WHITEPAPER

Bitdefender®

Security

Dokumentacja techniczna Anti-ransomware

www.bitdefender.pl

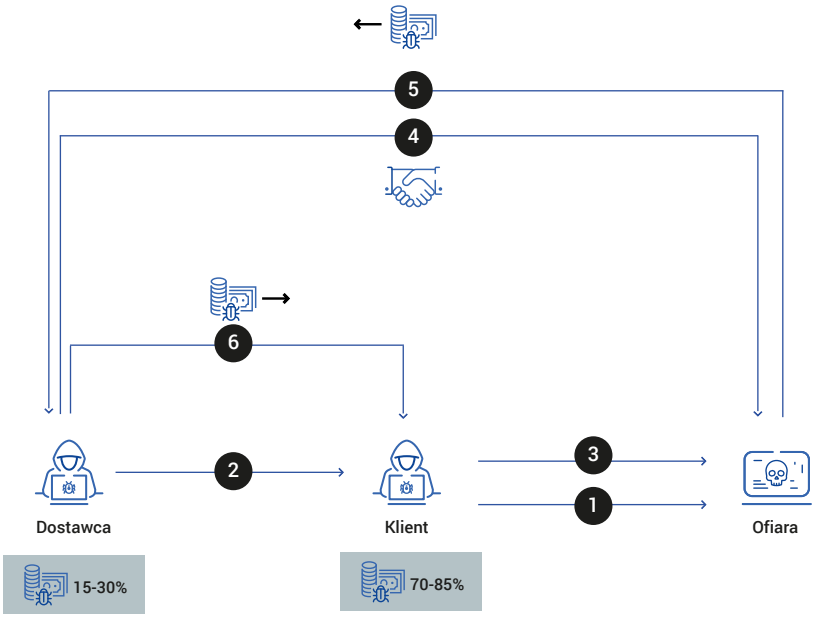
Spis treści

Ransomware jako usługa (Ransomware 2.0)

Ekosystemem cyberprzestępczości kierują te same siły ekonomiczne, które rządzą zwyczajnymi rynkami. Nowa koncepcja biznesowa lub pomysł mogą szybko stać się nowym standardem, zastępując ostatecznie poprzednie praktyki biznesowe.

Jedna z takich rewolucji przeprowadzona została w podziemiu przy pomocy modelu Ransomware-as-a-Service (Raas), opartego na podziale zysków. W jego ramach dostawcy kodu złośliwego oprogramowania pracują wspólnie z klientami, ale współpraca ta wykracza poza program sprzedaży abonamentowej, jak często się to opisuje. Dzisiaj prawdopodobieństwo ataku RaaS jest znacznie większe, niż zagrożenie ze strony cyberprzestępców wykorzystujących starsze metody pracy.

Dostawcy RaaS opracowują złośliwy kod i uruchamiają infrastrukturę. Zadaniem klientów, działających podobnie do samozatrudnionych podwykonawców, jest przełamanie ochrony sieci. Kiedy osiągną swój cel, a złośliwe oprogramowanie zostanie zainstalowane, dostawcy RaaS przystępują do negocjacji okupu, a uzyskaną kwotą dzielą się z klientami.
Jeśli przypomina ci to fabułę rodem z filmu sensacyjnego, to jesteś na dobrym tropie – grupa wykwalifikowanych specjalistów po wykonaniu swojej misji ucieka z dużą sumą pieniędzy. Grupy ransomware wykorzystują klientów do prowadzenia operacji na szeroką skalę, atakując jednocześnie wiele organizacji. Każdy kolejny sukces oznacza większe fundusze, lepsze narzędzia i bardziej zaawansowane praktyki.



1. Klient uzyskuje dostęp do sieci ofiary.
2. Dostawca RaaS zapewnia klientowi złośliwy kod wyposażony w unikalny identyfikator.
3. Klient uruchamia atak, pozyskując dane i wprowadzając oprogramowanie RaaS.
4. Dostawca kodu negocjuje wielkość okupu z ofiarą ataku.
5. Dostawca pobiera okup i przesyła klucz deszyfrujący.
6. Dostawca przekazuje klientowi uzgodnioną część zysku.

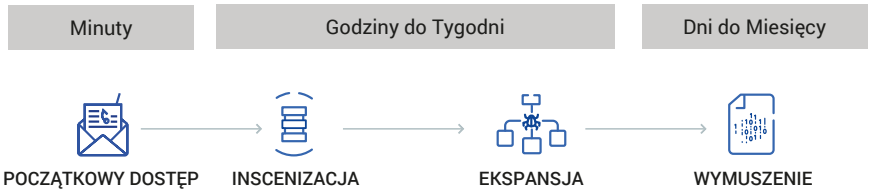
Podział zysków w ramach modelu Ransomware-as-a-Service – klienci z uwagi na dostęp do sieci otrzymują największą część zysków.

Ten nowy model stanowi dla cyberprzestępców nie lada motywację do poszukiwania nowych sposobów na zwiększenie uzyskiwanych korzyści. Atakujący myślą niczym wytrawni biznesmeni, reinwestując swoje zyski w doskonalenie taktyk i narzędzi do następnego ataku. Wraz ze wzrostem świadomości biznesowej zwiększa się także presja, co przekłada się na wielkość żądanego okupu. Ten uniwersalny model został sprawdzony na wszystkich szczeblach zarządzania w firmach o różnej wielkości.

Niewiadomą pozostaje jednak proporcja podziału zysków – zakłada się, że jest ona korzystniejsza dla atakujących klientów, którzy zazwyczaj otrzymują nawet 90% łupu. Z kolei dostawcy RaaS prowadzą negocjacje i zyskują popularność w przypadku udanego ataku. Umarł król, niech żyje król – w ciągu ostatnich kilku lat osoby zapewniające dostęp do sieci zdecydowanie przejęły władzę od dostawców złośliwego kodu.

