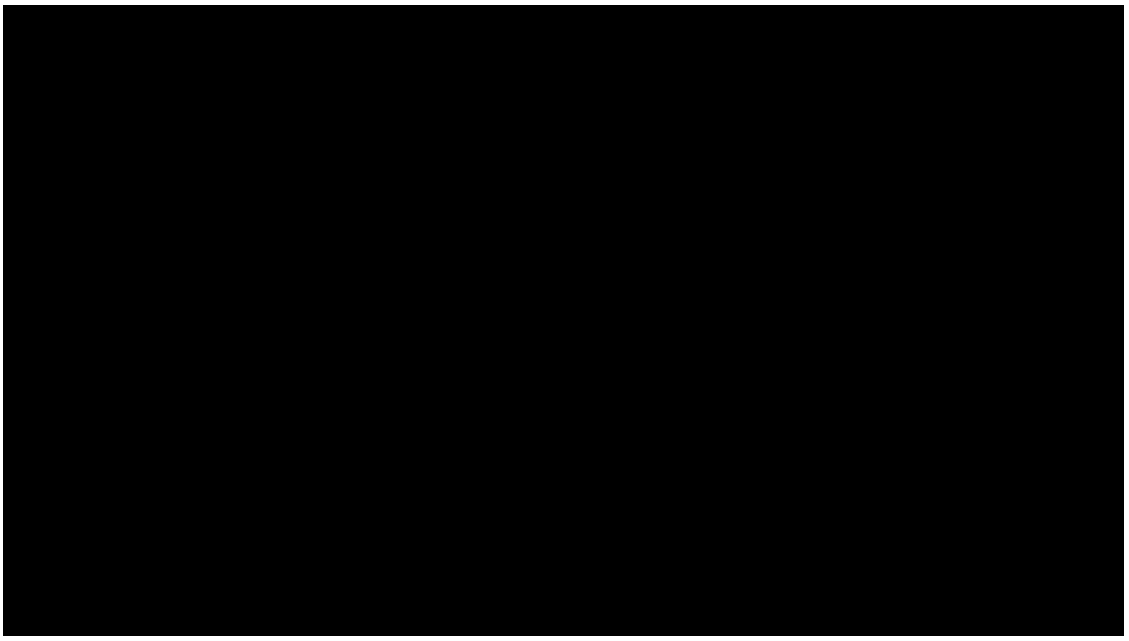
Cyber Intel Brief: NightEagle APT, AI deepfakes, SPNEGO flaw

Archived: 2026-04-02 10:41:31 UTC

Stay up to date the most pressing cyber threats, emerging trends and what they mean for enterprise security, critical infrastructure and global risk.

TLP: CLEAR



Executive Summary

The July 4-11 intelligence collection period revealed critical vulnerabilities requiring immediate attention and sophisticated campaigns targeting democratic institutions and critical infrastructure. Microsoft's July Patch Tuesday addressed 137 vulnerabilities including a critical wormable Windows SPNEGO flaw (CVE-2025-47981) with self-propagating potential similar to WannaCry, while CISA added six known exploited vulnerabilities to the KEV catalog with federal compliance deadlines of July 28-31, 2025.

Most significant this week was the emergence of NightEagle APT—representing a rare suspected North American state-sponsored operation targeting Chinese strategic technology sectors—alongside unprecedented AI-powered impersonation campaigns against U.S. Secretary of State Marco Rubio. These developments signal a concerning escalation in both offensive cyber capabilities and the weaponization of artificial intelligence against democratic institutions, requiring enhanced defensive measures across government and critical infrastructure sectors.

Critical Incidents

1. Wormable Windows SPNEGO Vulnerability Poses Enterprise Propagation Risk

Microsoft's July Patch Tuesday included CVE-2025-47981, a critical Windows SPNEGO Extended Negotiation vulnerability (CVSS 9.8) enabling unauthenticated remote code execution with wormable characteristics. The flaw affects Windows 10 version 1607 and above, allowing network-based exploitation through SMB, RDP, and IIS protocols without user interaction. Security experts are drawing parallels to WannaCry due to its self

propagating potential, with Microsoft addressing 137 total vulnerabilities including 14 critical flaws. Additionally, CVE-2025-49719 represents a publicly disclosed SQL Server information disclosure vulnerability with proof-of-concept code available.1

Analyst Comment: The combination of pre-authentication remote exploitation and wormable characteristics demands immediate patching prioritization across all Windows environments, particularly in enterprise networks with extensive lateral movement potential.

