**THREAT INTELLIGENCE ANALYSIS**

**CLOUDS**

**Melvin Baird**

**Security Operations Centre (SOC) Analyst**

**20th May, 2025**

**1. Executive Summary ……………………………………………………………………………………..3**

**2. Introduction ……………………………………………………………………………….3**

**3. Methodology ……………………………………………………………………………….3**

**4. Basic Threat Intel or OSINT …………………………………………………………………………..4**

**5. Security Risk Assessment ……………………………………………………………………….……5**

**6. Threat Actor Profiling ……………………………………………………………………..……………10**

**7. TTP mapping with MITRE Attack .……………………………………………………………………….16**

**i) The tools and Techniques used by UNC3944 … …………………………………………….…16**

**ii) MITRE Attack TTPs ………………………………………………………………………………………18**

**8. Final Findings & Impact ………………………………………………………………………………….19**

**9. Recommendations ………………………………………………………………………………20**

**10. Conclusion ….………………………………………………………………………………………..…21**

**11. References …….……………………………………………………………………………………….22**

**Executive Summery**

**Clouds’ large-scale and complex infrastructure makes it an attractive target for a wide range of threat actors, including those motivated by espionage, financial gain, or political and ideological reasons.**

**This report focuses on UNC3944, a financially motivated cybercrime group observed targeting organizations in the financial, retail, and technology sectors. UNC3944, also known as Scattered Spider, is known for using sophisticated social engineering techniques to gain initial access, followed by lateral movement and data exfiltration. Recently, the group has shown an increasing trend of deploying ransomware to maximize financial gain.**

**Organizations operating in these sectors are assessed to be at high risk of attack. An assessment was conducted on Clouds’ network environment, alongside a threat intelligence exercise, to highlight how potential threat actors may exploit identified vulnerabilities both online and within the internal network. Patterns of attack associated with UNC3944 and similar adversaries were also examined. Finally, recommendations are provided as a proactive approach to strengthening defenses against these threats.**

**Introduction**

**As a large and influential global organization engaged in e-commerce, cloud computing (AWS), digital streaming, and related services, Clouds faces a broad spectrum of potential cyber threats. These may originate from financially motivated groups as well as nation-state actors seeking espionage, disruption, or competitive advantage.**

**The purpose of this report is to:**

* **Identify threat actor groups most likely to target Clouds.**
* **Assess the organization’s threat landscape.**
* **Recommend actionable security measures to prevent or mitigate future cyberattacks.**

**Methodology**

**The following steps were taken to conduct this assessment:**

1. **Threat Actor Identification – Researched and identified top cyber threat actors relevant to Clouds’ industry and infrastructure.**
2. **Threat Landscape Assessment – Evaluated current and emerging risks, including tactics, techniques, and procedures (TTPs) used by known adversaries.**
3. **Threat Modeling – Applied modeling frameworks to understand potential attack vectors and adversary behaviors.**
4. **Descriptive Analysis – Analyzed findings to establish patterns of attacks and vulnerabilities.**
5. **Reporting & Recommendations – Compiled results into this report and provided recommendations aimed at reducing exposure and preventing future incidents.**

**1: Basic Threat Intel or OSINT (Information Gathering)**

**The major Cyber threat intelligence sources used for information gathering for this exercise are**

**• Threat intelligence feeds from social media**

**• Alien Vault OTX**

**• Open Cyber Threat Intelligence (Open CTI)**

**• Government Agencies**

**• Dark reading**

**• Malware Information Sharing Platform (MISP)**

**Some threat intelligence tools were also used for the information gathering. They include**

**• OSINT framework**

**• Google Dork**

**• The Harvester**

**• Virus Total**

**• Abuse IPDB**

**• MITRE Attack framework**

**To stay abreast on threat intelligence feeds, the organization is recommended to join these professional**

**organizations/advisory groups, where information on existing and new emerging threat intelligence**

**feeds/news are shared on their platforms.**

**• Cloud Security Alliance (CSA)**

**• Forum of incident response & security teams (FIRST)**

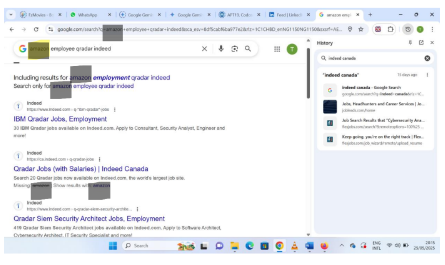
**• Information Sharing and Analysis Centre (ISAC)**

