Jardel Thomas
Kevin Cleary, Dave Murray
Cse 427
March 7th, 2024

Contents

INCIDENT OVERVIEW	
Team Number	13
Date/Time Identified	March 7th, 2024, 10:12am
Target of Attack	Jim

BUINESS IMPACT	
Attack Vector	The user Jim's account was compromised. The attacker created a new account on the computer granting them access to plant malware.
Functional Impact	Hindered the functionality of applications on the user's system.
Informational impact	The Attacker had full access to everything.
Recoverability	The system and accounts are still good to be used.

DESCRIPTION OF INCIDENT/ ACTIVITY			
Date/Time of initial breach	02/27/2022, 5:41pm	User(s) impacted	Jim
Record(s) Impacted	Applications on system	System(s) impacted	DESKTOP-CHO0HOF

Executive Summary:

This was a minor event with minimal impact to business functionality. The attack was identified earlier today when there was a report of a “Notepad problem” (see FIG 1: the error reported). After further investigation it is evaluated that User Jim’s account was compromised which led to the attacker planting malware on the machine (see FIG 2: malware on system). The investigation is still ongoing but Measures to prevent such attacks are cost effective, it is recommended to update your password policy for stronger passwords in the future.

Indicators of Compromise/Root Cause of incident: Users Jim's password was weak leading to his account being compromised. The attacker created a new account for which he had administrative privileges which he used to plant malware on the system (see FIG 6: initial attack).
Mitigation Action Taken: The attacker's account was removed along with pieces of persistent malware that was on the system (see FIG 3 : attackers account) and (Fig 4: persistent malware found 0 . User Jim's password was also reset to avoid future incidents.

Lessons learned/Opportunity for improvement:

It is highly recommended to update your password policy for users on your system to prepare against future attacks like this.

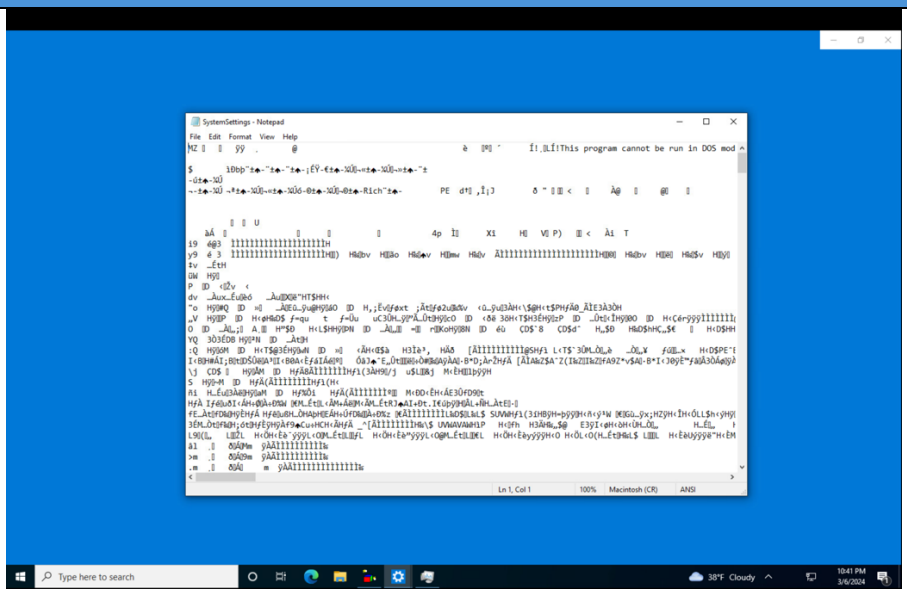


Figure 1: The error reported.

