Cyberdefence 24

aut. Szymon Palczewski 24.09.2020

ROSJA CELEM... RODZIMYCH HAKERÓW. PRECEDENS W ŚRODOWISKU CYBERPRZESTĘCÓW

Rosyjscy hakerzy złamali niepisaną zasadę mówiącą o nieatakowaniu celów w Rosji oraz w państwach postsowieckich, przeprowadzając serię cyberataków wymierzoną w największe firmy w kraju. Zdaniem specjalistów powstał precedens, który może odmienić rosyjskie środowisko cyberprzestępcze.

Rosyjskojęzyczni cyberprzestępcy odpowiadają za szereg kampanii hakerskich wymierzonych w największe firmy z sektora medycznego, finansowego, przemysłowego oraz IT w Rosji. Seria cyberataków rozpoczęła się pod koniec marca wraz z wybuchem pandemii koronawirusa i trwała do sierpnia br. Hakerzy podczas operacji wykorzystywali oprogramowanie ransomware, co pozwoliło im na skuteczne sparaliżowanie poszkodowanych podmiotów. Specjaliści mówią tu o precedensie, ponieważ w środowisku cyberprzestępczym istnieje niewypowiedziana zasada: rosyjscy hakerzy nie atakują celów w Rosji oraz państwach postsowieckich.

W ostatnim czasie zespół specjalistów Group-IB Threat Intelligence wykrył ślady udanego cyberataku wymierzonego w rosyjski koncern medyczny. Za incydent odpowiadają hakerzy nieznanej do tej pory grupy cyberprzestępczej, którą eksperci nazwali Old Gremlin. Na skutek cyberataku hakerom udało się zaszyfrować sieć wewnętrzną firmy. Cyberprzestępcy za jej odblokowanie zażądali okupu w wysokości 50 000 dolarów – czytamy w raporcie „Big Game Hunting: Now in Russia", opracowanym przez specjalistów Group-IB.

„Rosyjscy hakerzy mają niewypowiedzianą zasadę nie prowadzenia operacji w Rosji oraz krajach postsowieckich" – wskazują specjaliści. Tym razem jest jednak inaczej. Old Gremlin to grupa złożona z „rosyjskojęzycznych osób", atakująca... rosyjskie firmy, w tym banki, przedsiębiorstwa przemysłowe, instytucje medyczne oraz twórców oprogramowania.

Według śledztwa przeprowadzonego przez specjalistów, od wiosny hakerzy wspomnianej grupy przeprowadzili co najmniej siedem kampanii phishingowych. Podczas operacji cyberprzestępcy podszywali się między innymi pod rosyjski holding metalurgiczny, białoruski zakład Mińsk Tractor Works, klinikę dentystyczną czy holding medialny RBC.

Tajemniczy plik z fakturą

W sierpniu 2020 roku zespół specjalistów Group-IB ujawnił szczegóły ostatniego udanego cyberataku przeprowadzonego przez Old Gremlin. „Ofiarą była duża firma medyczna z siecią oddziałów regionalnych" – czytamy w raporcie. Pierwszym wektorem ataku był e-mail phishingowy wysłany rzekomo przez holding medialny RBC.

„E-mail nie wzbudził podejrzeń. Pracownik firmy śmiało kliknął w link i pobrał załączony plik ZIP. Wiadomość z tytułem >Należny rachunek< wyglądała jakby została wysłana przez Departament Finansów dużego rosyjskiego holdingu medialnego – grupy RBC. Po uruchomieniu pliku po zaledwie

dwudziestu sekundach program Windows Defender wykrył i usunął złośliwe oprogramowanie. Jednak te dwadzieścia sekund wystarczyło, aby trojan mógł uzyskać dostęp i pozostać w zainfekowanym systemie" – opisują sytuację specjaliści. „Ofiara niczego nie zauważyła. Trzy tygodnie później pracownicy firmy przyszli do pracy i zostali powitani alarmującą wiadomością na ekranach komputerów: >Twoje pliki zostały zaszyfrowane<. Wszystkie prace zostały wstrzymane. Atakujący zażądali 50 000 dolarów w kryptowalucie, aby odszyfrować pliki" – dodają.

