Iranian Threat Actors & Healthcare

November 03, 2022

Agenda

- Analysis of the Iranian Cyber Attack Landscape

- Iranian Cyber Threat Actors

- Iran Cyberattacks in the News

- Attack Analysis

- Tactics, Techniques, and Procedures (TTPs) & Mitigations

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center
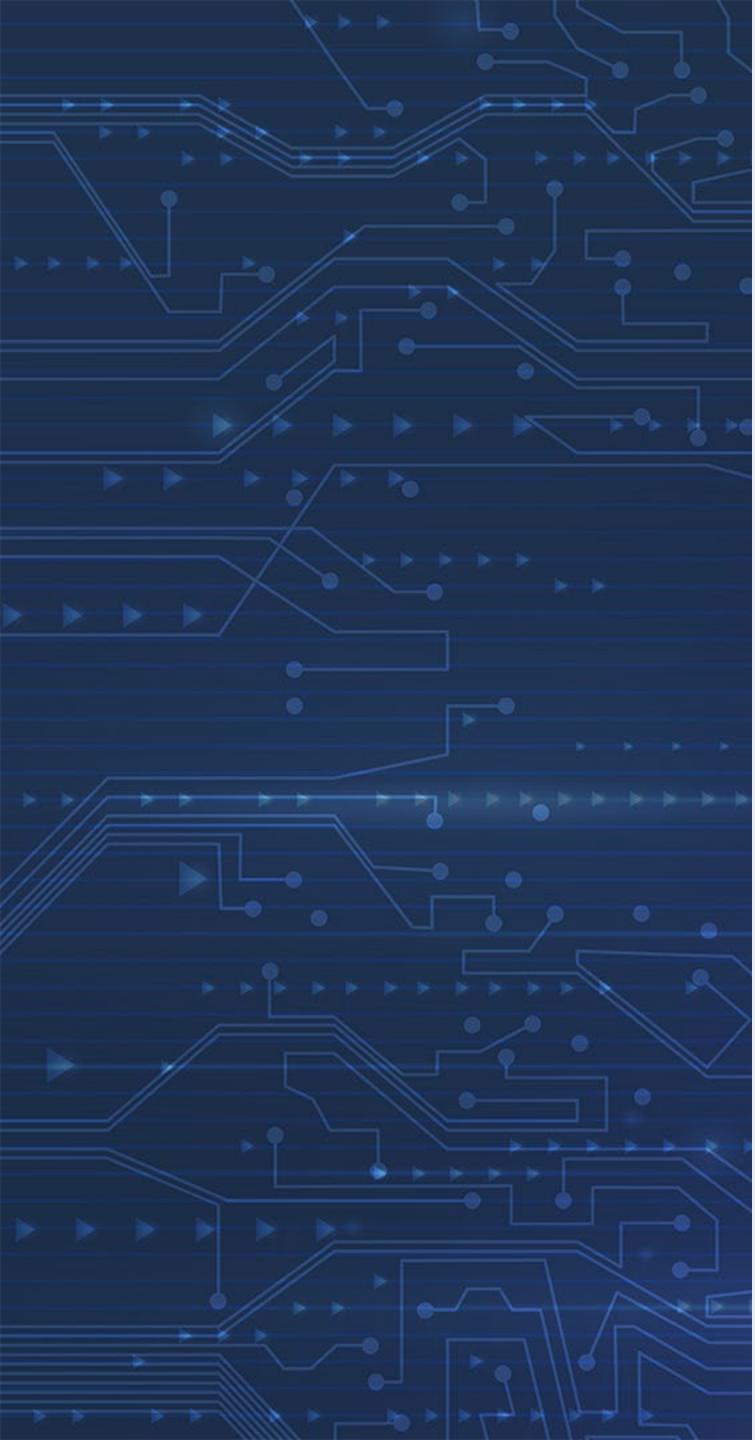
Analysis of the Iranian Cyber Attack Landscape

Iranian Cyber Attack Landscape

- Historically risk-averse actor

- Cyber provides a means to exploit enemy vulnerabilities while minimizing the risk of escalation/retaliation

- Infamous for wiper malware as well as retaliatory attack strategies

- Known to engage in:
  - Website defacement
  - Spear phishing
  - Distributed denial-of-service (DDoS)
  - Theft of personally identifiable information (PII)
  - Malware
  - Social media-driven operations

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Iranian Cyber Attack Landscape: Two Recent and Notable Agreements

- January 2021
  - Signed a cooperation agreement on cybersecurity and information and communications technology with Russia establishing:
    - Technology transfer
    - Combined training
    - Cybersecurity cooperation
  - Agreement largely defense oriented and driven by a mutual:
    - Animosity toward the U.S.
    - Desire for greater censorship
    - Ambition to reduce dependence on Western technology

- March 2021
  - Signed a 25-year cooperation agreement, establishing a partnership focused on economic and defense collaboration, including:
    - Joint training
    - Exercises
    - Research
    - Weapons development
    - Intelligence sharing
  - China has offered to help Iran deploy a greater internet censorship

