Kyberbezpečnostní experti z pražské pobočky ESET pomohli k narušení sítě útočníků v Brazílii

5.2.2024 - Rita Gabrielová, Lucie Mudráková | ESET software

Praha, 5. února 2024 – Společnost ESET, globální poskytovatel řešení v oblasti kybernetické bezpečnosti, pomohla ve spolupráci s brazilskou federální policií připravit akci k narušení botnetu Grandoreiro. Na přípravě této operace se významně podíleli kyberbezpečnostní experti z České republiky, konkrétně z pražské výzkumné pobočky. Společnost ESET přispěla k akci poskytnutím technické analýzy, statistických informací a známých doménových jmen a IP adres C&C serverů, jejichž prostřednictvím útočníci dokážou ovládnout napadené zařízení obětí a odcizit jejich finance. Akce byla zaměřena na osoby, které jsou pravděpodobně vysoko v operační hierarchii sítě Grandoreiro, a vedla k identifikaci pachatelů a jejich zatčení. Bankovní malware Grandoreiro je aktivní v Brazílii, Mexiku, Španělsku a Argentině. V České republice není tento malware detekován.

Společnost ESET ve spolupráci s brazilskou federální policií pomohla připravit akci k narušení botnetové sítě Grandoreiro. Bankovní malware Grandoreiro je aktivní minimálně od roku 2017 a útočníci se jeho prostřednictvím zaměřují především na Brazílii, Mexiko, Španělsko a od roku 2023 také na Argentinu. Podle bezpečnostních expertů v tuto chvíli nehrozí, že by se typ bankovního malwaru objevil také v České republice, protože banky, na které se škodlivý kód zaměřuje, zde nemají své pobočky. Na výzkumu a analýze této kybernetické hrozby se významně podílí především bezpečnostní experti z pražské výzkumné pobočky společnosti ESET.

„V pražské výzkumné pobočce se dlouhodobě zaměřujeme na mapování bankovního malwaru v zemích Latinské Ameriky v rámci takzvaného botnet trackingu. Naše týmy na monitorování objevených malware rodin pracují již od roku 2017. Této hrozbě přitom v minulosti nebylo věnováno příliš mnoho pozornosti, což se především dlouhodobou prací pražského týmu podařilo změnit," říká Jakub Souček, bezpečnostní expert z pražské výzkumné pobočky společnosti ESET.

Společná operace společnosti ESET a brazilské federální policie byla zaměřena na osoby, o nichž se předpokládá, že jsou vysoko v operační hierarchii botnetové sítě. Vyšetřování brazilské federální policie vedlo k několika zatčením v Brazílii a ve Španělsku. ESET k celé akci přispěl poskytnutím technické analýzy, statistických informací a získaných doménových jmen a IP adres C&C serverů. Poskytnuté informace byly klíčové pro identifikaci účtů, které byly odpovědné za zřízení a připojení k C&C serverům (řídící a kontrolní servery) malwaru Grandoreiro. Vlivem implementační chyby v síťovém protokolu mohli analytici společnosti ESET zjistit více informací také o obětech těchto útoků

Z hlediska funkčnosti se škodlivý kód Grandoreiro od roku 2020 příliš nezměnil, přesto prochází rychlým a neustálým vývojem. Bezpečnostní experti ze společnosti ESET během pozorování tohoto malwaru zaznamenali i několik nových verzí škodlivého kódu týdně – v období od února 2022 do června 2022 to například představovalo novou verzi škodlivého kódu v průměru každé čtyři dny.

Operátoři z řad útočníků musí napadené zařízení stále ovládat manuálně, aby mohli obětem ukrást jejich finanční prostředky. Škodlivý kód umožňuje například blokovat obrazovky obětí, zaznamenávat stisky kláves na klávesnici, simulovat činnost myši a klávesnice, sdílet obrazovku obětí či zobrazovat falešná vyskakovací okna.

„Latinskoamerické bankovní trojské koně jsou velmi odlišné od toho, co známe z jiných částí světa. Zatímco klasický bankovní trojan mění například data ve formulářích internetového bankovnictví a funguje na základě modifikace webového provozu, latinskoamerický malware funguje jinak. Tyto bankovní trojany monitorují chování uživatele a čekají, až v prohlížeči otevře internetové bankovnictví nebo jinou finanční aplikaci. Jakmile se tak stane, začne škodlivý kód, nainstalovaný na zařízení oběti jako jakýkoli jiný malware, komunikovat s C&C serverem, ke kterému má přístup útočník. Ten pak počká, až se uživatel do bankovnictví přihlásí, a následně převezme kontrolu nad počítačem uživatele – zablokuje mu obrazovku a zobrazí falešné okno s hláškou, která má uživatele přesvědčit, aby nevypínal aplikaci, například pod záminkou právě probíhající aktualizace bankovního systému. Zatímco uživatel čeká, útočník ovládá uživatelovu klávesnici a myš a manuálně provede transakci. V některých případech může dokonce zobrazit další falešné okno, které uživatele vyzývá k zadání ověřovacího kódu druhého faktoru," vysvětluje Souček.

Bezpečnostní experti z pražské výzkumné pobočky společnosti ESET využívají k monitorování latinskoamerického bankovního malwaru automatizované systémy, které jim umožňují speciálně sledovat změny škodlivého kódu v čase. Pražskému týmu se postupně podařilo zanalyzovat velké množství zachycených vzorků škodlivého kódu a jejich informace přispěly k celkovému zmapování oblasti latinskoamerického bankovního malwaru.

„Automatizované systémy společnosti ESET zpracovaly desítky tisíc vzorků bankovního malwaru Grandoreiro. Algoritmus generování domén DGA, který malware používá přibližně od října 2020, vytváří jednu doménu denně a je to jediný způsob, jakým je Grandoreiro schopen navázat spojení s C&C serverem. Kromě aktuálního data pracuje algoritmus také s obrovskou statickou konfigurací," říká Jakub Souček z ESETu.

Implementace síťového protokolu malwaru Grandoreiro umožnila analytikům ze společnosti ESET nahlédnout za oponu a získat informace také o obětech. Zkoumáním těchto údajů za více než rok dospěli k závěru, že 66 % tvořili uživatelé systému Windows 10, 13 % používalo systém Windows 7, systém Windows 8 představoval 12 % a 9 % tvořili uživatelé systému Windows 11.

Protože data škodlivého kódu Grandoreiro uvádí nespolehlivé informace o geografickém rozložení obětí, odkazují tyto informace na telemetrii společnosti ESET: 65 % všech obětí bylo detekováno ve Španělsku, následuje Mexiko se 14 % obětí, Brazílie se 7 % a Argentina s 5 %; zbývajících 9 % obětí se nachází v ostatních latinskoamerických zemích. V roce 2023 společnost ESET zaznamenala výrazný pokles aktivity Grandoreiro ve Španělsku, který byl kompenzován nárůstem kampaní v Mexiku a Argentině.

Další technické informace o bankovním malwaru Grandoreiro najdete v příspěvku na webu WeLiveSecurity.com.

Více informací o trendech v kyberbezpečnosti najdete například v online magazínu o IT bezpečnosti pro firmy Digital Security Guide.

Společnost ESET ve spolupráci s kyberbezpečnostními odborníky dále připravuje podcast True Positive. Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio produktů ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/kyberbezpecnostni-experti-z-prazske-pobocky-eset-pomohli-k-naruseni-site-utocniku-v-brazilii