HOSPODÁRSKE NOVINY
UTOROK 19. APRÍLA 2022

Útočníci zneužili vojnu a obavy Európanov

Útočníci cielia svoje útoky najmä na neziskové organizácie.

ILUSTRAČNÁ SNÍMKA: DREASMTIME

ŠPIONÁŽ

Špionážna kampaň trvá najmenej od augusta 2021. Skupina Mustang Panda svoje útoky cieli najmä na vládne a neziskové organizácie v Ázii.

Gabriela Alenová ©hn
gabriela.alenova@mafraslovakia.sk

Kým niektorí sa snažia obetiam vojnového konfliktu u našich východných susedov pomáhať, iní tragickú situáciu využili. Útočníci, ktorí zneužívajú vojnu na Ukrajine, cielia svoje útoky najmä na neziskové organizácie. Medzi obeťami špionážnej kampane sú výskumné organizácie, poskytovatelia internetových služieb a európske diplomatické misie. Útočníci využívajú na šírenie malvéru falošné dokumenty, ktoré sú pravidelne aktualizované a odkazujú na udalosti v Európe a vojnu na Ukrajine. Kybernetická operácia využíva vlastný loader na spustenie malvéru Hodur, ktorý je novým variantom trojanu Korplug. Každá fáza inštalácie škodlivého kódu využíva rôzne techniky na sťaženie analýzy programu vrátane skomplikovania toku jeho riadenia, čím sa odlišuje od iných kampaní.

Nový variant vírusu

Výskumníci spoločnosti ESET odhalili aktuálne prebiehajúcu špionážnu kampaň, ktorá využíva doposiaľ nezdokumentovaný variant trojanu Korplug z dielne APT skupiny Mustang Panda. ESET pomenoval tento nový variant Hodur pre jeho podobnosť s variantom THOR, ktorý bol objavený v roku 2020. V nórskej mytológii je Hodur slepý nevlastný brat boha Thora. Kampaň zneužíva vojnu na Ukrajine aj ďalšie témy, ktoré rezonujú v Európe.

Medzi známymi obeťami sú výskumné organizácie, poskytovatelia internetových služieb a európske diplomatické misie, ktoré sa nachádzajú najmä vo východnej a juhovýchodnej Ázii. Útočníci pravdepodobne lákajú obete prostredníctvom phishingových dokumentov, ktoré odkazujú na najnovšie udalosti v Európe vrátane ruskej invázie na Ukrajinu. Pred vojnou utiekli do okolitých krajín podľa Úradu vysokého komisára OSN pre utečencov už viac ako tri milióny ľudí, čo spôsobilo na ukrajinských hraniciach bezprecedentnú krízu. Jeden zo súborov, ktorý je súčasťou špionážnej kampane, má napríklad názov „Situácia na hraniciach Európskej únie s Ukrajinou“.

> Každá fáza inštalácie škodlivého kódu využíva rôzne techniky na sťaženie analýzy programu.
>
> **Alexandre Côté Cyr,** výskumník spoločnosti ESET

Ohrozená je najmä Ázia

Výskumníkom spoločnosti ESET sa nepodarilo určiť všetky obete, no táto kampaň má pravdepodobne rovnaké ciele ako predchádzajúce kampane skupiny Mustang Panda. Tak ako aj v iných prípadoch, obete tejto kampane sa nachádzajú najmä vo východnej a juhovýchodnej Ázii a v niekoľkých európskych a afrických krajinách. Podľa telemetrie spoločnosti ESET sa väčšina cieľov nachádza v Mongolsku a vo Vietname, po ktorých nasleduje Mjanmarsko. V ostatných krajinách – v Grécku, na Cypre, v Rusku, v Južnom Sudáne a v Juhoafrickej republike sa nachádza iba niekoľko obetí. Medzi identifikovanými zasiahnutými cieľmi sú diplomatické misie, výskumné organizácie a poskytovatelia internetových služieb. Skupina Mustang Panda vo svojich kampaniach často používa vlastné loadre pre verejne dostupné malvéry vrátane Cobalt Strike, Poison Ivy a Korplu, tiež známy ako PlugX. APT skupina je tiež známa pre vytváranie svojich vlastných Korplug variantov. „Na rozdiel od ostatných kampaní, ktoré využívajú Korplug, v tomto prípade každá fáza inštalácie škodlivého kódu využíva rôzne techniky na sťaženie analýzy programu, vrátane skomplikovania toku jeho riadenia. Útočníci nám tak chcú sťažiť prácu,“ dodal Alexandre Côté Cyr, výskumník spoločnosti ESET, ktorý objavil malvér Hodur.

