12
DEC

THREAT INTEL REPORT 2024

CONVERGE
TECHNOLOGY SOLUTIONS

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

Observations for December 2024

Cyber threats continue to evolve, targeting critical industries and exploiting vulnerabilities with alarming precision. This month's intelligence highlights key risks across telecommunications, cloud environments, and supply chains–sectors vital to national security and economic stability. From nation-state espionage campaigns to sophisticated malware adaptations and cascading supply chain disruptions, these incidents underscore the urgent need for proactive defense strategies to safeguard interconnected systems. Below, we explore the most pressing threats and their far-reaching implications.

The telecommunications sector has become a focal point for cyber-espionage, with Salt Typhoon, a Chinese-backed threat actor, breaching major providers like T-Mobile, AT&T, and Verizon. By compromising systems used for law enforcement surveillance, these attacks pose significant risks to both private communications and national security, underscoring the need for stronger defenses across the telecom industry.

Cloud environments face heightened risks as Gafgyt malware shifts its focus to misconfigured Docker Remote API servers. Attackers leverage legitimate Docker images to deploy botnets, enabling Distributed Denial-of-Service (DDoS) attacks and compromising host systems. This adaptation emphasizes the importance of securing cloud configurations and addressing potential misconfigurations to counter evolving threats.

Supply chain disruptions remain a significant concern, with the Blue Yonder ransomware attack and the Finastra breach revealing systemic vulnerabilities. These incidents caused widespread delays across industries, from retail to finance, during the critical holiday season. The cascading effects impacted millions of businesses and customer relationships, highlighting the need for robust cybersecurity measures to mitigate risks and ensure operational continuity in interconnected supply chain networks.

RETURN

Executive Overview

Telecom Under Siege: Rising Threats from State-Sponsored Cyber Attacks

Audience

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

SUMMARY: Recent intelligence indicates an alarming escalation in cyber-espionage campaigns targeting the telecommunications sector. Key incidents include breaches at T-Mobile, AT&T, Verizon, and Lumen Technologies, attributed to Salt Typhoon, a Chinese state-sponsored threat actor. The campaign, which compromised systems used for law enforcement surveillance, demonstrates the critical vulnerability of telecom infrastructure to nation-state attacks. Immediate steps to fortify telecom cybersecurity and ensure operational resilience are imperative.

Tactical guidance >> Telecom Under Siege: Rising Threats from State-Sponsored Cyber Attacks

Container Creeper: Gafgyt's Evolution into Docker Exploits

Audience

- CISO
- Security Managers
- Cybersecurity Professionals
- IT Engineering Teams

SUMMARY: The Gafgyt malware (also known as Bashlite or Lizkebab) has broadened its attack focus to include publicly exposed Docker Remote API servers. Previously targeting IoT devices, this malware demonstrates adaptability by exploiting misconfigured Docker environments to deploy botnet binaries. The attackers use legitimate Docker images, such as the "alpine" image, to create containers that execute the Gafgyt malware. Upon deployment, the malware enables Distributed Denial-of-Service (DDoS) attacks via multiple protocols.

Tactical guidance >> Container Creeper: Gafgyt's Evolution into Docker Exploits

Audience

- CISO
- C-Suite Executives
- Cybersecurity Professionals
- Security Managers

Ripple Effects of Ransomware: Supply Chain Vulnerabilities and Holiday Season Risks

SUMMARY: The ransomware attack on Blue Yonder disrupted operations across various sectors globally, highlighting the interconnected risks of supply chain software reliance. This incident impacted payroll systems, warehouse logistics, and inventory management for high-profile companies in industries ranging from retail to food services. The attack underscores the cascading operational and financial risks posed by third-party breaches, particularly during high-demand periods such as the holiday season.

Tactical guidance >> Ripple Effects of Ransomware: Supply Chain Vulnerabilities and Holiday Season Risks

Tactical Guidance

Telecom Under Siege: Rising Threats from State-Sponsored Cyber Attacks

Salt Typhoon breaches

critical telecom systems, jeopardizing security.

Overview & Impact

The telecommunications sector is under sustained attack by Salt Typhoon, also known as Earth Estries or Ghost Emperor. These breaches targeted systems mandated for law enforcement surveillance, threatening both private communications and national security.

- **National Security Risks:** Compromise of communications involving high-ranking U.S. officials.
- **Critical Infrastructure Vulnerability:** Exploitation of vulnerabilities in telecom systems for intelligence gathering.
- **Industry-Wide Breaches:** Multiple major telecom providers affected, highlighting systemic risks.

