Threat Intelligence PoC

Author: Anirudh Gautam

Intern ID: 163

Tactic: TA0043 - Reconnaissance

Gathering information about the target from public or semi-public sources.

Techniques

1. **T1593.001: Search Open Websites/Domains (Social Media)**

The person can search social media for information about victims that can e used during targeting. Often, social media sites contain certain personal data and various info about the victim organization about the roles, and its staff.

Threat actors may passively harvest data from these sites, as well as use information gathered to create fake profiles/groups to elicit victim's into revealing specific information. Information from these sources may reveal opportunities for other forms of reconnaissance, establishing operational resources and initial access.

Procedure Examples:

- **G1011** (Exotic Lily)
  Exotic Lily has copies data from social media sites to impersonate targeted individuals.
- **G0084** (Kimsuky)
  Kimsuky has used Twitter to monitor potential victims and to prepare targeted phishing e-mails.
- **C0022** (Operation Dream Job)
  Used LinkedIn to identify and target employees within a chosen organization.

What adversaries do:

- Monitor social media posts to collect details.
- Related the extracted info with the fingerprint the company's security posture and identify the potential targets.
- Craft highly personalized emails using that intel which would be embedded with the malicious links or attachments.
- The attachment sometimes via spear phishing contain ZIP having a script masquerading as a pdf. (as done my Kimsuky).

2. **T1595.002: Active Scanning (vulnerability scanning)**

The person may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.

These scans may also include more broad attempts to Gather Victim Host Information that can be used to identify more commonly known, exploitable vulnerabilities. Vulnerability scans typically harvest running software and version numbers via server banners, listening ports, or other network artifacts. Information from these scans may reveal opportunities for other forms of reconnaissance.

Procedure Examples:

- **G0016** (APT29)
  APT29 has conducted widespread scanning of target environments to identify vulnerabilities for exploit.
- **G0143** (Aquatic Panda)
  Aquatic Panda has used publicly accessible DNS logging services to identify servers vulnerable to Log4j (CVE 2021-44228)
- **C0029** (Cutting Edge)
  During Cutting Edge, threat actors used the publicly available Interactsh tool to identify Ivanti Connect Secure VPNs vulnerable to CVE-2024-21893

What adversaries do:

- Scan for Ivanti appliances vulnerable to CVE-2024-21893 (or any other attack) using get command.

- Use the SSRF to trigger CVE-2024-21887
- Establish a Python reverse TCP shell back to attacker and subsequently run LotL commands to enumerate host and the network.
- Deploy the attacking web shell variant into “querymanifest.cgi” by modifying the perl module to activate/deactivate the shell based on user agent.

- Attackers target a VMware Horizon Tomcat service vulnerable to CVE-2021-44228.
- Perform DNS lookups against a hard-coded subdomain under the Tomcat process and execute the linux commands on the windows host to download the exploit tools.
- Download and decode VBS/PowerShell scripts, load a reverse shell via DLL search-order hijacking.
- Dump the memory using LotL binaries and later compress the dump and delete traces from Temp and Program Data folder.

- Can also send a crafted payload via user agent pointing at attacked.
- Victims’ Log4j loads and the axecutes the returned Java class and fetch the modular powershell script, which later validates the connectivity and collect the system info.

3. **T1590.005 (Gather Victim Network Information (IP Adress)**

Hacker would gain the victims’ IP addresses that can be used furing targeting. Public IP address may be allocated to organizations by block or a range of sequential addresses. The info about the assigned addresses could contain details viz. Which Ip addresses are in use along with the physical location, ISP data.

Procedure Examples:

- **G0138** Andariel
  Andariel has limited its watering hole attacks to specific IP address range.
- **G0125** Hafnium
  Hafnium has obtained IP addresses for publicly-accessible exchange servers.
- **G0059** Magic Hound
  Magic Hound has captured the IP addresses of visitors to their phishing sites.

What adversaries do:

- Navigate to who.is and enter the target domain
- Record registrar, creation/expiration dates, and name servers.
- Note registrant contact emails or organization names for spear-phishing profiling.

- Go to dnsdumpster.com and input the target domain.
- Review the generated subdomain list and associated IP ranges.
- Download or screenshot the network map and identify potential public facing hosts.

- Study a past APT report to extract Indicators of Compromise (IoCs) and TTPs for social engineering or tooling mimicry.
- Open the archived AhnLab "Andariel Group" PDF via the Wayback Machine link.
- Skim the IoC appendix for domains, IPs, and file hashes previously used by the group
- Note their phishing lure samples, email subjects, and macro download URLs for crafting realistic decoys.

TTP Mapping

Tactic: Reconnaissance (TA0043)

Techniques: T1593, T1595.002, T1590.005

Procedures: Social-media harvest → Vulnerability scan → IP block enumeration

Mitigation

1. **T1593**

   Enforce API rate limits; monitor for fake profiles.

2. **T1595.002**

   Implement WAF rules; block mass-scan IPs; honeypot decoys.

3. **T1590.005**

Rate-limit WHOIS/DNS queries; block known reconnaissance tools.

Why This PoC Works

- All steps leverage free or widely available tools.
- Easy to look Social-media and DNS/IP data combine to give both human and technical views.
- Procedures can be automated or manually adjusted.
- Feeds directly into Initial Access (phishing, exploit) and discovery phases.