Cyberbezpieczeństwo 2015: coraz trudniejsze do odparcia ataki wyzwaniem dla współpracy branżowej

Napastnicy wykorzystują legalnie funkcjonującą infrastrukturę, czerpiąc milionowe zyski.

Broniący się przed atakiem starają się wykrywać i zwalczać zagrożenia, a ich zaufanie wobec zabezpieczeń jest coraz mniejsze.

Atakujący robią uniki i szybko się reorganizują

Atakujący zwiększają niezawodność i skuteczność swoich działań. W razie wykrycia atakujący potrafią szybko „zmienić szyk" i w ciągu paru minut zacząć korzystać z nowych systemów z nowymi adresami IP

Angler

– tego rodzaju atak często pozostaje niewykryty, ponieważ wykorzystuje serwery o dobrej reputacji

Strony przekierowujące ruch

15 tys. unikatowych witryn przekierowujących ruch za pomocą złośliwych reklam

Serwery proxy

Wiele serwerów bez złośliwego oprogramowania, wykorzystujących zasoby pochodzące od legalnych firm hostingowych, aby przekierować użytkowników do serwerów będących źródłem ataku

Serwery będące źródłem ataku

60% to obciążenia generowane przez oprogramowanie ransomware. Rozpowszechnianie globalne, przez wiele kanałów

Serwery informujące o stanie ataku

Atakujący otrzymują alerty o naruszeniu stanu operacji lub wykryciu manipulacji

Mała infrastruktura IP

Możliwość zaatakowania puli adresów IP 8–12 aktywnych systemów w ciągu dnia

60 mln USD

rocznie – szacowane zyski z zaledwie dwóch zidentyfikowanych kampanii

SSHPsycho

Globalny, oparty na współpracy, atak siłowy (tzw. brute force)

DDoS

Wykorzystanie 10 tys. komputerów

Sieci typu botnet

1. Zainicjowane w Chinach brutalne ataki w celu pozyskania haseł użytkowników i zbudowania sieci typu botnet
2. 24 godziny później, USA: logowanie przy użyciu zdobytych haseł w celu pobrania na zaatakowane urządzenia rootkita przeprowadzającego atak DDoS

Masowe oddziaływanie

35% całego ruchu SSH w Internecie zostało objęte atakiem SSHPsycho

Połączenie zasobów oraz złamanie zabezpieczeń

221% wzrost liczby witryn WordPress, których zabezpieczenia naruszono

Broniący się przed atakiem nie współpracują dość skutecznie

Broniący się przed atakiem są w coraz mniejszym stopniu przekonani, że są w stanie wykrywać cyberataki, bronić się przed nimi i naprawiać ich skutki; organy regulacyjne i inwestorzy dążą zaś do uzyskania lepszego wglądu w strategię organizacji związaną z cyberzagrożeniami.

Spadek poczucia bezpieczeństwa

Odsetek badanych przekonanych, że korzystają z najnowszej technologii: spadek do 59%

Odsetek badanych uważających, że wykorzystywana przez nich technologia NIE JEST najnowsza: wzrost do 37%

Przed atakiem

54% badanych uważa, że jest w stanie sprawdzić, czy atak miał miejsce

Podczas ataku

54% badanych wierzy w zdolność obronienia się przed atakiem

Po ataku

45% badanych wierzy w zdolność określenia i ograniczenia zakresu ataku

Naruszenie zabezpieczeń i luki w bezpieczeństwie

92% badanych urządzeń Cisco działających w Internecie miało znane luki w zabezpieczeniach (średnio po 26 na urządzenie)

31% badanych urządzeń Cisco to urządzenia EOS

5% badanych urządzeń Cisco to urządzenia EOL

56% badanych regularnie weryfikuje i aktualizuje zasady bezpieczeństwa

Ograniczenia

Niewystarczający zakres współpracy między organizacjami; podczas incydentów związanych z bezpieczeństwem tylko

21% powiadamia partnerów biznesowych

18% powiadamia instytucje zewnętrzne

15% powiadamia firmy ubezpieczeniowe

Bariery utrudniające wdrażanie zaawansowanej technologii zabezpieczeń

39% Budżet

32% Problemy ze zgodnością

25% Wymagania związane z certyfikacją

CISCO

Pobierz doroczny raport Cisco na temat bezpieczeństwa na 2016 r.
www.cisco.com/go/asr2016

© 2016 Cisco lub podmioty stowarzyszone. Inne nazwy firm, produktów i usług mogą być znakami towarowymi lub usługowymi innych podmiotów.