aut. Szymon Palczewski 06.10.2020

W EUROPIE LIDEREM… RANSOMWARE. KATALOG ZAGROŻEŃ WEDŁUG EUROPOLU

Głównym zagrożeniem w sieci dla Europejczyków jest ransomware – wynika z analizy Europolu, przeprowadzonej na podstawie obserwacji zjawiska cyberprzestępczości w ciągu ostatnich 12 miesięcy. Pandemia COVID-19 zmieniła krajobraz cyberzagrożeń, przyczyniając się również do wzrostu rozpowszechniania dziecięcej pornografii w internecie oraz cyberataków z udziałem złośliwego oprogramowania. Jakie nowe trendy pojawiły się jeszcze na przestrzeni ostatniego roku?

W raporcie „Internet Organised Crime Threat Assessment 2020", opracowanym przez Europol, podkreślono, że jednym z głównych zagrożeń w ostatnim okresie były cyberataki z udziałem złośliwego oprogramowania, w tym ransomware, oraz kampanie bazujące na inżynierii społecznej. Zdaniem specjalistów obecny krajobraz cyberprzestrzeni można opisać jednym zdaniem: cyberprzestępczość to ewolucja, nie rewolucja.

Europol wskazuje, że z biegiem czasu określone kategorie operacji hakerskich nie ulegają zmianie. Modyfikacjom podlegają jedynie narzędzia oraz taktyka działania cyberprzestępców. „Ta powtarzalność oznacza, że ryzyko nadal istnieje i w wielu przypadkach jest ono większe, co podkreśla potrzebę dalszego wzmacniania odporności oraz reagowania na dobrze znane zagrożenia" – czytamy w raporcie.

Kryzys związany z pandemią COVID-19 pokazał, w jaki sposób cyberprzestępcy wykorzystują społeczeństwo do swoich działań w okresie szczególnego zagrożenia i niepokoju. „Hakerzy dostosowali swoje działania, aby pasowały do narracji dotyczącej pandemii, nadużywali poczucia powszechnej niepewności oraz zapotrzebowania na wiarygodne informacje" – podkreślili specjaliści Europolu. Motyw związany z koronawirusem był obecny we wszystkich kategoriach nielegalnej działalności w sieci – od kampanii DDoS po rozpowszechnianie materiałów z dziecięcą pornografią.

Pandemia przyczyniła się do nasilenia cyberataków, co wynikało z lockdownu oraz konieczności przeniesienia większej aktywności ludzi do internetu. Według danych Europolu jest to najbardziej widoczne na przykładzie treści ukazujących wykorzystywanie seksualne dzieci (ang. child sexual abuse material – CSAM).

„Podobnie jak w poprzednich latach, liczba wykrytych w internecie CSAM nadal rośnie, dodatkowo zostało to zaostrzone przez kryzys COVID-19, który miał poważne konsekwencje dla skuteczności operacji organów ścigania" – czytamy w raporcie Europolu. – „Ponadto transmisje na żywo dotyczące dziecięcej pornografii stały się jeszcze bardziej popularne podczas pandemii".

Bardzo ważnym zagrożeniem jest również naruszenie bezpieczeństwa danych. W tym zakresie hakerzy opierają swoje działania na inżynierii społecznej, skutecznie wykorzystując ludzkie słabości. Analiza Europolu wykazała, że cyberprzestępcy stosują obecnie bardziej holistyczną strategię w tym zakresie, wykazując wysoki poziom koncentracji podczas operacji, podszywając się pod znane postaci

lub bliskie dla ofiary osoby.

Kreatywność hakerów rośnie, jednak większość cyberataków kończy się dla nich sukcesem z powodu nieodpowiednich środków bezpieczeństwa lub braku świadomości użytkowników, którzy sami narażają się na incydent.

Kolejnym zagrożeniem, na jakie eksperci Europolu zwrócili uwagę analizując działalność cyberprzestępców w ostatnich 12 miesiącach są oszustwa związane z płatnością bezgotówkową. Dzięki łatwemu dostępowi do danych hakerom bez problemu przychodzi przeprowadzanie ukierunkowanych cyberataków. Gromadząc liczne informacje z różnych źródeł, posiadają możliwość selektywnego wyboru ofiar.