Analiza incydentu wykazała, że na początkowym etapie operacji hakerzy użyli niestandardowego złośliwego oprogramowania o nazwie TinyNode – backdoora, który pobiera i uruchamia dodatkowe wirusy. Po uzyskaniu dostępu cyberprzestępcy z łatwością mogli przeprowadzić rozpoznanie sieci, zebrać cenne dane i rozprzestrzeniać kampanię na kolejne systemy.

Po tym, jak hakerzy przeprowadzili rozpoznanie i zidentyfikowali obszar sieci, który ich interesuje, nadal penetrowali systemy firmy. Ostatecznie udało im się uzyskać poświadczenie administratora, co pozwoliło im na utworzenie dodatkowego konta z takimi samymi uprawnieniami na wypadek, gdyby główny profil został zablokowany.

„W tym konkretnym przypadku utworzenie kopii zapasowej nie uratowało ofiary" – wskazali specjaliści Group-IB. Kilka tygodni po rozpoczęciu ataku cyberprzestępcy wyczyścili kopie zapasowe organizacji. W ciągu zaledwie kilku godzin podczas weekendu rozprzestrzenili oprogramowanie ransomware TinyCryptor na setkach komputerów w sieci wewnętrznej firmy.

Pracownicy przychodząc do firmy zostali zaskoczeni, gdy na ekranach komputerów widniała wiadomość: „Twoje pliki są zaszyfrowane. Aby je odszyfrować, skontaktuj się z nami pod... (tu widniał adres e-mail hostowany na ProtonMail – przyp. red.)". W wyniku kampanii regionalne oddziały firmy zostały sparaliżowane i nie mogły normalnie funkcjonować.

„Old Gremlin jest jedynym rosyjskojęzycznym aktorem ransomware, który narusza niewypowiedzianą zasadę niedziałania w Rosji i krajach postsowieckich" – podkreślił raz jeszcze specjalista i główny analityk Group-IB Oleg Skulkin. „Przeprowadzają wieloetapowe cyberataki wymierzone w rosyjskie firmy i banki przy użyciu wyrafinowanych taktyk oraz technik, podobnych do tych stosowanych przez grupy APT" – wskazał. Ekspert dodał, że Old Gremlin można sklasyfikować jako część Big Game Hunting, czyli sieci hakerów, która skupia operatorów ransomware atakujących duże sieci korporacyjne.

Covid-19. Najlepsza przynęta

Specjaliści Group-IB pierwszy cyberatak ze strony Old Gremlin wykryli między końcem marca a początkiem kwietnia br. Wówczas hakerzy wykorzystali pandemię koronawirusa jako przynętę, rozsyłając do instytucji finansowych fałszywe zalecenia dotyczące sposobu zorganizowania bezpiecznego środowiska pracy.

Podczas kampanii podszywali się pod rosyjskiego regulatora finansowego „Microfinance and Development" (ros. Микрофинансирование и Развитие). „To był pierwszy przypadek, kiedy cyberprzestępcy użyli TinyPosh, własnego trojana, który sami stworzyli" – czytamy w raporcie.

Drugi cyberatak miał miejsce 24 kwietnia br. Schemat operacji był taki sam, lecz tym razem hakerzy podszyli się pod klinikę dentystyczną Novadent.

Dwa tygodnie po tych wydarzeniach grupa Old Gremlin zmieniła taktykę. Cyberprzestępcy stworzyli fikcyjną wiadomość e-mail, którą następnie rozsyłali, podszywając się pod rosyjskiego dziennikarza RBC. W jej treści znajdowało się zaproszenie do wzięcia udziału w „Narodowym badaniu sektora bankowego i finansowego podczas pandemii koronawirusa".

