

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **14** ze dne **28.7.2022**

Útočníci přizpůsobili šíření spywaru letním dovoleným, útoky cílí také na Česko

V ČERVNU ZŮSTAL NEJVĚTŠÍ HROZBOU PRO OPERAČNÍ SYSTÉM WINDOWS V ČESKU SPYWARE AGENT TESLA. ŠKODLIVÉ KÓDY SE ŠÍŘÍ PROSTŘEDNICTVÍM FALEŠNÝCH FAKTUR NEBO POTVRZENÍ O REZERVACI POBYTŮ.

Kybernetické útoky

Nejčastěji detekovaným škodlivým kódem byl v červnu spyware Agent Tesla. Bezpečnostní analytici ho objevili téměř v pětině všech případů. Ačkoli v předešlých měsících obecně poklesl počet jeho detekcí, v České republice se objevuje dlouhodobě a stabilně. Největším rizikem je pro uživatelská hesla uložená v internetových prohlížečích nebo v účtech e-mailových klientů jako Microsoft Outlook, Mozilla Thunderbird nebo Yandex.

„V červnu neměl spyware Agent Tesla v Česku žádnou větší kampaň. Aktuálně ke svému šíření využívá škodlivé e-mailové přílohy s názvy 1224736#.exe nebo Inquiries.exe. Nejčastěji se můžeme setkat právě s e-maily, které obsahují přílohy odkazující na nějakou fakturu,“ říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET.

Útoky nejsou začátkem léta velké, ale přesně cílené

Ačkoli spyware v Česku v posledních měsících neútočil v žádné masivní kampani, rizikem zůstává i nadále. Kybernetičtí útočníci své strategie neustále proměňují na základě trendů a chování uživatelů.

„V případě spywaru Formbook jsme v červnu detekovali e-maily se škodlivými přílohami, které měly podobu potvrzení k rezervaci pobytu. Jasně tak vidíme, jak útočníci zneužívají hlavní sezónu dovolených, navíc první relativně standardní sezónu od vypuknutí pandemie. Největší útočnou kampaň jsme u Formbooku sledovali 6. června. Nejčastější škodlivá příloha měla název PO_87910219.exe,“ říká Jirkal.

V případě třetího nejčastěji detekovaného malwaru, password stealeru Fareit, objevili specialisté pokusy o cílené útoky v češtině.

„Password stealer Fareit se zhruba pěti procenty všech detekcí je ukázkovým příkladem současného trendu menších, ale přitom cílených útoků. Zatímco kampaně v případě spywaru Agent Tesla nebo spywaru Formbook se objevují především v angličtině, menší útočné kampaně malwaru Fareit se již cíleně zaměřují na Česko,“ vysvětluje Jirkal a dodává: *„V datech jsme tak objevili například české verze škodlivých příloh s názvy Cenová poptávka 2019 nebo Potvrzení platební faktury_INV_604-0335.“*

Kyberútočníci očekávají, že nebudeme věnovat pozornost zabezpečení

Období letních prázdnin a dovolených je každoročně více rizikové, stejně jako například období před vánočními svátky. Jako uživatelé trávíme více času na svých zařízeních. Nemusíme přitom věnovat takovou pozornost zabezpečení a pravděpodobnost, že nechtěně otevřeme nebo spustíme nebezpečnou přílohu v neznámém e-mailu, je tak vyšší.

Spyware je přitom druh malwaru, který se zaměřuje na jeden z nejdůležitějších ochranných prvků v online prostředí, a to na naše hesla. *„Dostatečně silné a složité heslo je stále jedním z nejspolehlivějších*

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **14** ze dne **28.7.2022**

bezpečnostních opatření, které máme k dispozici. Útočníci to samozřejmě vědí, a proto jsou uživatelská hesla tak cennou kořistí. Odcizené údaje mohou útočníci využívat k dalším útokům nebo je prodávat rozličným zájemcům na černém trhu,” vysvětluje Jirkal.

Odborníci tak i během dovolené a cestování doporučují nepodceňovat základní bezpečnostní pravidla. Na prvním místě bychom měli věnovat pozornost tvorbě silných hesel a jejich bezpečné správě.

„Heslo je klíčem k celé řadě našich online účtů, nejen v bankách, ale také na sociálních sítích a v e shopech. Ke každé takové službě bychom měli mít unikátní heslo, které bude složeno minimálně z deseti znaků, a to z číslic, písmen a případně i speciálních znaků, pokud to služba umožňuje. Hesla bychom také neměli nikam zapisovat a rozhodně je nedoporučujeme ukládat do internetových prohlížečů, které nejsou před spywarem dostatečně chráněné. Vhodnou alternativou jsou naopak správci hesel, programy, které uloží všechna vaše hesla v zašifrované podobě a vy si pak pamatujete pouze jedno heslo k přístupu do této služby,” shrnuje Jirkal z ESETu.

Zařízení s operačním systémem Windows nezapomeňte dále pravidelně aktualizovat. Celkovou úroveň zabezpečení zvýší také kvalitní bezpečnostní software, který současné hrozby včas rozpozná.

Nejčastější kybernetické hrozby pro operační systém Windows v České republice za červen 2022:

1. MSIL/Spy.AgentTesla trojan (19,13 %)
2. Win32/Formbook trojan (11,53 %)
3. Win32/PSW.Fareit trojan (5,34 %)
4. MSIL/Spy.Agent.AES trojan (4,16 %)
5. Win32/Spy.Weecnaw trojan, (3,76 %)
6. MSIL/Spy.Agent.DFY trojan (1,46 %)
7. Win32/Agent.TJS trojan (1,38 %)
8. Java/Adwind trojan (1,21 %)
9. MSIL/Agent.CFQ trojan (1,08 %)
10. BAT/CoinMiner.AUB trojan (1,01 %)

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

Zdroj: AVcentrum ČR