GRUDZIEŃ 2022

Raport ENISA 2022 Landscape Threat

część 1

AUTOR

Rafał Prabucki

SFINANSOWANO ZE ŚRODKÓW FUNDUSZU SPRAWIEDLIWOŚCI, KTÓREGO DYSPONENTEM JEST MINISTER SPRAWIEDLIWOŚCI

Phishing ciągle w formie

Najnowszy raport ENISA Threat Landscape 2022 nie pozostawia złudzeń. Phishing jest ciągle jednym z głównych wektorów stosowanych do uzyskania dostępu i zainstalowania złośliwego oprogramowania na urządzeniach użytkowników. W budowaniu tzw. „przynęt" stanowiących element cyberataku pomogły również ostatnie niepokoje światowe wynikające z pandemii COVID-19, czy też wojny na Ukrainie.
Phishing w raporcie przygotowanym przez ENISA jest jednym z cyberataków realizowanych w ramach inżynierii społecznej. Jak opisuje go ENISA: ma na celu kradzież ważnych informacji, takich jak numery kart kredytowych i hasła, poprzez e-maile wykorzystujące inżynierię społeczną i podstępy. Oprócz typowego phishingu raport wyróżnia też:

- Spear-phishing – spersonalizowany atak phishing, którego celem jest konkretna osoba lub organizacja;
- Whaling – atak typu spear-phishing skierowany do użytkowników na wysokich stanowiskach (np. kadra kierownicza, polityków itp.);
- Smishing – wedle ENISA: termin powstały z połączenia słów "SMS" i "phishing", ma miejsce,gdy informacje finansowe lub dane osobowe ofiar są zbierane za pomocą wiadomości SMS;
- Vishing – analogicznie, jak powyżej, połączenie phishingu z głosem. Występuje w przypadku przekazywania informacji przez telefon, gdzie atakujący manipulują atakowanym, aby wydobyć wrażliwe informacje od użytkowników;
- Business e-mail compromise (BEC) – zgodnie za ENISA: wyrafinowane oszustwo skierowane do firm i organizacji, polegające na tym, że przestępcy wykorzystują techniki inżynierii społecznej, aby uzyskać dostęp do konta e-mail pracownika lub członka zarządu w celu inicjowania przelewów bankowych na fałszywych warunkach;
- Oszustwo;
- Podszywanie się;
- Fałszerstwo.

Racjonalizacja kosztów ataku i niepowodzenie szkoleń kadry

Uwzględniając dane z poprzednich raportów ENISA należy zauważyć, że atakujący zracjonalizowali swoje taktyki. Zamiast podejścia technicznego, dominuje podejście miękkie w zdobyciu tak zwanego „przyczółku" w organizacji, który posłużyć ma do dalszego ataku. Za przyczółek należy w tym wypadku uznać pewne dane, które będą punktem wyjścia do dalszych ataków. W tym celu stosuje się rozwiązania z zakresu inżynierii społecznej, które są tanie i tym samym opłacalne dla atakujących. ENISA zauważa jednak, że wzrosty wykorzystania podobnych technik generalnie występują nie tylko w zakresie phishingu, ale w we wszystkich wektorach związanych z inżynierią społeczną. Należy podkreślić, że nie można łączyć inżynierii społecznej wyłącznie z e-mailem, choć należy podkreślić, że dla atakujących taki wektor ataku jest wciąż atrakcyjny.. Głównym celem jest w końcu pozyskanie danych, które posłużyć mogą dalej w konstruowaniu ataków typu BEC. Zebrane tak liczby pozwalaj też wysnuć smutny wniosek, że wielu użytkowników, mimo szkoleń i akcji uświadamiających, nadal staje się ofiarami manipulacji oraz mechanizmów opartych na inżynierii społecznej, w tym phishingu stosowanych przez cyberprzestępców.

Kto stosuje phishing?

