THREAT INTELLIGENCE - CAPSTONE PROJECT

Organization:

J-One Groups

Analyst:

EVANS MARTEY KORLEY JACKSON

Role:

Cybersecurity Analyst

Submission Date:

23rd May 2025

1. Table of Contents

2. Part1: Basic Threat Intel or OSINT (Information Gathering)

The 6 major sources of Cyber Threat Intelligence that were used for information gathering.

1. **Domain and Subdomain Enumeration Tools** (Sublist3r, intelx.io, crt.sh)
2. **OSINT (Open-Source Intelligence) Tools** (Apollo.io, Phonebook.cz, lendx, Maltego, Google Dorking, Hunter.io)
3. **IP Address and Network Intelligence Tools** (Shodan, AbuseIPDB, who.is)
4. **Malware and File Analysis Tools** (any.run, Virustotal, Malware Bazaar)
5. **Web Directory and File Discovery Tools** (Open Directory Crawler)
6. **Dark Web and Deep Web Monitoring:** Specialized tools and human intelligence used to monitor illicit marketplaces, hacker forums, and clandestine communities for emerging threats.

1.2 Tools:

- **VirusTotal:** A popular platform for analyzing files and URLs for malware and obtaining threat intelligence data.
- **AlienVault OTX (Open Threat Exchange):** A collaborative platform where security professionals share and receive threat data and IOCs.
- **MISP (Malware Information Sharing Platform & Threat Sharing):** An open-source threat intelligence platform designed to improve the sharing of structured threat information.
- **Shodan:** A search engine for internet-connected devices, useful for discovering vulnerable systems and attack surfaces.
- **Maltego:** An open-source intelligence and forensics application for link analysis and data visualization from multiple sources.

1.2 5 Suggest Professional Organizations/Advisory Groups that were chosen to Learn and Exchange Threat Intelligence News

- **Information Sharing and Analysis Centers (ISACs)**
  Industry-specific ISACs facilitate the sharing of cybersecurity threat intelligence among members within sectors such as finance, healthcare, energy, and more.
- **Cyber Threat Alliance (CTA)**
  An alliance of cybersecurity organizations and vendors dedicated to sharing threat intelligence to improve collective defense against cyber threats.
- **Forum of Incident Response and Security Teams (FIRST)**
  An international organization that brings together CERTs and CSIRTs to facilitate rapid information sharing and collaborative incident response.
- **Financial Services Information Sharing and Analysis Center (FS-ISAC)**
  Focused on the financial sector, FS-ISAC promotes sharing of cybersecurity threat intelligence among banks, financial institutions, and payment companies.
- **International Association of Privacy Professionals (IAPP)**
  While primarily focused on privacy, IAPP offers resources and communities for sharing threat intelligence related to data privacy and security issues.

3. Part 2- Security Risk Assessment

1.3 Security Risk Assessment table tailored to the categories you specified:

Email, Certificates, Job Postings, IPs, Subdomains. This table summarizes relevant information, sources, vulnerabilities, threats, risks, and recommended controls.

Category	Information Found	Sources	Vulnerabilities	Applicable Threats	Potential Risks	Controls
Email	Found 2 emails,(J-One Group) Phishing emails, leaked email addresses, email headers	Email logs, data leaks, open-source OSINT/theHarvester	Phishing susceptibility, weak email filtering, misconfiguration	Phishing attacks, credential compromise, malware delivery	Data theft, credential theft, malware infection	Use spam filters, email gateway security, employee training, DMARC/DKIM/SPF implementation
Certificates	SSL/TLS certificates, expired or misconfigured certificates	Certificate Transparency logs, SSL Labs	Expired/invalid certificates, weak encryption, misconfiguration	Man-in-the-middle (MITM), impersonation, eavesdropping	Data interception, loss of trust, man-in-the-middle attacks	Regular certificate audits, enforce TLS best practices, use trusted CAs, automate renewal processes
Job Postings	Publicly available job listings, technical skill requirements	Company career pages, LinkedIn, job boards	Leakage of internal tools or technologies, sensitive project info	Reconnaissance, social engineering, targeted attacks	Increased attack surface, targeted spear-phishing	Limit sensitive info in public postings, monitor postings, internal access controls
IPs	Found 185 IPs, (Amazon)	Port scans, OSINT tools, network scans	Open ports, outdated services,	Exploitation, scanning for vulnerabiliti	System compromise, service disruption	Firewall rules, network segmentation, patch

Category	Information Found	Sources	Vulnerabilities	Applicable Threats	Potential Risks	Controls
	Known or exposed IP addresses, open ports, geolocation info		unpatched systems	es, DDoS attacks	, data breach	management, intrusion detection systems
Subdomains	Discovered subdomains, DNS records, exposed endpoints	DNS enumeration tools, OSINT, certificate logs	Subdomain takeover, unpatched endpoints, misconfigured DNS records	Subdomain hijacking, reconnaissance, supply chain attacks	Unauthorized access, data exfiltration, service hijacking	DNS monitoring, subdomain management, enforce DNS security policies

Notes:

- **Prioritize** vulnerabilities based on impact and likelihood.
- **Implement controls** iteratively, with regular reviews and updates.
- **Monitor** for new leaks, certificate issues, or exposed subdomains/IPs.

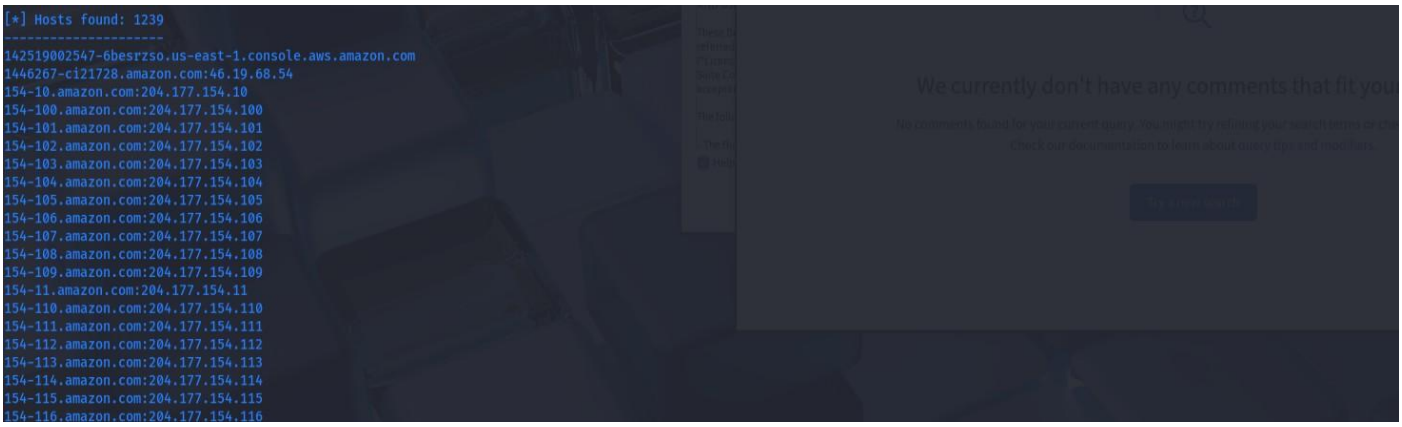

Fig.1 The screenshot demonstrates that theHarvester successfully performed a public data collection, revealing that there are 1,239 hosts associated with J-one Groups.

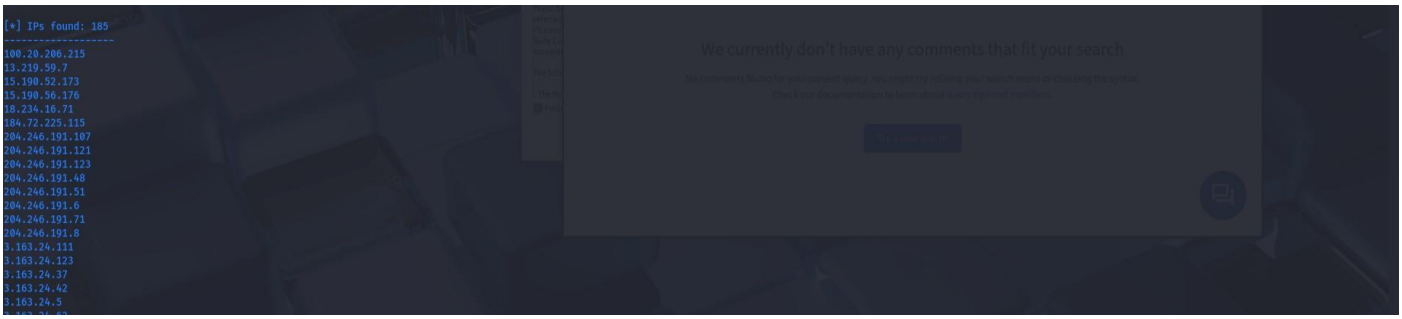

Fig. 2 The screenshot, it shows that theHarvester successfully collected public data, revealing a total of 185 IP addresses associated with J-one Groups.

