09
SEP

THREAT INTEL REPORT 2024

CONVERGE
TECHNOLOGY SOLUTIONS

Prepared by: Converge Cybersecurity Practice
convergetp.com/cybersecurity | 800.747.8585

Observations for September 2024

The recent surge in cyber threats demands heightened attention from organizations, especially those in critical infrastructure sectors. RansomHub, a Ransomware-as-a-Service (RaaS) operation, has rapidly gained momentum since its emergence earlier this year. With a focus on data theft over encryption and recruitment of affiliates from other major ransomware groups, the group has been linked to over 210 breaches across industries such as healthcare, finance, and telecommunications. This report outlines key strategies for mitigating these evolving threats.

Additionally, U.S. agencies have issued warnings regarding Iranian state-sponsored groups involved in enabling ransomware operations. These groups have targeted sectors like education, finance, healthcare, and defense, working with ransomware affiliates such as ALPHV and Ransomhouse. Their cyber activities aim to gather sensitive data that could serve national objectives, making it essential to understand their tactics and implement targeted defenses.

Misconfigurations in cloud environments, particularly within AWS, have also posed significant risks. Recent incidents, including the ALBeast misconfiguration issue and a large-scale extortion campaign exploiting exposed environment variable files, demonstrate how easily attackers can exploit weaknesses. Adhering to robust cloud security practices is critical to prevent unauthorized access and data breaches.

This report delves into these threats and provides actionable insights and mitigation techniques to help organizations strengthen their defenses against a dynamic and evolving cyber landscape.

RETURN

Executive Overview

RansomHub Ransomware-as-a-Service (RaaS)

Audience

- CISO
- C-Suite Executives
- IT Managers
- Risk Management Professionals
- Cybersecurity Professionals and Analysts

SUMMARY: RansomHub, a relatively new but highly active Ransomware-as-a-Service (RaaS) operation, has surged in activity since its debut in February 2024. Linked to over 210 breaches, the group primarily targets critical U.S. infrastructure sectors using double-extortion tactics. The group's aggressive expansion is bolstered by the recruitment of high-profile affiliates from other notorious ransomware strains like LockBit and ALPHV. RansomHub's focus on data theft over file encryption distinguishes it in the RaaS ecosystem, with their attacks resulting in severe data breaches across sectors including healthcare, financial services, and telecommunications. This report explores the operational methods of RansomHub and outlines strategic and tactical countermeasures for defending against these evolving threats.

Tactical guidance >> RansomHub Ransomware-as-a-Service (RaaS)

Iran's Threat on Critical Infrastructure

Audience

- CISO
- HR
- Security Managers
- Cybersecurity Professionals

SUMMARY: In August 2024, U.S. agencies issued a cybersecurity advisory warning critical infrastructure organizations of cyber threats emanating from Iranian state-sponsored groups. These threat actors, known in the private sector as Pioneer Kitten, UNC757, Rubidium, and Lemon Sandstorm, have targeted multiple sectors including education, finance, healthcare, and defense. The groups have shifted their focus toward enabling ransomware attacks, collaborating with ransomware affiliates such as NoEscape, Ransomhouse, and ALPHV (BlackCat). Their operations extend to stealing sensitive information, which is likely to support the Government of Iran's (GOI) objectives. This report provides a breakdown of their tactics, techniques, and procedures (TTPs) and suggests mitigation strategies.

Tactical guidance >> Iran's Threat on Critical Infrastructure

RETURN

Audience

- Organizations utilizing AWS
- C-Suite Executives
- Cybersecurity Professionals
- IT Engineering Teams
- Network and IT Administrators

Threat or Misconfiguration in SaaS Solutions

SUMMARY: Recent discoveries have underscored the risks posed by misconfigured cloud infrastructure, particularly within Amazon Web Services (AWS) environments. Two key developments—referred to as the "ALBeast" configuration issue involving AWS Application Load Balancer (ALB) and a large-scale extortion campaign exploiting exposed environment variable files (.env)—illustrate how misconfigurations, rather than inherent system vulnerabilities, can provide attackers with unauthorized access to sensitive data and systems. This report examines these incidents, emphasizing the importance of adhering to robust cloud security practices to mitigate such risks.

