CISA Alert AA22-264A - Iranian HomeLand Justice APT Group's TTPs

By Huseyin Can YUCEEL

Published: 2022-10-03 · Archived: 2026-04-05 15:32:32 UTC

On September 21, 2022, The Cybersecurity and Infrastructure Security Agency (CISA) released a joint advisory with the Federal Bureau of Investigation (FBI) on the Iranian state-sponsored cyber threat group HomeLand Justice. The threat actors stayed hidden in the Albanian government networks for nearly 14 months and conducted cyber espionage, ransomware, and destructive malware attacks.

Picus Labs added attack simulations to the Picus Threat Library for techniques and malware used by the HomeLand Justice Threat group. In this blog post, we explained the tactics, techniques, and procedures used by the Iranian threat group.

HomeLand Justice Threat Group

HomeLand Justice is another Iranian state-sponsored cyber threat group like MuddyWater and OilRig. The threat actors' earliest known malicious activity was in May 2021, and the CISA advisory estimates that is when the threat actors gained initial access to the Albanian government networks. Since then, they had stayed hidden in the victim's network and conducted cyber espionage on Albanian citizens and government officials, including the prime minister of Albania. In July and September 2022, HomeLand Justice group launched ransomware and destructive malware attacks against their victim and announced their criminal activities over their website. The announcement and ransom note strongly indicated that these cyber attacks were politically motivated.

In their cyber attacks, HomeLand Justice group gained initial access to the victim's network by exploiting the Microsoft SharePoint CVE-2019-0604 vulnerability. It is a remote code execution vulnerability with a CVSS score of 9.8 (Critical). Then, threat actors established persistence via webshells and moved laterally in the network via RDP, SMB, and FTP. During their attack, HomeLand Justice group exfiltrated the victim's sensitive data and stole credentials. Lastly, they made their presence known by launching ransomware and destructive malware attacks.

TTPs Used by HomeLand Justice Threat Group

HomeLand Justice Threat group uses the following tactics, techniques, and procedures (TTPs) in the MITRE ATT&CK framework:

Tactic: Initial Access

- T1190 Exploit Public Facing Application

HomeLand Justice threat actors exploited Microsoft SharePoint Remote Code Execution (CVE-2019-0604) vulnerability. Although the vulnerability was discovered in 2019, unpatched assets still pose risks due to the vulnerability's high CVSS score (9.8 Critical). Organizations are advised to patch their Microsoft SharePoint update to the latest version without delay.

Tactic: Execution

- T1059 Command and Scripting Interpreter

HomeLand Justice threat actors use many batch files in their ransomware attacks. For ransomware attacks, two batch files with the same name "win.bat". One file establishes persistence by running the ransomware encryptor at system startup, and the other one changes the desktop background after the attack.

start /min C:\ProgramData\Microsoft\Windows\GoXml.exe 1 2 3 4 5 6 7

Example 1: Contents of "win.bat" used for persistence

Tactic: Persistence

- T1505.003 Web Shell

HomeLand Justice threat actors use webshells that are named pickers.aspx, error4.aspx, and ClientBin.aspx to establish persistence in the victim's compromised hosts.

- T1098 Account Manipulation

HomeLand Justice group used compromised credentials to access Microsoft Exchange accounts, including administrator accounts. This level of access allowed threat actors to create other accounts and add them to the "Organization

Management" role group.

Tactic: Defense Evasion

- T1112 Modify Registry

HomeLand Justice threat actors modify the following registry keys to disable Windows Defender.

Modified Registry Key	Modified Value
HKLM\SOFTWARE\Microsoft\Windows Defender\Features\TamperProtection	0
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware	1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Explorer\StartupApproved\Run\SecurityHealth	03 00 00 00 5D 02 00 00 41 3B 47 9D
HKLM\SOFTWARE\Microsoft\Windows Defender\DisableAntiSpyware	1
HKLM\System\CurrentControlSet\Services\WinDefend\Start	3
HKLM\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring	1

- T1562:001 Impair Defenses: Disable or Modify Tools

HomeLand Justice group uses disable-defender.exe to disable Windows Defender. Also, the encryptor called GoXml.exe stops the services using the commands below

set SrvLst=vss sql svc$ memtas mepos sophos veeam backup GxVss GxBlr GxFWD GxCVD GxCIMgr DefWatch ccEvtMgr ccSetMgr SavRoam RTVscan QBFCService QBIDPService ntuit.QuickBooks.FCS QBCFMonitorService YooBackup YooIT zhudongfangyu sophos stc_raw_agent VSNAPVSS VeeamTransportSvc VeeamDeploymentService VeeamNFSSvc veeam PDVFSService BackupExecVSSProvider BackupExecAgentAccelerator BackupExecAgentBrowser BackupExecDiveciMediaService BackupExecJobEngine BackupExecManagementService BackupExecRPCService AcrSch2Svc AcronisAgent CASAD2DWebSvc CAARCUpdateSvc

for %C in (%SrvLst%) do @net stop %C

set SrvLst=

set PrcLst=mysql sql oracle ocssd dbsnmp synctime agntsvc isqlplussvc xfssvccon mydesktopservice ocautoupds encsvc tbirdconfig mydesktopqos ocomm dbeng50 sqbcoreservice excel infopath msaccess mspub onenote outlook powerpnt steam thebat thunderbird visio winword wordpad notepad

for %C in (%PrcLst%) do @taskkill /f /im "%C.exe"

set PrcLst=

Example 2: Commands in "GoXml.exe" that disable certain services

Tactic: Credential Access

- T1003.001 OS Credential Dumping: LSASS Memory

HomeLand Justice threat actors use Mimikatz to dump LSASS memory which can be used to extract credentials stored in the compromised host.

