Raport Acronis na temat cyberzagrożeń za pierwsze półrocze 2023 r.

Acronis

Od innowacji do ryzyka: zarządzanie konsekwencjami cyberataków opartych na sztucznej inteligencji

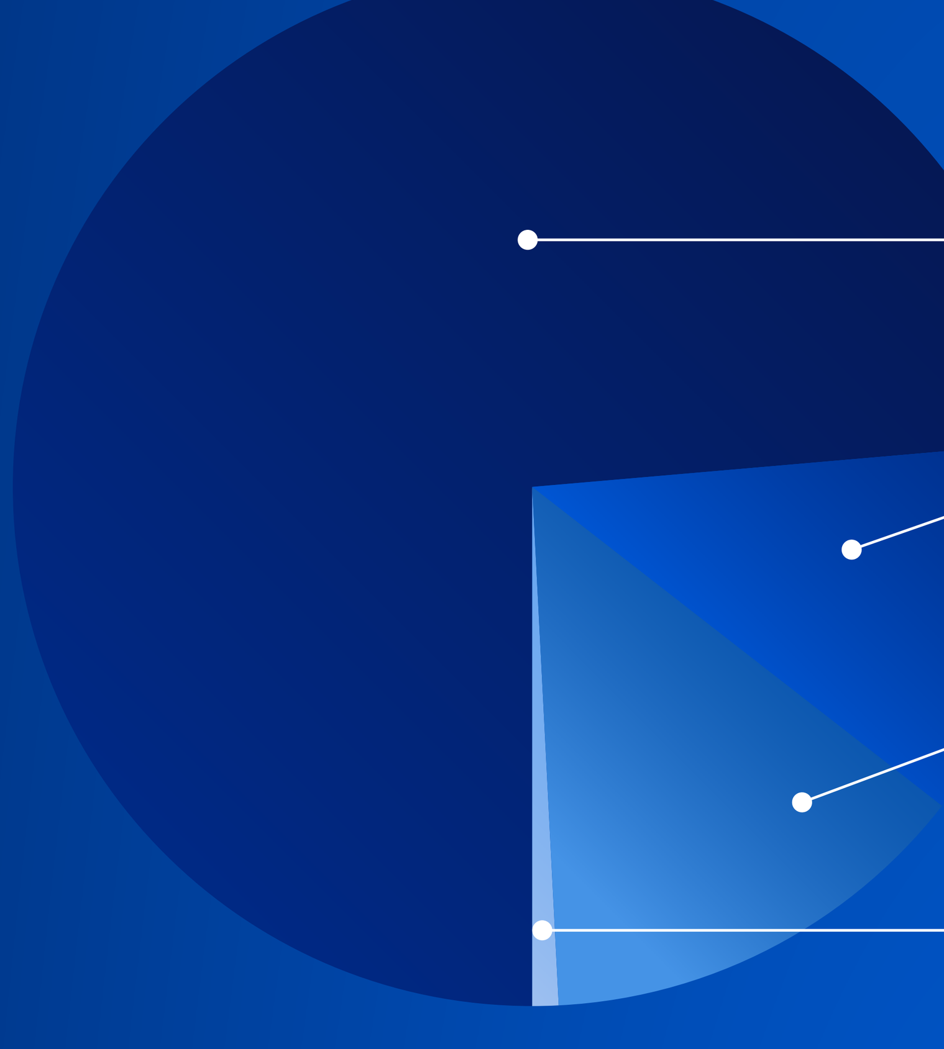
Zapoznaj się z kluczowymi wnioskami z naszego najnowszego raportu dotyczącego cyberzagrożeń, który przedstawia globalną perspektywę opartą na danych z ponad 1 000 000 unikalnych urządzeń końcowych rozmieszczonych na całym świecie. Większość omawianych statystyk koncentruje się na zagrożeniach dla systemów operacyjnych Windows, ponieważ są one znacznie bardziej rozpowszechnione w porównaniu z systemami macOS i Linux.

5 najważniejszych trendów w cyberbezpieczeństwie w I połowie 2023 r.

