LISTOPAD 2022

Największe zagrożenia w sieci.

Phishing.

fundacja instytut CYBERBEZPIECZEŃSTWA

AUTOR

Michał Podpora

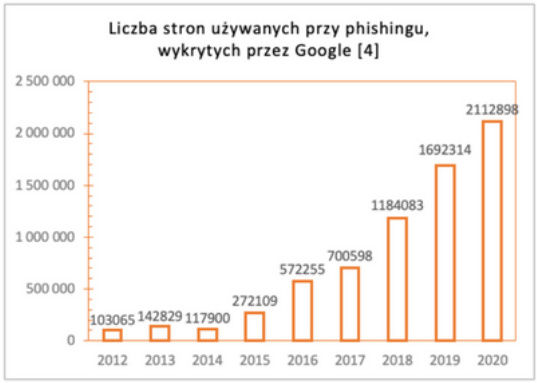
MINISTERSTWO SPRAWIEDLIWOŚCI
www.ms.gov.pl

FUNDUSZ SPRAWIEDLIWOŚCI

SFINANSOWANO ZE ŚRODKÓW FUNDUSZU SPRAWIEDLIWOŚCI, KTÓREGO DYSPONENTEM JEST MINISTER SPRAWIEDLIWOŚCI

Dziesięć lat temu termin „phishing” był nieznany zdecydowanej większości użytkowników internetu, aczkolwiek list otrzymany od nigeryjskiego księcia [1], napisany łamaną polszczyzną, wzbudzał uzasadnione obawy. Dzisiaj terminy „spam”, „phishing”, „malware” są w słowniku niemal każdego z nas, a mimo to zaskakująco często ludzie tracą dane oraz pieniądze.

Skąd pochodzi „sukces” phishingu? Dlaczego komukolwiek zależy na jego rozwoju? Według [2] i [3] już w roku 2013 roczne straty będące skutkiem działań cyberprzestępców zaczęły przekraczać roczną wartość globalnego rynku marihuany, kokainy i heroiny łącznie. Natomiast rok 2019 wraz z pandemią przyniósł 43%-owy wzrost [4] liczby stron internetowych wykorzystywanych do kapitalizowania phishingu (z 1.18 miliona do 1.69 miliona , a rok 2020 – dalszy 25%- owy wzrost (do 2.11 miliona). Spowodowane pandemią zjawiska takie jak upowszechnienie pracy zdalnej, intensyfikacja wykorzystania platform online, konieczność przełamywania nawyków i przyzwyczajeń konsumenckich na korzyść alternatyw obecnych w świecie wirtualnym spowodowały wytworzenie idealnych warunków dla rozwoju i rozkwitu wszelkich form cyberprzestępczości.



Popularne wektory ataków

Istnieje wiele ścieżek jakimi cyberprzestępcy próbują zdobyć nasze zaufanie. Najbardziej powszechne dotyczą albo obietnicy zysku (nigeryjski książę, kryptowaluty) albo „koniecznej dopłaty” (zakupy online, opłaty online) – ale to tylko ułamek większej całości. Warto lepiej poznać wachlarz metod, aby łatwiej rozpoznawać próby ataków.

Nigeryjski szwindel (Nigerian scam).
Mimo że jest to najstarsza metoda oszustwa, realizowana jeszcze za czasów poczty tradycyjnej, faksem lub nawet telefonicznie [5], którą pozornie każdy z nas doskonale potrafi rozpoznać, to jednak jej nazwa i pochodzenie niewiele mają wspólnego z jej współczesną postacią (wg [6], w 2005 roku najwięcej, bo 71% namierzonych oszustów pochodziło z USA, a dla porównania 7.9% z Nigerii). W tej grupie znajdują się rozmaite działania, które odnoszą się do „konieczności” wykonania przedpłaty, która ma doprowadzić do obiecywanego skutku, zazwyczaj naszej korzyści majątkowej [5],[7]:

