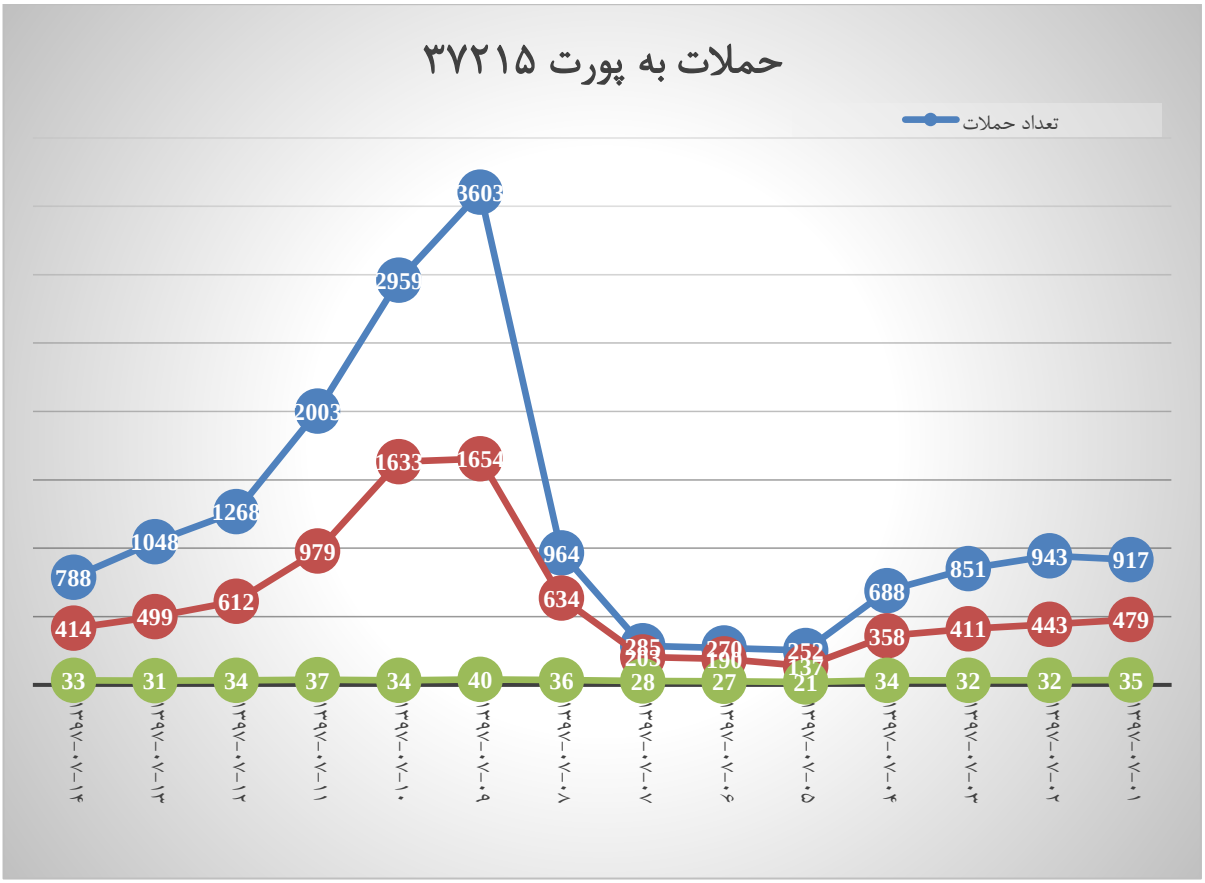
باسمه تعالی

# هشدار مرکز ماهر درخصوص افزایش حملات به پورت ۳۷۲۱۵ روترهای Huawei

مهرماه ۹۷

# ۱ گزارش حمله

در روزهای ۱۳۹۷/۰۷/۰۹ و ۱۳۹۷/۰۷/۱۰ طی رصد صورت گرفته، افزایش حملات بر روی پورت ۳۷۲۱۵ مرتبط با روترهای شرکت Huawei مشاهده شده است. جدول زیر اطلاعات حملات ثبت شده در روزهای مختلف مهر ماه را نمایش می‌دهد. همانطور که در این جدول و نمودارهای صفحات بعدی مشخص می‌شود، در دو روزهای نهم و دهم مهر افزایش حملات با افزایش تعداد آدرس‌های یکتا و کشورهای مهاجم همراه بوده است.