**• National institute of Standards and Technology (NIST)**

**• SANS Institute**

## ****Part 2 – Security Risk Assessment****

| **Category** | **Information Found** | **Sources** | **Vulnerabilities** | **Applicable Threats** | **Potential Risk** | **Controls** |
| --- | --- | --- | --- | --- | --- | --- |
| **Email** | **Open emails harvested in screenshot (Fig 2.1), could be cloned to send phishing emails to unsuspecting users.** | **The Harvester, OSINT Framework** | **Online exposure of open emails that can be harvested by threat actors.** | **Phishing emails, Spear phishing, Social engineering** | **Unauthorized access, Data breaches** | **Implement user access management and MFA; Conduct periodic employee training on phishing and security awareness.** |
| **Certificates** | **SSL/TLS certificates for web services, other exposed certificates can be found online.** | **crt.sh** | **Exposure of weak and/or expired certificates; revoked, expired, or compromised certificates.** | **Man-in-the-middle attack if certificates expire or are misconfigured.** | **Loss of client trust** | **Conduct regular audits of certificates; Enforce automatic renewal of expired certificates.** |
| **Job Postings** | **Online job postings exposing internal tools/software (Fig 2.2 & 2.3).** | **LinkedIn, Indeed.com, Google dorks** | **Online exposure of internally used tools/software that could be exploited.** | **Threat actors gain knowledge of internal tools; Exploitation of unpatched vulnerabilities.** | **Unauthorized access, software exploitation** | **Limit exposure of internal tool information online; Regular patch updates to mitigate vulnerabilities.** |
| **IPs** | **232 IP addresses identified across 14 ASNs (Fig 2.4).** | **OSINT tools (The Harvester)** | **Absence of DNS security, outdated services running on exposed IPs.** | **IP scanning and reconnaissance, DNS spoofing, hijacking.** | **Traffic redirection to malicious sites, unauthorized access and exploitation** | **Implement strict network control; Enable event monitoring and DNS security measures.** |
| **Subdomains** | **1,301 subdomains discovered (Fig 2.5).** | **OSINT tool (Sublist3r)** | **Shadow IT, inadequate monitoring, misconfigured DNS/CNAME records, forgotten or unpatched subdomains.** | **Attackers exploit misconfigured or unmonitored subdomains for DNS-based attacks.** | **Unauthorized access, introduction of security weaknesses** |  |

****

**Based on the information gathered above, it is shown that CLOUDS has done much by putting limited**

**Information online so as not to expose its weaknesses, but a few other unprotected information are still**

**online (ranging from internal and employee emails, IPs, internal working tools/software, etc.) through**

**which threat actors can gain unauthorized access to sensitive data**

**Part 3: Threat Actor Profiling**

**There are a long list of possible threat Actors that can pose the Cyber threats to the CLOUDS, as an**

**organization, ranging from Cybercriminal Groups (Ransomware groups, Data breach actors, Phishing and**

**social engineering groups), to Nation-State Actors (Espionage-focused groups potentially linked to China,**

**Russia, Vietnam (APT32/OceanLotus), North Korea, etc, Disruptive actors. Various nations may target**

**CLOUDS for intelligence gathering, political influence, or to disrupt their operations**

**5 Potential active threat actors/Ransomware groups that could pose biggest threats to CLOUDS are**

**stated below.**

**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 Espino**

## ****threat Actor Profiles****

### ****1. APT32 (Ocean Lotus/Sea lotus)****

**Overview:  
APT32, also known as Ocean Lotus/Sea lotus, is a state-sponsored Advanced Persistent Threat (APT) group linked to cyber espionage campaigns, particularly in Southeast Asia. The group is known for targeting government agencies, private organizations, and cybersecurity researchers.**

