Digital Forensics Technology and Practices:

Project 3 – Forensic Analysis of an Intrusion

CST-640 9040
Niknaz Sadehvandi
3/7/2025

Project 3 - Introduction

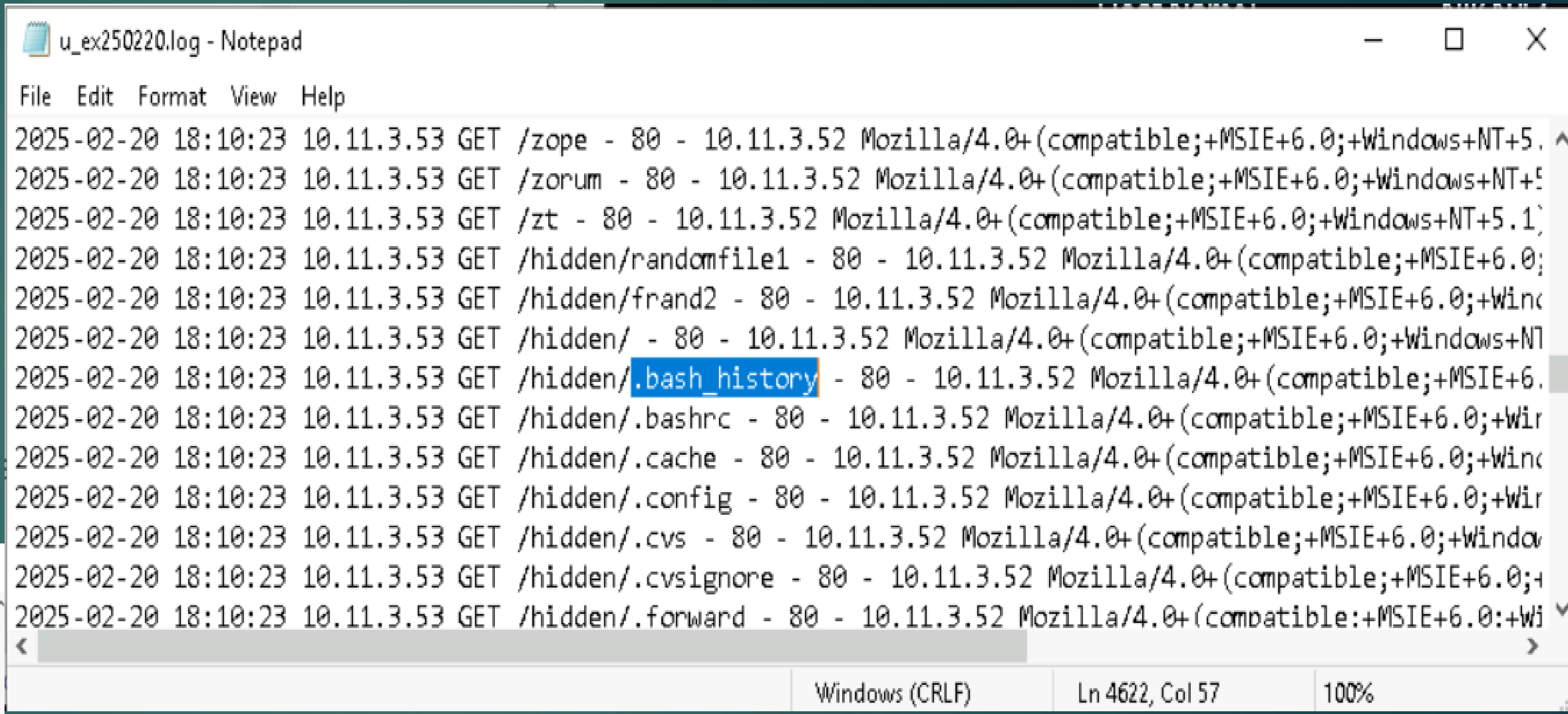
Forensic Analysis of Windows System Attack

- Utilized FTK Imager and Autopsy to analyze log files, registry settings, and system artifacts.
- Identified persistence mechanisms like Startup folder execution and scheduled tasks.
- Event Viewer logs revealed unauthorized administrator accounts
- Network forensics exposed SSH connections for data exfiltration.
- IIS logs confirmed credential theft, indicating a sophisticated attack.
- Emphasized the need for system reconstruction, IP restrictions, and enhanced monitoring.

