Główne przeglądarki porzuciły tajemniczą firmę uwierzytelniającą

6 grudnia 2022

Mozilla i Microsoft zrezygnowały z certyfikatów firmy TrustCor Systems po tym, jak „Washington Post" ujawnił powiązania firmy z kontrahentami rządowymi specjalizującymi się w oprogramowaniu szpiegowskim. Oto, co pisze o tym gazeta…

Firma offshore, której zaufały największe przeglądarki internetowe i inne firmy technologiczne, w kwestii poręczenia za legalność stron internetowych, ma powiązania z kontrahentami amerykańskich agencji wywiadowczych i organów ścigania – donoszą analitycy bezpieczeństwa, dokumenty i wywiady. Google Chrome, Apple Safari, non-profit Firefox i inne pozwalają firmie TrustCor Systems działać jako tzw. root certificate authority, czyli potężny punkt w infrastrukturze internetowej, który gwarantuje, że strony internetowe nie są fałszywe, prowadząc do nich użytkowników w sposób bezproblemowy.

Panamskie dane rejestracyjne firmy pokazują, że ma ona identyczny skład funkcjonariuszy, przedstawicieli i partnerów, jak producent oprogramowania szpiegowskiego zidentyfikowany w tym roku jako oddział firmy Packet Forensics z siedzibą w Arizonie, która, jak pokazują publiczne rejestry zamówień i dokumenty firmowe, sprzedawała usługi przechwytywania komunikacji amerykańskim agencjom rządowym przez ponad dekadę.

Jeden z owych partnerów TrustCor ma taką samą nazwę jak spółka holdingowa zarządzana przez Raymonda Saulino, który był cytowany w artykule „Wired" z roku 2010 jako rzecznik Packet Forensics. Saulino pojawił się również w roku 2021 jako osoba kontaktowa innej firmy, Global Resource Systems, która

spowodowała spekulacje w świecie technologii, gdy na krótko aktywowała i uruchomiła ponad 100 milionów wcześniej uśpionych adresów IP przypisanych dekady wcześniej Pentagonowi.

Pentagon odzyskał cyfrowe terytorium miesiące później i pozostaje niejasne, czego dotyczył ten krótki transfer, ale eksperci powiedzieli, że aktywacja wspomnianych adresów IP mogła dać wojsku dostęp do ogromnej ilości ruchu internetowego bez ujawniania, że to rząd był jego odbiorcą.

Pentagon nie odpowiedział na prośbę o komentarz w sprawie TrustCor. Po opublikowaniu tej historii, członek zarządu TrustCor powiedział, że firma nie współpracowała z żadnymi rządowymi prośbami o informacje ani nie pomagała w monitorowaniu klientów przez osoby trzecie w imieniu innych. Mozilla zażądała bardziej szczegółowych odpowiedzi i stwierdziła, że może odebrać TrustCorowi uprawnienia. Na kilka minut przed odejściem Trumpa z urzędu miliony uśpionych adresów IP Pentagonu ożyły.

Produkty TrustCor obejmują usługę poczty elektronicznej, która twierdzi, że jest szyfrowana end-to-end, choć eksperci konsultowani przez The Washington Post powiedzieli, że znaleźli dowody podważające takie twierdzenie. Wersja testowa usługi e-mail zawierała również oprogramowanie szpiegowskie stworzone przez firmę panamską powiązaną z Packet Forensics, powiedzieli analitycy. Google następnie wykluczył wszystkie programy zawierające ów kod spyware z jego sklepu z aplikacjami.

Osoba obeznana z pracą Packet Forensics potwierdziła, że wykorzystała ona proces certyfikacji TrustCor i jej usługę e-mailową, MsgSafe, do przechwytywania komunikacji i pomagania rządowi USA w wyłapywaniu osób podejrzanych o terroryzm. „Tak, Packet Forensics to robi” – powiedziała ta osoba, wypowiadając się pod warunkiem zachowania anonimowości, w celu omówienia poufnych praktyk.

