هشدار در خصوص افزایش حملات به ابزار phpMyAdmin بر روی سرویس‌دهنده‌های وب

طی هفته گذشته افزایش حملات شدیدی روی پورت‌های ۸۰، ۸۰۰۰ و ۸۴۴۳ در سطح شبکه کشور مشاهده شده است. این حملات بر بستر پروتکل http و از نوع SQL Injection بر روی صفحه لاگین phpMyAdmin صورت پذیرفته است. براساس بررسی های صورت گرفته توسط سنسورهای مرکز ماهر طی این مدت بیش از ۶۰۰ هزار حمله ثبت شده است. از میان مهاجمین آدرس اینترنتی ۴۶,۲۴۶,۳۶,۴ بیشترین تعداد حملات شامل ۱۲۱۱۲۵ حمله را انجام داده است. این حملات از آدرس‌های IP کشور سوئد صورت گرفته است.

بمنظور پیشگیری از موفقیت در این گونه از حملات، لازم است دسترسی به ابزار phpMyAdmin و ابزارهای مدیریتی مشابه تا حد امکان محدود گردد.

جزییات حمله

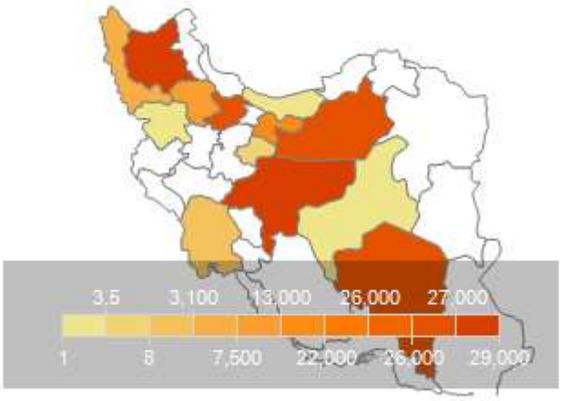
تحلیل حملات ثبت شده نشان می‌دهد که مهاجمین با استفاده از حمله SQL Injection به دنبال اجرای تابع Sleep() روی پایگاه‌داده متصل به سایت و همچنین صفحه phpMyAdmin بوده‌اند. تابع Sleep() در پایگاه‌های‌داده MySql مورد استفاده قرار می‌گیرد. اجرای این تابع در یک کوئری موجب می‌شود تا نخ اجرا کننده آن به خواب رفته و مسدود شود. تعداد زیاد نخ‌های مسدود شده روی یک پایگاه‌داده موجب از کار افتادن آن و عدم امکان ارائه سرویس به کاربران مجاز می‌شود. مهاجمین به طور میانگین روی هر مقصد تعداد بسیاری از حملات را روی سه پورت ۸۰، ۸۰۰۰ و ۸۴۴۳ از طریق فیلد ورودی تعبیه شده در صفحات وب و با دو درخواست متنوع Get و Post ارسال کرده‌اند. می‌توان بیان کرد هدف از حمله از کار انداختن سرویس (DoS) پایگاه‌داده از MySql بوده است.

حملات از نوع تزریق SQL Injection دارای تنوع بالایی بوده و امکان اجرای دستورات SQL، توابع سمت سرور و غیره را برای مهاجمین فراهم می‌کند. به منظور پیشگیری از وقوع چنین حملاتی لازم است تا تولیدکنندگان و توسعه‌دهندگان وب‌سایت‌ها ورودی‌های کاربر را اعتبارسنجی نمایند.

وضعیت حملات | پورت ۸۰ | ۱۳۹۷/۰۶/۱۵ تا ۱۳۹۷/۰۶/۲۳

مبدا حملات

مقصد حملات



روند حملات جهان

بدافزارهای برتر

بدافزار	تعداد

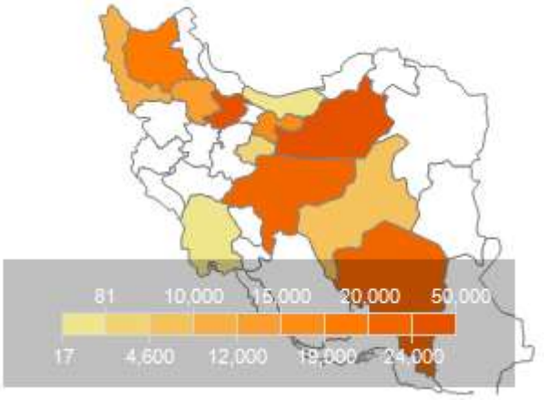
آدرس‌های برتر مهاجم

آدرس	کشور	تعداد
46.246.36.4	سوئد	40190
46.246.37.13	سوئد	29804
46.246.45.15	سوئد	29513
46.246.45.94	سوئد	27025
46.246.45.44	سوئد	22197
46.246.38.134	سوئد	11321
46.246.40.111	سوئد	9427
46.246.43.55	سوئد	19
46.246.62.169	سوئد	15
46.246.43.56	سوئد	14

