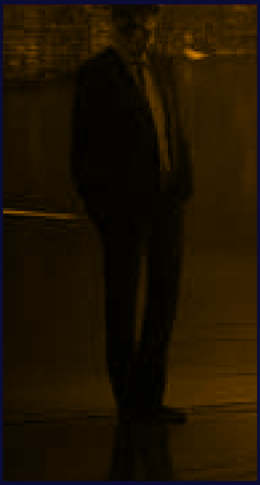
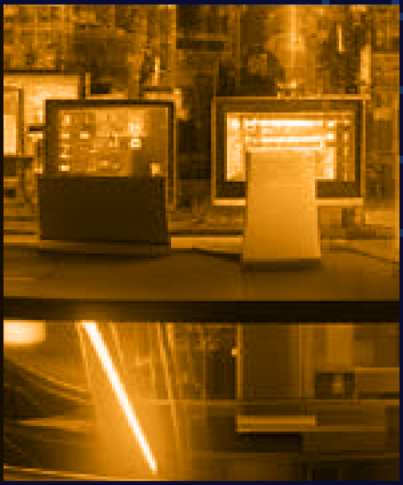
07
JUL

THREAT INTEL REPORT 2024





CONVERGE
TECHNOLOGY SOLUTIONS

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

Observations for July 2024

The most recent report on cyber threats highlights the increasing sophistication and boldness of attacks, targeting critical infrastructure and high-profile organizations. One major incident involved Russian cyberespionage group APT29, also known as Cozy Bear, hacking into TeamViewer's internal corporate IT system on June 26, 2024. The breach did not affect client data or the product environment, but the attackers gained access to and copied employee directory data. This incident, mitigated in collaboration with Microsoft, underscores the need for strong internal security measures and continuous monitoring to prevent such intrusions.

Another concerning event was the ransomware attack on Synnovis, a UK pathology lab services provider, attributed to the Russian cybercriminal group Qilin. This attack, which began on June 3, 2024, severely disrupted London's National Health Service (NHS), causing a significant healthcare crisis. The resulting blood shortages and reliance on limited blood types underscore the vulnerability of healthcare systems to cyber threats, emphasizing the urgent need for enhanced cybersecurity measures to protect critical infrastructure.

In addition to targeted attacks, the V3B phishing-as-a-service (PhaaS) platform poses a growing threat to European banking customers and potentially other industries. This sophisticated phishing kit, which features high-quality templates and mechanisms to intercept one-time passwords (OTPs), has targeted 54 major financial institutions. The increasing popularity of V3B among cybercriminals signals a potential expansion beyond the banking sector, raising concerns for other industries such as healthcare, retail, and government.

The recent wave of cyber threats highlights the need for financial institutions and other sectors to strengthen their security measures to counteract these escalating threats and ensure regulatory compliance to protect client data. Advanced phishing kits like V3B can cause severe operational disruption, enabling attackers to bypass multi-factor authentication (MFA) and intercept OTPs, leading to unauthorized access and significant financial losses. This report is a call to action for organizations globally to enhance their cybersecurity strategies and remain vigilant against evolving threats.

RETURN

Executive Overview

Midnight Intrusion: TeamViewer Thwarted by Russian APT29

Audience

- Cybersecurity Professionals and Analysts
- C-Suite Executives of Affected and Potentially Vulnerable Companies
- Network Administrators
- Organizations using TeamViewer

SUMMARY: TeamViewer has confirmed that the Russian cyberespionage group APT29 is behind a recent cyberattack on its internal corporate IT environment. The breach, detected on June 26, 2024, involved the theft of employee directory data but did not impact the product environment or client data. TeamViewer has taken immediate mitigation steps and is working with Microsoft to enhance security measures.

