32%-den 50%-e çenli: 2024-nji ýylda her ikinji kiberhadysa iş proseslerini bozýar
07.11.2024
39% ýagdaýda hünärmenler 17 belli APT toparynyň işjeňliginiň yzlaryny tapdylar.

Positive Technologies howpsuzlyk merkeziniň kiberhowplara jogap bermek bölüminiň hünärmenleri — bu kiberhowpsuzlyk boýunça ýöriteleşen rus kompaniýasy. Bu ugurda dünýäniň öňdebaryjy hyzmat we önüm üpjün edijileriniň biridir. Positive Technologies (PT ESC IR) SOC forumynda kiberhadysalary derňemek we ýylyň netijeleri boýunça retrospektiw analiz boýunça taslamalaryň statistikasyny hödürledi. 2023-nji ýylyň soňky çärýegi we 2024-nji ýylyň ilkinji üç çärýegi üçin hünärmenlere esasan senagat kärhanalary, döwlet edaralary we IT kompaniýalary ýüz tutdy. Üstünlikli hüjümleriň esasy sebäpleri könelen programma üpjünçiligi, iki faktorly autentifikasiýanyň ýoklugy we korporatiw toruň gowşak segmentasiýasy boldy.

Hasabata görä, analiz edilen kompaniýalaryň 39%-inde 17 belli guramaçylykly jenaýat toparynyň (APT) işjeňliginiň yzlary tapyldy. Bu toparlar ulanylýan gurallar we zyýanly programma üpjünçiligi, infrastruktura we taktikalary boýunça kesgitlenýär. Olar köplenç uzakdan elýeterlilik, maglumatlary ýygnamak we ogurlamak üçin ýöriteleşdirilen programma üpjünçiligini ulanýarlar. Tapylan toparlaryň köpüsi ýokary hünärli we maksatlaryna çalt ýetmäge ukyplydyr.

Işlenilen döwürde tapylan ähli toparlaryň arasynda PT ESC topary üçüsini aýratyn belledi: Hellhounds — tehnikalar babatynda iň ösenleriň biri hökmünde, ExCobalt — iň işjeň topar hökmünde we XDSpy — iň uzak wagtlap hereket edýän topar hökmünde (2011-nji ýyldan bäri Russiýadaky kompaniýalara hüjüm edýär).

Podratçylar arkaly hüjümleriň ýygylygy ýylda 15% ýokarlandy. Bu podratçylaryň köpüsi onlarça müşderä hyzmat edýär. “Şeýle hüjümleriň paýy henizem az bolsa-da, ygtybarly, ýöne goragsyz hyzmatdaşlaryň döwülmeginden ýüze çykýan hakyky we potensial zyýan çalt artýar” diýip, Positive Technologies belleýär. Ilkinji aralaşma usullarynyň arasynda web programmalaryndaky gowşaklyklardan peýdalanmak öňdebaryjy orny eýeleýär. Geçen ýylyň dowamynda hüjümleriň iň köp sany (33%) CMS “1C-Bitrix” esasly web sahypalaryna düşdi, bu olary gowşak web programmalary arkaly aralaşmagyň esasy ugruna öwürdi. Şol bir wagtyň özünde, Microsoft Exchange poçta serwerlerindäki gowşaklyklardan peýdalanmak bilen başlanan hüjümleriň paýy 50%-den 17%-e çenli azaldy.

Kompaniýalaryň 35%-inde “Kiberjenaýat” kategoriýasyna degişli hadysalar hasaba alyndy — maglumatlary şifrlemek we ýok etmek ýaly destruktiv hereketlere gönükdirilen hüjümler. Şeýle ýagdaýlarda hüjümçiler adatça şifrleýjiler, maglumatlary şifrlemek üçin kanuny

programma üpjünçiligi we maglumatlary doly ýok etmek üçin wiperler ulanýarlar. Bu gurallar hem yzlary gizlemek we hadysany derňemek prosesini mümkin boldugyça kynlaşdyrmak üçin ulanylýar.

Öňki ýyllar bilen deňeşdirilende, kiberhadysalaryň iş proseslerініň bozulmagyna sebäp bolan ýagdaýlarynyň paýy 32%-den 50%-e çenli ýokarlandy. Munuň sebäbi haktivistleriň we maliýe taýdan höweslendirilýän hüjümçileriň işjeňliginiň artmagy bolup biler. Taslamalaryň 19%-inde APT toparlarynyň işjeňligi bilen baglanyşykly gözleg we içalyçylyk işjeňliginiň yzlary tapyldy. 12% ýagdaýda hüjümçiler gizlin maglumatlary göçürip almaga synanyşdylar, şol bir wagtyň özünde kompaniýanyň infrastrukturasynda uzak wagtlap bolmakdan gaça durdular. Öňküsi ýaly, hüjümleriň esasy maksady Windows esasly düwünler bolup galdy, ýöne Linux esasly düwünlere edilen hüjümleriň paýy hem ep-esli boldy (28%).

Hünärmenler, ýerli kompaniýalaryň hadysalary derňemek boýunça işlere bolan isleginiň ep-esli ýokarlanandygyny belleýärler. Soňky iki ýylyň dowamynda olaryň sany üç esse artdy.