باسمه‌تعالی

حمله‌ی DDOS با سوءاستفاده از سرویس شناسایی تجهیزات بر روی محصولات Ubiquiti

(Open Ubiquiti DDOS)

چکیده حمله

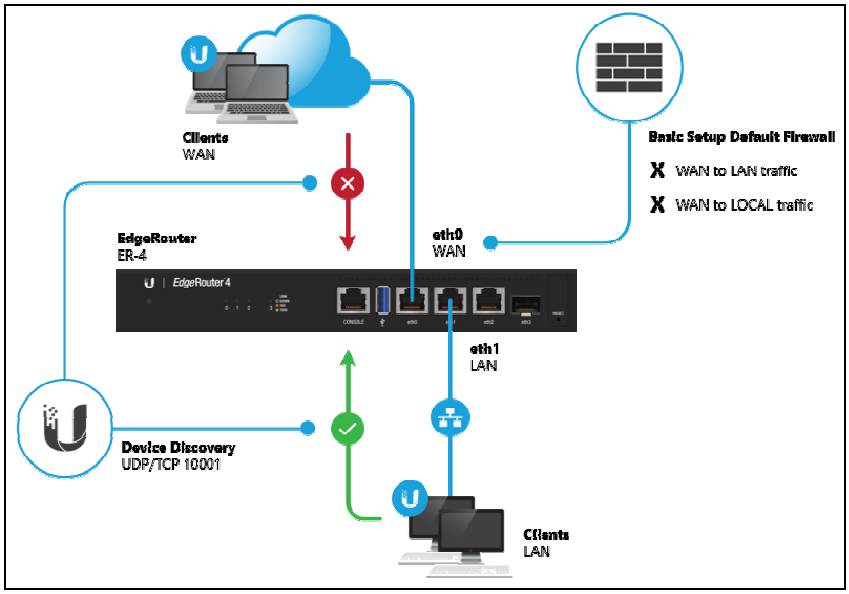
در ابتدای ماه فوریه ۲۰۱۹، تیم امنیت سایبری Rapid7 گزارشی از تهدید تجهیزات Ubiquiti برای اجرای حمله DOS منتشر کرد. در این حمله، از سرویس فعال بر روی پورت ۱۰۰۰۱ UDP استفاده می‌شود. این سرویس دارای کارکردهای متنوعی است که یکی از آن‌ها امکان شناسایی تجهیزات Ubiquiti توسط ISPها (عمدتاً Wireless ISPها) و شرکت‌ها است. با استفاده از این قابلیت می‌توان تنها با فرستادن یک بسته ۵۶ بایتی، پاسخ حجیمی که شامل نام، مدل، شماره نسخه firmware، IP Adressها، MAC Addressها و ESSID (درصورتی که تجهیز مورد نظر یک تجهیز wireless باشد) دریافت کرد. حجم این پاسخ به ۲۰۶ بایت می‌رسد. ضریب تقویت این حمله در گزارش‌ها ۳,۶۷ ذکر شده است اما این امکان وجود دارد تا به حدود ۳۰ الی ۳۵ نیز برسد. یکی از اثرات جانبی این حمله، قطع شدن دسترسی SSH به تجهیزات می‌باشد.

بر اساس اسکن انجام‌شده توسط تیم Rapid7، در سطح اینترنت بیش از ۴۸۵۰۰۰ تجهیز تحت تاثیر این حمله هستند. شایان ذکر است که این حمله تنها یک تجهیز خاص از شرکت Ubiquiti Network را مورد هدف قرار نمی‌دهد. Nanostation، AirGrid، LightBeam و PowerBeam از جمله این محصولات هستند. اکثر این محصولات در Wireless ISPها مورد استفاده قرار می‌گیرند.