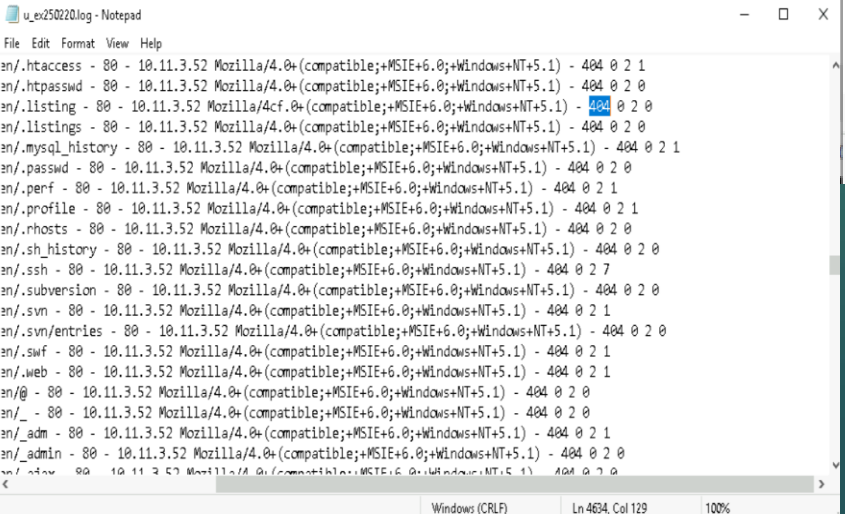
IIS Logs

IP 10.11.3.52 Exploits Secret Folders

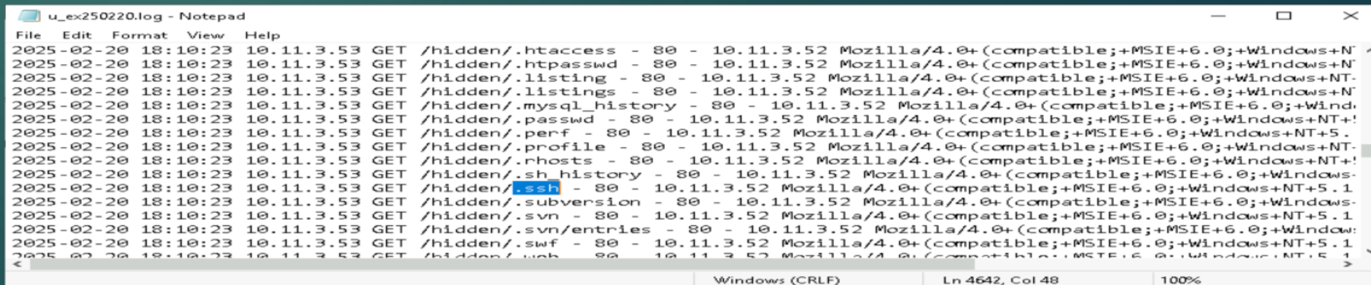
- **Unusual activity in secret folders.**
- **Attackers may seek command history, settings, and credentials.**
- **Demonstrates unauthorized access and reconnaissance.**



```
2025-02-20 18:10:23 10.11.3.53 GET /zope - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.
2025-02-20 18:10:23 10.11.3.53 GET /zorum - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5
2025-02-20 18:10:23 10.11.3.53 GET /zt - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1)
2025-02-20 18:10:23 10.11.3.53 GET /hidden/randomfile1 - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;
2025-02-20 18:10:23 10.11.3.53 GET /hidden/frand2 - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Winc
2025-02-20 18:10:23 10.11.3.53 GET /hidden/ - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.bash_history - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.bashrc - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Wir
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.cache - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Winc
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.config - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Wir
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.cvs - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windo
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.cvsignore - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.forward - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Wi
```



```
en/.htaccess - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 1
en/.htpasswd - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 0
en/.listing - 80 - 10.11.3.52 Mozilla/4cf.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 0
en/.listings - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 0
en/.mysql_history - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 1
en/.passwd - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 0
en/.perf - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 1
en/.profile - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 1
en/.rhosts - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 0
en/.sh_history - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 0
en/.ssh - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 7
en/.subversion - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 0
en/.svn - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 1
en/.svn/entries - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 0
en/.swf - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 1
en/.web - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 1
en/@ - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 0
en/_ - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 0
en/_adm - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 1
en/_admin - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 0
en/_ajax - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) - 404 0 2 0
```

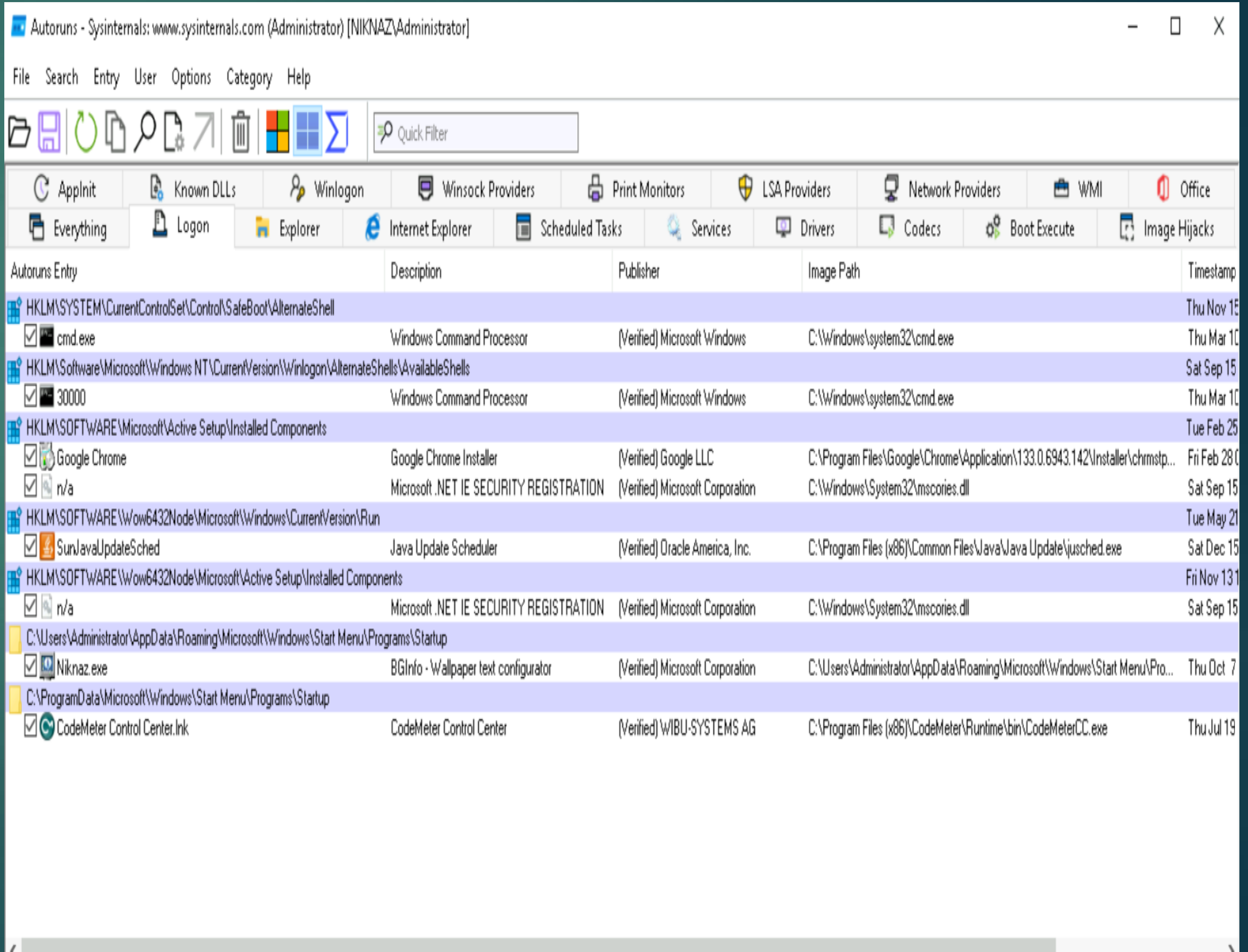


```
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.htaccess - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+N
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.htpasswd - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+N
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.listing - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT-
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.listings - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+N
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.mysql_history - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Wind
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.passwd - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+!
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.perf - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.profile - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT-
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.rhosts - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+!
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.sh_history - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows-
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.ssh - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.subversion - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows-
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.svn - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.svn/entries - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Window:
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.swf - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1
2025-02-20 18:10:23 10.11.3.53 GET /hidden/.web - 80 - 10.11.3.52 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1
```

