ThreatCure

Cyber Threat Advisory

Iranian Actor

Threat Actor Criminal

CATEGORY

Criminal Threat Actor

SEVERITY

High

Platforms

Windows

IMPACT

- Disruption to Critical Infrastructure
- Data Breaches and Credential Theft
- Economic and Reputational Damage

Description

Iranian Threat Actors

This advisory highlight the activities of Iranian cyber actors who are employing brute force techniques to infiltrate organizations across various critical infrastructure sectors, including healthcare, government, information technology, engineering, and energy. Their primary goal appears to be acquiring user credentials and network information that can be sold to cybercriminals for further exploitation.

Iranian cyber actors are targeting critical infrastructure of the different countries in the world, focusing on sectors like financial Institute, healthcare, government, and energy. They have used brute force methods, including password spraying, to gain unauthorized access to accounts. They employ tactics like "push bombing" to manipulate multi-factor authentication (MFA), allowing them to maintain persistent access by modifying MFA settings and selling compromised credentials.

Once inside, these actors conduct network reconnaissance to gather additional credentials and move laterally. They enhance their infiltration with techniques like Kerberos ticket harvesting and exploit vulnerabilities like CVE-2020-1472 (Zerologon) to impersonate domain controllers. Their overall aim is to disrupt services, steal data, and facilitate further criminal activities, posing significant threats to organizations.

Attacking Pattern

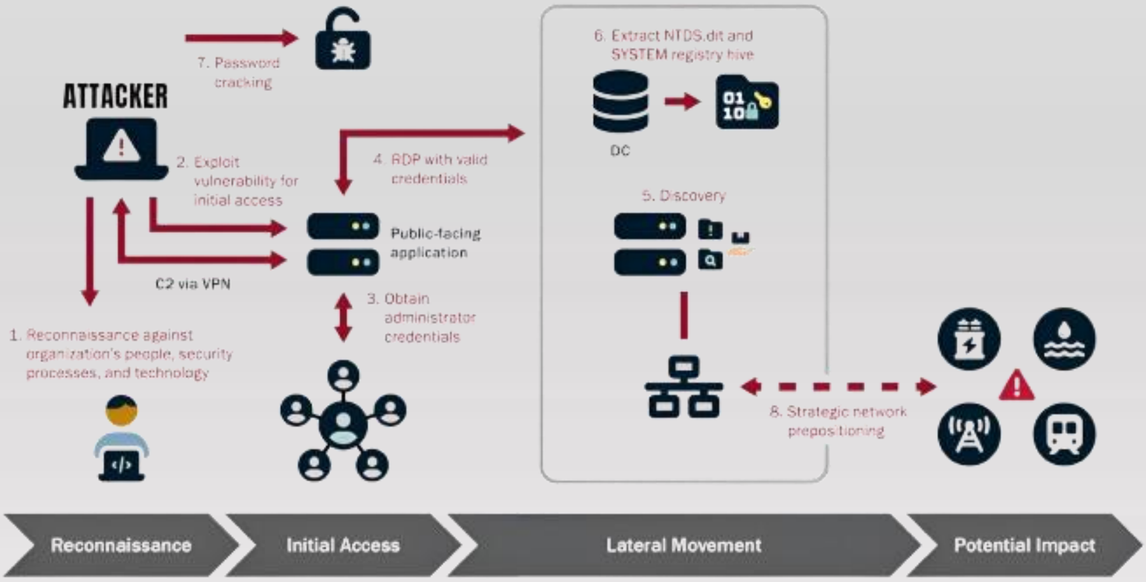
ATTACKER
7. Password cracking
2. Exploit vulnerability for initial access
4. RDP with valid credentials
C2 via VPN
Public-facing application
3. Obtain administrator credentials
1. Reconnaissance against organization's people, security processes, and technology
6. Extract NTDS.dit and SYSTEM registry hive
01 10
DC
5. Discovery
8. Strategic network prepositioning
Reconnaissance
Initial Access
Lateral Movement
Potential Impact

Figure 1 IRANIAN ATTACK CHAIN

Attacker: The central entity depicted in the diagram, representing an individual or group attempting to compromise a target organization's network and systems.

Phases of Attack:

- **Reconnaissance:**
  - The attacker conducts a thorough analysis of the target organization’s security posture, including personnel, security processes, and technological frameworks.
- **Initial Access:**
  - Exploitation of identified vulnerabilities occurs to establish initial access to the network, potentially through methods such as VPN exploitation.
- **Lateral Movement:**
  - Following initial access, the attacker navigates through the network to identify and access sensitive resources.
- **Potential Impact:**
  - The culmination of the attack seeks to achieve a significant negative impact, including data breaches, system disruptions, or unauthorized data manipulation.

Attack Steps:

- **Reconnaissance:** Gathering intelligence about the target’s security mechanisms.
- **Exploitation of Vulnerabilities**: Identifying and leveraging weaknesses to gain initial entry.
- **Credential Acquisition:** Obtaining administrator-level credentials to facilitate deeper network access.
- **Credential Extraction**: Utilizing tools to retrieve stored credentials from applications or systems.
- **Network Discovery**: Identifying additional resources, systems, and services within the network.
- **Privilege Escalation:** Attaining elevated permissions to expand access capabilities across the network.
- **Focused Attacks:** Conducting targeted attacks on specific systems or data repositories based on reconnaissance findings.

Indicator of Compromise

SHA-1

1F96D15B26416B2C7043EE7172357AF3AFBB002A

3D3CDF7CFC881678FEBCAFB26AE423FE5AA4EFEC

Remediation

- **Strong Password Policies**: Require complex passwords with a mix of characters and regular updates. Avoid password reuse.
- **Multi-Factor Authentication (MFA)**: Mandate MFA for sensitive accounts and educate users on recognizing MFA prompts.
- **Log Monitoring**: Regularly review authentication logs for suspicious activity and set alerts for multiple failed login attempts.
- **Software Updates**: Keep all software and operating systems up to date with the latest security patches.
- **Access Control**: Grant the minimum necessary access to users and periodically review access rights.
- **Block Indicators of Compromise (IOCs):** Ensure you're XDR, EDR, and other security tools are set to block all identified IOCs.

ThreatCure

Cyber Threat Advisory

Secure your byte world

Iranian Threat Actor

Threat Actor Criminal

Get Started Today

For more information about the ThreatCure ShieldOps Platform or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE