aut. Szymon Palczewski 18.11.2019

IRAŃSCY HAKERZY NIE ŚPIĄ. WOJSKOWE SZPITALE NOWYM CELEM

Irańska grupa państwowych hakerów wykorzystała botnety do infekowania systemów i sieci szpitali i uniwersytetów, znajdujących się na Bliskim Wschodzie, w Stanach Zjednoczonych oraz Azji. Na liście były również instytucje o kluczowym znaczeniu dla bezpieczeństwa USA. Incydent został odkryty przez specjalistów Trend Micro – informuje serwis CyberScoop.

Irańscy hakerzy należący do grupy APT33 wykorzystali botnety do przeprowadzenia ukierunkowanych cyberataków, wymierzonych w podmioty działające na terenie Bilskiego Wschodu, w Stanach Zjednoczonych oraz Azji. Hakerzy infekowali docelowe urządzenia oraz sieci złośliwym oprogramowaniem.

Według specjalistów cyberprzestępcy używali kilkunastu komputerów do prowadzenia złośliwych operacji. Za pomocą specjalnie opracowanego wirusa uzyskiwali trwały dostęp do konkretnych urządzeń, a następnie wewnętrznych sieci danej firmy lub organizacji. Dodatkowo hakerzy utworzyli własną sieć prywatną, w ramach której koordynowali swoje działania. Eksperci wpadli na jej ślad rok temu – wskazuje CyberScoop.

„Celem APT33 były firmy zajmujące się poszukiwaniem złóż ropy naftowej na Bliskim Wschodzie oraz tamtejsze szpitale wojskowe – wyjaśniają specjaliści Trend Micro. Dodają, że podczas kampanii cyberprzestępcy podszywali się pod jednego z uznanych europejskich polityków, aby wzbudzić zaufanie u ofiar.

Jak przypomniana CyberScoop, APT33 jest jedną z lepiej wyposażonych grup hakerskich, które działają na zlecenie Teheranu. Jej cyberprzestępcy zyskali popularność za sprawą cyberataków wymierzonych w Arabię Saudyjską oraz szereg amerykańskich firm, które znalazły się na liście „Fortune 500”.

Czytaj też: Wiązka lasera narzędziem hakerów? Produkty popularnych marek w niebezpieczeństwie