Anatomia ataku ransomware

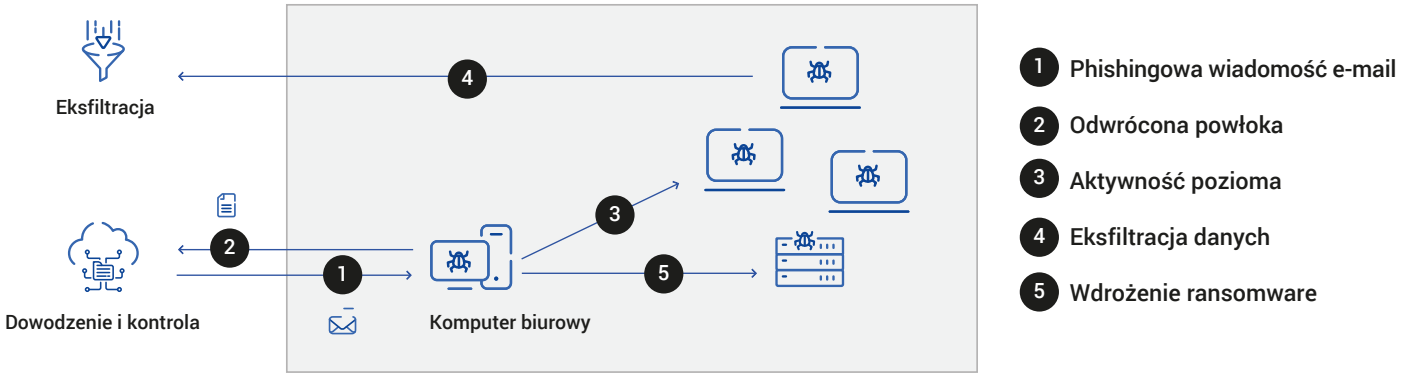
Zmiana osób „u władzy" mocno wpłynęła na strukturę ataków ransomware. Wcześniej bazowały one na metodzie działania robaków komputerowych (WannaCry) i skupiały się na jak najszybszej monetyzacji działań. Model podziału zysków jednak wymusza na cyberprzestępcach przyjęcie określonych taktyk, technik i procedur, stosowanych przez grupy APT (Advanced Persistend Threat Groups). Ataki tego typu nie skupiają się na szybkości, a na wyrządzeniu jak największych szkód i wywarciu jak najmocniejszego nacisku. Cyberprzestępcy potrafią spędzić całe miesiące na planowaniu i przygotowywaniu kolejnego ataku.



Zainstalowanie złośliwego oprogramowania na urządzeniu ofiary zazwyczaj poprzedzają tygodnie przygotowań.

W takim ujęciu nowoczesny kod ransomware to po prostu kolejny rodzaj oprogramowania, wdrażanego na ostatnim etapie tzw. „łańcucha zabójstw" kill chain, po uprzednim dokładnym zaplanowaniu całej akcji. Najskuteczniejszą strategią przeciwko tego typu atakom jest zastosowanie architektury opartej na zasadzie pogłębionego bezpieczeństwa. Najlepszą ochronę w tym zakresie zapewnia wysokiej jakości prewencyjna kontrola bezpieczeństwa, wzbogacona o funkcję wykrywania zagrożeń i reagowania na nie z naciskiem na szybkość i ograniczenie liczby fałszywych alarmów.

Ten schemat ilustruje strukturę typowego ataku ransomware. Użytkownik otrzymuje phishingową wiadomość e-mail. Po jej otwarciu na urządzeniu, zostaje ono zainfekowane (faza początkowa). Na serwerze C&C uruchomiona zostaje odwrócona powłoka (faza uruchomienia). Atakujący klient ransmoware przeprowadza rozpoznanie, wyszukuje i paraliżuje system bezpieczeństwa (faza ekspansji). Po eksfiltracji danych i pełnym uruchomieniu złośliwego oprogramowania, cyberprzestępca kontaktuje się ze swoją ofiarą w celu uzyskania okupu (faza wymuszenia).



Struktura typowego ataku ransomware. Nowym standardem w branży jest podwójne wymuszenie, gdzie pierwsza próba pobrania okupu następuje przed wdrożeniem złośliwego oprogramowania.

Przyjrzyjmy się poszczególnym elementom współczesnego „łańcucha zabójstw", czyli cyber kill chain ransomware.

Początkowy dostęp	Inscenizacja	Ekspansja	Wymuszenie

Kierunek fazy początkowej infekcji zazwyczaj zależy od wielkości celu oraz stopnia zaawansowania jego systemu zabezpieczeń. Ogólnie rzecz biorąc w przypadku mniejszych firm stosuje się zazwyczaj metodę ataków automatycznych dostosowanych do skali przedsięwzięcia, zaś w przypadku dużych korporacji – metodę spear phishing. Wysiłek, jaki w przygotowanie ataku wkłada cyberprzestępca, jest wprost proporcjonalny do oczekiwanych przez niego zysków.

Duże firmy, wyposażone w zaawansowane systemy bezpieczeństwa, to trudny cel. W ich przypadku hakerzy najczęściej skupiają się na phishingu i taktykach socjotechnicznych. Część przestępców jednak koncentruje się na łańcuchu dostaw. Ważni gracze to łakomy kąsek – czasem łatwiej dobrać się do nich, atakując od słabo strzeżonego zaplecza, zamiast szturmować dobrze chronioną bramę główną.

Małe i średnie firmy mogą znaleźć się na celowniku wyrafinowanych cyberprzestępców jako część zbiorczego celu w ramach operacji przeprowadzanych na większą skalę.

Piętą achillesową małych i średnich przedsiębiorstw często bywają luki w zabezpieczeniach zdalnego dostępu do sieci. Cyberprzestępcy doskonale zdają sobie z tego sprawę, wykorzystując tę słabość na swoją korzyść. Umożliwia ona hakerom uzyskanie dostępu za pośrednictwem pulpitu zdalnego, wykradzionych lub odgadniętych danych do logowania. Innym popularnym kierunkiem ataków ransmoware są niezabezpieczone programy internetowe. W tym przypadku cybeprzestępcy biorą na cel programy dostawców zewnętrznych, takie jak VPN czy rozwiązania do zdalnego udostępniania, i wykorzystują ich słabości. Ograniczenie ryzyka związanego z taką strategią wymaga ustanowienia mocnego hasła i loginu, które trudno będzie odgadnąć przestępcy.

Początkowy dostęp	**Inscenizacja**	Ekspansja	Wymuszenie

Po uzyskaniu dostępu cyberprzestępcy skupiają się na przygotowaniu środowiska do ataku. Ten etap ma zazwyczaj dwa cele – zwiększenie uprawnień i uniemożliwienie szybkiej neutralizacji złośliwego kodu, jednocześnie unikając wykrycia. Zwiększenie uprawnień na ogół zakłada użycie narzędzi hakerskich do kradzieży informacji o koncie i przeprowadzania testów penetracyjnych, takich jak Mimikatz czy Cobalt Strike.

Niektórzy cyberprzestępcy obierają sobie za główny cel ustanowienie stałego dostępu do infrastruktury firmy. Dostęp taki można spieniężyć na platformach sprzedażowych dark web, sprzedając go na przykład osobom, powiązanym z grupami ransomware.