یکی از مهم ترین کاربردهای این شماره پورت در برنامه کاربردی مرتبط با روتر Huawei است. برای مثال در سال ۲۰۱۵ آسیب‌پذیری CVE-2015-7254 کشف شد که به مهاجم راه دور اجازه مرور در دایرکتوری‌های سیستم را می‌دهد. مهاجم با سواستفاده از این آسیب‌پذیری می‌تواند با ارسال یک درخواست URL شامل دنباله (/../) بر روی پورت ۳۷۲۱۵ اقدام به مشاهده فایل‌های سیستم کند. به عبارتی درخواست خاصی در این روترها می‌تواند به گونه ای دستکاری شود تا مسیرهای مورد درخواست مهاجم را به او نمایش دهد. به عنوان مثال یک مهاجم راه‌دور می‌تواند با ارسال درخواست "http://<target_IP>:37215/icon/../../../etc/inittab" به دایرکتوری inittab دسترسی پیدا کند.

# ۲ تحلیل حمله

بررسی اطلاعات ثبت شده در شبکه هانی نت ملی حاکی از این است که با احتمال زیاد حملات چند روز اخیر از آسیب‌پذیری CVE-2017-17215 استفاده کرده است. این آسیب‌پذیری امکان اجرای کد راه‌دور بر روی برخی دستگاه‌های Huawei را می‌دهد. مهاجم شناسایی شده (Authenticated) با ارسال بسته‌های آلوده بر روی پورت ۳۷۲۱۵ می‌تواند این حمله را اجرا کند. یک اکسپلویت موفق می‌تواند باعث اجرای کد از راه دور شود. کد زیر فرمت درخواست مهاجم به سیستم‌های آسیب‌پذیر را نمایش می‌دهد. در بخش CMD درخواست کد مورد نظر مهاجم قرار دارد. این درخواست به آدرس URL دستگاه‌های Huawei و پورت ۳۷۲۱۵ به صورت زیر ارسال می‌شوند. همینطور مهاجم از نام کاربری و گذرواژه پیش‌فرض برای اتصال به این دستگاه ها استفاده می‌کند.

```
"http://" + ip + ":37215/ctrlt/DeviceUpgrade_1"
```

**کد ۱- آدرس URL**

```
"<?xml version=\"1.0\" ?>\n    <s:Envelope
xmlns:s=\"http://schemas.xmlsoap.org/soap/envelope/\"
s:encodingStyle=\"http://schemas.xmlsoap.org/soap/encoding/\">\n    <s:Body><u:Upgrad
e xmlns:u=\"urn:schemas-upnp-
org:service:WANPPPConnection:1\">\n    <NewStatusURL>$(" + cmd +
")</NewStatusURL>\n<NewDownloadURL>$(echo
HUAWEIUPNP)</NewDownloadURL>\n</u:Upgrade>\n    </s:Body>\n    </s:Envelope>
"
```

**کد ۲ - درخواست ارسال شده**

باید توجه داشت که در صورت وجود این آسیب‌پذیری و موفقیت این حمله، مهاجم امکان اجرای هرگونه کد دلخواه بر روی دستگاه آسیب‌پذیر را دارد.

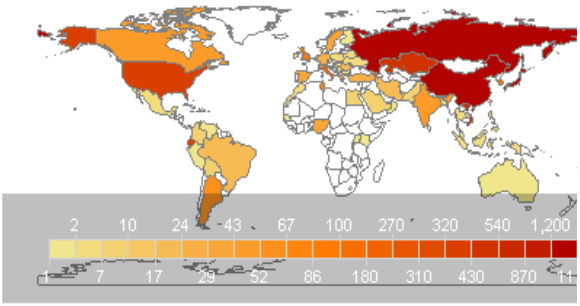
# ۳ روش مقابله و پیشگیری

با توجه به اینکه حملات مربوط به این پورت معمولاً مرتبط با نوع خاصی از دستگاه‌های روتر است، راه کار عمومی‌مقابله با این حملات به صورت زیر است:

