Demirgazyk Koreýaly hakerler zyýanly kody adaty bildirişler hökmünde nädip maskalaýarlar.

Demirgazyk Koreýanyň ScarCruft topary, Microsoft tarapyndan işlenip düzülen we çykarylan şahsy kompýuterler üçin operasiýa ulgamy bolan Windows-daky gowşaklygy ýene-de ulandy. OS ulanyja amatly interfeýs we kompýuter bilen işlemek üçin giňişleýin funksiýalary hödürleýär. Windows-yň ilkinji wersiýasy 1985-nji ýylda çykdy.

Windows-yň kömegi bilen ulanyjylar iş, okuw, güýmenje, programma üpjünçiligini işläp düzmek we ş.m. ýaly dürli zerurlyklary ýapyp bilerler.

Windows giň gerimli enjamlary goldaýar, bu ony dünýäde iň meşhur we giňden ulanylýan iş stoly OS edýär, şeýle hem ykjam enjamlarda hem işläp bilýär.

Demirgazyk Koreýanyň ScarCruft topary, zyýanly programma üpjünçiligi RokRAT-y ýaýratmak üçin Windows-daky gowşaklygy ýene-de ulandy. Ekspluatasiýa, Internet Explorer re modeiminde Edge arkaly uzakdan kod ýerine ýetirmäge mümkinçilik berýän Scripting Engine-de ýat ýalňyşlygy bilen baglanyşykly CVE-2024-38178 gowşaklygyny öz içine alýar.

Microsoft bu meseläni 2024-nji ýylyň awgust aýynda Patch Tuesday täzelenmeleri bilen düzetdi, ýöne hakerler tizligini peseltmän, täzelenmedik ulgamlara hüjüm edýärler.

Hüjümi işjeňleşdirmek üçin, hüjümçiler pidany ýörite taýýarlanan baglanyşyga geçmäge ynandyrmalydyr. AhnLab Howpsuzlyk Adatdan daşary ýagdaýlara jogap merkezi (ASEC) we Günorta Koreýanyň Milli kiberhowpsuzlyk merkezi (NCSC) bu kampaniýany “Code on Toast operasiýasy” diýip atlandyrdy. Halkara gurşawda ScarCruft topary TA-RedAnt, APT37, InkySquid, Reaper, Ricochet Chollima we Ruby Sleet ýaly atlar bilen hem tanalýar.