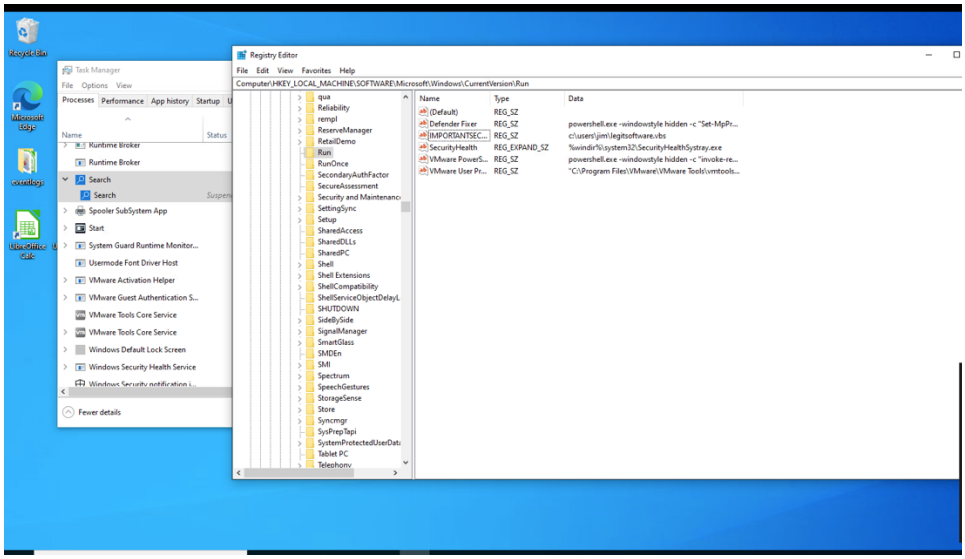


Figure 2: malware on system

Figure 3: Attackers Account.