Autoruns and/or the Startup Folder

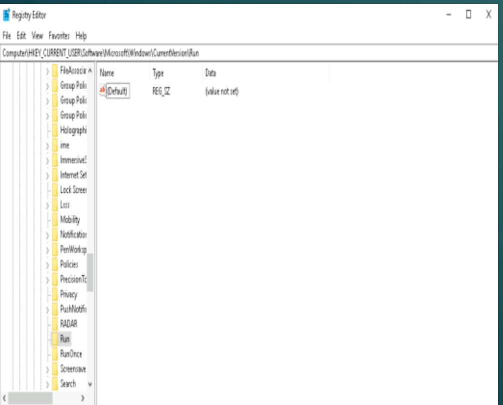
Autoruns Tool and VirusTotal Analysis

- Identifies suspicious startup entries for attacker persistence.
- Verifies malicious files through VirusTotal scan.
- Identifies unauthorized startup programs for system compromise forensic analysis.



Autoruns - Sysinternals: www.sysinternals.com (Administrator) [NIKNAZ\Administrator]

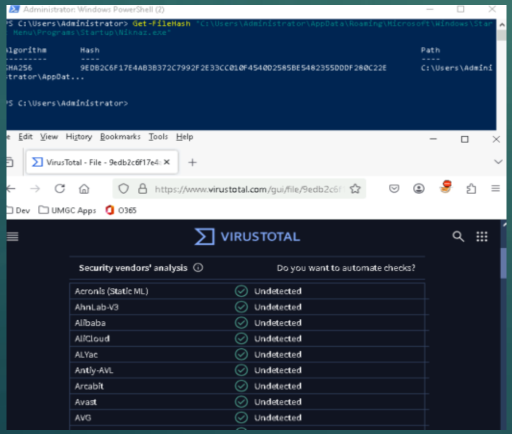
Autoruns Entry	Description	Publisher	Image Path	Timestamp
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				Thu Nov 15
☑ cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe	Thu Mar 1
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AlternateShells\AvailableShells				Sat Sep 15
☑ 30000	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe	Thu Mar 1
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				Tue Feb 25
☑ Google Chrome	Google Chrome Installer	(Verified) Google LLC	C:\Program Files\Google\Chrome\Application\133.0.6943.142\Installer\chrmstp...	Fri Feb 28
☑ n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Sat Sep 15
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				Tue May 21
☑ SunJavaUpdateSched	Java Update Scheduler	(Verified) Oracle America, Inc.	C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	Sat Dec 15
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				Fri Nov 13
☑ n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Sat Sep 15
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				
☑ Niknaz.exe	BGInfo - Wallpaper text configurator	(Verified) Microsoft Corporation	C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Pro...	Thu Oct 7
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup				
☑ CodeMeter Control Center.lnk	CodeMeter Control Center	(Verified) WIBU-SYSTEMS AG	C:\Program Files (x86)\CodeMeter\Runtime\bin\CodeMeterCC.exe	Thu Jul 19



Registry Editor

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)



Administrator: Windows PowerShell (2)

```
PS C:\Users\Administrator> Get-FileHash "C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Star
t Menu\Programs\Startup\Niknaz.exe"

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          9EDB2C6F17E4AB3B372C7992F2E33CC010F4540D2585BE5482355DDDF280C22E       C:\Users\Admini
strator\AppDat...


PS C:\Users\Administrator>
```

Edit View History Bookmarks Tools Help
VirusTotal - File - 9edb2c6f17e4
https://www.virustotal.com/gui/file/9edb2c6f
Dev
UMGC Apps
O365
VIRUSTOTAL

Security vendors' analysis

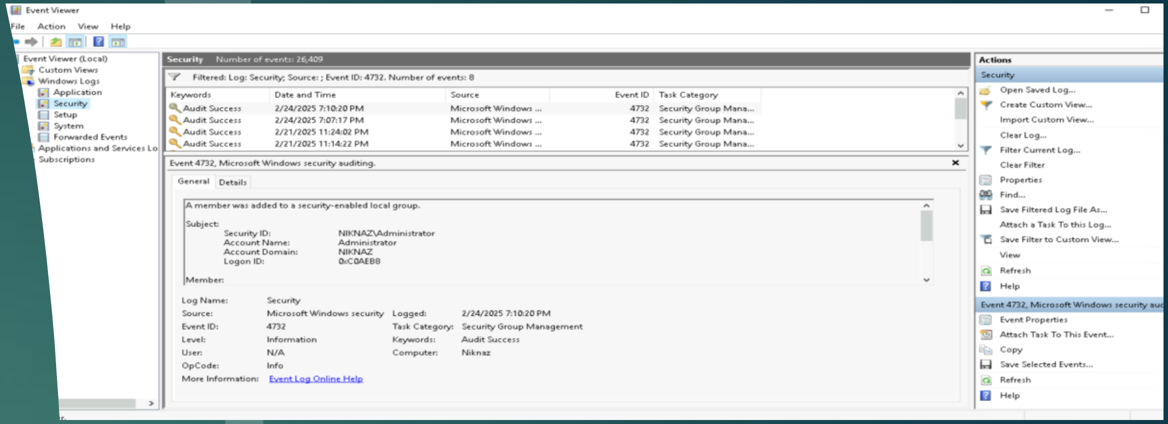
Do you want to automate checks?

