禪

بانک اطلاعاتی محبوب توسعهدهندگان و بدافزارنویسان

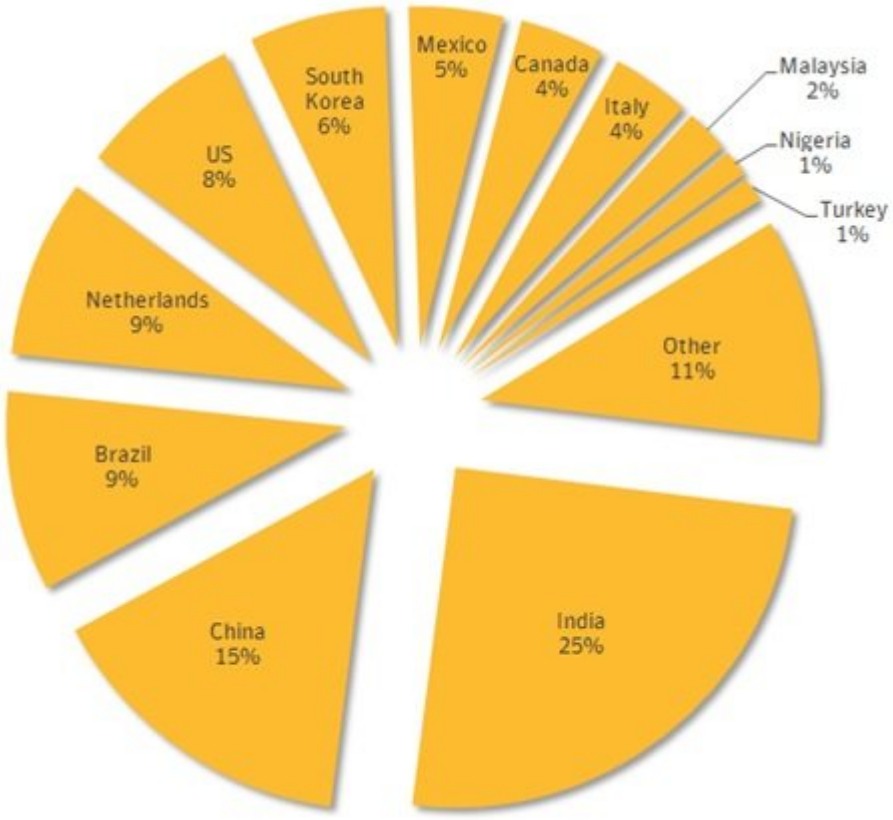
سرورهای MySQL قربانی حمله DDoS شدند

سیمانتک به تازگی بدافزاری را شناسایی کرده است که هدفش سرورهای MySQL بوده و با استفاده از آنها توانایی پیادهسازی حملات DDoS روی سایت های مختلف را دارد.

سیمانتک خبر از شناسایی یک کمپین هکری داده است که در آن هکرها با استفاده از بدافزار ویژهای سرورهای MySQL را ربایش میکنند. هکرها در نظر دارند با استفاده از یک باتنت ویژه گونه خاصی از حملات DDos را سازماندهی کرده و سایتهای مختلفی را تحت تأثیر این حمله قرار دهند.

مطلب پیشنهادی: سال رؤیایی هکرها (بزرگترین هکهای انجام شده در ۲۰۱۵)

آنگونه که جاوین اوگورمن از مؤسسه سیمانتک اعلام کرده است، هکرها ممکن است با تزریق کدهای SQL از طریق یک فایل UDF (سرنام user defined function) سرورهای MySQL را آلوده ساخته و در ادامه تروجان Downloader.Chikdos را به درون سرورها تزریق کنند. به دلیل این که فایلهای UDF به یک سرور MySQL اجازه مقداردهی اولیه فرآیندهای پیچیده روی سرور را میدهند، در نتیجه دسترسی به دستورات مرسوم SQL نیازی نیست، در نتیجه هکرها اقدام به فراخوانی فایلهای UDF و سپس بارگذاری یک تروجان خطرناکتر به نام Torjan.Chikdos.A میکنند. این تروجان گونهای از Trojan.Chikdos□□□□□□□□□□ بوده که بهطور ویژه در حملات DDos مورد استفاده قرار میگیرد. دادههای تلهمتری سیمانتک نشان دادهاند که این اکسپلویت بهطور جدی سرورهای MySQL مستقر در کشورهای هند، چین، هلند، برزیل و ایالات متحده را آلوده ساخته است. کمترین میزان آلودگی به کشورهای ترکیه، نیجریه و مالزی اختصاص دارد. تصویر زیر مقیاس آلودگی Downloader.Chikdos و Trojan.Chikdos را بر اساس مناطق آلوده شده نشان میدهد.



