Wspólne oświadczenie ministrów i przedstawicieli uczestniczących w spotkaniu Counter Ransomware Initiative
Październik 2021 r.

My, ministrowie i przedstawiciele Australii, Brazylii, Bułgarii, Czech, Dominikany, Estonii, Francji, Holandii, Indii, Irlandii, Izraela, Japonii, Kanady, Kenii, Korei Południowej, Litwy, Meksyku, Niemiec, Nigerii, Nowej Zelandii, Polski, Republiki Południowej Afryki, Rumunii, Singapuru, Stanów Zjednoczonych Ameryki, Szwajcarii, Szwecji, Ukrainy, Unii Europejskiej, Wielkiej Brytanii, Włoch, Zjednoczonych Emiratów Arabskich, zebrani na wirtualnym spotkaniu w dniach 13-14 października, aby omówić wzrost zagrożenia dla światowego bezpieczeństwa, jakim jest oprogramowanie typu ransomware, uznajemy, że oprogramowanie typu ransomware stanowi rosnące zagrożenie dla światowego bezpieczeństwa, z którym związane są poważne skutki gospodarcze i w dziedzinie bezpieczeństwa.

Oprogramowanie typu ransomware stanowi znaczne zagrożenie dla infrastruktury krytycznej, podstawowych usług, bezpieczeństwa publicznego, ochrony i prywatności konsumentów oraz dobrobytu gospodarczego, bez względu na to, czy celem jego złośliwych działań stają się krajowe podmioty służby zdrowia, czym zagrażają zdrowiu pacjentów, czy działania te są wymierzone w przedsiębiorstwa, ograniczając ich możliwości zaopatrywania społeczeństwa w paliwa, żywność i inne artykuły. Zagrożenie ze strony oprogramowania typu ransomware, podobnie jak w przypadku innych zagrożeń cybernetycznych, ma charakter złożony i globalny oraz wymaga wspólnej reakcji. Zdolności poszczególnych krajów do skutecznego zapobiegania atakom typu ransomware oraz ich wykrywania, łagodzenia i reagowania na nie zależą po części od zdolności, współpracy i odporności partnerów globalnych, sektora prywatnego, społeczeństwa obywatelskiego i pozostałych grup społecznych.

Rządy uznają potrzebę podjęcia niezwłocznych działań, wyznaczenia wspólnych priorytetów i podjęcia wzajemnie uzupełniających się wysiłków w celu ograniczenia ryzyka ze strony oprogramowania typu ransomware. Wspomniane wysiłki obejmą: poprawę zdolności sieci do zapobiegania takim zdarzeniom i podejmowania skutecznych działań, gdy takowe jednak zaistnieją; zajęcie się kwestią wykorzystania mechanizmów finansowych w celu legalizacji środków pochodzących z okupów lub innych działań warunkujących opłacalność tego procederu; rozbicie ekosystemu ransomware w drodze współpracy organów wymiaru sprawiedliwości w celu rozpoznania i ścigania uczestników procederu; rozwiązanie kwestii enklaw dla przestępców wykorzystujących ransomware oraz utrzymywanie wysokiego poziomu zaangażowania dyplomatycznego.

Odporność

Odporność sieci wykracza poza możliwości techniczne - wymaga ona także skutecznych ram politycznych, adekwatnych zasobów, przejrzystych struktur zarządczych, klarownych i wypraktykowanych procedur reakcji na zdarzenia, wyszkolonych pracowników pozostających w

gotowości do działania, partnerstwa z sektorem prywatnym oraz konsekwentnego stosowania rozwiązań prawnych i ustawowych. Oczywiście powyższe wysiłki będą uwzględniać lokalne uwarunkowania w poszczególnych krajach i mogą się różnić pomiędzy nimi.