Tactical guidance >> Midnight Intrusion: TeamViewer Thwarted by Russian APT29

Crippling Effects of Attacks on Critical Infrastructure

Audience

- IT Managers
- CTO
- Cybersecurity Professionals

SUMMARY: A ransomware attack on Synnovis, a major provider of pathology services in the UK, has severely affected London's NHS pathology services. This has led to significant healthcare disruptions and highlighted the serious consequences of attacks on our critical infrastructure. The attack has resulted in the rescheduling of over 800 planned operations and 700 outpatient appointments, including critical cancer treatments and C-sections. Hospitals have been compelled to rely solely on O-negative and O-positive blood types for all transfusions, leading to a severe blood shortage and prompting a public appeal for donations. The situation has put immense pressure on hospital resources, emphasized the vulnerability of healthcare systems to cyber threats, and underscored the urgent need for improved cybersecurity measures.

Tactical guidance >> Crippling Effects of Attacks on Critical Infrastructure

RETURN

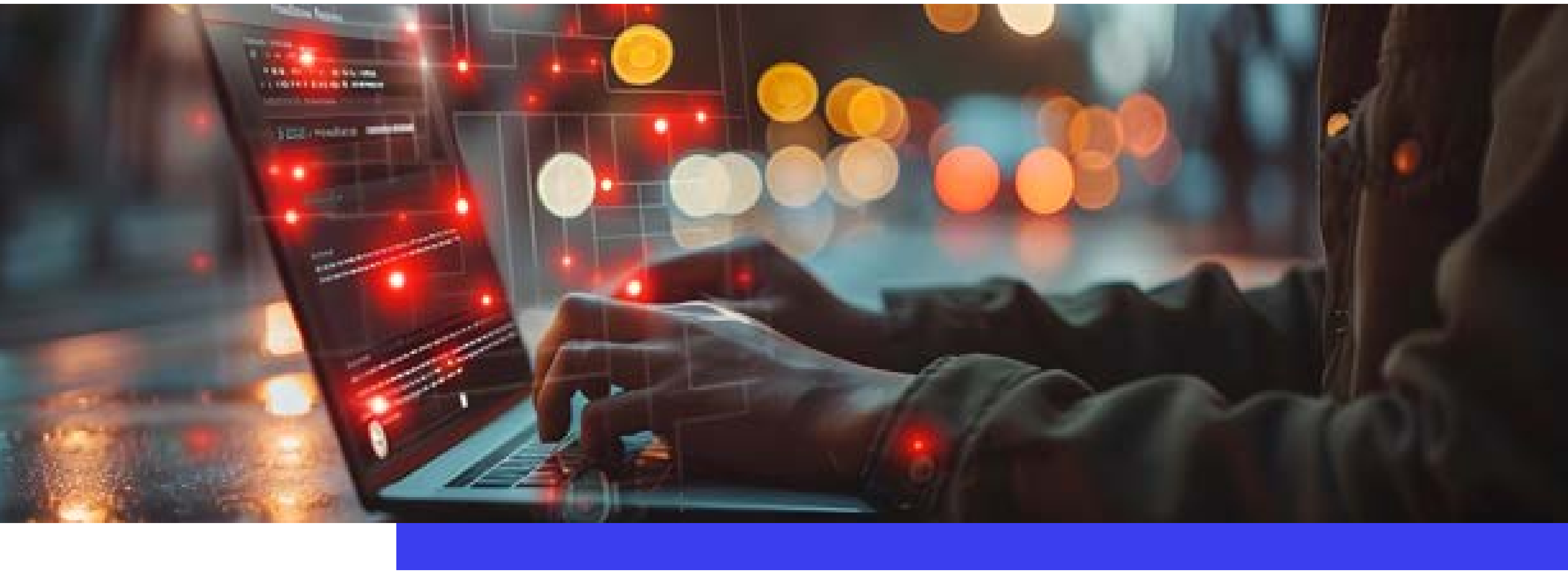
Audience

- Cybersecurity Professionals
- Financial Institutions' IT and Security Teams
- Bank Fraud Prevention Teams
- C-Suite Executives in Financial Services
- Network and IT Administrators
- Security Teams in Other Sectors

V3B Phishing Kit: A Growing Threat to European Banking and Beyond

SUMMARY: The V3B phishing kit, currently targeting banking customers in Europe, poses a significant threat with its advanced features and growing popularity among cybercriminals. While it has primarily affected financial institutions, it is highly likely to spread to other sectors, necessitating vigilance and robust security measures across various industries.

