CYBERZAGROŻENIA Z CHIN, ROSJI I... USA. 2021 WIDZIANY W CIEMNYCH BARWACH

Największym źródłem zagrożeń w sieci Orange Polska w 2020 roku były Chiny, Rosja oraz Stany Zjednoczone – wynika z raportu CERT Orange Polska. Niebezpieczeństwo wynikało głównie z cyberataków typu DDoS, kampanii phishingowych i infekcji złośliwym oprogramowaniem. Jednym z podstawowych kanałów działania hakerów były social media, w tym głównie Facebook. W przekroju bieżącego roku nie można liczyć na spadek zagrożenia, co warunkuje m.in. pandemia koronawirusa. Jakie trendy czekają nas w dalszej części 2021 roku?

DDoS

W „Raporcie CERT Orange Polska za rok 2020" jednoznacznie podkreślono, że ataki typu odmowa dostępu (ang. Distributed Denial of Service – DDos) nieustannie pozostają jednym z najprostszych i najpopularniejszych rodzajów cyberzagrożeń występujących w sieci Orange Polska, a przy tym najbardziej niebezpiecznych i groźnych w skutkach. Jak wskazują specjaliści, podstawowym celem tego typu kampanii jest sparaliżowanie infrastruktury ofiary.

Zgodnie z zaprezentowanymi w dokumencie danymi, CERT Orange Polska w 2020 roku reagował w związku z atakami DDoS ponad 65 tys. razy w ramach sieci stacjonarnej i 12,5 tys. w przypadku sieci mobilnej. „Od kilku już lat obserwujemy w CERT, że jednym z celów ataków są gracze on-line, a atak ma spowodować wyeliminowanie ich z gry lub takie opóźnienie w transferze danych, które nie pozwoli atakowanemu zrealizować celu. Ataki te są coraz mniej skuteczne (bo stale doskonalimy mechanizmy ochrony), ale powodują, że w zaatakowanym segmencie sieci przez krótką chwilę niektórzy użytkownicy mogą zaobserwować zmniejszoną wydajność dostępu do Internetu" – czytamy w raporcie.

Specjaliści zwracają uwagę, że wybuch pandemii i związana z tym popularyzacja pracy zdalnej przyczyniła się do wzrostu liczby incydentów w okresie od połowy marca ub.r. Co ciekawe, wraz z luzowaniem obostrzeń, spadała także aktywność hakerów. Ponowne ograniczenia nakładane przez rząd intensyfikowały wrogie działania w sieci.

Największy cyberatak DDoS w minionym roku został wymierzony w infrastrukturę komunikatora TeamSpeak, znajdującą się w północnej części Polski. Incydent wystąpił w czerwcu 2020 roku i miał szacowaną wielkość 303 Gbps, 88 Mpps i trwał około 8 minut – wskazano w raporcie. Jak dodano, cyberatak został skutecznie odparty, lecz pomimo to eksperci nazwali go „największym znanym w historii polskiego interentu atakiem DDoS".

Phishing

Specjaliści w dokumencie odnieśli się do kwestii phishingu. Mowa tutaj o kampaniach hakerskich, których celem jest wyłudzenie określonych danych lub informacji, umożliwiających np. dostęp do kont

bankowych. Podczas tego typu działań zewnętrzne podmioty wykorzystują m.in. strony internetowe czy bramki płatnicze, określane mianem „refereów", czyli tzw. „źródeł phishingu". Jednym z głównych jest Facebook (używany w ponad 80% przypadków). „Pokazuje to, jak bardzo sieci społecznościowe zaangażowały nas jako użytkowników internetu oraz jak za tym zaangażowaniem podążyli twórcy złośliwych treści i mechanizmów oszukiwania odbiorców" – czytamy w raporcie CERT Orange Polska.

„Mechanizmy działania większości z tych kampanii i stron sprowadzają się do tego, żeby skłonić użytkownika do wejścia na taką stronę i podania swoich danych (zazwyczaj danych logowania do bankowości internetowej, danych kart płatniczych, danych logowania do portali społecznościowych lub poczty e-mail)" – tłumaczą specjaliści. „Cel jest za każdym razem ten sam – przejęcie kont użytkowników i kradzież wszystkiego, co na nich da się ukraść, czyli pieniędzy (w postaci przelewów, kodów BLIK, transakcji kartą płatniczą), tożsamości, kont dostępu do innych usług i serwisów, czy nawet trofeów w grach on-line" – dodają.

Złośliwe oprogramowanie

Jak wskazano w raporcie, tylko w 2020 roku CERT Orange Polska przeprowadził łącznie 290 kampanii informujących o infekcjach i zagrożeniach, które objęły ponad 61 tys. użytkowników. Wśród najczęściej występujących (TOP 4) typów wirusów w sieci stacjonarnej specjaliści wskazali na: Mirai (6%), DanaBot (5%), RAT (5%) oraz TrickBot (4%). Z kolei w odniesieniu do mobilnych rozwiązań wygląda to następująco: Mirai (7%), DanaBot (4%), RAT (3%) i TrickBot (2%).

