禪

CryptoPHP [illegible]

[illegible]

[illegible] CryptoPHP [illegible] (Backdoor) [illegible] 23 [illegible]. [illegible] CryptoPHP [illegible] (Backdoor) [illegible] 23 [illegible]. [illegible] Fox-IT [illegible] CryptoPHP [illegible] CryptoPHP [illegible]

این پلاگینها و پوستهها جاسازی شده است .

سرورهای آلوده به CryptoPHP همانند یک باتنت عمل میکنند و از طریق یک کانال ارتباطی رمزنگاری شده فرامین و دستورات را از سرور اصلی دریافت و اجرا میکنند . این بدافزار که در کشور هلند شناسایی شده است، با کمک مرکز بینالمللی امنیت سایبر این کشور و چند شرکت تحقیقاتی و امنیتی دیگر مانند Spamhaus، Shadowserver، Abuse.ch و مؤسسه Fox-IT مهار شده و سرورهای آنها تحت کنترل درآمدند . همچنین، ارتباط سرورهای آلوده در سراسر جهان با سرورهای اصلی قطع شده است تا امکان برقراری ارتباط مجدد و اجرای دستورات جدید وجود نداشته باشد .

محققان مؤسسه امنیتی Fox-IT میگویند : «در مجموع، 23693 آدرس IP یکتا متصل به سرورهای آلوده هکرها شناسایی شده است.» این محققان اعتقاد دارند تعداد سرورهای آلوده به بدافزار CryptoPHP بیشتر از این تعداد است؛ زیرا برخی آدرسهای IP یکتا میان چند سرور به اشتراک گذاشته شده است . طبق گزارش اعلام شده، پنج کشوری که بیشترین آلودگی را دارند، به ترتیب امریکا (8657 آدرس IP)، آلمان (2877 آدرس IP)، فرانسه (1231 آدرس IP)، هلند (1008 آدرس IP) و ترکیه (749 آدرس IP یکتا) معرفی شدند. همچنین، در گزارش مؤسسه Fox-IT آمده است هکرها هنگامی که سرورها بار ترافیکی پایینی دارند، حملات خود را ترتیب میدهند که امکان نصب پلاگینها و پوستهها وجود داشته باشد و بتوانند امکانات جدید را راهاندازی کنند .

به علاوه، تلاشهایی ردگیری شده است که این هکرها در تلاشاند نسخه جدیدی از این بدافزار را بسازند و توزیع کنند تا از تشخیص و شناسایی و قطع ارتباط سرورهای آلوده با سرور مرکزی در امان باشند . این محققان دو اسکریپت پایتون در برنامه GitHub منتشر کردند تا مدیران و وبمسترهای سایتها با استفاده از آنها بتوانند سرورهای میزبانی سایت خود را اسکن و بدافزار CryptoPHP را شناسایی کنند . بهعلاوه، آنها دستورالعمل پاکسازی سیستم و حذف این بدافزار را در وبلاگ خود منتشر کردند، اما توصیه کردند بهتر است سیستم مدیریت محتوایی که آلوده شده است دوباره نصب شود تا امنیت کامل بهدست آید و کمترین خطری متوجه سرور نباشد.

دسته بندی:
امنیت
تاریخ انتشار :
14:44 - 24/10/1393
برچسب:
بدافزار - CryptoPHP - بدافزار درپشتی - سرور آلوده - بات نت - backdoor - درپشتی

□□□□□ منبع: https://www.shabakeh-mag.com/security/136