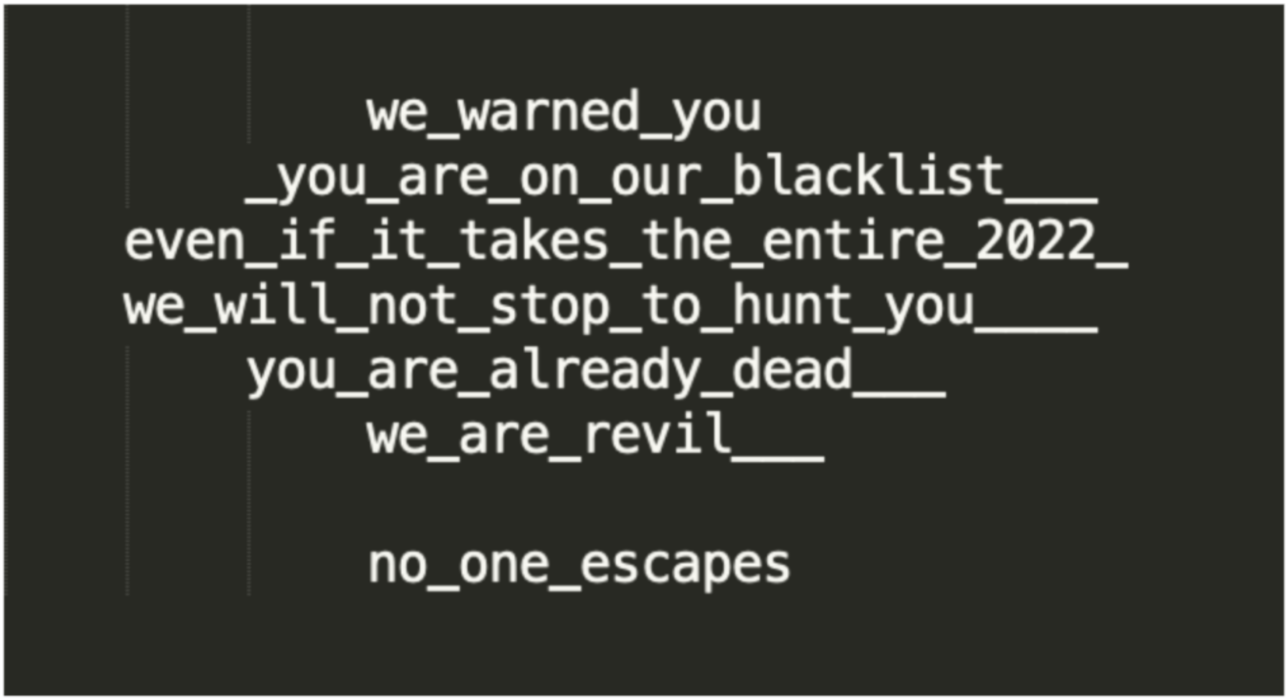
Imperva Mitigates Ransom DDoS Attack Measuring 2.5 Million Requests per Second

March 4, 2022

Application Security

We are only at the beginning of 2022 and it looks like it is going to be an interesting year for the Distributed Denial of Service (DDoS) landscape. We recently mitigated a ransom DDoS attack on a single website which reached a rate of 2.5 million requests per second (Mrps). And while ransom DDoS attacks are not new, they appear to be evolving and becoming more interesting with time and with each new phase. For example, we've seen instances where the ransom note is included in the attack itself embedded into a URL request.



```
          we_warned_you
      _you_are_on_our_blacklist___
  even_if_it_takes_the_entire_2022_
  we_will_not_stop_to_hunt_you____
      you_are_already_dead___
          we_are_revil___

          no_one_escapes
```