2. CISA KEV Catalog Additions Signal Active Federal Compliance Deadlines

CISA added six vulnerabilities to the Known Exploited Vulnerabilities catalog during the collection period, requiring federal agency remediation by July 28-31, 2025. Critical additions include CVE-2025-5777 (Citrix NetScaler, CVSS 9.3) dubbed "CitrixBleed 2," CVE-2014-3931 (Multi-Router Looking Glass, CVSS 9.8), CVE 2016-10033 (PHPMailer, CVSS 9.8), and CVE-2019-9621 (Zimbra Collaboration Suite, CVSS 7.5) previously exploited by Earth Lusca APT. All vulnerabilities show confirmed evidence of active exploitation in the wild, demonstrating continued targeting of federal infrastructure.2,3

3. Nippon Steel Solutions Zero-Day Breach Exposes Critical Infrastructure Vulnerabilities

Nippon Steel Solutions confirmed a sophisticated data breach following zero-day exploitation of network equipment on March 7, 2025, with disclosure delayed until July 9. The attack compromised customer, partner, and employee personal information, representing advanced adversary capabilities against critical infrastructure subsidiaries. The incident demonstrates ongoing targeting of strategic technology sectors, with the company implementing device isolation and reconstruction protocols while confirming no cloud service impact or dark web data exposure.4

Analyst Comment: The four-month disclosure delay highlights the critical need for enhanced zero-day detection capabilities across critical infrastructure networks, particularly for network equipment that forms the backbone of organizational security.

4. Qantas Airways Data Breach Exposes 5.7 Million Customer Records

Qantas Airways confirmed a cyber incident affecting 5.7 million unique customer records through a compromised third-party call center system, disclosed July 9, 2025. The breach exposed varying levels of personal information including four million records limited to name, email, and frequent flyer details, while 1.7 million records contained additional data including addresses (1.3M), dates of birth (1.1M), and phone numbers (900K). The airline confirmed no credit card details, financial information, passport data, or frequent flyer account credentials were compromised, with no evidence of stolen data being released publicly. The incident represents one of the largest transportation sector breaches of 2025, affecting Australia's flag carrier and prompting enhanced cybersecurity measures across the organization.5

Analyst Comment: The targeting of third-party call center infrastructure demonstrates sophisticated threat actors' focus on supply chain vulnerabilities as attack vectors into major transportation providers, requiring enhanced vendor security assessments.

Active Threat Actors

NightEagle APT (APT-Q-95)

QiAnXin researchers identified a sophisticated threat actor representing a rare suspected North American state-sponsored operation targeting Chinese strategic sectors. NightEagle exploits unknown Microsoft Exchange zero-day vulnerability chains to steal machineKey credentials, focusing on quantum technology, semiconductors, AI research, and military industrial targets. Operations occur exclusively between 9pm-6am Beijing time, suggesting North American time zone operators with substantial infrastructure investment indicating state-level funding. The group employs custom malware for each target, demonstrating advanced operational security and significant resource allocation against Chinese strategic technology development.6

Famous Chollima (North Korean APT)

The DPRK-linked threat actor deployed PylangGhost RAT, a Python-based variant of GolangGhost, targeting cryptocurrency and blockchain professionals in India since May 2025. The campaign uses fake job interview and skill-testing sites as initial infection vectors, demonstrating continued evolution in North Korean cryptocurrency-focused operations. The malware mirrors its Golang predecessor's capabilities while expanding targeting to Windows systems, representing ongoing North Korean efforts to compromise financial technology sectors through sophisticated social engineering campaigns.7