NOVELA

Blokovanie webov sa má predĺžiť do septembra

Bratislava – Možnosť blokovania škodlivých webov by sa mohla predĺžiť do 30. septembra. Predpokladá to návrh novely zákona o kybernetickej bezpečnosti, ktorý predložili poslanci Národnej rady Slovenskej republiky z OĽaNO, SaS a Za ľudí. Inštitút blokovania zatiaľ platí do konca júna. Využíva ho Národný bezpečnostný úrad na zamedzenie šírenia škodlivého obsahu na internete. Parlament ho zaviedol v rámci balíka opatrení súvisiacich so situáciou na Ukrajine. „V dôsledku pokračujúceho konfliktu je potrebné časové obdobie, počas ktorého je Národný bezpečnostný úrad oprávnený využívať svoju právomoc, predĺžiť,“ vysvetlili návrh predkladatelia. Na Slovensku sa podľa nich rozmohlo šírenie dezinformácií a podvodných statusov, ktorých cieľom je zahmlievať a spochybňovať realitu, ovplyvňovať verejnú mienku a nahrávať ruskej propagande pri informovaní o vojne na Ukrajine. Novela má byť účinná od prvého júla. Národný bezpečnostný úrad už zablokoval do 30. júna weby Hlavné správy, Armádny magazín, Hlavný denník a Infovojna. Na stránke identifikovali škodlivú aktivitu podľa zákona o kybernetickej bezpečnosti. Za škodlivý obsah sa považuje programový prostriedok alebo údaj, ktorý zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident. Zákon hovorí, že škodlivou aktivitou sa rozumie akákoľvek činnosť, ktorá zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident, podvodnú činnosť, odcudzenie osobných údajov, závažné dezinformácie a iné formy hybridných hrozieb. (TASR)

BEZPEČNOSŤ

Hrozby sú väčšie ako celková pripravenosť

Luxemburg – Úroveň kybernetickej pripravenosti sa v jednotlivých orgánoch Európskej únie líši a celkovo nezodpovedá silnejúcim hrozbám. Keďže orgány Európskej únie sú úzko prepojené, slabé miesto v jednom z nich môže vystaviť bezpečnostným hrozbám aj ostatné. Vyplýva to z osobitnej správy, ktorú v utorok zverejnil Európsky dvor audítorov so sídlom v Luxemburgu.

Podľa správy EDA sa počet závažných incidentov v oblasti kybernetickej bezpečnosti v orgánoch Európskej únie v rokoch 2018 až 2021 zvýšil viac než desaťnásobne.

Práca na diaľku výrazne zvýšila počet potenciálnych prístupových miest pre útočníkov, uvádza sa v správe. Hlavným zistením audítorov bolo, že inštitúcie, orgány a agentúry Európskej únie nie sú vždy dobre chránené pred kybernetickými hrozbami. Upozornili, že ku kybernetickej bezpečnosti nepristupujú jednotne, nemajú vždy zavedené základné kontroly a kľúčové osvedčené postupy týkajúce sa kybernetickej bezpečnosti, pričom poskytovaná odborná príprava v tejto oblasti nie je ani zďaleka systematická.

2021
BOL ROKOM
keď sa počet incidentov zvýšil viac než desaťnásobne.

„Inštitúcie, orgány a agentúry Európskej únie sú lákavým terčom pre potenciálnych útočníkov, najmä pre skupiny, ktoré sú schopné uskutočniť veľmi sofistikované utajené útoky s cieľom kybernetickej špionáže či na iné účely,“ uviedla Bettina Jakobsenová, členka EDA zodpovedná za túto správu. (TASR)

TECHNOLÓGIE

Bezpečnosť Slovenska rastie spoločnou silou

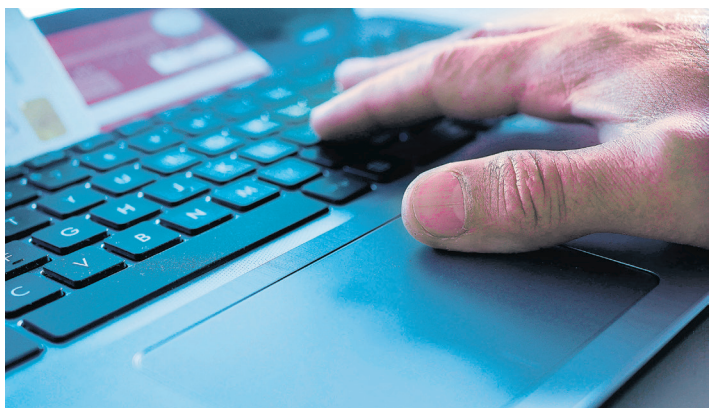
Bratislava – Národný bezpečnostný úrad podpísal memorandum o spolupráci s viacerými špičkovými IT firmami na Slovensku. Národný bezpečnostný úrad má ako garant kybernetickej bezpečnosti vo svojich dlhodobých úlohách aj rozvoj vzťahov so súkromným sektorom v tejto v oblasti. Zámer momentálne urýchlila a zintenzívnila bezpečnostná situácia na Ukrajine a neutíchajúce hrozby v kybernetickom priestore, ktoré sa už roky nevyhýbajú ani Slovensku. Aj Európska únia momentálne volá po koordinovanom postupe so zapojením všetkých možných prostriedkov vrátane komerčných subjektov a po efektívnejšej komunikácii či výmene informácií na úrovni členských štátov.