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center
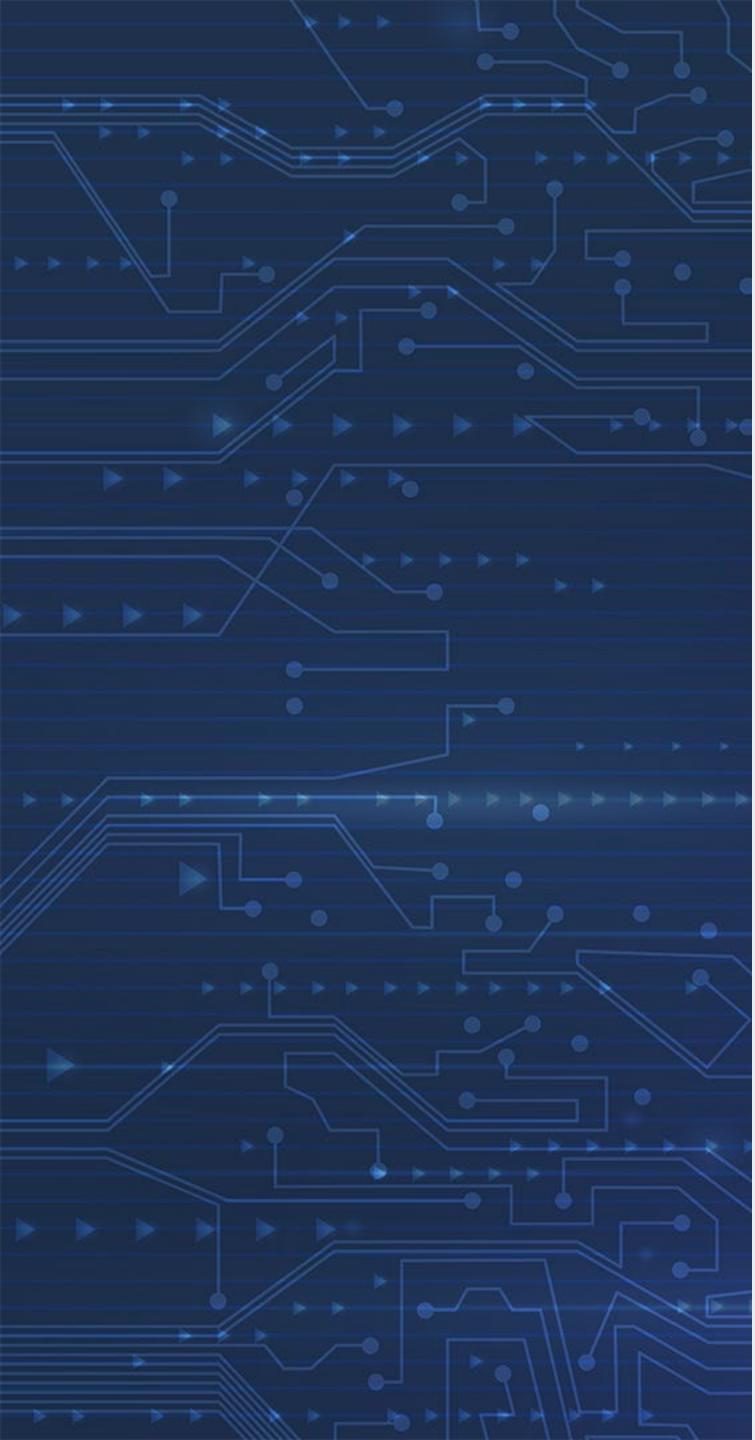
Iranian Cyber Threat Actors

Charming Kitten

- **Association:** Islamic Revolutionary Guard Corps (IRGC)
- **AKA:** TA453, Cobalt Illusion, Magic Hound, ITG18, Phosphorus, Newscaster, APT35
- **Known Targets:** Medical Researchers, Dissidents, Diplomats, Human Rights Activists, Media, Government, Military, Energy, Telecommunications
- **Tactics, Techniques, & Procedures (TTPs):**
  - Spear phishing as a common initial intrusion vector (often using lures related to health care, job postings, resumes, or password policies)
  - Leveraging fake personas and social media platforms to interact with their targets
  - Watering hole attacks using compromised legitimate websites that are relevant to their targeted victims
  - Impersonations of popular online sites (Google, Microsoft, Yahoo) to harvest user credentials

Source: Foreign Policy

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Static Kitten

- **AKA:** Earth Vetala, Mercury, MuddyWater, Seedworm, TEMP.Zagros

- **Known Targets:** Telecommunications, IT, Oil and Gas, NGOs, Tourism, Academia

- **Tactics, Techniques, & Procedures (TTPs):**
  - Spear phishing as a common initial intrusion vector
  - Use of PowerShell backdoor known as POWERSTATS
  - Weaponization of stolen legitimate documents
  - Use of legitimate file-sharing services to distribute files containing remote access software in order to distribute malware

Source: Business Insider

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Pioneer Kitten

- **AKA:** UNC757, Parisite, Fox Kitten

- **Known Targets:** Healthcare, Technology, Government, Defense, Aviation, Media, Academic, Engineering, Consulting & Professional Services, Chemical, Manufacturing, Financial Services, Insurance, Retail

- **Tactics, Techniques, & Procedures (TTPs):**
  - Exploitation of VPNs and other network appliances
  - Use of Secure Shell (SSH) tunneling to facilitate RDP (Remote Desktop Protocol) access to victims
  - Use of custom open-source and legitimate native software tools
  - CVE-2019-11510, CVE-2019-19781, & CVE-2020-5902

Source: CrowdStrike

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Remix Kitten

- **Association:** Iranian Ministry of Intelligence and Security (MOIS), Rana Intelligence Computing

- **AKA:** APT39, Chafer, Cadelle, ITG07

- **Known Targets:** Telecommunications, Aviation, IT, Travel, Government

- **Tactics, Techniques, & Procedures (TTPs):**
  - Spear phishing
  - Leveraging of domains resembling legitimate web services and businesses relevant to intended target
  - Structured Query Language (SQL) injection attacks via front-end web servers
  - Use of custom backdoors combined with publicly available software tools
  - Exploitation of a target's vulnerable web servers to install web shells
  - Use of stolen legitimate credentials to compromise externally facing Outlook Web Access resources