Pay2Key Ransomware-as-a-Service

Iranian-backed cybercriminals resurged the Pay2Key ransomware operation with 80% profit sharing for Iran supporters, hosted on the Invisible Internet Project (I2P) for enhanced anonymity. The group claims over 51 successful ransom payouts generating $4+ million in four months, primarily targeting Israeli and U.S. organizations for ideological reasons. The operation added Linux targeting capabilities as of June 2025 and represents the first known RaaS platform hosted entirely on I2P, demonstrating Iranian state-sponsored actors' adaptation to evade traditional detection methods.8

Trends

AI Weaponization Against Democratic Institutions Escalates

Unknown threat actors successfully impersonated U.S. Secretary of State Marco Rubio using artificial intelligence voice and text generation, contacting three foreign ministers, one U.S. Governor, and one member of Congress through Signal messaging. The campaign used sophisticated voice cloning and writing style mimicry with fake "**marco.rubio@state.gov**" display names, prompting State Department global diplomatic warnings on July 3.9 This represents part of a broader campaign targeting senior U.S. officials including previous impersonation of

Chief of Staff Susie Wiles, demonstrating the urgent need for voice authentication protocols and enhanced verification procedures across government communications.

Analyst Comment: The sophisticated AI capabilities demonstrated against high-level government officials signal a critical escalation requiring immediate implementation of voice authentication protocols across all government communications.

Financial Fraud Schemes Target U.S. Investors Through Social Engineering

FBI reported a 300% increase in "ramp-and-dump" stock manipulation schemes targeting U.S. investors through social media platforms.10 Criminals target investors through social media "investment clubs" using secure messaging apps and potentially employing bots or fake accounts to impersonate legitimate brokerage firms and stock analysts. The schemes involve coordinated efforts to artificially inflate low-priced stock prices before dumping shares, representing a significant evolution in financially motivated social engineering campaigns against retail investors.

Analyst Comment: The dramatic increase in coordinated financial manipulation through social media platforms demonstrates sophisticated threat actors' adaptation to exploit retail investor behavior and platform vulnerabilities.

Critical Infrastructure Zero-Day Exploitation Accelerates Across Technology Sectors

Analysis of the collection period reveals sophisticated threat actors increasingly targeting network equipment and communication platforms with zero-day vulnerabilities. Wing FTP Server (CVE-2025-47812, CVSS 10.0) experienced active exploitation starting July 1 with 8,103 publicly accessible instances globally,11 while TeleMessage SGNL platforms (CVE-2025-48927, CVE-2025-48928) were added to CISA KEV due to insecure defaults and core dump exposure.12 This pattern demonstrates systematic targeting of file transfer and communication infrastructure across critical sectors.

Analyst Comment: The focus on communication and file transfer platforms suggests coordinated campaigns to establish persistent access points into organizational networks through commonly overlooked infrastructure components.

Ransomware Group Ecosystem Evolution Shows 67% Victim Overlap Rates

Major ransomware operations experienced significant disruption with Hunters International shutting down July 3 while offering free decryption keys, and SatanLock ceasing operations July 7 while threatening to leak all stolen data. SatanLock claimed 67 victims since April 2025, with 65% previously compromised by other groups, indicating systematic targeting of already-vulnerable organizations. Both shutdowns follow increased law enforcement pressure and declining profitability, with groups pivoting to data theft-only models under new branding such as "World Leaks."13

Analyst Comment: The high victim overlap rate demonstrates that organizations successfully breached once face significantly elevated risk of repeated targeting, requiring enhanced monitoring and incident response capabilities beyond initial remediation.

Vulnerabilities

Critical Patches Required This Week

CVE	Vendor	Product	CVSS	Status	Federal Deadline
CVE-2025-47981	Microsoft	Windows SPNEGO	9.8	Patched July 8	N/A
CVE-2025-49719	Microsoft	SQL Server	7.5	Patched July 8	N/A
CVE-2025-6554	Google	Chrome V8 Engine	High	Patched July 1	N/A
CVE-2025-47812	Wing FTP	FTP Server	10.0	Patch Available	N/A

