**Kryminalistyka cyfrowa pomoże w walce z cyberprzestępcami?**

**Mając świadomość tego, że incydenty związane z bezpieczeństwem cybernetycznym są nieuchronne i prawdopodobnie nieuniknione, przedsiębiorstwa korzystają z pomocy wyspecjalizowanych agencji kryminalistyki cyfrowej. Chcą w ten sposób lepiej zrozumieć metody postępowania przestępców i zwiększyć swoje szanse na wczesne wykrycie ich destrukcyjnej działalności. Aby pomóc w ściganiu cyberprzestępców są również gotowe do posługiwania się „technologicznymi oszustwami”, takimi jak wystawianie przynęty czy rozsiewanie fałszywych danych. Do takich wniosków prowadzą badania przeprowadzone przez Neustar.**

O ile ponad połowa specjalistów ds. bezpieczeństwa z regionu EMEA (Europa, Środkowy Wschód i Afryka) i Stanów Zjednoczonych twierdzi, że phishing stanowi wciąż „rosnące zagrożenie”, to 49% z nich jest również zaniepokojonych atakami ukierunkowanymi i atakami DDoS.

Badania przeprowadzone w okresie od stycznia do marca 2019 r. pokazują, że grupy cyberprzestępcze przeniosły swoją uwagę z tradycyjnego celu, którym są usługi płatnicze, na firmy oferujące oprogramowanie jako usługę (ang. Software-as-a-Service – SaaS) i internetowe usługi e-mail, dwie najszybciej rozwijające się branże – zgodnie z raportem o trendach opublikowanym przez Anti-Phishing Working Group. Znacznie zmniejszyły się natomiast ataki na usługi magazynowania danych w chmurze i hostingu witryn internetowych – z 11,3% do zaledwie 2%.

 - *Platformy SaaS i usługi poczty internetowej zyskują na popularności, ponieważ zapewniają biznesowi możliwość działania online i są łatwo dostępne dla każdego, kto ma dostęp do internetu. Niezabezpieczone połączenia Wi-Fi są jednak przyczyną podatności platform pracy grupowej oraz systemów rozliczeniowych na ataki stron trzecich, które wykorzystują dane uzyskane poprzez phishing profilowany. Po zdobyciu niezbędnych informacji hakerzy wysyłają ukierunkowane, dobrze spreparowane e-maile do kadry kierowniczej najwyższego szczebla lub najważniejszych pracowników, próbując w ten sposób przeniknąć do infrastruktury organizacji i przejąć nad nią kontrolę* - **wyjaśnia Mariusz Politowicz, inżynier techniczny Bitdefender z firmy Marken Systemy Antywirusowe** (www.bitdefender.pl).

Według analiz przeprowadzonych nad zastosowaniem złośliwym oprogramowania, 36% ataków phishingowych z pierwszego kwartału 2019 r. dotyczyło właśnie tych dwóch kategorii. W tym przypadku celem hakerów jest kradzież poufnych danych osobistych i finansowych, takich jak lokalizacja, preferencje, numery kart kredytowych, szczegóły płatności i adresy e-mail. Liczba ta „wzrosła znacząco z 30% w czwartym kwartale 2018 r. i 20,1% w trzecim kwartale tego roku. Phishing przeciwko SaaS i chmurowej poczcie elektronicznej po raz pierwszy wysunął się na czoło, zdecydowanie wyprzedzając cel, jakim są usługi płatnicze” – mówi raport.

W normalnych okolicznościach, szyfrowana wersja protokołu (HTTPS) zabezpieczałaby ruch sieciowy i pozwalała na utrzymanie integralności danych. Jednak, zgodnie z wynikami badań, hakerzy muszą manipulować przy sygnaturach TLS, ponieważ „liczba ataków phishingowych na hostowane strony internetowe, które korzystają z protokołu HTTPS i certyfikatów SSL, osiągnęła nowy poziom”.

 - *Biorąc pod uwagę całkowitą liczbę ataków phishingowych z pierwszego kwartału 2019 r., która gwałtownie wzrosła w porównaniu z dwoma poprzednimi kwartałami, działalność firm może zagrozić prywatności danych ich klientów, jeżeli będą one zwlekać z wdrożeniem właściwej polityki bezpieczeństwa* - **komentuje Mariusz Politowicz, inżynier techniczny Bitdefender z firmy Marken Systemy Antywirusowe** (www.bitdefender.pl).

Spośród wszystkich ataków phishingowych, na przykład, 27% wymierzonych było przeciw usługom płatniczym, 16% – przeciwko instytucjom finansowym, a tylko 3% dotyczyło handlu elektronicznego i usług telekomunikacyjnych.