Mexico
5%
Canada
4%
Italy
4%
Malaysia
2%
Nigeria
1%
Turkey
1%
South
Korea
6%
US
8%
Netherlands
9%
Other
11%
Brazil
9%
China
15%
India
25%

تابع تعریف شده آلوده چگونه کار میکند؟

هکرها با استفاده از تابع تعریفی کاربر UDF (سرنام) (User Define Function Downloader.Chikdos را به درون سرورها تزریق میکنند . UDF تابع دستساز کاربر متشکل از کدهای کامپایل شدهای است که از درون MySQL فراخوانی شده و برای انجام عملیاتی فراتر از مدیریت سیستم بانکاطلاعاتی مورد استفاده قرار میگیرد . UDF به عنوان یک فایل سیستمی روی یک سرور به حیاتش ادامه میدهد.

به کارگیری UDF▯▯▯ مخرب برای دسترسی به سرورهای MySQL تکنیک جدیدی به شمار نمیرود . متیو زیرمن در سال 2005 میلادی گزارش جامع و کاملی در ارتباط با شیوه بهرهبرداری هکرها از UDF منتشر کرد . در این تکنیک، یک هکر یک فایل UDF را ایجاد میکند . این فایل با هدف پیادهسازی یکسری فعالیتهای مخرب ایجاد میشود . فرآیندهای مخرب میتوانند در ارتباط با ساخت یک remote shell یا دانلود یک بدافزار باشد . هکر در ادامه فایل UDF را از طریق حمله تزریق کد SQL درون سرور MySQL نصب میکند. اگر یک هکر توانایی اجرای دستورات SQL را داشته باشد از پارامتر DUMP برای آپلود مؤثر فایل UDF مخرب به درون سیستم استفاده میکند . در ادامه UDF اجرا شده و کدهای مخرب هکر را اجرا میکند .

تکنیک حمله **CHikdos**

Chikdos اولین بار در دسامبر سال 2013 میلادی توسط CERT-DL مستندسازی شد. این تهدید در آن روزگار هر دو پلتفرم لینوکس و ویندوز را نشانه رفته بود . در آخرین نسخه شناسایی شده از Chikdos ، هکرها از یک اسکنر خودکار یا احتمالا از طریق یک کرم به کشف سرورهای MYSQL و نصب UDF اقدام کردند . با این حال هیچگاه میزان دقیق آلودگی کشف نشد . زمانیکه سرورها آلوده میشوند، UDF یک ابزار DDos را دانلود میکند . این ابزار گونهای از تروجان Trojan.Chikdos.A است.

Dowloader.Chikdos

گونههای مختلف Downloader.Chikdos اغلب با نامهای تصادفی و با فرمت فایلی .dll ظاهر میشوند. فایلهای آلوده عمدتا در زیرپوشه نصب MySQL قرار میگیرند . وب مسترهایی که تمایل دارند بدانند آیا به این بدافزار آلوده شدهاند یا خیر باید نام فایلهای تصادفی Dll که در پوشههای زیر قرار دارند را مورد بررسی قرار دهند .

\Lib

Lib\Plugin

Bin\

[illegible] MySQL [illegible] Terminal Services [illegible] Terminal Services [illegible] Terminal Services [illegible]:

•HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\netcache\“Enabled” = “0”

•HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer\“EnableAdminTSRemote” = “1”

•HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermDD\“Start” = “2”

•HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService\“Start” = “2”

•HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\“TSEnabled” = “1”

•HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\“fDenyTSConnections” = “0”

[illegible]URL [illegible]

[illegible] MySQL [illegible]

[illegible] MySQL [illegible] MySQL [illegible] MySQL [

نویسنده :
حمیدرضا_تائبی

دسته بندی:
امنیت
تاریخ انتشار :
11:37 - 10/08/1394
برچسب:
DDoS - MySQL - امنیت - تزریق کد - User Define Function - SQL

▯▯▯▯▯ منبع: https://www.shabakeh-mag.com/security/2066