

Reported by: Bryan Rosado

Incident Description

Time of First Attack: 10:34:00 AM Time of Attack Detection: 2:35:00 PM  
Estimated Recovery Time: 01:33 Duration of Attack: 02:34  
Has the Attack Ended?: Yes Estimated Damage Account: SO MUCH   
Number of Hosts Affected: 12 Number of Users Affected: 50  
Severity of Attack: High Attack Category: NTP  
Type of Incident: Malware Execution  
How Did You Become Initially Aware of the Attack?  
Your mom!

Impact of Attack

Primary Purpose of Host: DC (AD/DNS)  
Host Name: HELIOS-HMI IP Address: 10.0.4.8  
Operating System: Windows Server 2012  
Applications Affected: MySQL

Data Loss/Compromise

Was there any loss or compromise of sensitive data?:  
None whatsoever  
Was there any change to the afflicted system?:  
SO many changes  
Was the HMI/ICS affected?:  
No  
Corrective measures enacted:  
I sucked my thumb.