- propozycja inwestycji (biznesmen lub prawnik obiecujący ogromne zyski),
- wygrana w loteriach (mały przelew „by potwierdzić prawdziwość danych” rachunku bankowego do przelewu wielkiej wygranej),

- oszustwa randkowe (poznana osoba potrzebuje pieniędzy na bilet by przyjechać lub sugeruje kupowanie prezentów),
- pomoc uchodźcy (nadawca oferuje sporą sumę w zamian za zakup biletu a później realizowanie kolejnych kroków/zakupów) ▪ Weteran armii (podobnie jak punkt poprzedni),
- szybki zakup (na sprzedawany przez nas przedmiot znalazł się kupiec, ale prosi o bardzo szybką wysyłkę wysyłając nam potwierdzenie przelewu, który „niestety będzie dłużej trwał"),
- spadek (nadawca informuje, że w wyniku śmierci krewnego został nam zapisany ogromny spadek, „pomaga nam" zapłacić „wszystkie niezbędne opłaty i podatki").

Szczególnie ostatnia z przedstawionych metod zasługuje na uwagę, gdyż jest obecnie najbardziej zaawansowaną i dopracowaną metodą, często poprzedzoną budowaniem bazy potencjalnych ofiar, analizą publicznie dostępnych informacji o wypadkach, katastrofach lotniczych lub działaniach wojennych i ich ofiarach, a następnie przeprowadzeniu dopracowanego, częściowo personalizowanego ataku.

Niedopłata rachunku

Jedna z nowszych metod, polegająca na wysyłaniu losowym osobom wiadomości (np. SMS-a z informacją o planowanym odłączeniu energii elektrycznej) w związku z niedopłatą. Po kliknięciu w link otwiera się strona informująca o (bardzo małej, np. 2 zł) niedopłacie [8] oraz link do podstawionej strony banku, gdzie mamy zrealizować przelew. Nasze dane zamiast do banku trafiają do oszustów, którzy mogą zrealizować dowolny przelew lub inną operację, nawet autoryzację nowego urządzenia (np. telefonu – by mogli sami autoryzować dowolne przelewy z naszego konta).

Zakupy online i link do wpłaty (tzw. OLX+WhatsApp)

Metoda polegająca na wmówieniu sprzedawcy, że musi się zalogować do banku i autoryzować przelew, aby otrzymać pieniądze [9] (oczywiście strona banku jest spreparowana by wyłudzić dane, a to kupujący autoryzuje przelew a nie sprzedawca).

Inne, równie popularne metody:

- nieopłacona faktura (invoice scam) – atakujący przesyła „nieopłaconą fakturę" którą nakazuje pilnie uregulować, wystawioną na dane jakiejś znanej firmy,
- awizo przesyłki za pobraniem – atakujący żąda zapłacenia za przesyłkę, którą nam dostarcza,
- ciekawy link – po kliknięciu otwiera stronę z podstawionym ekranem logowania do sieci społecznościowej lub poczty, celem uzyskania loginu i hasła,
- unsubscribe – wiele osób korzysta z linku „unsubscribe" (wypisz) który zawarty bywa w niechcianych wiadomościach (a ten link może działać tak jak opisano wcześniej),
- ciekawy załącznik – po kliknięciu uruchamia skrypt lub instaluje złośliwe oprogramowanie,
- smishing (SMS+phishing) – phishing inicjowany wiadomością SMS (daje pozory, że nadawca nas zna, skoro ma nasz numer telefonu),

- chatbot phishing – atak przekierowujący na stronę lub prowadzony jako SMSy/WhatsApp, gdzie dane są wyłudzane w formie rozmowy, prowadzonej przez chatbota,
- vishing (voice+phishing) – atak zawierający w sobie rozmowę głosową „z konsultantem" lub „pracownikiem instytucji" mający w ten sposób uwiarygodnić „potrzebę" podania informacji oraz umożliwić zastosowanie socjotechniki celem usprawnienia wyłudzenia,
- spear phishing (phishing profilowany) – taka wersja każdej z powyższych metod phishingowych, w której atakujący przynajmniej część informacji personalizował w celu uwiarygodnienia: nasze dane osobowe lub nazwę banku lub logo firmy, której jesteśmy klientami – jakakolwiek informacja, która uśpi czujność lub wzbudzi zaufanie,
- whaling – odmiana spear phishingu celowana w osoby decyzyjne dużych firm,
- BEC (business email compromise) – atak, który celuje w jedną z dwóch współpracujących firm, gdzie atakujący podaje się za pracownika tej drugiej, wykorzystując wzajemne zaufanie.