Europol zwrócił również uwagę na operacje wymierzone w karty SIM. Zdaniem ekspertów jest to nowy trend, który pojawił się w ostatnich kilku miesiącach. Tego typu działania hakerów mogą mieć „katastrofalne konsekwencje dla ofiar", ponieważ umożliwiają cyberprzestępcom ominięcie dwuetapowych środków uwierzytelniania, opartych na wiadomościach SMS, a przez to uzyskanie pełnej kontroli nad poufnymi kontami użytkowników.

Analiza ostatnich 12 miesięcy wykazała także, że nastąpił wzrost liczby przypadków naruszenia poczty e-mail wielu firm. „Cyberprzestępcy ostrożniej wybierają swoje cele, wykazując się dużym zrozumieniem wewnętrznych procesów biznesowych oraz luk w zabezpieczeniach systemów ofiar" – stwierdzono w raporcie.

Złośliwe oprogramowanie. Wiodąca rola ransomware

Przedstawiciele organów ścigania, którzy brali udział w analizie Europolu podkreślili, że po raz kolejny ransomware należy uznać za zagrożenie o najwyższym priorytecie. „Oprogramowanie ransomware pozostaje jednym z najbardziej dominujących zagrożeń, zwłaszcza dla organizacji publicznych i prywatnych w Europie i poza nią" – jednoznacznie stwierdzono w raporcie.

Problem przy kampaniach tego typu jest fakt, że ofiary niechętnie zgłaszają incydenty do organów ścigania, co znacznie utrudnia identyfikacje hakerów oraz szczegółowe zbadanie cyberataku. W raporcie nie wyjaśniono jednak dlaczego poszkodowane osoby lub podmioty decydują się na zachowanie operacji hakerskiej w tajemnicy.

Niestety, ransomware stanowi poważne zagrożenie dla podmiotów prywatnych, zwłaszcza odpowiedzialnych za infrastrukturę krytyczną. Często dochodzi do cyberataków na łańcuchy dostaw, co ma poważne konsekwencje dla wielu firm lub organizacji. Wywieranie presji poprzez żądanie okupu w zamian za niepublikowanie skradzionych danych jest obecnie jedną z głównych metod działania hakerów wykorzystujących ransomware. Kryptowaluty nieustannie pozostają podstawowym środkiem płatności, na jaki decydują się ofiary podczas kampanii tego typu.

Cyberprzestępcy sprawnie posługują się również innymi rodzajami złośliwego oprogramowania. Jako przykład Europol wskazuje tradycyjne trojany bankowe, które hakerzy skutecznie zmodyfikowali w bardziej zaawansowane wirusy, aby wywoływać większe skutki prowadzonych operacji. „Te zmodyfikowane formy złośliwego oprogramowania są głównym zagrożeniem w UE" – podkreślono w raporcie. Specjaliści tłumaczą, że coraz bardziej złożony i adaptacyjny charakter wirusów sprawia, iż skuteczna walka z hakerami jest trudniejsza oraz bardziej skomplikowana niż kiedykolwiek wcześniej.

Jedno z głównych narzędzi hakerskich powszechnie wykorzystywanych przez cyberprzestępców stanowi złośliwe oprogramowanie Emotet. „Jest wszechobecne ze względu na swoje szerokie zastosowanie" – tłumaczą specjaliści Europolu. – „Jest liderem w kategorii współczesnego złośliwego oprogramowania".

Eksperci wskazali, że wyciąganie ogólnych wniosków na temat poszczególnych zagrożeń w cyberprzestrzeni jest jednak bardzo trudne. Wynika w to z faktu różnorodności nie tylko samych narzędzi i taktyki, ale również charakteru samych ugrupowań hakerskich. „Podmioty te różnią się pod względem umiejętności, zdolności czy możliwości adaptacyjnych" – podkreślono w dokumencie.