**Malware Used:**

* **Cobalt Strike Beacons**
* **Ocean Lotus/Sea lotus Backdoors**
* **Wind Tail**
* **PHOREAL**
* **FORKBELLY**
* **SOUNDBITE**

**Tactics:**

* **Strategic web compromises to infect victims.**
* **Sophisticated and persistent cyber espionage operations.**
* **Use of custom malware to maintain long-term access.**

**Domain/IP Infrastructure:**

* **Domain IPs are not specific due to the group’s use of:**
  + **Dynamic Infrastructure: Leveraging dynamic DNS services and compromised websites, making IP tracking difficult.**
  + **Privacy Considerations: Specific, up-to-date IP lists are maintained within threat intelligence communities and security vendors to avoid alerting the group.**

**Recent Incident:  
APT32 was observed conducting a targeted attack where they:**

* **Released a malicious Cobalt Strike exploit plugin via GitHub, embedded with a Trojan.**
* **Aimed specifically at cybersecurity personnel and large enterprises in China.**
* **This campaign highlights the group’s evolving sophistication and focus on targeting security professionals.**

**References:**

* **Threat Book CTI Report**
* **JSIS Analysis on Ocean Lotu**

### ****2. Lock Bit (Ransomware-as-a-Service Group)****

**Overview:  
Lock Bit is one of the most prolific Ransomware-as-a-Service (Ragas) groups worldwide. It employs affiliates to conduct attacks, using aggressive extortion methods and wide-ranging targeting. Despite multiple law enforcement operations against them, Lock Bit remains active and a major global threat.**

**Motivation:**

* **Primarily financial gain through ransom payments.**
* **Secondary motivations include reputation and recognition in cybercriminal communities.**

**Targeted Industries:**

* **Healthcare**
* **Education**
* **Financial Services**
* **Retail websites**
* **Technology (including CLOUDS)**
* **Other critical sectors globally**

**Tactics & Techniques:**

* **Double extortion: encrypting data and threatening to leak stolen files.**
* **Frequent targeting of Windows and virtual machines.**
* **Broad industry targeting across multiple regions.**

**Indicators of Compromise (IoCs):**

* **Malware: Used to manipulate file systems, registry, network traffic, processes, and behaviors.**
* **Command and Control (C2) IPs:**
  + **185.229.191[.]41 (Associated with Any Desk C2)**
  + **81.19.135[.]219 (Russian IP, hosting malicious HTA files)**
  + **45.129.137[.]233 (Callouts from compromised devices)**
  + **192.229.221[.]95**
  + **193.201.9[.]224 (Russian IP, associated with FTP)**
  + **62.233.50[.]25 (Russian IP)**

