VECTRA
SECURITY THAT THINKS

E BOOK

Zatrzymać ransomware: wiadomości z linii frontu

AUTOMATYCZNE
ZARZĄDZANIE
ZAGROŻENIAMI

SKUTECZNOŚĆ OPERACJI

NATYWNE W CHMURZE

DLA PRZEDSIĘBIORSTW

Podsumowanie

Żadna organizacja nie chce otrzymać wiadomości, że w jej środowisku doszło do ataku ransomware. Jednak jeśli możliwa jest szybka identyfikacja odpowiednich sygnałów, szansa na powstrzymanie ataku jest większa. Jak to zrobić? O tym właśnie przeczytasz tutaj. Podamy przykłady prawdziwych sytuacji, w których nasi najważniejsi klienci pracują razem z zespołem Vectra Sidekick, aby zareagować na ataki ransomOps na wczesnym etapie i powstrzymać katastrofalne zakłócenia działalności przed wdrożeniem ransomware.

W niniejszym e-booku omawiamy wszystkie ważne kwestie, takie jak: dlaczego wykrywanie aktywności podmiotów atakujących i rekonesans zwany ransomOps ma kluczowe znaczenie dla zatrzymania ransomware oraz jakie kroki powinni podjąć specjaliści ds. bezpieczeństwa, aby skutecznie powstrzymać współczesne taktyki stosowane w ransomware. Przedstawiamy, w jaki sposób klienci korzystający z usług Vectra Sidekick są w stanie wykryć aktywne ataki niemal natychmiast oraz prezentujemy wybrane trudności, spostrzeżenia i zalecenia, o których powinna wiedzieć każda organizacja.

Jedna rzecz jest pewna: różnica pomiędzy sukcesem i porażką w powstrzymywaniu ransomware polega na szybkości reakcji i błyskawicznym działaniu. Powstrzymajmy ataki ransomware!

Usługa Vectra Sidekick MDR

Vectra Sidekick MDR to usługa całodobowego nieustannego monitorowania, która proaktywnie bada złośliwą działalność wykrytą przez Vectra Detect.

SideKick MDR zdecydowanie wzmacnia zespół ds. bezpieczeństwa, angażując doświadczonych analityków bezpieczeństwa, aby pomóc Ci w pełni wykorzystać sztuczną inteligencję Vectra, wcześnie dostrzec zagrożenia i powstrzymać naruszenia. Sidekick MDR nałożony na platformę Vectra to:

- Usprawnienie działalności Twojego zespołu ds. bezpieczeństwa dzięki zapewnieniu mu dostępu do doświadczonych analityków ds. bezpieczeństwa, którzy pomagają w usuwaniu wyrafinowanych przeciwników i podmiotów wykonujących atak ransomware.
- Wiedza specjalistyczna, kontekst i jasność w zakresie wczesnych charakterystycznych oznak ataku, zagrożenia lub ransomware, które Vectra Detect wykryło wraz z analitykami, aby aktywnie pomagać w szybkim reagowaniu.
- Całodobowe proaktywne monitorowanie, dzięki czemu możesz dowiedzieć się, kiedy priorytetowe wykrycie zagrożenia lub oprogramowania ransomware wymaga natychmiastowego działania i reakcji.
- Dostosowanie wdrożenia Vectra do Twojego unikalnego środowiska, celów biznesowych i zagrożeń branżowych. Obejmuje to dostosowywanie kontroli, przedstawianie zaleceń ekspertów, trendów i wskaźników środowiskowych oraz przyspieszanie dochodzeń.

Przede wszystkim ransomware to biznes

Mimo że to obrzydliwe, gangi ransomware i ich podmioty stowarzyszone prowadzą biznes i – tak jak w przypadku każdej innej działalności gospodarczej – ich celem jest zarabianie pieniędzy. Nastawiają się na zwrot z inwestycji i po prostu czerpią zyski na możliwości dotarcia do systemów i danych, które mogą bardzo szybko ukraść, jednocześnie obciążając użytkowników sporą sumą za zwrot ich własności.

