Lolifox – kto za nim stał i co się z nim stało?

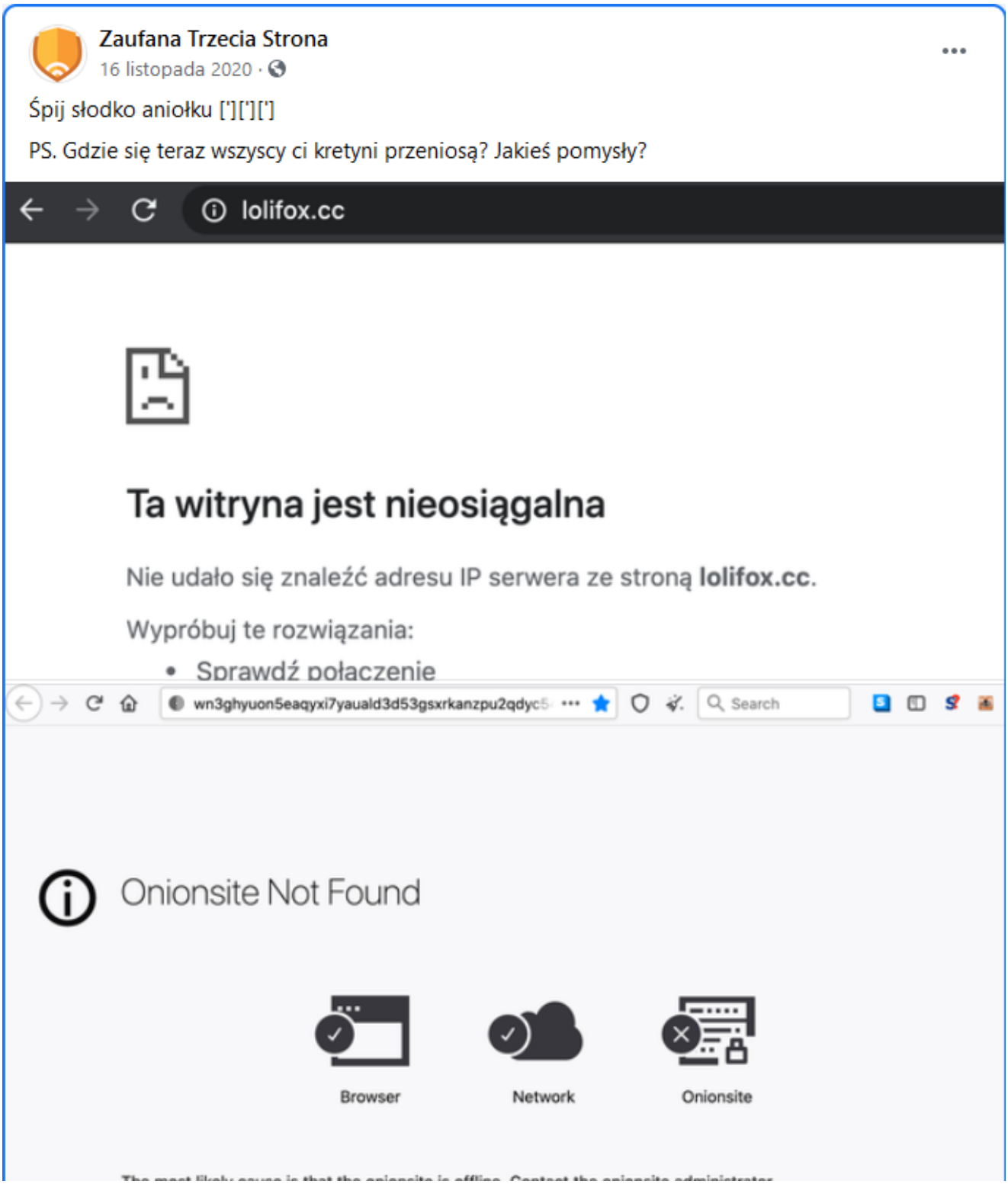
payload.pl/co-sie-stalo-z-lolifoxem/

June 21, 2021

K…&#a! co się stało? Czemu Lolifox nie działa? Czy to już koniec?! – takie pytania można było znaleźć w sieci w połowie listopada 2020, po nagłym zniknięciu jednego ze znanych for cyberprzestępczych w Polsce. Przyjrzyjmy się, kto mógł za tym stać.

