BitDefender

Ndërsa vazhdon puna nga shtëpia, studiuesit në Bitdefender zbuluan muajin e kaluar se ruterat e Linkys janë prekur nga një fushatë malware. Të paktën 1.200 përdorues të aplikacionit Smart Wi-Fi të L kishin ndryshime ne konfigurimet e DNS'se te cilat u ndryshuan për të ridrejtuar viktimat në një faqe interneti që shërben për malware që shpërndan vjedhësin e informacionit Oski si ngarkesën përfundimtare. Infostealer Oski, i zbuluar në dhjetor 2019, nxjerr kredencialet e përdoruesit nga shfletuesit e uebit, regjistrat i Windows, portofolat e cryptocurrency dhe bazat e të dhënave SQLite. Linksys u përgjigje duke bllokuar të gjitha llogaritë Wi-Fi Smart të Linksys që u kërkojnë përdoruesve të ndryshojnë fjalëkalimet e tyre. Sulmet ridrejtuan kërkesat për domene të tilla si: Disney.com, aws.amazon.com, cox.net, washington.edu, dhe të tjerët.

Ndërsa përdoruesi përpiqeshin të arrinin në një nga domain'et, ato ridrejtoheshin në një mesazh të supozuar nga Organizata Botërore e Shëndetësisë duke u kërkuar atyre të instalojnë një aplikacion që ofron udhëzime dhe informacione rreth COVID-19.

Ruterat e Linksys me firmware të perditesuar nuk duket te jene prekur.

Microsoft

Studiuesit në Microsoft kanë deklaruar se joshja më e frytshme me temë COVID-19 është malware Trickbot. Disa nga këto përpjekje për "spear-phishing" pretendojnë se janë organizata jo-fitimprurëse që ofrojnë një test COVID-19 falas (me një shtojcë makro-laced në mesazh).

Malware nga Trickbot u përdor fillimisht si një trojan bankar, por ka evoluar në ofrimin e mjeteve të hyrjes në distancë (remote Access_ dhe ransomware të tilla si Ryuk. Google raporton se po bllokon 240 milion emaile me tematikë korona virus të destinuara për përdoruesit e Gmail çdo ditë.

Netflix dhe Facebook

Duke përdorur një abonimi falas në Netflix si një joshës, aktorët me qëllim të keq po kërkojnë me anë të phishing për kredenciale përmes mesazheve me tekst dhe Messenger në Facebook. Viktimat duket se janë ridrejtuar në një faqe phishing të dizajnuar për të imituar Facebook-un, duke bërë që përdoruesit të regjistrohen me kredenciale të tyre të Facebook. Për më tepër, përdoruesve u kërkohet të postojnë lidhjen keqdashëse në profilin e tyre në Facebook, duke tërhequr më shumë viktima të mundshme.

Zoom

Aktorët me qëllim të keq duket se po përfitojnë nga pritja që platformat argëtuese të ulin pengesën e tyre për akses gjatë pandemisë COVID-19. Duke përmendur raportet se 500,000 kredencialet e Zoom u zbuluan pas një fushate marrjes të kredencialeve, qeveritë nëpër botë u bëjnë thirrje qytetarëve të tyre të tregohen të kujdesshëm kur përdorin platformën. Në përditësimin e tij të fundit, Zoom ka vazhduar azhurnimin e platformës për të adresuar shqetësimet e privacisë dhe sigurisë. Karakteristikat e trafikut të bllokuar sipas rajonit tani lejojnë përdoruesit të specifikojnë se në cilat qendra të të dhënave duhet të drejtojnë takimet e tyre. Përditësimi u shty në 18 Prill 2020.