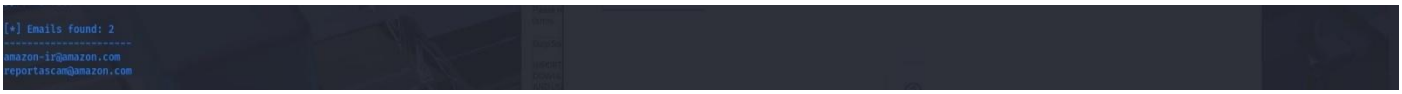

Fig.3 The screenshot shows that theHarvester successfully conducted a public data collection related to Amazon. It reveals that there are 2 emails addresses associated with J-one Groups.

4. Part 3: Threat Actor Profiling

There are a long list of possible threat Actors that can pose the Cyber threats to the Amazon, as an organization. Some of them are

Cybercriminal Groups:

- Ransomware groups (e.g., Clop), Data breach actors, Phishing and social engineering groups (e.g., TGR-UNK-0011 / JavaGhost)

Nation-State Actors:

- Espionage-focused groups (potentially linked to China, Russia, Vietnam (APT32/OceanLotus), North Korea, etc, Disruptive actors

Insider Threats:

- Disgruntled or compromised employees

Hacktivists:

- Groups motivated by protest

5Active threat actors/ransomware groups (Please provide links)

1. APT32

APT32, believed to be a cyber espionage group originating from Vietnam, has been operating since at least 2014. This threat actor has targeted a wide range of entities, including private companies and foreign governments, as well as individuals such as dissidents and journalists. Their operations show a significant interest in Southeast Asian nations, particularly Vietnam, the Philippines, Laos, and Cambodia. A key tactic they frequently employ to infiltrate their targets is the use of strategic web compromises

Target industries: Industries targeted are private sectors (Network security, manufacturing, hospitality, banking, Technology, media and consumer products), also, foreign governments are targeted.

Motivation: the primary aim is economic and political espionage.

Indicators of Compromise:

- **Malware: APT32** utilise custom malware such as Cobalt Strike Beacons, OceanLotus/SeaLotus Backdoors, WindTail, PHOREAL and FORKBELLY, SOUNDBITE.
- **Tactics:** They use strategic web compromises to compromise victims, exhibiting sophisticated and persistent approach to cyber espionage.

Domain IPs: Domain IPs for APT32 is not specific because**:**

- **Dynamic Infrastructure:** APT groups often use dynamic DNS services and compromised websites, which means their IP addresses can change frequently**.**
- **Privacy:** Specific, up-to-date lists are often kept within threat intelligence communities and security vendors to avoid tipping off the threat actors**.**

2. LockBit Overview

A prolific Ransomware-as-a-Service (RaaS) group. Known for its aggressive tactics, wide targeting across various sectors globally, and use of affiliates. Despite law enforcement actions, it remains a significant threat. They often employ double extortion tactics (encrypting data and threatening to leak it).

Target industries: these include healthcare, Education, Financial Services, Retail websites, (Amazon) Technology and more

Motivation: The primary motivation like most ransomware operations, is financial gain**.** Some groups have done this for recognition and reputation.

Indicators of Compromise:

- **Malware:**
- **Tactics:** They tend to infect Windows and virtual machines and have been observed targeting multiple industry verticals globally.
- **Domain Ips: Command and Control (C2) IPs:**

185.229.191.41 (Associated with AnyDesk C2)

81.19.135[.]219 (Russian geolocated IP, potentially hosting malicious HTA files)

45.129.137[.]233 (Callouts from known compromised devices)

192.229.221[.]95

193.201.9[.]224 (Russian geolocated IP, associated with FTP)

62.233.50[.]25 (Russian geolocated IP)

185.17.40[.]178

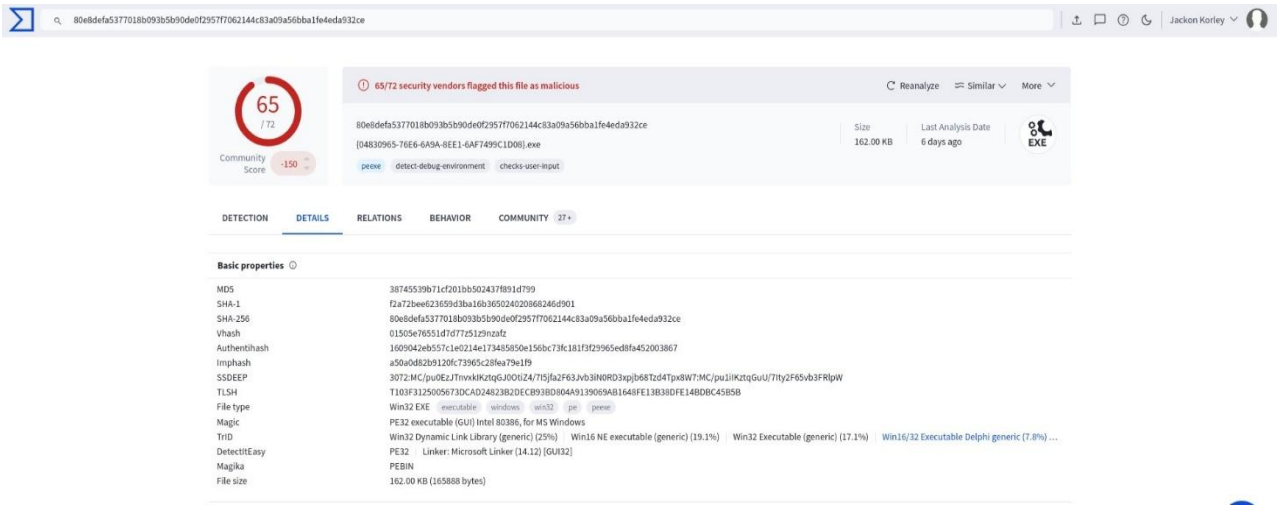

Fig.3 The Sample Testing with VirusTotal involved analyzing a file, and out of 72 security vendors evaluated, 65 identified the file as malicious. This indicates a high likelihood that the file is harmful based on the majority consensus among the tested security tools. (81.19.135[.]219 (Russian geolocated IP, potentially hosting malicious HTA files)

Known File Hashes (SHA256 examples):

- 74d9a91c4e6d2c15f3b6f8e7679e624f
- a3f2e7cb7315c1e48801cb8c6a86d2d2
- 80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce
- 506f3b12853375a1fbbf85c82ddf13341cf941c5acd4a39a51d6addf145a7a51

Recent incidence: AWS: A new ransomware threat called Codefinger targets users of AWS S3 buckets and makes recovery without payment impossible.

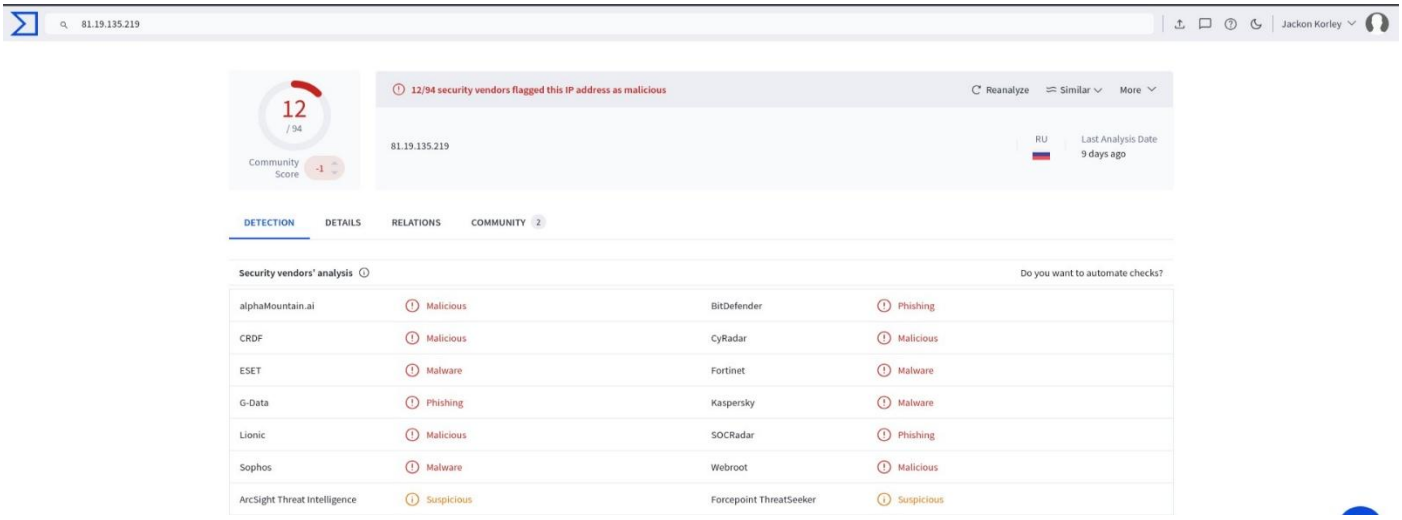

Fig.4 Screenshots from the test demonstrate how various security vendors flag the IP address as malicious and identify known malicious files based on their SHA256 hashes.
((80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce)

3. Ryuk Ransomware Overview:

Ryuk is a highly targeted and destructive ransomware strain first identified around August 2018. It is known for its deliberate, spear-phishing-based deployment, often following initial compromise through other malware such as TrickBot or Emotet. Ryuk encrypts files on infected systems and demands substantial ransom payments, often in Bitcoin, from organizations.