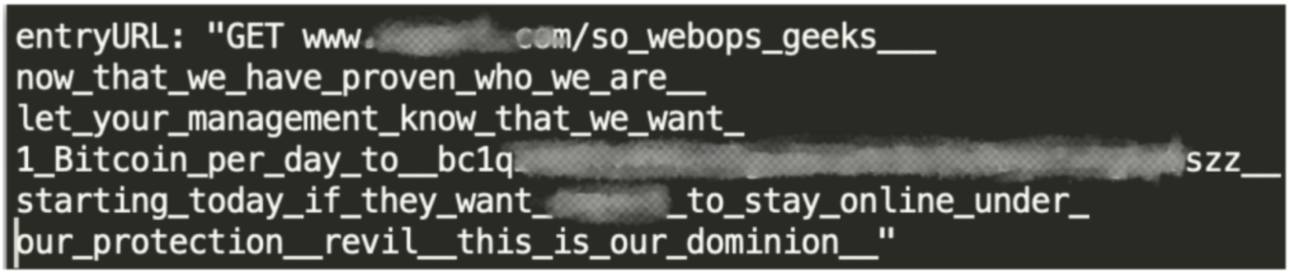
One of several ransom notes received by the customer before the attack started

A ransom note as part of the attack? Really?

Yes. Increasingly, we are observing more cases like this where the ransom note has been included as part of the attack itself, perhaps as a reminder to the target to send their bitcoin payment. Of course once the target receives this note the attack is already underway adding a sense of urgency to the threat. In the case of the 2.5 Mrps DDoS attack, the target had received several warning ransom notes before the first attack began.

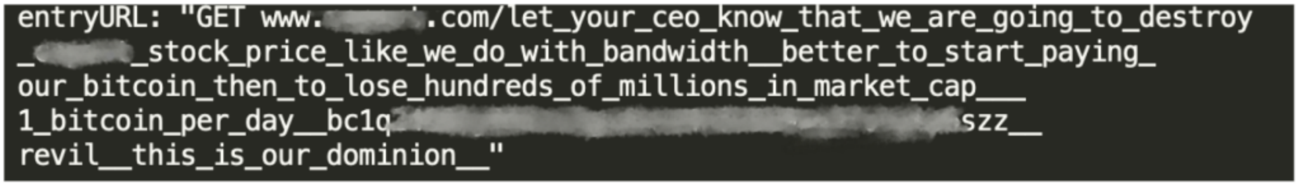
This tactic is not a one-off either. In the same DDoS attack, Imperva mitigated **over 12 million such embedded requests targeting** random URLs on the same site.

The following sinister message was incorporated into one of the URLs targeted.



```
entryURL: "GET www.[redacted]m/so_webops_geeks___
now_that_we_have_proven_who_we_are__
let_your_management_know_that_we_want_
1_Bitcoin_per_day_to__bc1q[redacted]szz__
starting_today_if_they_want_[redacted]_to_stay_online_under_
our_protection__revil__this_is_our_dominion__"
```

And the threats didn't stop there. The following day on the same site, Imperva mitigated **over 15 million** requests this time with the URL containing a different message but using the same scare tactics warning the CEO that they are going to destroy the company's stock price if they don't pay up.



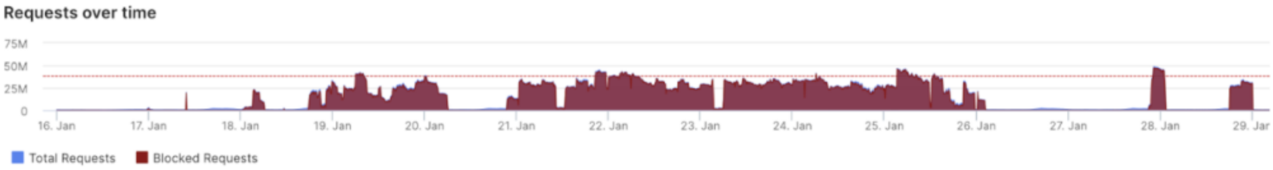
```
entryURL: "GET www.[redacted].com/let_your_ceo_know_that_we_are_going_to_destroy
_[redacted]_stock_price_like_we_do_with_bandwidth__better_to_start_paying_
our_bitcoin_then_to_lose_hundreds_of_millions_in_market_cap___
1_bitcoin_per_day__bc1q[redacted]szz__
revil__this_is_our_dominion__"
```