Tactical guidance >> Threat or Misconfiguration in SaaS Solutions

Tactical Guidance

RansomHub Ransomware-as-a-Service (RaaS)

Overview & Impact

RansomHub has become a leading player in the ransomware landscape in 2024, accounting for 43 attacks in July alone. Known for leveraging affiliates from other prominent ransomware groups, RansomHub specializes in exfiltration-based extortion, selling stolen data to the highest bidder if ransom negotiations fail. Their activity is notable for its impact on critical infrastructure sectors, with high-profile attacks on organizations such as Patelco Credit Union, Rite Aid, Halliburton, and Frontier Communications, which resulted in the exposure of over 750,000 individuals' data. The group has also exploited several critical vulnerabilities, including those in Citrix NetScaler (CVE-2023-3519) and F5 BIG-IP (CVE-2023-46747).

Linked to over 210 breaches, the group targets critical infrastructure sectors

Observations

- **RansomHub Affiliates:** Attracted former members of prominent ransomware groups such as LockBit and ALPHV.
- **Targeted Sectors:** Water and wastewater, healthcare, financial services, telecom, and critical infrastructure.
- **Double-Extortion Tactics:** Encrypts systems and exfiltrates sensitive data for ransom negotiations.
- **Use of Known Vulnerabilities:** Exploited vulnerabilities like CVE-2023-3519 (Citrix NetScaler) and CVE-2023-46747 (F5 BIG-IP).
- **Data Leak Strategy:** Uses a Tor-based data leak site to publish victim data, amplifying pressure to pay the ransom.

RETURN

Guidance

Strategic Intelligence

- **Ransomware-as-a-Service (RaaS) Model:** RansomHub's RaaS model has proven highly efficient, drawing in affiliates from other successful ransomware groups.
- **Affiliate Recruitment:** The group has a broad affiliate network, offering a 90-10 revenue split to partners, encouraging further expansion and attacks.
- **Geopolitical Dynamics:** RansomHub refrains from attacking organizations in CIS countries, suggesting ties to criminal entities in the region.
- **Continued Growth:** RansomHub's rapid growth, from 27 attacks in June to 43 in July, indicates continued recruitment and scaling of operations.

Operational Intelligence

- **Entry Points:** Exploits publicly exposed remote desktop protocols (RDP) services and vulnerabilities in widely used systems such as Citrix and F5.
- **Persistence Techniques:** Uses Mimikatz to harvest credentials and lateral movement via tools like PsExec, Cobalt Strike, and AnyDesk.
- **EDR Bypass:** Deploys custom tools to disable endpoint detection and response (EDR) systems.
- **Encryption Techniques:** Employs intermittent encryption using Curve 25519, appending unique byte sequences to encrypted files to complicate decryption.

Tactical Intelligence

- **Initial Access:** Phishing and exploitation of known vulnerabilities like CVE-2023-3519 are the main vectors.
- **Data Exfiltration:** Utilizes tools like WinSCP, rclone, and Cobalt Strike for exfiltration, often uploading data to cloud storage providers such as Mega.
- **Command-and-Control (C2):** Affiliates leverage PsExec, Metasploit, and other dual-use tools for lateral movement and C2 operations.
- **Indicators of Compromise (IOCs):** Identifiers include malicious RDP connections, high outbound traffic spikes (over 150 GB), and the presence of tools like AngryIPScanner and Nmap.

Threat Hunting Hypotheses

Data Exfiltration via High Network Traffic Spikes:

- **Hypothesis:** Large volumes of outbound traffic, particularly over short periods, may indicate ongoing data exfiltration efforts by RansomHub affiliates using tools such as rclone or WinSCP. These activities are likely to cause noticeable spikes in network traffic, especially in critical sectors.
- **Investigation Approach:**
  - Monitor outbound network traffic for unusual spikes exceeding normal data flow, particularly volumes over 150 GB.

RETURN

  - Use network security controls to flag data transfers involving external cloud storage services like Mega or AWS S3.
  - Set up alerts for sudden, large transfers to new or previously unused external endpoints.
  - Correlate the timing of traffic spikes with other indicators of compromise, such as suspicious login activity or the presence of known RansomHub tools like AngryIPScanner.