Lolifox to forum w sieci Tor budzące wiele kontrowersji z uwagi na poruszaną na nim tematykę (przestępczość, ataki hakerskie, pornografia itp.). To tzw. chan, czyli forum obrazkowe (wątki zamieszczane są w formie katalogów). W sieci niejednokrotnie pisano, że nie da się „odzobaczyć" tego, co się na nim przeczyta. O Lolifoxie pisaliśmy już tutaj i tutaj. Na jego stronach można było znaleźć instrukcje zainicjowania fałszywego alarmu bombowego, nawoływanie do formowania ruchów anarchistycznych, groźby zabójstwa adresowane do konkretnych polityków, urzędników państwowych czy innych osób publicznych.

W listopadzie 2020 forum niespodziewanie znikło z sieci. Niemożliwym jest fakt, żeby skończyły się tematy czy zainteresowanie stroną. Znikło nagle, bez żadnej zapowiedzi czy informacji o zmianie adresu…



Zbiegiem okoliczności (?) zniknięcie Lolifoxa nastąpiło w stosunkowo niedługim czasie po ataku hakerskim w maju 2020 roku na serwer Internetowego Forum Policyjnego (IFP). W ręce przestępców dostały się m.in. loginy, adresy e-mail i zahaszowane hasła użytkowników. To nie pierwszy ani jedyny taki atak w sieci. Jednak ze względu na specyfikę zaatakowanego serwisu sprawa budziła dużo więcej kontrowersji. Nie wiadomo, kiedy dokładnie doszło do ataku, ponieważ nie złapano nikogo za rękę. Administratorzy twierdzili, że o kradzieży

danych dowiedzieli się 24 maja 2020 roku. Serwis oficjalnie poinformował o tym fakcie zarówno na Facebooku, oraz w informacji rozesłanej do wszystkich użytkowników (o tym niżej).

Wróćmy jednak do samej witryny IFP

Internetowe Forum Policyjne nie było branżowym podwórkiem „niebieskich”. To społeczność składająca się zarówno z policjantów, jak i osób cywilnych. Łącznie 100 tys. użytkowników, strona posiadała 0,5 mln komentarzy. Jednym z głównych atutów forum była anonimowość wypowiedzi. Wpisów można było dokonywać wyłącznie po uprzedniej rejestracji. Publikowano na nim rożnego rodzaju informacje dotyczące pracy w policji, proponowanych zmian przepisów, użytkownicy (prawdopodobnie funkcjonariusze) wymieniali się doświadczeniami, radami, narzekali na przełożonych, opisywali ich absurdalne decyzje, a także komentowali decyzje szefów MSWiA. Bardzo często publikowano screeny poufnych policyjnych dokumentów. Po wspomnianym ataku obawiano się, że dane użytkowników wyjdą na jaw – co byłoby bardzo niekorzystne dla wielu użytkowników – wszak na forum często przedstawiano działania policji w bardzo negatywnym świetle. Obecnie strona internetowa IFP nie działa.

Zamiast charakterystycznego logo użytkowników witał komunikat: *Trwają prace techniczne. Przepraszamy….* To jednak nie była awaria. Administrator forum po ataku rozsyłał do użytkowników mail z informacją o ataku hakerskim, jednak wiadomość ta była wątpliwej treści:

