaac Sierra

Incident Description

Time of First Attack: 8:30:00 PM Time of Attack Detection: 8:35:00 AM  
Estimated Recovery Time: 00:00 Duration of Attack: 00:05  
Has the Attack Ended?: Yes Estimated Damage Account: $900  
Number of Hosts Affected: 1 Number of Users Affected: 35  
Severity of Attack: Low Attack Category: File Server  
Type of Incident: Active Reconnaissance  
How Did You Become Initially Aware of the Attack?

Impact of Attack

Primary Purpose of Host: FTP Server  
Host Name: HELIOS-WIN IP Address: 10.0.4.8  
Operating System: Windows Server 2012  
Applications Affected: FTP

Data Loss/Compromise

Was there any loss or compromise of sensitive data?:  
No there was not.   
Was there any change to the afflicted system?:  
No there was not.  
Was the HMI/ICS affected?:  
No  
Corrective measures enacted:  
Attackers attempted to use default "anonymous" account to access FTP server. Default user "anonymous" was removed from Server access upon discovery. Attackers attempted multiple time to connect to FTP server with invalid credentials. Through the use of active log monitoring, we were able to identify the attackers and kick their connection. We will keep note of the IP Address and deny future connections to our services.