

Metamorfoza phishingu w 2007 roku trendy i osiągnięcia

Autor: Marek
25.01.2008.
Zmieniony 06.06.2008.

Opis różnych trendów i osiągnięć, które były udziałem phisherów w roku 2007 oraz opis czynników napędzających, które kryją się za wielkim wzrostem procentowym w phishingowym mailingu w czasie ubiegłego roku.

Źródło: www.windowssecurity.com

Tłumaczenie: Monika Palonek, Bielsko-Biała

Rok 2007 był kolejnym okresem kiedy to osoby zajmujące się phishingiem zademonstrowały swój upór i pomysłowość w sposobach, aby przy użyciu metod socjo-technicznych zmusić on-line tyle osób ile to tylko możliwe do uwierzenia, że są tymi, za których się podają. Dlaczego phisherzy przyjęli ekonomicznie skali w roku 2007, jakie czynniki przyczyniły się do coraz mniejszego czasu potrzebnego phisherowi do wymyślenia fałszywego e-maila i jak to możliwe, że pomimo całej świadomości publicznej skierowanej na ten problem, ludzie wciąż padają ofiarami przekrętów phisherów? Celem tego artykułu jest przegląd kluczowych czynników, które przyczyniły się do wzrostu i ewolucji phishingu w ciągu zeszłego roku.

Stan phishingu w roku 2007 – ujednoczenie socjotechniki

Ostatni raport – dzięki uprzejmości Anti Phishing Group (APG) – dostarcza pouczających trendów, odnoszących się do czasu jaki strona phishera pozostaje on-line, co jest kluczowym czynnikiem dla sukcesu kampanii phishingu. Na przykład: sierpniowy raport APG stwierdza, że średni czas jaki strona jest on-line to 3,3 dnia, a najdłuższą stroną była otwarta przez 30 dni. Jak łatwo sobie wyobrazić im dłużej kampania phishingu pozostaje on-line, tym większe prawdopodobieństwo, że odbiorca wylądował na w pełni komunikatywnej stronie phishera i w ten sposób staje się jego ofiarą. Wśród internetowej zbiorowej inteligencji społecznej skupionej na koordynowaniu zamykania nowo-pojawiających się domen phishingowych we właściwym czasie, pojawili się dostawcy, którzy już próbują skomercjalizować proces zamykania kampanii phishingowych w szczególności poprzez atak na markę. Wyznaczenie takiego priorytetu może w rzeczywistości być finansowo uzasadnione w następstwie niektórych ostatnio opublikowanych wyników ankiet, twierdzących, że marki, do których klienci tracą zaufanie po otrzymaniu phishingowego e-maila udającego e-maila z danej firmy, co dzieje się tak często, że – aby być na bieżąco ze wszystkimi czynnościami tego typu – należy korzystać z Brandjacking Index.

Sprzedawcy zabezpieczeń, niezależne grupy badawcze oraz projekty społecznej internetowej takie jak Phishtank wskazują na olbrzymi wzrost liczby phishingowych e-maili krążących dziko jak i unikatowe nazwy domen korespondujące z nimi. Ten wzrost jest w dużej mierze spowodowany następującymi kluczowymi pomysłami, które omówię w tym artykule, a mianowicie: zestawy phishingowe typu „zrob to sam”, dostępność phishingowych szablonów stron każdej firmy finansowej i internetowej, które da się w ten sposób zaatakować, zjednoczenie phisherów, którzy są coraz lepsi w socjotechnikach ze spamerami, którzy przodują w dostarczaniu segmentowanych e-maili do lepszego celu. To wszystko przyczynia się do metamorfozy phishera od ¼le zarządzanej operacji pojedynczej grupy do skupionego na produktywności procesu, w skład którego wchodzi wiele farm domen, z której każda zawiera niezliczone pod-domeny mierzące w różne marki dzięki uprzejmości zestawu Rock Phish. Kilka lat temu koncepcja anty-phishingowych pasków narzędzi zaczęła przyciągać uwagę publiczną, ponieważ brakowało w przeglądarkach wbudowanego zabezpieczenia wykrywającego cechy charakterystyczne powszechnych stron phishingowych, a brak aktualnej dostępności ochrony przeglądarek przed atakami phishingowymi jasno dowodzi jak dużym problemem stał się phishing, szczególnie pod względem podkopywania zaufania w handel internetowy. Zilustrujemy ten problem i jego rozwój poprzez omówienie niektórych z jego najważniejszych aspektów dynamiki:

Kluczowe koncepcje przyczyniające się do wzrostu ataków phishingowych

Zjednoczenie ze spamerami

Gdy myślisz o zjednoczeniu, rozpocznij swoje przemyślenia od wzięcia pod rozważenie trwałe zjednoczenie pomiędzy spamerami a autorami złośliwego oprogramowania, które omawiam w poprzednim artykule, a mianowicie fakt, że spamerzy potrzebują infrastruktury, z której mogą wysyłać e-maile, a którzy otrzymują od właścicieli botnetów lub używają na życzenie. Phisherzy również muszą spełniać te same wymagania, aby przetrwać i tak naprawdę ten złośliwy ekosystem robi się coraz trudniejszy do zlikwidowania, ponieważ nie jest oczywiste kto w tej hierarchii jednoczy więcej niż inni, a konkretnie czy autorzy złośliwego oprogramowania spamują dla siebie w poszukiwaniu większego ruchu powrotnego, czy spamerzy także wysyłają phishingowe e-maile gdzieś pomiędzy złośliwym oprogramowaniem oraz jak realna jest sytuacja, kiedy to phisherzy wysyłają również Trojany bankowe na wypadek, gdyby odbiorca nie stał się ofiarą przekrętu phishera? Jedną rzeczą jest pewna: odnajdują oni nowe i bardziej skuteczne sposoby, aby pracować wspólnie. Co takiego phisher może chcieć od spamera i czy są to wzajemnie wykluczające się czy raczej takie same interesy?

To wszystko jest kwestią perspektywy. Phisher mógłby być zainteresowany lokalizacją wiadomości w języku lokalnym, segmentacją e-maili na zasadach „per country”, prawdopodobnie nawet danymi podkopującymi strony społecznościami internetowymi oraz publicznymi stronami internetowymi, aby tylko wpłynąć na pomysły jakiegokolwiek związku między e-mailem a marką, która ma zamiar zaatakować. Zilustrujmy to. Weź pod uwagę odbiorcę, który nie ma absolutnie żadnego związku biznesowego z marką, która informuje go o „zabezpieczeniu, które wymaga weryfikacji danych jego konta”. Odbiorca nie pada ofiarą i bierze to za e-maila phishingowego. Ponieważ phisherzy nie chcą, aby tak się stało, skorzystają z wiedzy spamerów w formie segmentowania do bazy danych e-maili, którą aktualnie posiadają na zasadach „per country” i „per city” i w ten sposób zwiększą szanse, że phishingowy e-mail, którego celem jest na przykład niemiecki bank, trafi do skrzynki e-mailowej obywatela Niemiec.

Zestawy phishingowe typu „zrób to sam” i pokolenie phishingowych e-maili „wskaż i kliknij”

Obniżenie bariery wejścia na scenie phishingu jest analogiczne do obniżenia bariery wejścia na scenie złośliwego oprogramowania, mianowicie jest to spowodowane wprowadzeniem zestawów phishingowych typu „zrób to sam” /DIY (do-it-yourself) Phishing Kits/, których celem jest oszczędność znacznej ilości czasu jaki phisher musi poświęcić na znalezienie skutecznego sposobu, aby wprowadzić narzędzie przekazywania danych logowania w tak wielu szablonach stron phishingowych jak to tylko możliwe. I o to właśnie chodzi w zestawach phishingowych typu „zrób to sam” i dokładnie te same zestawy pod koniec drugiej połowy roku 2007 stały się towarem, a jeden z tych zestawów osiągnął etap v.2.0. Takie zestawy umożliwiają prawie każdemu łatwe wejście do świata phishingu. Dlatego są oni bezpośrednio odpowiedzialni za wzrost ataków phisherów. Nowe wersje z bardziej zaawansowanymi funkcjami, takimi jak bezpośrednie przeniesienie strony phishera do wybranego zestawu adresów URL, są przygotowane, aby iść dalej na podwalinach sukcesu dwóch pierwszych wersji.

Zestaw „Rock Phish” i phishingowa ekonomia skali

Istnieje powszechne nieporozumienie dotyczące tego czym jest Rock Phish. Czy jest to gang phishingu, czy jakiś rodzaj zestawu typu „zrób to sam”, w którym phisherzy „wskazują i klikają”, aby wymyślić te doskonałe kampanie phishingowe, których „miejmy nadzieję” jesteście świadomi? Odpowiedź jest taka, że zestaw Rock Phish jest prostym skryptem z dużą ilością zmiennych, gdzie phisher korzysta z pojedynczej domeny, aby dojść do licznych pod-domen różnych firm, z których każda odpowiadałaby innej stronie phishera i byłaby ukierunkowana na inną markę. Oto przykład farmy domeny Rock Phish (Zobacz Obrazek).