- Ataki za pośrednictwem poczty elektronicznej wzrosły aż o 464%
- Ataki na łańcuch dostaw dotknęły ponad 60 000 klientów
- Rosnąca popularność ChatGPT – wykorzystywanie sztucznej inteligencji do przeprowadzania cyberataków i tworzenia złośliwych treści
- Kradzież danych stanowi drugie najczęściej występujące zagrożenie
- Ransomware nadal jest głównym zagrożeniem dla dużych i średnich firm – znaczny wzrost liczby ataków w marcu

Stany Zjednoczone były celem prawie połowy z 459 udanych zgłoszonych ataków w marcu – wymierzone były w 221 ofiar (48%)

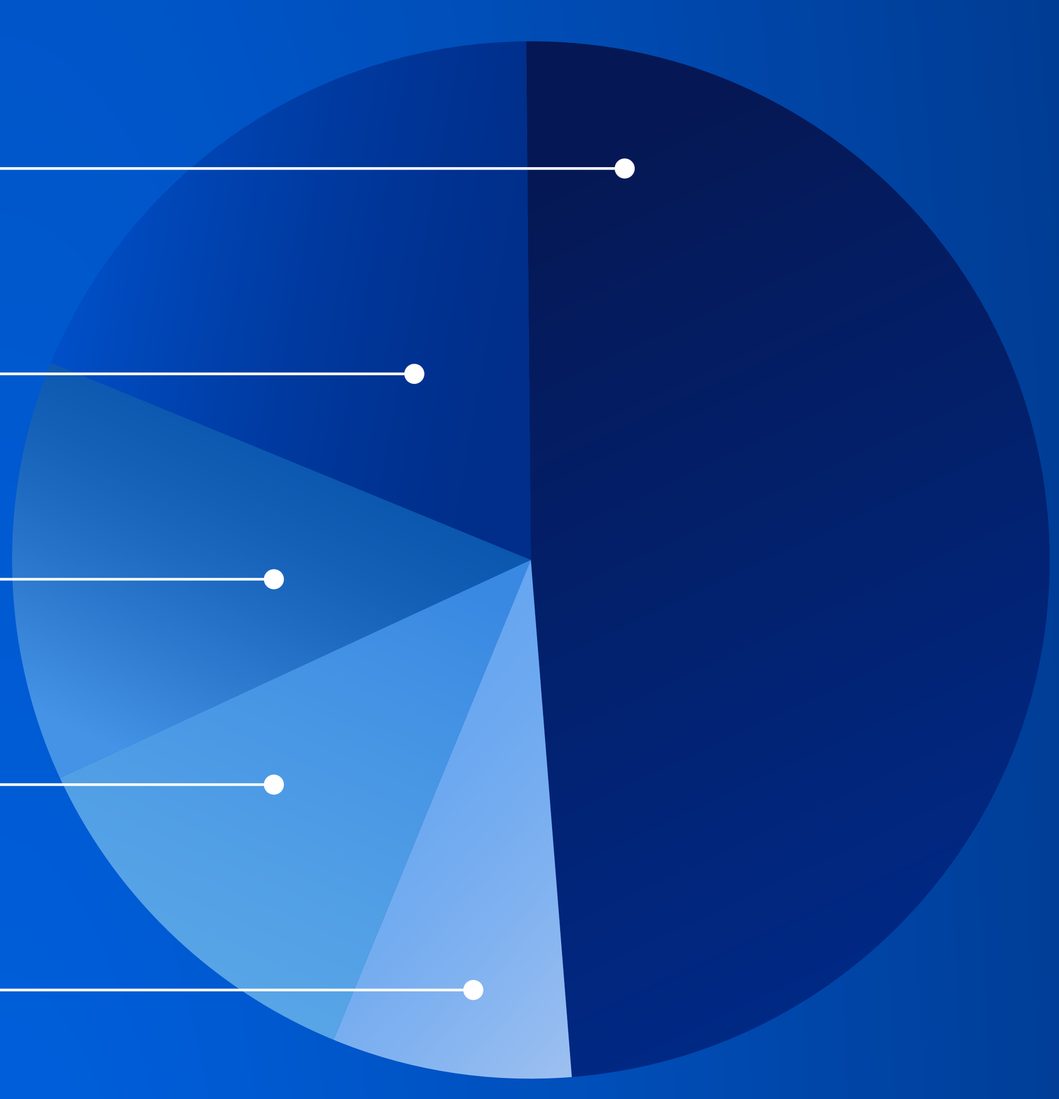
Najpopularniejsze zagrożenia cybernetyczne



- 73% Phishing
- 15% Inżynieria społeczna / włamania do firmowej poczty e-mail
- 11% Złośliwe oprogramowanie
- 1% Zaawansowane ataki

5 najważniejszych gangów ransomware według liczby ofiar

- 49% LockBit
- 19% Clop
- 13% BlackCat / ALPHV
- 12% Royal
- 7% Play



10 krajów z największą liczbą zablokowanych adresów URL w kwietniu 2023 r.