Acronis (Static ML)	Undetected
AhnLab-V3	Undetected
Alibaba	Undetected
AliCloud	Undetected
ALYac	Undetected
Antiy-AVL	Undetected
Arcabit	Undetected
Avast	Undetected
AVG	Undetected

Scheduled Tasks

Forensic Analysis Reveals Suspicious Scheduled Task

- **Task runs the unknown script at startup.**
- **Further investigation is needed to determine intent.**
- **No registry Run key found.**
- **Method allows execution at set intervals.**
- **Further log analysis is needed to determine maliciousness.**



Security Number of events: 26,409

Filtered: Log: Security; Source: ; Event ID: 4732. Number of events: 8

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	2/24/2025 7:10:20 PM	Microsoft Windows ...	4732	Security Group Mana...
Audit Success	2/24/2025 7:07:17 PM	Microsoft Windows ...	4732	Security Group Mana...
Audit Success	2/21/2025 11:24:02 PM	Microsoft Windows ...	4732	Security Group Mana...
Audit Success	2/21/2025 11:14:22 PM	Microsoft Windows ...	4732	Security Group Mana...

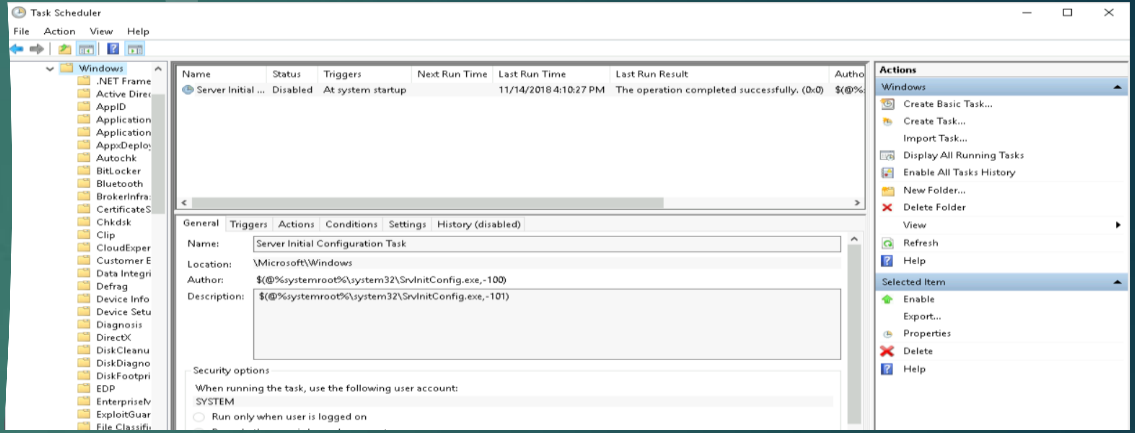
Event 4732, Microsoft Windows security auditing.

```
A member was added to a security-enabled local group.

Subject:
          Security ID:          NIKNAZ\Administrator
          Account Name:         Administrator
          Account Domain:       NIKNAZ
          Logon ID:             0xC0AEB8

Member:
```

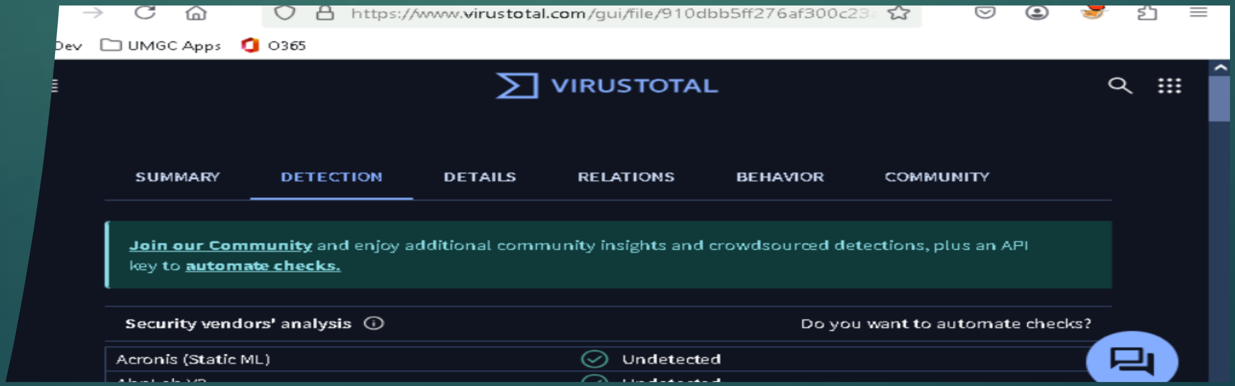
Log Name: Security
Source: Microsoft Windows security   Logged: 2/24/2025 7:10:20 PM
Event ID: 4732   Task Category: Security Group Management
Level: Information   Keywords: Audit Success
User: N/A   Computer: Niknaz
OpCode: Info
More Information: Event Log Online Help



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Autho
Server Initial ...	Disabled	At system startup		11/14/2018 4:10:27 PM	The operation completed successfully. (0x0)	$(@%:

Name: Server Initial Configuration Task
Location: \Microsoft\Windows
Author: $(@%systemroot%\system32\SrvInitConfig.exe,-100)
Description: $(@%systemroot%\system32\SrvInitConfig.exe,-101)

Security options
When running the task, use the following user account:
SYSTEM
○ Run only when user is logged on