Jednak zastosowanie kilku uniwersalnych najlepszych praktyk w zakresie cyberbezpieczeństwa może radykalnie obniżyć prawdopodobieństwo zdarzenia z wykorzystaniem ransomware oraz zmniejszyć ryzyko wielu innych zagrożeń cybernetycznych. Wspomniane proste praktyki obejmują: utrzymywanie kopii bezpieczeństwa danych w trybie offline, używanie silnych haseł i wieloetapowego uwierzytelniania, dbanie o aktualizację oprogramowania oraz działania uświadamiające w kontekście klikania podejrzanych linków i otwierania niezaufanych dokumentów. Jesteśmy zdecydowani kontynuować współpracę między sobą oraz z sektorem prywatnym w celu upowszechniania podstawowych zasad higieny cyberbezpieczeństwa, która zaowocuje zwiększeniem odporności sieci i zmniejszeniem ryzyka ataku z wykorzystaniem ransomware.

Poszczególne kraje powinny także rozważyć podjęcie działań w celu ułatwienia wymiany informacji o atakach ransomware między ich ofiarami, właściwymi organami wymiaru sprawiedliwości i zespołami reagowania na incydenty komputerowe (CERT) z jednoczesnym poszanowaniem prywatności i praw człowieka. Taka wymiana informacji umożliwia prowadzenie postępowań przygotowawczych i ściganie sprawców cyberprzestępstw oraz ułatwia upowszechnianie środków zapobiegania cyberzagrożeniom.

Ponadto pragniemy dzielić się zdobytym doświadczeniem i najlepszymi praktykami w celu wypracowania polityki reagowania na przypadki wypłacania okupu. Będziemy także współpracować z podmiotami sektora prywatnego w celu ułatwiania wymiany informacji o atakach ransomware oraz badania innych możliwości wspólnego obniżania poziomu ryzyka. Ponadto zauważamy, że wysiłki skierowane na budowanie odporności przynoszą najlepsze efekty, gdy w proces podejmowania decyzji w zakresie cyberbezpieczeństwa aktywnie zaangażowani są przywódcy wysokiego szczebla dysponujący umiejętnościami kierowania zasobami, wypracowywania kompromisów i osiągania celów.

Zwalczanie nielegalnego finansowania

Ransomware jest przede wszystkim przedsięwzięciem nakierowanym na zysk, które do transferu wpływów powszechnie wykorzystuje siatki trudniące się praniem pieniędzy. Dostrzegamy znaczny potencjał w zwalczaniu ataków ransomware w drodze zaawansowanej współpracy międzynarodowej nakierowanej na utrudnianie, śledzenie i zatrzymywanie przepływów pieniężnych z tytułu zapłaconego okupu, zgodnej z przepisami krajowymi, co ograniczy materialne motywacje osób przeprowadzających ataki ransomware. Współpraca może obejmować wiele obszarów, takich jak środki ułatwiające stosowanie należytej staranności wobec klientów, składanie raportów o podejrzanych działaniach i monitorowanie transakcji.

Podejmowanie działań mających uniemożliwiać korzystanie z modeli działania opartych na oprogramowaniu typu ransomware wymaga wspólnego reagowania na ryzyko nielegalnego finansowania, jakie stanowią wszystkie systemy przekazywania wartości majątkowych, w tym kryptoaktywa, które są podstawowym instrumentem wykorzystywanym przez przestępców do ataków ransomware, a następnie do prania pieniędzy. Zdajemy sobie sprawę, że niejednolite stosowanie na świecie norm Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy (FATF) dotyczących kryptoaktywów i dostawców usług w zakresie kryptoaktywów (VASP) stwarza okoliczności, dzięki którym podmioty działające w złej wierze mogą sięgać po arbitraż i dokonywać transferu nielegalnie uzyskanych korzyści za pomocą platform podlegających jurysdykcjom, w których nie obowiązują odpowiednie wymogi związane z m.in. przeciwdziałaniem praniu pieniędzy. Jesteśmy też świadomi wyzwań, z jakimi mierzą się niektóre jurysdykcje przy budowaniu struktur i tworzeniu zdolności dochodzeniowo-śledczych, aby zajmować się ciągle ewoluującymi i przeprowadzanymi w dużym rozproszeniu operacjami biznesowymi z wykorzystaniem kryptoaktywów.

