Polski CERT zbadał pułapki na cyberprzestępców

Użyteczność tzw. honeypotów, czyli zastawianych w sieci pułapek na cyberprzestępców, zbadał zespół CERT Polska działający w ramach instytutu badawczego NASK. Polacy szczegółowo zbadali 30 różnych darmowych pułapek, z których korzystają eksperci od bezpieczeństwa internetowego.
Jak wyjaśnili przedstawiciele CERT Polska w przesłanym PAP komunikacie, honeypot (z ang. „garnek miodu"), jest zasobem umieszczonym w sieci, którego jedynym zadaniem jest to, by dostać się w ręce hakerów czy cyberprzestępców i zostać wykorzystanym w nieautoryzowany sposób. Zasobem-pułapką może być np. specjalnie przygotowany serwis, aplikacja, system czy nawet jakaś informacja. Wszystko to kusić ma cyberprzestępców do ataku.

Podstawowym założeniem jest to, że każdy, kto próbuje się połączyć lub korzystać z honeypota w jakikolwiek sposób jest z definicji podejrzany. Cała interakcja pomiędzy honeypotem i podmiotem, który się z nim łączy jest monitorowana i analizowana, aby wykryć złośliwe działania i zrozumieć ich mechanizmy.

Honeypoty mogą być stosowane m.in. do monitorowania aktywności botnetów i robaków w Internecie, zbierania informacji o zainfekowanych komputerach w sieci, wykrywania i zbierania złośliwego oprogramowania, badania zachowań hakerów oraz szukania wewnętrznych infekcji w sieci lub ataków wewnętrznych.

Jak podkreślają specjaliści z CERT Polska, honeypoty, dzięki wczesnemu ostrzeganiu o infekcji i zachowaniu złośliwego oprogramowania, pozostają bardzo dobrą platformą do pozyskiwania informacji o zmianach w taktyce cyberprzestępców.

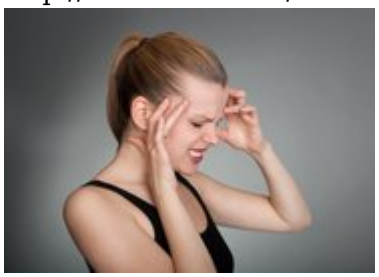
"W związku z dużą ilością dostępnych honeypotów warto było zbadać i wskazać te systemy, które mogą być najbardziej przydatne w praktyce dla ekspertów od cyberbezpieczeństwa na całym świecie, działających na przykład w krajowych zespołach reagowania na zagrożenia sieciowe. Mamy nadzieję, że nasze zestawienie przyczyni się do wyboru najlepszych narzędzi oraz metod zwalczania złośliwego oprogramowania i działalności cyberprzestępców" – mówi Piotr Kijewski, kierownik CERT Polska.

W badaniu, opublikowanym przez Europejską Agencję ds. Bezpieczeństwa Informacji, specjaliści z CERT Polska przeanalizowali pod kątem praktyczności 30 istniejących, darmowych honeypotów, które można samodzielnie zainstalować w sieci. Bezpośrednim celem było zestawienie dostępnych rozwiązań, analiza ich zalet i wad oraz wskazanie podmiotom zajmującym się cyberbezpieczeństwem najskuteczniejszych narzędzi do walki z zagrożeniami sieciowymi.

Wśród czynników branych pod uwagę były m.in. zakres wykrywania, jakość dostarczanych danych, wydajność i niezawodność oraz łatwość instalacji i obsługi. Cztery z badanych systemów - Dionaea, Glastopf, Kippo oraz Honeyd, zostały zidentyfikowane jako najbardziej użyteczne i najłatwiejsze do zainstalowania.

Więcej informacji na temat raportu CERT Polska o zastosowaniu honeypotów do wykrywania zagrożeń sieciowych (ang. „Proactive Detection of Security Incidents: Honeypots”) dla Europejskiej Agencji ds. Bezpieczeństwa Informacji, dostępnych jest na stronie: http://www.cert.pl/news/6609

źródło:www.naukawpolsce.pap.pl
http://laboratoria.net/aktualnosci/15827.html



24-09-2024

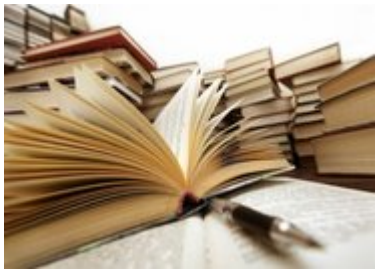
Migrena to choroba – można ją leczyć

Migrena to poważna choroba neurologiczna.

24-09-2024

Jeżeli zranimy się przy powodzi, uwaga na tężec

Szczepionki powinny być dostępne bezpłatnie w placówkach.



24-09-2024

I. Przychocka pełnomocnikiem ds. jakości

kształcenia na studiach

Będzie współpracowała na rzecz doskonalenia jakości kształcenia.

24-09-2024

Będzie kolejna edycja maratonu programistów

Zgłoszenia do 7 października.

24-09-2024

Przez dwa miesiące Ziemia będzie miała dwa księżyce

Od 29 września do 25 listopada.

24-09-2024

Astma oskrzelowa popowodziową konsekwencją

Powiedział PAP prof. Bolesław Samoliński, alergolog.

24-09-2024

SpaceX planuje wystrzelenie 5 bezzałogowych misji na Marsa

Ma się to odbyć w ciągu dwóch lat.

24-09-2024

Potrzebne są globalne ustalenia odnośnie mikroplastiku

Okazją do działania może być przygotowywany przez ONZ traktat.

Informacje dnia: Migrena to choroba – można ją leczyć Jeżeli zranimy się przy powodzi, uwaga na tężec I. Przychocka pełnomocnikiem ds. jakości kształcenia na studiach Będzie kolejna edycja maratonu programistów Przez dwa miesiące Ziemia będzie miała dwa księżyce Astma oskrzelowa popowodziową konsekwencją Migrena to choroba – można ją leczyć Jeżeli zranimy się przy powodzi, uwaga na tężec I. Przychocka pełnomocnikiem ds. jakości kształcenia na studiach Będzie kolejna edycja maratonu programistów Przez dwa miesiące Ziemia będzie miała dwa księżyce Astma oskrzelowa popowodziową konsekwencją Migrena to choroba – można ją leczyć Jeżeli zranimy się przy powodzi, uwaga na tężec I. Przychocka pełnomocnikiem ds. jakości kształcenia na studiach Będzie kolejna edycja maratonu programistów Przez dwa miesiące Ziemia będzie miała dwa księżyce Astma oskrzelowa popowodziową konsekwencją

Partnerzy