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

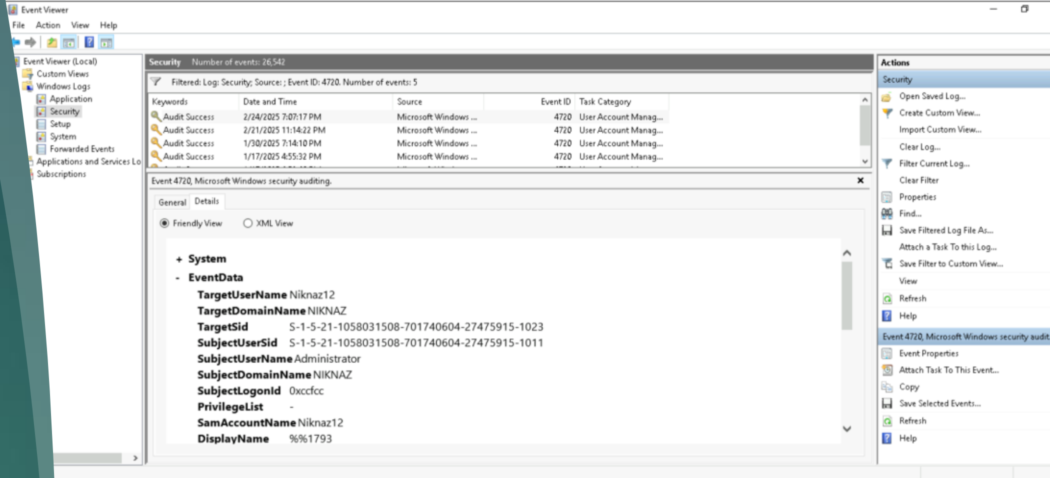
Security vendors' analysis   Do you want to automate checks?

Acronis (Static ML)   Undetected

Event Viewer – A New Administrator

Event Logs: New Administrator Account Creation

- Not part of regular system activity.
- Attackers often create such accounts for persistent access.
- Further investigation is needed to determine security risk.



Security Number of events: 26,542

Filtered: Log: Security; Source: ; Event ID: 4720. Number of events: 5

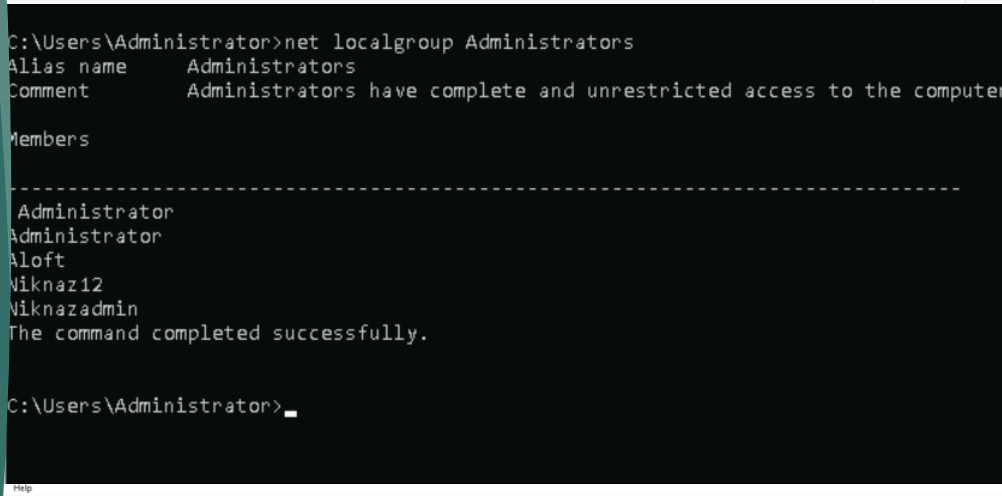
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	2/24/2025 7:07:17 PM	Microsoft Windows ...	4720	User Account Manag...
Audit Success	2/21/2025 11:14:22 PM	Microsoft Windows ...	4720	User Account Manag...
Audit Success	1/30/2025 7:14:10 PM	Microsoft Windows ...	4720	User Account Manag...
Audit Success	1/17/2025 4:55:32 PM	Microsoft Windows ...	4720	User Account Manag...

Event 4720, Microsoft Windows security auditing.

● Friendly View

+ System
- EventData

TargetUserName Niknaz12
TargetDomainName NIKNAZ
TargetSid S-1-5-21-1058031508-701740604-27475915-1023
SubjectUserSid S-1-5-21-1058031508-701740604-27475915-1011
SubjectUserName Administrator
SubjectDomainName NIKNAZ
SubjectLogonId 0xccfcc
PrivilegeList -
SamAccountName Niknaz12
DisplayName %%1793

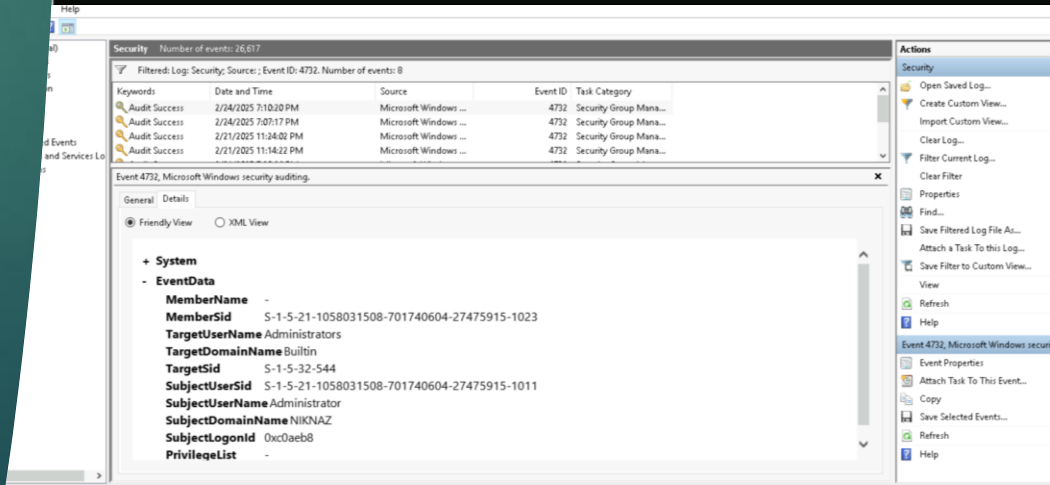


```
C:\Users\Administrator>net localgroup Administrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the compute

Members

-------------------------------------------------------------------------------
 Administrator
Administrator
Aloft
Niknaz12
Niknazadmin
The command completed successfully.


C:\Users\Administrator>_
```



