**Kaspersky Lab analizuje nową kampanię cyberszpiegowską wymierzoną w firmy produkujące gry online**

**Zespół ekspertów z Kaspersky Lab dokonał szczegółowej analizy aktywnej kampanii cyberszpiegowskiej prowadzonej przez cyberprzestępców z organizacji znanej jako „Winnti”. Według raportu Kaspersky Lab grupa Winnti od 2009 r. atakuje firmy zajmujące się produkcją gier online. Działania grupy obejmują kradzież cyfrowych certyfikatów podpisanych przez legalnych producentów oprogramowania oraz kradzież własności intelektualnej, w tym kodu źródłowego projektów gier internetowych.**

Pierwszy incydent, który skierował uwagę na szkodliwe działania grupy Winnti, miał miejsce jesienią 2011 r., kiedy to na dużej liczbie komputerów użytkowników końcowych na całym świecie został wykryty złośliwy trojan. Wyraźnym związkiem pomiędzy wszystkimi zainfekowanymi komputerami było to, że były one używane do grania w popularną grę online. Wkrótce po tym incydencie okazało się, że złośliwy program infekujący komputery użytkowników był częścią aktualizacji oprogramowania i pochodził z oficjalnego serwera firmy produkującej grę. Użytkownicy, których komputery zostały zainfekowane, i członkowie społeczności graczy podejrzewali, że wydawca gier komputerowych celowo wymusił zainstalowanie złośliwego oprogramowania, aby szpiegować swoich klientów. Jednak później okazało się, że szkodliwy program został zainstalowany na komputerach graczy przez przypadek, a rzeczywistym celem cyberprzestępców była właśnie firma produkująca gry komputerowe.

W odpowiedzi na incydent wydawca gier komputerowych, który był właścicielem serwerów rozprzestrzeniających trojana, zwrócił się do Kaspersky Lab z prośbą o analizę szkodliwego programu. Trojan okazał się być biblioteką DLL, przygotowaną dla 64-bitowego środowiska Windows i używającą prawidłowo podpisanego złośliwego certyfikatu. Szkodnik był w pełni funkcjonalnym narzędziem zdalnej administracji (RAT - Remote Administration Tool), które dawało napastnikowi możliwość kontrolowania komputera użytkownika bez jego wiedzy. Odkrycie było szczególnie ważne, ponieważ analizowany trojan był pierwszym szkodliwym programem na 64-bitową wersję systemu Microsoft Windows, który posiadał ważny podpis cyfrowy.

Specjaliści z Kaspersky Lab rozpoczęli analizę kampanii prowadzonej przez grupę Winnti. Na drodze dochodzenia okazało się, że ofiarami infekcji było ponad 30 firm z branży gier komputerowych. Większość z nich to firmy programistyczne produkujące gry wideo w Azji Południowo-Wschodniej, ale także producenci gier online z Niemiec, Stanów Zjednoczonych, Japonii, Chin, Rosji, Brazylii, Peru i Białorusi.

Fragment kodu trojana Winnti

Oprócz procederu szpiegostwa przemysłowego eksperci z Kaspersky Lab zidentyfikowali trzy główne systemy zarabiania pieniędzy, które mogą być wykorzystywane przez grupę Winnti do generowania nielegalnego przychodu:

Manipulowanie gromadzeniem waluty wewnątrz gier („runy”, „złoto” itp.), która jest wykorzystywana przez graczy do zamiany dóbr wirtualnych na prawdziwe pieniądze.

Używanie kodu źródłowego skradzionego z serwerów gier internetowych do wyszukiwania luk w zabezpieczeniach wewnątrz gier w celu zwiększenia przychodów wirtualnej waluty i jej akumulacji bez wywoływania żadnych podejrzeń.

Używanie kodu źródłowego skradzionego z serwerów popularnych gier online do wdrażania własnych pirackich serwerów.

Obecnie grupa Winnti pozostaje nadal aktywna, a śledztwo Kaspersky Lab jest w toku. Zespół ekspertów z firmy ściśle współpracuje ze społecznością zaangażowaną w bezpieczeństwo IT, przemysłem gier online i instytutami certyfikacji w celu identyfikacji kolejnych zainfekowanych serwerów i udzielania pomocy przy odwoływaniu skradzionych certyfikatów.

Więcej informacji dotyczących kampanii prowadzonej przez grupę Winnti, wraz ze szczegółową analizą techniczną, pojawi się już wkrótce w Encyklopedii Wirusów VirusList.pl prowadzonej przez Kaspersky Lab.

Produkty Kaspersky Lab wykrywają i neutralizują szkodliwe oprogramowanie wykorzystywane przez grupę Winnti. Szkodniki klasyfikowane są jako: Backdoor.Win32.Winnti, Backdoor.Win64.Winnti, Rootkit.Win32.Winnti oraz Rootkit.Win64.Winnti.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.