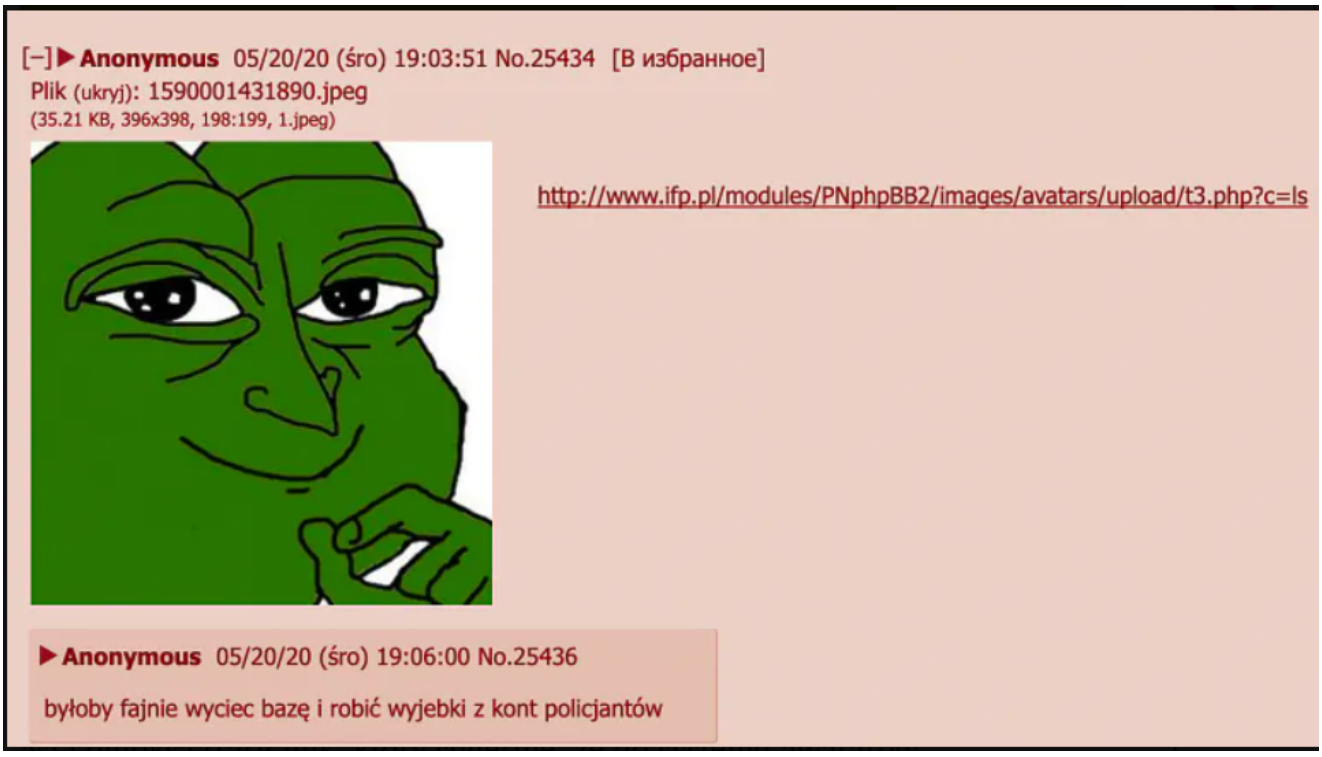
Odkryliśmy, że została ujawniona nieokreślona liczba loginów, adresów e-mail oraz zaszyfrowanych haseł użytkowników IFP. Sugerujemy wszystkim użytkownikom natychmiastowe dokonanie zmiany używanych do tej pory haseł szczególnie, jeśli używają takich samych na innych serwisach internetowych.

Podobna informacja pojawiła się na profilu społecznościowym forum. Policjanci byli zaniepokojeni, bo ich anonimowość stanęła pod znakiem zapytania.

W sieci huczało – kto za tym stoi? Media ujawniały kolejne ślady wskazujące na to, że „ciemna strona internetu" mogła mieć udział w ataku. Śledczy policji śląskiej twierdzili, że atak może być zaplanowaną akcją wymierzoną w dane użytkowników IFP.

I znów wracamy do Lolifoxa…

…gdyż jeden z tropów prowadzi właśnie do jego społeczności. Na kilka dni przed atakiem (20 maja 2020) na tej właśnie grupie dyskusyjnej pojawił się intrygujący wpis:



Zamieszczony w tej wiadomości link kierował do plików awatarów Internetowego Forum Policyjnego. Zapis: „*byłoby fajnie wyciec bazę i robić wyjebki z kont policjantów*” daje też wiele do myślenia.

Już wcześniej na Lolifox pojawiało się sporo „porad”, jak szkodzić organom ścigania. Ten wpis był jednak jednoznaczny. Zamieszczony w wiadomości wspomniany link sugerował, że do systemu awatarów Internetowego Forum Policyjnego przemycono webshell. (Złośliwy fragment kodu napisany w dowolnym języku programowania dołączany do skryptów znajdujących się na serwerze lub stanowiący samodzielny plik. Jego zadaniem jest udostępnienie prostego, tajnego panelu do zarządzania plikami na czyimś serwerze. Tę samą metodę ataku wykorzystano w przypadku Politechniki Warszawskiej.)