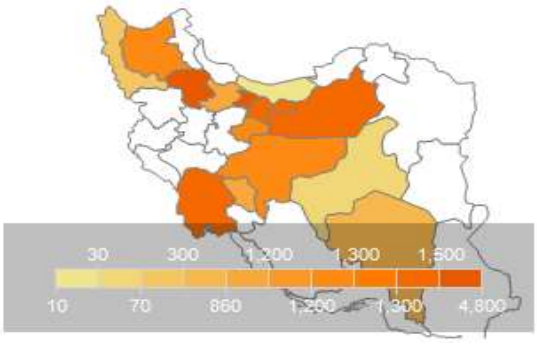
۱- بروزرسانی مداوم دستگاه ها جهت نصب وصله‌های امنیتی
۲- محدود کردن امکان دسترسی به دستگاه از شبکه ها و سیستم‌های مورد اعتماد و شناخته شده
۳- تغییر رمز عبور پیش فرض دستگاه

وضعیت حملات جهان از ۹۷/۰۷/۰۱ تا ۹۷/۰۷/۱۴

## مبدا حملات




## مقصد حملات




## روند حملات

## بدافزارهای برتر

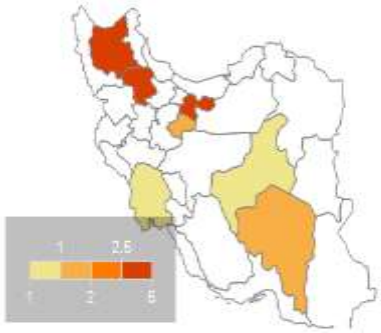
| بدافزار | تعداد |
|---|---|

## آدرس‌های برتر مهاجم

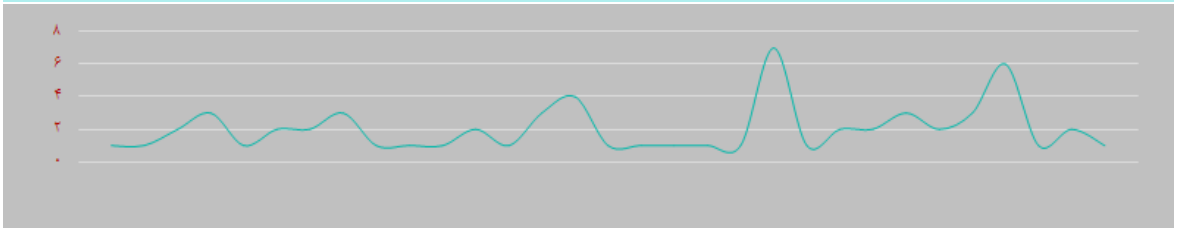
| آدرس | کشور | تعداد |
|---|---|---|
| 80.211.31.226 | ایتالیا | 115 |
| 80.211.216.182 | ایتالیا | 84 |
| 178.46.156.34 | روسیه | 76 |
| 138.68.19.29 | امریکا | 75 |
| 188.19.213.158 | روسیه | 49 |
| 115.231.86.11 | چین | 47 |
| 37.79.63.69 | روسیه | 47 |
| 113.120.95.152 | چین | 44 |
| 37.79.32.174 | روسیه | 43 |
| 223.202.202.208 | چین | 41 |

## افزایش حملات به پورت ۳۷۲۱۵ مرتبط با روترهای Huawei

وضعیت حملات ایران از ۹۷/۰۷/۰۱ تا ۹۷/۰۷/۱۴

| مبدا حملات | مقصد حملات از ایران |
|---|---|
|  |  |

روند حملات از ایران



| بدافزارهای برتر از ایران | |
|---|---|
| بدافزار | تعداد |

| آدرس‌های برتر مهاجم از ایران | | |
|---|---|---|
| آدرس | کشور | تعداد |
| 5.201.143.200 | ایران | 4 |
| 5.75.1.224 | ایران | 2 |
| 5.74.200.254 | ایران | 1 |
| 46.143.168.106 | ایران | 1 |
| 37.255.175.218 | ایران | 1 |
| 2.186.227.80 | ایران | 1 |
| 2.177.146.252 | ایران | 1 |
| 188.245.8.248 | ایران | 1 |