Source: CrowdStrike

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Helix Kitten

- **AKA:** Cobalt Gypsy, Irn2, Helix Kitten, Apt34
- **Known Targets:** Government, Finance, Energy, Telecommunications, Oil and Gas
- **Tactics, Techniques, & Procedures (TTPs):**
  - Custom PowerShell implant, Helminth
  - Use of malicious job opportunity documents as lures to deliver malware (often using social media as an initial delivery mechanism)
  - Spear phishing and social engineering
  - DNS exfiltration using both custom-built and open-source software tools
  - Extensive use of DNS tunneling for command and control (C2)
  - Email-based C2 using Exchange Web Services and steganography to insert data and commands into image files attached to emails
  - Credential harvesting and use of compromised accounts

Source: CrowdStrike

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Refined Kitten

- **Association:** Islamic Revolutionary Guard Corps (IRGC)
- **AKA:** Elfin, Magnallium, Holmium, APT33
- **Known Targets:** Aviation, Manufacturing, Engineering, Energy, Petrochemical
- **Tactics, Techniques, & Procedures (TTPs):**
  - Shamoon malware
  - Spear phishing as an initial intrusion vector
  - Brute-force and password-spraying attacks
  - Use of drive-wiping malware
  - Leveraging botnets, private VPNs, and cloud-hosted proxies to enhance obfuscation and operational security
  - Multi-staged attacks using weaponized documents, known productivity software vulnerabilities, and PowerShell backdoors

Source: Cyware

Magic Kitten and Infy

Magic Kitten

- **Known Targets:** Hospitals, Political Dissidents, Infrastructure
- **Tactics, Techniques, & Procedures (TTPs):**
  - Social engineering
  - Malware
  - Relay network to hide operations

Infy

- **AKA:** Prince of Persia, Foudre, Operation Mermaid
- **Known Targets:** Activists, Dissidents, Press, Government Entities, Private Companies
- **Tactics, Techniques, & Procedures (TTPs):**
  - Foudre malware and second-stage payload Tonnerre
  - Distribution of malicious documents containing Infy malware through spear phishing attacks
  - Use of keylogger malware with a failover C2 communication system
  - Use of an RSA signature verifying algorithm to check the veracity of a C2 domain
  - Watering hole attacks using compromised legitimate websites

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

UNC3890

- **Known Targets:** Healthcare, Shipping, Government, Energy

- **Tactics, Techniques, & Procedures (TTPs):**
  - Social engineering lures
  - Watering holes
  - Fake commercials for AI-based robotic dolls
  - Credentials harvesting by masquerading as legitimate services
  - Sugarush – a backdoor written to establish a connection with an embedded C2 and to execute CMD commands
  - Sugardump – a credential harvesting utility, capable of password collection from Chromium-based browsers

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**
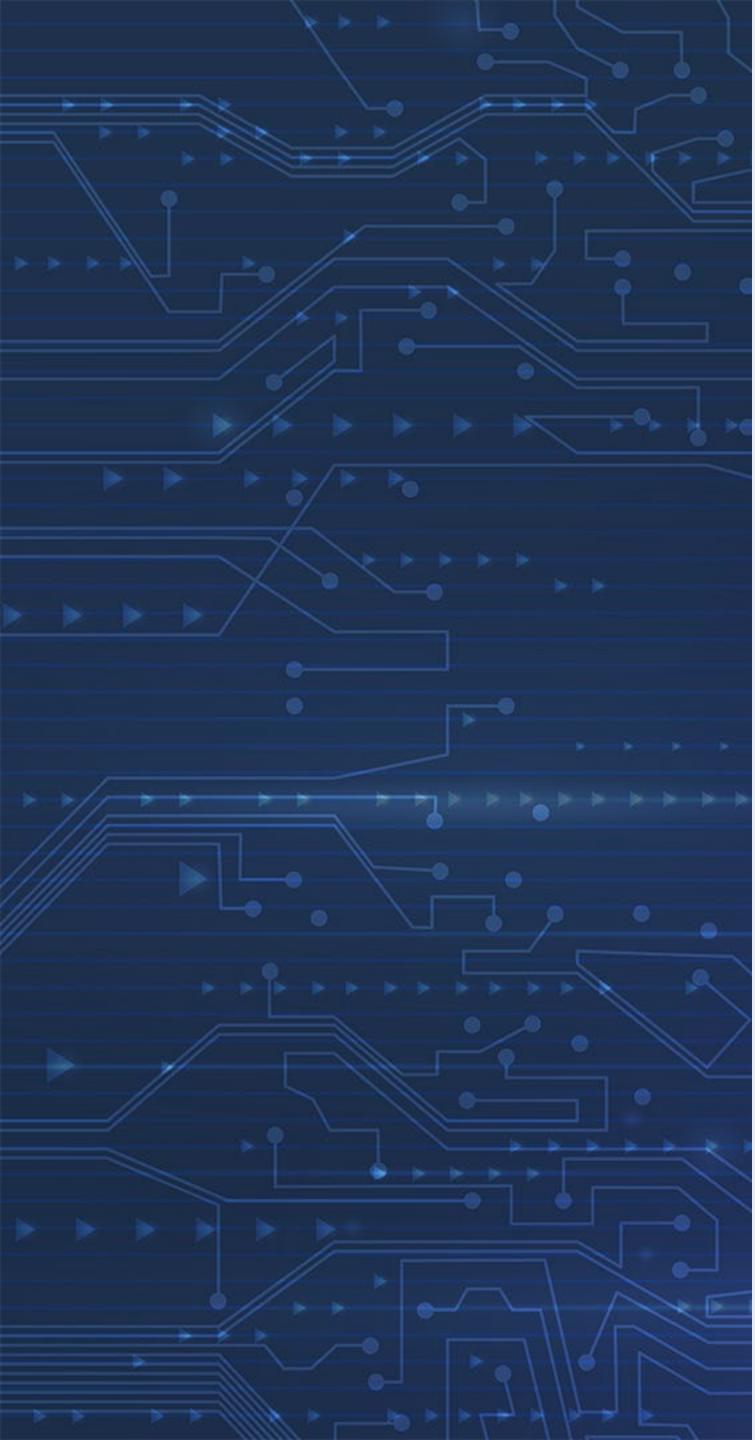
Iran Cyberattacks in the News

