

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **24** ze dne **20.12.2022**

Viry se teď nejčastěji schovávají v archivních souborech ZIP a RAR

Společnost HP vydala zprávu, na základě analýzy skutečných kybernetických útoků za třetí čtvrtletí tohoto roku. Podle ní jsou aktuálně nejčastějším typem souborů zneužívaným k šíření malwaru archivační formáty. Jedná se tak například o soubory ZIP a RAR, které poprvé po několika letech předstihly soubory Office. Zpráva ukazuje, že kombinace archivních souborů a propašování škodlivého kódu do HTML souborů pomáhá útočníkům účinně obelstít detekční nástroje.

Na základě údajů z milionů koncových zařízení se systémem HP Wolf Security bylo zjištěno, že 44 % malwaru bylo skryto v doručených archivních souborech, což je o 11 % více než v předchozím čtvrtletí, zatímco 32 % se skrývalo v souborech Office, jako jsou Microsoft Word, Excel a PowerPoint.

Zpráva také informuje o několika útočných kampaních, kombinujících použití archivních souborů s novými technikami propašování škodlivého kódu do souborů HTML. Kyberzločinci vkládají škodlivé archivní soubory do souborů HTML, aby obešli e-mailové brány, a následně provedli útok.

Například nedávne útoky QakBot a IceID využívaly soubory HTML k přesměrování uživatelů na falešné online prohlížeče dokumentů, které se vydávaly za stránky provozované firmou Adobe. Uživatelé byli následně instruováni, aby otevřeli soubor ZIP a zadali heslo pro rozbalení souborů, které pak do jejich počítačů nasadily malware.

Díky tomu že je malware v původním souboru HTML zakódován a zašifrován, je jeho detekce e-mailovou bránou nebo jinými bezpečnostními nástroji velmi obtížná. Útočník se spoléhá na sociální inženýrství a vytvoří přesvědčivou a graficky dobře zpracovanou webovou stránku, jejímž cílem je oklamat uživatele a přimět ho ke spuštění útoku otevřením škodlivého souboru ZIP. V říjnu se zjistilo, že titíž útočníci použili podvržené stránky GoogleDisku – rovněž s cílem přimět uživatele k otevření infikovaných souborů ZIP.

„Archivy lze jednoduše šifrovat, takže do nich útočníci mohou skrýt malware, a obejít tak webové proxy servery, sandboxy nebo programy na kontrolu e-mailů. To znesnadňuje odhalení útoků, zejména pokud při nich útočník zároveň použije techniky propašování HTML kódu. Na kampaních QakBot a IceID bylo pozoruhodné, kolik úsilí útočníci věnovali vytvoření falešných stránek. Tyto kampaně působily věrohodněji než dřívější útoky, a pro uživatele proto nebylo snadné rozpoznat, kterým souborům mohou či nemohou věřit,“ vysvětluje Alex Holland ze společnosti HP Inc.

Společnost HP odhalila také detailně propracovanou kampaň využívající modulární řetězec infekce, který by útočníkům dovolil změnit typ útoku i v průběhu kampaně. Například využít k útoku spyware, ransomware či keylogger – případně zavést nové funkce, jako je geo-fencing. To by útočníkovi umožnilo měnit taktiku v závislosti na napadeném cíli. Vzhledem k tomu, že malware není obsažen přímo v příloze odeslané adresátovi, je pro e-mailové brány také obtížnější tento typ útoku rozkrýt.

„Jak se ukázalo, útočníci neustále mění techniky, takže je pro detekční nástroje velmi obtížné je odhalit,“ podotýká dr. Ian Pratt, globální ředitel pro zabezpečení osobních systémů společnosti HP Inc. *„Při použití mikrovirtualizace mohou organizace uplatněním principu nulové důvěry a detailně propracované izolace zajistit, aby se potenciálně škodlivé úlohy – jako jsou procesy iniciované kliknutím na odkaz nebo otevřením škodlivé přílohy – spouštěly v jednorázovém virtuálním počítači, odděleném od základních systémů. Tento proces je z hlediska uživatele zcela neviditelný a dokáže zachytit veškerý skrytý malware, proto útočníci*

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **24** ze dne **20.12.2022**

nemohou získat přístup k citlivým datům, a nemohou tedy do systému proniknout a dále pokračovat v útoku.“

Zdroj: hp