Security Number of events: 26,617

Filtered: Log: Security; Source: ; Event ID: 4732. Number of events: 8

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	2/24/2025 7:10:20 PM	Microsoft Windows ...	4732	Security Group Mana...
Audit Success	2/24/2025 7:07:17 PM	Microsoft Windows ...	4732	Security Group Mana...
Audit Success	2/21/2025 11:24:02 PM	Microsoft Windows ...	4732	Security Group Mana...
Audit Success	2/21/2025 11:14:22 PM	Microsoft Windows ...	4732	Security Group Mana...

Event 4732, Microsoft Windows security auditing.

● Friendly View

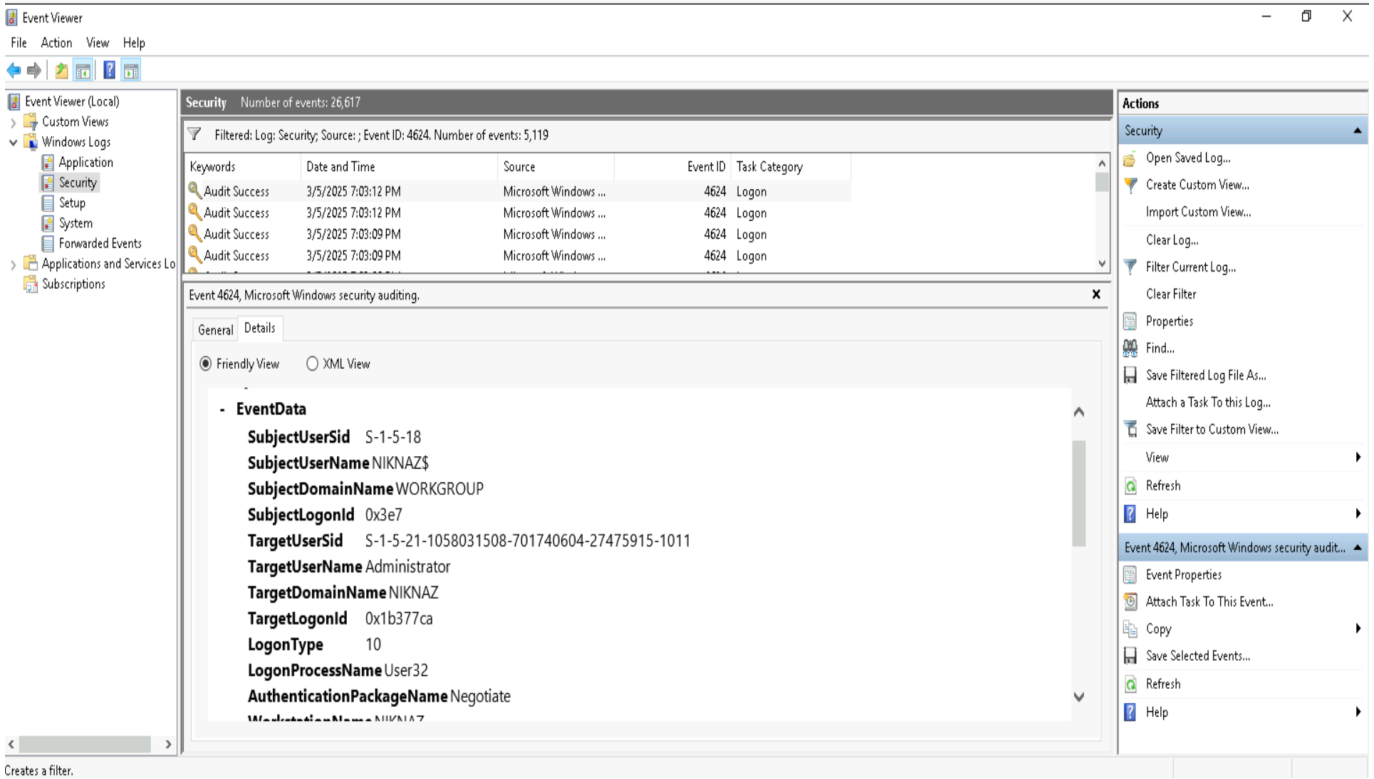
+ System
- EventData

MemberName -
MemberSid S-1-5-21-1058031508-701740604-27475915-1023
TargetUserName Administrators
TargetDomainName Builtin
TargetSid S-1-5-32-544
SubjectUserSid S-1-5-21-1058031508-701740604-27475915-1011
SubjectUserName Administrator
SubjectDomainName NIKNAZ
SubjectLogonId 0xc0aeb8
PrivilegeList -

Event Viewer – The When

Event Log Analysis

- Provides timestamps for critical system activities.
- Determines unauthorized logins and privilege escalations.
- Analyzes Event IDs 4624 and 4672.



Security Number of events: 26,617

Filtered: Log: Security; Source: ; Event ID: 4624. Number of events: 5,119

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	3/5/2025 7:03:12 PM	Microsoft Windows ...	4624	Logon
Audit Success	3/5/2025 7:03:12 PM	Microsoft Windows ...	4624	Logon
Audit Success	3/5/2025 7:03:09 PM	Microsoft Windows ...	4624	Logon
Audit Success	3/5/2025 7:03:09 PM	Microsoft Windows ...	4624	Logon

Event 4624, Microsoft Windows security auditing.

