Daily Intelligence Update | 15 September 2025

US authorities have attributed a recent wave of complex spear-phishing attacks to the Chinese state-sponsored group APT41, which allegedly impersonated Congressman John Moolenaar to gain access to sensitive targets during ongoing U.S.–China trade negotiations. The attackers reportedly used spoofed emails and abused developer tools and cloud infrastructure to create covert exfiltration channels. APT41—also tracked as Double Dragon, Winnti, and Wicked Panda—has a long history of espionage and financially motivated activity, including supply chain compromises, bootkits, and abuse of stolen digital certificates. Officials emphasized that the campaign demonstrates the group's strategy of infiltrating trusted communication channels to influence foreign policy. Defenders are urged to deploy phishing-resistant MFA, harden email and endpoint defenses, and increase user awareness training. Researchers have also reported that a rapidly growing malware delivery technique called ClickFix has become the dominant method in web-based attack campaigns. Replacing older fake browser update lures, ClickFix abuses deceptive CAPTCHA verification pages that trick victims into clicking "verify" buttons. The interaction covertly copies obfuscated PowerShell or shell commands to the clipboard, which when executed, install data-stealing malware. Initially developed as a red-team tool, the technique is now widely used by threat actors who distribute it via compromised sites, social media, GitHub repositories, and SEO-poisoned pages. By mid-2025, ClickFix had largely displaced malvertising campaigns such as ClearFake. Researchers note the campaigns leverage advanced evasion tactics including dynamic scripting, Google service abuse, and cross-platform payloads targeting Windows, macOS, and Linux. Infrastructure analysis of thousands of payloads revealed distinct attacker toolkits and shared hosting infrastructure.

In parallel, analysts identified a targeted phishing campaign against Web3 developers operated by a group tracked as LARVA-208. The attackers impersonated a fake AI platform called Norlax AI to lure victims through fraudulent job offers and interview invitations on platforms like Remote3. Victims were prompted to download a fake Realtek driver, which ran hidden PowerShell commands installing the Fickle malware. The malware exfiltrated credentials, system details, geolocation data, and development environment artifacts. The campaign was linked to infrastructure hosted by bulletproof provider FFv2, with overlaps to the APT group Luminous Mantis. Analysts highlighted that LARVA-208, which previously relied on malicious LNK files, has now evolved toward fake meeting platforms, social engineering, and file-sharing services like Filebin. Meanwhile, the FBI has released a FLASH alert with IOCs tied to UNC6040 and UNC6395, two groups actively targeting Salesforce environments. UNC6040 has been using vishing campaigns to impersonate IT staff, tricking employees into approving malicious OAuth apps, which grants bulk data exfiltration capabilities. Some victims received extortion demands shortly after data theft. Separately, UNC6395 exploited stolen OAuth tokens from the Salesloft Drift integration, prompting Salesforce and Google to disable the integration and revoke tokens on August 20, 2025. The FBI recommends enabling phishing-resistant MFA, tightening controls on third-party integrations, and training staff against social engineering.

Hacktivist groups including Keymous+, Team Fearless, and We Are Root Sec have launched DDoS attacks in connection with the ongoing #BloquonsTout protests in France. Claiming solidarity with protestors, the groups targeted municipal portals in multiple cities including Béziers, Pau, Quimper, Chambéry, Annecy, Chartres, Colmar, Valenciennes, Tarbes, and Montauban as well as national services such as Atout France and regional open-data platforms. Statements framed the campaign as

“hacktivism for democracy,” though the actual impact appears limited and disruptions remain unverified. Separately, Nullsec Philippines declared a new hacktivist campaign against China, branded PROJECT FUCKCHINA. The group claimed responsibility for DDoS attacks on Chinese military infrastructure and vowed further retaliation. Researchers note this aligns with an emerging trend of Southeast Asian hacktivist groups adopting nationalist rhetoric to justify offensive cyber operations.

Finally, researchers confirmed that a critical flaw in SAP S/4HANA systems (CVE-2025-42957) is being actively exploited. The vulnerability affects S4CORE versions 102–108 in both Private Cloud and On-Premise setups, allowing attackers with low-privileged accounts to bypass security checks, inject malicious code, and escalate to full administrative takeover. The Dutch NCSC issued warnings citing risks of ransomware deployment, data theft, and operational disruption. SAP released fixes on August 12, and experts stress immediate patching, disabling unsafe dynamic code execution, and monitoring for compromise indicators.