Target Industries:

Ryuk has predominantly targeted organizations across various sectors, including:

- Healthcare, Government agencies, financial institutions, Manufacturing, Retail, Critical infrastructure and Education

- **Motivation:**
  The primary motivation behind Ryuk appears to be financially driven. It is associated with targeted attacks designed to maximize ransom payments by organizations that cannot afford prolonged downtime or data loss. Additionally, Ryuk operators may seek to monetize their campaigns through:
  - Ransom payments
  - Data theft and extortion (in some cases)
  - Evasion of law enforcement detection

  Indicators of Compromise (IOCs):
  IOCs associated with Ryuk campaigns include:

- Malicious email attachments and links used in spear-phishing campaigns
- TrickBot or Emotet malware infections serving as initial infection vectors
- Specific file hashes associated with Ryuk binaries
- Suspicious PowerShell commands or scripts
- Unusual network activity, such as connections to known malicious domains or IPs
- Files encrypted with specific extensions (e.g., .ryk, .ryk, .locky)
- Ransom notes typically named "RyukReadMe.txt" or similar

Domains and IPs:
Ryuk operators often leverage malicious domains and IP addresses for command and control (C2) and payload delivery. These domains/IPs are periodically changed to evade detection. Examples of malicious domains have included:

- Domains registered via suspicious or compromised domains
- Domains associated with known malicious infrastructure

Here are some reputable sources for information and reports on Ryuk:

- **CISA (Cybersecurity and Infrastructure Security Agency):** CISA frequently publishes alerts and advisories on ransomware, including Ryuk.
    - **Ryuk Variant Report (CISA):**
    - https://www.cisa.gov/stopransomware/ryuk-variant-report
    - **StopRansomware Guidance (CISA):** https://www.cisa.gov/stopransomware

4. Vice Society Overview

Vice Society is a relatively new and emerging ransomware and threat actor group believed to have been active since 2021. It is known for deploying ransomware alongside data extortion tactics and targeting educational institutions and other organizations worldwide. The group often uses a variety of malware and hacking tools, including custom ransomware and living-off-the-land binaries (LOLBins), to achieve its objectives.

Target Industries:

Vice Society primarily targets organizations with high-value or sensitive data, including:

- **Educational institutions** (universities, colleges, K-12 schools), Healthcare organizations, Government agencies, Critical infrastructure entities, Financial services and Other enterprise sectors

Motivation:

- **Financial Gain:** The main motivation is extortion through ransom payments, often combined with data leaks.
- **Disruption and Coercion:** Disrupting operations to pressure victims into paying.
- **Data Exfiltration and Leak:** Threatening or executing data leaks to increase pressure.
- **Ideological/Political motives:** Less common but possible, especially given targeting of public institutions.

Indicators of Compromise (IOCs)

File and Process Indicators:

- Encrypted or ransom note files, typically named README.txt, How-to-decrypt.html, or similar.

- Malicious executables that may be named or disguised as legitimate software.
- Use of PowerShell or other scripting tools for lateral movement and exploitation.
- Commonly used file extensions after encryption: .vice, .locked, .crypt, among others.

Network Indicators:

- Connections to known malicious domains or IPs.
- Use of C2 infrastructure for command and control.
- Exfiltration traffic to external sites.

Behavioral Indicators:

- Unusual file modifications or deletions.
- Unauthorized access or credential misuse.
- Use of living-off-the-land techniques (LOLBins).

Domain, IPs, and Links

Vice Society operators often utilize a variety of dynamic infrastructure:

- **Malicious Domains:** Frequently changing domains registered for short periods, often hosted on cloud services, compromised websites, or malicious domains registered via privacy-protected services.
- **IP Addresses:** Multiple compromised or hosting provider IPs, often in data centers or cloud environments.
- **Links:** Phishing emails or exploit kits leading to malware download sites, or direct RDP access.

CISA (Cybersecurity and Infrastructure Security Agency):

- **Unit 42 by Palo Alto Networks:** They have published extensive research on Vice Society.
    - https://unit42.paloaltonetworks.com/vice-society-targets-education-sector/
    - https://unit42.paloaltonetworks.com/vice-society-ransomware-powershell/
    - https://www.sentinelone.com/anthology/vice-society/
    - https://www.microsoft.com/en-us/security/blog/2022/10/25/dev-0832-vice-society-opportunistic-ransomware-campaigns-impacting-us-education-sector/

5. Conti Ransomware Group Overview

Conti is a highly active and notorious cybercriminal ransomware organization believed to have originated around 2020. It is known for its sophisticated malware, extensive use of exploit kits, and a well-organized affiliate model. Conti has been linked to numerous high-profile attacks worldwide, often involving data theft, extortion, and disruptive tactics.

Key Characteristics

- Operates with a double-extortion model: encrypting data and threatening to leak sensitive information.
- Uses advanced techniques like living-off-the-land binaries (LOLBins), Cobalt Strike, and other post-exploitation tools.
- Maintains a significant presence on underground forums and has a dedicated team for operations, negotiations, and development.

Target Industries

Conti primarily targets sectors that are critical, high-value, or vulnerable:

- Healthcare (hospitals, clinics), Government and public sector agencies, Financial services and banking, Energy and utilities, Manufacturing and industrial sectors, Telecommunications and Educational institutions

Motivation

- **Financial Gain:** The primary driver is monetary ransom payments, often demanding millions of dollars.
- **Data Exfiltration & Leverage:** Use of stolen data to pressure victims into paying or to auction on dark web forums.
- **Disruption:** Causing operational paralysis to increase pressure.
- **Political & Strategic Goals:** While primarily financially motivated, some attacks may also serve geopolitical interests.

Indicators of Compromise (IOCs)

File Indicators:

- Ransom notes typically named README.txt, README.html, or #DECRYPT# files.
- Encrypted files with extensions such as .conti, .crypt, .locked, .id-<ID>.html.
- Malicious payloads often delivered via phishing, exploit kits, or remote access tools.

Process & Behavioral Indicators:

- Use of legitimate administrative tools like PowerShell, Cobalt Strike, Mimikatz, etc.
- Unusual process activity or command-line behavior.
- Lateral movement through SMB, RDP, or exploitation of vulnerabilities.

Network Indicators:

- Connections to known malicious domains or IPs.
- Data exfiltration traffic to external servers.
- Use of C2 servers with dynamic or suspicious hostnames.

Domain, IPs, and Links

Conti's infrastructure is dynamic and often leverages compromised or cloud-based hosting. Typical patterns include:

- **Malicious Domains:**
    - update-server[.]com
    - fileshare[.]xyz
    - exfiltration[.]net
    - Many domains are registered with privacy protection and are short-lived.
- **Associated IPs:**
    - IPs often originate from cloud providers like AWS, Azure, or compromised servers in various regions.
- **Links and Delivery Methods:**
    - Malicious email attachments or links leading to exploit kits or malware download sites.

- Phishing campaigns impersonating trusted entities.
- Exploiting known vulnerabilities in VPNs, RDP, or public-facing web apps.

CISA (Cybersecurity and Infrastructure Security Agency):

- https://unit42.paloaltonetworks.com/conti-ransomware-gang/
- https://www.akamai.com/glossary/what-is-conti-ransomware
- https://www.vectra.ai/threat-hunting/threat-actors/conti
- https://www.nccgroup.com/us/research-blog/conti-nuation-methods-and-techniques-observed-in-operations-post-the-leaks/
- https://www.picussecurity.com/resource/leaked-tools-ttps-and-iocs-used-by-conti-ransomware-group
- https://www.infosecurity-magazine.com/news-features/top-10-most-active-ransomware/

5. Part 4: TTP Mapping with MITRE ATT&CK

APT32 overview of high-level for (OceanBuffalo/Cobalt Mirage) TTPs mapped to the MITRE ATT&CK framework. It is a specific tactics, techniques, and procedures (TTPs) can evolve over time, so it's essential to stay updated with current threat intelligence reports.

