باسمه تعالی

هشدار درخصوص افزایش حملات به پورت ۷۵۴۷

در روزهای اخیر شاهد افزایش میزان حملات در سطح کشور بر روی پورت ۷۵۴۷ بوده‌ایم. فعالیت‌های این پورت که یکی از پورت‌های اصلی مورد هجوم بدافزار میرای است، می‌تواند تا حدودی وضعیت این بدافزار و میزان فعال بودن بات‌نت‌های مرتبط با آن را مشخص کند. با بررسی‌های انجام شده بر روی این پورت مشخص شد که در بازه زمانی ۱۳۹۷/۰۹/۰۱ تا ۱۳۹۷/۰۹/۳۰ نرخ حملات به شدت افزایشی بوده و متاسفانه اکثر حملات صورت گرفته از آدرس‌های مبدا ایران هستند، بگونه ای که در حملات رخ داده در این بازه زمانی حدود ۶۸ درصد حملات از آدرس‌های کشور ایران و تنها ۳۲ درصد حملات از سایر نقاط جهان ایجاد شده است. این نشان می‌دهد هنوز بسیاری از تجهیزات و سیستم‌های داخل کشور پاک‌سازی و بروزرسانی نشده و در حال انتقال آلودگی هستند. این در حالی است که در گزارش‌های پیشین نیز به اهمیت بروزرسانی تجهیزات و مقابله با بات‌های آلوده در کشور تاکید شده بود.
در ضمن قابل تاکید است که بیشترین حملات خارجی از کشور رومانی به این پورت صورت‌گرفته است و در بررسی جداگانه‌ای که درباره کشور رومانی صورت گرفت، مشخص شد که برخی زیرشبکه‌های این کشور آلوده به بات‌نت‌هایی هستند که پورت‌های ۲۳ و ۷۵۴۷ را در داخل کشور مورد هدف قرار می‌دهند.

بنابراین با توجه به تهدیدات داخلی و خارجی در این مورد، لازم است سازمان‌های ذی‌ربط در اسرع وقت نسبت به هشدار به مالکان تجهیزات آلوده اقدام نمایند تا میزان بات‌نت‌های فعال بر روی این پورت در کشور کاهش یابد. بیشتر تجهیزات آلوده که به این پورت حمله می‌کنند در دسته مودم‌ها و روترهای خانگی قرار دارند که با بروزرسانی Firmware در مقابل حملات بات‌نت‌ها و تبدیل شدن به بات ایمن می‌شوند.
در صفحات بعد جداول و اطلاعات آماری مربوط به حملات بر روی این پورت قابل مشاهده است.

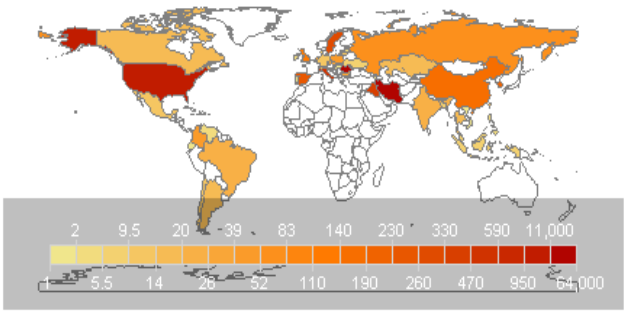
خلاصه اطلاعات حمله

اطلاعات	جهان	ایران
تعداد حملات	۹۲۹۶۱	۶۳۴۳۵
تعداد آدرس های مهاجم	۵۵۳۱	۴۹۹۴
تعداد بدافزارها	۱۱۰	۰
تعداد کشور مهاجم	۶۰	۱
درصد آلودگی	۳۱.۷۶	۶۸.۲۴