Tactical guidance >> V3B Phishing Kit: A Growing Threat to European Banking and Beyond



RETURN

Tactical Guidance | Emerging Threats

Midnight Intrusion: TeamViewer Thwarted by Russian APT29

TeamViewer hit by APT29 cyberattack, employee data was compromised.

Overview & Impact

On June 26, 2024, TeamViewer discovered an intrusion in its internal corporate IT environment. The breach was traced back to the Russian state-sponsored group APT29, known for targeting high-profile organizations. The attackers were able to obtain credentials for a standard employee account, gaining access to names, corporate contact information, and encrypted employee passwords. Fortunately, due to the separation of systems, the breach did not impact the TeamViewer connectivity platform or customer data. This incident highlights the critical need for strong internal security measures, including robust authentication protocols and continuous monitoring to prevent unauthorized access.

Observations

- **Initial Exploitation:** Attackers obtained credentials for a standard employee account, enabling unauthorized access to TeamViewer's internal corporate IT environment.
- **Service Access Abuse:** The attackers used the compromised credentials to copy employee directory data, including names, corporate contact information, and encrypted employee passwords.
- **Persistence Techniques:** The attackers leveraged existing access to maintain persistence within the compromised environment despite detection.
- **Data Exfiltration:** Employee directory data, including encrypted passwords, was extracted, posing potential risks despite encryption.
- **Security Measures Bypassed:** The exploitation succeeded due to initial reliance on standard employee account credentials, highlighting the need for multi-layered authentication.
- **Expanded Attack Surface:** The attack targeted the internal corporate environment but emphasized the importance of strict segregation to prevent lateral movement to the product environment.

Guidance

Strategic Intelligence

- **Policy Enhancement:** Review and update internal security policies to ensure strong segregation between IT environments.
- **Regulatory Compliance:** Stay updated with industry regulations and implement necessary changes to maintain compliance.

Operational Intelligence

- **Network Segregation:** Ensure strict segregation of internal, production, and connectivity environments to prevent lateral movement of threats.
- **Employee Training:** Conduct regular training sessions on cybersecurity best practices and the importance of strong password management.

Tactical Intelligence

- Configure Azure services to require strong network authentication, mitigating the risk posed by the vulnerability.
- Regularly update and review security tools and processes to identify and patch potential gaps in firewall rules.

Threat Hunting Hypotheses

Compromised Credentials Leading to Unauthorized Access

- **Hypothesis:** Unauthorized access could be gained through compromised employee credentials.
- **Investigation Approach:**
  - Monitor authentication logs for unusual login attempts and access patterns.
  - Conduct endpoint scans to identify signs of malware or unauthorized software.

Lateral Movement Within Segregated Environments

- **Hypothesis:** Attackers may attempt lateral movement within segregated environments to expand their access.
- **Investigation Approach:**
  - Analyze network traffic for unusual patterns indicating attempts to move laterally between segregated environments.
  - Review access logs for attempts to bypass network segmentation controls.

Data Exfiltration via Compromised Accounts

- **Hypothesis:** Extracted data could be exfiltrated through compromised accounts.
- **Investigation Approach:**
  - Implement data loss prevention (DLP) tools to monitor and block unauthorized data transfers.
  - Conduct regular audits of data access and transfer logs to detect any anomalies.

Sources

- ITPro: Everything you need to know about the TeamViewer breach
- BleepingComputer: TeamViewer's corporate network was breached in alleged APT hack
- The Hacker News: TeamViewer detects security breach in internal IT environment
- SecurityWeek: TeamViewer hack officially attributed to Russian cyberspies

RETURN

Crippling Effects of Attacks on Critical Infrastructure

Ransomware attack severely disrupted pathology services.