Początkowy dostęp	Inscenizacja	**Ekspansja**	Wymuszenie

Faza ekspansji zakłada rekonesans środowiska i tzw. aktywność poziomą, czyli przeprowadzanie infekcji w całej sieci. Na tym etapie używane są narzędzia do analizy danych, takie jak BloodHound – atakujący starają się uniknąć wykrycia i w tym celu wykorzystują „naturalne zasoby" otoczenia. Ta metoda znana jest pod nazwą „Living off the Land" (LotL) i obejmuje takie narzędzia, jak WMIC i PowerShell. Inna taktyką cyberprzestępców jest określenie, z jakich narzędzi korzystają administratorzy systemu, na przykład PsExec, TeamViewer, czy AnyDesk.

W takim przypadku cyberprzestępców może zdradzić wyłącznie ich podejrzane zachowanie, ponieważ nie korzystają z narzędzi hakerskich.

Początkowy dostęp	Inscenizacja	Ekspansja	**Wymuszenie**

Aby uzyskać astronomiczną kwotę okupu (w porównaniu ze średnią wielkością okupu zaledwie kilka lat wcześniej), cyberprzestępcy koncentrują się na wywarciu jak największego nacisku na ofiary. Samo zaszyfrowanie przypadkowych danych nie wystarczy. Standardową praktyką stają się podwójne i potrójne wymuszenia. Atak ransomware może iść w parze z eksfiltracją danych (w celu szantażowania ofiary), atakiem DoS, a także nękaniem kadry kierowniczej, partnerów handlowych i klientów. Ważną rolę podczas fazy wymuszania odgrywa wiedza na temat prowadzenia działalności i finansów firmy. Cyberprzestępcy często zdają sobie sprawę, jaki wpływ wywrą ich działania, wiedzą, które informacje są cenne, znają procedury reagowania na incydenty i są świadomi zakresu ubezpieczenia ofiary od ryzyk cybernetycznych.

Hakerzy jeszcze przed dostarczeniem złośliwego oprogramowania niszczą wszystkie dostępne kopie zapasowe danych. Kod ransomware można dostarczyć na różne sposoby, ale do jego uruchomienia na urządzeniu końcowym zazwyczaj używa się popularnych, prostych i niezawodnych narzędzi, takich jak PsExec/WMIC, Group Policy, a nawet narzędzi do zarządzania systemem jak Microsoft System Center Configuration Manager.

Jak bronić się przed nowoczesnymi atakami oprogramowania ransomware

Najskuteczniejszą strategią przeciwko tego typu atakom jest zastosowanie architektury opartej na zasadzie pogłębionego bezpieczeństwa. Warto zacząć od zwiększenia odporności na ataki, a następnie wdrożyć automatyczne, prewencyjne mechanizmy kontrolne, które pozwolą uniknąć większości incydentów. Z pozostałymi rozprawić powinny się procedury bezpieczeństwa, wspomagane przez narzędzia do wykrywania zagrożeń i reagowania na nie.

Zmniejszenie powierzchni ataku

W myśl powiedzenia, że najlepszy cyberatak, to taki, który nigdy się nie wydarzył, jednym z najlepszym sposobów, aby uniknąć zagrożeń ze strony hakerów, jest wdrożenie zestawu dobrych praktyk w sferze cyfrowej i ich skrupulatne przestrzeganie. Zwiększenie odporności na ataki to jeden z najtańszych i najskuteczniejszych sposób na poprawę bezpieczeństwa cyfrowego w twojej firmie. W tym celu należy wdrożyć rzetelne zarządzanie zasobami, automatyczne instalowanie aktualizacji oprogramowania, architekturę Zero Trust oraz politykę wykrywania i naprawiania błędnych konfiguracji i niezabezpieczonych ustawień domyślnych.

Ataki automatyczne dostosowane do skali przedsięwzięcia zazwyczaj zaczynają się od skanowania Internetu pod kątem systemów podatnych na cyberzagrożenia z uwagi na brak spójności albo opóźnioną procedurę instalowania aktualizacji. Wraz ze wzrostem popularności programów do współpracy zdalnej wzrosło także znaczenie ochrony cyfrowej. Jedną z głównych metod uniemożliwienia niepowołanym osobom dostępu do infrastruktury firmy z poziomu systemów peryferyjnych jest sprawna i ciągła aktualizacja oprogramowania. **GravityZone Patch Management** to zautomatyzowany moduł, którego zadaniem jest stała weryfikacja i aktualizacja systemów operacyjnych i aplikacji. Rozwiązanie oferuje funkcję raportowania, która zapewnia pełną widoczność i kontrolę nad stanem aktualizacji na wszystkich punktach końcowych.

Jeśli cyberprzestępcy nie będą w stanie namierzyć słabych stron twojego stosu technologicznego, skupią się na polityce bezpieczeństwa i wprowadzania nowych programów. **GravityZone Endpoint Risk Analytics** dostarcza najważniejsze informacje na temat nieprawidłowych konfiguracji na punktach końcowych oraz dane dotyczące słabych stron oprogramowania. Rozwiązanie oferuje także rekomendacje dla punktów końcowych (takie, jak dodatkowe zabezpieczenie systemu operacyjnego albo zmiany w zarządzaniu konfiguracjami) oraz wiedzę na temat zagrożeń związanych z użytkownikami, obejmującą na przykład informowanie o użytkownikach, którzy szczególnie często padają ofiarą ataków hakerskich. Rekomendacje są oceniane według ich wagi, a poprawki mogą być wdrażane automatycznie lub ręcznie.

Zarówno funkcja zarządzania aktualizacjami, jak i rozwiązanie do analizy ryzyka, zapewniają maksymalny poziom ochrony tylko, jeśli związane z nimi procesy są ciągłe. Dobrze dobrane, łatwe w obsłudze rozwiązanie pomoże twojej firmie przestrzegać najlepszych standardów cyberbezpieczeństwa.

