Sophos, firma specjalizująca się w technologiach ochrony informacji, opublikował dziś półroczny raport zagrożeń dla bezpieczeństwa, ujawniając wyniki badania postaw wobec cyberwojen oraz pozostałe trendy bezpieczeństwa IT w pierwszej połowie 2010 roku.

- 63% uważa cyber-szpiegostwo między krajami do przyjęcia

Światowe badanie Sophos przeprowadzone na 1077 użytkownikach komputerów odkrywa alarmujące postawy względem międzynarodowego cyber-szpiegostwa. Respondenci byli pytani o to czy uważają szpiegostwo za pośrednictwem hackingu lub ataków malware jako akceptowalną praktykę oraz czy sieci komputerowe prywatnych firm w innych krajach to dozwolone cele.

Niektóre kluczowe wnioski z badania wskazują na rozluźnione podejście do przestępczości internetowej sponsorowanej przez państwo:

* 63% ankietowanych uważa, że szpiegowanie innych narodów przez włamanie lub zainstalowanie szkodliwego oprogramowania jest dopuszczalne dla ich kraju (23% powiedziało tak w każdej chwili, 40% tylko w czasie wojny, 37% powiedziało nie)

* Aż 1 na 14 respondentów uważa, że paraliżujące ataki DoS przeciwko innemu państwu, a w szczególności na strony internetowe odpowiedzialne za infrastrukturę i finanse są do przyjęcia w czasie pokoju (49% stwierdziło, że tylko w czasie wojny, 44% było za tym, że nigdy)

* 32% uważa, że kraje powinny mieć prawo do instalacji złośliwego oprogramowania i włamu do prywatnych firm zagranicznych dla korzyści ekonomicznych (23% stwierdziło, że jest to możliwe tylko w czasie wojny, 9% stwierdziło, że w czasie pokoju, 68% było na nie)

"To może dziwić, że tak wiele ludzi uważa, że korzystanie z Internetu jako narzędzia do szpiegowania, a nawet jako broni, jest praktyką do przyjęcia", powiedział Graham Cluley, starszy konsultant ds. technologii w Sophos. "Dając zielone światło dla tego rodzaju działalności, ty też musisz się liczyć z konsekwencjami. Może twoja firma będzie następną, która zetknie się z zagranicznymi siłami?"

"Operacja Aurora", która po raz pierwszy ujrzała światło dzienne na początku roku, spowodowała oskarżenia Google w kierunku chińskich hakerów odpowiedzialnych za atak na serwery wyszukiwarki i 30 innych amerykańskich firm. To bardzo jasny sygnał początku nowej ery malware.

"Hacking i pisanie wirusów rozpoczęły się jako hobby, często projektowane raczej by programista mógł pokazać swoje umiejętności, niż wyrządzić poważne szkody," kontynuował Cluley. "Później ewoluowało do zorganizowanej działalności przestępczej wabionej dużymi kwotami pieniędzy i teraz, w 2010, można stwierdzić, że trzecim motywem jest wykorzystywanie malware i Internetu w celu uzyskania komercyjnych, politycznych i militarnych korzyści."

Specjaną edycję raportu Mid-year 2010 Security Threat Report, zawierającą szczegółowe dane z badania, można pobrać za darmo pod adresem: http://www.sophos.com/trmy10

USA nadal mocarstwem malware. Kraje europejskie dołączają do pierwszej dziesiątki.

USA nadal numerem jeden pod względem ilości stron internetowych, na których można znaleźć malware. Są to witryny stworzone z wyraźnym zamiarem zainfekowania użytkowników lub strony internetowe zaatakowane przez hakerów, którzy często wykorzystują też niedozwolone techniki optymalizacji wyników wyszukiwania (Black SEO) w celu zwiększaniu ruchu na zainfekowanych stronach i w konsekwencji zarażenia większej ilości komputerów.

Lista top 10 krajów hostingujących malware w okresie od stycznia do czerwca 2010:

Stany Zjednoczone 42,29%
Chiny 10,75%
Rosja 6,13%
Niemcy 4,08%
Francja 3,92%
Wielka Brytania 2,41%
Włochy 2,09%
Holandia 1,76%
Turcja 1,74%
Iran 1,53%

Pozostałe 23,3%

Pełny raport Sophos zawiera znacznie więcej informacji na temat najnowszych zagrożeń malware, sieci społecznościowych, spamu, a także przewidywania nowych trendów, i może być pobrany za darmo ze strony Sophos pod adresem: http://www.sophos.com/trmy10

** Ankieta online Sophos, 1077 respondentów.*

Sophos