

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **20** ze dne **19.10.2022**

Počet útoků na uživatelská hesla v září opět vzrostl

Počet detekcí spywaru Agent Tesla i spywaru Formbook v září vzrostl a u obou škodlivých kódů se objevovaly útočné kampaně namířené na české uživatele. Ačkoli mají oba škodlivé kódy především celosvětový dosah, bezpečnostní experti zachytili v září vysoký výskyt českých verzí nebezpečných e-mailových příloh, jejichž prostřednictvím se šíří. Mezi nejčastěji detekovanými škodlivými kódy pro operační systém Windows v Česku se tentokrát objevil spyware Weecnaw, který se také zaměřuje na odcizení přihlašovacích údajů k našim online účtům. Vyplývá to z pravidelné statistiky společnosti ESET.

I přestože je spyware Agent Tesla škodlivým kódem s celosvětovým dosahem a na Českou republiku se cíleně příliš nezaměřuje, ve 14 procentech všech svých útoků se v září objevil právě v Česku. Bezpečnostní specialisté upozorňují, že s ohledem na jeho globální působnost jde o poměrně významné procento výskytů.

„Motivem k provedení kybernetického útoku bývá pro útočníky především co největší finanční zisk, proto se můžeme setkat spíše s celosvětovými útoky než s těmi konkrétně cílenými pouze na jednu zemi. Aktivita spywaru Agent Tesla v Česku tak byla v září poměrně překvapivá,“ říká Martin Jirkal, vedoucí analytického týmu v pražské pobočce společnosti ESET. *„Ve třech čtvrtinách případů se mohli uživatelé v září setkat s nebezpečnou e-mailovou přílohou s českým názvem Zpusob_platby.jpg.exe. Nejsilnější útok proběhl 20. září,“* dodává Jirkal.

Kybernetičtí útočníci využívají k šíření spywaru především e-mailové přílohy, které svým názvem nejčastěji odkazují na faktury nebo objednávky. Přílohy mají také ve většině případů příponu .exe označující spustitelný soubor. Česky označené přílohy se přitom objevovaly v posledních měsících především u password stealeru Fareit a u spywaru Agent Tesla byly spíše výjimkou. Statistika ze září tak ukazuje, že útočníci aktuálně pozměnili své strategie.

V září doplnil škodlivé kódy spyware Weecnaw

V září se zvýšil počet detekcí také u spywaru Formbook a také v jeho případě se objevovala česky pojmenovaná příloha.

„Spyware Formbook byl aktivní především v první polovině měsíce, nejsilnější kampaň jsme zaznamenali 16. září. Útočníci ho v Česku tentokrát šířili prostřednictvím přílohy Nová objednávka pdf xxxLhHM.exe,“ říká Jirkal.

Na přední místa pravidelné měsíční statistiky se v září dále vyšplhal spyware Weecnaw. V Česku se neobjevil poprvé, doposud však nebyl detekován ve větším počtu případů.

„Spyware Weecnaw útočil jednorázově 5. a 6. září. V tuto chvíli ještě nedokážeme říct, zda se jednalo pouze o ojedinělý případ, nebo jde o první, testovací útok a my se s tímto škodlivým kódem budeme v Česku potkávat častěji,“ vysvětluje Jirkal.

Útočníci využili k šíření malwaru Weecnaw přílohu s názvem „Purchase Order No. PO2732559-022.pdf (742 KB).exe“. Pokud Weecnaw infikuje zařízení, dokáže odcizit uložená uživatelská jména a hesla k aplikacím a službám nebo další údaje o zařízení.

Věnujte pozornost e-mailům od neznámých odesílatelů

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **20** ze dne **19.10.2022**

Bezpečnostní experti uživatelům doporučují, aby rizika v podobě spywaru nepodceňovali a používali na svých zařízeních s operačním systémem Windows kvalitní bezpečnostní software. Celkové zabezpečení svých osobních údajů však mohou posílit také svou obezřetností.

“Uživatele se snažíme pravidelně varovat před otevíráním příloh z e-mailů, jejichž odesílatele neznají. Pokud jim přijde zpráva z e-mailové adresy, kterou nemají ve svých kontaktech, nebo se tato zpráva tváří jako komunikace od různých institucí, přepravních firem nebo dodavatelů energií, určitě bych jim doporučil si takový e-mail nejdříve ověřit na oficiálních stránkách nebo zákaznické podpoře,” říká Jirkal z ESETu.

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

- MSIL/Spy.AgentTesla trojan (23,25 %)
- Win32/Formbook trojan (17,48 %)
- Win32/Spy.Weecnaw trojan (10,95 %)
- MSIL/Spy.Agent.AES trojan (3,51 %)
- Win32/PSW.Fareit trojan (3,36 %)
- VBS/Agent.QHU trojan (0,95 %)
- Win32/Delf.NBX virus (0,95 %)
- MSIL/Spy.Agent.DFY trojan (0,94 %)
- MSIL/Agent.UDJ trojan (0,81 %)
- Java/Adwind trojan (0,78 %)

Uživatelé produktů ESET jsou před těmito hrozbami chráněni.

Zdroj: ESET