Badanie Sophos ujawnia dramatyczny wzrost malware, phishingu i spamu rozsyłanego poprzez portale społecznościowe.

Sophos, firma specjalizująca się w technologiach ochrony informacji, opublikował dziś raport zagrożeń - Security Threat Report 2011 - kompletną analizę cyberprzestępczości w ciągu ostatniego roku oraz prognozy trendów bezpieczeństwa IT w 2011. Kluczowym elementem raportu są wyniki najnowszej ankiety Sophos, dotyczącej bezpieczeństwa na portalach społecznościowych. Celem badania było zebranie doświadczeń internautów w zakresie zagrożeń w serwisach społecznościowych.

Ankieta koncentruje się na doświadczeniach użytkowników w sieciach społecznościowych, szczególnie w miejscu pracy.

Do połowy 2010, Facebook zarejstrował pół miliarda aktywnych użytkowników, co czyni go nie tylko największym portalem społecznościowym, ale także jednym z najbardziej popularnych miejsc w sieci. Nic więc dziwnego, że ta ogromna baza użytkowników stała się celem dla scammerów i cyberprzestępców. W 2010 obserwowaliśmy stały wzrost liczby ataków, które stały się coraz bardziej różnorodne - malware, phishing i spam w sieciach społecznościowych to najczęściej spotykane zagrożenia. Z badania Sophos wynika, że:

* 40% badanych otrzymało złośliwe oprogramowanie za pośrednictwem serwisów społecznościowych, to 90% wzrost od lata 2009 r.

* Dwie trzecie (67%) twierdzi, że było spamowanych za pośrednictwem serwisów społecznościowych, ponad dwukrotnie więcej niż to miało miejsce dwa lata temu.

* 43% było celem ataków phishingowych, ponad dwa razy więcej niż w 2009 r.

"Złożliwe aplikacje, clickjacking, ankiety scam - wszystkie te zagrożenia, zaledwie kilka lat temu zupełnie niespotykane, teraz pojawiają się na bieżąco w serwisach społecznościowych, takich jak Facebook," powiedział Graham Cluley, starszy konsultant ds. bezpieczeństwa w Sophos: "Dlaczego Faceboook i pozostałe sieci społecznościowe nie robią więcej, aby zapobiec pojawianiu się spamu i innych zagrożeń? Ludzie muszą być bardzo ostrożni, dbać o prywatność swoich danych osobowych i nie dać się nabrać na klikanie w podejrzane linki, które mogą prowadzić do zainfekowania komputera i zazwyczaj przynoszą zyski cyberprzestępcom."

Mimo że wyniki różnią się dla poszczególnych sieci - Facebook, Twitter, MySpace i LinedIn - najnowsze badanie pokazuje, że połowa ankietowanych ma nieograniczony dostęp do sieci społecznościowych w pracy. Paradoksalnie, 59% uważa, że aktywność pracownika w serwisach społecznościowych może narazić na szwank bezpieczeństwo sieci firmowej, a 57% obawia się, że ich znajomi udostępniają zbyt wiele informacji na portalach społecznościowych.

"Coraz rzadziej spotyka się całkowicie zablokowany dostępu do serwisów społecznościowych, gdyż firmy dostrzegają wartość, jaką te strony mogą wnieść w podnoszeniu świadomości marki poprzez przeprowadzanie tam kampanii marketingowych," wyjaśnił Cluley. "Jeśli twoja firma nie jest na Facebooku, a konkurenci są, to znajdziesz się w niekorzystnej sytuacji. Ale musisz być świadomy ryzyka i zadbać o bezpieczeństwo swoich użytkowników, gdy są online."

Chociaż 82% respondentów uznało Facebooka za najbardziej niebezpieczne miejsce w sieci, to zdaniem specjalistów Sophos największym pojedynczym incydentem był atak na sieć mikroblogów Twitter, który miał miejsce we wrześniu 2010 r.

Robak "onMouseOver" bardzo szybko rozprzestrzenił się po sieci Twitter i pokazał, jak łatwo ataki typuCross-site-scripting (XSS) potrafią wykorzystać lukę na portalu społecznościowym i dotknąć ogromną liczbę użytkowników.

Nagranie na YouTube przedstawiające atak robaka na Twitterze dostępne jest pod adresem: http://www.youtube.com/watch?v=EpG661S9u9A

Pełna wersja raportu zagrożeń Sophos Threat Report 2011, który zawiera dalsze wnioski z badania, jest do pobrania za darmo (nie wymaga rejestracji): http://www.sophos.com/threatreport2011

Bez wątpienia wydarzeniem o najwyższym profilu IT security w 2010 roku, była historia portalu WikiLeaks, który przyjął dużą liczbę ataków Denial-of-Service (DDoS), a w konsekwencji serwery z kontrowersyjną stroną odmówiły posłuszeństwa. Głośno było także o robaku "Stuxnet", atakującym systemy SCADA wykorzystywane w przemyśle, w tym w obiektach jądrowych. Robaki te są przykładem na to, jak rozwija się cyberprzestępczość, począwszy od etapu proof-of-concept i pisania złośliwego kodu, poprzez motywację finansową zorganizowanej działalności przestępczej, na motywach politycznych skończywszy. W kolejnych latach przewiduje się kontynuację tego trendu.

Poza nasileniem zagrożeń w sieciach społecznościowych, znane i sprawdzone taktyki cyberprzestępczości nadal zatruwają Internet. Niektóre witryny są tworzone z myślą o infekowaniu odwiedzających, ale to te popularne i obdarzone zaufaniem strony internetowe są najbardziej pożądanym celem ataków, ponieważ hakerzy, którzy zdołali przejąć kontrolę nad stroną, mogą w łatwy sposób rozsyłać malware niczego nie spodziewającym się użytkownikom. Większość zainfekowanych stron internetowych znajduje się w USA. Jednak w ciągu ostatnich sześciu miesięcy kraje europejskie stały się bardziej obfitym źródłem złośliwych stron, w szczególności Francja, która wyprzedziła Chiny, zwiększając swój udział z 3,82 do 10,00 procent stron z malware.

Lista 10 krajów hostingujących najwięcej zainfekowanych witryn w okresie od stycznia do grudnia 2010:

1. Stany Zjednoczone 39.39%
2. Francja 10.00%
3. Rosja 8.72%
4. Niemcy 5,87%
5. Chiny 5,04%
6. Wielka Brytania 2,68%
7. Polska 2,43%
8. Kanada 2,03%
9. Ukraina 1,97%
10. Węgry 1,84%

Pozostałe 20,03%

"Wielu użytkowników komputerów nadal nie zdaje sobie sprawy, że można złapać coś paskudnego, zwyczajnie odwiedzając stronę internetową, kontynuował Cluley. "W ciągu minionego roku obserwowaliśmy około 30.000 nowych złośliwych adresów URL dziennie - to jedna strona na dwie, trzy sekundy. Przeszło 70 procent z nich to zaufane witryny, które padły ofiarą hakerów - oznacza to, że firmy i właściciele stron internetowych mogli nieumyślnie infekować odwiedzających ".

Pełne wydanie Security Threat Report 2011 zawiera znacznie więcej informacji i statystyk dotyczących przestępczości internetowej w 2010 r., jak również prognozy i nowe trendy. Raporty można pobrać bezpłatnie ze strony Sophos pod adresem: http://www.sophos.com/threatreport2011

** Badanie Sophos przeprowadzone na 1273 respondentów w grudniu 2010.*

Sophos