Udało nam się zrealizować wywiad z grupą ransomware (Babuk), która zaszyfrowała policję metropolitarną w Waszyngtonie

sekurak.pl/udalo-nam-sie-zrealizowac-wywiad-z-grupa-ransomware-babuk-ktora-zaszyfrowala-policje-metropolitarna-w-waszyngtonie/

April 29, 2021

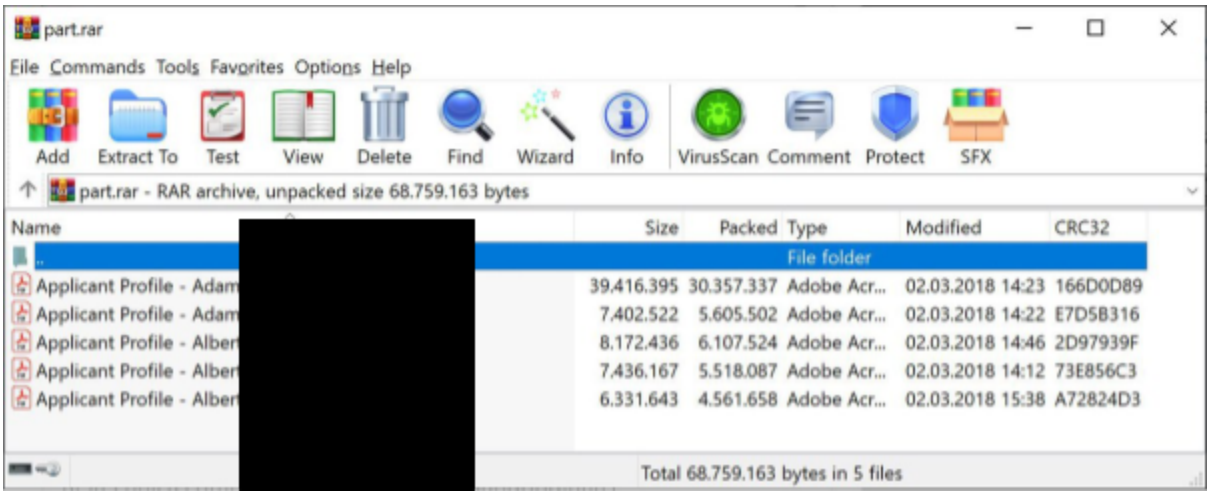
Policja metropolitalna w Waszyngtonie padła ofiarą ataku ransomware'owego. Operatorzy Babuka uzyskali dostęp do jej infrastruktury, wykradli poufne i bardzo wrażliwe dane, a w zamian za powstrzymanie się od publikacji całości wykradzionych informacji żądają zapłaty.

Wczoraj (28 kwietnia) wcześnie rano na stronie wyciekowej Babuka pojawiła się następująca wiadomość, skierowana do waszyngtońskiej policji:

We advise the police station to get in touch as soon as possible, you do not need this leak, because of it people may suffer, we also have software that allows you to view reports in the i2-analysts-notebook
—Operatorzy ransomware Babuk

Jeśli chcesz przejść do treści wywiadu – przeskroluj nieco niżej.
Wspomniane oprogramowanie i2-analysts-notebook jest powszechnie wykorzystywane przez analityków kryminalnych w oddziałach policji na całym świecie, w tym również w Polsce. Pozwala tworzyć *teczki*, w których umieszczane są szczegółowe informacje o analizowanych sprawach, w tym na przykład dane o osobach, przepływach pieniężnych i komunikacji oraz o relacjach pomiędzy poszczególnymi osobami w grupach przestępczych. Wczorajszy dowód pozyskania takich plików i ich odczytania przez osoby nieuprawnione, a następnie sama tylko groźba opublikowania tych danych na stronie wyciekowej lub sprzedaż tych informacji grupom przestępczym, z całą pewnością uwiarygodniły operatorów ransomware'a Babuk.

W godzinach popołudniowych na stronie wyciekowej Babuka pojawiła się pierwsza paczka z danymi z wycieku.



