Wielu przypuszcza, że cyberataki nie mogą zabijać ludzi. To nieprawda

Cyberataków nie należy lekceważyć i traktować jako niewinnej zabawy młodych ludzi. To poważne przestępstwa, które mogą prowadzić również do śmierci.

- Grupa ekspertów ostrzega, że Korea Północna mogłaby wykorzystać techniki groźnych cyberataków.
- Cyberprzestępcy mogą na przykład przejąć kontrolę nad oczyszczalnią wody i zmienić mieszankę chemiczną, aby była toksyczna…
- …albo przeniknąć do systemów komputerowych elektrowni jądrowej, powodując poważne awarie.

Koreański dziennikarz Jung Min-ho pisze:

> *Jednym z najbardziej niedocenianych zagrożeń bezpieczeństwa pochodzących z Korei Północnej są jej możliwości cyberataków. Wielu przypuszcza, że hakerzy nie mogą zabijać ludzi. Ale mogą.*

Cyberprzestępcy mogą przejąć kontrolę nad oczyszczalnią wody i zmienić mieszankę chemiczną, aby była toksyczna, lub mogą przeniknąć do systemów komputerowych elektrowni jądrowej, powodując poważne awarie. W ostatnich latach w wielu częściach świata podejmowano próby takich cyberataków, niektóre z nich zakończyły się pośrednio śmiercią lub obrażeniami.

Grupa ekspertów ostrzega, że □□Korea Północna mogłaby wykorzystać takie techniki, gdyby wybuchła wojna na Półwyspie Koreańskim, w raporcie RAND Corporation zatytułowanym “Charakterystyka zagrożeń związanych z północnokoreańską bronią chemiczną i biologiczną, impulsem elektromagnetycznym i zagrożeniami cybernetycznymi”.

Choi Kang, prezes Asan Institute for Policy Studies i jeden ze współautorów wspólnego raportu napisanego z think tankiem RAND Corporation, powiedział na konferencji prasowej w instytucie w Seulu we wtorek.

> *Infrastruktura w Korei Południowej wydaje się być bardzo podatna na cyberataki Północy. Widzieliśmy kilka przypadków w systemach bankowych… Ale co z inną infrastrukturą, taką jak zaopatrzenie w wodę lub elektryczność? To spowodowałoby chaos.*

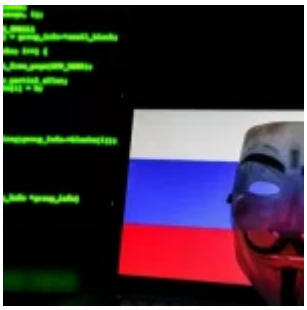
Możliwe scenariusze

Jednym z możliwych scenariuszy może być wykolejenie pociągów załadowanych śmiercionośnymi chemikaliami. Inne możliwe cele obejmują tamy, szpitale, lotniska i sieci energetyczne, których wiele systemów komputerowych zostało już wcześniej przenikniętych przez Koreę Północną.

Raport mówi, że domniemane rozmieszczenie wirusa Stuxnet przez Stany Zjednoczone i Izrael w celu uszkodzenia irańskich wirówek do wzbogacania nuklearnego oraz rosyjski program złośliwego oprogramowania towarzyszący inwazji na Ukrainę w tym roku mogą służyć jako przykłady do naśladowania i rozwijania przez Koreę Północną.

Źródło

Anonymous włamali się do kolejnego rosyjskiego banku. 800 GB danych



Anonymous poinformowało, że udało im się włamać do bazy danych banku kraju-agresora Rosji. Zagrozili wyciekiem do sieci 800 GB poufnych informacji.

Stało się to znane z anonimowej wiadomości na portalu społecznościowym Twitter . Został opublikowany w poniedziałek 18 kwietnia.

Mówimy o Społecznym Banku Handlowym w Petersburgu – PSCB. Klientami tej instytucji finansowej są rosyjscy oligarchowie.

https://twitter.com/Anonymous_Link/status/1516116675078377474?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1516116675078377474%7Ctwgr%5E%7Ctwcon%5Es1
„Anonymous złamał inny rosyjski bank. Planujemy uwolnić 800 GB poufnych danych! Zespół hakerów podpisujących papiery wartościowe Anonymous złamał rosyjski bank JSC Bank PSKB, z którego korzystają oligarchowie" – podał portal społecznościowy.

W przeddzień okazało się, że Anonymous złamał jedną z firm Gazpromu . Hakerzy umieścili w Internecie 768 000 listów od

pracowników Gazprom Linde Engineering, które są częścią rosyjskiego giganta gazowego. Firma specjalizuje się w projektowaniu obiektów dla rafinerii ropy naftowej.

