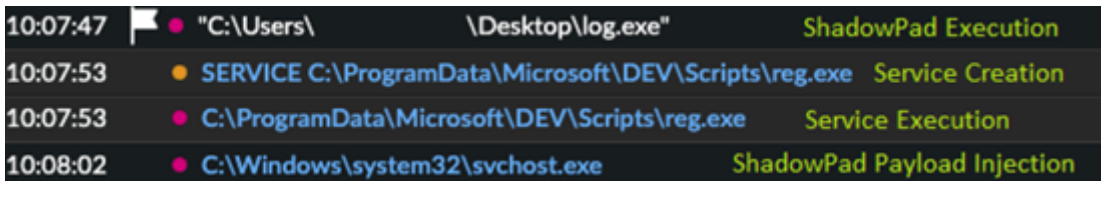
Severity

High

Analysis Summary

ShadowPad is a RAT (Remote Access Trojan) that being used frequently by several Chinese state-sponsored Threat actors. The activity using ShadowPad is also linked to the MSS (Chinese Ministry of State Security) and the People's Liberation Army (PLA). It is mostly a two-file execution malware; a DLL loader containing a ShadowPad payload embedded in it. Threat actors using ShadowPad are targeting South Korea, India, Japan, Ukraine, Russia, and Mongolia. One such group is TAG-38 which has recently targeted Indian power grid assets.



Observed timeline of ShadowPad execution, service creation, and payload injection on a compromised network.

Impact

- Unauthorized Access
- Financial Theft
- Information Theft

Indicators of Compromise

Domain Name

- vsmrcil[.]casacam[.]net
- exat[.]dnset[.]com
- dprouds[.]casacam[.]net
- secupdate[.]kozow[.]com

IP

- 172[.]197[.]18[.]30
- 172[.]200[.]21[.]190

MD5

- 9d686ceed21877821ab6170a348cc073
- 27d889c351ac2f48d31b91d06061ec8d
- 17e812958704f4ced297731ce47de020
- fac0b4fe5372d76607c36ccb51e6b7bb
- 17268032c7562fa9473bb85018cb1c2c

SHA-256

- 9c28c1b2ff0a84c8b667f128626f28b173feb07481192e214b5a29b98964a7f9
- d48e671df571b76ee94c734bdd5272e12fcd1362f1d75138ff547bc2bc0c31ef
- 0942f4a488899d5d78b31a0065e49c8689ccda88efc28186e29ee76861ba99da
- 4557e923602730aab7718b61eeaf3a93edd0339a3c89c8f7061b9818c2df5203
- bf3de88459f85ddd85245e3f1ce3bba6568919bbe46a808ad5d94d5415014926

SHA-1

- 3ebeb4e08c82b220365b1e7dd0cc199b765eed91
- f5b7ea5e705655a1bc08030b601443088a5af4dd
- 57b5ca13d7b2dd9287bdda548ccf7b21c1201464
- 952614358b37d2a519d66ee7759c70e31218ed36
- 3d1ae0779b304a8d54df142933158417440ca3f

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.