Informacja o rozwiązaniu

Nowoczesna technologia cyber deception

Metallic® ThreatWise™ - nowe podejście do ochrony przed ransomware

Oprogramowanie ransomware jak i inne cyfrowe zagrożenia nieustannie ewoluują. Mamy do czynienia z coraz bardziej wyrafinowanymi technologiami i taktykami. Dzisiaj to już praktycznie nowa forma zorganizowanej przestępczości cyfrowej. Funkcjonuje ona jak firma, która stale się rozwija i dostosowuje do zmieniających warunków, doskonaląc zarówno taktykę jak i stosowane techniki. Jednocześnie bariera wejścia do tej gry dla nowych uczestników stale maleje. Jedna rzecz się jednak nie zmienia... ciągłe polowanie na nasze dane.

Dane są klejnotem koronnym współczesnych firm i głównym celem ataków. W miarę jak pojawiają się nowe, zaawansowane wektory zagrożeń, coraz większe znaczenie zaczynają odgrywać solidne narzędzia. Tylko dysponując odpowiednim rozwiązaniem można proaktywnie izolować organizację od zagrożeń. Wykorzystując wyspecjalizowaną technologię cyber deception do ochrony danych, każda firma, niezależnie czy duża, czy mała, może zapewnić sobie nowoczesną ochronę przed atakami i ransomwarem. Dzięki niej możliwe stanie się wcześniejsze wykrywanie i eliminowanie zagrożeń.

Rozwiązanie do odtwarzania danych to za mało

Konwencjonalne ataki ransomware polegały na szyfrowaniu danych. Głównym celem było zablokowanie dostępu do krytycznych danych systemowych i aplikacji. W efekcie nie można było ich używać, co poważnie zakłócało (a potencjalnie zatrzymywało) procesy biznesowe. W końcu zostały jednak opracowane skuteczne rozwiązania do ochrony danych, które pozwoliły firmom zabezpieczyć się przed pełną utratą danych w wyniku takiego ataku. Zamiast spełniać żądania dotyczące wygórowanych okupów w zamian za odzyskanie swoich danych, organizacje mogą tworzyć czyste kopie zapasowe, które pozwalają na odtworzenie danych. W ten sposób można samodzielnie przywrócić normalne funkcjonowanie firmy. Przestępcy dostrzegli to i zmienili swoje podejście.

Dzisiaj 83% ataków wiąże się z jakąś formą wycieku/wprowadzenia, kradzieży lub uszkodzenia danych. Innymi słowy, większość cyberzagrożeń ma na celu coś więcej niż tylko zablokowanie dostępu do firmowych danych. Od kradzieży tajemnic handlowych po sprzedaż poufnych danych w dark webie - najnowsze zagrożenia typu ransomware szkodzą firmom na wiele różnych sposobów. Rozwiązania, które oferują wyłącznie możliwość odtworzenia danych, już nie zapewniają ochrony.

Przy tym, jakby taktyka podwójnego czy potrójnego wymuszenia nie była dostatecznie przerażająca, znacznie wzrosła szybkość z jaką prowadzone są ataki. Eksperci szacują, że średni czas potrzebny przestępcom na przejście od momentu uzyskania dostępu do zainfekowania środowiska ofiary wynosi około godziny i 30 minut. Tak krótki czas oznacza, że potrzebne są nowe, szybsze sposoby wykrywania zagrożeń. Możliwość dokonania tego na wcześniejszym etapie cyklu ataku pozwala firmom szybciej reagować i chronić krytyczne dane biznesowe oraz zasoby - zanim jeszcze nastąpi faktyczne uderzenie.

> **83% ataków ransomware wiąże się z jakąś formą wycieku, wyprowadzenia, kradzieży lub uszkodzenia danych.[1]**

Nowoczesna technologia cyber deception

Kiedy przestępcy zmieniają sposób działania, swoje podejście muszą także zmienić organizacje. Trzeba od nowa zaprojektować swoją strategię ochrony danych. Kluczem do sukcesu jest skupienie się na proaktywnym reagowaniu na zagrożenia, zanim jeszcze atakujący zdobędą dane, a nie tylko na ich odzyskiwaniu.

