Mga “Bulletproof” na hosting provider: Mga bitak sa armor sa imprastruktura ng cybercriminal

Umaasa ang mga matagumpay na cybercriminal sa ligtas, nakatago at matatag na imprastruktura. Sa likod ng bawat pagkakompromiso ng network, mga ninakaw na pagkakakilanlan, ransomware, o pagnakaw ng mga datos at pagbebenta ng mga iligal na plataporma, ay isang matatag na imprastruktura na nagbibigay-daan sa mga cybercriminal na magsagawa at mananatiling nakakubli.

Ngunit, para sa mga cybercriminal, ang pananatiling nakakubli at mahirap matukoy ay lalong nagiging mapanghamon. Ang pandaigdigang pagtutulungan sa pagitan ng mga gobyerno, tagapagpatupad ng batas at ng pribadong sektor ay nagpapahirap sa kanila na mananatiling di-nakikilala sa online. Dagdag pa dito, kakaunting mga cybercriminal ang may mga kakayahan at kadalubhasaan na kinakailangan sa pamamahala at pagmementena ng sarili nilang ligtas na imprastruktura. Dahil dito, naghahanap sila ng mga provider ng iligal na imprastruktura na makakapagbigay ng serbisyong ito para sa kanila, upang matutukan ng mga cybercriminal ang mga biktima at kikitain.

Ang ‘cybercrime-as-a-service’ ay tumutukoy sa iligal na merkado (underground market) na umusbong upang masuportahan ang hanay ng mga malisyosong cybercriminal. Ang underground market na ito ay kinabibilangan ng lumalaki at nagbabagong hanay ng mga gamit na nabibili, serbisyo, at impormasyon na siyang tumutulong sa mga cybercriminal sa pambibiktima sa kanilang mga online target. Ang mga gustong maging cybercriminal ay maaaring bumili ng pag-access sa mga network, bumili ng mga tool na tutulong sa pag-iiwas sa mga hakbang na pangseguridad, at ganoon din sa pagbili ng malware laban sa mga biktima upang manakaw ang kanilang personal na impormasyon. Ang mga bulletproof hosting (BPH) provider ay bahagi ng ekosistemang ito at nag-aalok sila ng matatag na imprastruktura para sa mga cybercriminal. Mahalagang tandaan, ang isang BPH provider ay maaaring direktang magbigay-daan sa daan-daang mga cybercriminal upang targetin ang mga biktima sa buong mundo.

Ano ang isang “Bulletproof” hosting provider?

Sa madaling salita, ang mga BPH provider ay nagpapaupa sa mga cybercriminal ng virtual at/o pisikal na imprastruktura para magamit sa kanilang operasyon. Ang mga BPH provider ay isang natatanging uri ng serbisyo sa imprastruktura ng internet na nagbibigay-daan sa mga malisyosong aktor (kabilang ang mga cybercriminal) na mag-host ng iligal na content at magsagawa ng mga operasyon sa internet.

Ang salitang “bulletproof” ay purong marketing lamang. Sa katunayan, ang mga serbisyong ito aymaaari ring magambala katulad ng iba pang provider ng imprastruktura. Sa halip, ang mga BPH provider ay ayaw sumunod sa mga ipinag-uutos ng tagapagpatupad ng batas at sa mga hiling na alisin ang content at hindi pinapansin ang mga reklamo ng pang-aabuso mula sa mga biktima at mga abiso ng kahilingan mula sa mga subscriber. Nangangahulugan ito na ang mga cybercriminal ay maaaring makipagkomunikasyon, magpatakbo ng mga ilegal na forum at mga website, magpakalat ng malware at phishing campaign, at gumawa ng money laundering nang walang takot na wawakasan ng opereytor ang kanilang pag-upa dahil sa mga kahilingan ng mga tagapagpatupad ng batas at iba pa.

May kaalamang nakikisali ang mga BPH provider sa ekosistema ng cybercrime at nagbibigay ng kakayahan sa mga seryosong cybercrime na ang motibasyon ay pera. Nangyari na ang mga malalaking insidente ng Cyber Security na nakakaapekto sa mga samahang Australyano at sa kanilang mga kustomer dahil sa paggamit ng mga kriminal sa mga BPH provider. Kasama sa mga resulta ng mga insidenteng ito ang mga mapanirang pag-atake ng ransomware, pangingikil kapalit ng mga datos at pagnanakaw ng mga sensitibong impormasyon.