W przeciwieństwie do e-maili wykorzystywanych w poprzednich atakach, wiadomość została zredagowana z wysoką starannością. Napisana była poprawnym językiem i dokładnie naśladowała slang dziennikarzy. W treści znajdowała się również oferta 30-minutowego wywiadu, który miał zostać umówiony za pośrednictwem platformy Calendly.

Następnie hakerzy wysyłali drugą wiadomość, w której rzekomy dziennikarz wskazał, że przesłał pytania do wywiadu do chmury internetowej i czeka na odpowiedzi. „E-mail miał na celu wzbudzenie zainteresowania ofiary i zachęcenie jej do kliknięcia w załącznik" – wyjaśnili specjaliści Group-IB. Jak dodali, aby wiadomość wyglądała bardziej przekonująco, każdy e-mail zawierał nazwę wiodącego dostawcy usług z zakresu cyberbezpieczeństwa, który rzekomo ją zweryfikował.

Cała Rosja pod ostrzałem hakerów

Hakerzy Old Gremlin na pewien okres wygasili swoją działalność, powracając w połowie sierpnia br. z nową kampanią cyberataków. CERT-GIB (komórka Group-IB) zidentyfikował dwie zakrojone na szeroką skalę operacje, w ramach których hakerzy podszywali się pod RBC oraz jedną z firm górniczo-metalurgicznych.

„W ciągu dwóch dni przestępcy wysłali około 250 szkodliwych wiadomości e-mail atakujących rosyjskie firmy z sektora finansowego i przemysłowego" – wskazano w raporcie. W tym przypadku za wabik cyberprzestępcy wykorzystali głośny w Rosji temat protestów na Białorusi.

O wczesnej porze 19 sierpnia zespół CERT-GIB wykrył cyberataki wymierzone w rosyjskie organizacje finansowe. E-maile pochodziły rzekomo od Mińsk Tractor Works. Specjaliści wykryli łącznie ponad 50 zainfekowanych wiadomości. Ich nadawcą była Alesya Vladimirovna, rzekomo CEO firmy. W rzeczywistości kieruje nią Witalij Wowk.

W e-mailach znajdowała się następująca treść: „Niestety, około tygodnia temu prokuratura przeprowadziła inspekcję firmy. Jest jasne, że stało się to z powodu protestów". W dalszej części wiadomości odbiorcy byli proszeni o kliknięcie w załącznik w celu pobrania archiwum i przesłanie brakujących dokumentów do weryfikacji. Otworzenie pliku powodowało zainstalowanie backdoora TinyPosh na urządzeniu ofiary. Dalszy schemat działania hakerów był podobny do wspomnianych wcześniej kampanii.

Old Gremlin to kolejna grupa hakerska, która została zidentyfikowana w ostatnim czasie przez środowisko specjalistów zajmujących się cyberbezpieczeństwem. Rozwój cyberprzestępczości jest w minionych miesiącach szczególnie widoczny. Skąd to wynika?

„Brak silnego kanału komunikacji między podmiotami odpowiedzialnymi za przeciwdziałanie cyberprzestępczości oraz niestabilność polityczna doprowadziły do pojawienia się nowych grup przestępczych, które uważają, że są bezkarne" – wyjaśnił specjalista Group-IB Rustam Mirkasymov. „Kolejnym czynnikiem, który pomaga hakerom w zarabianiu pieniędzy na okupach jest fakt, że firmy nie doceniają zagrożeń istniejących w sieci" – dodał ekspert, wskazując na brak odpowiedniej jakości kontroli cyberbezpieczeństwa w podmiotach prywatnych, co bezpośrednio przekłada się na większe ryzyko i możliwe straty w przypadku cyberataku.

Czytaj też: Tesla celem zaawansowanej operacji Rosjan