Zástupcovia desiatky popredných spoločností a organizácií podpísali memorandum s cieľom efektívnejšie plniť úlohy v zmysle zákona o kybernetickej bezpečnosti – ESET, Aliter Technologies, Disig, Lynx, Axenta, EMM, GAMO, Gordias, ALISON Slovakia a Združenie bezpečnostného a obranného priemyslu. „Oceňujem rýchlu reakciu jednotlivých spoločností a ich neutíchajúci záujem prispieť svojím dielom k spoločnej bezpečnosti. Obdobné spolupráce nie sú ani v zahraničí výnimočným javom. Vzájomná výmena skúseností, poznatkov a odborných postrehov môže byť na konci dňa rozhodujúcim prvkom v bezpečnosti štátu, organizácií a občanov,“ povedal na margo podpísaných dokumentov riaditeľ Národného bezpečnostného úradu Roman Konečný. Národný bezpečnostný úrad bude s firmami spolupracovať individuálne podľa ich zamerania či personálnych a technických kapacít pri riešení kybernetických bezpečnostných incidentov. Nebudú chýbať vzájomné odborné konzultácie, výmena informácií o zraniteľnostiach v informačných systémoch či forenzná analýza. (TASR)

HROZBY

Iba pätnásť percent Slovákov sa orientuje v kybernetickej bezpečnosti

Bratislava – Bezpečnosť na internete sa aj napriek častým útokom hackerov stále podceňuje. Podľa odborníka sa dá zvýšiť úroveň zabezpečenia pár jednoduchými krokmi, základom je mať silné heslo, používať antivírusový program a pravidelne aktualizovať systém. S útokom hackerov sa stretol už každý piaty Slovák, ľudia však stále podceňujú dôležitosť adekvátneho zabezpečenia svojich zariadení. Podľa prieskumu verejnej mienky, ktorý si dala spracovať spoločnosť Aliter Technologies, sa iba 15 percent Slovákov dostatočne orientuje v kybernetickej bezpečnosti. „Technológie sú každodennou súčasťou našich životov, treba však pri tom myslieť aj na bezpečnosť, ktorá je stále podceňovaná. Používanie inteligentných telefónov, hodiniek či bežných počítačov so sebou prináša aj riziká,“ uviedol Daniel Suchý, odborník na kyberbezpečnosť spoločnosti Aliter Technologies. Práve slabé zabezpečenie zariadení uľahčuje hackerom ich útoky.



Slabé zabezpečenie zariadení uľahčuje hackerom ich útoky.

ILUSTRAČNÁ SNÍMKA: DREAMSTIME

„V bežnej internetovej populácii si 43 percent ľudí nezvykne meniť heslo vôbec alebo len vtedy, keď ho zabudne. Problémom býva aj pohodlnosť ľudí, ktorí heslá recyklujú, teda používajú rovnaké heslo na viac účtov. Ak takéto heslo získa útočník, ohrozené sú viaceré účty či aplikácie, ktoré človek používa,“ vysvetľuje Daniel Suchý. Podľa odborníka je dnes kybernetická bezpečnosť aktuálna viac než kedykoľvek predtým. Na to, aby sme ochránili naše dáta a súkromie, sa treba riadiť jednoduchými tipmi. „Odporúčam vždy používať jedinečné heslo, ideálne zložené aspoň zo 14 malých a veľkých písmen, čísel a znakov plus ďalší faktor, ktorý chráni váš účet aj v prípade kompromitácie hesla. Pamätať si ich nemusíme, využiť môžeme správcu hesiel. Dôležité je tiež pravidelne zálohovať dáta, aktualizovať systém či používať antivírusový program.“ Ako dodáva Daniel Suchý, na to, aby mali ľudia dostatočne zabezpečené zariadenia, nemusia byť odborníkmi na IT. Zdôrazňuje tiež potrebu osvety či edukácie. „O bezpečnosti na internete treba hovoriť aj v rodinách, napríklad s deťmi, ktoré trávia voľný čas online, či so starými rodičmi, ktorí sú zraniteľnou skupinou a mohli by naletieť podvodníkom na internete.“ Ľudia by mali byť tiež obozretní aj pri registrácii do nových služieb, odhaliť nižšiu mieru zabezpečenia pomôže aj tento trik. „Zakaždým, keď sa registrujete do nejakej služby a potvrdzujúci email obsahuje vaše heslo v znení, v akom ste ho zadali, okamžite meňte heslo vo všetkých službách, kde ho recyklujete,“ uzatvára odborník na kyberbezpečnosť. (RED)