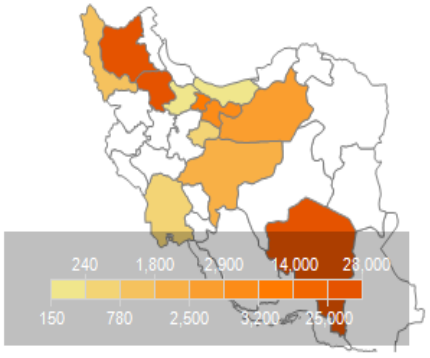
افزایش حملات به پورت ۷۵۴۷

وضعیت حملات جهان از ۱۳۹۷/۰۹/۰۱ تا ۱۳۹۷/۰۹/۳۰

مبدا حملات



مقصد حملات



روند حملات

بدافزارهای پرتکرار در آذرماه

بدافزار	تعداد
fa۵۰f۹۱۹a۸b۸ac۴۴۷da۹۲۶۶۱۷f۱۵۹۲cf	۱۵
c۴e۲e۱۷ef۴۸۱۵۸fae۰۵۴۷۹۵۰۰۳۸۲۳۴۰۵	۷
۳۲۰۹۷bad۵c۱۸۴a۹f۱beba۸۳۵۹۴۱۸۳۱۲۱	۶
۳e۰۶d۵۹da۲۳۰۰۰۹۹c۲۲۶e۵۸۰fe۸b۶۳b۷	۶
۴۹f۰fb۵e۹۰۰۸۰bcf۳f۸c۶aa۲cf۰ab۸۹a	۵
b۹۰c۲۲afc۸dffc۱c۸a۶f۸f۶۵۳۳a۶b۷۲۷	۵
cf۹۶۹۶ec۶۵۵۵aa۸a۳e۰۷cbeccbb۲۳a۹۷	۴
۷۲۰a۳۹b۷۸d۸۱۳۰d۰۵۹۰۶۱۴d۱bc۷۰bd۳d	۴
۸۰۹۴۵۰۷۹fa۸۸۸۵۶۰۱۴f۵a۶۷cff۳fd۰fe	۴
۹۰ee۴۷c۱dd۴a۰e۳b۸۰c۹f۹b۹۳e۶۴d۱۴۹	۴

آدرس‌های مهاجم پرتکرار در آذرماه

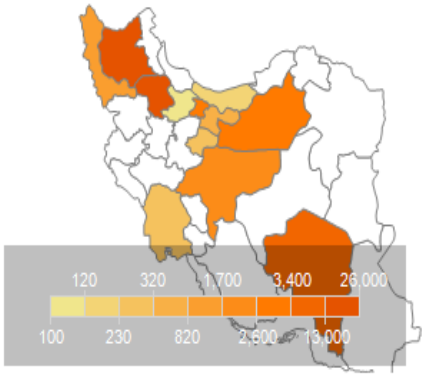
آدرس	کشور	تعداد
۸۹.۴۶.۲۳۲.۱۰۳	رومانی	۱۰۲۷
۸۹.۴۶.۲۳۲.۲۳	رومانی	۱۰۲۶
۸۹.۴۶.۲۳۸.۱۴۶	رومانی	۱۰۲۴
۸۹.۴۶.۲۳۷.۲۴۵	رومانی	۱۰۱۵
۸۹.۴۶.۲۳۸.۱۵۱	رومانی	۱۰۱۲
۸۹.۴۶.۲۳۷.۲۴۸	رومانی	۱۰۰۸
۸۹.۴۶.۲۳۸.۲۲۶	رومانی	۱۰۰۰
۸۹.۴۶.۲۳۸.۱۱۵	رومانی	۹۸۶
۸۹.۴۶.۲۳۹.۵۰	رومانی	۹۷۰
۸۹.۴۶.۲۳۵.۱۹۸	رومانی	۹۶۰

افزایش حملات به پورت ۷۵۴۷

وضعیت حملات ایران از ۱۳۹۷/۰۹/۰۱ تا ۱۳۹۷/۰۹/۳۰

مبدا حملات

مقصد حملات از ایران



روند حملات از ایران

آدرس‌های مهاجم پرتکرار از ایران

آدرس	کشور	تعداد
۲.۱۸۶.۱۱۶.۳۳	ایران	۵۳۶
۷۸.۳۸.۳۰.۱۱۸	ایران	۳۸۷
۷۸.۳۸.۳۱.۲۲۰	ایران	۳۷۶
۷۸.۳۸.۳۰.۸۹	ایران	۳۶۱
۷۸.۳۸.۳۱.۴۶	ایران	۳۴۹
۱۸۵.۸۳.۱۹۹.۲۳۸	ایران	۳۴۶
۷۸.۳۸.۳۰.۱۲۵	ایران	۳۱۴
۱۸۵.۸۳.۱۹۸.۹۰	ایران	۲۹۲

پراکندگی زیرشبکه های هدف حمله در کشور