Zdaniem Europolu cyberprzestępcy z „najwyższej półki" potrafią prowadzić swoją działalność jak „profesjonalne przedsiębiorstwo", podczas gdy mniej wyrafinowane ugrupowania zwykle polegają na gotowych narzędziach oraz sposobach prowadzenia operacji. Skalę problemu podkreśla również fakt nawiązywania współpracy między organizacjami hakerskimi, które często łączą siły, aby wspólnie przeprowadzić określoną kampanię i tym samym zwiększyć jej skuteczność. To z kolei sprawia, że organy ścigania mają znacznie utrudnioną pracę, co jedynie potęguje zagrożenie.

„Ogólnie rzecz biorąc, cyberprzestępcy wykazują wyższy poziom bezpieczeństwa operacyjnego oraz są świadomi tego, jak skutecznie ukryć swoją działalność przed organami ścigania lub firmami zajmującymi się cyberbezpieczeństwem" – wskazano w raporcie.

Głos ekspertów

Catherine De Bolle, dyrektor wykonawczy Europolu, jednoznacznie podkreśliła, że cyberprzestępczość to problem dotykający obywateli, przedsiębiorstwa i organizacje w całej Unii Europejskiej. „Europol odgrywa kluczową rolę w zwalczaniu cyberprzestępczości, współpracując z wieloma partnerami" – wskazała, dodając, że raport powinien zwrócić uwagę na istniejące w sieci zagrożenie i tym samym „uczynić Europę bezpieczniejszą".

Margaritis Schinas, odpowiedzialny za kierowanie pracami Komisji Europejskiej w obszarze Europejskiej Unii Bezpieczeństwa, nie ma wątpliwości, że działalność hakerów w sieci jest jedną z cech „trudnej rzeczywistości". Jego zdaniem obecna transformacja cyfrowa przyczynia się do ewolucji nie tylko społeczeństwa, ale także cyberprzestępczości, która staje się coraz bardziej wyrafinowana. „Nie będziemy szczędzić wysiłków na rzecz zwiększania naszego cyberbezpieczeństwa" – zadeklarował Margaritis Schinas.

Z kolei komisarz UE ds. wewnętrznych Ylva Johansson zwróciła uwagę na fakt, że pandemia koronawirusa miała wpływ na wiele aspektów codziennego życia Europejczyków. „Niestety, wzmocniło to działalność przestępczą w internecie" – wskazała przedstawicielka Komisji Europejskiej. Jak dodała, hakerzy z premedytacją przeprowadzają cyberataki wymierzone w osoby bezrobotne oraz dzieci, których czujność na zagrożenie w sieci jest osłabiona.

Jak walczyć z hakerami?

Według Europolu, aby skutecznie walczyć z cyberprzestępczością konieczna jest skuteczna wymiana informacji, która stanowi podstawę każdej strategii. Dzielenie się wiedzą oraz danymi musi być świadome i w konkretnym celu. Wymaga to również koordynacji, a także współpracy z partnerami państwowymi i prywatnymi. Skuteczna wymiana informacji musi opierać się na ramach prawnych.

Bardzo ważnym aspektem jest także budowanie kultury przejrzystości, która ma szczególne znaczenie w momencie, gdy organizacje lub pojedynczy użytkownicy padają ofiarą hakerów. Poważnym wyzwaniem dla służb jest nakłonienie ofiar cyberataków do zgłaszania incydentów oraz nieukrywanie żadnych informacji w tej kwestii.

Podstawowym elementem walki z cyberprzestępczością jest również – zdaniem Europolu – zapobieganie oraz zwiększanie świadomości na temat zagrożeń w sieci. „Możemy realnie obniżyć wskaźnik skuteczności wielu formom cyberprzestepczości, edukując użytkowników oraz organizacje w zakresie rozpoznawania wrogiej działalności, zanim padną jej ofiarą" – stwierdzili specjaliści w

raporcie.

Czytaj też: Pierwsza ofiara śmiertelna ataku ransomware. Zarzut nieumyślnego spowodowania śmierci