**Known File Hashes (SHA256 examples):**

**• 74d9a91c4e6d2c15f3b6f8e7679e624f**

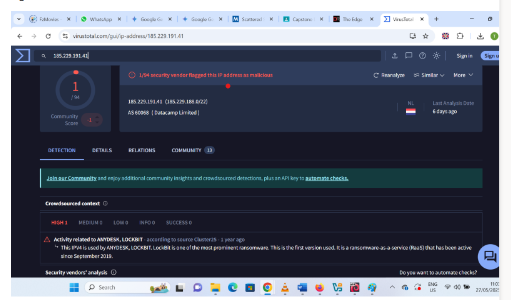
**• a3f2e7cb7315c1e48801cb8c6a86d2d2**

**• 80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce**

**• 506f3b12853375a1fbbf85c82ddf13341cf941c5acd4a39a51d6addf145a7a51**

**A screenshot of the test for the C2 IP above is shown in fig 3.2.1**

**Recent incidence: AWS: A new ransomware threat called Code finger targets users of AWS S3**

**buckets and makes recovery without payment impossible. **

**APT19 is a Chinese-based threat group that has. Also known as deep panda group, they go with**

**different aliases like Codes Team, Codoso, C0d0so0, Sun shop Group, TG-3551, Bronze Firestone,**

**Pupa, Red Pegasus. They infiltrate networks through methods like spear-phishing and exploits to steal**

**information by establishing persistence, moving laterally, and exfiltration data via command-andcontrol channels**

**Target industries: they have targeted a variety of industries, including defence, finance, energy,**

**pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services**

**Motivation: Primarily cyber espionage and information theft, potentially in support of broader**

**economic or strategic interests of China**

**Indicators of Compromise:**

**• Malware: Suspicious filenames that don't match legitimate software, especially those with**

**double extensions (e.g., report.pdf.exe) or generic-sounding names that might be out of place.**

**• Tactics: These often involve spear-phishing for initial access, leveraging system tools and**

**vulnerabilities for execution and lateral movement, and establishing command and control for**

**data exfiltration.**

**• Domain IPs:**

**File hashes: SHA256:**

**DE33DFCE8143F9F929ABDA910632F7536FFA809603EC027A4193D5E57880B292**

**SHA256:**

**76e7ce4ab6d520f0717bb0dea8ff6973e1f7c6ea39f7138a5eb5d5483fd21e21 (Mentioned in the**

**LMNTRIX blog analysis as exploiting CVE-2017-0199)**

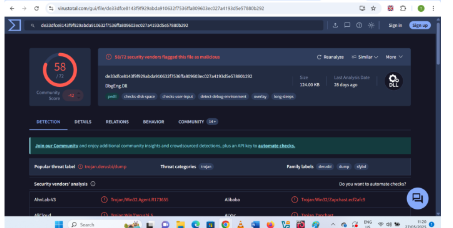
**Fig 3.3.1 below shows a test result of the file hash above.**

