Altnet s.r.o.

Virus motherfucker – bezpečnost v sítích

Martin MaKr Kratochvíl

skvely.net: používáme AirOS

Síť skvely.net – řeší cca 4500 zákazníků

3000 Airos zařízení u zákazníka
1000 Airos zařízení na našich vysílačích

Airos je modifikovaný linuxový systém

Virus: Zneužívá neznalost správce

Virus – co potřebuje k šíření?
- vstup do systému
  – násilím
  – dírou
  – znalostí univerzálních hesel
- pracovat v systému
- mít se jak a kam šířit

Skynet: První díra v Airosu (2011)

AirOS <= 5.3.3

Vstup do systému:
– pomocí „ladící“ stránky /admin.cgi
– heslo obchází pomocí hacku admin.cgi/.gif

Šíření:
– pomocí „nc“ - požadavky na $IP/admin.cgi

Zabezpečení: lighttpd.conf a povolení „.gif“

Skynet: Druhá díra v Airosu (2016)

AirOS <= 5.6.2

Vstup do systému:
- web rozhraní (php2) neověřovalo USER/PASS při nahrání souboru. Soubor se nahrál do cesty uvedené v požadavku!
- nahrál se ssh klíč či /etc/passwd a následně ssh/telnet
- wget to neumí, CURL však řezal jak nůž do másla

Šíření:
- pomocí „curl“ - v AirOSu není. Wget lze však curl stáhnout!
- http (https) požadavek, následně ssh/telnet přístup

Zabezpečení: Oprava php2 „binárky“

AIROS a jeho zabezpečení?

Skynet - fw po té
– zmizela binárka „nc“
– odstraněna stránka /admin.cgi z firmware

Motherfucker
- fw >= 5.6.3, opravený php2
  (Changelog: php2 buffer overflow)
- fw >= 5.6.5 zakáz možnosti vlastních skriptů

AIROS a skvely.net

Skynet: Upozornily nás časté restarty (nagios – logy)
--> vlastní firmware z SDK úprava konfigurace =>
kompilace

Firmware: problém aktualizací modifikací – pracné

Motherfucker: Zařízení mimo naši správu
- shield.tgz sada skriptů do starších fw
- modifikovaný firmware pomocí „rozbalení“ -
„zabalení“ vydané verze

Jak zabezpečit svoji síť?

ZAŘÍZENÍ JSOU DĚRAVÁ

FIREWALL
- rozlišujte provoz skrz zařízení
  a provoz do zařízení (iptables input / forward)
- přístup do internetu? Přístup od zákazníka?
- administrativní VLAN / či aspoň rozsah IP

MONITORUJTE provoz, vyhodnocujte LOGY

HROMADNÁ SPRÁVA – skripty? Aplikace?