Scattered Spider conducts SIM swapping attacks

Date: 17th April 2024 | Severity: High

Summary

The Scattered Spider threat group (AKA Roasted 0ktapus, UNC3944) has been financially motivated group primarily targets telecommunication service providers. the victims are usually large (Fortune 2000) organizations that have valuable intellectual property assets. Scattered Spider seems to be connected to the operations of the ALPHV ransomware group (AKA BlackCat), either as an initial access broker or an affiliate.

Attack Vectors

Scattered Spider conducts SIM swapping attacks using different social engineering techniques,

- Callback phishing (in which the threat actors impersonate IT experts to obtain user credentials)
- Telegram and SMS phishing messages (smishing) that lead the victims to seemingly legitimate credential-harvesting pages.
- The threat actors also leverage known system vulnerabilities using “Bring Your Own Vulnerable Driver” (BYOVD) techniques to gain administrative privileges and evade detection from endpoint security products.
- The vulnerable drivers used by Scattered Spider are signed by stolen certificates from well-known authorities, such as Microsoft, NVIDIA, and Global Software LLC, which makes them appear legitimate. According to Mandiant, these drivers are part of a toolkit that consists of two components, STONESTOP (loader) and POORTRY (kernel-mode driver). A similar toolkit has been used by different threat actors, such as the Cuba and Hive ransomware groups.
- A successful Scattered Spider intrusion is usually followed by the injection of malware or commercial remote management tools to maintain persistent access to mobile carrier networks and SIM card information.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Hashes	721b40a0c2a0257443f7dcc2c697e28a fe7ecd399eec7036a63f0b7eb5ebcfb1 b8783155d6be5bb3a6d75edaa7ae7f71 ddee86b84dcb72835b57b1d049e9e0cd aba1be25da0691761f593725e9c067e5 0080fde587d6aedccb08db1317360d32 adab615712eac2719691d01b69254f29 de4b5043c82ab3b36b4ae73a2e96d969 6e1bb443369973923c8eced16fcbd5cf 6d32d2d7a44584c92115ac2a2c3ba3af c0471f78648643950217620f6e7e24cc 4b2e59a821589ab091a63770f4a658ed 6c3180163e4a5371647e734c7c817de5 1548b70d8581cbde703b1fb50b48a6a8 4e1f656001af3677856f664e96282a6f 4e8d5c44bfdeffd0168f8a05f6a04e8b fbd-9ba2b8b2d677d41c30a01c02cfd01 b5c73db8e70d6f46ad9b693f3ce060d2 934d0cda4cba428e9b75ff16d5f4b0b1 6e4e37641e24edc89cfa3e999962ea34 24eb9eef-69475e4980a555898b25f0c1 f9aad310a5d5c80bbc61d10cc797e4f0 7c6c1b7e6378b4c0b-cceee84e0e26fde c43de22826a424b2d24cf1b4b694ce07 9a8323bc7187441a0d85b9a2e-8f580e3 63960dbc7d63767edb6e1e2dc6f0707b bb46eb379caae3b05e32d3089c0dd6d0 b34403502499741762912c7bfc9ff21f 3db8146544ee26866a8e99bacb11188c d6b2947d8ff985fa84d697cc6cfdb7ff b164daf106566f444dfb280d743bc2f7 4d4c17d8b52cd89da0b17cc9653b2010 35deaa9d004714dc6ef9661b91889148 6a893aab7b79b73da7a049c2707aabf1 7f9309f5e4defec132b622fadbcad511 9f1d3b0f-b49e063f4804aa60b7b708ac a9541530619a3ac2615b92603b705fe6 d11b9a4664ea03d-fe3e8e1d737cd15f8 48bf11dd6c22e241b745d3bb1d562ca1 7ee0c884e7d282958c5b3a9e-47f23e13 69fa8946c326d4b66a371608d8ffbe5e 0f16a43f7989034641fd2de3eb268bf1 29506adae5c1e97de49e3a0d3cd974d4 7cb012393114dfb35d60e70166a97986 1f929f-d617471c4977b522c71b4c91ed 7182ed3da406ba19bb9ffd8e4948d858 9e91e55c89f-9c17c0a2acaf4376cd72b d60d8f3f12550dca4ba07ff61263b67f b500ee8d8cb-045936d2996a1747bcded e6960ae657786979493da1786191bcf4
IP	185.243.218.41 | 193.37.255.114 | 146.70.45.182 | 198.54.133.52 | 98.100.141.70 207.148.0.54 | 105.158.12.236 | 146.70.103.228 | 134.209.48.68 | 152.89.196.111 45.134.140.171 | 138.68.27.0 | 143.244.214.243 | 100.35.70.106 | 31.222.238.70 146.190.44.66 | 185.195.19.206 | 185.45.15.217 | 82.180.146.31 | 188.166.92.55 35.175.153.217 146.70.45.166 146.70.127.42 198.54.133.45 136.144.19.51 172.96.11.245 89.46.114.164 | 93.115.7.238 | 45.134.140.177 | 185.156.46.141 | 45.32.221.250 180.190.113.87 | 172.98.33.195 | 159.223.213.174 | 185.123.143.205 | 157.245.4.113 185.123.143.197 | 193.149.129.177 | 37.19.200.151 | 119.93.5.239 | 173.239.204.132 173.239.204.130 | 159.223.208.47 | 62.182.98.170 | 144.76.136.153 | 45.86.200.81 91.242.237.100 | 169.150.203.51 | 83.97.20.88 | 64.190.113.28 | 68.235.43.38 105.101.56.49 | 173.239.204.131 | 159.223.238.0 | 185.56.80.28 | 45.132.227.211 185.181.102.18 | 37.19.200.142 | 185.240.244.3 | 45.91.21.61 | 51.210.161.12

Recommendation

- Employee Training and Awareness.
- Stay up to date with known vulnerabilities.
- Use strong passwords on all the devices on your network and change them regularly.
- Do not open suspicious email attachments.
- While good access control, risk management, and design will limit the impact of a known vulnerability, it's better to just ensure you have few known vulnerabilities and mitigate them as needed.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://www.cbsnews.com/news/scattered-spider-blackcat-hackers-ransomware-team-up-60-minutes/
- https://www.darkowl.com/blog-content/threat-actor-spotlight-scattered-spider/