**Recent incidence: in September 2024, APT19 targeted organizations in North America and**

**Australia for intelligence and espionage purposes. Their toolkit included Drubs backdoor,**

**Poison Ivy and cobalt strike as a payload. The infection chain started with a spear-phishing**

**campaign using an RTF exploit (CVE-2017-0199) delivered via a linked external URL.**

****

**Also known as Scattered Spider and Octo Tempest, is a cybercriminal group known for its**

**sophisticated social engineering tactics used to gain initial access to target organizations, often**

**leading to data theft and/or ransomware deployment (frequently with Black Cat/ALPHV ransomware).**

**UNC3944 is experimenting with proactive persistence mechanisms, using remote monitoring tools**

**like Altera and Synchro, and leveraging legitimate services to evade detection. They continue to use**

**social engineering as a primary initial access method, including help desk impersonation**

**Target Industries: Telecommunications, , hospitality, retail, media and entertainment, financial**

**services, and technology. They have notably targeted casinos**

**Motivation: Primarily financial gain through data extortion and ransomware to disrupt operations**

**Indicators of Compromise**

**• Malware: Unexpected files appearing in startup folders or registry run keys.**

**Unfamiliar processes running in Task Manager.**

**Unusual network traffic patterns**

**Modifications to system files or configurations without legitimate reasons**

**• Tactics: It heavily involves sophisticated social engineering like phishing, help desk**

**Impersonation, SIM swapping, and MFA fatigue to gain initial access, followed by "living off the**

**Land" techniques, credential theft, and potentially data exfiltration and ransomware deployment**

**• Domain/IPs:**

**- Phishing Pages: Subdomains designed to mimic legitimate login portals**

**- Data Exfiltration: They might use subdomains for temporary storage or C2 related to commodity**

**Malware**

**- Look for newly registered subdomains that closely resemble legitimate company domains**

**Recent incidence: UK Retail Attacks (April-May 2025): There has been a notable surge in attacks against**

**Major UK retailers, including Marks & Spencer (M&S) and Co-op. These attacks are believed to be linked**

**13 | P a g e**

**To Scattered Spider and have caused significant disruption. The M&S attack, which occurred around the**

**Easter weekend, impacted online ordering and contactless payments, with disruptions expected to last**

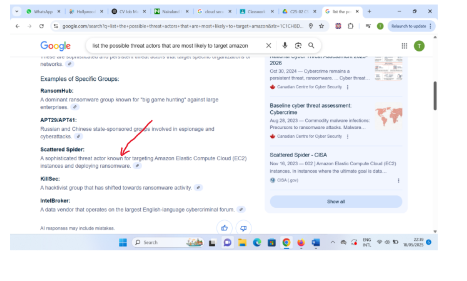
**Until July and cost the company significantly. The Co-op also experienced a ransomware attack affecting**

**Store operations.**

**http://cybermagazine.com/technology-and-ai/m-ss-cyber-incident-what-do-we-know-so-far**

**https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-**

**320a#:~:text=Scattered%20Spider%20is%20a%20cybercriminal,cyberattack%20by%20Scattered%20S**

****

**5. AKIRA**

**This group emerged in 2023 and is believed to have ties to the former Conti ransomware group. They**

**have been actively targeting organizations and are known for using a double-extortion model**

**(encrypting data and exfiltration it for ransom)**

**Target industries: Retail, manufacturing, Education institutions, Finance, Healthcare/Medical, IT**

**service providers and technology companies, and Construction.**

**Motivation: financial gain through the double extortion model: encrypting victims' data and**

**exfiltration sensitive information, threatening to leak it if the ransom is not paid.**

**Indicators of compromise**

**14 | P a g e**

**• Malware: Look for specific filenames associated with their ransomware executable or related**

**tools**

**File Hashes: SHA256, MD5, or SHA1 hashes**

**• Tactics: include exploiting VPN vulnerabilities or compromised RDP for initial access, followed**

**by credential theft, data exfiltration, and ultimately ransomware deployment.**

**• Domains/IPs:**

**- Tor Sites**

**- Command and Control (C2) Servers**

**Recent Incidences:**

**April 2025: Hitachi Vantaa Disruption: The IT services management subsidiary of Hitachi reportedly**

**had its servers taken down by an Akira ransomware attack. Files were allegedly infiltrated, impacting both**

**Hitachi Vantaa Manufacturing and its systems. There were also reports of government organization project being affected**

