ALISON

Keď nájdete výhražný mail: Platiť či neplatiť?

Útok, vyjednávanie a platba. Alebo aj nie. Čo mesiac, to rekord v ransomvérových útokoch. Za scénou sa toho však deje omnoho viac.

Ups, dáta sú zašifrované

Obete útokov si nachádzajú rôzne výhražné správy. Niektoré agresívne, iné nedôstojné alebo falošne ospravedlňujúce. Stretnúť sa môžete naozaj s kadečím – *„Ľutujeme, vaše súbory sú šifrované. Nie sme blázni, my vieme o vás viac ako vy o sebe“*.

V iných správach sa môžete dočítať, ako je vaše podnikanie a dobré meno v ohrození a je načase konať.

Správy zvyčajne odkazujú na darkweb. Prístup si vyžaduje špeciálny softvér a obeť sa tam len tak ľahko nedostane. Útočník tam má pre svoju obeť pripravené hodiny odpočítavajúce čas do zaplatenia výkupného. Obeť sa musí rozhodovať rýchlo.

Čísla rastú, ale aj akcie, ktoré nasledujú „po“

Rekord pre platbu výkupného si stále drží podľa oficiálnych štatistík cestovná agentúra CWT Global. V júli minulého roka zaplatila 5,4 milióna amerických dolárov v bitcoinoch. Dvojka v rebríčku je tohoročné výkupné, 4,4 milióna amerických dolárov, ktoré zaplatil Colonial Pipeline. Stalo sa však osudným pre gang DarSide, ktoré po odvetnom útoku vládnej agentúry musel ukončiť aktivity.

Akonáhle sa spoločnosti ocitnú v situácii, keď prichádzajú o milióny dolárov denne, výkupné za „niekoľko“ miliónov dolárov sa stáva obchodným rozhodnutím. Najmä ak časť škôd pokryje poistenie proti kybernetickým útokom.

Miesto na trhu si našli aj poradenské firmy, ktorá pomáhajú vyjednávať s kybernetickými zločincami a sprostredkovať vyplatenie výkupného. Do centra pozornosti sa dostali títo vyjednávači práve v ostatných mesiacoch a tímy sú tvorené často veteránmi vládnych bezpečnostných agentúr. Presne tými, ktoré varovali pred platením výkupného. O kybernetických gangoch hovoria ako o sofistikovaných organizovaných štruktúrach, ktoré stoja na špičke zločineckej hierarchie.

Obete sú zúfalé a ochotné robiť zúfalé činy

Obete ransomvéru vo väčšine prípadov netušia, s kým je zločinecká skupina spojená. A už vôbec nevedia, kam smeruje platba výkupného. Podľa odborníkov z FBI je zrejmé, že tieto skupiny často priamo alebo nepriamo spolupracujú s nepriateľskými vládami, či globálnymi protivníkmi USA.

Platenie výkupného je spojené s ďalšími rizikami. Medzi tie najväčšie patrí neúmyselné vyplatenie miliónov v bitcoinoch aktérom vedeným na sankčných zoznamoch, kam patria napríklad Severná Kórea alebo Irán. Konzultačné spoločnosti pomáhajúce obetiam kybernetických útokov tvrdia, že toto riziko je možné zmierniť. Stačí vykonať viacero kontrol a sledovať, kam platby smerujú. Aspoň to tak tvrdia.

A čo robia napadnuté štáty?

Vlády jednotlivých štátov kategoricky odmietajú vyplácanie výkupného. Tvrdia, že platenie výkupného neochráni siete pred skrytou infiltráciou ani nezabráni budúcim únikom údajov. Zaplatenie s najväčšou pravdepodobnosťou podporí kriminalitu a jej ďalší rozmach. Rovnaké stanovisko majú aj spoločnosti venujúce sa kybernetickej bezpečnosti.

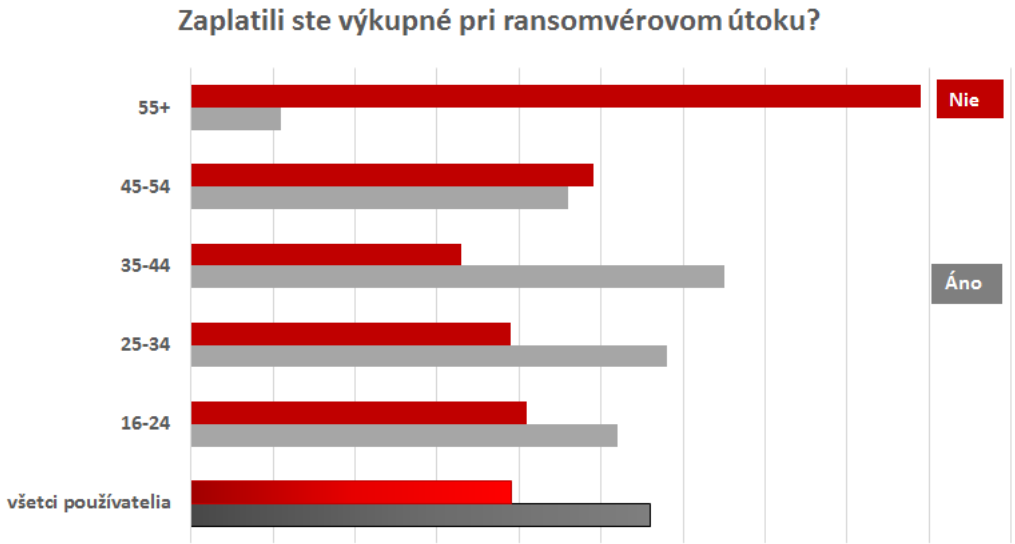
Zaplatenie výkupného nezaručuje ani jednotlivcom ani organizáciám vrátenie akýchkoľvek údajov. A dokonca to motivuje páchateľov, aby útočili na čoraz väčšie množstvo cieľov.

A čo jednotlivec na bojovom poli?

Podľa globálnej štúdie s 15-tisíc spotrebiteľmi, ktorú realizovala spoločnosť Kaspersky, viac ako polovica obetí ransomvéru zaplatila výkupné za obnovenie prístupu k svojim údajom. Konkrétne – v roku 2020 zaplatilo výkupné 56 percent obetí.

Čísla ukazujú, že **mladší používatelia s väčšou pravdepodobnosťou zaplatia výkupné**.

Vo veku 35 - 44 rokov zaplatilo výkupné až 65 percent obetí, osoby staršie ako 55 rokov platili iba v 11 percentách prípadov.



	všetci používatelia	16-24	25-34	35-44	45-54	55+
nie	39,0%	41,0%	39,0%	33,0%	49,0%	89,0%
áno	56,0%	52,0%	58,0%	65,0%	46,0%	11,0%

Zdroj: Global Study, Kaspersky 2021

ALISON

Straty po útoku

Či už sa rozhodli zaplatiť výkupné, alebo neplatiť, iba 29 percent používateľov dokázalo obnoviť šifrované alebo blokované súbory. Polovica napadnutých uviedla, že stratili časť súborov. A 13 percent obetí incidentu prišlo o takmer všetky súbory.

The 5 biggest ransomware pay-outs of all time

Over half of ransomware victims pay the ransom, but only a quarter see their full data returned

$12 Billion Government Contractor Booz Allen Facilitates Ransomware Payments—Even Though The FBI Says Never Pay

Ransomware: Don't pay up, it just shows cyber criminals that attacks work, warns home secretary