Ten sposób myślenia jest podstawą wielu procesów omawianych w niniejszym e-booku, a zrozumienie powodów działań atakujących jest kluczowym elementem w każdej strategii bezpieczeństwa. Gdy wiesz, co kryje się za działaniami atakujących i potrafisz jasno zidentyfikować systemy i dane w środowisku, których naruszenie mogłoby spowodować zakłócenia, możliwe będzie maksymalne utrudnienie ataku na Twoją organizację.

Zobaczmy, dlaczego komputery stacjonarne mogą pomóc w zrozumieniu tego zagadnienia i w jaki sposób Red Team może obiektywnie ocenić aktualny stan gotowości organizacji.

Zacznijmy od podstaw

Oczywiście najlepszym rozwiązaniem jest powstrzymanie gangów ransomware przed uzyskaniem dostępu do Twojego środowiska. Chociaż zawsze warto zapobiegać zagrożeniom, nastawienie na zwrot z inwestycji może działać na Twoją korzyść. Właściwie możesz radykalnie zmniejszyć ryzyko, wprowadzając odpowiednie podstawy procesów uwierzytelniania i instalowania poprawek.

A to dlatego, że atakujący uzyskują początkowy dostęp do danych najczęściej za pośrednictwem niezałatanej i narażonej na DMZ luki w zabezpieczeniach, konta bez MFA lub podobnego, łatwo osiągalnego celu. Zasadniczo, jeśli organizacje pomijają niektóre z podstawowych metod zapobiegania niebezpieczeństwu, atakujący nie muszą stosować wyrafinowanych i czasochłonnych taktyk, aby uzyskać dostęp do danych.

> Najlepszym rozwiązaniem jest powstrzymanie gangów ransomware przed uzyskaniem dostępu do Twojego środowiska.

Dobrą wiadomością jest to, że włączając MFA (uwierzytelnianie wieloskładnikowe) w sieci VPN, IDP i innych punktach dostępu, utrudnisz życie atakującym, którzy być może porzucą swoje zamiary i wybiorą sobie inny cel. To samo dotyczy zarządzania poprawkami – zadbanie o to, aby prawidłowe postępowanie z poprawkami obejmowało obszar DMZ pomoże odwracać ataki. Mimo że żadna strategia zapobiegania nie jest niezawodna, odpowiednie inwestycje w zapobieganie utrudnią atakującym uzyskanie dostępu.

Gotowość do szybkiej reakcji – w dzień i w nocy

Zadbanie o podstawowe strategie poprawi sytuację, ale nie wyeliminuje ryzyka. Istnieje wiele powodów takiego stanu rzeczy. W rzeczywistości jednak wystarczy jeden błąd w konfiguracji konta, jedna pominięta łatka, jeden użytkownik klikający w link, którego nie powinien otwierać... lub jeden nowy atak typu zero-day w wybranym przez Ciebie VPN (sfinansowanym z ogromnych kwot pieniędzy wpływających do ekosystemu ransomware), aby złamać zabezpieczenia. Widzieliśmy wiele takich przypadków.

A kiedy ransomware dostanie się do Twojego środowiska, możesz spodziewać się, że będzie działał SZYBKO. Z łatwością reagujemy na ataki, które przebiegają powoli, przez kilka dni, jednak często zdarza się, że do ataków dochodzi w ciągu jednego wieczoru, po godzinach pracy. Pamiętaj, że czas to pieniądz dla atakujących nastawionych na zwrot z inwestycji. Niezależnie od tego, czy dajemy osobom broniącym przed atakami jak najmniej czasu na reakcję, czy też wierzymy w łut szczęścia, zazwyczaj dostrzegamy niewiele sygnałów, że napastnicy próbują pozostać w ukryciu. W rzeczywistości globalny czas przebywania ataków ransomware znacznie się skrócił w ciągu ostatnich kilku lat.

