MŮJ KÁMOŠ HACKER

ROBERT SATTLER

RANSOMWARE. Slovo, s nímž se dostatečně seznámili už i neznalí v digitálním světě. Tento vyděračský software v nedávné době vyřadil z provozu dvě české nemocnice, OKD, ale také školy a úřady či velké globální firmy. Jak konkrétně to ale vypadá za oponou těchto útoků, když se poškození rozhodnou přistoupit na špinavou hru hackerů?

Dejme teď stranou, že výkupné kyberzločincům by žádná instituce hradit neměla, neboť tím podporuje kriminální byznys. Vedle této skutečnosti totiž existuje ještě jedna: firmy hackerům stejně platí. A platí hodně. Proč? Mnohdy proto, že jde o výhodnější variantu. „Je to, jako když vám unesou rodiče a hrozí, že když nezaplatíte, zabijí je. Jde o vaši firmu a ona může skončit. Těžce se v takové chvíli říká: Dodržujme pravidla," tvrdí Martin Haller, expert na IT bezpečnost. Právě on na svých stránkách nedávno uveřejnil zprostředkovanou konverzaci, která dává nahlédnout, jak vyjednávání mezi obětí a útočníky probíhá (viz grafika).

„Pokud se společnost ocitne v situaci, kdy má kritická data zašifrovaná a nemá zálohy, z nichž by je mohla obnovit, musí zaplatit," přibližuje.

K platbě výkupného se ale prý uchylují i silné firmy, jež data zálohovaná mají, jenže jejich několikadenní obnova (den nečinnosti něco stojí) by byla nákladnější než okamžitá úhrada a nastartování systému. Často přitom společnosti neplatí původní částku, ale podaří se jim vyjednat slevu. Útočníci takový scénář očekávají a s ochotou na něj přistupují. Jak ostatně ukazuje i zmíněná konverzace. Každá koruna se počítá.

OBĚŤ (1. 2. 2020 20:32):
Zdravím, dobrá práce! Jmenuji se XXX. Byl jsem požádán, abych se podíval na bezpečnost sítě jednoho našeho zákazníka, kterého jste hackli. Navrhl jsem mu zaplatit, jestli bude částka dávat smysl a ušetří to čas. Jaká je vaše cena?

HACKEŘI (1. 2. 2020 23:18)
Dva bitcoiny za dekryptor.

OBĚŤ (2. 2. 2020 0:02)
Náš zákazník je hodně malý, může vám dát akorát 500 eur. Zase tolik ta data nepotřebuje, má poměrně čerstvé zálohy.

HACKEŘI (2. 2. 2020 0:06)
Jen naše snídaně stojí každý den 1000–1500 eur. Už nám sem znovu nepiš.

OBĚŤ (2. 2. 2020 0:18)
Jsme z Česka, lidé si tu za 1500 eur kupují auto :-(1000 eur? Snažím se vám pomoct, abyste dostali alespoň něco, když už jste si s tím hackováním dali práci.

OBĚŤ (2. 2. 2020 13:41)
Zdravím, jestli data odšifrujete dneska, může vám dát 0,5 bitcoinu. Poslední nabídka, nebo spustí obnovu z 10 dní staré zálohy a budou pracovat dál, jako by se nic nestalo. Jestli chcete peníze, dejte vědět rychle.

HACKEŘI (2. 2. 2020 13:51)
Dobře, 0,5 bitcoinu, dohodnuto. Náš účet: XXX. Kolik potřebuješ času na platbu?

OBĚŤ (2. 2. 2020 20:11)
Bohužel, dohoda padla. Peníze v bitcoinech máme, ale zákazník se rozhodl raději pro zálohu, vyhodnotil si to jako levnější variantu.

HACKEŘI (2. 2. 2020 20:13)
Nabídni mu slevu, očekáváme 0,3 bitcoinu.

OBĚŤ (2. 2. 2020 20:27)
Abych byl upřímný, zaplatil by, ale chce mít stoprocentní jistotu, že data pak dostane.

HACKEŘI (2. 2. 2020 23:03)
Člověče, co od nás chceš? Poslali jsme ti příklady odemknutých souborů jako záruku, a furt ti to není dost. Odmítl jsi dohodu. Zítra klíč k datům smažeme.

OBĚŤ (2. 2. 2020 23:14)
Jenom se snažím vydělat vám nějaké peníze. Zákazník odmítl zaplatit, protože nevěří, že k odemknutí dojde. Takže chci gentlemanské slovo, že data odemknete, pokud pošlu 0,3 bitcoinu.

HACKEŘI (2. 2. 2020 23:23)
Částka je 0,5 bitcoinu. Nebudeme dávat žádnou slevu. Zaplať a dostaneš dekodér, nebo nám dál nepiš.

OBĚŤ (3. 2. 2020 0:00)
Zákazník zvažoval 0,5 bitcoinu, ale pak se rozhodl odmítnout a požádal mě o obnovu dat ze záloh. Prosím, vezměte si 0,3 bitcoinu a můžeme jít všichni spát.

HACKEŘI (3. 2. 2020 0:10)
Už jsme z tebe unavení. Dali jsme ti skvělou cenu, co zas ku*va smlouváš? 0,4 bitcoinu – poslední nabídka. Máš pět minut na platbu.

TERČ: KORPORACE

Vyjednávání s hackery připomíná turecký bazar. Je to psychologická hra, říká v rozhovoru etický hacker Martin Haller.