To show they mean business the attackers claim responsibility for a previous attack on the service provider Bandwidth, naming themselves the well-known Ransomware as a service (RaaS) operator REvil . *It is not clear however whether the threats were really made by the original REvil group or by an imposter.*

2.5 million requests per second in under a minute

Throughout the course of the same day the targeted company was hit by several DDoS attacks; the largest of which lasted less than one minute and measured up to 2.5 Mrps, setting a new mitigation record for Imperva. Multiple sites from the same company came under attack with one site sustaining an attack lasting around 10 minutes. The attackers applied sophisticated tactics to avert mitigation with the ransom messages and attack vectors changing constantly. At the same time, to shock the target, the payment amounts demanded kept increasing in size. Despite these tactics Imperva successfully mitigated all of the attacks and demonstrated how important it is to have a fast, accurate and automated DDoS solution in place.

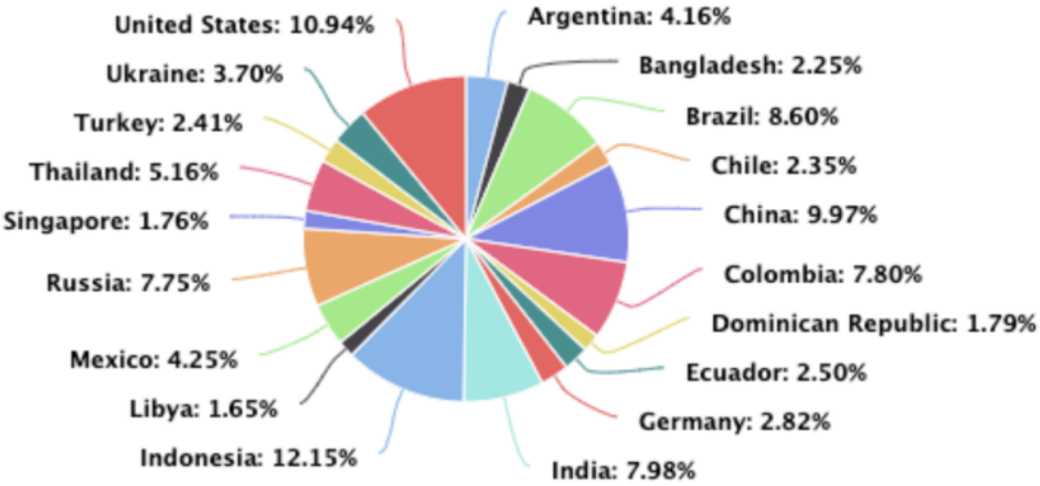
The story did not end there for the customer as the attacks continued for several days; sometimes lasting up to several hours and in 20 percent of cases reaching a size of between 90 and 750 thousand requests per second (Krps) as the chart below shows.



Attack origins

The attacks originated from 34,815 sources and looking at the number of requests per source, there were 2 million requests per IP sent from the top sources during the attack.