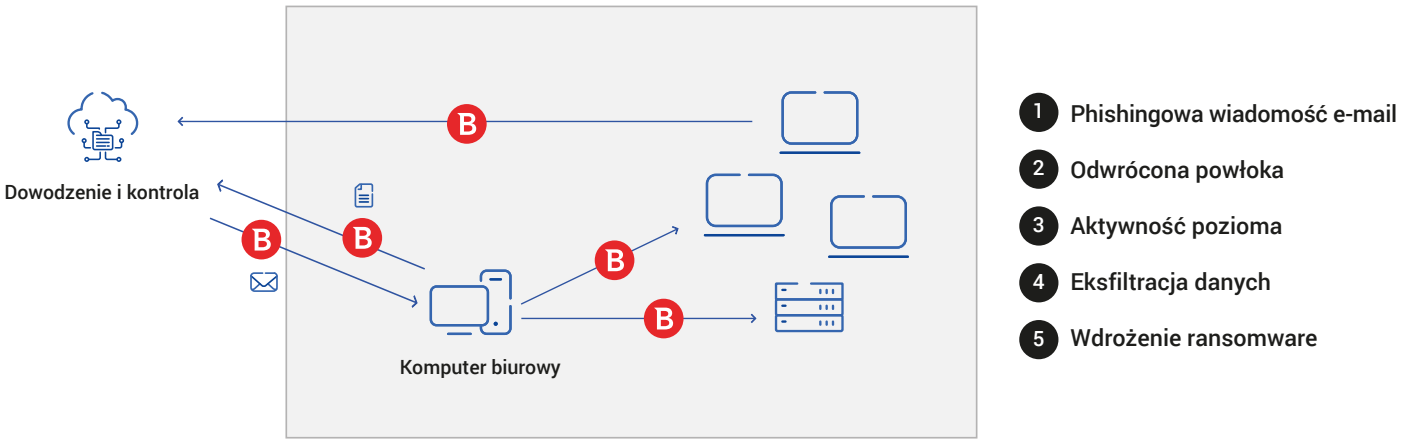
Wielowarstwowa ochrona

Zwiększenie odporności systemu na ataki świetnie sprawdzi się w przypadku cyberprzestępców, bazujących na metodzie działania robaków komputerów, ale raczej nie poradzi sobie z atakami ukierunkowanymi, czy długotrwałymi (ATP). Zdeterminowany haker znajdzie inny sposób, aby uzyskać dostęp do twojej organizacji, decydując się na skorzystanie z technik manipulacji społecznej albo zaatakowanie łańcucha dostaw.

Najskuteczniejszą strategią przeciwko tego typu zagrożeniom jest zastosowanie architektury opartej na zasadzie pogłębionego bezpieczeństwa. Jej fundamentem powinien być szereg prewencyjnych mechanizmów kontrolnych z zakresu bezpieczeństwa o szerokim zasięgu z wykorzystaniem różnych technik rozpoznawania złośliwej zawartości.

Tutaj ważna jest także harmonia – wykrywanie zagrożeń nie może generować zbyt wiele zamieszania w formie fałszywych alarmów. Zespół Bitdefender spędził ponad 20 lat, szlifując swoje algorytmy, aby znaleźć złoty środek.

Na każdym etapie ataku cyberprzestępca musi ominąć wiele kontroli bezpieczeństwa, co oznacza, że podejrzany plik może uruchomić kilka alarmów na raz! Poniższy schemat obrazuje, jak wygląda faza początkowa ataku w przypadku phishingowej wiadomości e-mail.

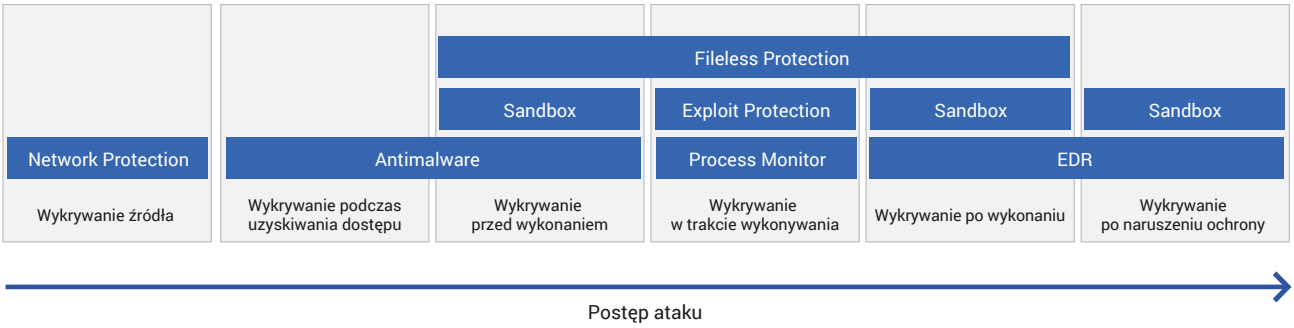


Przykład działania funkcji automatycznego wykrywania zagrożeń Bitdefender podczas pierwszej fazy kill chain ataku ransomware.

Ten prosty atak jest wykrywany na platformie GravityZone kilkukrotnie.