MARTIN HALLER

Třiatřicetiletý etický hacker, spoluzakladatel firmy Patron-IT, zabývající se kyberbezpečností. Správě počítačových sítí se věnuje od studií. Specializuje se na malé a střední firmy.

TAKTO, JAK VIDÍME V GRAFICE, VYPADÁ STANDARDNÍ KOMUNIKACE S ÚTOČNÍKY?

Ano, to je typické. Jako napadený vždy víte, že chcete slevu, nikdy nechcete zaplatit první požadovanou částku. Tedy pokud ji útočníci špatně nenastřelí. Uvedu příklad: zašifrují firmu, která každý den nečinnosti přijde o tři miliony korun, ale oni si řeknou za odemčení o 300 tisíc. Co upřednostníte? Vyjednávání totiž také zabere nějaký čas, nemůžete tlačit na pilu. Musíte ukázat, že o nic nejde a den to počká. Je to psychologická hra, která připomíná turecký bazar. Výkupné se dá časem snížit a vy hledáte bod, kdy se to vyplatí.

KDE MÁM ALE JISTOTU, ŽE DATA PO ZAPLACENÍ DOSTANU ZPĚT?

Pro útočníky je důležité, abyste je dostal. Jejich byznys totiž bude fungovat jen tak dlouho, dokud se bude vědět, že když zaplatíte, dostanete dešifrovací klíč. Kdyby někdo začal říkat, že zaplatil, a data nedostal, další firmy nebudou chtít platit. Další příklad, o kterém vím. Jeden člověk útočníkům napsal, že pokud mu klíč nepošlou, bude na fórech psát, že zaplatil, a nedostal nic. Víte, co se stalo? Oni mu ho dali zadarmo. Jen aby to nezačal šířit.

NAVZDORY TOMU, ŽE NA VÝKUPNÉ ÚTOČNÍKŮM BY FIRMY PŘISTOUPIT NEMĚLY, JAK ČASTO SE TAK DĚJE?

U soukromých firem je to zcela běžné, ty se snaží situaci řešit potichu. Občas ale platí i samosprávy nebo univerzity, jako třeba v USA nebo Nizozemsku. Ukázkovým příkladem první skupiny je nedávný incident Garminu. Jeho zástupci neřekli, že je napadl ransomware, mluvili o technických obtížích. Že to byl ransomware, uteklo až později, ale oni už to dávno museli vědět. Systémy Garminu se zastavily ve středu večer a už o den a půl později měla firma k dispozici dekryptor, klíč. Není na to důkaz, ale spekuluje se, že zaplatila, jak jinak by ho totiž dostala.

STEJNĚ TAK SE TUTLAJÍ INFORMACE OHLEDNĚ ÚNIKŮ OSOBNÍCH DAT?

Dříve se tvrdilo, že ransomware data jen šifruje, ale ukazuje se, že si umí také část dat zkopírovat a vydírat napadeného i jejich možným zveřejněním. Je to dobrý trik, který útočníky stojí dva kliky navíc, jenže firmy to samozřejmě nikdy nepřiznají. Nejspíš znáte ten scénář. Nějakou náhodou nám někdo kompromitoval síť, my si toho nevšimli. Byl tam několik týdnů, my si toho nevšimli. Pak nám prolomil servery, my si toho nevšimli. Následně nám zašifroval síť a my si toho všimli nad ránem, když nám nešly počítače. Takže teď máme vše naprosto pod kontrolou a žádná data nám neunikla. To má logiku, ne? Ale co jiného mají říct.

JSOU ÚTOČNÍCI NAPŘED?

Máme lepší obránce, než jsou útočníci. Problém je v tom, že jich není tolik jako firem. Dobrých lidí v IT bezpečnosti je málo a jsou přetížení. Řada firem se tak nebrání, jak by měly, a právě na ně útočníci útočí, protože ty dobře zabezpečené pochopitelně přeskočí.

MĚNÍ SE VÝRAZNĚ POČÍNÁNÍ ÚTOČNÍKŮ?

Hackeři jsou čím dál tím lepší. Začali cílit na nadnárodní korporace, z nichž tahají velké peníze. Zatímco loni touto dobou se průměrná výše výkupného pohybovala kolem 50 tisíc dolarů, teď se blíží čtyřnásobku. Takhle rychle nerostou ani akciové indexy. A firmy o tom vědí. Dokonce jsem četl, že šéfové velkých IT korporací mají nakoupené kryptoměny, kdyby se něco stalo. Přece jen když máte zaplatit miliony dolarů v bitcoinech, neseženete je hned.

POJISTKA PRO STRÝČKA PŘÍHODU?

Tím, že je v korporacích spousta zaměstnanců, je velká pravděpodobnost, že se udělá chyba. Nedávný ransomwarový případ navíc ukázal na jednu zajímavost. Američané tehdy zadrželi Rusa a obvinili jej z uplácení zaměstnance Tesly. Měl mu nabídnout milion dolarů, pokud nainstaluje virus do její sítě a dobře to dopadne. Rus se pak přiznal, že už takto postupovali u dalších firem. Je tak možné, že se zpětně dozvíme, že řada v poslední době napadených společností, jako je Garmin nebo LG Electronics, byla napadena touhle cestou. V tomhle byznysu je hodně peněz, tudíž lze čekat, že se nezastaví. Ale tohle je novinka. Pokud útočníci budou jezdit po světě a uplácet pracovníky, bude to zajímavá změna.