**Part Four: TTP Mapping with MITRE ATT&CK**

**The biggest threat actor amongst the above listed is the scattered spider, also known as UNC3944, also**

**goes by many aliases, (Octo Tempest, Roasted Oktapus, Scatter Swine, Storm-0875) is a notorious**

**cybercriminal group who are financially motivated and known for their sophisticated social engineering**

**tactics. The group has been active since 2022. They have been known to target industries like**

**telecommunications, customer relationship management and technology companies. But have over the**

**years, expanded their targets to include retail, hospitality, manufacturing and financial sectors. Scattered**

**Spider's operations have involved targeted social engineering and attempts to evade common endpoint**

**security. More recently, their activities have expanded to include ransomware deployment for financial**

**profit.**

**15 | P a g e**

**Their combination of advanced social engineering, ability to bypass strong authentication,**

**persistence techniques, and their shift towards ransomware, coupled with their growing focus on**

**cloud environments, makes them a highly capable and dangerous threat actor for any large**

**organization, including CLOUDS. Their past successes against major corporations further underscore**

**this threat.**

**Sources: https://attack.mitre.org/groups/G1015/**

**https://www.darkreading.com/search?q=UNC3944**

**https://otx.alienvault.com/pulse/6808456074f76f5b134bac73**

**https://www.silentpush.com/blog/scattered-spider-2025/**

**Google dorks.**

**The tools and techniques used by UNC3944**

**UNC3944 often leverages a mix of legitimate software, custom phishing kits, and publicly available**

**reconnaissance tools.**

**• Any Desk: A legitimate remote desktop software often deployed for persistent access and**

**control. They are known to install multiple Remote Monitoring and Management (RMM) tools to**

**ensure a back door remains, e.g Altera, Synchro.**

**Technique used: T1219: “Remote Access Software”**

**T1021.001 “Remote Services: RDP”**

**• EIGHTBAIT: A phishing kit used to send intercepted login data to attacker-controlled T Part Four: TTP Mapping with MITRE ATT&CK**