Observations

- Salt Typhoon used advanced tactics, including exploiting vulnerabilities in Cisco routers, to access wiretap systems.
- Breaches spanned at least eight months, involving targeted attacks on high-value intelligence and government personnel.
- Despite statements from T-Mobile downplaying impacts, metadata and private communications may have been exfiltrated.
- This is part of a broader campaign impacting at least three major U.S. telecom providers in the past year.

RETURN

Guidance

Strategic Intelligence

- Trend Analysis
  - **Telecom Sector Under Persistent Attack:** The Salt Typhoon campaign reveals a sustained focus on breaching telecommunications networks. This emphasizes the vulnerability of critical infrastructure to nation-state actors and highlights the increasing importance of protecting communications systems.
  - **Nation-State Targeting of Wiretap Systems:** The exploitation of law enforcement surveillance tools for espionage indicates an evolution in attacker priorities, with strategic emphasis on intelligence gathering from sensitive sources.
  - **Systemic Weaknesses Across Telecom Providers:** The wide-reaching impact on multiple providers, including T-Mobile, Verizon, and AT&T, underscores systemic vulnerabilities in the telecom industry's security posture.
- Implications for Security Frameworks
  - **Strengthening Critical Infrastructure Protections:** The campaign illustrates the urgency of adopting robust, multi-layered defenses for critical infrastructure.
  - **Sector Collaboration Imperative:** Telecom providers must coordinate threat intelligence sharing and response efforts to address shared vulnerabilities effectively.
  - **Potential for Long-Term Espionage:** The breaches may serve as a precursor to prolonged intelligence operations, emphasizing the need for continuous monitoring and resilience planning.

Operational Intelligence

- Attack Vectors
  - **Initial Access:** Exploitation of vulnerabilities in Cisco routers and law enforcement wiretap systems to gain entry
  - **Execution:** Deployment of advanced tools to access and exfiltrate call metadata, private communications, and law enforcement data
  - **C2 Channels:** Use of encrypted communications and persistent backdoors to maintain undetected access
- Detection Challenges
  - **Trusted System Exploitation:** Wiretap systems, being integral to telecom infrastructure, operate with high privilege levels, making unauthorized activities harder to detect.
  - **Hardware-Specific Weaknesses:** Focused attacks on network devices like routers demand specialized detection approaches beyond standard endpoint monitoring.
  - **Sophisticated Evasion Techniques:** Threat actors employ encryption and low-profile malware, reducing visibility and complicating identification of their actions.

RETURN

Tactical Intelligence

- Mitigation Strategies
  - **Comprehensive Infrastructure Assessments:** Conduct thorough security reviews of telecom hardware and wiretap systems to identify and address potential vulnerabilities.
  - **Enhanced Monitoring of Key Systems:** Deploy advanced monitoring solutions to detect unauthorized access or configuration changes in wiretap systems and routers.
  - **Network Traffic Inspection:** Set up alerts for suspicious outbound traffic patterns, particularly involving connections to known or suspected C2 servers.
  - **Zero-Trust Architecture:** Implement strict identity and access management controls, including phishing-resistant authentication, to minimize unauthorized access risks.
- Preventive Measures
  - **Securing the Supply Chain:** Ensure vendors of network hardware and software adhere to rigorous security standards to reduce the risk of supply chain attacks.
  - **Employee Training:** Provide ongoing training for telecom personnel to recognize and respond to social engineering attempts and protect critical systems.
  - **Isolating Surveillance Systems:** Apply strict access controls and implement isolation policies for wiretap systems to contain potential breaches.
  - **Preparedness in Incident Response:** Develop and regularly rehearse incident response protocols tailored to telecom infrastructure breaches to mitigate impact.

Sources

- Infosecurity Magazine: T-Mobile Breached by Chinese State-Sponsored Hackers
- Bleeping Computer: T-Mobile Confirms Hack in Recent Telecom Breaches
- Forbes: T-Mobile Hack Linked to Chinese State-Sponsored Hackers
- Reuters: Massive Chinese Breach of Telecom Networks

Container Creeper: Gafgyt's Evolution into Docker Exploits

Overview & Impact

Gafgyt malware, previously focused on IoT devices, has been observed targeting misconfigured Docker Remote API servers. Attackers create Docker containers using legitimate images, such as "alpine," to deploy botnet binaries. These binaries allow attackers to escalate privileges, access host systems, and execute DDoS attacks. Successful exploitation enables attackers to control infected systems through command-and-control servers, compromising the integrity and security of the environment. Systems with exposed and misconfigured Docker Remote APIs are at a high risk of being compromised.