Thwarted Attack on a Children's Hospital and Facebook Attack Campaign

- Thwarted attack on a children's hospital
  - Iranian hackers exploited a Fortigate appliance to access the environmental control networks of a U.S.-based children's hospital
  - Accessed known user accounts at the hospital from an IP address that the FBI associates with the Iranian government

- Tortoiseshell Facebook attack campaign
  - Tracked and partially disrupted an Iranian attack campaign that used accounts to pose as recruiters and draw in U.S. targets before sending them either malware-infected files, or tricking them into entering sensitive credentials on phishing sites
  - The attackers pretended to work in hospitality, medicine, journalism, NGOs, and at airlines
  - Largely targeted Americans and Europeans
  - Hackers identified as the group Tortoiseshell, believed to work on behalf of the Iranian government

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Iranian Hackers Use Fake Personas to Make Phishing Attacks More Realistic

On the right: An example of the attack shared in Proofpoint's report. The attacker/sender is masquerading as the Director of Research at the Foreign Policy Research Institute (FRPI) and has the Director of Global Attitudes Research at the Pew Research Center—also the attacker—cc'ed.

Source: Bleeping Computer

Indictment from the U.S. Government

In September 2022, the U.S. imposed another round of sanctions against Iran for its recent APT activity.

Roadsweep ransomware note from the "HomeLand Justice" attack on the Albanian government.
Source: Mandiant
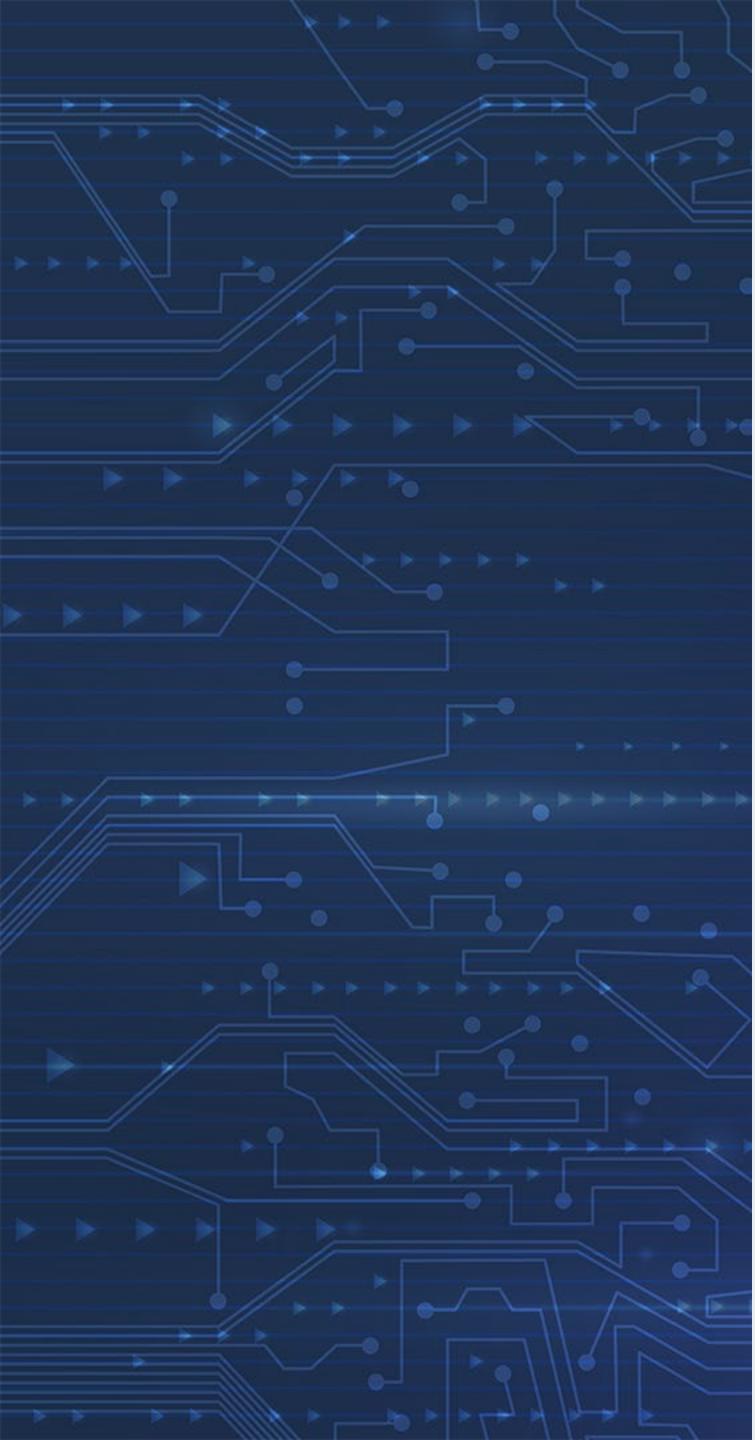
Attack Analysis

Iranian Cyber Operations Against the Government of Albania

Attack Analysis: An Overview

- July 2022
  - Iranian state cyber actors—identifying as HomeLand Justice—launched a destructive cyberattack against the Government of Albania, rendering websites and services unavailable.
  - An FBI investigation indicated that Iranian state cyber actors acquired initial access to the victim's network ~14 months before launching the destructive cyberattack, which included a ransomware-style file encryptor and disk-wiping malware.
  - The actors maintained continuous network access for approximately a year, periodically accessing and exfiltrating email content.