Radca prawny Packet Forensics, Kathryn Tremel, powiedziała, że firma nie ma żadnych relacji biznesowych z TrustCor ale nie chciała powiedzieć czy miała je wcześniej. Najnowsze odkrycie pokazuje, jak technologiczne i biznesowe zawiłości wewnętrznego funkcjonowania Internetu mogą być wykorzystywane w zakresie, który rzadko jest ujawniany.

Obawy dotyczące głównych urzędów certyfikacji pojawiały się już wcześniej.

W roku 2019, firma ochroniarska kontrolowana przez rząd Zjednoczonych Emiratów Arabskich, która była znana jako DarkMatter, złożyła wniosek o podniesienie jej pozycji do top-level root authority z poziomu intermediate authority o mniejszej niezależności. Stało się to po doniesieniach o tym, że DarkMatter hakuje dysydentów, a nawet niektórych Amerykanów; Mozilla odmówiła jej uprawnień tzw. roota.

W roku 2015 Google wycofał uprawnienia root authority wobec China Internet Network Information Center (CNNIC) po tym, jak zezwolił on organowi pośredniemu na wydawanie fałszywych certyfikatów dla stron Google. W przypadku Packet Forensics, ślad papierowy doprowadził do tego, że został zidentyfikowany przez ekspertów dwukrotnie w tym roku. Firma, znana głównie ze sprzedaży organom władzy urządzeń przechwytujących i usług śledzenia, ma za sobą cztery miesiące kontraktu z Pentagonem o wartości 4,6 mln dolarów na „przetwarzanie danych, hosting i usługi powiązane”.

We wcześniejszej sprawie dotyczącej spyware, badacze Joel Reardon z University of Calgary i Serge Egelman z University of California at Berkeley odkryli, że panamska firma, Measurement Systems, płaciła deweloperom za włączenie kodu do różnych niewinnych aplikacji, aby nagrywać i przesyłać numery telefonów użytkowników, adresy e-mail i dokładne lokalizacje. Oszacowano, że aplikacje te zostały pobrane ponad 60 milionów razy, w tym 10 milionów pobrań muzułmańskich aplikacji modlitewnych.

Strona internetowa Measurement Systems została zarejestrowana przez Vostrom Holdings, jak wynika z historycznych zapisów nazw domen. Vostrom złożył papiery w roku 2007, aby prowadzić działalność gospodarczą jako Packet Forensics, jak podają rejestry stanu Virginia. Measurement Systems został zarejestrowany w Wirginii przez Saulino, zgodnie z inną dokumentacją stanową.

Po tym jak badacze podzielili się swoimi odkryciami, Google wyrzucił wszystkie aplikacje z kodem szpiegowskim ze swojego sklepu Play. Tremel powiedziała, że „firma wcześniej związana z Packet Forensics była klientem Measurement Systems w pewnym momencie", ale nie było żadnych udziałów własnościowych.

Kiedy Reardon i Egelman przyjrzeli się bliżej Vostromowi, odkryli, że zarejestrował on domenę TrustCor.co, która kierowała odwiedzających na główną stronę TrustCor. TrustCor ma tego samego prezesa, przedstawicieli i partnerów spółki holdingowej wymienionych w panamskich rejestrach co Measurement Systems.

Firma o tej samej nazwie, co jedna z firm holdingowych stojących za TrustCor i Measurement Systems – Frigate Bay Holdings, złożyła w marcu tego roku dokumenty o rozwiązanie w sekretariacie stanu w Wyoming, gdzie została utworzona. Dokumenty zostały podpisane przez Saulino, który wymienił swój tytuł jako menedżer. Nie udało się z nim skontaktować celem uzyskania komentarza.