Ponadto otrzymali dostęp do 700 GB danych rządu rosyjskiego. Anonymous przejął także kontrolę nad systemem monitoringu Kremla i pokazał pierwszy materiał filmowy z wnętrza.

Światowe Forum Ekonomiczne naciska na Wielki Reset poprzez „cyberatak o cechach podobnych do COVID”

Światowe Forum Ekonomiczne (WEF) to międzynarodowa organizacja pozarządowa rzekomo poświęcona ulepszaniu świata poprzez biznes, politykę i środowisko akademickie. Ostatnio zagłębia się w świat cyberbezpieczeństwa. W rzeczywistości WEF dąży do Wielkiego Resetu za pomocą „ cyberataku o cechach podobnych do COVID”.

WEF odegrał wiodącą rolę w plandemii COVID-19. Naciskało na paszporty szczepionkowe, cyfrowe śledzenie kodów kreskowych i, co najważniejsze, Wielki Reset. Teraz ostrzega świat przed możliwym cyberatakiem obejmującym cały świat, który może sparaliżować globalny system finansowy.

WEF przygotowuje ludzi do oczekiwania cyberataku obejmującego cały świat

Na początku 2021 r. WEF Center for Cybersecurity ogłosiło Cyber Polygon 2021. To internetowa konferencja poświęcona cyberbezpieczeństwu. Tegoroczny Cyber Polygon ma jeden cel: dowiedzieć się, jak wygląda „cyberatak z cechami podobnymi do COVID".

We wcześniejszych wersjach WEF powiedziało, że Cyber Polygon 2021 skupi się na oprogramowaniu ransomware, podatności globalnego łańcucha dostaw na cyberataki i waluty cyfrowe. WEF obiecało również przeprowadzenie „ćwiczeń szkoleniowych na żywo", które są odpowiedzią na „ukierunkowany atak łańcucha dostaw na ekosystem korporacyjny w prawdziwym życiu".

„Wszyscy wiemy, ale wciąż nie zwracamy na niego wystarczającej uwagi, przerażający scenariusz kompleksowego cyberataku, który całkowicie wstrzymałby dostawy energii, transport, usługi szpitalne, nasze społeczeństwo jako całość" – powiedział Klaus Schwab, założyciel i prezes wykonawczy WEF. „Kryzys COVID-19 byłby pod tym względem postrzegany jako niewielkie zakłócenie w porównaniu z poważnym cyberatakiem".

Schwab dodał, że ważne jest, aby WEF wykorzystał trwającą pandemię COVID-19, aby „przemyśleć lekcje społeczności cyberbezpieczeństwa, aby wyciągnąć i poprawić naszą nieprzygotowanie na potencjalną cyberpandemię".

Schwab wygłosił te komentarze w zeszłym roku, pokazując, że WEF od pewnego czasu planuje przygotowywać ludzi do Wielkiego Resetu wywołanego cyberatakiem. 9 lipca, w dniu rozpoczęcia konferencji Cyber Polygon, Schwab powtórzył swoje sianie strachu, przypominając ludziom o ostatnich cyberatakach, które miały miejsce.

„W ciągu ostatnich kilku miesięcy widzieliśmy na przykład ataki ransomware wymierzone w szpitale, infrastrukturę krytyczną, systemy szkolne, sieć energetyczną i wiele innych

podstawowych usług” – powiedział.

„Ataki ransomware są złożone, a przedsiębiorstwa przestępcze zwiększają swoją skalę i wpływ. Podkreśla to potrzebę ustrukturyzowanego wielostronnego, wielostronnego podejścia do zabezpieczenia naszego społeczeństwa przed nimi”.

Trwają ogólnoświatowe ćwiczenia WEF w zakresie cyberpandemii

Ćwiczenie szkoleniowe Cyber Polygon składa się z ponad 200 zespołów z 48 krajów. Firmy takie jak IBM, Santander i Ernst and Young wysłały swoje zespoły ds. bezpieczeństwa cybernetycznego, aby wziąć udział w tym ogólnoświatowym ćwiczeniu.

„Nieuniknione jest, że pewnego dnia dojdzie do większego ataku”, powiedział John Sancenito, prezes firmy konsultingowej ds. bezpieczeństwa z siedzibą w Pensylwanii. „To, o czym mówi się dzisiaj i w ciągu najbliższych kilku dni, jest potencjalną sytuacją w świecie rzeczywistym”.

Sancenito jest zainteresowane tematem tegorocznego ćwiczenia na żywo. Jeśli cyberatak wycelowany jest w łańcuch dostaw w Stanach Zjednoczonych, może wpłynąć na codzienne życie ludzi poprzez zamknięcie infrastruktury krytycznej, takiej jak sieć energetyczna lub oczyszczalnie ścieków.