Source: The Conversation

Attack Analysis: Phases I and II

- Phase I
  - Approximately fourteen months before the attack
  - Initial access obtained via exploitation of an Internet-facing Microsoft SharePoint that exploited CVE-2019-0604

- Phase II
  - Stage 1: Persistence and Lateral Movement
    - Approximately several days to two months after initial compromise
    - Several .aspx web shells used to maintain persistence
    - RDP, SMB, and FTP used for lateral movement throughout the victim environment
  - Stage 2: Exchange Server Compromise
    - Approximately one to six months after initial compromise
    - Compromised Microsoft Exchange account used to run searches on various mailboxes; attacker searched for administrator accounts
    - A compromised account was also used to create a new Exchange account and add it to the Organization Management role group

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Attack Analysis: Phase II

- Phase II (continued):
    - Stage 3: Likely Email exfiltration
        - Approximately eight months after initial compromise
        - Thousands of HTTP POST requests to Exchange servers of the victim organization
        - The FBI observed the client transferring roughly 70-160 MB of data and the server transferring roughly 3-20 GB of data
    - Stage 4: VPN activity
        - Approximately twelve to fourteen months after initial compromise
        - Connections made to IP addresses belonging to the victim organization's Virtual Private Network (VPN) appliance
        - Execution of advanced_port_scanner.exe
        - The FBI found evidence of Mimikatz usage and LSASS dumping
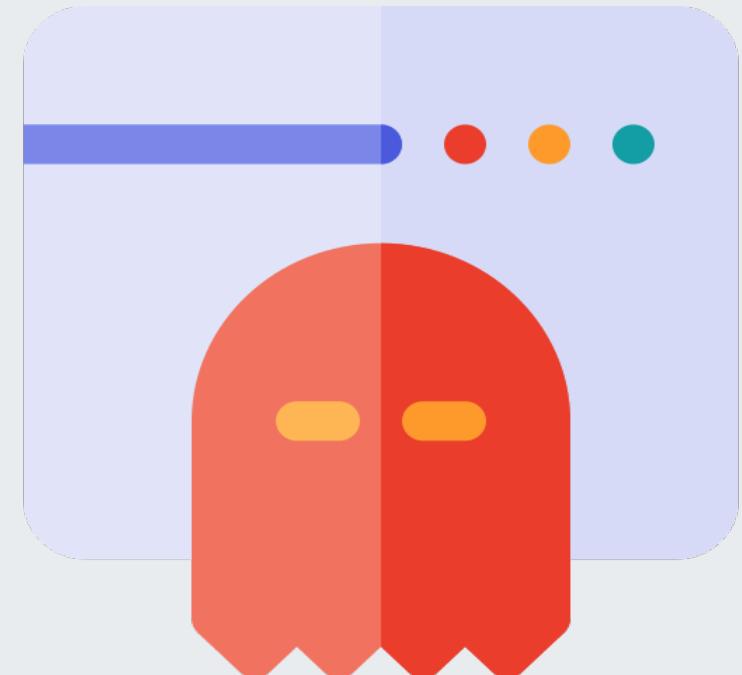
Attack Analysis: Phase III

- June 2022
  - HomeLand Justice created a website and multiple social media profiles posting anti-Mujahedeen-el-Khalq (MEK) messages

- July 18, 2022
  - The Albanian government published a statement announcing that it had to "temporarily close access to online public services and other government websites" due to disruptive cyber activity
  - HomeLand Justice claimed credit for this activity

- July 19, 2022
  - While network defenders identified and responded to the malicious activity, cyber actors deployed a new version of the ZeroClear destructive malware
    - ZeroClear takes in command line arguments from the operator, which results in the corruption of the file system using the RawDisk driver

- July 21, 2022
  - HomeLand Justice leveraged the website "homelandjustice.ru" to publish news stories on the ransomware operation against the Albanian government

Why should our taxes be spent on terrorists of Durres?
Contact us: 0682031701 , 0682099450
0697047470 , 0682030272

Pse duhet të shpenzohen taksat tona për terroristët e Durrësit?
Na kontaktoni: 0682031701 , 0682099450
0697047470 , 0682030272

@homelandjustice

Source: Mandiant

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Attack Analysis: Phase III (continued)

