**Przeglądanie stron z pornografią przyczyną zainfekowania złośliwym kodem infrastruktury IT rządu Stanów Zjednoczonych**

**Przeprowadzone w Earth Resources Observation and Science Center (EROS Center), amerykańskim centrum badawczym zajmującym się monitorowaniem zasobów Ziemi, śledztwo w sprawie podejrzanego ruchu sieciowego ujawniło rażące zaniedbania pracowników w obszarze zarządzania bezpieczeństwem.**

W raporcie ze śledztwa ujawniono, że pracownicy EROS wykorzystywali infrastrukturę rządu Stanów Zjednoczonych do przeglądania ok 9000 stron z erotyką i pornografią.

Problem wypłynął, gdy w należącej do EROS sieci wewnętrznej wykryto szybko rozprzestrzeniającego się wirusa. Śledztwo wykazało, że niektóre z odwiedzanych przez pracowników stron pornograficznych przekierowywały ruch na rosyjskie serwery ze złośliwym kodem. Lekkomyślny pracownik, przy okazji pobierania zdjęć pornograficznych na prywatny telefon oraz pendrive, pobrał złośliwy kod. Następnie podłączył te urządzenia do komputera w centrum EROS.

W raporcie ze śledztwa wskazano na dwa rażące błędy, które doprowadziły do naruszenia bezpieczeństwa. Pierwszy, to nieograniczony dostęp do stron internetowych za pośrednictwem należącej do centrum EROS infrastruktury IT. Drugim błędem był brak blokady portów USB na komputerach pracowników. W celu zapobiegnięcia podobnym incydentom w przyszłości, amerykański Departament Spraw Wewnętrznych nakazał blokadę dostępu, za pośrednictwem rządowej infrastruktury, do stron z pornografią oraz wprowadzenie zakazu korzystania z pamięci przenośnych. Przeprowadzono również szkolenie pracowników z obowiązujących procedur bezpieczeństwa.

Matthew T. Elliott , asystent Generalnego Inspektora prowadzącego śledztwo w sprawie naruszenia zaleca, w celu uniknięcia podobnych incydentów w przyszłości, stosowanie czarnych list podejrzanych adresów internetowych oraz stały monitoring historii odwiedzanych przez pracowników stron www.

„Zaraz po incydencie agencja EROS wdrożyła zaawansowany system detekcji zagrożeń oraz zaporę sieciową, które mają chronić infrastrukturę przed atakami hakerskimi już w najwcześniejszej fazie ich wystąpienia” – potwierdził Elliott.

„Przedsiębiorstwa powinny stosować zaawansowane środki ostrożności. Błędy pracowników powodują, że firmy są narażone na zainfekowanie infrastruktury IT. Blokowanie portów USB oraz ograniczony dostęp do stron internetowych, szczególnie tych podejrzanych, może uchronić firmę przed ogromnymi stratami” komentuje Dariusz Woźniak, inżynier techniczny Bitdefender z firmy Marken.