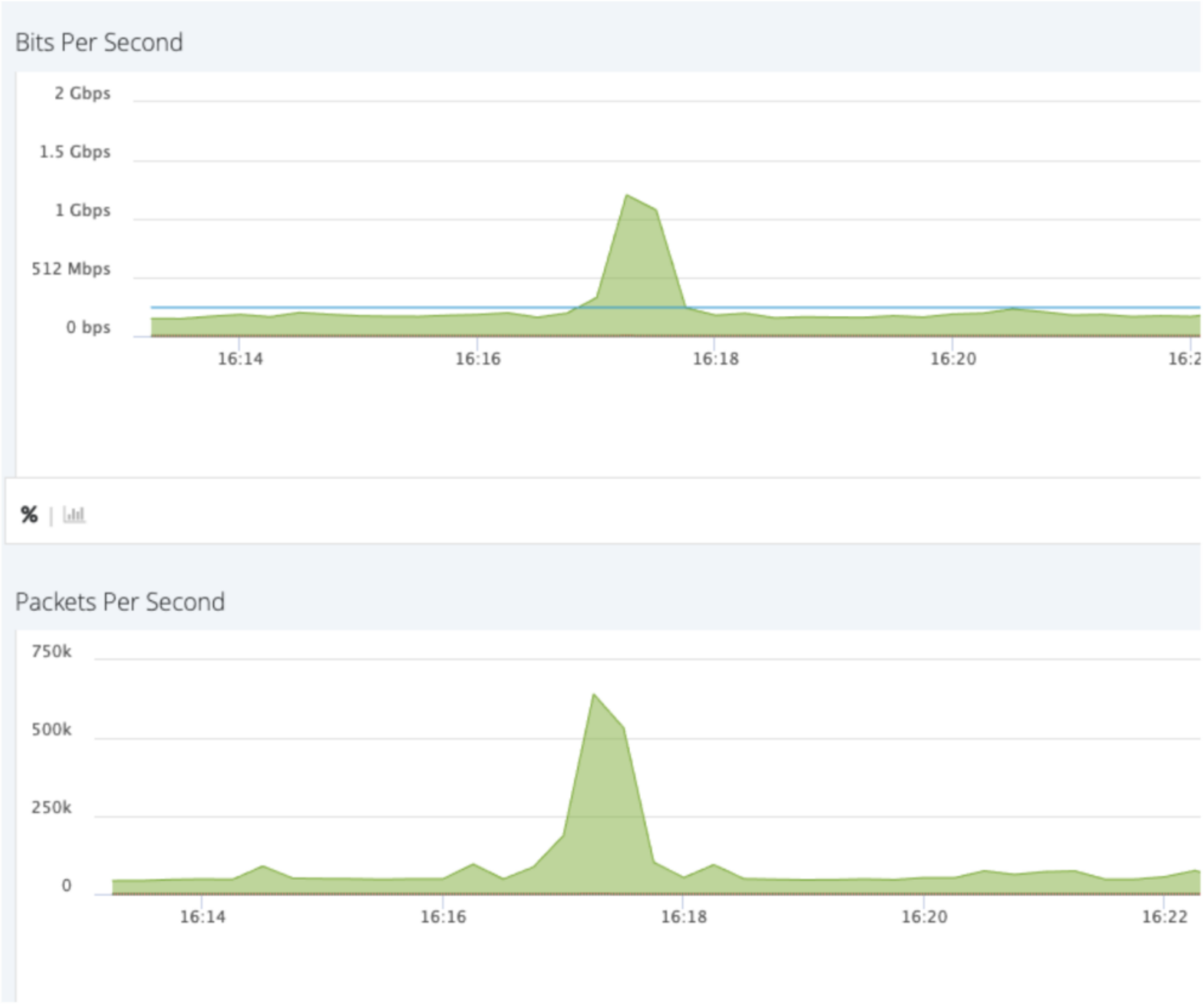
The top source locations for the **2.5 Mrps** attack were Indonesia followed by the United States. And we have seen a pattern emerging of almost identical source locations for different attacks indicating that the same botnet was used many times.