Dobrą wiadomością dla osób broniących się przed zagrożeniami jest to, że szybkie działanie za pomocą odpowiedniej technologii wykrywania pozwala ujawnić atak. W Vectra udało się nam dostrzec krytyczne hosty w ciągu dwóch minut od uzyskania początkowego dostępu. Szybkość przebiegu ataku sprawia, że trzeba być przygotowanym na błyskawiczną i zdecydowaną reakcję w celu powstrzymania zagrożenia zanim ransomware zostanie wdrożone.

Niestety ta możliwość szybkiego reagowania nie ogranicza się do godzin pracy. Zaobserwowaliśmy, że na wczesnym etapie rekonesans i ruchy boczne występują o każdej porze, najwyraźniej zawsze wtedy, gdy podmiot wykonujący atak ransomware miał trochę czasu. Czasami będzie to w środku dnia, innym razem w nocy, w weekend, a nawet podczas wakacji. Jednak z naszych obserwacji wynika, że ostateczny impuls do eksfiltracji i szyfrowania jest bardziej prawdopodobny w środku nocy, w weekend lub wakacje – czyli wtedy, gdy możliwości reagowania na incydenty są najsłabsze.

W praktyce oznacza to konieczność całodobowego monitorowania.

Przygotuj plan reakcji

Pierwszym krokiem reakcji na zagrożenie ransomware jest wykrycie przeciwnika w Twoim środowisku. Równie ważne jest, aby wiedzieć, co należy zrobić w różnych sytuacjach, aby powstrzymać atak. Jak daleko chcesz się posunąć? W jednym z naszych działań atakujący dotarł do administratora domeny na kontrolerze domeny, gdzie zaangażowany zespół ds. bezpieczeństwa musiał w ułamku sekundy podjąć decyzję o całkowitym odłączeniu swoich systemów od Internetu, aby zyskać czas na odpowiedź. Na szczęście taka strategia okazała się skuteczna.

Ten zespół był wprawdzie blisko przebiegającego ataku, ale ten scenariusz nie jest wcale taki rzadki. Warto zadać sobie pytanie: co Ty zrobisz, gdy Twoja organizacja znajdzie się w takiej samej sytuacji? Czy taki poziom zakłóceń byłby akceptowalny dla Twojej firmy? Czy będziesz w stanie skutecznie reagować bez łączności ze swoim zdalnym personelem ds. bezpieczeństwa? Czy są inne opcje reakcji, w które trzeba zainwestować?

Zauważyliśmy, że szybkie, zdecydowane działania pod presją są kluczowym składnikiem skutecznej reakcji. Znajomość i ćwiczenie planu działań, zanim konieczne będzie jego wykonanie, może mieć ogromne znaczenie.

Nie szukaj ransomware, aby go zatrzymać

Nowoczesne ataki ransomware (naprawdę są to ransomOps) wdrażają binarne oprogramowanie ransomware dopiero na samym końcu ataku. Oznacza to, że jeśli zauważysz samo ransomware, najprawdopodobniej będzie już za późno.

Jest to więc sprzeczne z powszechnie panującym błędnym przekonaniem. W rzeczywistości, aby zatrzymać te ataki, należy wykryć i zareagować na działania, które pojawiają się PRZED wdrożeniem ransomware. Prawie na pewno będziesz działać bez pełnej wiedzy o Twoim przeciwniku lub o jego celu. W wielu przypadkach zauważysz szybko postępujący atak i być może pewne charakterystyczne oznaki w narzędziach lub infrastrukturze C2, które pozwolą odgadnąć, co się dzieje.

Twój plan reakcji będzie musiał skoncentrować się na bardziej ogólnej kategorii wtargnięcia i postępu ataku, następnie na zrozumieniu, że ostateczny cel jest tylko prawdopodobnym, a nie pewnym celem.