- July 22
  - Roadsweep was submitted to a public malware repository from Albania
  - It dropped a ransom note with the text: "Why should our taxes be spent on the benefit of Durrës terrorists?"
  - Durrës is a port city and the second most populous city in Albania. It is also the MEK headquarters and was the location for the World Summit of Free Iran conference on July 23-24
  - The attack introduced a previously unknown backdoor called Chimneysweep that shares code with Roadsweep and is used for C2, taking screenshots, listing and collecting files, spawning a reverse shell, and supporting keylogging functionality
- Late July
  - HomeLand Justice claimed credit for the entire operation on its Telegram channel
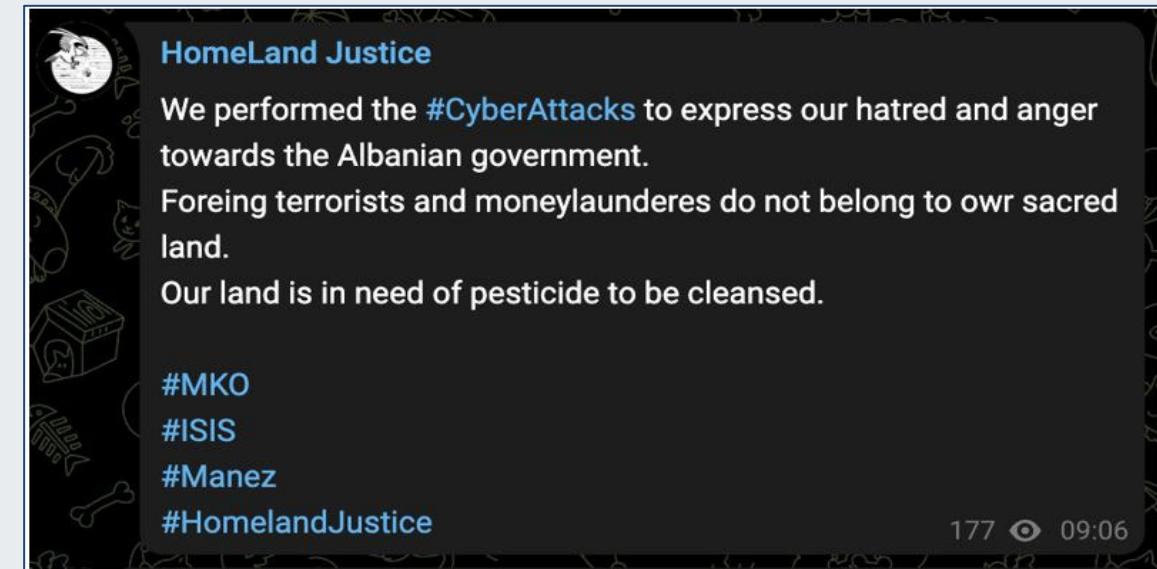
> **HomeLand Justice**
>
> We performed the #CyberAttacks to express our hatred and anger towards the Albanian government.
> Foreing terrorists and moneylaunderes do not belong to owr sacred land.
> Our land is in need of pesticide to be cleansed.
>
> #MKO
> #ISIS
> #Manez
> #HomelandJustice
>
> 177 👁 09:06

Source: Mandiant

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Attack Analysis: Aftermath

- **From late July to mid-August 2022**
  - Social media accounts associated with HomeLand Justice advertised Albanian Government information for release, posting a poll asking respondents to select the government information to be released, and then releasing that information either in a .zip file or in a screen recording
- **September 2022**
  - Iranian cyber actors launched another wave of cyberattacks against the Government of Albania, using TTPs and malware similar to that of the cyberattacks in July
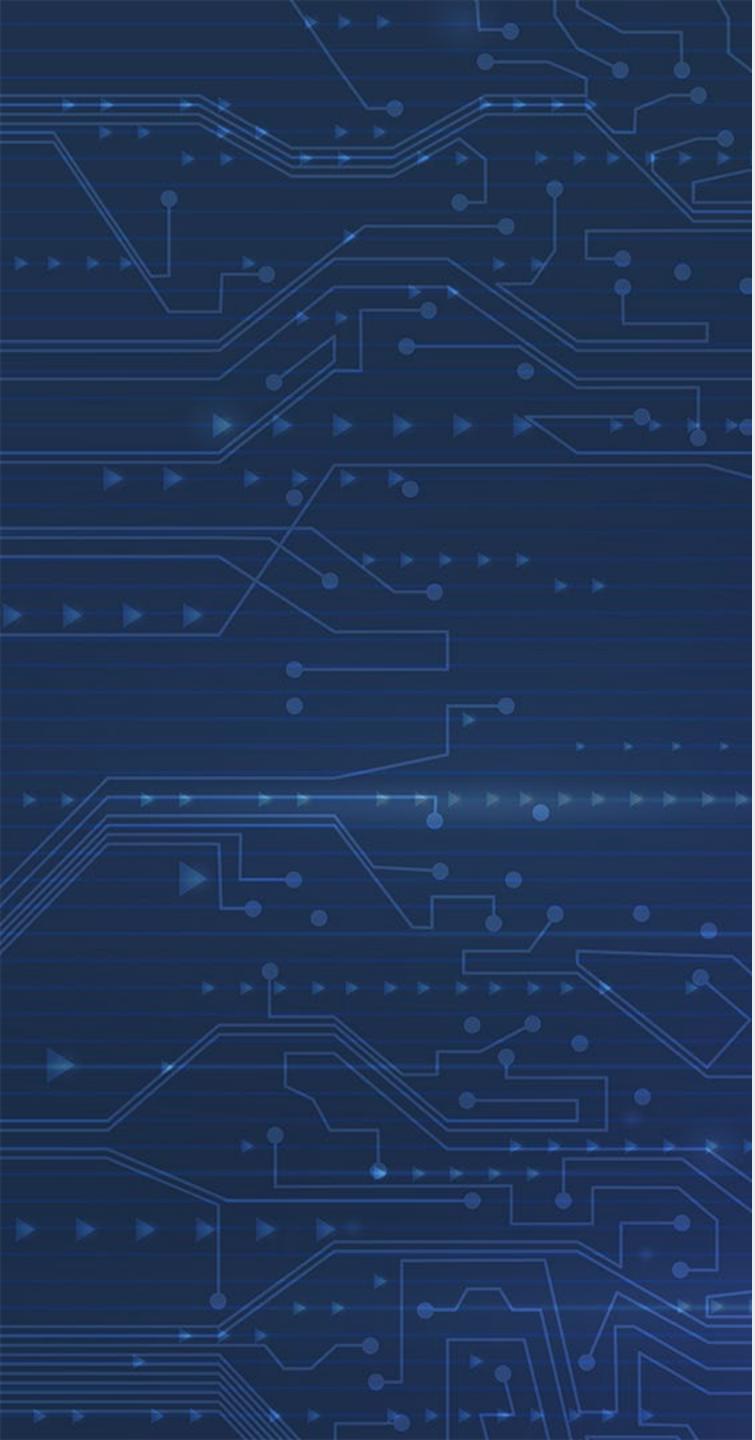
Tactics, Techniques, and Procedures (TTPs) & Mitigations