**The biggest threat actor amongst the above listed is the scattered spider, also known as UNC3944, also**

**goes by many aliases, (Octo Tempest, Roasted Octopus, Scatter Swine, Storm-0875) is a notorious**

**cybercriminal group who are financially motivated and known for their sophisticated social engineering**

**tactics. The group has been active since 2022. They have been known to target industries like**

**telecommunications, customer relationship management and technology companies. But have over the**

**years, expanded their targets to include retail, hospitality, manufacturing and financial sectors. Scattered**

**Spider's operations have involved targeted social engineering and attempts to evade common endpoint**

**security. More recently, their activities have expanded to include ransomware deployment for financial**

**profit.**

**15 | P a g e**

**Their combination of advanced social engineering, ability to bypass strong authentication,**

**persistence techniques, and their shift towards ransomware, coupled with their growing focus on**

**cloud environments, makes them a highly capable and dangerous threat actor for any large**

**organization, including CLOUDS. Their past successes against major corporations further underscore**

**this threat.**

**Sources: https://attack.mitre.org/groups/G1015/**

**https://www.darkreading.com/search?q=UNC3944**

**https://otx.alienvault.com/pulse/6808456074f76f5b134bac73**

**https://www.silentpush.com/blog/scattered-spider-2025/**

**Google dorks.**

**The tools and techniques used by UNC3944**

**UNC3944 often leverages a mix of legitimate software, custom phishing kits, and publicly available**

**reconnaissance tools.**

**• Any Desk: A legitimate remote desktop software often deployed for persistent access and**

**control. They are known to install multiple Remote Monitoring and Management (RMM) tools to**

**ensure a back door remains, e.g Altera, Synchro.**

**Technique used: T1219: “Remote Access Software”**

**T1021.001 “Remote Services: RDP”**

**• EIGHTBAIT: A phishing kit used to send intercepted login data to attacker-controlled**

## ****MITRE ATT&CK TTP Mapping – Scattered Spider (UNC3944 / Octo Tempest / Storm-0875)****

| **Tool / Method** | **Description** | **MITRE Technique ID** | **Technique Name** | **Observed Impact on Victims** |
| --- | --- | --- | --- | --- |
| **Any Desk (RMM Tools: Altera, Synchro, etc.)** | **Legitimate remote desktop & RMM tools installed for persistent access and control.** | **T1219** | **Remote Access Software** | **Long-term persistence, remote control of compromised systems.** |
|  |  | **T1021.001** | **Remote Services: RDP** | **Unauthorized access to internal networks.** |
| **EIGHTBAIT (Phishing Kit)** | **Used to send intercepted login data to attacker-controlled infrastructure.** | **T1566** | **Phishing** | **Credential theft, initial foothold in victim networks.** |
|  |  | **T1078** | **Valid Accounts** | **Abuse of legitimate credentials to evade detection.** |
| **Custom & Public Reconnaissance Tools** | **Open-source tools and Google Dorks for information gathering on targets.** | **T1592** | **Gather Victim Host Information** | **Identification of vulnerable assets and targets.** |
|  |  | **T1593** | **Search Open Websites/Domains** | **Discovery of public-facing systems.** |
|  |  | **T1596** | **Search Open Technical Databases** | **Leveraging public info (e.g., GitHub, WHOIS) for attack planning.** |
| **Social Engineering Attacks** | **Direct engagement with victims (SMS, calls, chats) to trick them into giving credentials or MFA codes.** | **T1078.004** | **Valid Accounts: Cloud Accounts** | **Unauthorized cloud access.** |
|  |  | **T1621** | **Multi-Factor Authentication Request Generation** | **MFA fatigue attacks leading to compromise.** |
|  |  | **T1656** | **Impersonation** | **Deception of employees to escalate privileges.** |
| **Ransomware Deployment** | **Encrypting victim systems and demanding ransom for financial gain.** | **T1486** | **Data Encrypted for Impact** | **Business disruption, financial extortion, reputational damage.** |
| **Persistence Techniques** | **Multiple RMM tools + stolen accounts for long-term access.** | **T1136** | **Create Account** | **Creation of hidden backdoor accounts.** |
|  |  | **T1547** | **Boot or Logon Auto start Execution** | **Ensures malware or access tools reload after reboot.** |
| **Cloud Targeting** | **Abuse of cloud environments for access, data theft, and ransomware.** | **T1530** | **Data from Cloud Storage** | **Theft of sensitive corporate/customer data.** |
|  |  | **T1078.004** | **Valid Accounts: Cloud Accounts** | **Expanded control over cloud infrastructure.** |

**FINAL FINDINGS & IMPACT**

**After analyzing the different Indicators of Compromise of these threat actors, the different TTPs, the**

**Applicable threats, potential risks and vulnerabilities found during a security risk assessment, the**

**Weaknesses discovered were information shared publicly online such as internal emails, URLs,**

**Unmonitored IPs and domains, online Job postings detailing internal tools used for day to day operations.**

**These make CLOUDS susceptible to lurking threat actors who can capitalize on this information to gain**

**Unauthorized access, implement command and control (C2), lateral movements across the network and**

**Ultimately deploy ransomware to encrypt data, giving them leverage to demand ransom in huge sums.**

**Impact: The financial impact cannot be overemphasized, neglecting actions on threat intelligence feeds**

**and recommendations can lead to heavy financial losses, ranging from law suits, to multi-million dollar**

**ransoms, in many cases. The company suffers reputational dents and loss of trust by its clients. In 2024,**

**the average cost of a ransomware attack reached $5.13 million USD, including ransom payments and**

**recovery costs. Prevention is the most effective way to avoid these substantial expenses.**

### Recommendations

**Based on the findings, the following measures are recommended. CLOUDS should adopt a defense-in-depth strategy that directly addresses the tactics, techniques, and procedures (TTPs) leveraged by financially motivated threat actors such as UNC3944 (Scattered Spider) and ransomware operators like Lock Bit. This requires a strong focus on user awareness, robust identity and access management, and proactive detection and response.**

#### Specific Actions

1. **Enhance Social Engineering Awareness Training**
   * **Conduct regular, comprehensive training programs on tactics such as help desk impersonation, phishing, smashing, and MFA fatigue.**
   * **Reinforce the practice of verifying requests through trusted, out-of-band channels.**
2. **Strengthen Identity and Access Management (IAM)**
   * **Enforce Multi-Factor Authentication (MFA) across all critical accounts, using resilient methods (e.g., FIDO2 keys).**
   * **Regularly review and audit user privileges, applying the principle of least privilege.**
   * **Enforce strong password policies and promote the use of password managers, while remaining aware of potential threats targeting them.**
3. **Bolster Help Desk Security Protocols**
   * **Introduce strict identity verification for requests involving password resets, MFA changes, or account access.**
   * **Train help desk staff to treat unsolicited requests with caution and verify identities via pre-established, out-of-band communication methods.**
4. **Improve Endpoint Security**
   * **Deploy and maintain Endpoint Detection and Response (EDR) solutions capable of detecting suspicious use of legitimate remote access tools and attempts to disable security defenses.**
5. **Implement Network Segmentation**
   * **Segment networks to restrict lateral movement and minimize the impact of a successful intrusion.**
6. **Maintain Robust Backup and Recovery**
   * **Regularly back up critical data to offline and immutable storage.**
   * **Test recovery procedures frequently to ensure rapid and reliable restoration during an incident.**
7. **Enhance Monitoring and Threat Intelligence**
   * **Continuously monitor logs, network traffic, and authentication activity for anomalies.**
   * **Integrate external threat intelligence feeds to stay current on the latest TTPs and indicators of compromise (IOCs) associated with UNC3944 and LockBit.**

