AEC

Možné aktivity TA505 v ČR v prosinci 2019

Suspected TA505 activities in Czech Republic in December 2019

11. prosince 2019 / December 11, 2019

Shrnutí

Phishingová kampaň na finanční instituce v České republice byla zahájena nejpozději 9. 12. 2019. Se střední mírou jistoty je tato kampaň připisována kriminální skupině TA505 (také známé jako Evil Corp, autor bankovního trojanu Dridex, ransomwaru Locky a dalších).

AEC Cyber Defense Center zveřejňuje IOC (indikátory kompromitace) zanechané skupinou při této kampani k získání a udržení přístupu. Doporučujeme bezpečnostním týmům kontrolu těchto IOC, aby se ujistily, že nedošlo ke kompromitaci jejich prostředí.

Summary

A phishing campaign targeting financial institutions in the Czech Republic was launched no later than October 9, 2019. With medium confidence, the campaign is attributed to known cyber-crime group TA505 (a.k.a. Evil Corp, author of Dridex banking Trojan, Locky ransomware and others).

AEC Cyber Defense Center publishes IOCs (Indicators of Compromise) left by the group during this campaign to gain and maintain access. We advise the security teams to check these IOCs to confirm their environments were/are not compromised.

www.aec.cz/cdc
cdc@aec.cz

AEC

Indikátory kompromitace / Indicators of Compromise

Type	IOC
Domain	onms-home.com
IPv4	45.67.229.220
Domain	upgrade-ms-home.com
IPv4	185.176.221.154
SMTP Subject	Faktura FV20586324
SMTP Subject	Faktura FV20810288
SMTP Subject	Faktura FV20134685
SMTP Subject	tabulka registrace
SMTP Subject	need payment
SMTP Subject	faktura
SMTP Subject	oznámení o platbě
SMTP Subject	vzorek
MD5	40d7a07636c81dbc56ffe334a817a696
SHA1	89db75be84c74958b3dd95363feb8c89d0cb7ec4
SHA256	18eacc8f80d1638e2e6dda6cba8e8b57fe9d07faa51082a5773a4ec07e8ab453
MD5	24ccb38ce1f35b4e124b7aee6ab82861
SHA1	83313f3156aa0e3cc98ff5dea9d58e5d9e5f802b
SHA256	5327f14dd9ab62371f8537952bb86b8410d7346bfdd601f7910447fb20b24f8d
MD5	40d7a07636c81dbc56ffe334a817a696
SHA1	89db75be84c74958b3dd95363feb8c89d0cb7ec4
SHA256	18eacc8f80d1638e2e6dda6cba8e8b57fe9d07faa51082a5773a4ec07e8ab453
MD5	516dac7047225d806f226d9af107cc77
SHA1	186cee7cae4d37fcac82f3c0a67d39ae66c0f314
SHA256	4f1400473ee37e6ea4c0cb49b68d66b213bbb326970e90bca217777428abdc7c
MD5	402386d80af36fc24239b23ef519e3f2
SHA1	7b27c4e9095d10ba07df25f92825bdca036edc08
SHA256	c9fff049dfe7e17a3b52bb74389f793cc163d33cd034ce40365b7531e14f8cf5
MD5	7E99D116BF2938C40E1F124E0A019352
SHA1	0DDB735AE6E04D04719DF1AFD7854B3C5B95CE63
SHA256	3C164FE76E2AA7CCB488D99FB38EF22CD431FA90445E492B30C16647977F1CB0