سرویس شناسایی و کشف تجهیزات Ubiquiti

امروزه محصولات شرکت Ubiquitie Networks در حوزه‌ی شبکه‌های سیمی و بدون سیم با نام‌های تجاری مختلفی به فروش می‌رسند. شبکه‌هایی که از این تجهیزات استفاده می‌کنند بعضاً با همین اسم شناخته می‌شوند. از جمله محصولات معروف این شرکت که در ایران به وفور مورد استفاده قرار می‌گیرد، Access Pointهایی با نام UniFi AP است. این شبکه‌ها برای اتصال به شبکه‌ی خارجی به یک Edge-Router نیاز دارند. ویژگی Ubiquiti Device Discovery این امکان را می‌دهد تا تجهیزات این شرکت توسط ابزاری به نام UBNT Device Discovery Tool کشف و شناسایی شوند. همچنین به وسیله‌ی این خصوصیت، Edge-Routerها می‌توانند دیگر تجهیرات شبکه که متعلق به این شرکت هستند را شناسایی کنند. این خصوصیت متشکل از دو سرویس با نام‌های ubnt-discover و ubnt-discover-server است که به صورت پیش‌فرض بر روی بسیاری ار تجهیزات و ورژن‌های مختلف firmware فعال می‌باشد.

اینکه Edge-router امکان شناسایی تجهیزات Ubiquiti مجاور را دارد یا نه، توسط سرویس اول تعیین می‌شود. همچنین با فعال بودن سرویس دوم، Edge-Router توسط دیگر تجهیزات قابل شناسایی خواهد بود.



نحوه شناسایی تجهیزات آسیب‌پذیر

با استفاده از metasploit می‌توان تجهیزات Ubiquiti ای که این سرویس بر روی آن‌ها فعال هست را شناسایی کرد. برای این کار کافی است از ماژول auxiliary در مسیر auxiliary/scanner/ubiquiti/ubiquiti_discover استفاده نمود. شبکه‌ای که قرار است اسکن شود، توسط RHOSTS معرفی خواهد شد. با این کار آدرس IP، MAC، مدل، ورژن firmware و نام تجهیز مشخص خواهد شد.

```
       =[ metasploit v5.0.4-dev-d4211b1399                ]
+ -- --=[ 1852 exploits - 1047 auxiliary - 325 post       ]
+ -- --=[ 541 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]

msf5 > use auxiliary/scanner/ubiquiti/ubiquiti_discover
msf5 auxiliary(scanner/ubiquiti/ubiquiti_discover) > set RHOSTS 10.6.67.0/24
RHOSTS => 10.6.67.0/24
msf5 auxiliary(scanner/ubiquiti/ubiquiti_discover) > run

[+] 10.6.67.25:10001 Ubiquiti Discovery metadata: {"ips"=>["10.6.67.25"], "macs"=>["f0:9f:c2:4c:50:51"], "name"=>"mFi4c5051"
, "model_short"=>"P8U", "firmware"=>"MF.ar933x.v2.0.25.1238.140624.1356"}
[+] 10.6.67.28:10001 Ubiquiti Discovery metadata: {"ips"=>["10.6.67.28"], "macs"=>["f0:9f:c2:92:71:98"], "name"=>"mFi927198"
, "model_short"=>"P8U", "firmware"=>"MF.ar933x.v2.0.25.1238.140624.1356"}
```

با استفاده از ابزار NMAP نیز می‌توان این تجهیزات را شناسایی نمود. برای این کار کافی است از Script ای به نام ubiquiti-discovery.nse استفاده کرد. دستور اجرای آن به شکل زیر است:

```
nmap -sU -p 10001 --script ubiquiti-discovery.nse <target>
```

راه‌کارها

ابتدای امر بایستی مدیران شبکه‌ها از به روز بودن firmwareهای تجهیزات اطمینان حاصل کنند. دسترسی به سرویس پورت ۱۰۰۰۱ UDP بایستی توسط firewall یا قوانین ACL محدود و کنترل شود. در این صورت Edge-Routerها دیگر در شبکه‌ی WAN قابل شناسایی نخواهند بود. یکی دیگر از راه‌کارهای معرفی شده توسط شرکت Ubiquiti، غیر فعال کردن سرویس مورد نظر به طور کلی می‌باشد. برای این کار کافی است به وسیله‌ی سرویس SSH به تجهیز مورد نظر متصل شده و دستورات زیر را وارد نمود:

غیرفعال کردن سرویس ubnt-discover

```
configure
set service ubnt-discover disable
commit ; save
```

غیرفعال کردن سرویس ubnt-discover-server

```
configure
set service ubnt-discover-server disable
commit ; save
```

برای تایید وضعیت سرویس

```
show ubnt discover [detail]

show ubnt discover-server
```