Continuing Active Exploitation

CVE	Vendor	Product	CVSS	Weeks Covered	Current Status
CVE-2025-5777	Citrix	NetScaler ADC/Gateway	9.3	2	KEV Added July 10
CVE-2014-3931	MRLG	Multi-Router Looking Glass	9.8	Multiple	KEV Added July 7
CVE-2016-10033	PHPMailer	Email Library	9.8	Multiple	KEV Added July 7
CVE-2019-9621	Zimbra	Collaboration Suite	7.5	Multiple	KEV Added July 7
CVE-2025-48927	TeleMessage	TM SGNL	TBD	2	KEV Added July 1
CVE-2025-48928	TeleMessage	TM SGNL	TBD	2	KEV Added July 1

Recommendations

Immediate Actions (0-24 Hours)

• Deploy Microsoft July 2025 patches immediately, prioritizing CVE-2025-47981 and CVE-2025-49719 across all Windows environments

• Update Wing FTP Server to version 7.4.4+ and audit for unauthorized Lua files or ScreenConnect installations

• Validate all six CISA KEV catalog vulnerabilities are remediated by federal compliance deadlines (July 28-31, 2025)

• Implement enhanced voice authentication protocols for sensitive government and executive communications

• Scan for and remediate PHPMailer, MRLG, and Zimbra vulnerabilities across all federal systems

1. Bleeping Computer. (2025, July 8). Microsoft July 2025 Patch Tuesday fixes one zero-day, 137 flaws. **https://www.bleepingcomputer.com/news/microsoft/microsoft-july-2025-patch-tuesday-fixes-one-zero-day-137-flaws/**
2. Cybersecurity and Infrastructure Security Agency. (2025, July 10). CISA adds one known exploited vulnerability to catalog. **https://www.cisa.gov/news-events/alerts/2025/07/10/cisa-adds-one-known-exploited-vulnerability-catalog**
3. Cybersecurity and Infrastructure Security Agency. (2025, July 7). CISA adds four known exploited vulnerabilities to catalog. **https://www.cisa.gov/news-events/alerts/2025/07/07/cisa-adds-four-known-exploited-vulnerabilities-catalog**
4. Security Affairs. (2025, July 9). Nippon Steel Solutions suffered a data breach following a zero-day attack. **https://securityaffairs.com/179766/data-breach/nippon-steel-solutions-data-breach.html**
5. Qantas Airways. (2025, July 9). Update on Qantas cyber incident: Wednesday 9 July 2025. Qantas Newsroom. **https://www.qantasnewsroom.com.au/media-releases/update-on-qantas-cyber-incident-wednesday-9-july-2025/**
6. The Hacker News. (2025, July 5). NightEagle APT Exploits Microsoft Exchange Flaw to Target China's Military and Tech Sectors. **https://thehackernews.com/2025/07/nighteagle-apt-exploits-microsoft.html**
7. Check Point Research. (2025, July 6). 6th July -- Threat intelligence report. https://research.checkpoint.com/2025/6th-july-threat-intelligence-report/
8. The Hacker News. (2025, July 3). Iranian-Backed Pay2Key Ransomware Resurfaces with 80% Profit Share for Cybercriminals. **https://thehackernews.com/2025/07/iranian-backed-pay2key-ransomware.html**
9. The Washington Post. (2025, July 8). A Marco Rubio impostor is using AI voice to call high-level officials. **https://www.washingtonpost.com/national-security/2025/07/08/marco-rubio-ai-imposter-signal/**
10. Federal Bureau of Investigation Internet Crime Complaint Center. (2025, July 3). Fraudsters target US stock investors through investment clubs accessed on social media and messaging applications [Alert I-070325-PSA]. **https://www.ic3.gov/PSA/2025/PSA250703**
11. The Hacker News. (2025, July 2). Critical Wing FTP Server Vulnerability (CVE-2025-47812) Actively Being Exploited in the Wild. **https://thehackernews.com/2025/07/critical-wing-ftp-server-vulnerability.html**
12. Cybersecurity and Infrastructure Security Agency. (2025, July 7). CISA adds four known exploited vulnerabilities to catalog. **https://www.cisa.gov/news-events/alerts/2025/07/07/cisa-adds-four-known-exploited-vulnerabilities-catalog**
13. Check Point Research. (2025, July 6). 6th July -- Threat intelligence report. https://research.checkpoint.com/2025/6th-july-threat-intelligence-report/

Tags

Threat intelligence
