Threat Hunting Guide Template

Threat Hunting Guide: [AsyncRAT]

1. Overview

- **Threat Name:** Async RAT
- **Aliases:**
- **Category:** Remote Access Trojan
- **Targeted Sectors:** IT, hospitality, transportation industries, Oil, Government, Education.
- **Geographic Focus:** North, South, Central America, Europe, Middle East
- **First Seen:** 2019
- **Last Known Activity:** Today
- **Known Malware Families Utilized:**

2. Threat Description

- **Summary:** AsyncRAT was introduced on GitHub as a legitimate open-source remote administration software, but hackers use it for its many powerful malicious functions. This malware is often delivered through phishing campaigns utilizing social engineering tactics, such as fake news groups and deceptive emails impersonating legitimate services like Booking.com.
- **Tactics, Techniques, and Procedures (TTPs):** Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, collection.
- **Notable Campaigns:** Python Payloads and try cloudflare tunnels, clickfix phising campaign.

3. Indicators of Compromise (IOCs)

- **File Hashes:**
  - 27dc626f052cde7ca5c99e09ba2c3bc5
- **Malicious Domains & URLs:**
  - trabajovalle2019.duckdns.org

- **IP Addresses:**
  - 64.7.199.144
- **Registry Modifications:**
  - [Key locations and values modified]
- **File Paths & Artifacts:**
  - 'C:\Users\Public\Music\Loader.vbs'
- **Command and Control (C2) Servers:**
  - [Communication methods, IPs, domains]
- **Malicious Email Indicators:**
  - Booking.com, Dropbox, etc
- **Other Notable Indicators**
  - [Other data (ex: specific configuration setting change)]

4. Indicators of Attack (IOAs)

- **Behavioral Indicators:** Abnormal system behavior
- **Persistence Mechanisms:** [How the malware or APT maintains access]
- **Privilege Escalation Techniques:** [Methods used to gain higher-level permissions]
- **Lateral Movement Methods:** Unusual network activity
- **Data Exfiltration Indicators:** C2 servers, dynamic domains

5. Threat Hunting Queries

You may find Yara and Sigma rules online which you should convert to CrowdStrike queries, Sentinel queries, or Splunk queries. If the detection pertains to an endpoint, then a CrowdStrike query is appropriate. If the detection pertains to network logs which would not be on an endpoint, then a Sentinel query is appropriate.

SIEM Queries (Sentinel Query)

- Example query to identify sample information
  - Query

EDR Queries (CrowdStrike Query)

- Example query to identify sample information
  - Query

Splunk Queries

6. Response & Mitigation Strategies

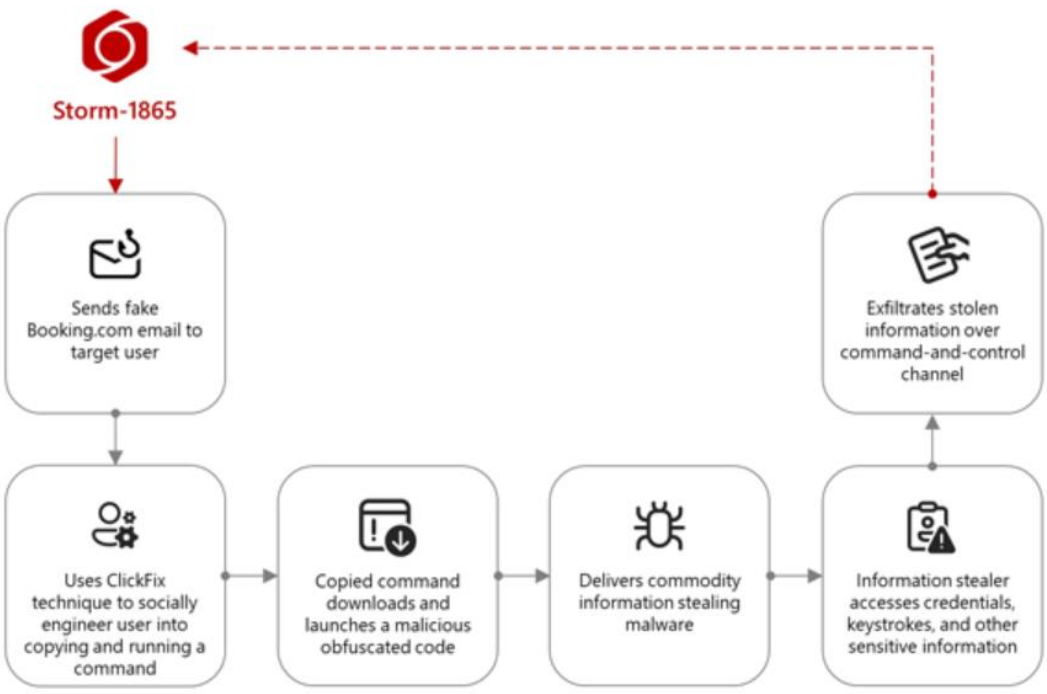
Explain how we can mitigate and respond to any of the actions we the threat actor observed performing in this guide. This may be blocking any of the IOCs we found at a device or network level. Or it could be patching systems to remediate CVEs, it could even be informing users of a potential threat if it is something we are unable to block (for example, if the threat actor is phishing users).

- **Immediate Containment Actions:** [Steps to isolate and mitigate threats]
- **Patching & Updates:** [Recommended security patches]
- **User Awareness Training:** [Key points to educate employees]
- **Endpoint Protection Recommendations:** [Endpoint or EDR configurations (ex: Creating CrowdStrike IOC to block process from executing)]
- **Network Segmentation Strategies:** [Reducing attack surface]

7. References & Further Reading

Document sources used to craft threat hunt guide.

- **Reports from Security Vendors:** C:\Users\sbethu\Downloads\IP, Domains.csv
  MITRE ATT&CK Mapping: C:\Users\sbethu\Downloads\TTP.json
- **Threat Intelligence Feeds:** [Relevant sources for tracking updates]
- Features include keylogging, audio/video recording, info-stealing, remote desktop control, password recovery, launching remote shell, webcam, injecting payloads, among other functions.


Storm-1865
Sends fake Booking.com email to target user
Uses ClickFix technique to socially engineer user into copying and running a command
Copied command downloads and launches a malicious obfuscated code
Delivers commodity information stealing malware
Information stealer accesses credentials, keystrokes, and other sensitive information
Exfiltrates stolen information over command-and-control channel

Tactic	Technique
Initial Access	T0819 – Exploit Public-Facing Application
Initial Access	T1566 – Phishing
Lateral Movement	T0859 – Valid Accounts
Persistence	T0859 – Valid Accounts
Reconnaissance	T1591 – Gather Victim Org Information
Reconnaissance	T1590 – Gather Victim Network Information
Persistence	T1078 – Valid Accounts
Defense Evasion	T1078 – Valid Accounts
Privilege Escalation	T1078 – Valid Accounts
Initial Access	T1078 – Valid Accounts
Initial Access	T1190 – Exploit Public-Facing Application
Initial Access	T1189 – Drive-by Compromise
Initial Access	T1474 – Supply Chain Compromise
Initial Access	T0862 – Supply Chain Compromise
Reconnaissance	T1592 – Gather Victim Host Information
Initial Access	T1456 – Drive-By Compromise
Initial Access	T0817 – Drive-by Compromise
Initial Access	T1199 – Trusted Relationship
Initial Access	T1195 – Supply Chain Compromise