Exploitation of Known Vulnerabilities (e.g., Citrix, F5, Fortinet):

- **Hypothesis:** RansomHub affiliates often exploit publicly disclosed vulnerabilities, such as CVE-2023-3519 (Citrix NetScaler) and CVE-2023-46747 (F5 BIG-IP). Unpatched systems are at risk of compromise through these vulnerabilities.
- **Investigation Approach:**
  - Conduct regular scans for systems running vulnerable software versions, particularly Citrix and F5 appliances.
  - Review security logs for exploit attempts targeting these CVEs.
  - Prioritize patching for systems identified with vulnerabilities that are actively exploited in the wild.
  - Set up alerts to detect abnormal access attempts or configuration changes on Citrix, F5, and Fortinet devices.

Suspicious Lateral Movement Across the Network:

- **Hypothesis:** RansomHub affiliates use lateral movement tools like PsExec, Cobalt Strike, and Metasploit to gain broader access across compromised networks. Unexpected lateral movements, especially from lower-privileged accounts, could indicate an ongoing attack.
- **Investigation Approach:**
  - Monitor for unusual or unauthorized PsExec executions, particularly on critical servers.
  - Track lateral movement patterns within the network, including the use of remote desktop protocols (RDP) and suspicious service creations.
  - Set up detection rules to identify Cobalt Strike beacons or Metasploit usage.
  - Analyze logs for the use of Windows Management Instrumentation (WMI) for privilege escalation and antivirus deactivation.

Use of Anonymizing Tools for Persistence and Evasion:

- **Hypothesis:** Threat actors may deploy VPNs, proxy servers, or TOR to mask their true location and evade detection. These tools are often used to maintain persistence while accessing compromised systems.
- **Investigation Approach:**
  - Analyze network traffic for signs of VPN or proxy tool usage that might indicate an adversary attempting to obfuscate their actions.

Sources

- Bleeping Computer: RansomHub Ransomware Breached 210 Victims Since February
- Check Point: What is RansomHub Ransomware?
- Group-B: RansomHub RaaS Group Expands Operations
- SOC Prime: RansomHub Detection: Growing Threat to Critical Infrastructure
- Industrial Cyber: CISA and FBI Issue Joint Advisory on RansomHub Ransomware Threat

RETURN

  - Correlate login activity with known VPN and anonymization tool usage, especially when accessing sensitive systems.
  - Flag persistent connections to TOR exit nodes or proxy servers associated with high-risk activities.
  - Implement geofencing to detect access attempts from unexpected or masked locations.

The groups have shifted their focus toward enabling ransomware attacks

Iran’s Threat on Critical Infrastructure

Overview & Impact

The Iranian threat actors identified in this advisory are involved in a variety of malicious activities, primarily focusing on exploiting vulnerabilities in widely used networking devices to gain access to critical infrastructure systems. They then collaborate with ransomware affiliates, offering network access and assisting in ransomware deployments. The impact of these activities includes significant operational disruptions, potential data breaches, and financial loss from ransomware extortion.

Key sectors affected include:

- **Education**
- **Finance**
- **Healthcare**
- **Defense**
- **Local Governments**

These sectors have reported unauthorized network access and instances of ransomware attacks orchestrated by these actors. The collaborative nature of these campaigns, particularly with ransomware affiliates, highlights the growing complexity and sophistication of the cyber threat landscape.

Observations

- **Targeted Sectors:** Education, finance, healthcare, defense, and local governments in the U.S., Israel, Azerbaijan, and UAE.
- **Actor Collaboration:** The identified groups are facilitating ransomware operations by providing access to compromised networks.
- **TTPs:**
  - **Exploitation of Public-Facing Networking Devices:** Vulnerabilities such as CVE-2024-3400 (PanOS firewalls), CVE-2022-1388 (BIG-IP F5 devices), and CVE-2023-3519 (Citrix Netscaler).