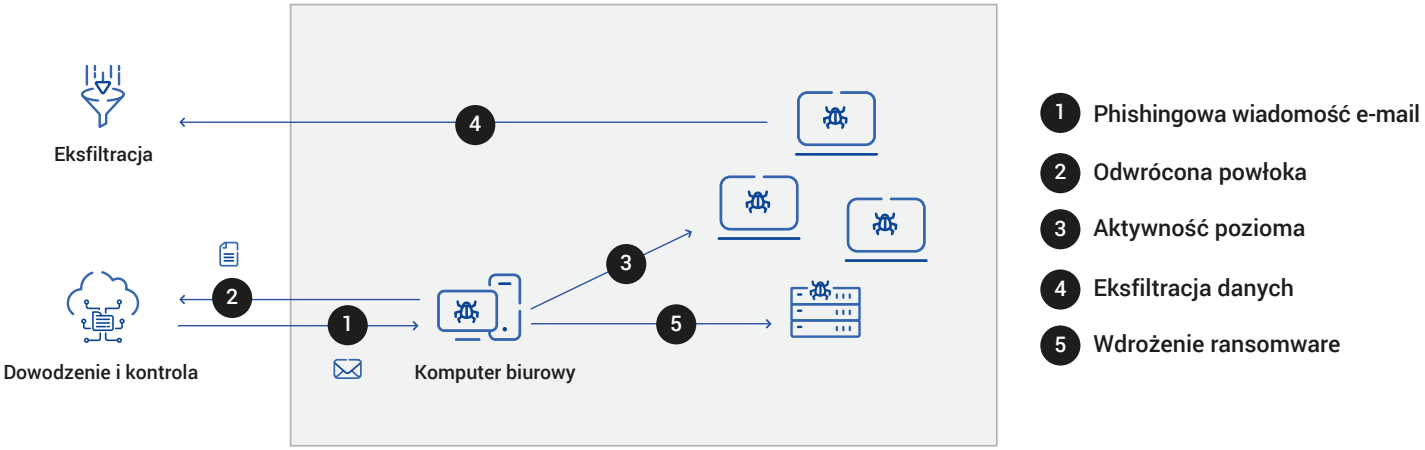
1. Przed dostarczeniem wiadomości z podejrzanym załącznikiem do skrzynki użytkownika, funkcja **GravityZone Security for Email** kilkukrotnie ją skanuje i analizuje, aby wykryć potencjalne zagrożenie.
2. Po otwarciu załącznika silnik analizy statycznej skanuje jego zawartość i sprawdza, czy zagrożenie jest mu znane. Rozwiązanie najlepiej radzi sobie ze złośliwym oprogramowaniem, z którym miało do czynienia wcześniej. Jeśli plik nie zostanie rozpoznany podczas analizy statycznej, do gry wkracza nasz **moduł maszynowego uczenia się**, zapewniający możliwość wykrywania najbardziej wyrafinowanych zagrożeń, obsługę zaciemnionego kodu i różnych formatów archiwów.
3. Po otwarciu dokumentu, zanim zawarty w nim kod zostanie uruchomiony, plik przesyłany jest do narzędzia **Sandbox Analyzer**. Podejrzany obiekt jest detonowany w środowisku zamkniętym, zapewniając w ten sposób możliwość dogłębnej analizy jego zachowania i uzyskanie informacji na temat funkcjonowania kodu VBA.
4. Jeśli kod VBA zostanie uruchomiony w pamięci, aktywuje się kilka mechanizmów kontroli bezpieczeństwa. Najpierw uruchamiana jest **funkcja ochrony przeciwko atakom bezplikowym**. Obejmuje ona analizę wykonywanego kodu, ochronę w czasie rzeczywistym przy pomocy Antimalware Scan Interface (AMSI), ochronę przed tzw. „wstrzykiwaniem kodu" (ang. code injection) oraz skanowanie pamięci po odpakowaniu pliku. Następnie do gry wchodzi **Exploit Defence** – rozwiązanie zaprojektowane, aby zapewnić dodatkową ochronę najpopularniejszym programom, w tym programom Microsoft Office. Jeśli pojawi się podejrzany proces, na przykład jeśli plik wykonywalny Microsoft Office będzie próbował utworzyć nowy wiersz poleceń, uruchomiona zostanie technologia **Process Inspector**, która umożliwia monitorowanie procesów w czasie rzeczywistym w oparciu o anomalie zachowań.
5. Złośliwe mini-programy zapisane w języku VBA, zaczynają atak od pobrania większej ilości kodu z serwera C&C. Jednak przed rozpoczęciem pobierania wirus musi stawić czoła rozwiązaniu **Network Attack Defence**, które skanuje dane przy użyciu zaawansowanych informacji o zagrożeniach i reputacji konkretnych adresów IP i URL , aby określić, czy adres serwera C&C nie jest przypadkiem powiązany ze złośliwym kodem i czy pobieranie nie powinno zostać zablokowane. Jeśli program dopuści do pobrania pliku, jego uruchomienie spowoduje aktywację całego łańcucha kontroli bezpieczeństwa.
6. Uruchomienie złośliwego kodu skutkuje powstaniem odwróconej powłoki dla atakującego. To z kolei powoduje ponowne uruchomienie wszystkich wspomnianych wyżej procedur detekcji, w tym sprawdzenia reputacji adresu IP / URL. Na tym etapie narzędzie **Network Attack Defence** rozpoznaje schemat zachowania programu jako odwróconej powłoki i blokuje go.

To przykład nakładania się pracy kilku modułów bezpieczeństwa podczas jednego etapu ataku. Taki sam stos bezpieczeństwa zostałby zastosowany podczas pozostałych etapów ataku ransomware – od rozszerzania przywilejów, aż po aktywność poziomą w całej sieci. Każda detekcja może uruchomić funkcję reagowania na incydenty, co uniemożliwi cyberprzestępcy rozwinięcie skrzydeł. Stos bezpieczeństwa Bitdefender zapewnia ochronę przed, w trakcie, a nawet po pojawieniu się podejrzanego incydentu.



Prezentacja wielowarstwowej ochrony podczas różnych etapów uruchomienia złośliwego oprogramowania.

Każdy z wyżej opisanych mechanizmów kontroli bezpieczeństwa to potężne narzędzie, ale to ich połączenie sprawia, że Bitdefender króluje w niezależnych testach wydajności. Sprawna integracja rozwiązań umożliwia spójną współpracę mechanizmów, a nasz centralny silnik stale analizuje dane zbierane z różnych źródeł. Nawet gdy działalność cyberprzestępcy nie ma typowo złośliwej natury, może ona uruchomić alarm w oparciu o kontekst wcześniejszych działań, na przykład w przypadku gdy skrypt PowerShell próbuje przesłać dane po wykryciu przez system aktywności poziomej.



Różne etapy wdrożenia ransomware są w stanie uruchomić funkcję wykrywania incydentów. Współczesne ataki ransmoware generują dostatecznie dużo zamieszania, aby zespoły zajmujące się bezpiczeństwem były w stanie je wykryć.

Minimalizacja ekspozycji na zagrożenia

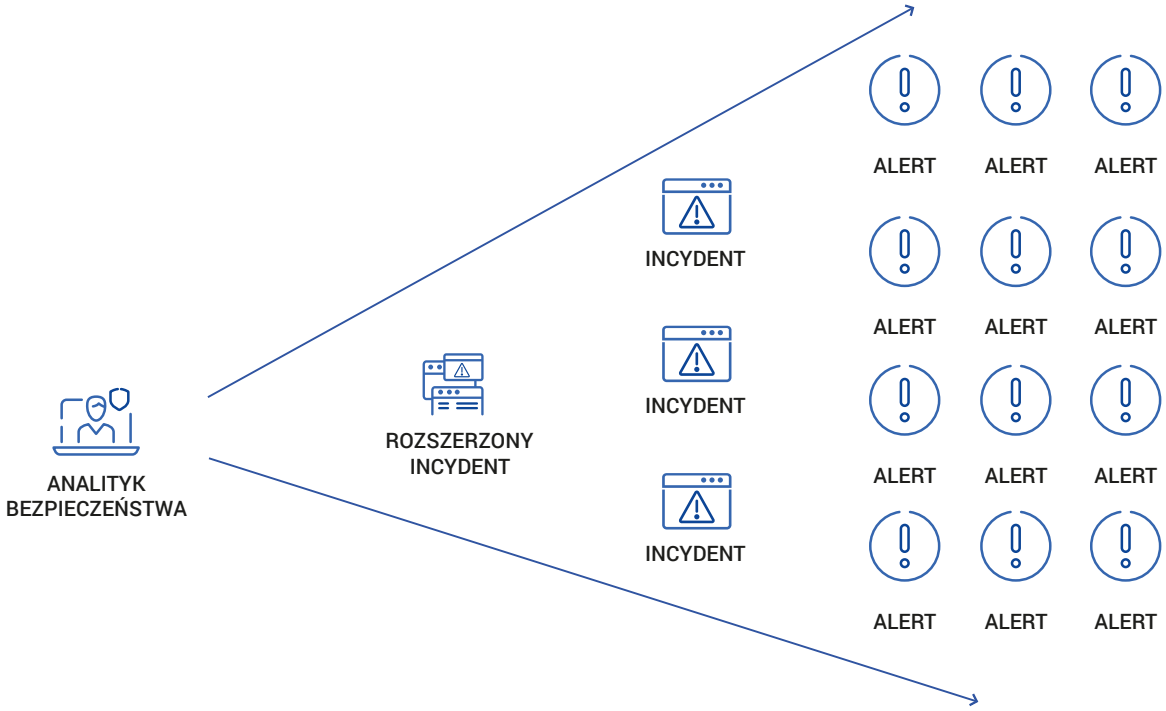
Poleganie na kopiach zapasowych i działaniach prewencyjnych okazało się mało efektywne już w starciu z atakami ransomware, bazującymi na metodzie działania robaków komputerowych poprzedniej generacji. Nic dziwnego, że w przypadku współczesnych zagrożeń ransomware, skoncentrowanych na maksymalizacji szkód i wywarciu jak największej presji na ofiary, to podejście kompletnie straciło sens.