Tactic: Discovery

- T1046 Network Service Discovery

HomeLand Justice group used "Advanced Port Scanner" to discover open ports and services in the victim's environment.

Tactic: Lateral Movement

- T1021.001 Remote Services: Remote Desktop Protocol

HomeLand Justice threat actors primarily used Remote Desktop Protocol (RDP) to move laterally in the victim's network.

- T1021.001 Remote Services: SMB/Windows Admin Shares

HomeLand Justice threat actors also used SMB protocol to move laterally in the victim's network.

Tactic: Exfiltration

- T1048.003 Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol

HomeLand Justice threat actors were able to access administrator accounts of Microsoft Exchange service via compromised credentials. Using this access, they searched and exfiltrated emails and other sensitive data belonging to the victim.

Tactic: Impact

- T1486 Data Encrypted for Impact

HomeLand Justice threat actors used an executable called Mellona.exe to spread GoXml.exe encryptor to internal assets in the victim's network. GoXml.exe encrypted all files in the infected hosts and left a ransom note named "How_To_Unlock_MyFiles.txt" in each folder that was encrypted.

- T1490 Inhibit System Recovery

The encryptor GoXml.exe also deletes volume shadow copies to prevent the victim from recovering the encrypted files.

- T1485 Data Destruction

HomeLand Justice threat actors used ZeroClear disk wiper malware to delete data via raw access to the hard drive.

How Picus Helps Simulate HomeLand Justice Cyber Attacks?

We also strongly suggest simulating HomeLand Justice cyber threats to test the effectiveness of your security controls against ransomware attacks using the Picus Complete Security Control Validation Platform. You can test your defenses against HomeLand Justice threat actors and other Iranian state-sponsored APT threats such as MuddyWater, OilRig, and PHOSPHORUS within minutes with a 14-day free trial of the Picus Platform.

Picus Threat Library includes the following threats for HomeLand Justice Threat Group:

Threat ID	Action Name	Attack Module
36690	HomeLand Justice Threat Group Campaign 2022	Endpoint
48961	HomeLand Justice Threat Group Campaign Malware Download Threat	Network Infiltration
52959	HomeLand Justice Threat Group Campaign Email Threat	Email Infiltration (Phishing)

Start simulating emerging threats today and get actionable mitigation insights with a **14-day free trial** of Picus Complete Security Control Validation Platform.

Indicators of Compromises

SHA-256	MD5	SHA-1
e1204ebbd8f15dbf5f2e41dddc5337e3182fc4daf75b05acc948b8b965480ca0	7b71764236f244ae971742ee1bc6b098	f22a7ec80fbfdc4d8ed7961
f116acc6508843f59e59fb5a8d643370dce82f492a217764521f46a856cc4cb5	bbe983dba3bf319621b447618548b740	5d117d8ef075f3f8ed1d4ec

63dd02c371e84323c4fd9a161a75e0f525423219e8a6ec1b95dd9eda182af2c9	0738242a521bdfe1f3ecc173f1726aa1	683eaec2b3bb5436f00b21
7ad64b64e0a4e510be42ba631868bbda8779139dc0daad9395ab048306cc83c5	a9fa6cfdba41c57d8094545e9b56db36	e03edd9114e7a0138d130
bad65769c0b416bb16a82b5be11f1d4788239f8b2ba77ae57948b53a69e230a6	1635e1acd72809479e21b0ac5497a79b	14b8c155e01f25e749a972
ec4cd040fd14bff86f6f6e7ba357e5bcf150c455532800edf97782836e97f6d2	18e01dee14167c1cf8a58b6a648ee049	fce0db6e66d227d3b82d45
45bf0057b3121c6e444b316afafdd802d16083282d1cbfde3cdbf2a9d0915ace	60afb1e62ac61424a542b8c7b4d2cf01	e866cc6b1507f21f688ecc
3c9dc8ada56adf9cebfc501a2d3946680dcb0534a137e2e27a7fcb5994cd9de6	8f6e7653807ebb57ecc549cef991d505	5e061701b14faf9adec9dd
cad2bc224108142b5aa19d787c19df236b0d12c779273d05f9b0298a63dc1fe5	e9b6ecbf0783fa9d6981bba76d949c94	49fd8de33aa0ea0c7432d6
	78562ba0069d4235f28efd01e3f32a82	
	8f766dea3afd410ebcd5df5994a3c571	
	59a85e8ec23ef5b5c215cd5c8e5bc2ab	
	81e123351eb80e605ad73268a5653ff3	