Cyberdefence 24

aut. Szymon Palczewski 11.09.2020

HAKERZY ZAKŁÓCĄ WYBORY PREZYDENCKIE W USA? FALA CYBERATAKÓW Z ROSJI, CHIN I IRANU

Amerykańskie środowisko polityczne znajduje się „pod ostrzałem" serii cyberataków, które są prowadzone przez ugrupowania hakerskie największych przeciwników Stanów Zjednoczonych. Kampanie trwają nieprzerwanie od wielu miesięcy, a ich podstawowym celem jest zakłócenie listopadowych wyborów prezydenckich w USA.

W ostatnich tygodniach Microsoft wykrył cyberataki wymierzone w osoby i organizacje zaangażowane w listopadowe wybory prezydenckie w Stanach Zjednoczonych. Operacje hakerskie ukierunkowano zarówno w kampanię kandydata Demokratów Joe Bidena, jak i obecnego prezydenta USA Donalda Trumpa – informuje w oficjalnym komunikacie Microsoft.

„Działalność, o której informujemy, jasno pokazuje, że zagraniczne grupy hakerskie zintensyfikowały swoje wysiłki w celu uderzenia w wybory w 2020 roku" – czytamy na blogu amerykańskiego giganta.

Specjaliści wskazują, że większość cyberataków została wykryta i skutecznie zatrzymana przez innowacyjne narzędzia bezpieczeństwa. „Bezpośrednio powiadomiliśmy osoby, które były celem, aby mogły podjąć działania w rzecz własnej ochrony" – dodają eksperci.

W komunikacie podkreślono, że operacje hakerskie wymierzono nie tylko w kandydatów na fotel prezydenta USA i ich sztaby, ale także osoby, które się z nimi konsultują w kluczowych sprawach. To wszystko sprawia, że zagrożenie dotyczy wszystkich ze środowiska politycznego zaangażowanych w proces wyborczy. Ryzyko będzie zwiększać się z każdym dniem aż do rozstrzygnięcia kampanii.

Rosyjskie uderzenie

W komunikacie wyróżniono grupę hakerską Strontium (inna nazwa Fancy Bear), którą uznano za jedno z poważniejszych zagrożeń dla procesów wyborczych w USA. To rosyjski podmiot, jaki Microsoft już wcześniej powiązał z kampaniami mającymi na celu zakłócanie procesów demokratycznych w Stanach Zjednoczonych. „Zidentyfikowano ją (grupę - przyp. red.) jako główną organizację odpowiedzialną za ataki na kampanię prezydencką w 2016 roku" – czytamy w komunikacie firmy.

Cyberataki ze strony Strontium trwają od września 2019 roku do dnia dzisiejszego. Hakerzy podczas operacji – podobnie jak to miało miejsce 4 lata wcześniej – zbierają dane do logowania osób będących celem lub naruszają ich konta, aby w ten sposób móc następnie wykradać dane o znaczeniu wywiadowczym bądź zakłócać określone procesy i operacje.

Działania Strontium zostały wymierzone w ponad 200 organizacji, które są bezpośrednio lub pośrednio związane z nadchodzącymi wyborami oraz w podmioty polityczne działające na terenie Europy. Wśród nich znajdują się: konsultanci współpracujący z Demokratami i Republikanami, think tanki, takie jak The German Marshall Fund of the United States i inne organizacje wspierające, krajowe i stanowe

organizacje partyjne w USA, brytyjskie partie polityczne, w tym The European People's Party.

Kilkumiesięczna obserwacja kampanii hakerskiej pozwoliła specjalistom Microsoftu przypisać złośliwą działalność grupie Strontium. Analiza dodatkowo wykazała, że jej członkowie rozwinęli swoją taktykę od 2016 roku, wprowadzając nowe narzędzia oraz możliwości ukrycia operacji.

„W 2016 roku grupa polegała głównie na spear phishingu, aby przechwytywać dane uwierzytelniające ludzi" – wyjaśniają specjaliści. „W ostatnich miesiącach zaangażował się w ataki >brutalnej siły<".