TrustCor wydał ponad 10 000 certyfikatów, wiele z nich dla stron hostowanych u dostawcy usług dynamicznych nazw domen o nazwie No-IP, powiedzieli analitycy. Usługa ta pozwala na hostowanie stron z ciągle zmieniającymi się adresami protokołu internetowego. Ponieważ root authority jest tak potężny, TrustCor może również dać innym prawo do wydawania certyfikatów.

Certyfikaty dla stron internetowych są publicznie widoczne,

więc złe powinny zostać wcześniej czy później ujawnione. Jak dotąd nie było żadnych doniesień o tym, że certyfikaty TrustCor zostały wykorzystane w niewłaściwy sposób, np. poprzez ręczenie za strony internetowe oszustów. Badacze spekulowali, że system jest wykorzystywany tylko przeciwko celom o wysokiej wartości w krótkich oknach czasowych. Osoba zaznajomiona z operacjami Packet Forensics potwierdziła, że w rzeczywistości tak właśnie był on wykorzystywany. „Mają tę pozycję ostatecznego zaufania, gdzie mogą wydawać klucze szyfrujące dla każdej dowolnej strony internetowej i każdego adresu e-mail" – powiedział Egelman. „To przerażające, że robi to jakaś podejrzana prywatna firma".

Strona dotycząca kierownictwa spółki TrustCor wymienia zaledwie dwóch mężczyzn, zidentyfikowanych jako współzałożyciele. Chociaż ta strona tego nie mówi, jeden z nich zmarł miesiące temu, a drugi profil LinkedIn mówi, że odszedł jako główny oficer technologiczny w 2019 roku. Ten człowiek odmówił komentarza.

Strona internetowa wymienia numer telefonu kontaktowego w Panamie, który został odłączony, i jeden w Toronto, gdzie wiadomość nie została zwrócona po ponad tygodniu. Formularz kontaktowy e-mail na stronie nie działa. Fizyczny adres w Toronto, podany w raporcie audytora, 371 Front St. West, jest punktem odbioru poczty UPS Store.

TrustCor wprowadza kolejną warstwę tajemniczości za sprawą swojej zewnętrznej firmy audytorskiej. Zamiast skorzystać z usług dużej firmy księgowej, która ocenia bezpieczeństwo firm zajmujących się infrastrukturą internetową, TrustCor wybrał firmę o nazwie Princeton Audit Group, która podaje swój adres jako dom mieszkalny w Princeton, N.J.

W komentarzach we wtorek do listy e-mailowej dla deweloperów Mozilli, dyrektor wykonawczy TrustCor – Rachel McPherson powiedziała, że jej firma padła ofiarą złożonych ataków, które objęły rejestrację firm o nazwach podobnych do nazwisk jej

udziałowców, być może w celu ułatwienia zorganizowania jakiegoś ataku phishingowego. Powiedziała, że będzie badać, dlaczego niektóre osoby zostały wymienione jako funkcjonariusze.

Oprócz kompetencji certyfikatów TrustCor, firma oferuje to, co rzekomo ma być end-to-end szyfrowany e-mail, MsgSafe.io. Ale badacze powiedzieli, że e-mail nie jest zaszyfrowany i może być odczytany przez firmę, która wprowadziła go do różnych grup obawiających się nadzoru. https://www.msgsafe.io/

MsgSafe wychwalał swoje bezpieczeństwo wśród różnych potencjalnych klientów, w tym zwolenników Trumpa zdenerwowanych tym, że Parler został porzucony przez sklepy z aplikacjami w styczniu 2021 roku, a także przed użytkownikami szyfrowanej usługi pocztowej Tutanota, którzy zostali zablokowani przy logowaniu się do usług Microsoftu. „Stwórz swoją darmową, szyfrowaną pocztę end-to-end już dziś z ponad 40 domenami do wyboru, które gwarantują współpracę z Microsoft Teams" – zatweetowała firma w sierpniu.

Reardon wysłał próbne wiadomości przez MsgSafe, które okazały się niezaszyfrowane podczas transmisji, co oznacza, że MsgSafe mógł je czytać do woli. Egelman przeprowadził ten sam test z takim samym wynikiem.