● Friendly View ○ XML View

```
- EventData
    SubjectUserSid            S-1-5-18
    SubjectUserName           NIKNAZ$
    SubjectDomainName         WORKGROUP
    SubjectLogonId            0x3e7
    TargetUserSid             S-1-5-21-1058031508-701740604-27475915-1011
    TargetUserName            Administrator
    TargetDomainName          NIKNAZ
    TargetLogonId             0x1b377ca
    LogonType                 10
    LogonProcessName          User32
    AuthenticationPackageName Negotiate
    WorkstationName           NIKNAZ
```

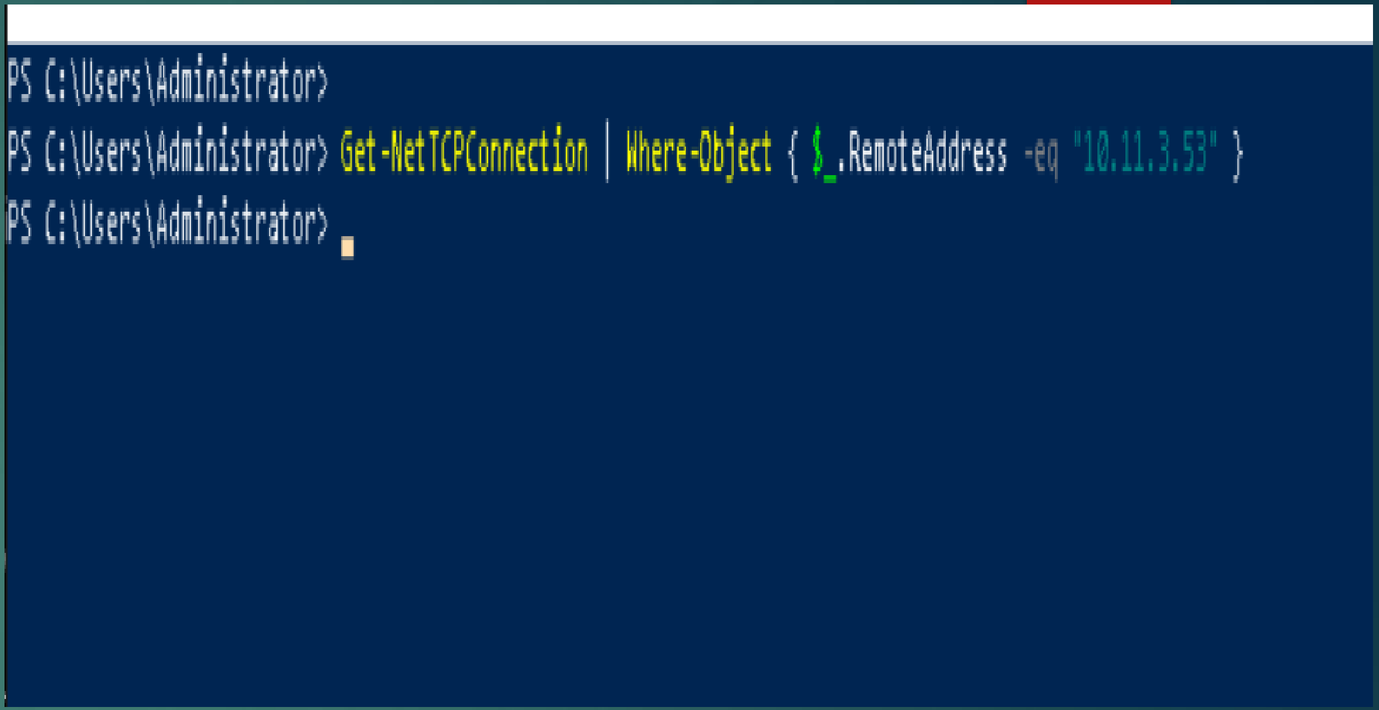
The Golden Nugget - Exfiltration

Forensic Examination Findings:

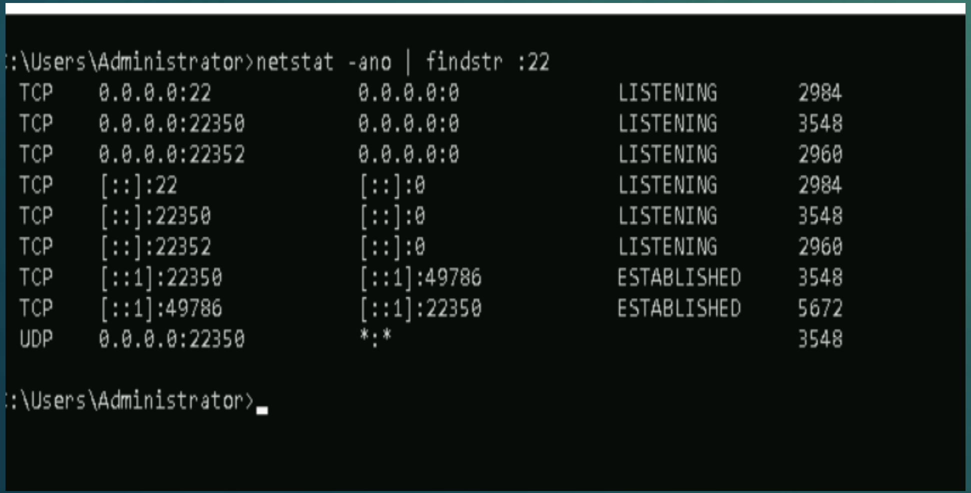
- Data exfiltration evidence found

.• SSH (port 22) connection established with external IP 10.11.3.53.

- Acquired sensitive information, including private key and stored credentials.
- Additional investigation is necessary to prevent further unauthorized access or data leaking.