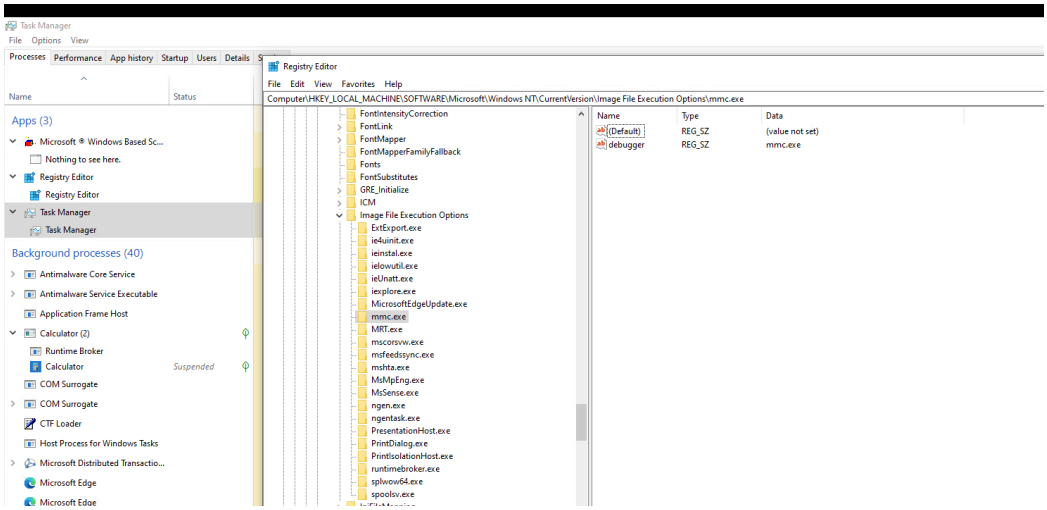


Figure 4: persistent malware found

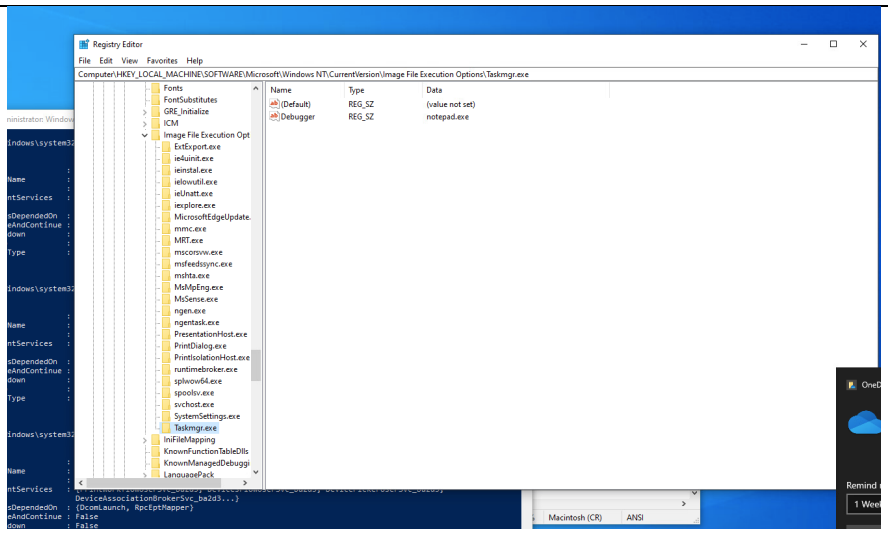


Figure 5: persistent malware on system.

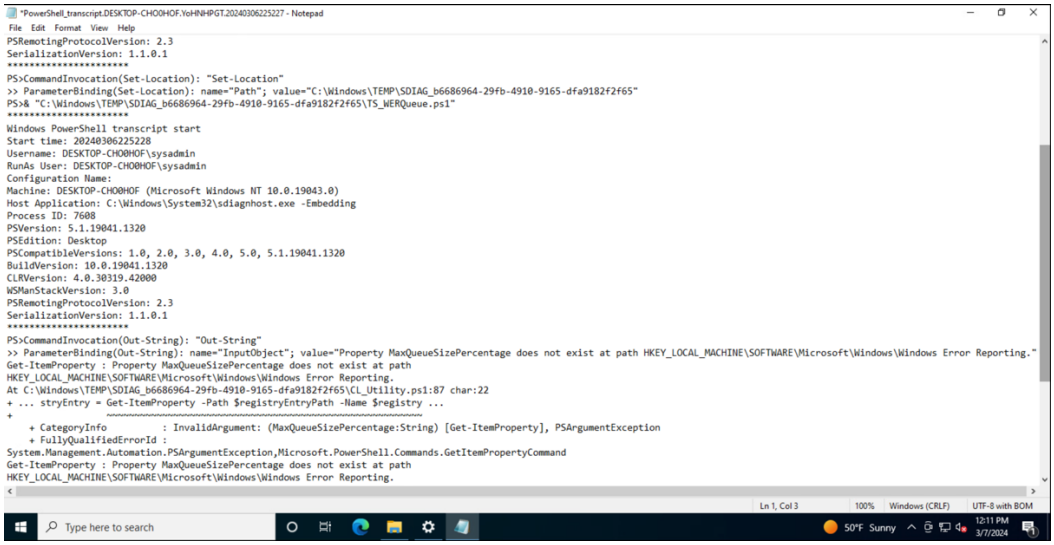
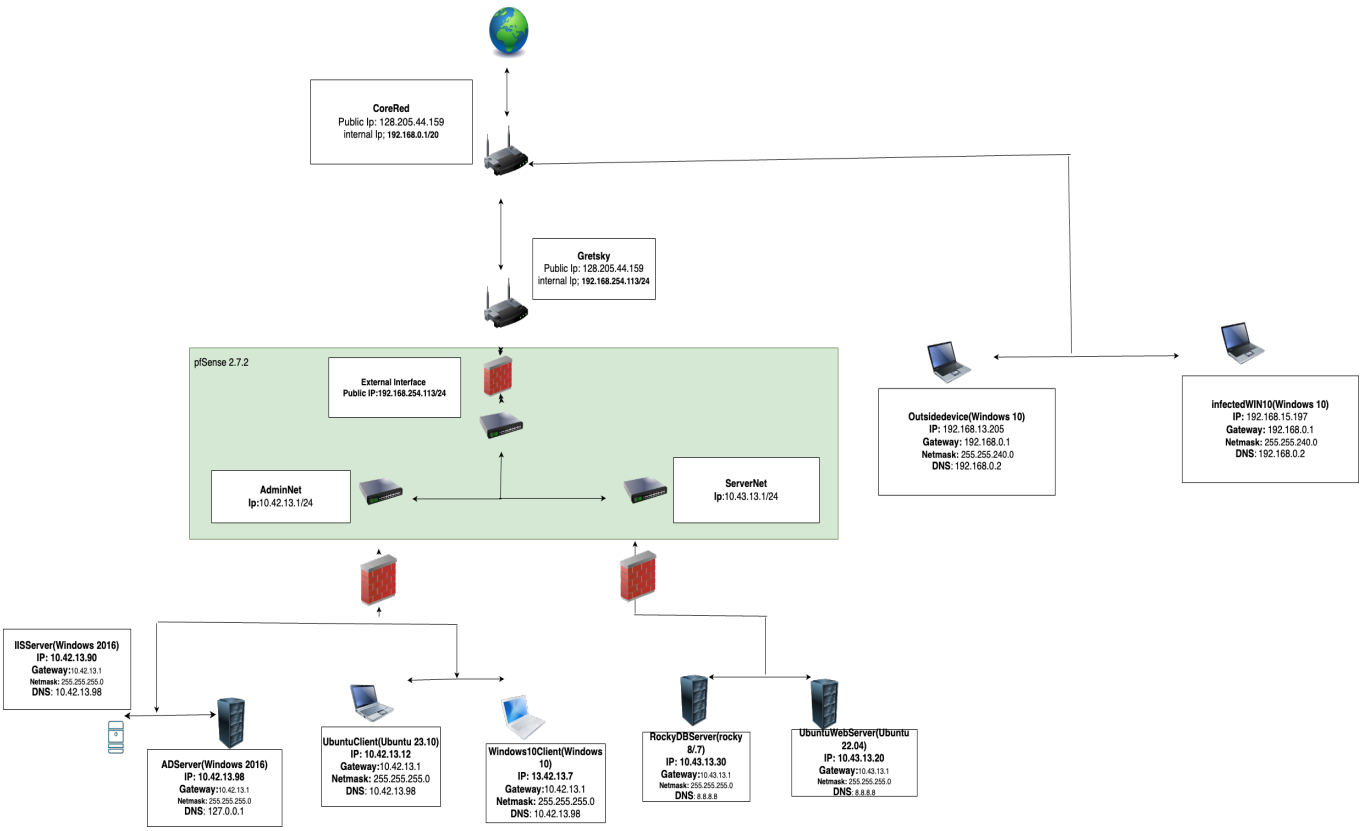