APT32 (OceanBuffalo) — TTP Mapping with MITRE ATT&CK

MITRE ATT&CK Tactic	Description	Common Techniques (TTPs)	Examples / Notes
Initial Access (TA0001)	Gaining entry into target networks	- Phishing (Spear Phishing) (T1566) - Exploit Public-Facing Applications (T1190) - Supply Chain Compromise	Spear-phishing campaigns with malicious attachments or links; exploiting vulnerable internet-facing services.
Execution (TA0002)	Running malicious code	- PowerShell (T1059.001) - Command and Scripting Interpreter (T1059) - Malicious Scripts	Use of PowerShell or other scripting languages to execute payloads.
Persistence (TA0003)	Maintaining foothold	- Registry Run Keys / Startup Folder (T1060) - Scheduled Task/Job (T1053) - Service Registry Permissions Weakness (T1050)	Establishing persistence via scheduled tasks, services, or registry modifications.
Privilege Escalation (TA0004)	Gaining higher-level access	- Exploitation of Vulnerability (T1068) - DLL Side-Loading (T1073) - Token Impersonation (T1134)	Exploiting known vulnerabilities or DLL hijacking for privilege escalation.

MITRE ATT&CK Tactic	Description	Common Techniques (TTPs)	Examples / Notes
Defense Evasion (TA0005)	Avoiding detection	- Obfuscated Files or Information (T1027) - Masquerading (T1036) - Timestomping (T1099)	Use of obfuscation, masquerading, or timestomping techniques to evade detection.
Credential Access (TA0006)	Obtaining credentials	- Credential Dumping (T1003) - OS Credential Dumping (T1003.001) - Brute Force (T1110)	Dumping credentials from LSASS or SAM; harvesting stored passwords.
Discovery (TA0007)	Understanding environment	- Network Service Scanning (T1046) - System Network Configuration Discovery (T1016) - Remote System Discovery (T1018)	Mapping network and system configurations to plan further actions.
Lateral Movement (TA0008)	Moving within the network	- Remote Desktop Protocol (T1076) - Windows Admin Shares (T1021.002) - Pass the Hash (T1550.002)	Using RDP, SMB, or credential theft to move laterally.
Collection (TA0009)	Gathering data	- Data from Local System (T1005) - Email Collection (T1114) - Audio Capture (T1123)	Collecting documents, emails, or other sensitive info.
Exfiltration (TA0010)	Stealing data	- Exfiltration Over C2 Channel (T1041) - Data Transfer Size Limits (T1020) - Exfiltration Over Web Service (T1567)	Using HTTP/HTTPS, DNS, or other channels to exfiltrate data.
Command and Control (TA0011)	Maintaining communication	- Standard Application Layer Protocol (T1071) - Custom Command and Control Protocol (T1095) - Encrypted channels	Use of HTTPS, DNS tunneling, or custom protocols to control malware.

Additional Notes:

- **Malware Families & Techniques:** APT32 is known to use custom malware, malware loaders, and backdoors tailored for their campaigns.

- **Operational Focus:** They often target Southeast Asian governments, organizations, and corporations involved in geopolitics, economics, or intellectual property.
- **Evasion & Persistence:** Techniques include living off the land binaries, obfuscation, and using legitimate tools to blend in.

References:

- MITRE ATT&CK Framework
- APT32 (OceanBuffalo) Threat Reports

LockBit (a prominent Ransomware-as-a-Service group) Tactics, Techniques, and Procedures (TTPs) aligned with the MITRE ATT&CK framework. This overview summarizes common behaviors observed in LockBit operations based on publicly available threat intelligence.

LockBit Ransomware — TTP Mapping with MITRE ATT&CK

MITRE ATT&CK Tactic	Description	Common Techniques (TTPs)	Notes / Examples
Initial Access (TA0001)	Gaining entry into target environments	- Phishing (T1566) - Exploit Public-Facing Application (T1190) - Valid Accounts (T1078) - Supply Chain Compromise	LockBit operators often leverage phishing, exploited vulnerabilities, or compromised credentials to initiate access.
Execution (TA0002)	Running malicious code	- PowerShell (T1059.001) - Command and Scripting Interpreter (T1059) - Scheduled Task (T1053) - Service Execution (T1035)	Use of PowerShell, batch scripts, or scheduled tasks to execute ransomware payloads.
Persistence (TA0003)	Maintaining access	- Service Registry Permissions Weakness (T1050) - Scheduled Task/Job (T1053) - New Service (T1050)	Creating scheduled tasks or services to ensure persistence across reboots.
Privilege Escalation (TA0004)	Increasing privileges	- Exploitation of Vulnerability (T1068) - Token Impersonation (T1134) - DLL Side-Loading (T1073)	Exploiting known vulnerabilities or using DLL hijacking for privilege escalation.

MITRE ATT&CK Tactic	Description	Common Techniques (TTPs)	Notes / Examples
Defense Evasion (TA0005)	Avoiding detection	- Obfuscated Files or Information (T1027) - Masquerading (T1036) - Timestomping (T1099) - Use of Living off the Land Binaries (T1552)	Obfuscation, legitimate tools, or timestomping to evade detection.
Credential Access (TA0006)	Harvesting credentials	- Credential Dumping (T1003) - LSASS Memory (T1003.001) - Brute Force (T1110)	Dumping credentials for lateral movement and further access.
Discovery (TA0007)	Mapping environment	- Network Service Scanning (T1046) - System Network Configuration Discovery (T1016) - Remote System Discovery (T1018)	Identifying network topology, shares, and other systems.
Lateral Movement (TA0008)	Moving within the network	- Remote Desktop Protocol (T1076) - SMB/Windows Admin Shares (T1021.002) - Pass the Hash (T1550.002) - Remote File Copy (T1105)	Using tools like RDP, SMB, or credential theft to propagate.
Collection (TA0009)	Gathering data	- Data from Local System (T1005) - Email Collection (T1114) - Clipboard Data (T1115)	Collecting documents, emails, or sensitive info before encryption/ransom.
Exfiltration (TA0010)	Stealing data	- Exfiltration Over C2 Channel (T1041) - Exfiltration Over Web Service (T1567) - Data Transfer Size Limits (T1020)	Uploading data to attacker-controlled servers via HTTP, HTTPS, or cloud services.
Command and Control (TA0001)	Maintaining control	- Standard Application Layer Protocol (T1071) - Custom C2 Protocol (T1095) - Encrypted Channels	Using HTTPS, DNS tunneling, or other protocols for command and control communication.

MITRE ATT&CK Tactic	Description	Common Techniques (TTPs)	Notes / Examples
Impact (TA0040)	Disrupting or damaging systems	- Data Encrypted for Impact (T1486) - Data Destruction (T1489) - Service Stop (T1489)	Encrypting files, deleting data, or disrupting operations to maximize ransom leverage.

Additional Observations:

- **Initial Access:** LockBit often leverages exploited vulnerabilities (e.g., RDP exploits, VPN vulnerabilities), phishing, or compromised credentials.
- **Lateral Movement & Persistence:** They tend to use legitimate tools (Living off the Land binaries), scheduled tasks, and services.
- **Data Exfiltration:** Typically, exfiltrate data before encryption to threaten data leak-based extortion.
- **Operational Security:** Use of obfuscation, VPNs, and encrypted C2 channels to evade detection.

References:

- MITRE ATT&CK Framework
- LockBit Threat Reports & Analyses
- Unit 42 LockBit Analysis

Conti ransomware group's typical Tactics, Techniques, and Procedures (TTPs) aligned with the MITRE ATT&CK framework. This provides an overview of their operational behavior based on publicly available threat intelligence.

Conti Ransomware — TTP Mapping with MITRE ATT&CK

MITRE ATT&CK Tactic	Description	Common Techniques (TTPs)	Notes / Examples
Initial Access (TA0001)	Gaining initial foothold	- Phishing (T1566) - Exploit Public-Facing Application (T1190) - Valid Accounts (T1078) - Supply Chain Compromise	Often exploits vulnerabilities in VPNs, RDP, or uses phishing to obtain credentials.