Pozycja	Kraj	Odsetek zablokowanych adresów URL w kwietniu 2023 r.
1	Niemcy	20,9
2	Singapur	13,9
3	Włochy	11,7
4	Wielka Brytania	10,3
5	Szwajcaria	9,1
6	Japonia	9
7	Francja	7,1
8	Hiszpania	4,5
9	Indie	4,4
10	Holandia	2,6

10 krajów z największą liczbą wykrytego złośliwego oprogramowania w kwietniu 2023 r.

Pozycja	Kraj	Odsetek wykrytego złośliwego oprogramowania w kwietniu 2023 r.
1	Korea Południowa	26
2	Egipt	25,7
3	Singapur	23,2
4	Tajwan	21,1
5	Chiny	20,4
6	Wietnam	18,2
7	Maroko	17,1
8	Argentyna	16,3
9	Turcja	15,7
10	Nigeria	14,5

Wzrost wykorzystania AI:

Cyberprzestępcy eksperymentują z nową generacją sztucznej inteligencji w celu optymalizowania ataków. Mogą użyć sztucznej inteligencji do tworzenia, automatyzacji, skalowania i ulepszania nowych ataków przez aktywne uczenie się.

Dostępność dużych modeli językowych (LLM), takich jak ChatGPT, umożliwia cyberprzestępcom przeprowadzanie jeszcze większej liczby ataków przez automatyzację i powtarzanie. Doprowadziło to do wzrostu liczby podmiotów aktywnych na rynku ransomware.

W I kwartale 2023 roku pojawiło się 10 nowych grup, które łącznie przyznały się do 61 cyberataków na całym świecie.

Abyss	1
Dark Power	10
Akira	9
Money Message	8
Trigona	7
Do it	7
Vendetta	3
Cryptnet	2
CrossLock	1
Nevada	0

Jak zapewnić bezpieczeństwo cybernetyczne w przyszłości i stać się #CyberFit?

Współczesne cyberataki, wycieki danych i epidemie ransomware wskazują na to samo: obecne podejście do cyberbezpieczeństwa zawodzi. Aby zwalczyć te zagrożenia, zastosuj poniższe wskazówki:

1. Korzystaj ze zintegrowanego rozwiązania do ochrony cybernetycznej (takiego jak Acronis Cyber Protect), które łączy ochronę przed złośliwym oprogramowaniem, EDR, DLP, ochronę poczty e-mail, ocenę podatności na zagrożenia, zarządzanie poprawkami, RMM i tworzenie kopii zapasowych w jednym agencie.
2. Wprowadź rozwiązanie do wykrywania i reagowania w punktach końcowych (EDR), aby zapewnić widoczność potrzebną do zrozumienia ataków, jednocześnie upraszczając kontekst dla administratorów i umożliwiając skuteczne usuwanie wszelkich zagrożeń.
3. Stale aktualizuj system operacyjny i aplikacje. Wiele ataków okazuje się skutecznymi z powodu niezałatanych luk w zabezpieczeniach. Regularnie stosuj funkcje oceny podatności na zagrożenia i zarządzania poprawkami.
4. Uważaj na próby wyłudzania informacji. Korzystanie z dodatkowej, specjalnej funkcji filtrowania adresów URL może pomóc w odfiltrowaniu wiadomości wyłudzających informacje i podejrzanych linków.
5. Upewnij się, że Twoje rozwiązanie do spraw cyberbezpieczeństwa jest poprawnie skonfigurowane. Co najmniej raz dziennie należy wykonywać pełne skanowanie, a skanowanie na żądanie i przy dostępie (w czasie rzeczywistym) powinno być włączone i reagować na każdą nową instalację lub uruchomienie oprogramowania.
6. Najważniejsza porada dotycząca bezpieczeństwa: zachowaj prywatność haseł i przestrzeni roboczych. Upewnij się, że Twoje hasła są silne i nigdy nikomu ich nie udostępniaj.

Acronis