What to Share with the FBI: High-Value Cyber Threat Information

FBI CYBER

FBI Cyber Division highly values information voluntarily provided by our industry partners to assist in combating malicious cyber activity. In particular, information related to the following topics are critical to our ability to identify and counter nation state and criminal cyber activity:

- **The targeting of operational technology (OT) networks** to include access attempts and maintenance; network escalation tactics; the targeting of safety systems, programmable logic controllers (PLCs), and human machine interfaces (HMIs); targeting directed at or against critical infrastructure to include senstive data exfiltration or manipulation of IT systems supporting critical functions; evidence of IT-to-OT pivoting; remote access paths into OT environments; and OT vendor/software versions.
- **The targeting of the communications sector** (including public sector and closed government network providers) directed against US government entities and employees, US persons and organizations, as well as supply chain and third-party compromises; suspicious vendor updates; and poisoned dependencies.
- **Signatures and infrastructure used by malicious cyber actors**, including indicators of compromise (IOCs), IPs, domains, URLs; malware samples, hashes, and command lines; legitimate tools abused (i.e. file transfer, cloud admin tools); initial access vectors (exploited edge devices [Virtual Private Networks (VPNs), gateways, firewalls]; exposed remote OT access; spoofed or weak authenticators); and targeting patterns used in confirmed intrusions or reconnaissance campaigns, or associated with known threat actors.
- **Threat actor plans for obfuscation, cyber intrusions, or cyber attacks** including malware attack activity (e.g. ransomware); variants; use cases; Advanced Persistent Threat (APT) group affiliation; theft of US data; and analysis on exfiltration trends among and within threat actors.
- **Companies or third-party providers** based in the US or abroad **that provide support to illegal cyber activities.**
- **Victimology and targeting**: sector/subsector; geography; role-based targeting (IT admins, finance office, OT engineers); business relationships. (The FBI can support anonymized reports; however, victim identification for attribution purposes is preferred.)
- **Evidence of monetary motivation**: ransom notes and their content; negotiation chats; payment instructions; wallet addresses; SMS messages; evidence of spoofing.

Please contact your local FBI Field Office if you see any of the above information on your networks. Your partnership is essential in the fight to keep America safe.