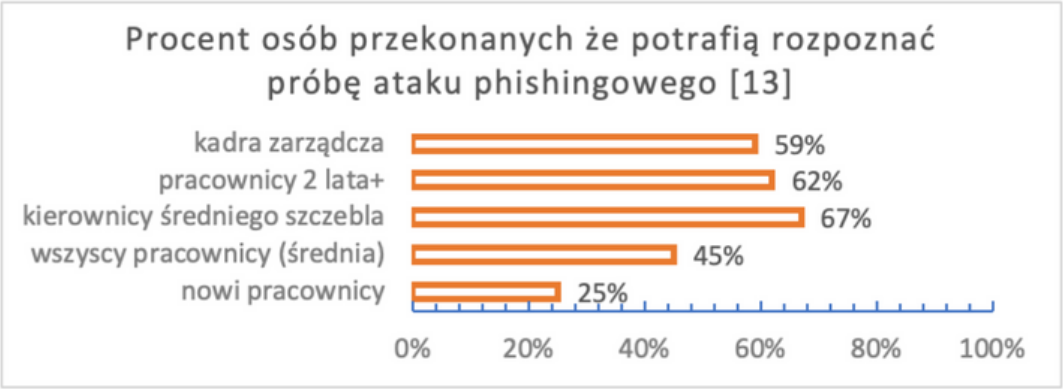
Powyższa lista [10],[11],[12] nie zamyka klasyfikacji metod wyłudzania danych i/lub pieniędzy, dlatego warto zawsze zachować czujność i trzeźwe myślenie. Co chwilę pojawiają się nowe pomysły – zarówno techniczne (np. smishing, vishing) jak i socjotechniczne (np. Zombie Phish, gdzie atakujący przejmuje jakiekolwiek konto email, a następnie podszywa się pod jego właściciela mając zaufanie osób z którymi właściciel korespondował).

Przyczyny wzrostu ilościowego i jakościowego ataków phishingowych

Rok 2019 wielu wskazuje jako rok o rekordowym przyroście liczby ataków, obwiniając za ten stan rzeczy pandemię [4] i zmianę stylu korzystania z globalnej sieci. Jednak gdyby to było prawdą, rok 2021 powinien przynieść wytchnienie, tymczasem grudzień 2021 miał ponad 300000 ataków phishingowych [15] – ponad trzy razy więcej niż dwa lata wcześniej. Dodatkowo, coraz bardziej powszechną platformą docelową phishingu są urządzenia mobilne, sieci społecznościowe i usługi chmurowe – według [16] tzw. mobile phishing w 2021 wzrosło o 161%. Wzrost liczby ataków po części wynika z wzrostu dostępności informacji dla początkujących hakerów, ale także z dostępności wielu zaawansowanych „kombajnów" do wynajęcia, oferowanych w modelu RaaS (ransomware as a service) [2] które znacznie skracają przestępcom odległość między kampanią phishingową a kapitalizacją zysków.