Pragniemy wzmóc starania, aby uniemożliwiać korzystanie z modeli działania opartych na oprogramowaniu typu ransomware i powiązanych z nimi praktyk prania pieniędzy. Jednym ze sposobów, aby to osiągnąć, jest zadbanie o to, aby nasze krajowe struktury służące przeciwdziałaniu praniu pieniędzy skutecznie identyfikowały i minimalizowały zagrożenia ze strony dostawców usług w zakresie kryptoaktywów i te związane z działalnością podobnego rodzaju. Zwiększymy kompetencje naszych organów krajowych, angażując organy regulacyjne, jednostki analityki finansowej i organy ścigania, aby objąć wykorzystywanie kryptoaktywów regulacjami prawnymi, nadzorem oraz czynnościami dochodzeniowo-śledczymi i prewencyjnymi, przy odpowiedniej ochronie prywatności i z uwzględnieniem, że poszczególne działania mogą różnić się w zależności od kontekstu krajowego. Wypracujemy ponadto formy współpracy z sektorem kryptoaktywów, aby zintensyfikować wymianę informacji dotyczących oprogramowania typu ransomware.

Rozbicie ekosystemu i inne działania organów ścigania

Poza podejmowaniem działań służących zwiększeniu odporności i wzmocnieniu naszego systemu finansowego, aby chronić go przed nieuprawnionym wykorzystywaniem, musimy również dążyć do tego, aby podmioty prowadzące działalność przestępczą związaną z oprogramowaniem typu ransomware były pozbawiane możliwości działania i pociągane do odpowiedzialności. Taka działalność przestępcza często ma charakter transgraniczny, a walka z nią wymaga podejmowanej w odpowiednim czasie i konsekwentnej współpracy między organami ścigania, krajowymi organami ds. bezpieczeństwa, agencjami ds. cyberbezpieczeństwa i jednostkami analityki finansowej. Tego rodzaju współpraca musi przebiegać zgodnie z krajowymi wymogami prawnymi, a także może być prowadzona z jednoczesnym wykorzystaniem środków dyplomatycznych, aby można było wykrywać szkodliwe działania i reagować na nie, a ich sprawców obejmować postępowaniem przygotowawczym i aktem oskarżenia. Musimy wspólnie podejmować odpowiednie działania, aby przeciwdziałać cyberprzestępczości występującej na naszym

terytorium i wymagać tego samego od innych, a w rezultacie likwidować enklawy dla podmiotów prowadzących taką szkodliwą i destabilizującą działalność.

Zamierzamy współpracować między sobą i z innymi partnerami na arenie międzynarodowej, aby rozszerzać wymianę informacji i w miarę możliwości udzielać pomocy temu, kto się o to zwróci, aby walczyć z działalnością polegającą na wykorzystywaniu oprogramowania typu ransomware z użyciem infrastruktury i instytucji finansowych na terytorium naszych krajów. Rozważymy użycie wszelkich dostępnych narzędzi krajowych do podjęcia działań przeciwko podmiotom odpowiedzialnym za wykorzystywanie oprogramowania typu ransomware w sposób zagrażający infrastrukturze krytycznej i bezpieczeństwu publicznemu.

Dyplomacja

Poza rozbiciem ekosystemu umożliwiającego stosowanie oprogramowania typu ransomware można podejmować działania dyplomatyczne, aby upowszechniać postępowanie oparte na zasadach i zachęcać państwa do tego, by w uzasadniony sposób przeciwdziałały korzystaniu z oprogramowania typu ransomware na ich obszarze. Będziemy sięgać po dyplomację, podejmując skoordynowane działania wobec państw, które nie reagują na działalność cyberprzestępców. Taka współpraca będzie istotnie przyczyniać się do znacznego ograniczania enklaw dla podmiotów stosujących oprogramowanie typu ransomware.

Jako że egzekwowanie prawa i zdolności w obszarze cyberbezpieczeństwa to aspekty mogące znacznie ograniczać możliwości danego państwa, jeśli chodzi o reagowanie na cyberprzestępczość, dyplomacja w formie skoordynowanego budowania zdolności ma szansę przysłużyć się temu, aby wydatnie rozbudowywać arsenał środków do walki z oprogramowaniem typu ransomware. Będziemy wymieniać się metodami budowania zdolności, zwracać uwagę na dostępne zasoby i programy, a także podejmować działania, aby w razie potrzeby koordynować prace w tych obszarach, zapewniając, by budowanie zdolności uzupełniało pozostałe działania służące ograniczaniu zagrożenia ze strony oprogramowania typu ransomware.