Figure 6: initial attack

5 Topology


CoreRed
Public Ip: 128.205.44.159
internal Ip; 192.168.0.1/20
Gretsky
Public Ip: 128.205.44.159
internal Ip; 192.168.254.113/24
pfSense 2.7.2
External Interface
Public IP:192.168.254.113/24
AdminNet
Ip:10.42.13.1/24
ServerNet
Ip:10.43.13.1/24
Outsidedevice(Windows 10)
IP: 192.168.13.205
Gateway: 192.168.0.1
Netmask: 255.255.240.0
DNS: 192.168.0.2
infectedWIN10(Windows 10)
IP: 192.168.15.197
Gateway: 192.168.0.1
Netmask: 255.255.240.0
DNS: 192.168.0.2
IISServer(Windows 2016)
IP: 10.42.13.90
Gateway:10.42.13.1
Netmask: 255.255.255.0
DNS: 10.42.13.98
ADServer(Windows 2016)
IP: 10.42.13.98
Gateway:10.42.13.1
Netmask: 255.255.255.0
DNS: 127.0.0.1
UbuntuClient(Ubuntu 23.10)
IP: 10.42.13.12
Gateway:10.42.13.1
Netmask: 255.255.255.0
DNS: 10.42.13.98
Windows10Client(Windows 10)
IP: 13.42.13.7
Gateway:10.42.13.1
Netmask: 255.255.255.0
DNS: 10.42.13.98
RockyDBServer(rocky 8/.7)
IP: 10.43.13.30
Gateway:10.43.13.1
Netmask: 255.255.255.0
DNS: 8.8.8.8
UbuntuWebServer(Ubuntu 22.04)
IP: 10.43.13.20
Gateway:10.43.13.1
Netmask: 255.255.255.0
DNS: 8.8.8.8