MITRE ATT&CK Tactic	Description	Common Techniques (TTPs)	Notes / Examples
Execution (TA0002)	Running malicious code	- PowerShell (T1059.001) - Command and Scripting Interpreter (T1059) - Service Execution (T1035) - Scheduled Task (T1053)	Executes payloads via PowerShell, batch scripts, or scheduled tasks.
Persistence (TA0003)	Maintaining access	- Registry Run Keys / Startup Folder (T1060) - Scheduled Task/Job (T1053) - New Service (T1050) - DLL Search Order Hijacking (T1574.002)	Establishes persistence through scheduled tasks, services, or registry modifications.
Privilege Escalation (TA0004)	Gaining higher privileges	- Exploitation of Vulnerability (T1068) - Token Impersonation (T1134) - DLL Side-Loading (T1073)	Uses exploits or DLL hijacking for privilege escalation.
Defense Evasion (TA0005)	Avoiding detection	- Obfuscated Files or Information (T1027) - Masquerading (T1036) - Timestomping (T1099) - Living off the Land Binaries (T1552)	Uses obfuscation, legitimate tools, or timestomping to evade detection.
Credential Access (TA0006)	Stealing account info	- Credential Dumping (T1003) - LSASS Memory (T1003.001) - Brute Force (T1110)	Dumps credentials from LSASS memory or hashes.
Discovery (TA0007)	Map environment	- Network Service Scanning (T1046) - System Network Configuration Discovery (T1016) - Remote System Discovery (T1018)	Gathers info about network and systems to identify targets.
Lateral Movement (TA0008)	Moving within the network	- Remote Desktop Protocol (T1076) - Windows Admin Shares (T1021.002) - Pass the Hash (T1550.002) - Remote File Copy (T1105)	Uses RDP, SMB, or stolen creds for lateral spread.

MITRE ATT&CK Tactic	Description	Common Techniques (TTPs)	Notes / Examples
Collection (TA0009)	Data gathering	- Data from Local System (T1005) - Email Collection (T1114) - Clipboard Data (T1115)	Collects sensitive data/files before encryption.
Exfiltration (TA0010)	Data theft	- Exfiltration Over C2 Channel (T1041) - Exfiltration Over Web Service (T1567) - Data Transfer Size Limits (T1020)	Sends stolen data via HTTP, DNS, or other channels to command servers.
Command and Control (TA0001)	Maintaining control	- Standard Application Layer Protocol (T1071) - Custom C2 Protocol (T1095) - Encrypted Channels	Uses HTTPS, DNS tunneling, or other encrypted channels for C2 communication.
Impact (TA0040)	Disruption or damage	- Data Encrypted for Impact (T1486) - Data Destruction (T1489) - Service Stop (T1489)	Encrypts files, deletes data, or disrupts services to maximize ransom leverage.

Additional Observations:

- **Initial Access:** Frequently involves exploiting VPN vulnerabilities, RDP brute-force, or phishing campaigns to acquire credentials.
- **Lateral Movement & Persistence:** Employs legitimate Windows tools (Living off the Land binaries) and scheduled tasks/services.
- **Data Exfiltration & Ransom:** Often exfiltrates data before encrypting to threaten data leak-based extortion.
- **Operational Security:** Uses obfuscation, VPNs, and encrypted communications to evade detection.

References:

- MITRE ATT&CK Framework
- Conti Ransomware Analysis and Reports

Vice Society's typical Tactics, Techniques, and Procedures (TTPs) mapped to the MITRE ATT&CK framework. This reflects observed behaviors and techniques based on publicly available threat intelligence.

Vice Society — TTP Mapping with MITRE ATT&CK

MITRE ATT&CK Tactic	Description	Common Techniques (TTPs)	Notes / Observations
Initial Access (TA0001)	Gaining initial foothold	- Phishing (T1566) - Exploit Public-Facing Application (T1190) - Valid Accounts (T1078) - Drive-by Compromise (T1189)	Often exploits vulnerabilities or uses phishing to obtain credentials.
Execution (TA0002)	Running malicious code	- PowerShell (T1059.001) - Command and Scripting Interpreter (T1059) - Windows Management Instrumentation (T1047) - Malicious Scripts (T1064)	Uses PowerShell, WMI, or scripts for execution.
Persistence (TA0003)	Maintaining access	- Registry Run Keys / Startup Folder (T1060) - Scheduled Task/Job (T1053) - New Service (T1050) - DLL Search Order Hijacking (T1574.002)	Maintains persistence via scheduled tasks or registry modifications.
Privilege Escalation (TA0004)	Gaining higher privileges	- Exploitation of Vulnerability (T1068) - Token Impersonation (T1134) - DLL Side-Loading (T1073)	Exploits vulnerabilities or uses DLL hijacking to escalate privileges.
Defense Evasion (TA0005)	Evading detection	- Obfuscated Files or Information (T1027) - Masquerading (T1036) - Timestomping (T1099) - Living off the Land Binaries (T1552)	Uses obfuscation and legitimate tools to evade detection.
Credential Access (TA0006)	Harvesting credentials	- Credential Dumping (T1003) - LSASS Memory (T1003.001) - Brute Force (T1110)	Dumps credentials from LSASS or hashes stored in memory.
Discovery (TA0007)	Mapping the environment	- Network Service Scanning (T1046) - System Network Configuration Discovery (T1016) - Remote System Discovery (T1018)	Gathers info about network topology, shares, and systems.

MITRE ATT&CK Tactic	Description	Common Techniques (TTPs)	Notes / Observations
Lateral Movement (TA0008)	Moving within the network	- RDP (T1076) - SMB/Windows Admin Shares (T1021.002) - Pass the Hash (T1550.002) - Remote File Copy (T1105)	Uses RDP, SMB, or stolen credentials for lateral movement.
Collection (TA0009)	Data collection	- Data from Local System (T1005) - Email Collection (T1114) - Clipboard Data (T1115)	Collects files, emails, or sensitive data before encryption or exfiltration.
Exfiltration (TA0010)	Stealing data	- Exfiltration Over C2 Channel (T1041) - Exfiltration Over Web Service (T1567) - Data Transfer Size Limits (T1020)	Exfiltrates data via HTTP, DNS, or cloud storage channels.
Command and Control (TA0001)	Maintaining C2	- Standard Application Layer Protocol (T1071) - Custom C2 Protocol (T1095) - Encrypted Channels	Communicates via HTTPS, DNS tunneling, or custom protocols to hide C2 traffic.
Impact (TA0040)	Disruption or damage	- Data Encrypted for Impact (T1486) - Data Destruction (T1489) - Service Stop (T1489)	Encrypts files, deletes data, or disrupts systems to maximize impact and ransom leverage.

Additional Notes:

- **Initial Access:** Vice Society has been observed exploiting vulnerabilities, phishing, or stealing credentials.
- **Lateral Movement & Persistence:** Leverages legitimate tools, scheduled tasks, and registry modifications.
- **Ransom & Data Theft:** Often encrypts data and threatens data leaks to pressure victims.
- **Operational Security:** Uses obfuscation, encrypted C2 channels, and living-off-the-land techniques to evade detection.

References:

- MITRE ATT&CK Framework
- Threat reports on Vice Society from various cybersecurity firms (e.g., Mandiant, SentinelOne)

Ryuk ransomware's known tactics, techniques, and procedures (TTPs) aligned with the MITRE ATT&CK framework, based on publicly available intelligence and observed behaviors.

Ryuk Ransomware — TTP Mapping with MITRE ATT&CK

MITRE ATT&CK Tactic	Description	Common Techniques (TTPs)	Notes / Examples
Initial Access (TA0001)	Gaining entry into the environment	- Exploit Public-Facing Application (T1190) - Valid Accounts (T1078) - Phishing (T1566) - Malware Dropper (T1105)	Often leverages exploited vulnerabilities (e.g., RDP, VPN), or phishing campaigns to obtain initial access.
Execution (TA0002)	Running malicious code	- PowerShell (T1059.001) - Command and Scripting Interpreter (T1059) - Windows Management Instrumentation (T1047) - Malicious Scripts (T1064)	Uses PowerShell, WMI, or batch scripts to execute payloads.
Persistence (TA0003)	Maintaining access	- Registry Run Keys / Startup Folder (T1060) - Scheduled Task/Job (T1053) - New Service (T1050) - DLL Search Order Hijacking (T1574.002)	Establishes persistence via scheduled tasks, registry entries, or services.
Privilege Escalation (TA0004)	Gaining higher privileges	- Exploitation of Vulnerability (T1068) - Token Impersonation (T1134) - DLL Side-Loading (T1073)	Exploits known vulnerabilities or DLL hijacking to escalate privileges.
Defense Evasion (TA0005)	Evading detection	- Obfuscated Files or Information (T1027) - Masquerading (T1036) - Timestomping (T1099) - Living off the Land Binaries (T1552)	Uses obfuscation, legitimate tools, or timestomping to evade detection.
Credential Access (TA0006)	Harvesting credentials	- Credential Dumping (T1003) - LSASS Memory (T1003.001)	Dumps credentials from LSASS or hashes stored in memory.