Szczęście w nieszczęściu, że techniki sponsorowanych przez państwo grup ATP, jakimi posługują się nowocześni cyberprzestępcy, wymagają więcej czasu i przygotowań przed przeprowadzeniem ataku, generują sporo zamieszania i pozostawiają za sobą ślady działalności, które pozwalają zespołom zajmującym się bezpieczeństwem na ich wykrycie i dokładną identyfikację. Najlepszym sposobem na stawienie czoła takim metodom jest zastosowanie narzędzi defensywnych, które świetnie sprawdzają się w przypadku grup APT.

Ale łatwiej powiedzieć, niż zrobić. W wielu małych i średnich firmach brakuje zaawansowanych procedur bezpieczeństwa i wykwalifikowanych pracowników. Chociaż braki w kadrach to akurat problem, z którym borykają się wszystkie organizacje, niezależnie od ich rozmiaru. Niemniej jednak jedną z przyczyn tak dużej efektywności nowych taktyk ransomware jest właśnie brak przygotowania ze strony potencjalnych ofiar.

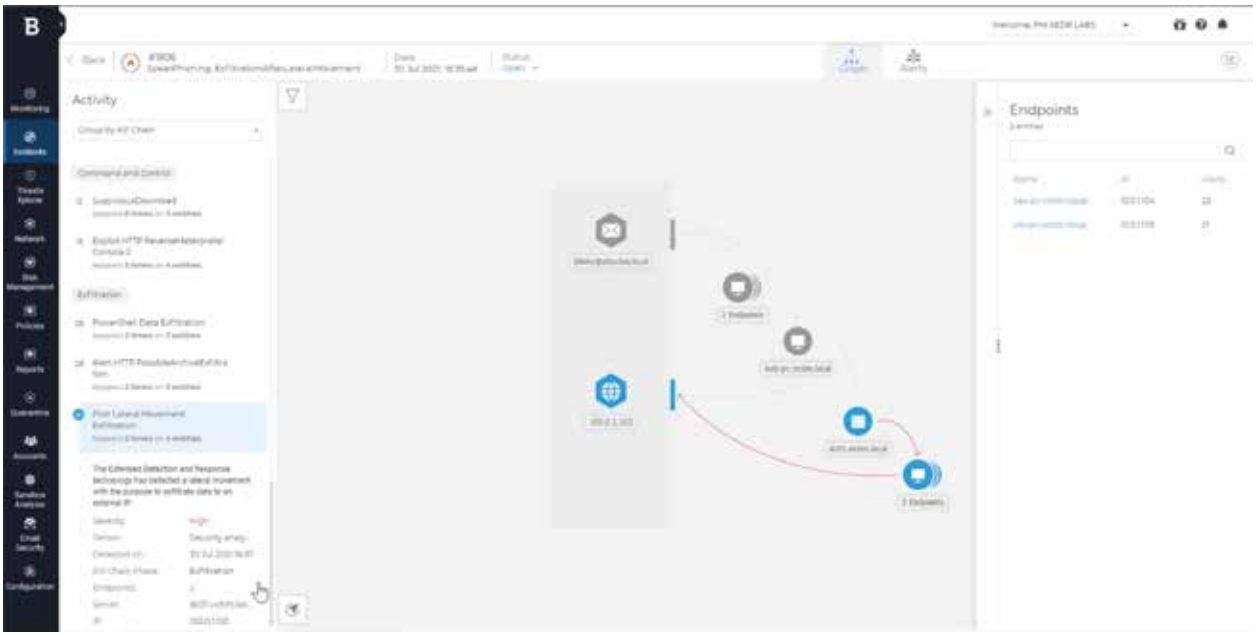
Bitdefender MDR Threat Hunting to wszechstronne rozwiązanie, umożliwiające ograniczenie ryzyka dla systemów biznesowych i minimalizację ekspozycji na zagrożenia. Ciągła proaktywna ocena ryzyka, z jakim mierzy się twoja firma, w połączeniu z rozległą wiedzą na temat działania sieci i systemów, umożliwia nam wykrywanie wszelkich anomalii. Bitdefender MDR stale monitoruje także dark web pod kątem informacji na temat klientów i marki, w tym danych do logowania, własności intelektualnej, holdingów i oddziałów, a także innych danych dotyczących klienta.

Część klientów przyjmuje bardziej praktyczne podejście i decyduje się na dodanie rozwiązania **Bitdefender Endpoint Detection and Response (EDR)** do swojego stosu bezpieczeństwa. Rozwiązaniu takiemu sprzyja możliwość zintegrowania narzędzia z prewencyjnymi mechanizmami kontrolnymi i uzyskania w wyniku tej działalności spójnego systemu od jednego dostawcy, z jednym pulpitem zarządzania. Bitdefender EDR został zaprojektowany w celu skrócenia czasu ekspozycji na zagrożenia ze strony cyberprzestępców, które mogą zostać przeoczone po zakończeniu pierwszego etapu ataku. Wymaga to od narzędzia EDR wyszukiwania i wykrywania oznak podejrzanych zachowań. Rozwiązanie wykorzystuje punkty końcowe jako czujniki, analizując procesy, pliki, klucze rejestru, skrypty i wiele innych źródeł danych. Informacje o zdarzeniach są gromadzone, a następne analizowane pod kątem podejrzanego zachowania i oceniane zgodnie ze skalą ryzyka. W przypadku dużego prawdopodobieństwa wystąpienia złośliwej motywacji, system zgłasza zdarzenie jako incydent bezpieczeństwa. Oprócz analizowania pojedynczych incydentów bezpieczeństwa, analitycy badają także związki pomiędzy nimi, a poszczególnymi alertami. Korelacja między punktami końcowymi pozwala na szybsze wykrywanie incydentów bezpieczeństwa i, w rezultacie, efektywniejsze przerywanie „łańcucha zabójstw", tym samym blokując rozwój wydarzeń.



