**Groundhog wykorzystuje dziury w Twoim serwerze Linux**

**W czerwcu 2015, zespół reagowania na incydenty bezpieczeństwa firmy Check Point został poinformowany przez klienta o niecodziennej aktywności na jednym z jego serwerów DNS BIND działającym pod kontrolą systemu operacyjnego Linux. Dziwne zachowanie polegało na zapisywaniu dużej ilości podejrzanych plików w katalogach systemowych.**

Szczegółowa analiza zainfekowanego systemu dokonana przez zespoły reagowania na incydenty bezpieczeństwa oraz badania złośliwego oprogramowania firmy Check Point szybko wykazała, że na wspomnianym serwerze rzeczywiście doszło do włamania. Atak został przeprowadzony metodą brute force poprzez SSH wcześniej tego samego miesiąca. Adresy IP atakujących pochodziły z zakresów należących głównie do chińskich dostawców internetowych. Wykorzystując sieć komputerów do ataku, włamywaczom zajęło jedynie kilka dni, aby uzyskać dostęp roota i przejąć pełną kontrolę nad serwerem.

Po przejęciu kontroli nad serwerem, atakujący zainfekowali system dwoma złośliwymi programami. Były to XOR.DDoS oraz Groundhog, które zostały specjalnie zaprojektowane, aby zarażać systemy Linux i zmuszać je do uczestniczenia w wielkich atakach typu DDoS (Distributed Denial of Service). Skuteczność tego złośliwego oprogramowania pokazuje duży krok naprzód w możliwościach wykorzystania ataków DDoS w celach przestępczych. Efektywność kodu w połączeniu z faktem, że programy te infekują jedynie serwery Linux z dostępem do wysokoprzepustowych łączy, mogą spowodować, że będziemy świadkami ataków DDoS na niespotykaną dotąd skalę.

Podczas gdy XOR.DDoS był już przedtem znany i przeanalizowany, program Groundhog to nowo odkryte zagrożenie. Dochodzenie Check Pointa wykazało bardzo duże podobieństwo tych dwóch aplikacji: używają one podobnej konfiguracji, metod ochrony oraz sposobu komunikacji. Po głębszej analizie próbek można stwierdzić, że istnieje duże prawdopodobieństwo, że są to różne moduły tej samej rodziny złośliwego oprogramowania i że zostały one zaprojektowane i napisane przez tego samego autora.

Dane badawcze pokazały, że atakujący niedawno zmienili sieci używane do ataków, najprawdopodobniej wskutek wykrycia i działań prewencyjnych przeprowadzonych w ostatnim czasie. [Ten raport](http://blog.checkpoint.com/wp-content/uploads/2015/10/sb-report-threat-intelligence-groundhog.pdf) podsumowuje badania Check Pointa i dostarcza szczegółowych danych na temat całego ataku, włączając zaobserwowane metody zarażeń, techniki wykorzystywane przez złośliwe oprogramowanie oraz analizę plików wykonywalnych.

Klienci korzystający z systemu IPS blade firmy Check Point mogą ochronić się przed początkowym atakiem SSH typu brute force wykonywanym przez ten botnet poprzez włączenie i odpowiednią konfigurację zabezpieczenia IPS „Wielokrotne żądania inicjujące połączenie SSH”.

Oprogramowanie antywirusowe i antybotowe firmy Check Point oferuje różne sygnatury, aby ochronić klientów przed infekcjami wykonywanymi przez ten botnet. Sygnatury te są znane pod następującymi nazwami:

Backdoor.Linux.Xorddos.\*

Operator.Xorddos.\*