Ofiarami rosyjskich hakerów są między innymi pracownicy firmy SKDKnickerbocker, odpowiedzialnej za strategię kampanii Joe Bidena. Osoba zaznajomiona za sprawą, która pragnie pozostać anonimowa, wskazała dla agencji Reutera, że hakerzy nie uzyskali dostępu do sieci przedsiębiorstwa. „Są dobrze zabezpieczone, więc nie doszło do incydentu" – podkreśliła.

Rzecznik Kremla Dmitrij Pieskow odrzucił zarzuty jakoby Rosja stała za cyberatakmi, uznając je za całkowite „bzdury". Oczywiście należy pamiętać, że Moskwa wielokrotnie zaprzeczała faktom, wskazując, że nie wykorzystuje hakerów do realizacji własnych celów.

Chiny – kluczem jest informacja

Microsoft, badając serię cyberataków na amerykańskie środowisko polityczne, zaobserwował również wysoką aktywność chińskiej grupy Zirconium. Jej głównym zadaniem było zdobycie informacji o organizacjach i podmiotach powiązanych z listopadowymi wyborami w Stanach Zjednoczonych. „Wykryliśmy tysiące ataków między marcem a wrześniem 2020 roku, które wywołały prawie 150 incydentów" – czytamy w komunikacie.

Cele Zirconium w ostatnich miesiącach można podzielić na dwie kategorie. Pierwszą stanowią osoby ściśle związane z kampaniami kandydatów na prezydenta USA oraz ich sztabami. Przykładem mogą być nieudane operacje wymierzone w środowisko Joe Bidena, które odbywały się między innymi za pomocą fikcyjnych kont e-mail. „Grupa zaatakowała również co najmniej jedną prominentną osobę związaną wcześniej z administracją Trumpa" – wskazuje Microsoft.

Druga kategoria obejmuje wybitne osobistości zajmujące się sprawami międzynarodowymi oraz naukowców z ponad 15 uniwersytetów. Hakerzy uderzyli również w organizacje zajmujące się polityką, w tym Atlantic Council i Stimson Center.

„Zirconium używa tak zwanych błędów internetowych lub sygnałów nawigacyjnych w sieci Web, powiązanych z domeną, którą wykupiła i zapełniła treścią" – tłumaczą eksperci. „Następnie wysyła powiązany adres URL w treści wiadomości e-mail lub w załączniku na docelowe konto".

Iran wie, co robi

Microsoft zidentyfikował także wysoką aktywność irańskich hakerów, działających w ramach grupy Phosphorus. Prowadzą oni głównie kampanie cyberszpiegowskie, które są wymierzone w szeroką gamę podmiotów powiązanych z interesami geopolitycznymi, gospodarczymi lub prawami człowieka w regionie Bliskiego Wschodu.

W ostatnim czasie hakerzy usiłowali uzyskać dostęp do kont osobistych lub służbowych osób zaangażowanych bezpośrednio lub pośrednio w wybory prezydenckie w USA. „Od maja do czerwca 2020 roku grupa Phosphorus bezskutecznie próbowała zalogować się na konta urzędników obecnej administracji oraz samego Donalda Trumpa" – podkreślają eksperci amerykańskiego giganta.

Opublikowane wyniki analiz i obserwacji przeprowadzonych w ostatnim czasie przez Microsoft

pokazują, że wiele aktorów jest żywo zainteresowanych ingerencją w amerykańskie wybory prezydenckie. Od ich wyników zależy wygląd przyszłej sceny politycznej w tym kraju, dlatego też są one atrakcyjnym celem wrogich państw, które za pomocą kampanii hakerskich „chcą coś ugrać". Obserwacje specjalistów są potwierdzeniem, że ryzyko poważnego incydentu podczas listopadowych wyborów jest wysokie, a złośliwe operacje rozpoczęły się wiele miesięcy wcześniej i trwają do dziś. Należy spodziewać się, że z każdym dniem intensywność cyberataków będzie wzrastać.

Czytaj też: Amerykanie drżą o bezpieczeństwo wyborów. Służby wskazują na kolejne państwa