Overview & Impact

On June 3, 2024, Synnovis experienced a ransomware attack that was attributed to the Russian cybercriminal group Qilin. This attack severely impacted two primary NHS hospital trusts, Guy's and St. Thomas', and King's College, crippling their pathology services. Pathology labs play a crucial role in conducting blood and other bodily fluids tests to support medical diagnoses and treatments. As a result of the attack, the hospitals lost thousands of blood samples, leading to a situation where they had to rely on O-negative and O-positive blood types for all transfusions. This caused a public appeal for blood donations.

The impact of the recent cyber attack on the hospital was significant. More than 800 planned surgeries and 700 outpatient appointments, including critical cancer treatments and C-sections, had to be postponed. Pathology services were only operating at 10 percent capacity, resulting in severe blood shortages, particularly for O-negative and O-positive blood types, which required urgent public donations. The attack caused operational disruptions, financial losses, and strained hospital resources, leading to an urgent call for medical student volunteers to support pathology services. Additionally, there was a backlog of thousands of unprocessed blood samples and the hospitals had to resort to manual recording methods, increasing the risk of errors. It is suspected that the ransomware group Qilin was responsible for the attack, emphasizing the critical need for improved cybersecurity measures across essential infrastructure sectors.

Observations

- **Severe Service Disruption:** The ransomware attack paralyzed Synnovis's IT systems, causing widespread service disruptions across multiple NHS hospital trusts.
- **Postponed Medical Procedures:** Over 800 surgeries and 700 outpatient appointments, including critical cancer treatments and C-sections, were rescheduled due to the attack.
- **Blood Transfusion Impact:** Blood transfusion services were severely impacted, leading to a public appeal for O-negative and O-positive blood donations.
- **Manual Recording Methods:** The NHS employed manual recording methods for pathology services, which increased the risk of errors and reduced efficiency.
- **Backlog of Blood Samples:** Hospitals faced a backlog of thousands of unprocessed blood samples, further straining resources and delaying diagnoses.

- **Suspected Perpetrators:** The ransomware group Qilin is suspected to be behind the attack, highlighting the persistent threat of cybercriminal groups to critical infrastructure.
- **Need for Enhanced Cybersecurity:** The incident highlights the critical need for enhanced cybersecurity measures across essential infrastructure sectors to prevent similar attacks in the future.

Guidance

Strategic Intelligence

- **Cybersecurity Awareness Campaigns:** Launch comprehensive cybersecurity awareness campaigns targeting senior leadership, policymakers, and employees to highlight the risks associated with ransomware and the importance of proactive defense measures.
- **Public Awareness:** Engage in public awareness initiatives to educate the general public about the impacts of ransomware attacks on critical infrastructure and the importance of personal cybersecurity hygiene.
- **Industry Collaboration:** Promote collaboration and information sharing among industry peers and sectors to enhance collective defense against ransomware attacks.
- **Monitor Regulatory Changes:** Continuously monitor changes in data protection and cybersecurity regulations to ensure that organizational policies and practices comply with the latest legal requirements.
- **Implement Best Practices:** Adopt and implement industry best practices for cybersecurity, such as those outlined by the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO).
- **Regular Compliance Audits:** Conduct regular compliance audits to verify adherence to regulatory standards and identify areas for improvement in cybersecurity posture.
- **Data Protection Policies:** Develop and enforce robust data protection policies that align with regulatory requirements to safeguard sensitive information from cyber threats.
- **Regulatory Reporting:** Establish protocols for timely reporting of cybersecurity incidents to relevant regulatory bodies to ensure transparency and compliance with legal obligations.

Operational Intelligence

- **Audit and Review:** Conduct regular audits of IT systems and security protocols to identify and mitigate vulnerabilities.
- **Emergency Preparedness:** Develop and regularly update incident response plans for ransomware attacks.
- **Multi-Factor Authentication (MFA):** Implement MFA across all systems to enhance security.
- **Software Updates:** Regularly update software and systems to ensure all known vulnerabilities are patched.