Jon Callas, ekspert ds. kryptografii w Electronic Frontier Foundation, również przetestował system na prośbę „The Post" i powiedział, że MsgSafe wygenerował i przechowywał klucz prywatny dla jego konta, tak że mógł odszyfrować wszystko, co wysłał. „Klucz prywatny musi znajdować się pod kontrolą danej osoby, aby był end-to-end" – wyjaśnił Callas.

Packet Forensics po raz pierwszy zwrócił uwagę rzeczników prywatności kilkanaście lat temu. W roku 2010, badacz Chris Soghoian wziął udział w konferencji branżowej zwanej Wiretapper's Ball i otrzymał broszurę Packet Forensics skierowaną do klientów z branży organów ścigania i agencji

wywiadowczych. Broszura dotyczyła sprzętu, który miał pomóc nabywcom w odczytywaniu ruchu internetowego, który strony uważały za bezpieczny. Choć nie był. „Komunikacja IP dyktuje potrzebę badania ruchu szyfrowanego na życzenie" – czytamy w broszurze, zgodnie z raportem w Wired, który cytuje Saulino jako rzecznika Packet Forensics. "Twoi śledczy będą zbierać najcenniejsze dowody, podczas gdy użytkownicy będą się łudzić fałszywym poczuciem bezpieczeństwa, jakie daje szyfrowanie stron internetowych, poczty elektronicznej lub VOIP" – czytamy w broszurze. Publikacja informowała klientów, że mogą użyć klucza deszyfrującego dostarczonego przez nakaz sądowy lub "klucza podobnego".

Badacze uważali wówczas, że najprawdopodobniej skrzynka była używana przy użyciu certyfikatu wydanego przez urząd za pieniądze lub na podstawie nakazu sądowego, który miałby gwarantować prawdziwość witryny komunikacyjnej impostora. Nie wywnioskowali, że cały urząd certyfikacji sam w sobie może być zdyskredytowany.

Otrzymanie tytułu zaufanego urzędu certyfikacji wymaga czasu i pieniędzy na infrastrukturę oraz na audyt, którego wymagają przeglądarki – mówią eksperci. Każda przeglądarka ma nieco inne wymagania. Jak chodzi o Firefoxa Mozilli, proces trwa dwa lata i obejmuje crowdsourcing i bezpośrednią weryfikację, a także audyt. Ale wszystko to skupia się zazwyczaj na formalnych oświadczeniach dotyczących działań technologicznych, a nie na sekretach dotyczących własności i zamiarów. Osoba zaznajomiona z Packet Forensics powiedziała, że duże firmy technologiczne prawdopodobnie były nieświadomymi uczestnikami spektaklu TrustCor: „Większość ludzi nie zwraca na to uwagi". „Mając wystarczająco dużo pieniędzy, ty lub ja możemy stać się zaufanym głównym urzędem certyfikacji" – powiedział Daniel Schwalbe, wiceprezes ds. technologii w firmie śledzącej dane internetowe DomainTools.

Mozilla uznaje obecnie 169 urzędów certyfikacji, w tym trzy z TrustCor.

Przypadek sprawia, że problemy z takim systemem, w którym najważniejsze firmy technologiczne obdarzają zaufaniem strony trzecie posiadające własne agendy, nabierają nowego znaczenia. „Nie można uruchomić zaufania, musi ono skądś pochodzić” – powiedział Reardon. „Centralne urzędy certyfikacji są jądrem zaufania, na którym to wszystko jest zbudowane. A to zawsze będzie chwiejne, bo zawsze będzie angażować ludzi, gremia i procesy podejmowania decyzji”.

Autorstwo: Rob Wright
Na podstawie: WashingtonPost.com
Źródło zagraniczne: Techtarget.com
Źródło polskie: BabylonianEmpire.wordpress.com