Ticket: 473822
Incident: Tangerine Yellow
Date: 2/15/2019 14:54:03
Description: cmd.exe commands via Pineapple RAT
Status: Assigned

The following commands were collected via Sysmon following Pineapple RAT execution on the beachhead box.

ipconfig /all **Discovery - System Network Configuration Discovery (T1016)**
Execution - Command and Scripting Interpreter (T1059)

arp -a **Discovery - System Network Configuration Discovery (T1016)**
Execution - Command and Scripting Interpreter (T1059)

echo %USERDOMAIN%\%USERNAME% **Discovery - System Owner / User Discovery (T1033)**
Execution - Command and Scripting Interpreter (T1059)

tasklist /v **Discovery - Process Discovery (T1057)**
Execution - Command and Scripting Interpreter (T1059)

sc query **Discovery - System Service Discovery (T1007)**
Execution - Command and Scripting Interpreter (T1059)

systeminfo **Discovery - System Information Discovery (T1082)**
Execution - Command and Scripting Interpreter (T1059)

net group "Domain Admins" /domain **Discovery - Permission Groups Discovery: Domain Groups (T1069.002)**
Execution - Command and Scripting Interpreter (T1059)

net user /domain **Discovery - Account Discovery: Domain Account (T1087.002)**
Execution - Command and Scripting Interpreter (T1059)

net group "Domain Controllers" /domain **Discovery - Remote System Discovery (T1018)**
Execution - Command and Scripting Interpreter (T1059)

netsh advfirewall show allprofiles **Discovery - System Network Configuration Discovery (T1016)**
Execution - Command and Scripting Interpreter (T1059)

netstat -ano **Discovery - System Network Connections Discovery (T1049)**
Execution - Command and Scripting Interpreter (T1059)