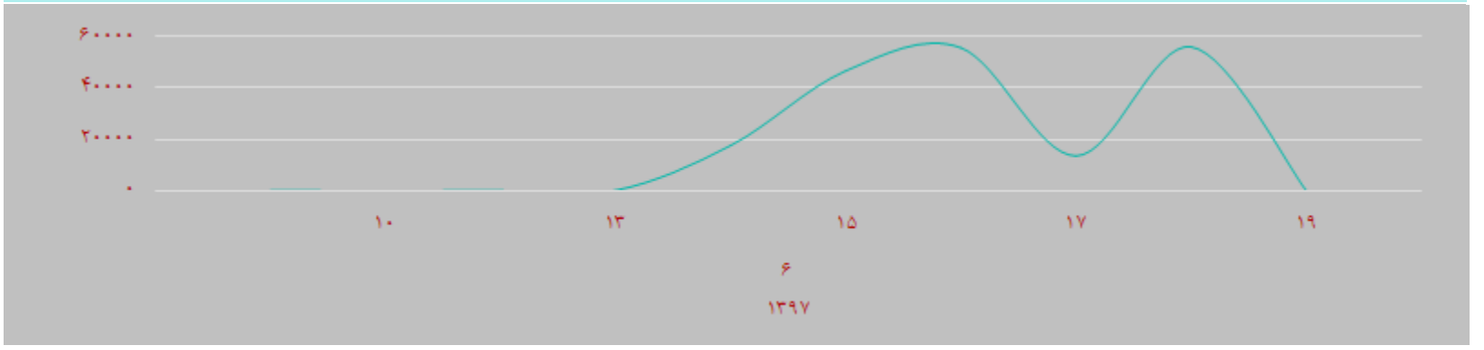
وضعیت حملات | پورت ۸۰۰۰ | ۱۳۹۷/۰۶/۱۵ تا ۱۳۹۷/۰۶/۲۳

مبدا حملات

مقصد حملات



روند حملات جهان



بدافزارهای برتر

بدافزار	تعداد

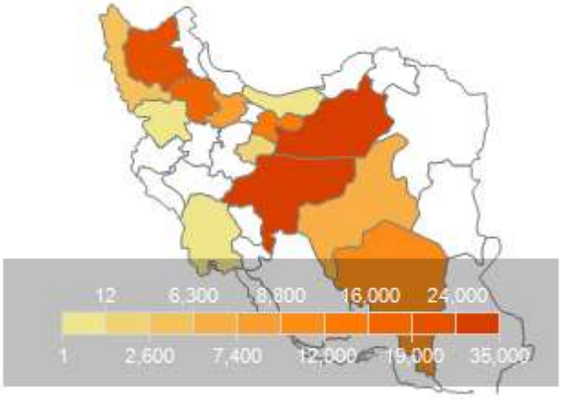
آدرس‌های برتر مهاجم

آدرس	کشور	تعداد
46.246.45.94	سوئد	42052
46.246.38.134	سوئد	34336
46.246.45.44	سوئد	29530
46.246.36.4	سوئد	28527
46.246.37.13	سوئد	27063
46.246.45.15	سوئد	17782
46.246.40.111	سوئد	10160
46.246.43.56	سوئد	19
46.246.43.55	سوئد	18
46.246.62.169	سوئد	12

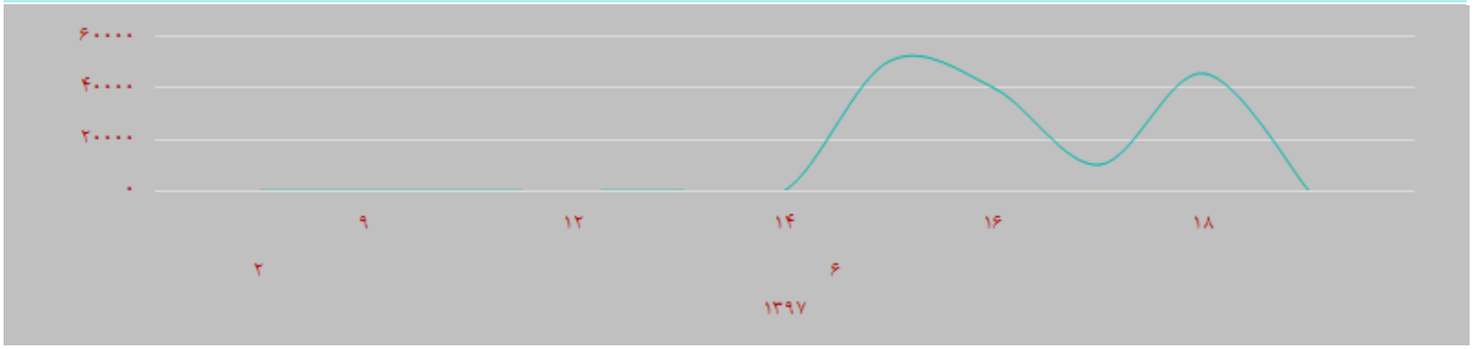
وضعیت حملات | پورت۸۴۴۳ | ۱۳۹۷/۰۶/۱۵ تا ۱۳۹۷/۰۶/۲۳

مبدا حملات

مقصد حملات



روند حملات جهان



بدافزارهای برتر

بدافزار	تعداد

آدرس‌های برتر مهاجم

آدرس	کشور	تعداد
46.246.36.4	سوئد	52408
46.246.37.13	سوئد	29714
46.246.38.134	سوئد	25845
46.246.45.94	سوئد	13835
46.246.45.15	سوئد	11866
46.246.40.111	سوئد	9067
46.246.45.44	سوئد	3902
46.246.43.55	سوئد	18
46.246.43.56	سوئد	18
46.246.40.143	سوئد	17