The botnet

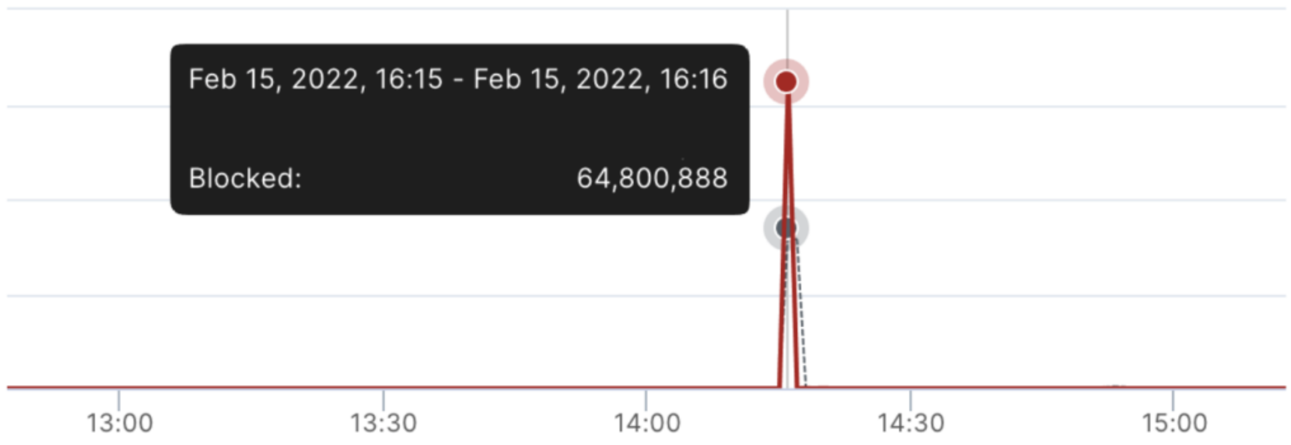
We have a strong indication that the Meris botnet played a role in these attacks. Although CVE-2018-14847 was published a while ago, attackers can still take advantage of it. The CVE refers to a MikroTik vulnerability where thousands of internet of things (IoT) devices, in this case a huge number of MikroTik routers, were manipulated to create a botnet network which can still be used to carry out DDoS and other forms of attack.

In terms of bandwidth, the results reached a volume of 1.5Gbps of TCP traffic. The dashboard below represents the traffic in our scrubbing centers, before it reached our proxies that mitigated the attacks in the application layer:



Threat intelligence and Bot protection

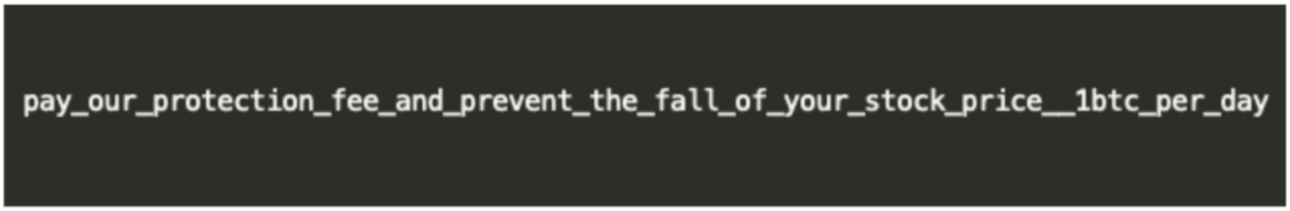
Despite the changing attack patterns, Imperva successfully mitigated the attacks within seconds using mainly threat intelligence, as the sources were known to us as malicious; and bot protection, as the clients were impersonating a legitimate browser or google bot. While the largest attack measured 2.5 Mrps the graph below shows how we blocked over 64 million requests in under one minute.



Repeat performance

We have since monitored a repeat of this attack pattern against several other customers. While each of the targets receives a unique bitcoin address they are all part of the same coordinated attack.

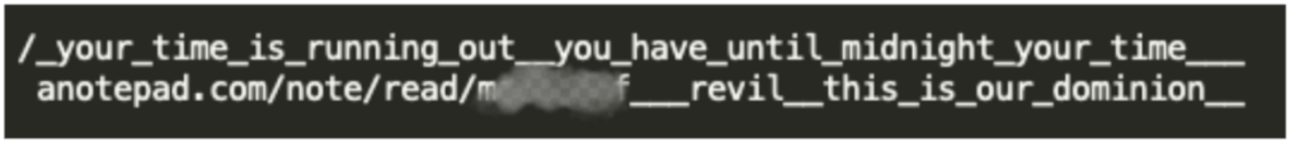
The types of sites the threat actors are after appear to be business sites focusing on sales and communications. Targets tend to be US- or Europe-based with the one thing they all have in common being that they are all exchange-listed companies and the threat actors use this to their advantage by referring to the potential damage a DDoS attack could do to the company stock price. See example below.



```
pay_our_protection_fee_and_prevent_the_fall_of_your_stock_price__1btc_per_day
```