Koszty walki z skutkami phishingu w 2021 r. wzrosły w organizacjach ponad trzykrotnie od 2015 r. Do najbardziej czasochłonnych zadań związanych z rozwiązywaniem skutków takich ataków należy zakwalifikować czyszczenie i naprawianie zainfekowanych systemów oraz prowadzenie śledztwa. Phishing niezawsze bowiem kończy się wyłącznie na wyłudzeniu danych. Niekiedy ten cyberatak jest skonstruowany w sposób, który ma zachęcić oraz że zmanipulować zaatakowanego do pobrania również złośliwego oprogramowania. Grupy przestępcze, które zajmują się złośliwym oprogramowaniem przeważnie odpowiadają za znaczne ilości kampanii phishingowych. Pomimo wychwytywania przez służby policyjne takich zorganizowanych grup przestępczych następuje wyłącznie tymczasowy spadek określonych ataków phishinogywch do momentu, aż w ich miejscu nie pojawi się nowa grupa przestępcza.

Jaki jest cel takiej działalności i model biznesowy?

Celem inżynierii społecznej jest głównie uzyskanie dostępu do informacji lub usług albo zdobycie wiedzy na określony temat, która mogłaby być następnie wykorzystywana w celu osiągnięcia zysku finansowego. W czołówce organizacji, pod które podszywali się atakujący poprzez phishing, znalazły się instytucje finansowe. Obok sektora finansowego, atakujący koncentrowali swoje kampanie socjotechniczne wokół branży technologicznej, w której na pierwszym miejscu przestępcy podszywali się pod firmy takie jak Microsoft, Apple i Google. Wykorzystując logo wybranego przedsiębiorcy i jego styl w komunikowaniu się z użytkownikiem, atak stawał się wiarygodniejszy. Nie można też nie wspomnieć przy tej okazji o samym złośliwym oprogramowaniu, które jest instalowane, jeżeli taki model działania został przewidziany przez atakującego. Przeważnie jest to Ransomware. ENISA definiuje ten typ złośliwego oprogramowania jako rodzaj ataku, w którym podmioty stanowiące zagrożenie przejmują kontrolę nad aktywami informacyjnymi wybranego przez siebie celu i żądają okupu w zamian za przywrócenie dostępności do tychże aktywów. Oczywiście, w celu zainstalowania owo złośliwego oprogramowania stosuje się phishing.

Biznes ten jest na tyle intratny, że obecnie funkcjonuje już cały model "Phishing-as-a-Service" (PhaaS), w którym atakujący mogą korzystać z gotowych materiałów. Co ciekawe nierzadko pośrednik lub dostawca rozwiązania do przeprowadzenia ataku, sam też wykorzystuje atak, aby pozyskać dane zdobyte przez atakującego. W ten sposób cały proceder staje się jeszcze bardziej dotkliwy dla atakowanego, ponieważ informacje dotyczącego jego osoby mogą znaleźć się w posiadaniu kilku niezależnych grup przestępczych. W ten sposób nie tylko sam atakujący przejmuje dane, ale trafiają one jednocześnie do pośrednika oferującego PhaaS, a sam atakujący nie wie, że nie jest jedynym podmiotem, który przejął dane.

Poza tym wątkiem należy podkreślić, że PhaaS oferowane jest nawet z uwzględnieniem różnic regionalnych, co pokazuje, że działania te stanowią już zaawansowane i profesjonalne „usługi dla przestępców". Rozszerzeniem PhaaS jest wykorzystanie również Brokerów Dostępu Początkowego, ang. Initial Access Brokers (IAB). W ramach takiej usługi specjaliści od inżynierii społecznej pozyskują i przekazują dostęp, często dane uwierzytelniające lub zainstalowane narzędzia zdalnego dostępu, swoim klientom.