W ujawnionych plikach opublikowano objęte klauzulą poufności raporty, które (choć bardzo interesujące) nigdy nie powinny zostać ujawniane osobom postronnym. Zawierały dane osobowe, w tym dotyczące wykształcenia, doświadczenia zawodowego, miejsca zamieszkania i sytuacji finansowej funkcjonariuszy policji waszyngtońskiej. Amerykańska stacja NBC potwierdziła autentyczność tych danych z jedną z osób, której dane ujawniono.

Należy więc przyjąć za pewne, że operatorzy ransomware Babuk:

1. uzyskali dostęp do infrastruktury policji metropolitalnej w Waszyngtonie,
2. pozyskali policyjne dane, oraz
3. w razie odmowy zawarcia stosownego porozumienia, opublikują wszystko, co pobrali (ok. 250 GB danych, w tym kartoteki policyjne, akta spraw, dane konkretnych funkcjonariuszy).

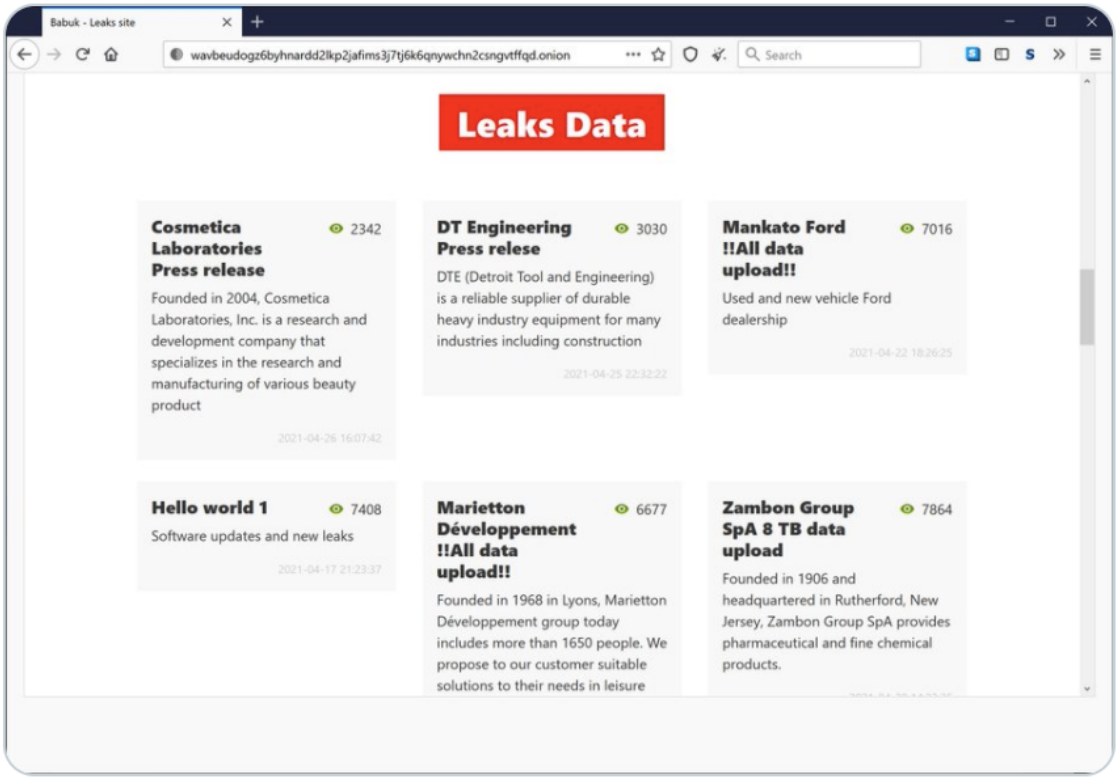
Po opublikowaniu powyższych pięciu raportów, ze strony wyciekowej Babuka usunięte zostały wszystkie artykuły dotyczące policji metropolitalnej w Waszyngtonie. Użytkownicy Twittera zastanawiają się, czy to znaczy że policja metropolitalna zapłaciła okup.

Intelligence X
@_IntelligenceX

W odpowiedzi do @_IntelligenceX

Babuk has updated their ransomware website and removed the DC police leak. Did the DC police pay the ransom?