RETURN

Gafgyt exploits misconfigured Docker APIs for DDoS attacks and system access.

Observations

- Attack Process
  - Attackers exploit exposed Docker Remote API servers to deploy Docker containers using legitimate images (e.g., “alpine”).
  - Techniques Involved
    - **Privilege Escalation:** Use of chroot and bind to access host system files.
    - **Malware Deployment:** Download and execution of Gafgyt botnet binaries (e.g., “rbot” and “atlas.i586”).
    - **Fallback Mechanism:** If initial deployment fails, alternative binaries or scripts (e.g., “cve.sh”) are used to deploy architecture-specific botnet binaries.
- Malware Behavior
  - Hardcoded C&C server IP addresses facilitate control over infected systems.
  - Victim systems are used to execute multi-vector DDoS attacks employing protocols such as UDP, TCP, HTTP, ICMP, and SYN.
  - Local IP discovery uses DNS queries to identify network configurations, enabling targeted attack execution.

Guidance

Strategic Intelligence

- Trend Analysis
  - **Expansion of Targets:** Gafgyt malware, historically focused on IoT devices, is now targeting misconfigured Docker Remote API servers, indicating a shift toward exploiting containerized environments.
  - **Evolving Techniques:** Attackers leverage legitimate tools, such as Docker images, combined with privilege escalation tactics (chroot and bind), to compromise host systems and deploy botnet binaries.
- Implications for Security Frameworks
  - **Container Security Challenges:** The use of legitimate container images to deliver malware highlights the need for robust monitoring of container activity and image integrity.
  - **Increased Risk for Cloud-Native Infrastructure:** The targeting of Docker APIs underscores vulnerabilities in cloud-native environments, emphasizing the need for stronger security practices in DevOps pipelines and containerized workloads.

Operational Intelligence

- Attack Vectors
  - **Initial Access:** Attackers exploit exposed and misconfigured Docker Remote API servers to create containers with legitimate images, such as “alpine.”

RETURN

- **Privilege Escalation:** Attackers use commands like chroot and bind to gain access to the host's root directory and escalate privileges.
- **Malware Deployment:** Gafgyt binaries (e.g., "rbot" and "atlas.i586") are downloaded and executed within the containers.
- **Command-and-Control (C2):** Malware communicates with hardcoded C2 servers (e.g., 178.215.238.31) to receive instructions and initiate DDoS attacks.

- Detection Challenges
  - **Legitimate Tool Usage:** The use of legitimate Docker images and standard API commands makes distinguishing malicious activity from normal operations difficult.
  - **Fallback Mechanisms:** Repeated container creation attempts and use of alternative binaries or scripts (e.g., "cve.sh") increase the attack's resilience against detection and mitigation.

Tactical Intelligence

- Mitigation Strategies
  - **Docker API Hardening:** Implement strict authentication and access controls for Docker Remote API servers to prevent unauthorized access.
  - **Privilege Management:** Avoid deploying containers in privileged mode and monitor API requests for commands involving privilege escalation.
  - **Network Monitoring:** Set alerts for traffic to known malicious C2 IPs, such as 178.215.238.24 and 178.215.238.31, and track unusual outbound connections from Docker containers.
  - **File Integrity Checks:** Monitor container activities for unauthorized downloads and execution of binaries, particularly those associated with known IoCs like "rbot" and "atlas.i586."
- Preventive Measures
  - **Training and Awareness:** Educate DevOps teams on container security best practices, including the risks associated with exposed APIs and privilege escalation.
  - **Patch Management:** Regularly update Docker and related software to address vulnerabilities that attackers could exploit.
  - **Container Image Validation:** Use trusted image repositories and scan images for vulnerabilities before deployment.
  - **Incident Response Playbooks:** Develop and test response plans for container-related incidents, ensuring rapid containment and recovery from attacks.

Threat Hunting Hypotheses

Gafgyt Malware Exploitation of Docker Remote API Servers

- **Hypothesis:** Threat actors are exploiting misconfigured Docker Remote API servers to deploy Gafgyt malware, enabling privilege escalation, botnet deployment, and DDoS attacks.