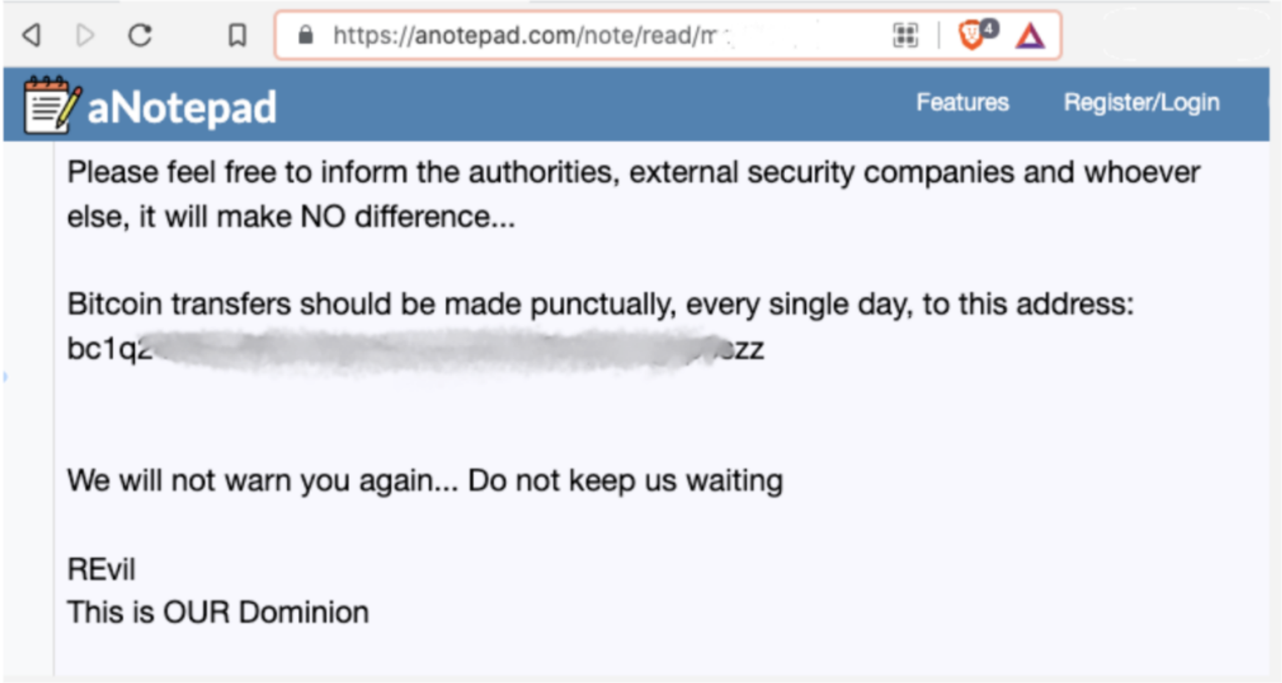
Ransom within a ransom

Another example of a threat embedded in the attack itself was found in a GET request sent with a link to a notepad.com note.



```
/_your_time_is_running_out__you_have_until_midnight_your_time___
 anotepad.com/note/read/m[redacted]f___revil__this_is_our_dominion__
```

Another note (below) contains the now familiar pattern of a ransom demand for payment in bitcoin.



Please feel free to inform the authorities, external security companies and whoever else, it will make NO difference...

Bitcoin transfers should be made punctually, every single day, to this address:
bc1q[redacted]zz

We will not warn you again... Do not keep us waiting

REvil
This is OUR Dominion

What’s Next?

As the REvil threat gang mentioned, we can expect more of the same throughout 2022. If you don’t already have DDoS Protection in place, now is a good time to prepare for a potential attack. Find out more about Imperva DDoS Protection here.

Try Imperva for Free

Protect your business for 30 days on Imperva.

Start Now