Podnoszenie świadomości w firmie - symulacje typu "go phishing"

W raporcie opracowanym przez Osterman Research [13] w bardzo ciekawy sposób przedstawiono zaobserwowane zależności między działaniami (m.in. ochroną, szkoleniami, identyfikacją, świadomością) przeciwdziałającymi phishingowi w firmach, a skutecznością ataków. Przedstawiono tam także średni roczny budżet bezpieczeństwa informatycznego na pracownika (który wzrósł z 333$ w 2020 na 400$ w 2021), co zdaje się być jedną z przyczyn wyraźnie zauważalnej zmiany wewnętrznego przekonania co do umiejętności identyfikacji zagrożenia phishingowego – z 25% w grupie nowych pracowników do 62% w grupie zatrudnionych przynajmniej 2 lata w danej firmie. Kolejnym niezwykle ważnym czynnikiem wpływającym na postrzeganie i identyfikację zagrożeń tego typu są bez wątpienia działania kadry odpowiedzialnej za cyberbezpieczeństwo instytucji – szkolenia, nadzór przestrzegania procedur i uprawnień dostępu do systemów i danych, a także okresowe próby typu „go phishing", polegające na kontrolowanych testach phishingowych.



Podnoszenie świadomości „w domu"

Instytucje i firmy mogą (powinny) przewidzieć czas i pieniądze na uszczelnianie procedur i podnoszenie świadomości pracowników, widzą bardzo konkretną wartość posiadanych informacji, rozumieją straty wynikające z utraty informacji lub ich przejęcia przez konkurencję, mogą zatem łatwo wyliczyć „opłacalność" zapewniania cyberbezpieczeństwa. O wiele trudniejsza sytuacja ma miejsce w najmniejszych firmach i na komputerach prywatnych. Wg [14], 27% badanych Polaków używających komputera nie posiada programu antywirusowego, a 10% nigdy nie zmieniła hasła lub danych uwierzytelniających. Zważywszy, że tematyka służbowej korespondencji zwykle dotyczy węższego wycinka rzeczywistości niż maile prywatne, łatwiej być czujnym w pracy niż w domu. Ponadto nie każdy pracuje w instytucji o wysokich standardach bezpieczeństwa informacji, stając się tym samym bardziej podatnym – potencjalną ofiarą ataku lub dobrodusznym użytkownikiem oferującym swój sprzęt do dyspozycji przestępców. Dlatego bardzo istotne są wszelkie działania mające na celu podnoszenie świadomości i nagłaśnianie najbardziej szkodliwych aktualnych odmian ataków, aby uchronić obywateli od nieprzyjemności lub strat – również finansowych.

Si vis pacem para bellum

Jak należy działać? Po czym poznać, że dany email to próba wyłudzenia danych a nie faktycznie niedopłacona faktura? Warto bez emocji zastanowić się nad faktami które łączą mnie i sprawę przedstawioną w mailu, a także zwrócić uwagę na kilka technicznych wskazówek, o których często przypominają fachowcy [15]:
(1) Czy adres nadawcy zgadza się z osobą za którą nadawca się podaje?
(2) Czy adres nadawcy i ewentualne linki w treści prowadzą do domeny/serwera instytucji nadawcy?
(3) Czy nadawca prosi nas o podanie jakichkolwiek danych lub haseł?
(4) Czy mail jest napisany właściwym dla danej firmy stylem?
(5) Czy linki w mailu prowadzą na ten sam adres serwera który jest na nich widoczny?
(6) Czy po kliknięciu linka jesteśmy na serwerze który na pewno należy do tej instytucji?
(7) Nie ufajmy we wspaniałe okazje do inwestowania które przytrafiły się akurat nam, ani
(8) w loterie w które nigdy nie graliśmy, a jednak jesteśmy zwycięzcami.

Pamiętajmy także, że „inteligencja naturalna" (człowiek) [15,13] to najlepsza ochrona przed phishingiem. Warto być odrobinę nieufnym, pilnować swoich danych, hasła zmieniać, a w razie wątpliwości zapytać profesjonalistów.