**✅ By implementing these recommendations, CLOUDS can significantly reduce its exposure to persistent, evolving threats and strengthen resilience against sophisticated ransomware campaigns and social engineering-drive: CONCLUSION**

**This report has shown the availability of some sensitive information on CLOUDS, exposed publicly online**

**through which threat Actors can gain access to the Network by exploiting weaknesses and vulnerabilities.**

**It also outlined the tactics, techniques, and procedures (TTPs) associated with the financially motivated**

**cybercriminal group UNC3944 (Scattered Spider) and other prevalent Lock Bit ransomware operation.**

**UNC3944 distinguishes itself through its sophisticated social engineering capabilities, often serving as an**

**initial access vector for subsequent malicious activities, including ransomware deployment. Their**

**methods frequently involve manipulating individuals, particularly help desk personnel, to gain**

**unauthorized access, bypass multi-factor authentication, and establish a foothold within target**

**Environments. They also leverage legitimate tools for persistence, lateral movement, and command and**

**control.**

**Therefore, CLOUDS must adopt a proactive and multi-layered security approach (as outlined in the**

**Recommendations) to defend against these threats.**

**References:**

**1. Threat book CTI: https://threatbook.io/blog/APT32-Poisoning-GitHub,-Targeting-ChineseCybersecurity-Professionals-and-Specific-Large-Enterprises**

**2. The Henry M. Jackson School of International Studies**

**University of Washington May 20, 2025, AUTHOR: RICHIE DOAN**

**https://jsis.washington.edu/news/analyzing-oceanlotus-apt32-indicators-of-stateassociation/#:~:text=Threatbook%20CTI.,January%208%2C%202025.**

**3. LMNTRIX: September 25, 2024 https://lmntrix.com/blog/analysis-of-apt19-campaign/**

**4. Cyber Magazine: April 28, 2025 http://cybermagazine.com/technology-and-ai/m-sscyber-incident-what-do-we-know-so-far**

**5. America’s Cyber Defense Agency: November 16, 2023**

**https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-**

**320a#:~:text=Scattered%20Spider%20is%20a%20cybercriminal,cyberattack%20by%20**

**Scattered%20Spider%20actors.**

**6. MITRE Attack framework https://attack.mitre.org/groups/G1015/**

**7. Alien Vault OTX: https://otx.alienvault.com/pulse/6808456074f76f5b134bac73**

**8. Silent push: https://www.silentpush.com/blog/scattered-spider-2025/**

**9. Spin.ai: 2025 https://spin.ai/resources/ransomware-tracker/**

**10. Office of Information Technology, State of Alabama : May 2025**

**https://oit.alabama.gov/cybereventmay2025/#:~:text=5%2F12%2F2025,OFFICE%20OF**

**%20INFORMATION%20TECHNOLOGY**

**21 | P a g e**

**11. Perplexity.ai: https://www.perplexity.ai/discover/top/nucor-halts-production-due-toG7w\_F8JrTlSGEtVbx2vaAg#:~:text=Nucor%20halts%20production%20due%20to,Produ**

**ction%20Restart%20Timeline**

**12. DARKREADING: https://dr-resources.darkreading.com/free/w\_zsca59/?p=w\_zsca59**

**Top of Form**

**Bottom of Form**

**Top of Form**

**Bottom of Form**

**Top of Form**

**Bottom of Form**