  - **Credential Reuse:** Compromised credentials from networking devices reused to access additional applications and infrastructure.
  - **Ransomware Collaboration:** Working with ransomware groups including NoEscape, Ransomhouse, and ALPHV (BlackCat) to monetize network access.
  - **Hack-and-Leak Operations:** Historical campaigns, such as Pay2Key, suggest motivations beyond financial gain, with a focus on information operations aimed at undermining foreign cyber infrastructures.

Guidance

Strategic Intelligence

- **Iranian State Sponsorship:** The groups are linked to the Government of Iran, operating through the IT company Danesh Novin Sahand, likely as a front for cyber operations.
- **Geopolitical Motivations:** Beyond ransomware, these actors conduct campaigns to steal sensitive information, particularly in Israel and the UAE, supporting GOI intelligence efforts.
- **Increased Collaboration:** The actors' partnership with ransomware affiliates indicates a shift in strategy, where cyber espionage and financial gain are intertwined.

Operational Intelligence

- **Indicators of Compromise (IOCs):**
  - Targeting of devices vulnerable to CVE-2024-3400, CVE-2022-1388, CVE-2019-19781, and CVE-2023-3519.
  - Use of compromised credentials for lateral movement within victim networks.
  - Reuse of usernames and deployment of NGROK and Ligolo for network tunneling.
  - Creation of webshells in specific directories to maintain persistence.
- **Mitigation Strategies:**
  - Patch known vulnerabilities (CVE-2024-3400, CVE-2022-1388, CVE-2019-19781).
  - Monitor network traffic for unusual activities, especially around VPN and firewall devices.
  - Implement stringent password policies and multi-factor authentication (MFA) to prevent credential reuse.

Tactical Intelligence

- **Ransomware Affiliates:** Collaboration with NoEscape, Ransomhouse, and ALPHV (BlackCat) provides ransomware affiliates with access to networks, enabling them to lock down systems and extort victims.
- **Exploitation Methods:**
  - **Initial Access:** Through VPN and firewall vulnerabilities.

RETURN

- ◦ **Privilege Escalation:** Reuse of compromised administrator credentials to gain domain control.
- ◦ **Persistence:** Deployment of webshells and use of tools like PowerShell to reduce security configurations.
- ◦ **Reconnaissance:** Use of Shodan search engine to identify vulnerable IP addresses.

Threat Hunting Hypotheses

Exploitation of Known CVEs in Public-Facing Networking Devices

- **Hypothesis:** Threat actors are leveraging known vulnerabilities in public-facing devices, such as VPNs and firewalls, to gain unauthorized access to critical infrastructure networks. Focused exploitation of vulnerabilities, such as CVE-2024-3400 (PanOS firewalls) and CVE-2022-1388 (BIG-IP F5 devices), may indicate the initial access point for the attackers.
- **Investigation Approach:**
    - Monitor for exploitation attempts or suspicious traffic related to these specific CVEs (CVE-2024-3400, CVE-2022-1388, CVE-2019-19781, CVE-2023-3519).
    - Analyze firewall, VPN, and endpoint logs for abnormal access patterns or brute force attempts targeting vulnerable devices.
    - Cross-reference traffic data with known Indicators of Compromise (IOCs), such as specific IP addresses scanning for these vulnerabilities.
    - Implement real-time alerts for any unauthorized or unexpected changes in configuration files or credentials on public-facing devices.

Credential Reuse from Exploited Devices for Privilege Escalation

- **Hypothesis:** Threat actors may be reusing credentials obtained from compromised VPNs or firewall devices to escalate privileges and gain further access to critical systems, such as domain controllers.
- **Investigation Approach:**
    - Monitor authentication logs for abnormal login patterns using administrative credentials on critical systems like domain controllers.
    - Audit account usage to detect signs of lateral movement, particularly the use of previously compromised credentials across different services.
    - Implement alerts for the creation of new administrative accounts or unusual privilege escalation events.

Collaboration with Ransomware Affiliates for Network Lockdown

- **Hypothesis:** After initial compromise, threat actors collaborate with ransomware affiliates (e.g., NoEscape, Ransomhouse, ALPHV/BlackCat) to lock victim networks and extort ransom payments.
- **Investigation Approach:**
    - Monitor for encrypted files or abnormal encryption-related activities on critical systems.
    - Analyze logs for signs of ransomware affiliates' known TTPs, including the use of tools like NGROK and Ligolo to establish tunnels for remote access.

