Cyberdefence 24

aut. Szymon Palczewski 05.08.2020

COVID-19 WZMACNIA CYBERPRZESTĘPCZOŚĆ. GLOBALNA „PANDEMIA CYBERATKÓW”

Podczas pandemii koronawirusa hakerzy zredefiniowali swoje cele skupiając się na organizacjach rządowych, instytucjach ochrony zdrowia oraz podmiotach infrastruktury krytycznej. Alarmująca jest również forma cyberataków, których skutki mogą zagrażać zdrowiu i życiu ludzi ze względu na możliwość sparaliżowania placówek medycznych. Cyberprzestępcy bez wahania wykorzystują ludzki strach przed pandemią, generując ogromne straty dla wielu branż.

W raporcie „Cybercrime: Covid-19 Impact”, opracowanym przez Interpol, wyraźnie podkreślono, że pandemia koronawirusa ma głęboki wpływ na krajobraz cyberzagrożeń. „Połączenie światowego kryzysu zdrowotnego z gwałtownym wzrostem działań cyberprzestępczych związanych z Covid-19 stanowi istotne obciążenie dla organów ścigania na całym świecie” – czytamy w raporcie.

Dokument powstał w oparciu o dane ze 194 państw członkowskich i partnerów prywatnych, aby zapewnić kompleksowy przegląd sytuacji związanej z cyberprzestępczością w czasie pandemii. Informacje pozyskiwano w ramach „INTERPOL Global Cybercrime Survey”, która została przeprowadzona w okresie kwiecień-maj bieżącego roku.

Według zamieszczonych w raporcie danych, w przedziale czasowym od stycznia do 24 kwietnia 2020 roku Interpol wykrył 907 000 wiadomości spamowych, 737 incydentów związanych z użyciem zainfekowanego ładunku i 48 000 złośliwych adresów URL – wszystkie wykorzystywały tematykę dotyczącą obecnej pandemii.

Interpol zaobserwował niepokojący trend, w którym hakerzy przedefiniowali swoje cele, aby generować możliwie maksymalne zyski dla siebie i jak największe straty dla ofiary. Cyberprzestępcy nie koncentrują się już głównie na małych firmach i osobach fizycznych, lecz coraz więcej złośliwych kampanii wymierzonych jest w duże korporacje, organizacje rządowe oraz instytucje odpowiedzialne za infrastrukturę krytyczną. Są to podmioty mające kluczowe znaczenie w walce z pandemią koronawirusa.

Covid-19 przyczynił się także do zmiany formy pracy w wielu placówkach. Zdaniem Interpolu to kolejna „zachęta” dla hakerów. Wynika to z faktu nagłego i koniecznego przejścia na pracę zdalną. W związku z tym firmy, instytucje oraz inne organizacje zostały zmuszone do szybkiego wdrażania systemów, sieci i aplikacji, które to umożliwiły. W rezultacie ich jakoś cyberzabezpieczeń nie mogła spełniać najwyższych standardów, co przyczyniało się do powstawania luk i podatności, które sprawnie wykorzystywali hakerzy. Do czego? Głównie do kampanii nastawionych na generowanie środków finansowych, kradzież danych czy powodowanie zakłóceń.

Analiza Interpolu skupia się wokół takich cyberzagrożeń jak: oszustwa internetowe i phishing, cyberatak z użyciem złośliwego oprogramowania (ransomware oraz kampanie DDoS), zbieranie danych, złośliwe witryny czy dezinformacja.

Oszustwa i phishing

Hakerzy bardzo sprawnie wykorzystują pandemię do zwiększenia szans na powodzenie cyberataków. Dostosowali taktykę i metody działania do obecnej sytuacji. Skutecznie posługują się wiadomościami phishingowymi o tematyce Covid-19, podszywając się bardzo często pod organy państwowe oraz służbę zdrowia. W ten sposób hakerzy zachęcają swoje ofiary do interakcji i podania na przykład wrażliwych danych czy pobrania zainfekowanego pliku.

Ransomware oraz DDoS

„Cyberprzestępcy coraz częściej wykorzystują złośliwe oprogramowanie przeciwko infrastrukturze krytycznej i instytucjom opieki zdrowotnej ze względu na potencjalny duży wpływ i korzyści finansowe" – czytamy w raporcie Interpolu. Ransomware czy też kampanie DDoS mogą wywoływać poważne zakłócenia lub nawet całkowicie sparaliżować funkcjonowanie danej placówki, co w okresie pandemii koronawirusa może mieć bezpośredni wpływ na zdrowie i życie ludzi.

Kradzież danych

Interpol zaobserwował regularny wzrost cyberataków, w ramach których hakerzy wykorzystują złośliwe oprogramowanie przeznaczone do zbierania danych, w tym trojanów zdalnego dostępu, wirusów bankowych czy narzędzi szpiegowskich. Jak wynika z dokumentu, cyberprzestępcy, wykorzystując informacje dotyczące pandemii jako przynętę, infiltrują systemy ofiary w celu włamania do sieci, kradzieży danych, przekierowania pieniędzy i tworzenia botnetów.