RETURN

- **Backup Strategies:** Establish strong and robust backup strategies to ensure critical data is regularly backed up and stored securely offline.

Tactical Intelligence

- **Suspicious Activity Alerts:** Set up alerts for unusual login times, locations, and patterns indicating a compromised account.
- **Session Monitoring:** Enforce continuous session monitoring to detect and respond to abnormal user activities in real-time.
- **Privileged Account Management (PAM):** Implement PAM solutions to secure, control, and monitor access to critical systems by privileged accounts.

Threat Hunting Hypotheses

Single-Factor Authentication Exploitation

- **Hypothesis:** Attackers exploited single-factor authentication weaknesses to gain access to Synnovis's systems.
- **Investigation Approach:**
  - Monitor for unusual network activity and data exfiltration attempts.
  - Conduct detailed reviews of authentication and access logs for anomalies.
  - Scan endpoints for indicators of compromise and deploy necessary patches.

Phishing Email Distribution

- **Hypothesis:** Attackers used phishing emails to distribute the ransomware to Synnovis employees.
- **Investigation Approach:**
  - Analyze email logs for patterns of phishing attempts and suspicious email activity.
  - Implement and review email filtering rules to block malicious attachments and links.

Persistence Through Compromised Admin Accounts

- **Hypothesis:** Attackers maintained persistence through compromised admin accounts.
- **Investigation Approach:**
  - Review account activity logs for signs of unauthorized access or unusual behavior.
  - Implement stricter access controls and monitor admin account activities.
  - Enforce regular password changes and enable multi-factor authentication for admin accounts.

Sources

- BleepingComputer: Major London hospitals disrupted by Synnovis ransomware attack
- DarkReading: Blood shortages hit London hospitals after ransomware attack
- Reuters: London hospital cyber attack causing significant impact on services
- AP News: Cyberattack disrupts healthcare services in London hospitals

RETURN

V3B Phishing Kit: A Growing Threat to European Banking and Beyond

V3B phishing targets European banking clients, and a threat beyond the financial sector.

Overview & Impact

The V3B phishing kit has quickly become a favored tool among cybercriminals due to its effectiveness in bypassing security measures and its accessibility through Telegram. Initially identified as a threat to the banking sector, its advanced features and growing user base indicate a potential spread to other industries. This expansion could lead to broader implications for organizations globally, underscoring the need for enhanced cybersecurity measures across sectors.

The V3B can lead to significant operational disruptions by allowing attackers to intercept OTPs and bypass multi-factor authentication (MFA), leading to unauthorized access and substantial financial losses. Attackers can easily manipulate victims, making detecting and preventing fraud more difficult. While the current focus is on banking, its success and ease of use suggest that it could be adapted for attacks in other sectors such as healthcare, retail, and government. This potential spread requires vigilance and robust security measures across various industries.

Financial institutions and other sectors must ensure that their security protocols meet regulatory requirements to protect client data from a regulatory and compliance standpoint. The increasing popularity and effectiveness of the V3B phishing kit presents a growing challenge for cybersecurity professionals, emphasizing the need for ongoing vigilance and comprehensive security strategies.

Observations

- **High-Quality Templates:** Realistic templates closely resembling popular banking websites.
- **Multi-Language Support:** Availability in multiple languages makes targeting clients in different countries easier.
- **OTP Interception:** Capability to intercept OTPs and other authentication codes, bypassing traditional security measures.
- **Real-Time Interaction:** The admin panel allows scammers to interact with victims via chat, increasing the success rate of phishing attacks.
- **Wide Adoption:** Over 1,250 members in the Telegram group indicate a growing user base among cybercriminals.
- **Potential Expansion:** Although currently focused on banking, the success and ease of use of the kit suggest it could be adapted for attacks in other sectors.