Adres IP, 212.199.95.108 pojawia się na moim radarze od dłuższego czasu i dlatego jest idealnym przykładem domeny Rock Phish, a konkretnie domeny, która zarządza (is hosting) wieloma pod-domenami, z których każda decyduje o osobnej kampanii phishingowej, a służy stworzeniu unikatowego i usankcjonowanego wyglądu strony phishingowej. A

oto jak wyglądają przykładowe adresy URL rock phish:

- userconfirmationform-id91705.ebay.com.buhank.info
- moneymanagergps.session-569906917.citizensbank.com.floher.biz
- webinfocus.id-40462.mandtbank.com.hobotid.hk
- myonlineaccounts5.abbey.co.uk.refid83617.njexnz3.xz.cn
- nfbconnect-18108.northforkbank.com.stack.kg
- onlinetreasurymanager-id9038673.suntrust.com.utr.hk
- business-eb.bbt.com.mio23.mobi
- id-57546.citizensbankmoneymanagergps.com.gkiier.hk
- securelogin-03788828.moneymanagergps.com.dfv92.com
- citizensbankmoneymanagergps.com.yrmat3.xz.cn

Monitorowanie domen Rock Phish zawsze dostarcza wielu informacji, ponieważ skrypt, który uruchamia setki tysięcy tych kampanii phishingowych powoli staje się na dużym skali domyślnym pakietem narzędziowym. Na przykład: kilka miesięcy temu domyślna wiadomość na konkretnym domenie Rock Phish brzmiała: "Host 209 Zamknięty", ale ponieważ stosunkowo łatwo było zlokalizować takie domeny, phisherzy niedawno zmienili to na "Host 66.1 Zamknięty". Jedynym sposobem na Rock Phish'a jest ta związana z nastawieniem na wydajność. Gdy zamknie się IP, które utrzymuje farmę domen, wszystkie kampanie phishingowe przestaną odpowiadać. Ponadto scentralizowanie kampanii phishingowej w taki sposób ułatwia jej blokadę.

Podsumowanie

Monitorowanie procesu dotyczącego ile wysiłku promocyjnego wkładają instytucje finansowe w zapewnienie usług e-bankowych i e-transakcyjnych jest bardzo interesujące, lecz z drugiej strony czerpią korzyści z faktu, że to klient, który podpisał umowę bezwarunkowo twierdzi, że bank nie może ponosić odpowiedzialności za żadne nieuczciwe transakcje. Phishing nie powinien być traktowany jak coś innego niż spam. Jest to niechciana wiadomość, a porównując do wiadomości spammerskiej, phishingowy e-mail może spowodować o wiele poważniejsze szkody finansowe. Sęk w tym, że nie powinien on trafiać do skrzynki mailowej użytkownika i nie powinien wyjść poza pewne zainfekowane sieci macierzyste (host's network). Phishing wciąż jest w dużej części w swoim etapie 1.0. Jest to, mianowicie, podejście wpychania maili do swoich ofiar, obok bardziej zaawansowanego podejścia takiego jak "pharming";

Co więcej, phisherzy tak samo jak spamerzy łatwo się przystosowują, a ostatnia kampania phishingowa MySpace pokazuje ich zainteresowanie w stosowaniu różnych taktyk nie tylko po to, aby ustanowić większe zaufanie wizualne poprzez użycie typosquatting, lecz także poprzez wymyślenie jak ustrzec się radaru dostawcy. W kampanii MySpace nie spamowali phishingowych adresów URL, ale posyłałi je jako wewnętrzne komentarze spammerskie i w ten sposób żaden czujnik dostawcy nie był w stanie ich wyśledzić. I pomimo logicznej metamorfozy phishingu od dobrze sformułowanej wiadomości marketingu bezpośredniego do swojego aktualnego modelu komunikacji masowej, budowania wiadomości poprzez rozwiązania technologiczne w formie wbudowanego zabezpieczenia przeglądarki częściowo stawia opór na dzień dzisiejszy. "Najlepsze"; dopiero nadchodzi.

Źródło: www.windowssecurity.com

Tłumaczenie: Monika Palonek, Bielsko-Biała