RETURN

- **Investigation Approach:**
  - Monitor Docker logs for unusual container creation requests, especially those using legitimate images like "alpine" combined with privilege escalation options (chroot or binds).
  - Track network connections from containers to known malicious IP addresses, such as 178.215.238.31, indicating command-and-control communication.
  - Analyze file activity within Docker containers for unauthorized downloads or execution of binaries like "rbot" or "atlas.i586."
  - Look for repeated container creation attempts following initial failures, particularly involving alternative binaries or deployment scripts such as "cve.sh."
  - Inspect DNS queries originating from containers to detect patterns of local IP discovery, such as repeated lookups for 8.8.8.8.

Persistence via Privilege Escalation in Docker Containers

- **Hypothesis:** Attackers are establishing persistence by leveraging Docker container capabilities to access and modify host systems.
- **Investigation Approach:**
  - Monitor for Docker API requests that attempt to mount the host root directory (/:) to container directories, indicating attempts to modify host files.
  - Review access logs for unexpected modifications to host system configuration files or the introduction of SSH keys for persistent remote access.
  - Set alerts for containers executing with elevated privileges or non-standard runtime parameters that could allow host compromise.

Fallback Deployment Using Shell Scripts

- **Hypothesis:** Threat actors are deploying fallback mechanisms, such as shell scripts, to install multiple versions of Gafgyt binaries targeting various system architectures.
- **Investigation Approach:**
  - **Identify Docker containers executing scripts like "cve.sh" that download binaries from known malicious URLs (e.g., http://178.215.238.31).**
  - Audit HTTP traffic from containers to detect downloads of binaries for multiple architectures from the same source.
  - Set alerts for unusual container activity involving shell scripts executed shortly after container creation.

Command-and-Control Communication via Hardcoded Servers

- **Hypothesis:** Gafgyt malware relies on hardcoded IP addresses for command-and-control (C2) operations, enabling remote execution of DDoS attacks and other activities.
- **Investigation Approach:**
  - Monitor outbound traffic from Docker containers to IP addresses listed in IoC list for consistent communication patterns.

RETURN

- Analyze network logs for multi-protocol traffic (UDP, TCP, HTTP) originating from containers, indicating DDoS activity controlled by the C2 server.
- Review process activity within containers to detect execution of binaries linked to known C2 IP addresses.

Privilege Escalation Attempts Using Docker Bind Options

- **Hypothesis:** Threat actors are using Docker bind options to access host file systems and escalate privileges.
- **Investigation Approach:**
  - Audit Docker API logs for container creation commands that include Binds:["/:/mnt"] or similar parameters mapping the host root directory.
  - Investigate containers showing unexpected access to host directories, focusing on any writes to critical files or system configurations.
  - Set up alerts for Docker containers that exhibit excessive file system access indicative of privilege escalation attempts.

Sources

- Gafgyt Malware Broadens Its Scope - Gurucul
- Hackers Hijack Docker APIs - CyberPress
- Trend Micro Research - Gafgyt Malware
- Gafgyt Malware Attacks Docker API Servers - Cybersecurity News

The November 2024 Blue Yonder attack

affected 3,000+ clients, causing widespread supply chain delays.

Ripple Effects of Ransomware: Supply Chain Vulnerabilities and Holiday Season Risks

Overview & Impact

The ransomware attack on Blue Yonder, which began on November 21, 2024, severely disrupted operations across multiple industries reliant on its supply chain management software. Targeting the company's private cloud services, the attack impacted over 3,000 global clients, including major retail, food service, and technology companies. This disruption led to delayed payroll systems, inventory shortages, and logistical bottlenecks during the critical holiday season. The Termite ransomware group claimed responsibility for the attack and alleged the theft of 680GB of sensitive data, further amplifying the incident's consequences.

Retail operations were particularly hard hit. UK grocery chains, such as Morrisons and Sainsbury's, experienced significant delays in warehouse logistics, disrupting the distribution of fresh produce and other perishable goods. In the United States, Starbucks faced payroll processing issues at

RETURN

11,000 North American locations, forcing managers to manually calculate wages. Beyond retail, companies in the technology and food service sectors reported interruptions in supply chain visibility, delayed order fulfillment, and shipping delays. Notably, major clients like Microsoft and Lenovo faced coordination challenges, while food service giants Dole Foods and Nestlé Purina encountered shipping setbacks, affecting consumer goods availability.

The broader impact of the attack underscores the interconnected vulnerabilities within supply chain networks. Blue Yonder's downstream dependencies placed over 3.5 million companies at risk of disruption, spanning across Tiers 1, 2, and 3 of its extended supply chain. The geographical reach of affected businesses was extensive, with 70% based in the United States, followed by notable exposures in India, the United Kingdom, and Germany. The cascading effects of the attack strained over 40 million customer relationships, disrupting routine business activities and delaying service delivery across critical sectors.