„Co byś zrobił, gdybyś nie mógł uzyskać dostępu do swoich kont bankowych, Internetu lub nagle przestał działać telefon komórkowy? Są to rzeczy, które ludzie naprawdę muszą przemyśleć, ponieważ pewnego dnia możemy stanąć w obliczu takiego kryzysu” – powiedział Sancenito.

Ćwiczenie na żywo Cyber Polygon trwa kilka dni. W chwili obecnej trwa nadal.

Artykuł przetłumaczono z: newstarget.com

Wyciekły dokumenty: KPCh wykorzystała płatnych trolli do przeciwdziałania wiadomościom o epidemii pomoru świń w Internecie

Seria wewnętrznych dokumentów chińskich władz cenzurujących ujawniła, w jaki sposób trolle internetowe są wykorzystywane aby manipulować opinią publiczną na korzyść chińskiego reżimu.

Zapisy z miejskiego oddziału Luoyang Administracji Cyberprzestrzeni – głównej chińskiej agencji cenzury internetowej – pokazują, że władze wynajęły internetowe trolle do pisania postów w mediach społecznościowych wychwalających władze. Dokumenty wyciekły przez zaufane źródło.

Tym trollom zapłacono 11 juanów (około 1,62 $) za każdy post, który napisali.

Manipulacja opinią publiczną

Luoyang to miasto położone w prowincji Henan w środkowych Chinach.

W połowie lutego 2019 r. Wokół firmy Sanquan Food z siedzibą w Henan wybuchł skandal dotyczący bezpieczeństwa

żywności. Stwierdzono, że pierogi tej marki zawierają ślady wirusa wywołującego afrykański pomór świń (ASF).

ASF po raz pierwszy wybuchł wśród populacji świń w Chinach w sierpniu 2018 roku i szybko rozprzestrzenił się po całym kraju. ASF jest śmiertelny dla świń i wieprzy, ale nie ma wpływu na ludzi. Zwierzęta hodowlane są zwykle poddawane ubojowi, aby zapobiec rozprzestrzenianiu się choroby.

Wielu chińskich rolników używa ludzkich odchodów jako nawozu. Jeśli taki nawóz zawiera aktywne wirusy ASF, może zanieczyścić źródła wody i potencjalnie przenosić chorobę na więcej świń.

Informacje o skażonych pierogach szybko rozprzestrzeniły się na chińskich platformach społecznościowych, zmuszając władze do publicznego przyznania się do incydentu.

16 lutego 2019 r. wszystkie internetowe i fizyczne sklepy spożywcze w kraju zdjęły pierogi Sanquan z półek.

Administracja Luoyang Cyberspace zgłosiła władzom miasta, jak wynajęte trolle internetowe próbowały manipulować opinią publiczną po skandalu żywnościowym w Sanquan.

Jeden troll z internetowym pseudonimem „Qingqi Suoyou” napisał: „Od czasu pierwszej [na świecie] epidemii ASF około sto lat temu, żaden człowiek nie został zarażony wirusem ASF. Tak więc wirus ASF nie wpłynie na produkty wieprzowe. Możesz jeść mięso i produkty z nim związane”.

Zrzut ekranu z komentarzem opublikowanym przez wynajętego trolla, mającym na celu przeciwdziałanie negatywnym wiadomościom o produktach wieprzowych chińskiej firmy spożywczej zawierającej wirusa afrykańskiego pomoru świń.
Inny wynajęty troll o imieniu „Ruguo” napisał: „Wirus ASF zostanie zabity w wysokich temperaturach. Możesz jeść [pierogi], gotując je w całości.”

Inni próbowali bagatelizować wiadomości jako plotki. Wynajęty troll o internetowej nazwie „Qinghe” napisał: „Nie wierz w plotki i nie rozpowszechniaj ich. Wszystkie duże przedsiębiorstwa mogą prześledzić źródło użytych surowców”.

Niektórzy próbowali wykorzystać okazję, by chwalić władze.

Troll „Kantaiyang” napisał: „Nasz kraj zawsze traktuje bezpieczeństwo żywności jako coś bardzo ważnego. Wierzę, że rząd udzieli naszym ludziom odpowiedzi [o źródle wirusa]”.

„Hai’ai” napisał: „Nie możemy wątpić, że chińska Państwowa Administracja ds. Żywności i Leków oraz Sanquan Food są proaktywne w obliczu problemu. Najważniejsze jest rozwiązanie problemu. Nie powinniśmy wszystkiego kwestionować, a spokojnie czekać”.