RETURN

  - Investigate any unauthorized changes to network security configurations, particularly firewalls, to identify where ransomware actors may be preparing for encryption operations.

Use of Shodan for Vulnerability Scanning and Reconnaissance

- **Hypothesis:** Threat actors use tools like Shodan to search for publicly available devices that are vulnerable to specific CVEs, conducting reconnaissance before attempting exploitation.
- **Investigation Approach:**
  - Review external traffic logs to identify incoming connections from known reconnaissance tools like Shodan.
  - Correlate traffic patterns with suspicious scanning activities targeting specific ports or services associated with known vulnerable devices.
  - Implement defensive measures such as geofencing or rate-limiting on exposed services to mitigate potential reconnaissance activities.

Sources

- Industrial Cyber: Critical Infrastructure Under Attack as US Agencies Sound Alarm on Cyber Threat from Iranian-Linked Groups
- The Record: Iran Cyber Operations Exposed in Reports from Google, Microsoft
- Reuters: US Says Iran Cyber Operations Targeted Trump, Harris Campaigns
- InfoSecurity Magazine: Iran Hackers Secretly Aid Ransomware Operations
- CISA: Iran-Based Cyber Actors Enabling Ransomware Attacks on U.S. Organizations

The "ALBeast" config issue exposed environment variable files (.env)

Threat or Misconfiguration in SaaS Solutions

Overview & Impact

Misconfigurations in cloud environments, such as improper AWS Application Load Balancer usage and exposed .env files, represent significant security threats. These misconfigurations enable attackers to bypass authentication protocols, access sensitive information, and escalate their access rights. The ALBeast issue and the extensive campaign targeting 230 million cloud environments highlight the severe consequences of insecure cloud setups, including data exfiltration and extortion. Despite AWS's updates and recommendations, organizations must prioritize secure configurations and vigilance to avoid becoming vulnerable to these threats.

Observations

- **ALBeast Configuration Risk:** Up to 15,000 applications using AWS's Application Load Balancer (ALB) for authentication may be susceptible to unauthorized access due to misconfigurations. This allows attackers to forge tokens and impersonate legitimate users, circumventing authentication mechanisms.

RETURN

- **Exploitation of Exposed .env Files:** Attackers exploited over 230 million cloud environments by accessing publicly available .env files. These files contained sensitive credentials, which facilitated unauthorized access, data exfiltration, and extortion attempts.
- **IAM Privilege Escalation:** Using compromised IAM credentials obtained from exposed .env files, attackers were able to create new roles with administrative privileges, enabling further exploitation of cloud environments.
- **AWS Mitigation Efforts:** AWS has responded by updating its documentation and recommending best practices, such as limiting traffic to ALBs and verifying token signatures to prevent exploitation.

Guidance

Strategic Intelligence

- **Cloud Misconfigurations as a Persistent Threat:** Misconfigured cloud services continue to be a primary vector for unauthorized access and exploitation. These security lapses are increasingly being targeted by threat actors, who leverage them to bypass access controls and infiltrate systems.
- **Automated Attack Techniques:** The extensive use of automated tools by attackers, which allowed them to scan over 110,000 domains for vulnerabilities, highlights the critical need for continuous security monitoring and stringent configuration management in cloud environments.
- **Evolving Tactics in Cloud Exploitation:** Attackers are shifting their focus to cloud infrastructure, leveraging weaknesses such as misconfigured AWS IAM policies, exposed S3 buckets, and unsecured Lambda functions to carry out data exfiltration and extortion.

Operational Intelligence

- **AWS Response to ALBeast:** AWS disputes the classification of ALBeast as a vulnerability, attributing the issue to misconfigured customer applications. AWS advises users to implement security best practices, such as restricting inbound traffic to the ALB and validating signatures to prevent unauthorized access.
- **Best Practices for ALB Security:** Organizations are urged to configure their applications to authenticate traffic only from their designated ALB and to ensure proper verification of token signatures. This helps mitigate the risk of attackers exploiting misconfigurations to gain access.
- **Mitigating Risks from Exposed .env Files:** Secure configuration practices, including access controls and secret management, are essential to avoid exposing sensitive credentials via publicly accessible .env files. Organizations should routinely audit their cloud environments to detect and rectify these vulnerabilities.