Konta i narzędzia administracyjne są kluczowe

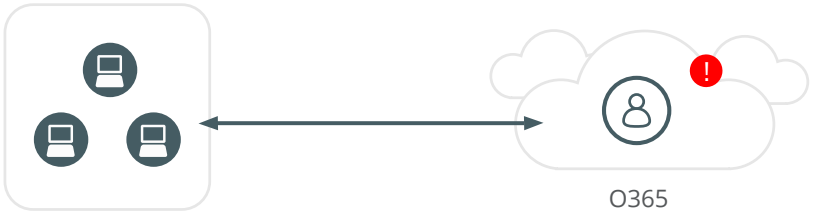
Zaobserwowaliśmy, że do uzyskania początkowego dostępu, a czasami do wykonywania ruchu bocznego, używa się exploitów. Jednak, podobnie jak w przypadku większości nowoczesnych ataków, nacisk kładziony jest na dane uwierzytelniające – konta administratora i usług. Wraz z protokołami administracyjnymi są to preferowane taktyki dla praktycznie wszystkich podmiotów stowarzyszonych ransomware.

Celem, podobnie jak w przypadku wielu ataków, jest dotarcie do administratora domeny na kontrolerze domeny, aby uruchomić ostatnią fazę ataku. Z tego punktu widzenia łatwo uzyskać dostęp do najcenniejszych danych. Możliwe jest również błyskawiczne wdrożenie ransomware za pomocą narzędzi administracyjnych, w tym GPO.

Ze względu na skupienie się na danych uwierzytelniających absolutnie istotne jest, aby uważnie monitorować użycie wszystkich uprzywilejowanych kont, ponieważ przekonaliśmy się, że jest to jeden z najcenniejszych sygnałów wykrywania ataków, który zapewnia niezawodność.

Wspólne motywy

Analitycy Vectra połączyli wyzwania związane z użytkownikami, procesami i bezpieczeństwem, które powtarzały się w różnych działaniach klientów.



Początkowy dostęp:

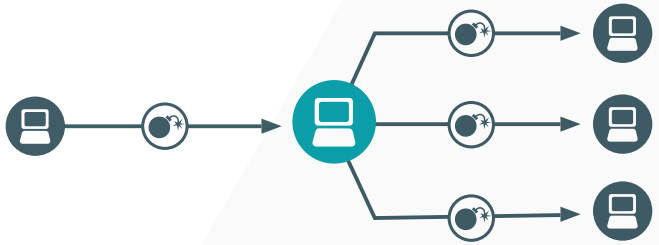
- Atakujący kontynuują skanowanie w poszukiwaniu luk w publicznie dostępnych usługach i systemach z dostępem do Internetu.
- Popularnymi celami są serwery obsługujące protokół RDP, FTP lub VPN, które zapewniają wstępny dostęp do przedsiębiorstw i chmury.
- Brak MFA to luka, w którą często wymierzane są ataki.
- Przebieg ataku w niektórych przypadkach trwał kilka godzin od momentu uzyskania pierwszego dostępu, a w innych było to kilka dni lub nawet tygodni. Zespoły ds. bezpieczeństwa mają czas na wczesne wykrycie i zareagowanie, ale wymaga to całodobowej czujności.

C2:

- Cobalt Strike jest obecnie ulubionym narzędziem.
- Popularne narzędzia zdalnego dostępu, niezależnie od tego, czy podlegały sankcjom, czy nie, były również wykorzystywane do sterowania systemami. W jednym przypadku wykryliśmy, że oprogramowanie Cisco AnyConnect zostało użyte do sterowania maszynami wewnątrz, przez człowieka znajdującego się na zewnątrz.