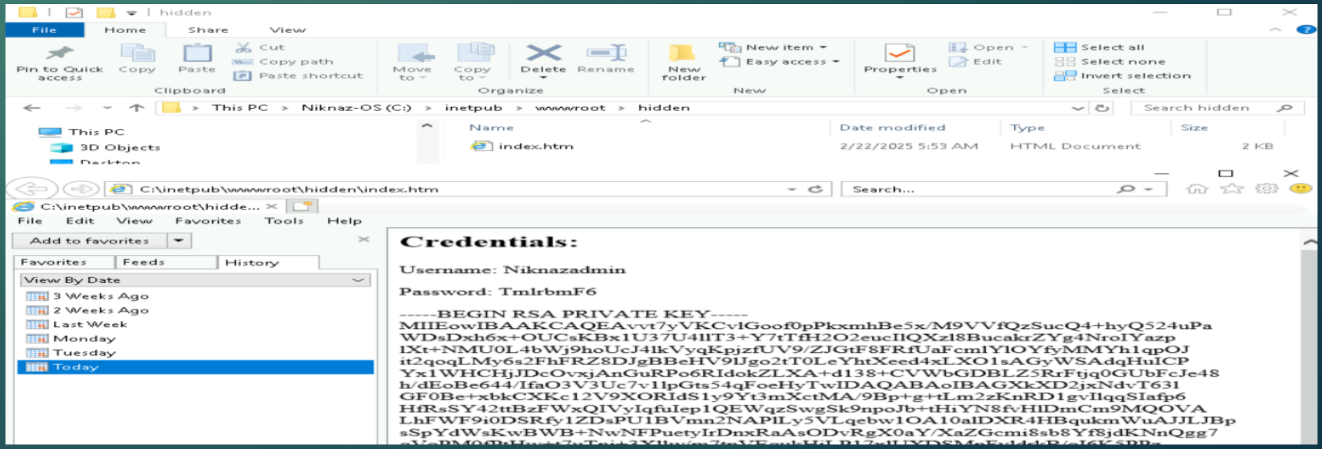


```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-NetTCPConnection | Where-Object { $_.RemoteAddress -eq "10.11.3.53" }
PS C:\Users\Administrator> _
```



```
:\Users\Administrator>netstat -ano | findstr :22
  TCP    0.0.0.0:22             0.0.0.0:0              LISTENING       2984
  TCP    0.0.0.0:22350          0.0.0.0:0              LISTENING       3548
  TCP    0.0.0.0:22352          0.0.0.0:0              LISTENING       2960
  TCP    [::]:22                [::]:0                 LISTENING       2984
  TCP    [::]:22350             [::]:0                 LISTENING       3548
  TCP    [::]:22352             [::]:0                 LISTENING       2960
  TCP    [::1]:22350            [::1]:49786            ESTABLISHED     3548
  TCP    [::1]:49786            [::1]:22350            ESTABLISHED     5672
  UDP    0.0.0.0:22350          *:*                                    3548

:\Users\Administrator>_
```



Name	Date modified	Type	Size
index.htm	2/22/2025 5:53 AM	HTML Document	2 KB

Credentials:

Username: Niknazadmin

Password: TmlrbmF6

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAvvt7yVKCvlGoof0pPkxmhBe5x/M9VVfQzSucQ4+hyQ524uPa
WDsDxh6x+OUCsKBx1U37U4lIT3+Y7tTfH2O2eucIlQXzl8BucakrZYg4NroIYazp
lXt+NMU0L4bWj9hoUcJ4lkVyqKpjzfUV9/ZJGtF8FRfUaFcmlYlOYfyMMYh1qpOJ
it2qoqLMy6s2FhFRZ8DJgBBeHV9lJgo2tT0LeYhtXeed4xLXO1sAGyWSAdqHuICP
Yx1WHCHjJDcOvxjAnGuRPo6RIdokZLXA+d138+CVWbGDBLZ5RrFtjq0GUbFcJe48
h/dEoBe644/IfaO3V3Uc7v1lpGts54qFoeHyTwIDAQABAoIBAGXkXD2jxNdvT631
GF0Be+xbkCXKc12V9XORIdS1y9Yt3mXctMA/9Bp+g+tLm2zKnRD1gvIlqqSIafp6
HfRsSY42ttBzFWxQIVyIqfuIep1QEWqzSwgSk9npoJb+tHiYN8fvHlDmCm9MQOVA
LhFWF9i0DSRfy1ZDsPU1BVmn2NAPlLy5VLqebw1OA10alDXR4HBqukmWuAJJLJBp
sSpYdWsKwBWB+NwNFPuetyIrDnxRaAsODvRgX0aY/XaZGcmi8sb8Yf8jdKNnQgg7
```

Summary

Status:

- *Fully Compromised*

Crucial Evidence:

- *The Startup Folder guarantees persistence - Niknaz.exe. /hidden/index.htm was visited and contains credentials, according to the IIS logs.*
- *Added to the Event Viewer Logs: Niknaz12, an unauthorized administrator account*
- *Updated Default Time.htm - Possible manipulation Discovered at 06:10:47 on February 22, 2025, the time of hacker access Proof of Data Exfiltration - Password and RSA key discovered*

Remedial Strategy:

- *System Rebuild* – Make sure all repairs are done.
- *Protect Against Malicious IPs* – Prevent further access.
- *Improve Tracking* – Improve monitoring and logging.

References

Batamig. (2024, November 27). Configure audit policies for Windows event logs - Microsoft Defender for Identity. Microsoft Learn. https://learn.microsoft.com/en-us/defender-for-identity/deploy/configure-windows-event-collection

Markruss. (2024, February 6). Autoruns - sysinternals. Microsoft Learn. https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns

Luttgens, J. T., Pepe, M., & Mandia, K. (2014). Incident response & computer forensics. McGraw-Hill Education Group.

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.

Grance, T., Kent, K., Kim, B., National Institute of Standards and Technology, & Booz Allen Hamilton. (2004). Computer Security Incident Handling Guide. In NIST Special Publication 800-61. http://www.eprivacy.com/lectures/IV-2_denialofservice/incident_prevention_and_response.pdf

SANS Institute, Filkins, B., & Filkins, B. (2018). An Evaluator’s Guide to NextGen SIEM (By SANS Institute & LogRhythm) [SANS Analyst Program]. https://www.sans.org/media/vendor/evaluator-039-s-guide-nextgen-siem-38720.pdf

Sikorski, M., & Honig, A. (2012). Practical malware analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press. https://www.cise.ufl.edu/~jnw/MalwareReverseEngineeringSyllabus.pdf