**Indicators of Compromise**

|  |  |  |
| --- | --- | --- |
| **INDICATOR** | **TYPE** | **DESCRIPTION** |
| 1d970f2e7af9962ae6786c35fcd6bc48bb860e2c8ca74d3b81899c0d3a978b2b | SHA256 | Loader DLL |
| 3a47e59c37dce42304b345a16ba6a3d78fc44b21c4d0e3a0332eee21f1d13845 | SHA256 | Loader DLL |
| 3aa746bb94acee94c86a34cb0b355317de8404c91de3f00b40e8257b80c64741 | SHA256 | Loader DLL |
| 56e96ce15ebd90c197a1638a91e8634dbc5b0b4d8ef28891dcf470ca28d08078 | SHA256 | Loader DLL |
| 5937746fc1a511d9a8404294b0caa2aedae2f86b5b5be8159385b6c7a4d6fb40 | SHA256 | Loader DLL |
| 7330fa1ca4e40cdfea9492134636ef06cd999efb71f510074d185840ac16675d | SHA256 | Loader DLL |
| 78471db16d7bd484932c8eb72f7001db510f4643b3449d71d637567911ca363b | SHA256 | Loader DLL |
| 814357417aa8a57e43d50cb3347c9d287b99955b0b8aee4e53e12b463f7441a0 | SHA256 | Loader DLL |
| 92a8b74cafa5eda3851cc494f26db70e5ef0259bc7926133902013e5d73fd285 | SHA256 | Loader DLL |
| a765df03fffa343aa7a420a0a57d4b5c64366392ab6162c3561ff9f7b0ad5623 | SHA256 | Loader DLL |
| c3b3f46a5c850971e1269d09870db755391dcbe575dc7976f90ccb1f3812d5ea | SHA256 | Loader DLL |
| c9400b2fff71c401fe752aba967fa8e7009b64114c9c431e9e91ac39e8f79497 | SHA256 | Loader DLL |
| d271569d5557087aecc340bb570179b73265b29bed2e774d9a2403546c7dd5ff | SHA256 | Loader DLL |
| de44656b4a3dde6e0acdc6f59f73114ce6bb6342bec0dcd45da8676d78b0042e | SHA256 | Loader DLL |
| e0f22863c84ee634b2650b322e6def6e5bb74460952f72556715272c6c18fe8e | SHA256 | Loader DLL |
| ea27862bd01ee8882817067f19df1e61edca7364ce649ae4d09e1a1cae14f7cc | SHA256 | Loader DLL |
| edd1480fe3d83dc4dc59992fc8436bc1f33bc065504dccf4b14670e9e2c57a89 | SHA256 | Loader DLL |
| f9290cd938d134a480b41d99ac2c5513a964de001602ed34c6383dfeb577b8f7 | SHA256 | Loader DLL |
| 366d47b95e216863ee64e0024e2bbf0bf1b66420986fe0a5b3e805ce795dcf9f | SHA256 | Encrypted Payload |
| d031081b8c211994b5406bf3f2544c0d6ebcbab384f23e393f084b49563e1d12 | SHA256 | Encrypted Payload |
| f466bc20544bf203155142cf14456e55b0e756aa93ecfb5edc74ba7ed60f9573 | SHA256 | Encrypted Payload |
| ca68f02bd01650383af68f0c129482faf283329dd1e6a18821ad26fc2c3d00b2 | SHA256 | Encrypted Payload |
| d776235e628422ada7f1e976a3cf771049286edf2219583028fbbd6229af72b9 | SHA256 | Encrypted Payload |
| 50a4b19b38caea4eea042704314f5ae1acf2162c7353fb92bc896dcada14b86a | SHA256 | Encrypted Payload |
| 610c3536ceafc0e4ad0d60c683052ee7272e29049ceac909b1d1e55ac1206f49 | SHA256 | Encrypted Payload |
| 7ee6235f0e653a36a818a12531657f6dac5f3fb41efa1e1c63f6761ba3faeb90 | SHA256 | Encrypted Payload |
| 265e5e1389b3145bf2ac1a017b67a54d84bc361dc3795120656dcabc1212c34a | SHA256 | Encrypted Payload |
| 8d2b3b0cbb32618b86ec362acd142177f5890917ae384cb58bd64f61255e9c7f | SHA256 | PyXie RAT interpreter |
| d1429f54baaad423a8596140a3f70f7d9f762373ad625bda730051929463847d | SHA256 | PyXie RAT bytecode |
| ade8f07bf7918343bf307ec35837327efc7a85a0edac5ab5b2cd037134af8d57 | SHA256 | Cobalt Mode |
| fd93858f4e7356bebe30dd0dfe07367e3ddf6164bb78725e1c543b093558cf64 | SHA256 | Cobalt Strike Loader |
| a50b58e24eb261157c4f85d02412d80911abe8501b011493c7b393c1905fc234 | SHA256 | Cobalt Strike Loader |
| 0d14a1b5574dc12f6286d37d0a624232fb63079416b98c2e1cb5c61f8c2b66ff | SHA256 | Cobalt Strike Loader |
| 625c22b21277c8a7e1b701da9c1c21b64bfa02baef5d7a530a38f6d70a7a16d0 | SHA256 | Cobalt Strike Loader |
| bd7da341a28a19618b53e649a27740dfeac13444ce0e0d505704b56335cc55bd | SHA256 | Cobalt Strike Loader |
| d612144c1f6d4a063530ba5bfae7ef4e4ae134bc55dcf067439471934b841b00 | SHA256 | Cobalt Strike Loader |
| ce0936366976f07ea24e86733888e97e421393829ecfd0fde66bd943d4b992ab | SHA256 | Cobalt Strike Loader |
| 3259dd0efed1d28a149d4e8c4f980a19199d9bead951ee1231e3a26521185f2f | SHA256 | Cobalt Strike Loader |