**Gwardia Narodową stanu Indiana zaatakowano wirusem szantażującym.**

**Na oficjalnej stronie Gwardii Narodowej Stanu Indiana pojawił się komunikat o skutecznym ataku z wykorzystaniem wirusa szyfrującego dane w celu wyłudzenia okupu.**

Celem przestępców był należący do Gwardii cywilny serwer, na którym znajdowały się dane dotyczące personelu służb cywilnych oraz wojskowych. W raporcie podsumowującym przeprowadzone śledztwo stwierdzono, że nie był to atak ukierunkowany bezpośrednio na serwer Gwardii. Wg. śledczych, był to atak zautomatyzowany, który charakteryzuje się losowo obieranymi celami oraz bardzo dużym zasięgiem.

Atak można uznać za ukierunkowany, gdy spełnia trzy następujące warunki:

- Napastnicy kierują swoje działania przeciwko konkretnemu celowi, oraz angażują dużo czasu i zasobów, by go osiągnąć.

- Atak przeprowadzany jest w celu kradzieży konkretnych informacji.

- Atakujący podejmują znaczny wysiłek, by ukryć fakt złamania zabezpieczeń i zdobycia pożądanych informacji. Hakerom zależy na jak najdłuższym okresie pozostania niezauważonym, w celu dogłębnej infiltracji sieci.

W komunikacie prasowym rzecznika Gwardii Narodowej Stanu Indiana można przeczytać, że personel objęty potencjalnym wyciekiem jest na bieżąco informowany o incydencie. Osoby te powinny zwiększyć czujność i zwracać uwagę na podejrzane działania, np. na zakładanie fałszywych kont w ich imieniu.

W oświadczeniu nie podano, jakich narzędzi użyto do przeprowadzenia ataku. Jednak ostatnia seria ataków szantażujących wymierzonych w amerykańską infrastrukturę z wykorzystaniem nowej odmiany ransomware nazwanego Gamma (nazwa pochodzi od znaku „Gamma” umieszczanego w rozszerzeniu zaszyfrowanych plików) wskazuje na ten rodzaj szkodnika. Jest to nowy szczep wirusa, wywodzący się z rodziny zagrożeń typu Troldesh / Crysis.

Specjaliści z Bitdefender analizujący ransomware Gamma odkryli, że nowe zagrożenie wykorzystuje luki w protokole RDP (Remote Desktop Protocol) oraz technikę brut-force (najprostsza metoda łamania haseł polegająca na testowaniu wszystkich możliwych kombinacji) wykorzystywane do przemycenia złośliwego kodu na komputery końcowe, zazwyczaj zabezpieczone prostymi hasłami uwierzytelniającymi. Zwracają jednocześnie uwagę, że ransomware Troldesh / Crysis jest najczęściej wykorzystywany do przeprowadzenia ukierunkowanych ataków. Jeśli śledczy badający atak na serwery Gwardii stanu Indiana mają rację odnośnie zautomatyzowanej techniki ataku, to można przypuszczać, że w tym przypadku nie wykorzystano ransomware z rodziny Crysis.