The Finastra breach, although not a ransomware incident, revealed similar vulnerabilities within supply chain ecosystems. Over 25% of the world's top 100 banks were directly impacted by the breach, causing significant disruptions in financial services such as loan processing and payment systems. Downstream effects extended to over 3.4 million companies, further emphasizing the systemic risks posed by breaches in supply chain software providers.

Compounding the issue, the timing of these incidents during the holiday season amplified their impact. Ransomware attacks have historically spiked during this period, as threat actors exploit increased demand and the time pressures on affected organizations. The financial repercussions are significant, with supply chain disruptions costing enterprises an estimated $100 million annually. These incidents highlight the urgent need for enhanced cybersecurity measures and strategic planning to mitigate the cascading risks posed by supply chain vulnerabilities.

Observations

- **Sectoral Impact of Blue Yonder Attack:**
  - Retail grocery chains and consumer goods providers faced operational delays during peak holiday demand.
  - Technology companies reported interruptions in supply chain coordination and delayed fulfillment of hardware and software orders.
  - Apparel retailers and food service providers experienced delays in stocking and order management systems, affecting customer satisfaction.
- **Widespread Downstream Effects:**
  - Over 3.5 million businesses across Tiers 1, 2, and 3 impacted by supply chain disruptions
  - 40 million customer relationships between buyers and suppliers strained by delayed operations

RETURN

- **Geographical Reach:**
  - 70% of affected companies located in the U.S., followed by significant exposure in India (9%), the UK (8%), and Germany (4%).
- **Ripple Effects on Major Organizations:**
  - **Starbucks:** Shifted to manual payroll processes, increasing administrative burdens and risking pay delays
  - **Morrisons:** Reverted to backup logistics systems, causing bottlenecks in produce distribution
  - **Sainsbury's:** Activated contingency plans to minimize disruptions in fresh food supply
  - **Anheuser-Busch:** Faced shipping delays, impacting beverage distribution networks
  - **Renault and Ford:** Encountered disruptions in automotive supply chain management, risking production delays

Guidance

Strategic Intelligence

- **Trend Analysis:**
  - Ransomware operators target supply chain software providers due to their widespread integration with client operations.
  - Attackers exploit high-demand periods, such as holidays, to maximize disruption and extortion leverage.
- **Implications for Enterprise Security:**
  - **Supply Chain Risk Assessments:** Regularly evaluate third-party vendors for security weaknesses.
  - **Cross-Industry Collaboration:** Share intelligence and response strategies among affected sectors to reduce recovery timelines.
  - **Enhanced Resilience Planning:** Prepare contingency strategies to manage extended disruptions in key service areas.

Operational Intelligence

- **Key Actions for Organizations:**
  - Implement real-time monitoring of supply chain dependencies to identify vulnerabilities quickly.
  - Establish collaborative incident response frameworks with third-party vendors for swift recovery.
  - Develop alternative workflows, such as manual processes, to manage critical operations during outages.
- **Enhanced Incident Communication:**
  - Companies like Blue Yonder benefited from proactive and transparent updates, fostering customer confidence and facilitating collaborative recovery.

Tactical Intelligence

- **Indicators of Compromise (IoCs):**
  - Termite ransomware's modified Babuk code base and associated file hashes
  - Network behaviors indicating unauthorized access to private cloud systems
- **Preventive Measures:**
  - Use AI-powered tools to map and monitor extended supply chains for early detection of anomalies.
  - Regularly update security protocols for third-party integrations and access controls.
  - Conduct tabletop exercises to simulate ransomware scenarios and improve response effectiveness.

Threat Hunting Hypotheses

Supply Chain Ransomware Exploitation via Third-Party SaaS Providers

- **Hypothesis:** Threat actors are exploiting vulnerabilities in third-party SaaS providers, like Blue Yonder, to deploy ransomware, disrupt operations, and exfiltrate sensitive data, leading to widespread supply chain impacts.
- **Investigation Approach:**
  - **Log Analysis:**
    - Review access logs for anomalous activity, such as unauthorized login attempts or changes to managed cloud service configurations.
    - Identify unusual data transfer volumes or spikes in network activity indicative of exfiltration efforts.
  - **Endpoint Monitoring:**
    - Detect unauthorized encryption processes on endpoints within the SaaS environment.
    - Track file modifications, particularly for critical files or databases, suggesting preparation for ransomware deployment.
  - **Network Traffic Analysis:**
    - Monitor outbound connections to known malicious IPs or newly registered domains associated with ransomware command-and-control (C2) operations.
    - Flag encrypted data transmissions to external servers, signaling potential double extortion tactics.
  - **User Behavior Analytics (UBA):**
    - Investigate privileged account activity for abnormal patterns, such as login attempts from unusual locations or devices.
    - Identify excessive privilege escalations or role changes for accounts interacting with SaaS environments.

