- بررسی سامانه سئو semalt.com :
  - ✓ از سال 2014 شروع به کار کرده.
  - ✓ به طور اولیه شرکت در کشور هلند تشکیل شد ولی هاستینگ سامانه در روسیه انجام می شده.
  - ✓ از متد های مختلف اقدام به تشکیل بات نت می کرده.
  - ✓ به طور کلی هرچند خیلی از فعالیت ها از جمله استفاده از سیستم کاربر برای تشکیل بات نت ناخواسته بوده ولی هیچ اقدام مخرب از هیچ نوعی از این سامانه مشاهده نشده.
  - ✓ با جستجو در وب وبرسی گزارش های موجود نتیجه می گیریم فعالیت های مورد دار این سامانه در سال های ابتدایی از شروع به کار سامانه بوده و در سال های اخیر هیچ رفتار مورد داری مشاهده نشده.
- نحوه فعالیت بات نت:

نام دامنه کاربران به بهونه ارایه سرویس سئو یا خدمات متناسب دیگر جمع آوری می شود. این دامنه را "دامنه هدف" می نامیم. هر چند هدف ارتقا رتبه "دامنه هدف" است ولی خیلی وقت ها این سرویس ناخواسته ارایه می شود و کاربر حتی اگه بخواد نمی تواند پروسه رو متوقف کند. و نهایتا همانطور که در ادامه ذکر می کنم نحوه عملکرد این سرویس می تواند تاثیر معکوس داشته باشه رتبه "دامنه هدف" را پایین بیاورد.

بعد از تشکیل لیستی از "دامنه های هدف" در ادامه از طریق متد های مختلف به طور موقت یا دائم از سیستم هزاران نفر به طور ناخواسته برای تشکیل یک بات نت وسیع استفاده می شود. وبسایت های زیادی برای پیدا کردن آسیب پذیری کنترل دسترسی فایل log در سطح اینترنت توسط بات نت کاوش می شوند.

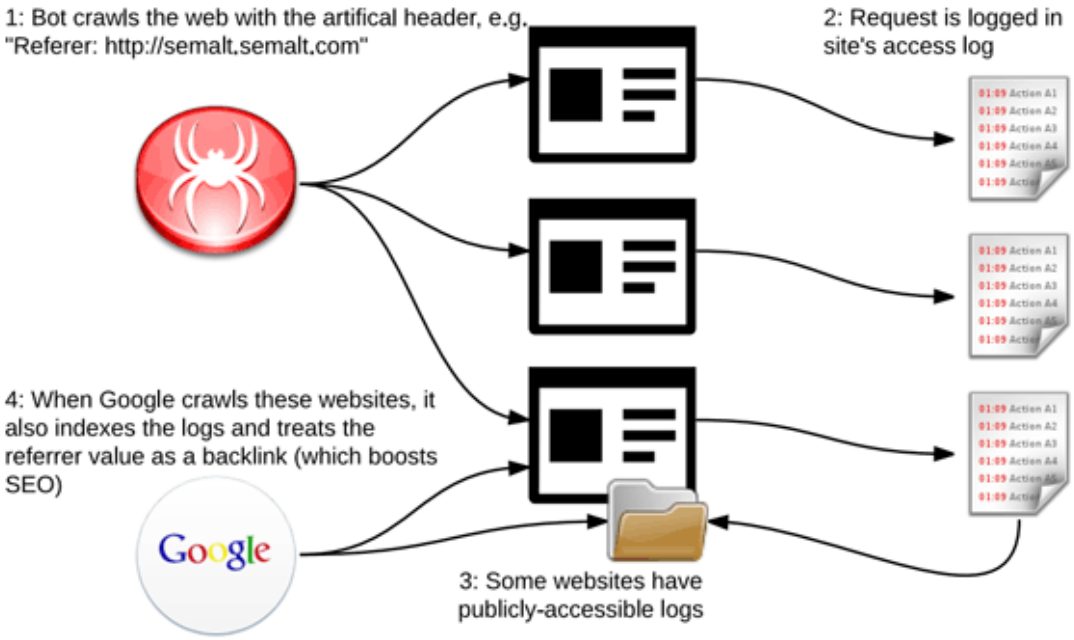
بعضی وب سرور ها فایل log که حاوی همه ارتباطات http سرور با کاربران است را در معرض دسترسی public قرار می دهند. (یعنی این فایل هم از اینترنت قابل دسترسی است و هم در فایل robots.txt ذکر نشده.) در نتیجه این فایل توسط موتور های جستجو پردازش می شود.

وقتی این آسیب پذیری در یک وبسایت مشاهده بشه، از بات نت تشکیل شده برای ارسال http request به این وبسایت استفاده می شود و آدرس "دامنه هدف" در فیلد referrer در http header قرار داده می شود.

حالا وقتی گوگل و موتور های جستجو فایل log این وبسایت رو پردازش کنند،

مشاهده می کنند کاربران زیادی از طریق "دامنه هدف" به این وب سایت ارجاع داده شده اند. موتور های جستجو به اشتباه در نظر می گیرن همه این کاربران از "دامنه هدف" بازدید می کرده اند در حالی که نود های موجود در بات نت هیچ اطلاعی از "دامنه هدف" ندارند و آمار بازدید واقعی این دامنه ممکنه خیلی کم باشه.

این تکنیک شاید رتبه "دامنه هدف" رو در رتبه بندی موتور های جستجو بالا ببره، اما با تاثیر منفی روی پارامتر "Bounce Rate" وب سایت دارای آسیب پذیری، رتبه این وبسایت را پایین می آورند.



www.imperva.com

- پارامتر Bounce Rate و تاثیر آن در رتبه وبسایت

موتور های جستجو و سیستم های رتبه بندی وبسایت از یه ملاک به اسم "Bounce Rate" استفاده می کنند.

Bounce Rating نشان گر میزان زمانی است که کاربر در سایت سپری می کنه و در در بازه صفر تا صد درصد تعریف میشه که هر چی بالا باشه، بد تره به این معنی که کاربران بلافاصله بعد از ویزیت، وبسایت رو ترک می کنند.

(واژه bounce به معنی برگشت و پرش پس از رسیدن یا برخورد به یه سطح است، مثلا توپ وقتی به زمین برخورد میکنه دوباره برمیگرده و نمیمونه و اگه آمار bounce کاربران یک وبسایت 100% باشه به این معنی که کاربران هیچ وقتی در وبسایت نمی گذرانند و بلافاصله بعد بازکردن، وبسایت رو ترک می کنند.)

به طور متوسط آمار بین 40 تا 60 درصد مقداد خوبی است. پارامتر Bounce Rating از طریق اسکریپت های موتور های جستجو که کاربران در وبسایت خود قرار می دهند سنجیده می شود مثل google analytics.

از اونجایی که بات نت مورد استفاده توسط semalt صرفا درخواست های http به طور خودکار میفرسته و برخلاف رفتار یک کاربر واقعی هیچ زمانی صرف باز کردن وبسایت سواستفاده شده در مرورگر (و درواقع اجرای اسکریپت google analytics یا غیره) نمی کنه. این مقدار bounce rating رو خیلی بالا میبره و باعث کاهش شدید رتبه وبسایت هدف قرار گرفته می شود.

منابع

https://www.imperva.com/blog/semalt-botnet-spam

https://www.kdm.com.au/what-is-semalt-doing-on-your-website