Gdzie znajduje się główne źródło zagrożenia? Eksperci jednoznacznie mówią o dominacji Chin, USA i Rosji w tym zakresie. „Należy pamiętać, że duży udział Stanów Zjednoczonych wynika głównie z lokalizacji w tym kraju dużych dostawców usług chmurowych. W przypadku pozostałych dwóch państw, obserwujemy na naszych honeypot'ach ataki pochodzące z sieci dużych ISP. Najczęściej występujący typ ataku to atak brute force na konta administratorskie" – wyjaśniono w raporcie.

Inne rodzaje zagrożeń

W dokumencie podkreślono, że istnieją takie typy cyberataków, przed którymi specjaliści nie są w stanie ochronić użytkowników. Mowa tu o m.in. oszustwie polegającym na instalacji oprogramowania, umożliwiającego zdalny dostęp do komputera. „Mechanizm oszustwa wygląda tak: bazując na informacjach skradzionych z jednej z giełd kryptowalutowych oszuści kontaktują się z użytkownikiem i proponują mu „wspaniałą" inwestycję. W trakcie finalizowania transakcji okazuje się jednak, że występują nieprzewidziane trudności, ale oszust oczywiście pomoże je przezwyciężyć. W tym celu niezbędne okazuje się najpierw zainstalowanie oprogramowania zdalnego dostępu, a następnie zalogowanie na konto bankowe lub portfel bitcoinowy. I w tym właśnie momencie, na oczach użytkownika oszust dokonuje kradzieży" – opisują cały proces specjaliści CERT Orange Polska.

To jednak nie koniec. Eksperci zwracają również uwagę na niezabezpieczone DNS i NTP. Są one często wykorzystywane przez hakerów do cyberataków Reflected DDoS, które są wymierzone w inne cele. „Jeśli usługi te zostaną faktycznie wykorzystane w atakach DDoS, ich właścicielom grożą co najmniej czasowe ograniczenia w dostępie do Internetu (ze względu na bezpieczeństwo sieci Internet) lub nawet konsekwencje prawne" – czytamy w raporcie.

Równie niebezpieczne – zdaniem specjalistów – są dostępne w sieci panele logowania do urządzeń, jakie użytkownicy podłączyli do swojej infrastruktury (np. modemy, drukarki, kamerki). To zachęta dla hakerów, ponieważ tego typu panel jest widoczny w internecie. W ten sposób wiedzą, że podjęcie określonych działań może pozwolić im na uzyskanie nieautoryzowanego dostępu do określonego sprzętu, a następnie przejęcia kontroli nad pozostałymi częściami infrastruktury.

Co nas czeka w 2021 roku?

Zgodnie z raportem CERT Orange Polska w bieżącym roku należy spodziewać się wzrostu złośliwych aplikacji mobilnych w krajobrazie zagrożeń, a także nieustannie wysokiego udziału malware RAT w odniesieniu do infrastruktury stacjonarnej. Jak precyzują specjaliści, będą one powiązane z atakami socjotechnicznymi.

Co również warto odnotować, to także wzrost liczby kampanii typu vishing, smishing oraz phishing. W przypadku tych ostatnich coraz częściej hakerzy będą wykorzystywać social media oraz komunikatory internetowe.

Ponadto, utrzyma się skala operacji bazujących na socjotechnice, związanych ze zdalnym dostępem do infrastruktury firm, poprzez np. użycie backdoorów. „Trend jest szczególnie wyraźny w czasie pandemii, gdzie mogą tak naprawdę wystąpić różne wektory ataku, również próby pozyskania danych do konta firmowego" – czytamy w raporcie.

Eksperci ostrzegają także przed malvertisment w cyberatakach, zwiększeniem zaawansowania i skomplikowania operacji phishingowych oraz rozszerzeniem skali incydentów związanych z kradzieżą portfeli kryptowalut. Co więcej, w dokumencie jednoznacznie wskazano, że należy spodziewać się rekordów w przypadku kampanii DDoS, utrzymania zakresu ataków na „sztuczną inteligencję" oraz prób wyłudzenia informacji płatniczych.

Warto także odnotować, że zgodnie z przewidywaniami czas trwania ataków phishingowych ma skrócić się do kilkunastu lub nawet kilku minut na kampanię. Specjaliści mówią również o „dużym" udziale ransomware w operacjach wymierzonych w firmy i jednostki w przekroju bieżącego roku.

Czytaj też: Ekspert: ostatnie cyberataki przesuwają nas w kategorię aktów wojny