Jako, że działalność ze względu na swoją intratność dynamicznie się rozwija, zdaniem ENISA w najbliższym czasie zobaczymy jeszcze więcej przypadków działalności IAB. Brokerzy, którzy najpierw różnymi sposobami uzyskają dostęp do organizacji, a następnie wykorzystają swoje mechanizmu do prowadzenia dalszej działalności przestępczej, mogą tym samym stać się również elementem kampanii szpiegowskich. Na chwilę obecną najlepiej udokumentowaną kampanią tego typu brokerów jest opisana przez ekspertów z TAG Google „Exotic Lily".

Wojna i szpiedzy

ENISA przytacza też ciekawe studium przypadku związane z działalnością szpiegowską. W 2021 roku w październiku i listopadzie doświadczona grupa atakujących obrała sobie za cel różne europejskieplacówki dyplomatyczne i ministerstwa spraw zagranicznych. W mailach atakujący tak manipulowali odbiorcą, aby ten otworzył plik HTML, który następnie pobierał obraz dysku (format ISO lub VHDX). Takie działanie pozwalało obejść zabezpieczenia techniczne i zainstalować złośliwe oprogramowanie na urządzeniu ofiary. W tym celu efektywnie wykorzystywano czynnik ludzki, który przejawiał się dobrowolnym pobraniem pliku przez użytkownika.

Rozwój phishingu i innych wektorów inżynierii społecznej będzie również rozwijaj się ze względu na trwającą wojnę w Ukrainie. Nie chodzi tylko o działania szpiegowskie, ale też i konstruowanie przynęt na bazie emocji związanych z wojną (np. uchodźcami). Nie można też wykluczyć, że cześć kampanii phishingowych będzie finansowana przez kraje, które będą miały interes w ich realizacji. Szczególnie w zakresie spear-phishingu i whalingu.

Mail ciągle najkorzystniejszy, ale pojawiają się alternatywy

Z punktu widzenia finansowego ciągle najlepszym rozwiązaniem dla atakujących jest mail, stąd wysoka popularność BEC. Chociaż atak BEC może być postrzegany jako phishing, nie jest on związany z dystrybucją złośliwego oprogramowania ani nie bazuje na złośliwych linkach, jest on po prostu nadużywaniem zaufania, , podszywaniem się lub jest on zbiorem różnych technik inżynierii społecznej.

Stosunkowo innowacyjnym pomysłem jest jednak phishing polegający na wyłudzeniu zgody. Działanie to polega to spreparowaniu maila dostępowego do usługi przez udzielenie potrzebnej zgody dla rzekomej aplikacji. Kliknięcie w link przyznający zgodę przez atakowanego użytkownika powoduje, że atakujący pobierają token dostępu, a następnie ma dostęp na poziomie konta do danych atakowanego bez konieczności posiadania dodatkowych poświadczeń użytkownika. Ten model wymaga jednak również atakującego znajomości technik związanych z przygotowaniem aplikacji, która pomoże mu wyłudzić zgodę. Włożony trud w w cały proces jest jednak kuszący, ponieważ w tym modelu zdecydowanie ciężej jest wykryć przeprowadzany ataku z powodu chociażby braku widoczności niepokojących oznak cyberataku, czy też wiedzy większości organizacji o tego typu zagrożeniu.