Złośliwe domeny

Hakerzy są świadomi potrzeb, jakie posiada społeczeństwo w okresie pandemii. Jednostki poszukują materiałów medycznych i informacji na temat Covid-19. W związku z tym cyberprzestępcy sprawnie wykorzystują ludzki strach oraz ciekawość tworząc fikcyjne witryny internetowe, zawierające słowa kluczowe takie jak „koronawirus" czy „Covid-19". Spreparowane strony stanowią podstawę wielu kampanii hakerskich.

Dezinformacja

„Coraz więcej fałszywych wiadomości szybko rozprzestrzenia się wśród opinii publicznej" – wskazuje Interpol. Zjawisko to jest „napędzane" niepewną sytuacją społeczno-gospodarczą na świecie, a także niezweryfikowanymi informacjami oraz niezrozumieniem istniejącego zagrożenia. Tworzone teorie spiskowe przyczyniły się do wywołania uczucia strachu i lęku, co skutecznie wykorzystują hakerzy w swoich działaniach.

Trendy w regionach świata

Interpol zauważył, że dominujące formy cyberprzestępczości różnią się w zależności od regionu. Pomimo że w skali globalnej wzrost cyerataków jest zauważalny ich charakter różni się w zależności od konkretnego obszaru, w jakim działają hakerzy.

- Kontynent afrykański – specjaliści zauważyli gwałtowny wzrost płatności elektronicznych lub bezgotówkowych od początku pandemii, co stworzyło atrakcyjne pole do działania cyberprzestępców. Co więcej, zaobserwowano większą liczbę ataków phishingowych, co wynika z konieczności przejścia na tryb pracy zdalnej. Dodatkowo „wzrósł obieg fałszywych wiadomości związanych z COVID-19 w mediach społecznościowych" – czytamy w raporcie.

- Ameryka Północna i Południowa – na tym obszarze pojawił się gwałtowny wzrost liczby kampanii

phishingowych i oszustw związanych z pandemią koronawirusa. Jedną z dominujących form cyberprzestępczości jest kradzież poufnych danych za pomocą uzyskania zdalnego dostępu do sieci i systemów. „Kampania ransomware przeprowadzona głównie za pośrednictwem złośliwego oprogramowania LOCKBIT dotyka obecnie średniej wielkości firmy w niektórych krajach tego regionu” – dodaje Interpol.

- Azja i Południowy Pacyfik – wśród głównych trendów w tym obszarze należy wskazać na kampanie oszustw i phishingu związane z koronawirusem, a także nielegalną sprzedaż internetową fałszywych materiałów medycznych, leków i środków ochrony osobistej. Cyberprzestępcy wykorzystują również luki w zabezpieczeniach narzędzi telekonferencyjnych. Co więcej, bardzo dużym problemem jest rozpowszechnianie fake newsów na temat Covid-19.

- Europa – dwie trzecie państw członkowskich z Europy zgłosiło znaczny wzrost liczby złośliwych domen poruszających tematykę pandemii. Interpol nie ma wątpliwości, że hakerzy wykorzystują Covid-19 jako przynętę do wdrażania oprogramowania ransomware w instytucjach opieki zdrowotnej, będącej podstawą walki z koronawirusem. „Coraz częściej występuje kopiowanie oficjalnych rządowych stron internetowych w celu kradzieży wrażliwych danych użytkowników, które można później wykorzystać w kolejnych cyberatakach” – czytamy w raporcie.

- Bliski Wschód – podstawowym zagrożeniem w tym regionie są złośliwe kampanie w mediach społecznościowych. Służą one jako kanał rozpowszechniania fake newsów na temat Covid-19. Co więcej, platformy social mediów są często rynkiem nielegalnej sprzedaży produktów farmaceutycznych na koronawirusa. Intrepol podkreślił również trend związany z rosnąca liczbą ataków phishingowych, oszustw internetowych oraz tworzeniem nowych fałszywych domen, które deklarują udostępnianie „prawdziwych” danych i informacji na temat pandemii.

Cyberprzestępcy nieustannie rozwijają swoje zdolności i sprawie wykorzystują ludzki strach związany z niestabilną sytuacją społeczną i gospodarczą, co jest następstwem pandemii koronawirusa. Skalę zagrożenia potęguje większa zależność od łączności i infrastruktury cyfrowej ze względu na konieczność przejścia w tryb pracy zdalnej. To wszystko jedynie zachęca hakerów do prowadzenia złośliwych operacji.

Czytaj też: Pozytywny skutek COVID-19? Rośnie wiedza na temat cyberbezpieczeństwa