MITRE ATT&CK Tactic	Description	Common Techniques (TTPs)	Notes / Examples
Discovery (TA0007)	Mapping network environment	- Network Service Scanning (T1046) - System Network Configuration Discovery (T1016) - Remote System Discovery (T1018)	Gathers info about network topology and connected systems.
Lateral Movement (TA0008)	Moving across systems	- RDP (T1076) - SMB/Windows Admin Shares (T1021.002) - Pass the Hash (T1550.002) - Remote File Copy (T1105)	Uses RDP, SMB, or stolen credentials to spread laterally.
Collection (TA0009)	Collecting victim data	- Data from Local System (T1005) - Email Collection (T1114) - Clipboard Data (T1115)	Collects files, emails, or other data before encryption.
Exfiltration (TA0010)	Stealing data	- Exfiltration Over C2 Channel (T1041) - Exfiltration Over Web Service (T1567) - Data Transfer Size Limits (T1020)	Exfiltrates data via HTTP, DNS, or cloud channels, often to pressure victims or for data theft.
Impact (TA0040)	Disrupting or damaging systems	- Data Encrypted for Impact (T1486) - Data Destruction (T1489) - Service Stop (T1489)	Encrypts files, deletes data, or terminates services to maximize ransom leverage.
Command and Control (TA0001)	Maintaining control over compromised systems	- Standard Application Layer Protocol (T1071) - Custom C2 Protocol (T1095) - Encrypted Communications	Uses HTTPS, DNS, or other encrypted channels for command and control.

Additional Notes:

- **Initial Access:** Ryuk operators often leverage exploited RDP vulnerabilities, phishing, or malware dropper campaigns.
- **Lateral Movement & Privilege Escalation:** Uses legitimate Windows tools, exploits vulnerabilities, or stolen credentials.
- **Ransom & Data Theft:** Frequently exfiltrates data before encrypting to increase pressure.
- **Operational Security:** Employs obfuscation, encrypted C2 channels, and living-off-the-land binaries to evade detection.

References:

- MITRE ATT&CK Framework
- Various cybersecurity reports detailing Ryuk activity (e.g., FireEye, CrowdStrike, Mandiant)

6. Part 5: Final Report Structure

Executive Summary

This report details a threat intelligence exercise conducted by J-one Groups to identify and understand its top cyber threats. The process involved pinpointing critical risks, assessing the current threat environment relevant to J-one Group's industry and operations, engaging in threat modeling to anticipate attack scenarios, and analyzing organizational vulnerabilities. This comprehensive approach helps Amazon prioritize security efforts, enhance defenses, and better prepare for potential cyberattacks.

Additionally, the report provides an in-depth analysis of three major ransomware groups: Ryuk, Vice Society, and Conti. Although Conti has officially disbanded, its legacy and members continue to influence the ransomware landscape through new variants. These groups are known for targeting organizations with tactics like "big game hunting," double extortion, and sophisticated operational methods. Their campaigns are primarily driven by financial motives, utilizing initial access brokers and exploiting common vulnerabilities for infiltration and lateral movement. The insights gained are vital for establishing effective defense strategies against these persistent and adaptable adversaries.

Project Objectives

The detailed rationale for this project is to equip J-one Groups with a comprehensive understanding of its cybersecurity environment, enabling it to proactively manage and mitigate risks. By identifying the top cyber threats the organization faces, the project helps prioritize security efforts on the most impactful risks. Assessing the current threat landscape provides context on emerging trends, attack methods, and threat actor motivations relevant to Amazon's industry and operations.

- Engaging in threat modeling allows the organization to anticipate potential attack scenarios, identify vulnerabilities, and evaluate how adversaries might exploit them.
- Analyzing the findings offers insights into security gaps, enabling targeted improvements. Finally, communicating these insights effectively to stakeholders ensures that decision-makers, employees, and security teams are informed, aligned, and prepared to implement appropriate mitigation strategies.
- Overall, this project aims to strengthen Amazon's cybersecurity posture, reduce potential damage from cyber incidents, and foster a culture of awareness and resilience across the organization.

2. OSINT Findings – Summary of Discovered Digital Footprint

Open-Source Intelligence (OSINT) reveals that ransomware groups maintain a digital footprint primarily through their leak sites, communication channels, and associated malware infrastructure.

- **Leak Sites:** All three groups utilized (or their successors continue to use) dedicated leak sites, often hosted on Tor hidden services, to publish exfiltrated data as part of their double extortion strategy. These sites serve as public shaming platforms, increasing pressure on victims to pay the ransom. Examples include "Conti News" and Vice Society's various .onion addresses.
- **Communication Channels:** Ransom demands typically direct victims to email addresses (e.g., ProtonMail, Tutanota, OnionMail) or private chat services on their leak sites for negotiation. This allows for direct, discreet communication while maintaining anonymity.

- **Initial Access Brokers (IABs) and Malware Infrastructure:** A significant portion of the digital footprint is tied to the preceding malware used for initial access. Ryuk often followed Emotet and TrickBot infections, while Conti heavily leveraged TrickBot and BazarLoader. Vice Society has also been observed using tools like SystemBC. These infections establish C2 channels, which are typically dynamic and utilize various IP addresses and domains that change frequently to evade detection. The infrastructure supporting these operations includes a network of compromised servers, bulletproof hosting, and privacy-enhancing services (VPNs, Tor).
- **Underground Forums and Marketplaces:** Intelligence suggests these groups and their affiliates are active on dark web forums and marketplaces, where they recruit members, share TTPs, and sell stolen access credentials or data. The internal communications of Conti, for instance, revealed a structured "corporate" environment, indicating a high level of organization and resource allocation in their digital operations.

3. Malware Analysis – Observations, IoCs, and Threat Indicators

Ryuk

- **Observations:** Known for highly targeted attacks on large organizations, rapid encryption, and deletion of shadow copies. Often deployed as a late-stage payload after initial infection by Emotet or TrickBot.
- **IoCs:**
    - **Ransom Note:** RyukReadMe.txt or similar .txt/.html files.
    - **File Extension:** Encrypted files appended with .ryk or .ryk-encrypted.
    - **Associated Malware:** Presence of Emotet/TrickBot/BazarLoader artifacts.
    - **Network Activity:** Outbound C2 connections, unusual internal traffic (lateral movement), TrickBot C2 traffic over ports like 446, 447, 449, 8082.
    - **System Commands:** Execution of vssadmin.exe delete shadows /all /quiet, disabling of security services.
- **Threat Indicators:** Sudden, widespread file encryption, deletion of shadow copies, unusual network scans, and lateral movement.

Vice Society

- **Observations:** Specializes in "double extortion" (data exfiltration + encryption), heavily targeting education and healthcare sectors. Known for using readily available payloads (Hello Kitty/Five Hands, Zeppelin) but now also custom encryptors like "PolyVice."
- **IoCs:**
    - **Ransom Note:** ReadMe.txt or similar, often including threats to publish data.
    - **File Extension:** Encrypted files with .v-s0ciety, .v-society, .locked, or Hello Kitty/Zeppelin extensions.
    - **Email Contact:** v-society.official@onionmail[.]org, ViceSociety@onionmail[.]org, or other OnionMail accounts.
    - **Tools Used:** Detection of Cobalt Strike, Mimikatz, SystemBC, PowerShell Empire, Rclone.
    - **Vulnerability Exploitation:** Evidence of PrintNightmare (CVE-2021-1675, CVE-2021-34527) exploitation.
    - **System Commands:** Extensive use of PowerShell for data exfiltration (w1.ps1), wevtutil for log clearing, disabling of security software.
- **Threat Indicators:** Large volumes of outbound data, unusual file compression activities, exploitation attempts on public-facing applications, sudden deployment of custom encryptors.

Conti (and Successors)

- **Observations:** Former prolific RaaS operation, now splintered into groups like BlackBasta, Quantum, BlackSuit, Akira. Known for high impact, rapid encryption, double extortion, and sophisticated, "corporate-like" operations.
- **IoCs:**
    - **Ransom Note:** RANSOM_README.txt or similar.
    - **File Extension:** Encrypted files typically .conti, but also .ryk, .crypt, or .lock depending on the successor.
    - **Associated Malware:** Prior infection with TrickBot, BazarLoader, Emotet.
    - **Tools Used:** Extensive use of Cobalt Strike, Mimikatz, AdFind, BloodHound, PowerSploit, PsExec, Rclone.
    - **Network Activity:** Signs of extensive reconnaissance, lateral movement via SMB/RDP, exfiltration via Rclone.
    - **System Commands:** vssadmin.exe delete shadows /all /quiet, disabling security solutions, modifying Group Policy.
- **Threat Indicators:** Compromised RDP/VPN accounts, rapid network-wide encryption, large-scale data exfiltration, and signs of extensive internal network reconnaissance before impact.