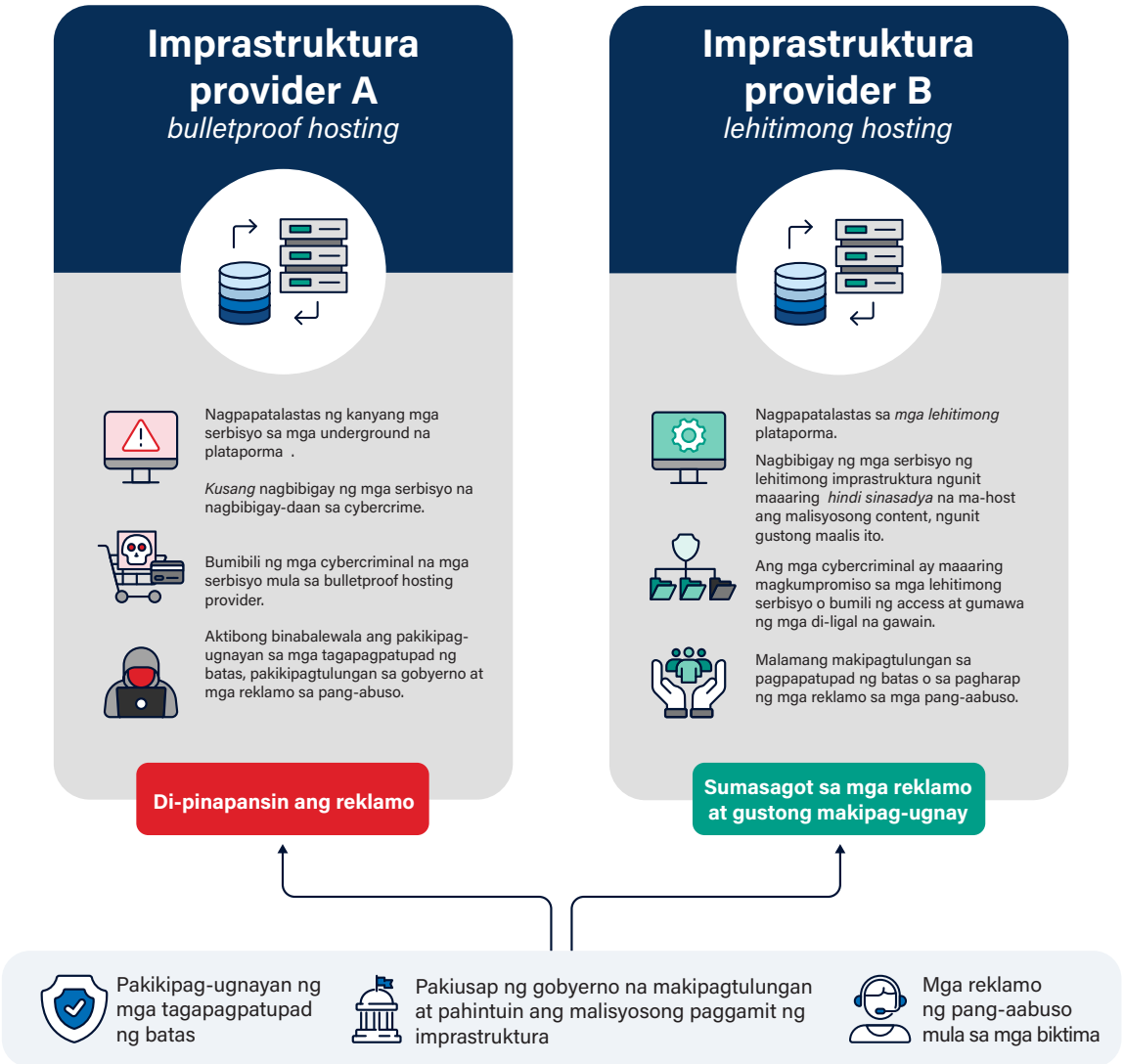
Ang mga halimbawa ng advertisement ng isang bulletproof hosting provider sa mga underground forum:

Paaano gumagana ang mga BPH provider?