Kolejną ciekawostką jest fakt, że na facebookowym profilu Polska Policja na początku maja na krótko pojawił się adres witryny `president-soviet.ru`:

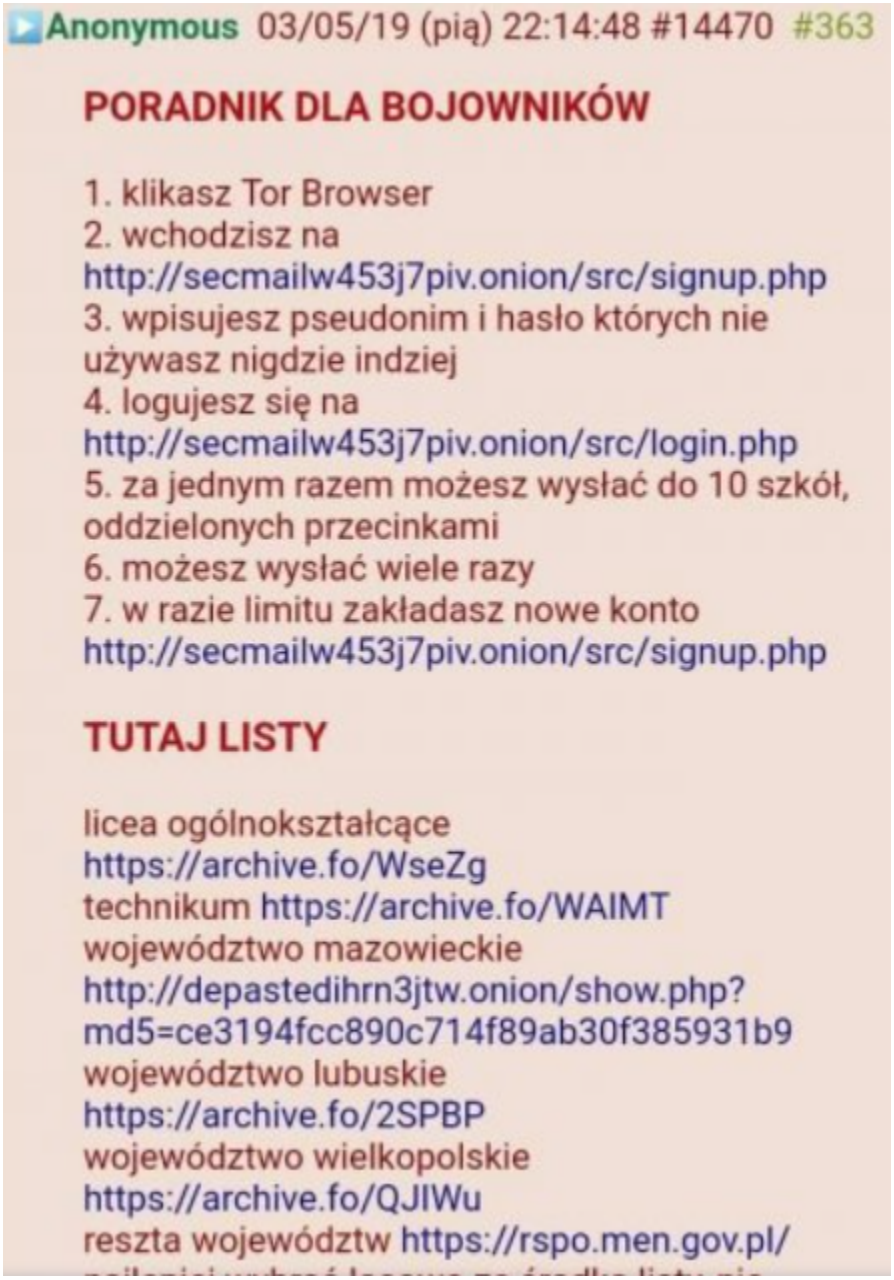
Czemu miała służyć taka informacja? Nie wiadomo. Jednak kojarząc oba fakty można było się domyśleć, że przestępca może być w posiadaniu całej bazy danych IFP, a jednym z użytkowników forum mógł być ktoś z policyjnego zespołu social media.

Jak już wspomniałam, krótko po tym incydencie Lolifox zniknął ze sceny, a ci, którzy go szukali, pisali w sieci, że jeszcze kilka tygodni po tym, ze stary link do forum na Torze przekierowuje stronę na archiwum i pojawiają się świeże wpisy.

Przypuszczano że strona żyje a hakerzy planują kolejne akcje. Czy to możliwe, że znikło bez echa, skoro jego użytkownicy ciągle planowali działalność wywrotową w Polsce?