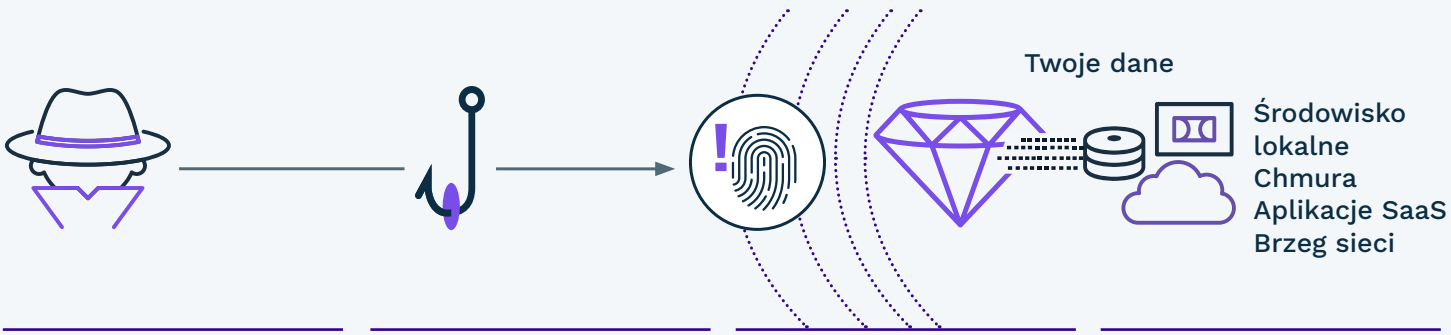
Sprawdzonym rozwiązaniem w obliczu nowych wyzwań jest technologia cyber deception czyli cyfrowej dywersji. Daje firmom ogromne możliwości aktywnej obrony i zapewnienia ochrony na wcześniejszych etapach.

Nowoczesne rozwiązania cyber deception to pułapki zastawione na przestępców. Prezentują się hakerom jako faktyczne zasoby biznesowe i skupiają całą siłę ataku na sobie, zamiast na środowiskach produkcyjnych. Takie "pułapki" sprawiają, że przestępcy wykradają fałszywe dane. To jednak nie wszystko. Technologia cyber deception to system wczesnego ostrzegania przed nieznanymi zagrożeniami. Pozwala szybko wykrywać obecność przestępców i umożliwia proaktywne eliminowanie zagrożeń. To technologia i podejście obecne w defensywnych frameworkach MITRE (MITRE D3FEND i MITRE Engage), których skuteczność jako środka ograniczającego cyber-ryzyko została potwierdzona.

Metallic® ThreatWise™

Wykorzystując opatentowaną technologię cyber deception, Metallic® ThreatWise™ zmienia reguły gry ochrony przed ransomwarem i innymi zagrożeniami. Zapewnia zarazem zaawansowane mechanizmy wczesnego ostrzegania i podejmowania działań zapobiegawczych oraz kompleksową ochronę danych. Umożliwia wszystkim firmom - małym i dużym - neutralizowanie "cichych" ataków, zanim spowodują szkody; wykrywanie i przekierowywanie najbardziej wyrafinowanych ataków typu Zero Day, które pozostają niewidoczne dla konwencjonalnej technologii wykrywania i omijają zabezpieczenia.

W przeciwieństwie do technologii tradycyjnych pułapek typu honeypot, ThreatWise™ jest lekki, szybki i prosty w obsłudze. To oznacza szybsze uruchamianie bardziej skutecznych wabików i pułapek przy znacznie niższych kosztach. To rozwiązanie specjalnie zaprojektowane do bezpośredniego skupiania na sobie zagrożeń — wykrywania działań rozpoznawczych, ruchu poprzecznego w sieci oraz nieautoryzowanego uprzywilejowanego dostępu, które pozostają poza zasięgiem konwencjonalnych systemów bezpieczeństwa. Dzięki natychmiastowym ostrzeżeniom o trwających atakach, organizacje mogą wykrywać najbardziej wyrafinowane zagrożenia w różnych środowiskach, zanim jeszcze dojdzie do wycieku danych, ich zaszyfrowania, eksfiltracji czy kradzieży. Całość składa się na wyjątkowe, wielowarstwowe rozwiązanie do ochrony zróżnicowanych firmowych środowisk IT.



1 Uruchamianie fałszywych zasobów i wabików, nie do odróżnienia od prawdziwych dla atakującego

2 Przekierowanie i wabienie przestępców, żeby skupili się na fałszywych zasobach

3 Wykrywanie zagrożeń bez fałszywych alarmów i nadmiernej ilości incydentów

4 Eliminowanie zagrożeń, zanim dotrą do krytycznych danych

- Płynna replikacja najbardziej wartościowych zasobów
- Angażowanie atakujących i wykrywanie aktywności w czasie rzeczywistym
- Natychmiastowe szczegółowe informacje o zagrożeniach na wczesnych etapach ataków
- Szybkie skalowanie zapewniające ochronę całej powierzchni ataku

Więcej informacji można znaleźć na stronie metallic.io

1. https://www.computerweekly.com/news/252513735/Backups-no-longer-effective-for-stopping-ransomware-attacks
2. https://www.sophos.com/en-us/press-office/press-releases/2022/06/attacker-dwell-time-increased-by-36-percent-sophos-active-adversary-playbook-2022-reveals