Rozszerzony EDR zapewnia precyzyjne wykrywanie incydentów na wczesnym etapie ataku.

Rozwiązanie EDR rozróżnia alerty pod względem przypisanego priorytetu i traktuje je w odpowiedni sposób. Na przykład automatyczne zablokowanie złośliwego kodu, znajdującego się w wiadomości e-mail, jest traktowane jako pojedynczy incydent, który nie wymaga interwencji człowieka. Z drugiej strony wykrycie wewnętrznego ataku ZeroLogon z sieci na jeden z kontrolerów domen potraktowane zostanie jako incydent wymagający natychmiastowej reakcji. Podczas korelacji między punktami końcowymi ten incydent zostanie wykorzystany to stworzenia mapy całego „łańcucha zabójstw" wraz z detekcjami, uruchamiającymi alarm, które w innym przypadku mogłyby pozostać niezauważone. Na przykład zablokowany zostanie pozornie nieszkodliwy skrypt PowerShell, jeśli system powiąże go z przeszłymi działaniami cyberprzestrzępców (eksfiltracja PowerShell po wykryciu aktywności poziomej).

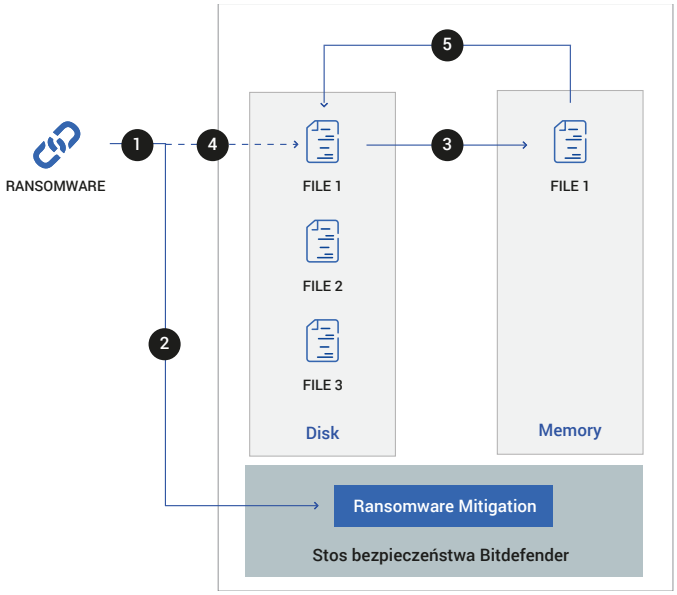


Przykład rozszerzonej wizualizacji incydentów. Automatycznie wykryto eksfiltrację danych PowerShell po zanotowaniu aktywności poziomej.

Ransomware Mitigation

Jednym z najważniejszych aspektów projektowania architektury pogłębionego bezpieczeństwa jest założenie, że cyberprzestępcy zawsze znajdą sposób, aby ominąć istniejące kontrole bezpieczeństwa. Haker może na przykład wykorzystać do uruchomienia ataku ransomware urządzenie pozostawione bez nadzoru.

Funkcja Ransomware Mitigation skupia się przede wszystkim na zmniejszeniu wpływu ataku ransomware na firmę. Zaszyfrowany plik ma znacznie wyższy poziom losowości (lub entropii), dlatego rozwiązanie Ransomware Mitigation monitoruje pod tym kątem pliki na dysku i w trakcie edycji. Polecenie zaszyfrowania pliku (jeśli poziom jego losowości osiągnie określony limit) powoduje utworzenie jego tymczasowej kopii zapasowej w pamięci, a oryginalny plik jest przywracany po dokonaniu zmian. Co ważniejsze, ta metoda nie bazuje na usłudze kopiowania woluminów w tle, czy innych statycznych rozwiązaniach do tworzenia kopii zapasowych, ponieważ te prawie zawsze padają ofiarą cyberprzestępców. Polecenie usunięcia kopii plików w tle jest jednym z sygnałów ostrzegających narzędzie EDR o niebezpieczeństwie. Takie podejście pozwala zapewnić ograniczenie ryzyka związanego z atakami ransomware również w przypadku niespotykanych wcześniej metod pracy cyberprzestępców.

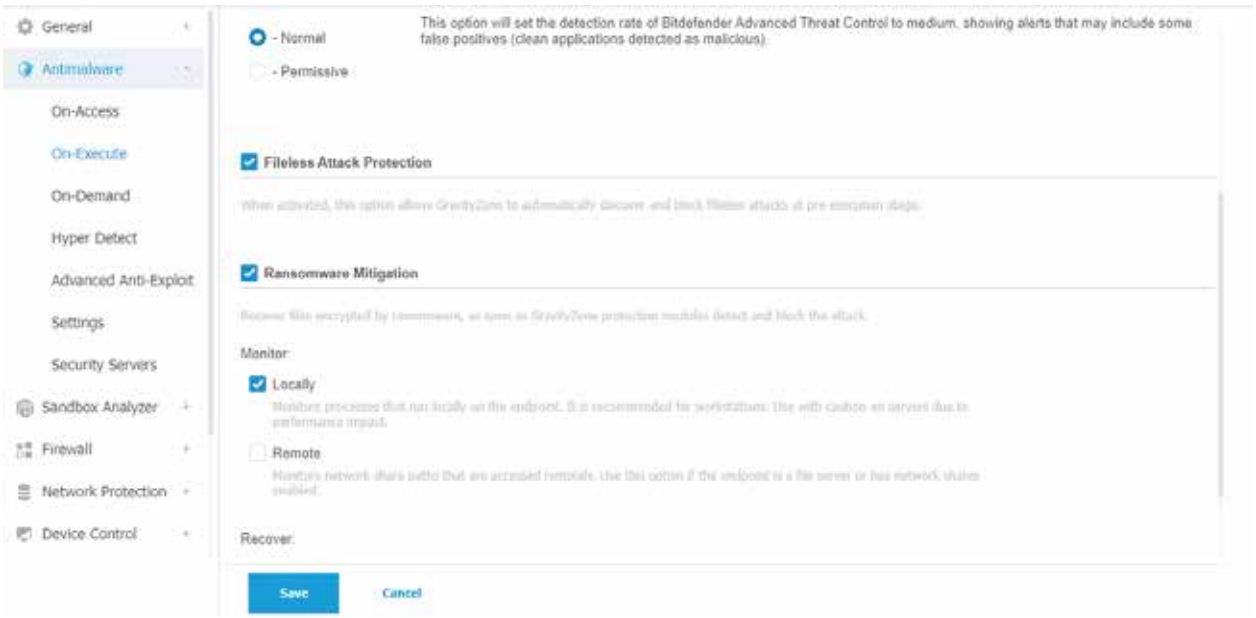


1. Ransomware próbuje zaszyfrować plik
2. Żądanie zostaje przechwycone, algorytm określa prawdopodobieństwo złośliwej zmiany
3. Jeśli prawdopodobieństwo jest wysoki tworzona jest kopia zapasowa pliku
4. Żądanie zostało wznowione, plik został zaszyfrowany
5. Oryginalny plik zostaje odzyskany z kopii zapasowej

Funkcja Ransomware Mitigation przywraca treść zaszyfrowanych plików przy pomocy kopii zapasowej zapisanej w pamięci.