[1] Stojnic, T., Vatsalan, D., & Arachchilage, N. A. (2021). Phishing email strategies: Understanding cybercriminals' strategies of crafting phishing emails. Security and Privacy, 4(5), e165.
[2] Woods, E. (2016). The Real Reason For Successful Phishing Attacks. uSecure, (dostęp: 2022-11) https://blog.usecure.io/the-real-reason-why-phishing-attacks-are-so-successful
[3] Dimitrova, M. (2016). Cybercrime and money – Cause and Effect. Tripwire, (dostęp: 2022-11) https://www.tripwire.com/state-of-security/cyber-crime-and-money-cause-and-effect
[4] Edward, G. (2021). A record 2 million phishing sites reported in 2020, highest in a decade. atlasVPN, (dostęp: 2022-11) https://atlasvpn.com/blog/a-record-2-million-phishing-sites-reported-in-2020-highest-in-a decade
[5] Bischoff, P. (2019). What is Nigerian scam (418 scam) with examples. Comparitech, (dostęp: 2022-11) https://www.comparitech.com/identity-theft-protection/nigerian-scam/
[6] State of Georgia Consumer Protection Division (2005). Nigerian Fraud Scams. consumer.georgia.gov, (dostęp: 2022-11) https://consumer.georgia.gov/consumer-topics/nigerian-fraud-scams
[7] Biuro Kryminalne KGP (2009) Oszustwo Nigeryjskie. policja.pl, (dostęp: 2022-11) https://www.policja.pl/pol/aktualnosci/39149,quotNigeryjski-szwindelquot.html
[8] Wroczyński, D. (2022) Oszustwo na niedopłatę rachunku za prąd. Uważajmy i nie klikajmy w przesłane linki. mazowiecka.policja.gov.pl, (dostęp: 2022-11) https://mazowiecka.policja.gov.pl/wwy/aktualnosci/65014,Oszustwo-na-niedoplate-rachunku-za-prad Uwazajmy-i-nie-klikajmy-w-przeslane-link.html
[9] Komenda Policji w Ostródzie (2020) Nowa metoda oszustw przy pomocy portalu OLX oraz aplikacji WhatsApp. ostroda.policja.gov.pl, (dostęp: 2022-11) https://ostroda.policja.gov.pl/o15/aktualnosci/79299,UWAGA-Nowa-metoda-oszustw-przy-pomocy-portalu OLX-oraz-aplikacji-WhatsApp.html
[10] Microsoft Learn (2022) Phishing trends and techniques. Microsoft, (dostęp: 2022-11) https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/phishing-trends
[11] Bolland, E. (2021) The Surge in Phishing Attacks and Changing Threats in 2021. uSecure, (dostęp: 2022-11) https://blog.usecure.io/a-complete-guide-to-phishing-threats?hsLang=en
[12] Kowalska, M. (2021) Co to jest vishing i dlaczego jest niebezpieczny? Polityka Bezpieczeństwa, (dostęp: 2022-11) https://www.politykabezpieczenstwa.pl/pl/a/co-to-jest-vishing-i-dlaczego-jest-niebezpieczny
[13] Osterman Research (2021) How to reduce the Risk of Phishing and Ransomware. Osterman Research/ Trend Micro, (dostęp: 2022-11) https://resources.trendmicro.com/rs/945-CXD-062/images/Reduce-Phishing Ransomware_Trend-Micro.pdf
[14] Europ Assistance Polska (2022) Badanie „Bezpieczeństwo w internecie". ARC Rynek /Europ Assitance Polska.
[15] Cook, S. (2022) Phishing statistics and facts for 2019-2022. Comparitech, (dostęp: 2022-11) https://www.comparitech.com/blog/vpn-privacy/phishing-statistics-facts/
[16] securitymagazine.com (2021) Mobile phishing threats surged 161% in 2021. Security, (dostęp: 2022-11) https://www.securitymagazine.com/articles/96430-mobile-phishing-threats-surged-161-in-202

MINISTERSTWO SPRAWIEDLIWOŚCI

www.ms.gov.pl

FUNDUSZ SPRAWIEDLIWOŚCI

SFINANSOWANO ZE ŚRODKÓW FUNDUSZU SPRAWIEDLIWOŚCI, KTÓREGO DYSPONENTEM JEST MINISTER SPRAWIEDLIWOŚCI

fundacja@instytutcyber.pl
www.instytutcyber.pl