Magkakaiba ang business model sa bawat BPH provider. Ang pinakakaraniwang pamamaraan ay ang pagpapaupa ng mga IP address sa mga kustomer na cybercriminal at paggamit ng mga kumplikadong pamamaraan sa pagpapalit ng network upang maitago ang kanilang mga lokasyon, pagkakakilanlan at aktibidad. Sa maraming kaso, ang mga BPH provider ay muling ibinebenta o ipinapaupa ang mga IP address at server mula sa mga ibang lehitimong hosting provider, data centre o Internet Service Providers (ISPs). Ang mga ‘upstream’ na provider na ito ay maaaring hindi alam na sila ay nagbibigay ng imprastruktura sa mga BPH provider na sila namang nagbibigay ng mga serbisyo ‘downstream’ sa mga cybercriminal.

Ang mga BPH provider ay binabago ang anyo ng kanilang mga network at sistemang arkitektura upang mas mahirap na matukoy ang kanilang mga kustomer. Halimbawa, palagi nilang binabago ang kanilang mga internet facing identifier na kaugnay sa mga aktibidad ng mga kustomer – katulad ng kanilang mga nakatalagang IP address at domain name. Ang mga ganitong pamamaraan ay nagpapahirap sa mga taga-depensa at imbestigador na maiugnay ang isang insidente sa IP address na ginagamit ng isang aktor o kustomer sa anumang partikular na oras. Dagdag pa dito, ang mga BPH provider ay palaging gumagamit ng imprastruktura sa mga bansang di-istrikto sa pamamahala ng mga cyber, kung saan wala o maluwag ang mga pormal na paraan sa pag-iimbestiga at pagpigil sa mga malisyosong aktibidad sa cyber.

Paano naiiba ang mga bulletproof hosting provider sa mga provider ng lehitimong imprastruktura?



Paano maaapektuhan ng pag-target sa mga BPH provider ang banta ng cybercrime

Ang mga BPH provider ay mahalagang pagkakataon upang mapatigil nang sabay-sabay ang daan-daan hanggang libo-libong mga cybercriminal. Iba’t ibang mga cybercriminal at malisyosong cyber actor ang gumagamit sa mga serbisyong ito upang mas madali silang makagawa ng kanilang panloloko – naniniwala na ang kanilang mga aktibidad ay mananatiling nakatago at gumagana kahit na may mga kahilingang ipatigil at mga reklamo ng pang-aabuso.

Ngunit, ang mga tagapagpatupad ng batas, ahensya ng Gobyerno at ang pribadong sektor ay nagtutulungang targetin at patigilin ang mga provider ng mga iligal na imprastrukturang ito, kasama dito ang paggamit ng mga Depensibong hakbang katulad ng mga maagap na paghadlang sa trapiko ng internet mula sa mga kilalang BPH provider. Ang mga gawaing ito ay tumutulong sa pagbawas sa bilang ng cybercrime na nakikipag-ugnay sa mga network ng Australya at kaalyado nito, kasama ang mga lehitimong ‘upstream’ infrastructure provider at ISP na maaaring hindi alam na ginagamit sila ng mga BPH provider upang ma-access ang internet at makapagpigay ng ligtas na imprastruktura sa mga cybercriminal.

Ang mga BPH provider ay hindi lamang nag-iisang kategorya ng provider ng imprastruktura sa loob ng cybercrime-as-a-service ecosystem. Ang mga serbisyong ito ay nagpapalaganap at nagbibigay-daan sa banta ng cybercrime sa Australya sa pamamagitan ng aktibong pagsuporta sa mga kampanya ng cybercriminal at sadyang hinahadlangan ang lehitimong pag-imbestiga at pagresponde ng awtoridad. Ang pagkilos laban sa mga BPH provider ay nagpapakita ng kahinaan ng mga serbisyong ito at ng mga malisyosong cyber actor na gumagamit ng mga ito.