Funkcja Ransomware Mitigation może być używana zarówno lokalnie, jak i zdalnie. W przypadku funkcji Local Ransomware Mitigation, administratorzy mogą skonfigurować politykę bezpieczeństwa Bitdefender w taki sposób, aby monitorować procesy na punktach końcowych i odzyskiwać zaszyfrowane pliki, gdy tylko wykryty i zablokowany zostanie atak. Jeśli złośliwemu oprogramowaniu uda się jednak zaszyfrować lokalne pliki, do akcji wkroczy narzędzie do ograniczania ryzyka związanego z atakiem ransomware, natychmiast przywracając zapisane w pamięci kopie automatycznie albo na żądanie użytkownika (w tym wariancie administrator może określić, kiedy zaszyfrowane pliki mają zostać przywrócone).

Z kolei w przypadku funkcji Remote Ransomware Mitigation administrator może włączyć funkcję monitorowania ścieżek sieciowych z ustanowionym dostępem zdalnym i zapobiec szyfrowaniu plików. Na zdalnym punkcie końcowym agent użytkownika potwierdza, że rozwiązanie Ransomware Mitigation wychwyciło podejrzane zachowanie podczas dostępu zdalnego i zabezpieczyło pliki. Administratorzy Bitdefender natychmiast otrzymują raport z kontroli i mogą szybko uzyskać więcej informacji na temat adresu IP, z którego został zapoczątkowany zdalny atak ransomware oraz modułu bezpieczeństwa, który chronił punkt końcowy. Mogą oni także otrzymywać powiadomienia e-mail z adresem IP hakera, gdy atak zostanie zablokowany.

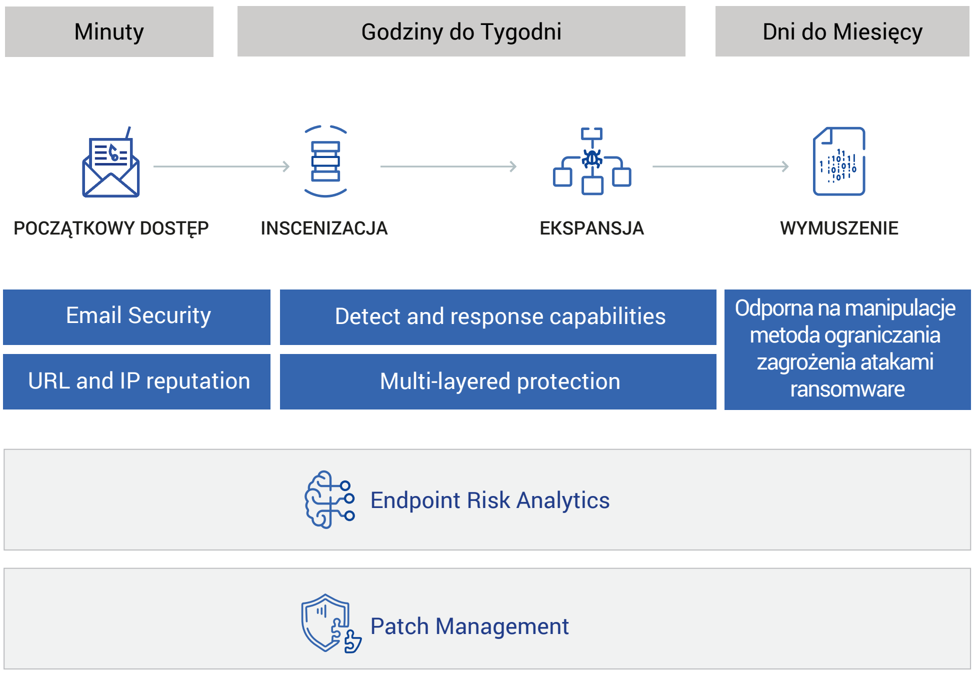


Funkcja Ransomware Mitigation jest w stanie ograniczyć zagrożenie atakiem na pliki przechowywane lokalnie i zdalnie.

Platforma GravityZone oferuje także raporty o aktywności ransomware, które pozwalają szybko zapoznać się ze stanem zainfekowanych urządzeń i przywrócić ich status. Po wykryciu aktywnego ataku możesz szybko dowiedzieć się, w jaki sposób wpłynął on na twoje punkty końcowe, oraz jakie kroki podjąć, aby zażegnać niebezpieczeństwo.

Wniosek

Podsumowując – cyberbezpieczeństwo to gra w kotka i myszkę, w której obie strony dbają o ciągłe wprowadzanie innowacji i ulepszanie stosowanych narzędzi oraz technik. Efektywna działalność zapobiegawcza bez wątpienia nadal odgrywa największą rolę w powstrzymywaniu cybeprzestępców, ale w przypadku nowoczesnych grup, działających w oparciu o model Ransomware-as-a-Service i podział zysków, a także współczesnych cyberprzestępców sponsorowanych przez państwo, nacisk kładziony jest przede wszystkim na innowacje w zakresie wykrywania zagrożeń i reagowania na nie. Incydenty bezpieczeństwa są nieuniknione. Tym, do czego nie wolno dopuścić są przypadki przełamania ochrony. Aby to osiągnąć, niezbędne są najwyższej jakości narzędzia, ustanowienie odpowiedniego zaplecza oraz opracowanie solidnej strategii pogłębionego bezpieczeństwa – to absolutny fundament cyfrowego spokoju. Aby uzyskać lepszą efektywność i odporność na cybernetyczne zagrożenia, możesz także skupić się na udoskonaleniu procedur bezpieczeństwa (wewnętrznie lub z pomocą usług zarządzanych).



Bitdefender
BUILT FOR RESILIENCE

Centrala
Siedziba przedsiębiorstwa – Santa Clara, Kalifornia, USA
Centrala technologiczna – Bukareszt, Rumunia

Przedstawiciel marki Bitdefender w Polsce
Marken Systemy Antywirusowe
Tel: 58 667 49 49
E-mail: kontakt@marken.com.pl
www.bitdefender.pl

Bitdefender-Whitepaper-AntiRansomewareSolution-creat6004-en_EN
CD-03/05/20 • MD-May 2, 2022 10:38 pm