Tactics, Techniques, and Procedures (TTPs)

- Spear phishing as a common initial intrusion vector
- Social engineering lures
- Watering holes
- Exploiting vulnerabilities for initial access:
  - *Log4j:* CVE-2021-44228, CVE-2021-45046, CVE-2021- 45105
  - *Microsoft Exchange ProxyShell:* CVE-2021-34473, CVE-2021- 34523, CVE-2021-31207
  - *Microsoft Exchange:* CVE-2021- 31196, CVE-2021-31206, CVE-2021-33768, CVE-2021-33766, CVE-2021-34470
  - *Fortinet FortiOS:* CVE-2018-13379, CVE-2020-12812, CVE-2019-5591
- Utilization of legitimate file-sharing services to distribute files containing remote access software in order to distribute malware
- Extensive use of DNS tunneling for command and control (C2)

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Tactics, Techniques, and Procedures (TTPs), Part 2

- Multi-staged attacks using weaponized documents, known productivity software vulnerabilities, and PowerShell backdoors
- Use of drive-wiping malware
- Leveraging of domains resembling legitimate web services and businesses relevant to intended target
- Credential harvesting and use of compromised accounts
- Leveraging fake personas and social media platforms to interact with their targets
- Use of PowerShell backdoor known as POWERSTATS

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**
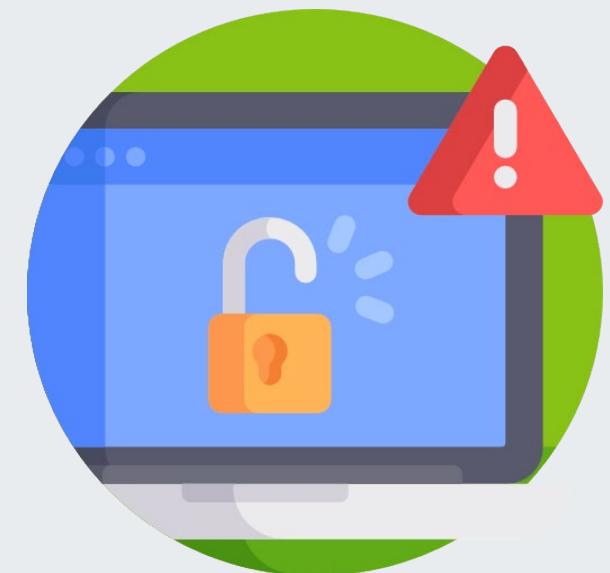
Mitigations

- User training on spotting phishing and how to report it, as well as training on social engineering
- Review Log4j vulnerabilities, especially CVE-2021-44228, CVE-2021-45046, and CVE-2021-45105
- Review Microsoft Exchange ProxyShell vulnerabilities, including CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207
- Review Microsoft Exchange vulnerabilities, including CVE-2021- 31196, CVE-2021-31206, CVE-2021-33768, CVE-2021-33766, and CVE-2021-34470
- Investigate exposed Microsoft Exchange servers, both patched and unpatched, for compromise
- Review Fortinet FortiOS vulnerabilities, including CVE-2018-13379, CVE-2020-12812, and CVE-2019-5591
- Look for WinRAR and FileZilla in unexpected locations

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Mitigations

- Implement network segmentation to restrict a malicious threat actor's lateral movement
- Maintain offline (i.e., physically disconnected) backups of data, and regularly test backup and restoration
- Ensure all backup data is encrypted, immutable (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure
- Review antivirus logs for indications that they were unexpectedly turned off
- Audit user accounts with administrative privileges and configure access controls under the principles of least privilege and separation of duties
- Have an IR (Incident Response) plan and regularly conduct exercises that utilize it
- Use strong passwords and implement multi-factor authentication
- Require administrator credentials to install software

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Reference Materials

References

- "Advanced Persistent Threats (APTs)," Mandiant. N.D. https://www.mandiant.com/resources/insights/apt-groups

- Ahmed, Debra. "Iran's COBALT MIRAGE Threat Group Behind Ransomware Attacks in US," HackRead. 16 May 2022. https://www.hackread.com/irans-cobalt-mirage-threat-group-ransomware-attacks-us/

- Anderson, Colin and Karim Sadjadpour. "Iran's Cyber Threat," Carnegie Endowment for International Peace. 04 January 2018. https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf

- "APT39," Mitre Att&ck. N.D. https://attack.mitre.org/groups/G0087/

- Bertrand, Natasha. "These Are The Hacker Groups That Should Be Keeping You Up At Night," Business Insider. 27 October 2014. https://www.businessinsider.com/hacker-groups-you-should-be-worrying-about-2014-10

- Haeghebaert, Emiel, Luke Jenkins, Ben Read, and Alice Revelli. "Likely Iranian Threat Actor Conducts Politically Motivated Disruptive Activity Against Albanian Government Organizations," Mandiant. 04 August 2022. https://www.mandiant.com/resources/blog/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

References

- "Hello, Charming Kitten: Alleged HBO hacker, two others possibly linked to Iranian APT group," Cyware. 05 December 2017. https://cyware.com/news/hello-charming-kitten-alleged-hbo-hacker-two-others-possibly-linked-to-iranian-apt-group-3a03969f

