Team: Team 02 - ASU

Inject Number: 24

Inject Duration: 45 Minutes

Inject Start Date/Time: Sat, 28 Jan 2017 14:39:26 -0800

From: Felonius Gru

To: IT Staff

Subject: Search logs for specific Indicators of Compromise

Team,

I need to ask you to prioritize a search for specific indicators of compromise (IOCs). The company president, has insisted on hiring an audit team for a full post mortem of the events today. The audit team wants you to review your log files and systems. Specifically they are looking for virus signatures, IP addresses, MD5 hashes of malware files or URLs or domain names of botnet command and control servers, etc.

Please prepare a report on what you find. Certainly we need all info you have on current indicators and know you are working on a solution but please include past indicators and mitigation steps. Much of this info is probably already in your Incident Reports so feel to copy and paste. Just make sure everything is formatted into a proper business report.

Thank you.

Felonius Gru