Tactical Intelligence

- **ALBeast Attack Process:**
  - The attacker sets up an ALB instance within their account, configured to authenticate requests.
  - A forged token is signed by the attacker's ALB, impersonating a legitimate user.

RETURN

    - The attacker alters the ALB configuration to make it appear as though the token originated from the victim, bypassing authentication protocols and gaining unauthorized access.

- **Exploitation of .env Files:**
    - Attackers scan domains for publicly exposed .env files, which often contain sensitive information such as API keys and credentials.
    - These credentials are then used to escalate privileges within AWS, allowing the attackers to create new IAM roles with full administrative rights.
    - After infiltrating systems, attackers exfiltrate data and place ransom notes within compromised S3 buckets, demanding payment to prevent the public release of the stolen information.

Threat Hunting Hypotheses

Threat Hunt Hypothesis: Exploitation of AWS ALB Misconfigurations

- **Hypothesis:** Threat actors may attempt to exploit misconfigured AWS Application Load Balancers (ALB) to bypass authentication and authorization controls, gaining unauthorized access to cloud applications and sensitive resources.
- **Investigation Approach:**
    - Monitor ALB traffic patterns for any unusual or unauthorized requests, particularly those that bypass normal authentication flows or originate from unfamiliar IP addresses.
    - Analyze authentication logs and AWS CloudTrail events for indicators of token forgery, focusing on discrepancies in JWT signatures or unexpected alterations in the token issuer field.
    - Cross-reference any application access logs with corresponding ALB configurations to identify whether requests are being improperly accepted from sources other than the expected ALB instance.
    - Set up alerts for any modifications to ALB configurations, especially those involving authentication settings or security group changes, that are not in line with standard operational procedures.

Threat Hunt Hypothesis: Unauthorized Access via Exposed .env Files

- **Hypothesis:** Adversaries may exploit publicly accessible environment variable (.env) files containing sensitive credentials to gain unauthorized access to AWS environments and escalate privileges.
- **Investigation Approach:**
    - Scan AWS environments and connected web applications for any exposed .env files, paying particular attention to files that contain API keys, AWS IAM credentials, or other sensitive information.
    - Review CloudTrail logs for API calls, such as ListUsers, GetCallerIdentity, and ListBuckets, that could indicate reconnaissance activities stemming from compromised credentials.
    - Correlate AWS activity with exposed .env file discovery to detect patterns of unauthorized access or privilege escalation attempts.

RETURN

- Set up alerts for the creation of new IAM roles or the use of sensitive API keys found in .env files, focusing on administrative actions that could compromise security settings.
- **Threat Hunt Hypothesis:** Post-Exploitation Data Exfiltration

- **Hypothesis:** After successfully exploiting misconfigured AWS environments, attackers may attempt to exfiltrate sensitive data from S3 buckets or other storage services.
- **Investigation Approach:**
  - Monitor for unusual spikes in S3 operations, such as GetObject and DeleteObject API calls, particularly those originating from newly created IAM roles or users.
  - Review AWS Cost and Usage Reports for unexpected increases in data transfer volumes that could suggest exfiltration attempts.
  - Analyze object-level logging in S3 buckets to detect unauthorized access or modification, including the placement of ransom notes or deletion of critical data.
  - Set up alerts for the creation of new storage buckets or changes to existing bucket permissions that could facilitate data exfiltration or subsequent attacks.

Sources

- Cyber Security News - AWS .env Extortion Campaign Targeting 110,000 Domains
- Security Week - Thousands of Apps Using AWS ALB Exposed Due to Configuration Issue
- Cyber Security News - Massive AWS Cyber Attack Targeting 230 Million Environments
- The Hacker News - ALBeast Vulnerability Exposes AWS Applications

CONVERGE
TECHNOLOGY SOLUTIONS

Contact the Converge Threat Intel Group at cybersecurity@convergetp.com

convergetp.com/cybersecurity