Alarmy bombowe

W feralnym 2020 roku głośno było także o fałszywych alarmach bombowych. O plagach tych ataków pisaliśmy już tutaj. Wiele miejsc w Polsce zostało wówczas sparaliżowanych fałszywymi alarmami bombowymi. Były to szczególnie instytucje państwowe: prokuratury, sądy, przedszkola, szkoły, uczelnie, szpitale, centra handlowe, media i transport publiczny). W mediach mówiło się, że maile są wysyłane z adresów z końcówką @secmail.pro. Prócz podejrzeń rzucanych na Rosję, czy działalność wywiadów, uwagę skupiali przedstawiciele darknetu i znanego już nam Lolifoxa.



Zorganizowana grupa czy przypadkowy przestępca?

Śledczy mieli nie lada zagwozdkę. Wiele informacji w darknecie wskazywało na to, że maile wysyłała zbieranina przypadkowych, aspołecznych ludzi z internetu, którzy uważają to za doskonałą zabawę. Chcą poczuć adrenalinę i to, że mogą mieć wpływ na czyjeś życie w tak ważnym jego momencie, jak matura, rozpoczęcie roku szkolnego itp.

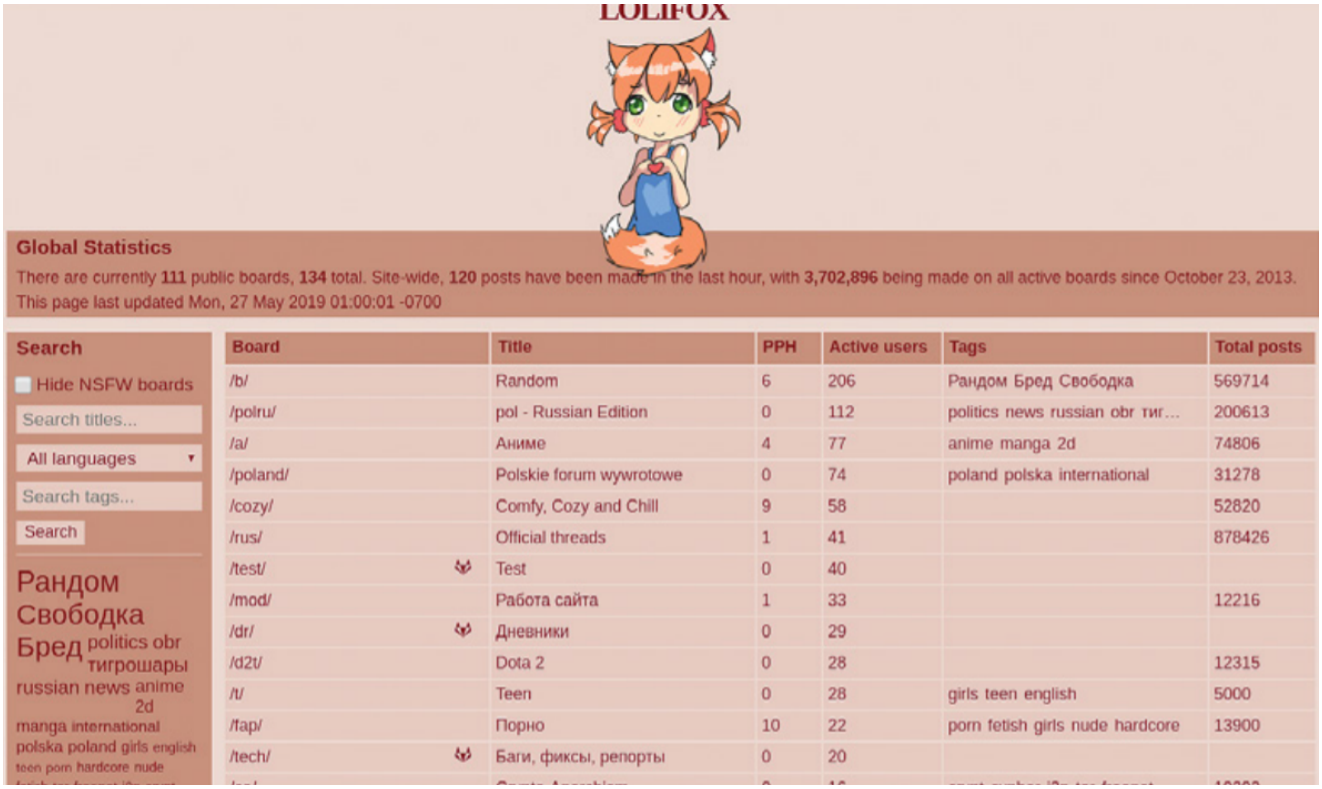
W sieci dudniło od komentarzy: *alarmy bombowe w szkołach to głupi żart użytkowników jednego z chanów, prawdopodobnie Lolifox Poland.* Podczas matur w 2019 roku doszło do ponad 700 alarmów. Rok później jako winnego wskazano rosyjski wywiad GRU. „*Dokładne badanie treści e-maili z fałszywymi informacjami naprowadziło naszych ekspertów na serwery usytuowane w Sankt Petersburgu. Ustalono, że były już w przeszłości*

