Dedikované servery

FTP malware

Mezi zvláště nebezpečné patří malware, který dokáže získat uložená hesla z FTP klientů. Nejčastějším důvodem k takovému útoku je získat přístup ke všem souborům na webserveru, protože tyto jsou většinou spravovány přes FTP. Jakmile získá útočník přístup k FTP serveru, má možnost měnit existující dynamický obsah (PHP, ASP a další) tak, aby obsahoval škodlivý kód. Tímto získává útočník možnost nakazit návštěvníky upraveného webu prostřednictvím validních stránek.

Existuje velké množství FTP klientů, kteří nabízí široké spektrum funkcí. Jednou z nich je i schopnost uchovávat přihlašovací údaje navštívených serverů, která je obzvláště zajímavá pro útočníky. Většina těchto klientů ukládá tyto hesla lokálně a často nešifrovaně.

Jak to celé funguje?

Oběť otevře email nebo navštíví stránku, která je napadená. Jak jsme uvedli výše, může být zdrojem škodlivého kódu i validní stránka. Proto je dobré používat aktualizovaný operační systém, webový prohlížeč a antivirus.

Po napadení trojan nalezne všechny FTP přihlašovací údaje uložené ve FTP software jako Filezilla, WS_FTP, CuteFTP a dalších. Získané přístupové údaje jsou odeslány centálnímu serveru spravovanému útočníkem a jsou uchovány pro pozdější použití. Je pravděpodobné, že jsou tyto dále sdíleny mezi komunitou.

Centrální server automaticky zjišťuje, jestli nějaký z ukradených účtů patří k FTP, na kterém se nachází veřejný web. Poté skript uploaduje soubory se jmény jako "70f70c620045f63c38a2dc3705b7bb80.html", "ftpchk3.php" or "ftpchk3.txt" a v případě úspěchu reportuje zpět. Dále skript ověří, že je obsah čitelný z Internetu a pokud ano, tak je uveden jako schopný přenosu nákazy. Poté skript smaže všechny vytvořené HTML, PHP nebo TXT soubory, aby nezůstaly zjevné stopy škodlivé aktivity.

Jak se bránit?

Proti tomuto typu útoku je těžké se bránit a odpovědnost je především na straně klienta. Abyste předešli potenciálnímu zneužití, je potřeba se ujistit, že používáte pravidelně antivirus s aktualizovanou databází hrozeb a vyhýbáte se podezřelému obsahu na webu nebo v emailové komunikaci. Ideální je hesla k FTP účtům v počítači neukládat nešifrovaně.

Unikátní ID: #1052
Autor: Technicka podpora
Aktualizováno: 2020-08-07 20:33

(c) 2020 Podpora Vshosting <tech@vshosting.cz> | 2020-08-09 19:12

URL: https://support.vshosting.cz/content/11/53/cs/ftp-malware.html