RETURN

Lateral Movement within SaaS-Integrated Supply Chains

- **Hypothesis:** Threat actors use compromised SaaS platforms to pivot into downstream supply chain networks, targeting client organizations through lateral movement.
- **Investigation Approach:**
  - **Integration Monitoring:**
    - Track API activity between SaaS platforms and downstream clients for anomalous requests or unauthorized data access.
    - Analyze shared resource configurations for misconfigured permissions allowing lateral access.
  - **Inter-Organization Traffic Analysis:**
    - Review communication logs between SaaS and client networks for unusual data transfers or access attempts.
    - Set alerts for cross-organization activity originating from IP addresses linked to known threat actors.
  - **Behavior Analysis:**
    - Monitor automated workflows within SaaS applications for modifications indicating abuse of legitimate processes.
    - Identify unexpected file sharing or collaborative actions involving sensitive customer data.

Exploitation of SaaS Misconfigurations to Deploy Ransomware

- **Hypothesis:** Threat actors are leveraging misconfigured SaaS environments to inject ransomware into critical supply chain operations, enabling privilege escalation and data compromise.
- **Investigation Approach:**
  - **Configuration Audits:**
    - Review SaaS settings for misconfigurations, such as open admin panels or overly permissive access controls.
    - Check for unsecured cloud storage buckets containing sensitive data or ransomware payloads.
  - **Privilege Escalation Detection:**
    - Analyze logs for unauthorized privilege escalations within SaaS management portals.
    - Investigate actions involving admin accounts that introduce new users, change security settings, or disable protective measures.
  - **Payload Detection:**
    - Scan for unusual script execution within SaaS environments, such as PowerShell commands or encoded payloads.
    - Audit uploaded files for known ransomware signatures or anomalous file types.

RETURN

Double Extortion Tactics Targeting Supply Chain SaaS Clients

- **Hypothesis:** Ransomware operators are utilizing double extortion techniques, encrypting data within SaaS systems while threatening to leak stolen information to increase pressure for ransom payments.
- **Investigation Approach:**
  - **Data Access Monitoring:**
    - Identify large-scale data accesses or downloads not aligned with normal user behavior.
    - Check for access to sensitive files or directories by accounts without proper authorization.
  - **Exfiltration Detection:**
    - Analyze outbound traffic for indications of bulk data transfers to external destinations.
    - Flag network communications with destinations on IoC lists related to ransomware campaigns.
  - **Dark Web Surveillance:**
    - Monitor dark web forums and marketplaces for mentions of the affected organization or its data being listed for sale.
    - Correlate leaked data samples with known SaaS storage directories to confirm compromise.

Privilege Escalation via SaaS System Integrations

- **Hypothesis:** Attackers exploit SaaS integrations with on-premise systems to escalate privileges and execute ransomware, targeting both the SaaS environment and connected networks.
- **Investigation Approach:**
  - **Integration Analysis:**
    - Audit integration logs for suspicious requests or unauthorized system calls between SaaS and on-premise environments.
    - Monitor connector scripts or API tokens for modifications indicating compromise.
  - **Privilege Audit:**
    - Track accounts with cross-environment access for signs of privilege escalation or misuse.
    - Review SaaS and on-premise logs for unauthorized changes to admin-level permissions.
  - **Incident Isolation:**
    - Inspect compromised accounts or systems for malware artifacts, such as ransomware executables or C2 communications.
    - Conduct forensic analysis on SaaS environments to detect lingering backdoors or persistence mechanisms.

Sources

- Cybersecurity Dive: Blue Yonder Recovery
- Tech Monitor: Blue Yonder Investigates Ransomware Attack
- SOCRadar: Termite Ransomware Attack on Blue Yonder
- SecurityWeek: Blue Yonder Probing Data Theft Claims
- CyberNews: Blue Yonder Ransomware Impact
- CyberScoop: Blue Yonder Ransomware Attack
- Recorded Future: Retailers Struggle After Ransomware Attack
- Interos.ai: Blue Yonder and Finastra Analysis

RETURN

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

convergetp.com/cybersecurity