- Greenberg, Andy. "Facebook catches Iranian spies catfishing US military targets," ArsTechnica. 17 July 2021. https://arstechnica.com/information-technology/2021/07/facebook-catches-iranian-spies-catfishing-us-military-targets/

- Groll, Elias. "Meet 'Charming Kitten,' the Iranian Hackers Linked to Air Force Defector," Foreign Policy. 15 February 2019. https://foreignpolicy.com/2019/02/15/meet-charming-kitten-the-iranian-hackers-linked-to-air-force-defector/

- "Iran Cyber Threat Overview and Advisories," CISA. N.D. https://www.cisa.gov/uscert/iran

- "Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations," CISA. 14 September 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-257a

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

References

- "Iranian State Actors Conduct Cyber Operations Against the Government of Albania," CISA. 21 September 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-264a

- IronNet Threat Research and Intelligence Teams, with lead analysis by Morgan Demboski, "Analysis of the Iranian cyber-attack landscape," IronNet. 14 September 2021. https://www.ironnet.com/blog/iranian-cyber-attack-updates

- Jercich, Kat. "CISA issues alert for Iran-sponsored hacker group targeting healthcare," Healthcare IT News. 18 November 2021. https://www.healthcareitnews.com/news/cisa-issues-alert-iran-sponsored-hacker-group-targeting-healthcare

- Karagiannopoulos, Vasileios. "How real is the threat of cyberwar between Iran and the US?," The Conversation. 10 January 2020. https://theconversation.com/how-real-is-the-threat-of-cyberwar-between-iran-and-the-us-129573

- "Magic Hound," Mitre Att&ck. N.D. https://attack.mitre.org/groups/G0059/

- Mandiant Israel Research Team. "Suspected Iranian Actor Targeting Israeli Shipping, Healthcare, Government and Energy Sectors," Mandiant. 17 August 2022. https://www.mandiant.com/resources/blog/suspected-iranian-actor-targeting-israeli-shipping

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

References

- McKeon, Jill. "CISA: Iranian Government-Sponsored Threat Actors Targeting Healthcare," Health IT Security. 17 November 2021. https://healthitsecurity.com/news/cisa-iranian-government-sponsored-threat-actors-targeting-healthcare

- Meyers, Adam. "Meet CrowdStrike's Adversary of the Month for November: HELIX KITTEN," CrowdStrike. 27 November 2018. https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-november-helix-kitten/

- Meyers, Adam. "Who is REFINED KITTEN?," CrowdStrike. 12 December 2019. https://www.crowdstrike.com/blog/who-is-refined-kitten/

- Microsoft Threat Intelligence Center (MSTIC). "Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021," Microsoft. 16 November 2021. https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

References

- "MuddyWater," Mitre Att&ck. N.D. https://attack.mitre.org/groups/G0069/

- "OilRig," Mitre Att&ck. N.D. https://attack.mitre.org/groups/G0049/

- Orleans, Alex. "Who Is PIONEER KITTEN?," CrowdStrike. 31 August 2020. https://www.crowdstrike.com/blog/who-is-pioneer-kitten/

- "Remix Kitten," CrowdStrike. N.D. https://adversary.crowdstrike.com/en-US/adversary/remix-kitten/

- Riley, Tonya. "Iranian hackers planned attack on Boston Children's Hospital last summer, FBI director says," Cyberscoop. 01 June 2022. https://www.cyberscoop.com/iran-hospital-wray-fbi-boston-children/

- Toulas, Bill. "Hackers now use 'sock puppets' for more realistic phishing attacks," Bleeping Computer. 13 September 2022. https://www.bleepingcomputer.com/news/security/hackers-now-use-sock-puppets-for-more-realistic-phishing-attacks/

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

References

- Meyers, Adam. "Who is REFINED KITTEN?," CrowdStrike. 12 December 2019. https://www.crowdstrike.com/blog/who-is-refined-kitten/

- Microsoft Threat Intelligence Center (MSTIC). "Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021," Microsoft. 16 November 2021. https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/

- Montalbano, Elizabeth. "Unflagging Iranian Threat Activity Spurs Warnings, Indictments From US Government," Dark Reading. 15 September 2022. https://www.darkreading.com/attacks-breaches/iranian-threat-activity-warnings-indictments-us-government

- "MuddyWater," Mitre Att&ck. N.D. https://attack.mitre.org/groups/G0069/

- "OilRig," Mitre Att&ck. N.D. https://attack.mitre.org/groups/G0049/

- Orleans, Alex. "Who Is PIONEER KITTEN?," CrowdStrike. 31 August 2020. https://www.crowdstrike.com/blog/who-is-pioneer-kitten/

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

References

- "Remix Kitten," CrowdStrike. N.D. https://adversary.crowdstrike.com/en-US/adversary/remix-kitten/

- Riley, Tonya. "Iranian hackers planned attack on Boston Children's Hospital last summer, FBI director says," Cyberscoop. 01 June 2022. https://www.cyberscoop.com/iran-hospital-wray-fbi-boston-children/

- Toulas, Bill. "Hackers now use 'sock puppets' for more realistic phishing attacks," Bleeping Computer. 13 September 2022. https://www.bleepingcomputer.com/news/security/hackers-now-use-sock-puppets-for-more-realistic-phishing-attacks/

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

? Questions

FAQ

Upcoming Briefing

- 12/08 – Automation & Hacking

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are **highly encouraged** to provide feedback. To provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

Disclaimer

These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

What We Offer

Sector and Victim Notifications
Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

Alerts and Analyst Notes
Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings
Presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Contacts

HHS.GOV/HC3

HC3@HHS.GOV