Guidance

Strategic Intelligence

- **Awareness Initiatives:**
    - **User Training:** Regular training sessions for employees to recognize phishing attempts and understand the latest phishing tactics. Training should include simulated phishing exercises to test and improve user vigilance.
    - **Email Security Products:** Deploy advanced email security solutions, including spam filtering, malware detection, and phishing prevention features. Products that offer machine learning and AI capabilities can more effectively adapt to new phishing techniques.
    - **Security Awareness Programs:** Develop comprehensive security awareness programs that emphasize the importance of cybersecurity hygiene, including password management, recognizing social engineering tactics, and reporting suspicious activities.
    - **Executive Briefings:** Conduct regular briefings for senior leadership on emerging threats and the strategic importance of robust cybersecurity measures. These briefings should highlight the potential financial and reputation impact of phishing attacks.
- **Regulatory Compliance:**
    - Ensure that security measures meet regulatory requirements and protect against advanced phishing threats. Stay informed about changes in data protection regulations and ensure that the organization’s use of email security and user training aligns with compliance requirements.

Operational Intelligence

- **Enhanced Authentication:** Implement strong authentication methods like hardware tokens or biometric verification and enforce MFA across critical systems and services.

Tactical Intelligence

- **Intelligence Feeds and Ingestion:**
    - **Integration of Threat Intelligence Feeds:** Implement a robust system for integrating threat intelligence feeds from multiple sources into your security operations, including open-source intelligence (OSINT), commercial threat intelligence providers, and industry-specific Information Sharing and Analysis Centers (ISACs).
    - **Automated Ingestion and Correlation:** Utilize Security Information and Event Management (SIEM) systems for automated ingestion and correlation of threat intelligence data, enabling real-time threat detection and response.
    - **Continuous Monitoring and Analysis:** Establish continuous monitoring of threat intelligence feeds to identify indicators of compromise (IOCs) related to the V3B phishing kit and other emerging threats. Regularly update detection rules and signatures based on the latest intelligence.
    - **Collaborative Threat Sharing:** Participate in threat intelligence sharing communities to exchange information on phishing attacks and tactics. This collaborative approach helps enhance overall security posture and facilitates timely responses to new threats.

RETURN

Threat Hunting Hypotheses

Forged Requests Exploiting OTP/TAN Validation Mechanisms

- **Hypothesis:** Threat actors may exploit weaknesses in OTP/TAN validation mechanisms to gain unauthorized access.
- **Investigation Approach:** Monitor network traffic for unusual patterns, analyze HTTP requests for exploitation attempts, and conduct endpoint scans for malware indicators.

Anomaly Detection in Network Traffic

- **Hypothesis:** Abnormal network traffic patterns may be a sign of phishing activity.
- **Investigation Approach:** Implement deep packet inspection to detect suspicious traffic, utilize network flow analysis tools, and cross-reference network traffic logs with access logs.

Unauthorized Access via Custom HTTP Requests

- **Hypothesis:** Custom HTTP requests can be utilized to exploit vulnerabilities and gain access to internal services.
- **Investigation Approach:** Review server logs for unusual HTTP requests, monitor for deviations from typical access patterns, and implement logging and alerting for suspicious requests.

Configuration and Access Control Weaknesses

- **Hypothesis:** Attackers may exploit weak configurations and access controls.
- **Investigation Approach:** Audit service configurations, verify robust authentication mechanisms and assess network rules for permissiveness.

Potential for Cross-Sector Attacks

- **Hypothesis:** The V3B phishing kit could be modified to target industries other than banking.
- **Investigation Approach:** Monitor for phishing campaigns targeting other sectors, share intelligence across industries, and prepare cross-sector response strategies.

Sources

- BleepingComputer: New V3B Phishing Kit Targets Customers of 54 European Banks
- Resecurity: Cybercriminals Attack Banking Customers in EU with V3B Phishing Kit
- TechRadar: This Dangerous New Phishing Kit is Hitting Victims Across Europe
- SC Magazine: Attacks with V3B Phishing Kit Set Sights on EU Banking Customers
- CyberFraud Centre: V3B Phishing Kit - A New Threat Targeting European Banking Customers

CONVERGE
TECHNOLOGY SOLUTIONS

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

convergetp.com/cybersecurity