INTEL471

INTELLIGENCE & RESEARCH

CYBER THREAT UPDATES

July 2025

THREAT SUMMARY

In this month's Threat Hunt Intel Update, Intel 471's Intelligence & Research Team is reviewing six cyber threats that include the newly discovered and new campaigns and activity from infamous threat actors.

In June of 2025, several advanced persistent threat (APT) groups were reported to have launched cyber campaigns targeting geopolitical and economic sectors across the globe. The Silver Fox APT focused on Taiwan, employing spear-phishing and leveraging RATs like Gh0stCringe and HoldingHands to infiltrate government and tech networks, aiming to steal intellectual property. Concurrently, remnants of the dismantled Black Basta group resurfaced under affiliations like CACTUS and BlackSuit, targeting finance and construction sectors using Teams phishing, email bombing, and stealthy multi-stage tools like Rust-based loaders and QDoor. Meanwhile, APT28 (Fancy Bear) employed Signal messaging to compromise Ukrainian entities, deploying malware such as SlimAgent to exfiltrate sensitive data.

Other campaigns underscored a global increase in disruptive and destructive cyberattacks. Fog ransomware targeted an Asian financial organization with stealthy dwell times and novel persistence methods, even incentivizing victims to propagate the ransomware. Ukraine also faced attacks from PathWiper, a destructive malware designed to erase critical infrastructure data via timed triggers and anti-recovery techniques. Iranian APTs (APT33, APT34, APT39) executed widespread attacks across North America, Europe, and the Middle East, using advanced tactics like registry tampering, credential reuse, and encrypted data exfiltration to disrupt vital sectors and harvest sensitive information.

TRENDING THREATS

Silver Fox APT Targets Taiwan

Summary

The Hacker News highlights a campaign by the Silver Fox APT group in June 2025, focusing on targeting Taiwanese government and technology sectors. The group utilizes targeted spear-phishing emails containing malicious document attachments designed to exploit known vulnerabilities in Microsoft Office for initial access. Variants of the remote access trojan Gh0st RAT have been observed to be used by Chinese hacking groups and in this case, the article mentions HoldingHands RAT and Gh0stCringe as examples. Post-compromise, Silver Fox abuses custom backdoors and conducts remote command execution, file exfiltration, and lateral movement within the victim's environment. Activity indicates an intent to steal intellectual property and sensitive documents from Taiwan's public and private sector.[1]

New Group Emerges Post-Black Basta

Summary

Earlier this year, the Black Basta threat group was essentially dismantled after the very public leak that uncovered the inner workings of their operation. Then in June of 2025, The Hacker News reported that former Black Basta members have resurfaced. These members have been observed to be affiliated with CACTUS or BlackSuit, and leveraging Microsoft Teams phishing, email bombing, and vishing to gain entry into finance, insurance, and construction networks. They also were seen to use backdoor tunneling (e.g. QDoor) and Rust-based loaders for SSH utilities, signaling an evolution in tooling. These techniques demonstrate a clear pivot toward multi-stage, stealthy campaigns and underscore the need for analytics focused on Teams-based phishing, remote tool abuse, and script-based payload delivery.[2]

APT28: Signal-Based Malware Attacks

Summary

BleepingComputer documented a campaign conducted by APT28 (also known as Fancy Bear) in June of 2025 targeting Ukrainian entities through the abuse of Signal messaging chat. First discovered by Ukraine's Computer and Emergency Response (CERT-UA) in March, attackers were observed sending malicious links in Signal group chats and leading to the deployment of custom Windows malware focused on data theft and remote access (such as SlimAgent). The campaign demonstrates a novel social engineering approach for initial compromise, with subsequent malware enabling persistence, file collection, and C2 communications. The attacks are attributed to the Russian state-linked group, continuing their operations against Ukrainian political, government, and military targets. [3]

Fog Ransomware’s Disruptive Attacks

Summary

Researchers at Symantec released intel on a string of disruptive attacks involving Fog ransomware that occurred in May of 2025 that targeted an Asian financial entity. The group deployed Syteca monitoring software, GC2, Adaptix, and Stowaway proxies to facilitate stealthy reconnaissance and persistence over a two-week dwell time before encryption. It's notable that the campaign also utilized several tactics not commonly seen in other ransomware incidents, including the use of dual-use and open-source penetration testing tools not previously observed in such attacks, the creation of a persistence-establishing service days after the ransomware was deployed, and ransom notes that uniquely offered a "decrypt for free" option if victims chose to spread the ransomware to another system. [4]

PathWiper Hits Ukrainian Infrastructure

Summary

Talos Intelligence has uncovered PathWiper, a wiper malware variant observed in attacks against Ukrainian government and critical infrastructure through June 2025. Delivered primarily via spear-phishing emails and malicious document attachments, PathWiper is engineered to erase data, hinder recovery, and disrupt operations. The malware features time-based triggers, anti-recovery routines, and C2 enabled status reporting, signaling intent to cause destructive impact rather than financial gain." [5]

Iranian State Cyberattacks 2025

Summary

Unit 42 provided a thorough review of Iranian state-sponsored cyber activity throughout 2025, covering campaigns targeting government agencies, energy providers, telecommunications, and critical infrastructure across North America, Europe, and the Middle East. With recent global events, it is important that we stay in tune with related cyber activity. The threat actors, associated with Iranian APT groups such as APT33 (Elfin), APT34 (OilRig), and APT39 (Remix Kitten), deployed spear-phishing, credential harvesting, ransomware, and destructive wiper malware to gain initial access and cause operational disruptions. These campaigns demonstrated advanced techniques including multi-stage delivery, custom malware, credential reuse, lateral movement using living-off-the-land binaries, registry manipulation for persistence, and automated data exfiltration over encrypted channels. The report highlights a particular focus on exfiltrating intellectual property, sensitive communications, and industrial control system data during early to mid-2025. Additionally, in response to ongoing regional developments, Intel471 released Threat Hunt Coverage Analysis of Iranian Threat Actors documenting refinements to existing Hunt Packages and the development of new hypotheses to address related cyber activity. [6]

RELATED HUNT PACKAGES

Blacksuit Ransomware Collection

Gh0stcringe Malware Profile

Cactus Ransomware Collection

Threat Actor APT28 Related Hunt Packages

Fog Ransomware Collection

PathWiper Malware Profile

HUNTER — Iranian Threat Actor Coverage

REFERENCES

1. Fortinet. (2025, June). Threat group targets companies in Taiwan. Fortinet Blog. https://www.fortinet.com/blog/threat-research/threat-group-targets-companies-in-taiwan

2. The Hacker News. (2025, June). Former Black Basta members use Microsoft Teams phishing and vishing attacks. https://thehackernews.com/2025/06/former-black-basta-members-use.html

3. Cimpanu, C. (2025, June). APT28 hackers use Signal chats to launch new malware attacks on Ukraine. BleepingComputer. https://www.bleepingcomputer.com/news/security/apt28-hackers-use-signal-chats-to-launch-new-malware-attacks-on-ukraine/

4. Security.com. (2025, May). Fog ransomware attack leverages new techniques for persistence and disruption. https://www.security.com/threat-intelligence/fog-ransomware-attack

5. Talos Intelligence. (2025, June). PathWiper targets Ukrainian government and infrastructure. https://blog.talosintelligence.com/pathwiper-targets-ukraine/

6. Unit 42. (2025). Iranian cyberattacks 2025: State-sponsored threats evolve with global conflict. Palo Alto Networks. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2025/