Przetłumacz Tweeta

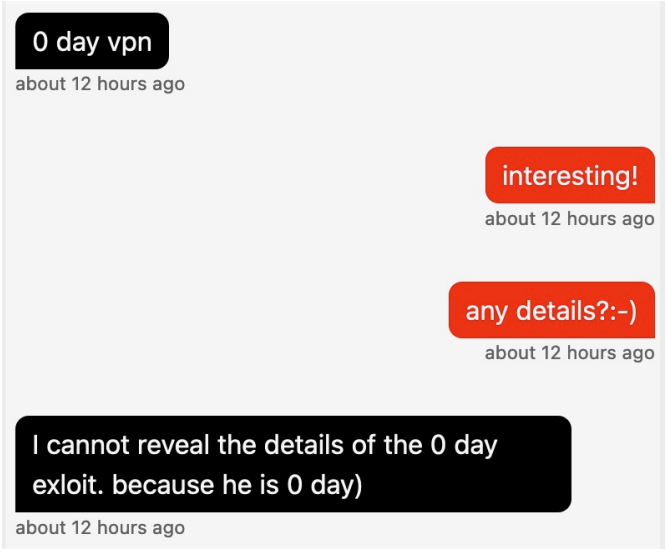


7:39 PM · 28 kwi 2021 · Twitter Web App

Sekurak, zamiast spekulować, po prostu sprawdził.

Operatorzy ransomware'a Babuk udzielili nam unikalnego wywiadu, bowiem na razie nikomu innemu się to nie udało. Jak to zrobiliśmy? Oficjalnym kanałem. Zadawaliśmy pytania i dostawaliśmy odpowiedzi. Wywiad jest autoryzowany.

Fragment rozmowy wygląda tak, a tłumaczenie z angielskiego na polski jest nasze:



Babuk: Jesteście pierwszymi i ostatnimi dziennikarzami, którym udzielamy wywiadu. Nie jesteśmy tacy, jak inne grupy. Nie udzielamy wywiadów. Nie potrzebujemy sławy.

sekurak: Mówicie o sobie, że jesteście cyberpunkami. W mediach, w ciągu ostatnich kilkudziesięciu godzin z *cyberpunków* staliście się *rosyjskimi hakerami*. Kim tak naprawdę jesteście?

Babuk: To prawda, jesteśmy cyberpunkami. Na marginesie – policja metropolitalna w Waszyngtonie jest ostatnią instytucją rządową, którą zaatakowaliśmy. Nie chcemy być kojarzeni z polityką, czy rosyjskimi „państwowymi" hakerami. Nie jesteśmy nimi i uważamy ich działania za niedorzeczne. Nie potrzebujemy też sławy.

sekurak: Policja waszyngtońska jest ostatnią zaatakowaną instytucją – to znaczy, że już więcej nie będziecie audytować sieci instytucji rządowych czy że zaatakowaliście też inne podmioty, a policja jest ostatnią z nich?

Babuk: Policja waszyngtońska jest ostatnią rządową instytucją, którą audytowaliśmy. Nie będziemy więcej atakować podmiotów z sektora rządowego, ponieważ nie chcemy wywołać konfliktu między Federacją Rosyjską a Stanami Zjednoczonymi.

sekurak: Czy to oznacza, że zapoznaliście się z najnowszą wspólną publikacją CISA, DHS i FBI o aktywności rosyjskich hakerów w Stanach Zjednoczonych?

Babuk: Tak, zapoznaliśmy się. Nie jesteśmy sponsorowani przez żadne konkretne państwo, działamy samodzielnie. Nie atakujemy ofiar w niektórych państwach, takich jak Rosja, Polska, czy inne kraje postsowieckie. Z prostego powodu – one zwyczajnie nie mają pieniędzy, żeby zapłacić za nasze usługi.

sekurak: To kogo atakujecie?

Babuk: Na początku lata tego roku przeprowadzimy zmasowany atak na największe firmy informatyczne. Powiedzmy więc, że giganci IT powinni poszukać naszych kotwic w swoich systemach i być może to udaremni przeprowadzenie naszego ataku.

sekurak: A co w przypadku takiego scenariusza, kiedy audytujecie sieć korporacyjną, znajdujecie podatności, wykradacie i szyfrujecie dane, ale ofiara nie ma środków na zapłatę oczekiwanego przez was wynagrodzenia?

