**Tylko co trzecia firma odzyskuje dostęp do wszystkich danych. Co zrobić w obliczu ataku ransomware?**

****

**Podczas dokonywania 82 proc. umotywowanych finansowo cyberprzestępstw wykorzystywane jest oprogramowanie ransomware – wynika z raportu** [**Global Ransomware 2023**](https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2023-ransomware-global-research.pdf) **sporządzonego przez firmę Fortinet. Ataki z wykorzystaniem złośliwych narzędzi polegają na zaszyfrowaniu plików na urządzeniu, a następnie żądaniu okupu w zamian za ich odblokowanie. Tylko 35 proc. zaatakowanych w ten sposób przedsiębiorstw odzyskało dostęp do wszystkich danych. Eksperci Fortinet podpowiadają, jak postępować w obliczu ataku, aby zminimalizować wiążące się z nim straty.**

Dla 90 proc. firm uwzględnionych w raporcie Fortinet strategia przeciwdziałania atakom ransomware jest jednym z najważniejszych priorytetów dla ich zespołów ds. cyberbezpieczeństwa. Równocześnie jednak 50 proc. wszystkich respondentów przyznało, że ich firma padła ofiarą tego typu ataku w 2023 roku. 46 proc. ankietowanych firm zgłosiło zaś, że znalazło się na celowniku cyberprzestępców więcej niż raz.

**Objawy zainfekowania urządzenia**

Pierwszą reakcją potencjalnej ofiary ataku ransomware powinna być weryfikacja podejrzeń dotyczących jego wystąpienia. Najbardziej oczywistym objawem jest otrzymanie notki z żądaniem okupu, tzw. *ransom note*. Ta jednak nie zawsze musi się pojawić. Dlatego eksperci Fortinet sporządzili listę czynności pozwalających na ustalenie, czy urządzenie zostało zainfekowane.

1. **Próba otworzenia plików** – W przypadku aktywności oprogramowania ransomware na urządzeniu zazwyczaj okaże się to niemożliwe ze względu na zaszyfrowanie plików (zdarzały się jednak przypadki, że w wyniku ataku ransomware dane nie były szyfrowane, lecz tylko wykradane w celu wymuszenia okupu za zaniechanie ich upubliczniania).
2. **Przeskanowanie urządzenia za pomocą oprogramowania antywirusowego** – Jeżeli użyte w ataku złośliwe oprogramowanie jest powszechnie znane oraz nie potrafi omijać zainstalowanego rozwiązania antywirusowego, istnieje duża szansa, że zostanie wykryte.
3. **Weryfikacja nazw plików** –Jeżeli uległy one zmianie, może oznaczać to aktywność oprogramowania ransomware.
4. **Przegląd rozszerzeń plików** –Jeśli popularne rozszerzenia plików, takie jak *.docx* lub *.jpg,* zostały zastąpione dziwnymi kombinacjami liter, mogło zdarzyć się to na skutek działania złośliwego oprogramowania.
5. **Sprawdzenie aktywności sieciowej** –Większość wariantów złośliwego oprogramowania wymaga zewnętrznej ingerencji ze strony atakującego. Polega ona na zdalnym wydawaniu poleceń oraz odbiorze skradzionych danych. Komunikacja ta zachodzi za pośrednictwem tzw. serwerów zarządzających (Command and Control, C2), znajdujących się pod kontrolą cyberprzestępcy. Istnieją narzędzia umożliwiające wykrycieruchu sieciowego zawierającego przesyłane w ten sposób treści. Jego występowanie zazwyczaj wskazuje na obecność oprogramowania ransomware na urządzeniu.
6. **Weryfikacja aktywności procesora i dysku twardego** –Ransomware może powodować wzrost poziomu wykorzystania zasobów sprzętowych. W przypadku podejrzenia infekcji, warto więc sprawdzić, czy komputer używa procesora intensywniej niż zwykle. Można to zrobić poprzez zamknięcie zwykłych programów oraz zakończenie procesów odbywających się w tle. Jeżeli krok ten nie spowoduje zmniejszenia obciążenia procesora lub twardego dysku, może być to oznaką działania oprogramowania ransomware.

**Jak usunąć oprogramowanie ransomware z komputera i zneutralizować jego skutki?**

W pierwszej kolejności konieczne jest jak najszybsze odłączenie urządzenia od internetu. Należy także odłączyć od niego zewnętrzne dyski twarde i inne nośniki pamięci. Następnie pamięć komputera oraz twarde dyski powinny zostać przeskanowane za pomocą oprogramowania antywirusowego – jeśli nie jest ono zainstalowane, należy je pobrać z internetu na czysty pendrive na innym komputerze i zainstalować na podejrzanym urządzeniu. Po wykryciu zagrożeń, wszystkie pliki skategoryzowane jako niebezpieczne powinny zostać poddane kwarantannie lub usunięte. Krok ten można wykonać ręcznie lub zlecić go oprogramowaniu ochronnemu.

Specjaliści Fortinet zachęcają do korzystania z profesjonalnych narzędzi, ponieważ manualne usuwanie skutków ataku wymaga dużej wiedzy i doświadczenia. Następnie należy użyć rozwiązania deszyfrującego. W tym celu zaleca się skontaktowanie z ekspertem ds. bezpieczeństwa i sprawdzenie, czy jest on w posiadaniu odpowiedniego narzędzia (często są one udostępniane bezpłatnie). Przydatna może okazać się również strona NoMoreRansom.org. Znajduje się na niej szeroki asortyment rozwiązań umożliwiających odszyfrowanie danych. Jeżeli jednak nie będzie ona oferowała poszukiwanego rozwiązania, warto zgłosić sytuację do Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT NASK (csirt.gov.pl).

Jedną z najskuteczniejszych metod obrony przed skutkami zaszyfrowania plików przez ransomware jest odzyskanie danych z regularnie wykonywanych kopii zapasowych (backup) – te okazują się bezcenne także w innych przypadkach utraty dostępu do cyfrowych zasobów, np. na skutek awarii twardego dysku komputera. Kopie powinny być wykonywane na różne nośniki (zewnętrzny twardy dysk lub pendrive, serwer NAS, zasoby chmurowe), a za poprawne i systematyczne prowadzenie tego procesu odpowiada specjalne oprogramowanie, które zwalnia użytkownika z konieczności pamiętania o zabezpieczeniu plików. Koniecznie natomiast trzeba pamiętać, aby przynajmniej jedna kopia była wykonywana na nośnik odłączony od komputera podczas normalnej pracy. Twórcy narzędzi ransomware wiedzą, że backup jest ich największym wrogiem, więc starają się zaszyfrować także nośniki z kopiami (również w chmurze), jeśli te mają stałe połączenie z komputerem.

**Oszacowanie kosztów związanych ze skutkami ataku ransomware**

Skutki finansowe związane z atakiem ransomware mogą różnić się w zależności od wielkości przedsiębiorstwa, skali incydentu oraz kraju, w którym znajduje się firma. Składają się na nie koszty związane z robocizną (odtworzenie danych, kontrola antywirusowa całego środowiska itd.), przestojem działalności, konsultacjami prawnymi, ewentualnymi grzywnami, a także utratą reputacji marki.