Problematyczne są też boty rozsyłające wiadomości SMS lub MMS, jak na przykład wskazany przez ENISA zlikwidowany w 2022 roku FluBot. Atakowani są zalewani wiadomościami SMS (smishing, czyli de facto SMS phishing), które podszywają się pod przedsiębiorstwa dostarczające paczki, notatki poczty głosowej lub fałszywe oprogramowanie. Wiadomość zawiera łącze, które następnie przekierowuje na stronę internetową instruującą użytkownika, aby zainstalował aplikację. Po jej zainstalowaniu przyznawane są atakującym żądane uprawnienia na urządzeniu atakowanego użytkownika lub czasami nawet wyłączane są funkcje bezpieczeństwa. Warto jeszcze zwrócić uwagę, że niekiedy programy takie, jak FluBot mogą realizować więcej problemów na urządzeniu, na którym działają. ENISA na bazie studium przypadku usuniętego bota pokazuje, że tego typu oprogramowania mogą wysyłać z numeru zaatakowanego wiadomości tekstowe na bazie dostępnej na urządzeniu listy kontaktów. Owa lista może też być udostępniona organizatorom kampanii phishingowej, tak samo jak numery kart kredytowych, dane uwierzytelniające do bankowości online, czy przechwycone wiadomości SMS. ENISA dodaje, że chociaż na przykład FluBot nie działał na urządzeniach Apple (iOS), to nie znaczy, że użytkownicy tych telefonów są zabezpieczeni przed phishingiem.

Ciekawe jest też spostrzeżenie ENISA dotyczące użytkowników kryptowalut. Ich popularność spowodowała, że cyberprzestępcy obrali za cel ich posiadaczy, jak i podmioty zajmujące się wymianą kryptowaktywów. ENISA zauważa, że obszarem powiązanym, który szczególnie zwrócił uwagę przestępców są tak zwane tokeny NFT. Nie chodzi jednak w tym obszarze o innowacyjność w zakresie stosowanych wektorów ataku, czy technik, ale o sam obszar działania. Wykorzystywane metody nie różnią się od tych stosowanych w przypadku "tradycyjnych" rynków.

Obrona i reakcja atakujących

Nie rzadko w phishingu i inżynierii społecznej, chodzi o pozyskanie danych uwierzytelniających. Jak zauważa ENISA, zastosowanie wieloczynnikowego uwierzytelniania (MFA od ang. multi-factor authentication) pomaga zmniejszyć ryzyko potencjalnych szkód cyberataku. Wdrażanie nowych zabezpieczeń przekłada się też na zmianę modeli działania atakujących stosujących phishing. Zamiast przejmować skrzynki i z nich prowadzić atak, skłonni są oni wykorzystywać legalną infrastrukturę dla swoich kampanii poprzez szukanie luk w systemach, takich jak Microsoft Exchange, wykorzystywanych następnie w celu dystrybucji phishingu. Ciekawym zjawiskiem w zakresie działania osób stosujących phishing jest wyłączenie domyślnych makr
w skoroszytach Microsoft Excel przez producenta. Jak widać, również i osoby odpowiedzialne za programy, które mogą być wykorzystane przez cyberprzestępców starają się zapobiegać wykorzystaniu ich rozwiązań do ataków.

Niezależnie od wszystkiego, najlepszym rozwiązaniem jest świadomość tego, jak działają atakujący. Mimo, iż raport wskazywał, że niekiedy osoby przeszkolone i tak popełniają błędy powodując, że phishing jest skuteczny, to nie należy zaprzestawać aktywności mających na celu budowanie odporności organizacji. Wydaje się, że problemem może być jakość szkoleń, a także nasze fałszywe przekonanie, że nie do końca chce nam się wierzyć, że damy się nabrać na tego typu „sztuczki", które brzmią bardzo naiwnie.

Na koniec należy podkreślić, że różnego rodzaju techniczne zabezpieczenia wspierające użytkownika wydają się pewnego rodzaju dobrym dodatkiem do wszelkich szkoleń i akcji uświadamiania. Warto z nich skorzystać, szczególnie przy projektowaniu wspomnianych rozwiązań MFA

Rafał Prabucki

MINISTERSTWO SPRAWIEDLIWOŚCI
www.ms.gov.pl
FUNDUSZ SPRAWIEDLIWOŚCI
SFINANSOWANO ZE ŚRODKÓW FUNDUSZU SPRAWIEDLIWOŚCI, KTÓREGO DYSPONENTEM JEST MINISTER SPRAWIEDLIWOŚCI

fundacja@instytutcyber.pl
www.instytutcyber.pl