Vážení zákazníci,

Dnes se mi již ozvalo 7 operátorů se zablokovaným přístupem na své stroje MikroTik.
Virus je nyní velmi systematický, napadá stroje po SSH čímž si testuje přístup. Dále využije chybu přetečení bufferu NetBiosu (tedy blokace IP protokolu nepomůže) a lokálně po L2 vrstvě napadá okolní stroje.
Tato chyba je popsána cca rok zpět, MikroTik prohlašuje, že definitivně je opravena ve verzi **6.42.1**, viz zde https://www.coresecurity.com/advisories/mikrotik-routeros-smb-buffer-overflow

Jediná výhoda je v PPPoE či routovaných sítích, že šíření tam trvá podstatně déle než na transparentních sítích, kde je šíření přímo lavinové.
Virus si nahraje script do MikroTiku, ten Vám zahesluje a zároveň si vytvoří NOVOU PARTITION – TAKŽE FYZICKÝ NETINSTALL NUTNÝ !!! PŘÍPADNĚ U PC PŘEINSTALACE Z CD !!!
Pokud stroj pouze vyresetujete, použije svou vytvořenou partition a znovu se spustí, virus je velmi rychlý

Problém Vašich PC a notebooků :
DÁLE SE INFIKUJÍ DLL knihovny, které si stahujete jakýmkoli starším WinBoxem než 3.11 (nejedná se o verzi software MikroTik ale o verzi Winboxu, kterou najdete nahoře v řádku po spuštění WinBoxu před zalogováním kamkoli)
!!! TYTO POZMĚNĚNÉ KNIHOVNY SI STÁHNETE DO VAŠICH PC A TAKTO SNADNĚ SE PAK VIRUS ŠÍŘÍ NA DALŠÍ STROJE, KTERÉ JENOM WINBOXEM NAVŠTÍVÍTE !!!!
!! JE TŘEBA ve Vašich PC -> TEDY SMAZAT VŠECHNY STAŽENÉ DLL V ADRESÁŘI /User/AppData/Roaming/MikroTik/Winbox !!!

Postup pro dezinfekci PC : (tím začít, jinak si to šíříte sami)
Upgrade Winbox na 3.13 z MikroTik.com (nebo stačí při spuštění WinBoxu nahoře tlačítko Check for Update v Advanced Mode)
SMAZAT VŠECHNY STAŽENÉ DLL V ADRESÁŘI /User/AppData/Roaming/MikroTik/Winbox !!!
Dále raději reinstalaci PC – antivir toto nepovažuje za vir, je to útok cílený jen na administrátory sítí, takže to virové společnosti ještě nezachytily ;-(

Postup pro dezinfekci routerů co jsou napadené :

Provést NEINSTALL na RB, případně instalaci z CD na PC verze, je to nutnost, pro smazání virové partition (viditelné jedině při použití OpenWRT v-instalované do flashky jako druhý systém – návody jsou na netu)
Instalaci provést s verzí 6.41.3 a výš, kde je dle MikroTiku chyba odstraněna. Dokonce na verzích TILE pro CCR je změněno DH šifrování SSH klíčování – nebude pak fungovat ani automatizované připojování skrze SSH z jiných systémů

Postup pro zamezení šíření na zdravých strojích :

Povýšit verzi nad 6.41.3. která je MikroTikem vyhlášena již za bezpečnou !!!
Změnit přístup v IP SERVICES – zakázat WWW, API (použít API-SSL s certifikátem), FTP, TELNET – změnit port na SSH SSH a WINBOX omezit přístup jen na lokální sítě, vzdáleně jen přes VPN
POZOR vir se šíří chybou SMB overflow popsanou výše, tedy blokace IP protokolu ve firewallu nepomůže !!!

Hodně štěstí všem postiženým, silné nervy a funčkní auta ;-)

Zatím zdravím a přeju krásný den,

Kryštof Klíma ****
poskytování poradenství v oblasti sítí Lan a Wan, servis a prodej výpočetní techniky
Mobil: +420 774 331 774 **E-mail: klima@wifiprofi.cz**