4. Threat Actor Profile

Ryuk

- **Group Attribution:** Believed to be operated by a Russian-speaking cybercriminal group, with observed ties to **Wizard Spider** (also known as Grim Spider). This group is also associated with Emotet and TrickBot, often serving as initial access vectors for Ryuk.
- **Known Motives:** Primarily **financial gain** through "big game hunting." They target large organizations with high revenue and critical infrastructure to maximize ransom payments. The focus is on disruptive impact to force rapid payment.
- **Operations:** Highly selective and manual operations, where attackers conduct extensive reconnaissance to identify high-value targets. They leverage established malware ecosystems (Emotet/TrickBot) for initial access, followed by lateral movement and privilege escalation to prepare for the final Ryuk deployment. Their operational discipline makes them highly effective.

Vice Society

- **Group Attribution:** An independent ransomware group that emerged in mid-2021. They do not typically operate as a RaaS, handling their own intrusions and deployments. Less is publicly known about the precise composition of the group, but they are clearly a professional and dedicated operation.
- **Known Motives:** Purely **financial gain** through ransomware and double extortion. They exploit the high sensitivity of data and the critical services provided by their targets to compel ransom payment, especially in the education and healthcare sectors, which are often less prepared for advanced cyberattacks.
- **Operations:** Characterized by "smash-and-grab" tactics, albeit with an initial reconnaissance phase. They often gain initial access through credential compromise or exploitation of public-facing applications. Their attacks are distinguished by rapid data exfiltration, followed by encryption, with the threat of public data leakage used as additional leverage.

Conti (and Successors)

- **Group Attribution:** Formerly one of the most prolific and organized Russian-speaking RaaS operations, associated with **Wizard Spider**. The group officially disbanded in May 2022 due to internal strife and public backlash following their pro-

Russia stance on the Ukraine invasion. However, its members and affiliates have largely reformed into new, highly active ransomware groups such as **BlackBasta, Quantum, BlackSuit, and Akira**.

- **Known Motives:** Predominantly **financial gain**. Conti was renowned for its high ransom demands and efficient monetization through its RaaS model. The successor groups continue this profit-driven approach, utilizing similar highly effective tactics.
- **Operations:** Conti operated with a highly structured, almost corporate-like hierarchy, with specialized teams for development, negotiation, and operations. They pioneered advanced double extortion, combining rapid encryption with massive data exfiltration. Their successors maintain this level of sophistication, focusing on rapid deployment, efficient lateral movement, and the exfiltration of sensitive data to maximize leverage for ransom payments. They frequently exploit common vulnerabilities and utilize a wide array of legitimate tools to achieve their objectives.

5. TTP Mapping with MITRE ATT&CK

Below is a summarized heatmap and explanation of common tactics observed across Ryuk, Vice Society, and Conti (and their successors), mapped to the MITRE ATT&CK framework.

MITRE ATT&CK Heatmap (Common TTPs)

Tactic	Techniques (T-ID)	Ryuk	Vice Society	Conti
Initial Access	T1566.001 (Spearphishing Attachment)	Yes	Yes	Yes
	T1078 (Valid Accounts)	Yes	Yes	Yes
	T1190 (Exploit Public-Facing Application)	(Indirect)	Yes	Yes
Execution	T1059.003 (Windows Command Shell)	Yes	Yes	Yes
	T1059.001 (PowerShell)	Yes	Yes	Yes
	T1569.002 (System Services: Service Execution - PsExec)	Yes	Yes	Yes
Persistence	T1547.001 (Registry Run Keys)	Yes	Yes	Yes
	T1078 (Valid Accounts)	Yes	Yes	Yes
Privilege Escalation	T1068 (Exploitation for Privilege Escalation)	(Indirect)	Yes	Yes
	T1078.002 (Domain Accounts)	Yes	Yes	Yes
Defense Evasion	T1490 (Inhibit System Recovery)	Yes	Yes	Yes
	T1562.001 (Impair Defenses: Disable/Modify Tools)	Yes	Yes	Yes
	T1027 (Obfuscated Files/Information)	Yes	Yes	Yes
Credential Access	T1003 (OS Credential Dumping - LSASS, SAM)	(Indirect)	Yes	Yes
	T1558 (Kerberos Tickets)	No	(Limited)	Yes
Discovery	T1087 (Account Discovery)	Yes	Yes	Yes
	T1046 (Network Share Discovery)	Yes	Yes	Yes

	T1018 (Remote System Discovery)	Yes	Yes	Yes
Lateral Movement	T1021.002 (SMB/Windows Admin Shares)	Yes	Yes	Yes
	T1021.001 (RDP)	Yes	Yes	Yes
	T1569.002 (Service Execution - PsExec)	Yes	Yes	Yes
Collection	T1074.001 (Data Staged: Local)	(Limited)	Yes	Yes
	T1560.001 (Archive Collected Data)	(Limited)	Yes	Yes
Command and Control	T1071.001 (Web Protocols)	Yes	Yes	Yes
	T1573.002 (Encrypted Channel)	Yes	Yes	Yes
Exfiltration	T1041 (Exfiltration Over C2 Channel)	No	Yes	Yes
	T1567 (Exfiltration Over Web Service / Cloud)	No	Yes	Yes
Impact	T1486 (Data Encrypted for Impact)	Yes	Yes	Yes
	T1490 (Inhibit System Recovery)	Yes	Yes	Yes
	T1489 (Service Stop)	Yes	Yes	Yes

Export to Sheets

Explanation of Tactics

- **Initial Access (TA0001):** All three groups frequently rely on **T1566.001 (Spearphishing Attachment)** as a common entry point, often delivering initial droppers like TrickBot or BazarLoader. They also exploit **T1078 (Valid Accounts)**, leveraging compromised RDP/VPN credentials, and in Vice Society's and Conti's case, **T1190 (Exploit Public-Facing Application)**, particularly through vulnerabilities in perimeter devices or web applications.
- **Execution (TA0002):** They extensively use native Windows command-line tools like **T1059.003 (Windows Command Shell)** and **T1059.001 (PowerShell)** for various malicious tasks, including reconnaissance, defense evasion, and payload execution. **T1569.002 (System Services: Service Execution)** via PsExec is a common technique for remote execution.
- **Persistence (TA0003):** Adversaries ensure continued access by modifying **T1547.001 (Registry Run Keys / Startup Folder)** and maintaining control over **T1078 (Valid Accounts)**, especially domain administrator accounts.
- **Privilege Escalation (TA0004):** Gaining higher privileges is crucial. They exploit vulnerabilities (e.g., PrintNightmare for Vice Society, various kernel exploits for Conti/TrickBot), mapped to **T1068 (Exploitation for Privilege Escalation)**, and abuse **T1078.002 (Valid Accounts: Domain Accounts)** that already possess elevated permissions.
- **Defense Evasion (TA0005):** A critical aspect of their operations. All groups use **T1490 (Inhibit System Recovery)** by deleting shadow copies and **T1562.001 (Impair Defenses: Disable or Modify Tools)** to neutralize security software and backup solutions. They also employ **T1027 (Obfuscated Files or Information)** and **T1036 (Masquerading)** to hide their activities.
- **Credential Access (TA0006):** While Ryuk's direct credential access is often handled by preceding malware, Vice Society and Conti actively engage in **T1003 (OS Credential Dumping)** (e.g., Mimikatz against LSASS) and sometimes **T1558 (Steal or Forge Kerberos Tickets)** for lateral movement.

- **Discovery (TA0007):** Extensive reconnaissance is a hallmark of these targeted attacks. They perform **T1087 (Account Discovery)**, **T1046 (Network Share Discovery)**, and **T1018 (Remote System Discovery)** to map the network and identify valuable assets.
- **Lateral Movement (TA0008):** They spread through the network using legitimate tools like **T1021.002 (SMB/Windows Admin Shares)** and **T1021.001 (RDP)**. **T1569.002 (System Services: Service Execution)** via PsExec is commonly used for remote deployment of tools and ransomware.
- **Collection (TA0009):** Vice Society and Conti (and their successors) engage in **T1074.001 (Data Staged: Local Data Staging)** and **T1560.001 (Archive Collected Data)** using tools like 7-Zip or Rclone to prepare data for exfiltration.
- **Command and Control (TA0011):** They maintain C2 communication through various protocols, often **T1071.001 (Application Layer Protocol: Web Protocols)** and **T1573.002 (Encrypted Channel: Asymmetric Cryptography)** to secure their communications.
- **Exfiltration (TA0010):** A core component of the "double extortion" model for Vice Society and Conti. They use **T1041 (Exfiltration Over C2 Channel)** or **T1567 (Exfiltration Over Web Service)**, often leveraging tools like Rclone to upload large volumes of data.
- **Impact (TA0040):** The final stage involves **T1486 (Data Encrypted for Impact)**, rendering systems inoperable. They also actively engage in **T1490 (Inhibit System Recovery)** by deleting shadow copies and **T1489 (Service Stop)** to halt critical services that might interfere with encryption.

