# OVERVIEW:

The objective of this lab is to explore adversary emulation techniques based on known Advanced Persistent Threats (APTs) using tools like MITRE ATT&CK and Atomic Red Team. The goal is to understand how to simulate and observe APT tactics, techniques, and procedures (TTPs) in a controlled environment. By researching a specific APT group, we can identify and implement defensive solutions to prevent the exploitation of these TTPs, enhancing our ability to defend against real-world threats.

# ANALYSIS:

APT37 is a North Korean state-sponsored cyber espionage group active since 2012. It mostly targets victims in South Korea, as well as Japan, Vietnam, Russia, Nepal, China, India, and others.

They are associated with groups such as InkySquid, ScarCruft, Reaper, Group123, TEMP.Reaper, Richochet Chollima.

Techniques they use are

- Elevation control
- Capture Audio using capturing utilities
- Ruby scripts
- Exploiting using Windows command shell
- Exploiting using VBA and shellcode
- Exploiting using python scripts
- Harvests usernames and passwords using credential stealers
- Using Malware
- Exploiting torrent file-sharing sites to disseminate malware
- Uses invalid certificates
- Steganography
- Phishing / Spearphising
- Bulk collection of information

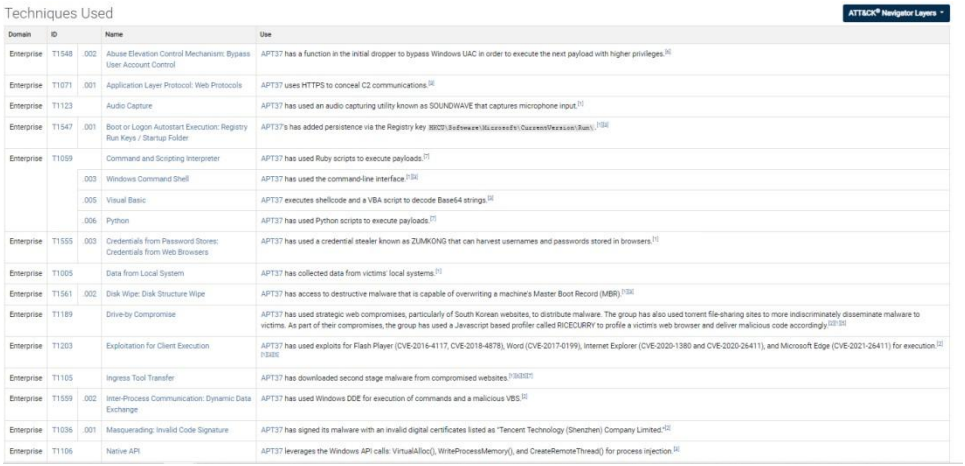
Some recommendations to help prevent some of the TTPs used by APT37 are to

- Validate data you don’t control
- Keep things up to date
- Use protective tools
- Use personal vigilance

- Educate yourself on potential exploits
- Use secure connections
- Encrypt your data
- Monitor activity
- Make backups of data
- Restrict access when not necessary (Physical/Virtual)
- Escape user input / validate user input/ sanitize data

On Atomic Red Team there are loads of tactics that can be emulated.

Looking at the MITRE ATT&CK website on APT37 we can see a list of their techniques. Along with the techniques is an ID



Techniques Used

ATT&CK® Navigator Layers

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1548 | .002 | Abuse Elevation Control Mechanism: Bypass User Account Control | APT37 has a function in the initial dropper to bypass Windows UAC in order to execute the next payload with higher privileges.[6] |
| Enterprise | T1071 | .001 | Application Layer Protocol: Web Protocols | APT37 uses HTTPS to conceal C2 communications.[9] |
| Enterprise | T1123 | | Audio Capture | APT37 has used an audio capturing utility known as SOUNDWAVE that captures microphone input.[1] |
| Enterprise | T1547 | .001 | Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder | APT37's has added persistence via the Registry key HKCU\Software\Microsoft\CurrentVersion\Run\.[1][3] |
| Enterprise | T1059 | | Command and Scripting Interpreter | APT37 has used Ruby scripts to execute payloads.[7] |
| | | .003 | Windows Command Shell | APT37 has used the command-line interface.[1][3] |
| | | .005 | Visual Basic | APT37 executes shellcode and a VBA script to decode Base64 strings.[9] |
| | | .006 | Python | APT37 has used Python scripts to execute payloads.[7] |
| Enterprise | T1555 | .003 | Credentials from Password Stores: Credentials from Web Browsers | APT37 has used a credential stealer known as ZUMKONG that can harvest usernames and passwords stored in browsers.[1] |
| Enterprise | T1005 | | Data from Local System | APT37 has collected data from victims' local systems.[1] |
| Enterprise | T1561 | .002 | Disk Wipe: Disk Structure Wipe | APT37 has access to destructive malware that is capable of overwriting a machine's Master Boot Record (MBR).[1][3] |
| Enterprise | T1189 | | Drive-by Compromise | APT37 has used strategic web compromises, particularly of South Korean websites, to distribute malware. The group has also used torrent file-sharing sites to more indiscriminately disseminate malware to victims. As part of their compromises, the group has used a Javascript based profiler called RICECURRY to profile a victim's web browser and deliver malicious code accordingly.[1][2][3] |
| Enterprise | T1203 | | Exploitation for Client Execution | APT37 has used exploits for Flash Player (CVE-2016-4117, CVE-2018-4878), Word (CVE-2017-0199), Internet Explorer (CVE-2020-1380 and CVE-2020-26411), and Microsoft Edge (CVE-2021-26411) for execution.[1][2][3][5][6] |
| Enterprise | T1105 | | Ingress Tool Transfer | APT37 has downloaded second stage malware from compromised websites.[1][2][3][7] |
| Enterprise | T1559 | .002 | Inter-Process Communication: Dynamic Data Exchange | APT37 has used Windows DDE for execution of commands and a malicious VBS.[9] |
| Enterprise | T1036 | .001 | Masquerading: Invalid Code Signature | APT37 has signed its malware with an invalid digital certificates listed as "Tencent Technology (Shenzhen) Company Limited."[12] |
| Enterprise | T1106 | | Native API | APT37 leverages the Windows API calls: VirtualAlloc(), WriteProcessMemory(), and CreateRemoteThread() for process injection.[6] |

If you look up an ID on Explore Atomic Red Team, you will be given a page. This page can help simulate these attacks. For example, abuse elevation control. On MITRE it has the ID T1548. Entering that onto ART we get this page.


Along with tests you can use.

## Atomic Test #1 - Sudo usage

Common Sudo enumeration methods.

**Supported Platforms:** macos,linux

**auto_generated_guid:** 150c3a08-ee6e-48a6-aeaf-3659d24ceb4e

**Inputs:**

None

Attack Commands: Run with **sh**! Elevation Required (e.g. root or admin)

```
sudo -l
sudo cat /etc/sudoers
sudo vim /etc/sudoers
```