Rekonesans i ruch boczny

- W większości przypadków skanowanie było agresywne i obejmowało mapowanie sieci, zapytania rDNS i wyliczanie udostępniania. Szybkie skanowanie ogólnie sprawiało, że ataki były widoczne w ciągu kilku minut od uzyskania pierwszego dostępu.
- Rekonesans związany z danymi uwierzytelniającymi, w tym zapytania LDAP i wywołania RPC w celu mapowania lokalizacji danych uwierzytelniających również był powszechny.
- Ruchy boczne we wczesnych fazach obejmowały typowe exploity. Późniejsze etapy opierały się głównie na danych uwierzytelniających i protokołach administracyjnych.



Eksfiltracja

- Darmowe witryny do udostępniania plików były powszechnie używane do przesyłania informacji rozpoznawczych do analizy. Do witryn tych należą np. Mega Upload (mega.com) i temp.sh.

Zalecenia

Nasz zespół codziennie ściśle współpracuje z zespołami ds. bezpieczeństwa, reagując na krytyczne alerty generowane przez rozwiązania Vectra do wykrywania zagrożeń i reagowania na zagrożenia. Gdy na początku kontaktujemy się z klientami, nie jest oczywiste, czy zagrożeniem jest ransomware. Wraz ze wzrostem ważności alertów jesteśmy w stanie uzyskać dodatkową jasność i kontekst dotyczący ataku oraz określić, czy rzeczywiście jest to ransomware. Znaleźliśmy wiele różnych narzędzi i praktyk bezpieczeństwa, które utrudniają przeprowadzanie udanych kampanii ransomware i ostateczne ich powstrzymywanie. Należą do nich:

Zapobieganie

- Regularnie oceniaj swój stan bezpieczeństwa zewnętrznego i wdrażaj poprawki o wysokim priorytecie. Skoncentruj się w szczególności na infrastrukturze dostępu zdalnego i usługach powszechnie podatnych na ataki, takich jak RDP i FTP, które są zwykle popularnymi celami.
- W miarę możliwości włączaj usługę MFA u każdego dostawcy tożsamości lub infrastruktury dostępu zdalnego.
- Ogólnie rzecz biorąc, silne kontrole prewencyjne, zasady i polityki utrudniają eskalację uprawnień nawet po uzyskaniu dostępu, co daje więcej czasu na reakcję.
- Szczególnym obszarem zainteresowania są konta uprzywilejowane. Chociaż jest to trudne pod względem operacyjnym, im więcej można zrobić, aby skoncentrować się na korzystaniu z serwerów przesiadkowych i uprzywilejowanych systemów zarządzania kontami, tym trudniejsza będzie ścieżka eskalacji.

Wykrywanie

- Jest czas na zatrzymanie ataku po uzyskaniu dostępu do ransomware i przed wykradzeniem danych lub wdrożeniem ransomware.
- Zainwestuj w wykrywanie zagrożeń i reagowanie w całej sieci, infrastrukturze tożsamości, chmurze i punkcie końcowym, aby zmaksymalizować szanse na wczesne wykrycie.

Dochodzenie i reakcja

- Ataki ransomware mogą przebiegać szybko i odbywać się o każdej porze dnia i nocy. Ważne jest, aby zapewnić monitorowanie krytycznych alertów przez całą dobę, 7 dni w tygodniu, 365 dni w roku, przez wzmocnienie wewnętrznych zespołów lub skorzystanie z ofert zarządzanego wykrywania i reagowania (MDR) lub MSSP.
- Integracja telemetrii z dzienników sieci, punktów końcowych i chmury zapewnia najlepszy kontekst, przejrzystość i dokładne dane w badaniu zagrożeń i dotarciu do ostatecznej przyczyny źródłowej.
- Analiza zwiększonej aktywności skanowania w strefie DMZ, do której doszło przed pierwszym dostępem oraz OSINT mogą zapewnić wczesną ocenę potencjalnego podmiotu stanowiącego zagrożenie i zapewnić większą przejrzystość reakcji.

Więcej informacji można uzyskać, kontaktując się z nami pod adresem info@vectra.ai.

E-mail info@vectra.ai vectra.ai