Babuk: Zdarza się tak, że ofiara twierdzi, że nie ma środków na zapłatę naszego wynagrodzenia. Weryfikujemy wtedy sytuację finansową ofiary i podejmujemy decyzję o wysokości naszego honorarium. Ostatnio zdarzyła się taka sytuacja, że zaatakowaliśmy afrykańską firmę, która handlowała paliwem, jednak w związku z pandemią, utraciła płynność finansową i faktycznie nie miała środków, aby nam zapłacić. Zrezygnowaliśmy z wynagrodzenia i nieodpłatnie przekazaliśmy narzędzie deszyfrujące.

sekurak: Czyli pomagacie ofiarom, nie zawsze oczekując za to wynagrodzenia?

Babuk: Tak. Opisujemy to na naszej stronie internetowej. Ostatnio pomogliśmy domowi opieki. Znaleźliśmy podatności w ich sieci i spatchowaliśmy je, totalnie pro bono. Szanujemy osoby starsze i tych, którzy im pomagają. To nie jest kwestia kultury czy wyznania – po prostu każda osoba powinna odnosić się z szacunkiem do osób starszych, niepełnosprawnych oraz tych osób i instytucji, które im pomagają.

sekurak: Czy ofiary wam płacą?

Babuk: Tak. Co najmniej 7 firm nam zapłaciło, w tym jedna $2.000.000.

sekurak: Czy policja metropolitalna w Waszyngtonie również wam zapłaciła?

Babuk: W każdym przypadku są dwa scenariusze. Pierwszy, kiedy ofiara płaci – wtedy usuwamy artykuły z naszej strony internetowej. Drugi, kiedy ofiara nie płaci – wtedy publikujemy wyciek.

sekurak: Skoro artykuły o policji zniknęły, oznacza to, że policja wam zapłaciła?

Babuk: Trwają negocjacje. Obiecaliśmy, że nie opublikujemy nic więcej, dopóki negocjacje trwają. W tej chwili nie możemy powiedzieć więcej.

sekurak: Jak dostaliście się do infrastruktury policji w Waszyngtonie?

Babuk: 0-day w VPN. Nie możemy powiedzieć nic więcej, w końcu to 0-day.

sekurak: Kiedy policja waszyngtońska zorientowała się, że Babuk uzyskał dostęp do sieci?

Babuk: Zorientowali się zbyt późno, już po tym jak wykradliśmy dane.

sekurak: Wykradliście dane z policji waszyngtońskiej, czy również zaszyfrowaliście?

Babuk: Nie zaszyfrowaliśmy wszystkich 6,000 hostów, ponieważ nie chcieliśmy, żeby policja nie mogła pracować. Żądamy zapłaty za niepublikowanie danych. Jeśli chcielibyśmy zaszyfrować dane policji metropolitalnej, po prostu byśmy je zaszyfrowali.

sekurak: Co najczęściej wykorzystujecie? RDP wystawione na świat? Socjotechnikę? 0-day'e?

Babuk: RDP naprawdę nie jest taki zły, jednak te RDP, które są dostępne z zewnątrz, są wykorzystywane przez małe firmy, a one nie są dla nas interesujące. VPN jest już używany przez większe firmy, które nas interesują. Wykorzystywaliśmy również lukę ProxyLogon (0-day w serwerach MS Exchange).

sekurak: Co na koniec chcielibyście przekazać osobom, które czytają ten wywiad?

Babuk: Nie chcemy nikogo straszyć. Po prostu, zabezpieczcie brzeg waszej sieci i nie będzie więcej problemów. Chcemy również podziękować wszystkim badaczom za pomoc w znalezieniu podatności w naszym produkcie. Szczególne podziękowania należą się dla Chuong Donga, dzięki któremu poprawiliśmy nasze szyfrowanie, oraz dla firmy Emsisoft za pomoc w poprawieniu naszego dekryptora.

–unk