wykorzystywane do rozsyłania różnych treści, które miały wywołać zamieszanie w różnych częściach świata. Udało się też ustalić autorów całej akcji: to osoby zalogowane na kontach wykorzystywanych przez GRU – rosyjski wywiad wojskowy" – pisały media.

Co mają wspólnego Rosja i Lolifox?

Autor tych wiadomości namawiał internautów, by rozsyłali je do poszczególnych szkół, w których miały się odbyć matury / premiery filmowe w kinach itp. Resztę wykonali już – nieświadomi, że działają dla Rosjan – internauci, którzy zainspirowani rozsyłali fałszywe informacje. Część alarmów wysyłanych było też z automatycznych kont. Analiza wykazała, że ataków mogła dokonać grupa osób „skoordynowana" pod adresem lolifox.org. Pisano przykładowe szablony wiadomości e-mail, instrukcje dotyczące uzyskiwania adresów szkolnych, w tym listy gotowe do pobrania oraz informacje o anonimowym sposobie dystrybucji wiadomości e-mail.

W zabawę w alarmy bombowe czy inne cyberataki przestępcy bawili się już dużo wcześniej. Już w 2019 roku na Lolifox określanym jako „polskie forum wywrotowe" jeden z wątków z 23 stycznia 2019 roku, dotyczył bombardowania alarmów i nosił nazwę: „POMYSŁ NA ZABAWĘ? CZY TO JEST ATAK TERRORYSTYCZNY?"



Anonimowy autor wątku zamieścił codzienną listę artykułów opisujących kolejne alarmy bombowe, możliwe, że sprowokowane przez niego samego.

Przestępcy wzajemnie informowali się, w jaki sposób zachować anonimowość. Nakręcali się, podsyłając linki z informacjami o kolejnych alarmach bombowych (patrz wyżej). Internetowi dywersanci, działający na niekorzyść swojego państwa, szczególnie przykuwają uwagę obcych służb, które nakierowują ich działanie na własne cele. Niczego nieświadomi przyczyniają się do tego, że służby realizują swoje cele w białych rękawiczkach. A te cele to destabilizacja państwa polskiego, podważenie poczucia bezpieczeństwa obywateli i testowanie skuteczności działania służb bezpieczeństwa.

W styczniu 2020 alarmów bombowych było aż 125. Istnieje duże prawdopodobieństwo, że było ich więcej. Nie każdy alarm był opisany w mediach. Niektóre artykuły były archiwizowane w sieci Tor. Z biegiem czasu wątek było tam coraz więcej wpisów. Omawiały kwestie anonimowości, pomysły na nowe alarmy itp.

Ostatni wpis na forum Lolifox pojawił się w grudniu 2020 roku, a więc już po „zdjęciu” aliasu lolifox.cc, który umożliwiał czytanie forum z poziomu otwartego Internetu.Jednak alarmy bombowe nadal miały miejsce. Choć zakres tych ataków wydawał się być duży mniejszy…

Społeczność Lolifox… jest, czy jej nie ma?

Analizując opisane zajścia i niewiele późniejsze zniknięcie Lolifoxa najpierw z otwartego Internetu, a chwilę potem również samej ukrytej usługi w sieci Tor – kusi stwierdzenie, że kwestie te mogą być powiązane. Trudno uwierzyć w to, że buntownicza społeczność Lolifoxa

zwyczajnie odeszła w cień. Znudziła się swoją działalnością? Wystraszyła? Może gdzieś w przepastnej cyberprzestrzeni działają pod inną nazwą (jakaś niewielka część działa pod adresem https://endchan.org/4/).

A Wy co o tym myślicie? Czy użytkownicy wywrotowego forum działają gdzieś jeszcze w czeluściach darknetu? Dajcie znać w komentarzach, albo tradycyjnie secmailem.