6. Recommendations

To defend against ransomware groups like Ryuk, Vice Society, and Conti (and their evolving successors), a multi-layered and proactive cybersecurity strategy is essential.

Detection Rules

1. **Endpoint Detection and Response (EDR) & Extended Detection and Response (XDR) Alerts:**
    - **Suspicious Process Execution:** Alert on vssadmin.exe commands with /delete and /quiet flags.
    - **Service/Process Termination:** Monitor for attempts to stop security-related services (antivirus, backup solutions).
    - **New Service Creation:** Alert on the creation of new, unrecognized services, especially those with random names or short lifetimes.
    - **Credential Dumping Activity:** High-fidelity alerts for tools like Mimikatz interacting with LSASS.
    - **PowerShell Activity:** Monitor for highly obfuscated or encoded PowerShell commands, and execution of scripts related to system enumeration, data staging, or exfiltration (e.g., w1.ps1).
    - **Lateral Movement Tools:** Alert on PsExec, Cobalt Strike, or other remote administration tools being used in unusual patterns or from non-standard accounts.
    - **File Extension Changes:** High-fidelity alerts on rapid, widespread file renames to known ransomware extensions (.ryk, .v-s0ciety, .conti, etc.).
    - **Volume Shadow Copy Deletion:** Monitor event logs for Event ID 7036 (Service Control Manager) indicating services being stopped, followed by VSS deletions.
2. **Network Intrusion Detection/Prevention Systems (NIDS/NIPS):**
    - **C2 Traffic:** Block known C2 IP addresses and domains (ensure threat intelligence feeds are current).

- **Anomalous Outbound Traffic:** Detect unusual outbound connections, especially large data transfers to external, non-corporate IPs (signaling exfiltration).
- **Internal Scanning:** Alert on excessive internal network scanning (ports 445, 3389, etc.) indicative of discovery and lateral movement.
- **RDP/SMB Brute-Force/Exploitation:** Detect and block repeated failed login attempts or known exploit patterns on RDP (3389/TCP) and SMB (445/TCP) ports.

3. **Security Information and Event Management (SIEM) Rules:**
   - **Failed Logins:** Correlate multiple failed login attempts from a single source across different accounts or systems.
   - **Privileged Account Activity:** Alert on anomalous activity from domain administrator accounts (e.g., logins from unusual locations or at strange times).
   - **Mass File Creation/Modification:** Baseline normal file activity and alert on sudden, high-volume file creation or modification events on network shares and endpoints.
   - **Antivirus/EDR Disabling:** Alerts if security software reports being disabled or tampered with.

Hardening Suggestions

1. **Implement Strong Access Controls:**
   - **Multi-Factor Authentication (MFA):** Enforce MFA for all external access (VPN, RDP, web applications) and all privileged accounts.
   - **Least Privilege Principle:** Grant users and systems only the minimum necessary permissions required to perform their functions.
   - **Role-Based Access Control (RBAC):** Implement RBAC to segment user permissions based on their job roles.
2. **Robust Backup and Recovery Strategy:**
   - **3-2-1 Rule:** Maintain at least three copies of your data, on two different media types, with one copy stored off-site and offline (air-gapped or immutable cloud storage).
   - **Regular Testing:** Periodically test backup restoration procedures to ensure data integrity and rapid recovery capabilities.
   - **Immutable Backups:** Utilize storage solutions that prevent modification or deletion of backup data.
3. **Patch Management and Vulnerability Management:**
   - **Regular Patching:** Implement a rigorous patch management program to ensure all operating systems, applications, and firmware are up to date, prioritizing critical security patches.
   - **Vulnerability Scanning:** Conduct regular vulnerability assessments and penetration tests to identify and remediate weaknesses in your infrastructure.
   - **Asset Inventory:** Maintain an accurate inventory of all IT assets to ensure comprehensive patching.
4. **Network Segmentation and Micro-segmentation:**
   - Divide your network into smaller, isolated segments. This limits lateral movement of attackers if a segment is compromised, reducing the blast radius of a ransomware attack.
   - Micro-segmentation can further isolate individual workloads and applications.

5. **Endpoint Security:**
    - Deploy advanced Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR) solutions capable of behavioral analysis and real-time threat prevention.
    - Implement application whitelisting to prevent unauthorized executables from running.
6. **Strong Credential Hygiene:**
    - Enforce strong, unique passwords for all accounts.
    - Regularly rotate passwords for privileged accounts.
    - Implement privileged access management (PAM) solutions to secure and manage privileged credentials.
7. **Disable/Harden Unnecessary Services:**
    - Disable unused ports, services, and protocols (e.g., SMBv1, unnecessary RDP access).
    - Harden critical services by following vendor best practices and security guidelines.

Awareness Tips

1. **Comprehensive Security Awareness Training:**
    - **Regular & Engaging Training:** Conduct mandatory, regular, and engaging training sessions for all employees on cybersecurity best practices. Use real-world examples and interactive modules.
    - **Phishing Simulation Drills:** Conduct frequent phishing simulation exercises to train employees on how to identify and report suspicious emails, links, and attachments (including AI-generated phishing). Track reporting rates and dwell times.
    - **Social Engineering Awareness:** Educate employees about various social engineering tactics (vishing, smishing, deepfakes) used by adversaries.
    - **Data Handling:** Train employees on proper handling of sensitive data, especially regarding exfiltration vectors (e.g., not uploading sensitive data to personal cloud storage).
2. **Incident Reporting Culture:**
    - **Clear Reporting Channels:** Establish and communicate clear procedures for reporting suspicious activities or potential security incidents. Emphasize that "when in doubt, report it."
    - **No Blame Culture:** Foster a no-blame culture to encourage employees to report incidents without fear of reprisal, ensuring early detection.
3. **Remote Work Security:**
    - **Secure Remote Access:** Provide clear guidelines and mandatory training on securing remote work environments, including Wi-Fi security, device management, and secure remote access protocols (e.g., always use VPN).
    - **Device Protection:** Emphasize the importance of keeping work devices secure, locked when unattended, and not used for personal, high-risk activities.
4. **Consequences of Ransomware:**
    - Educate employees on the devastating impact of ransomware attacks on organizations (downtime, financial losses, reputational damage, data loss) to underscore the importance of their role in prevention.

By implementing these recommendations, organizations can significantly improve their resilience against the evolving threat landscape posed by ransomware groups like Ryuk, Vice Society, and the successors of Conti. Continuous monitoring, adaptation to new threat intelligence, and a strong security culture are paramount for long-term protection.

7. CONCLUSION

This comprehensive threat intelligence report illustrates that J-one Groups successfully conducted public data collection using tools like theHarvester, revealing extensive infrastructure associated with J-one Groups, including over 1,200 hosts, 185 IP addresses, and 2 email addresses. The analysis highlights the importance of multi-source OSINT, cyber threat intelligence platforms, and collaboration with professional organizations such as ISACs, CTA, FIRST, FS-ISAC, and IAPP to enhance threat awareness.

The risk assessment identified key vulnerabilities across email, certificates, job postings, IPs, and subdomains, emphasizing the need for controls like strong email filtering, certificate management, access restrictions, network segmentation, and continuous monitoring.

The report profiles several advanced threat actors—APT32, LockBit, Ryuk, Vice Society, and Conti—detailing their TTPs mapped to the MITRE ATT&CK framework. Common tactics include spear-phishing, exploitation of public-facing apps, lateral movement via legitimate tools, data exfiltration, and deployment of ransomware with double extortion techniques. These actors often leverage dynamic infrastructure, exploit known vulnerabilities, and employ obfuscation to evade detection.

In conclusion, understanding these threat actors and their methodologies enables organizations like J-one Groups to implement targeted defenses, such as advanced detection rules, robust access controls, regular patching, network segmentation, and security awareness training. Continuous intelligence gathering and collaboration with industry groups are essential to stay ahead of evolving cyber threats, particularly sophisticated ransomware campaigns exemplified by Ryuk, Vice Society, and Conti successors.