OnePageCRM

Surviving a DDoS attack

30/10/2024

OnePageCRM

A little bit of Theory

- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems
  - Risk Management
- ISO/IEC 27035-2:2023 Information technology — Information security incident management
  - Guidelines to plan and prepare for incident response

Risk Assessment

Risk ID	Risk	Likelihood	Impact	Risk Level	Treatment Action
1	Unauthorized Access to Sensitive Data	High	Critical	Very High	Implement MFA and strong password policies
2	Data Loss due to System Failure	Medium	High	High	Set up automated backups and offsite storage
3	Phishing Attacks on Employees	High	Medium	High	Conduct security awareness training
4	DDoS Attack	Low	High	High	Apply specialized DDoS protection service

OnePageCRM

Incident Response

- Plan and prepare
  - Incident Response Plan (IRP)
  - Incident Response Team (IRT)
- Learn lessons
  - Areas for improvement
  - IRP & IRT evaluation

OnePageCRM

How story started

- Nice friday evening, colleagues goes for pints
- 2 weeks to Christmas holidays
- All work is sorted out and time to close office and enjoy nice weekend
- 5:41pm Just before closing laptop message from remote developer pointing to slack message: alert from pingdom our SSO server is not available
- 5:42pm Pingdom shows red lines and reports that requests from 3 servers failed
- 5:43pm sso in browser gives 404 not found
- 5:45pm sso server accessible by ssh and nginx logs shows unusual bunch of requests coming from several different ip addresses

Customer support

- 5:45pm Custom Support received messages in Customer Support chat

Our securely team found sql injection vulnerability. With this security hole opened It is possible to keep your site closed for months off. Our security team can provide you with a detailed report and tell you where the vulnerability is:

https://secure.onepagecrm.com/ check your site down. If you care about your customers, we will provide you with the solution and why the problem is, welcome to contact. ***After paying $5000 to the Bitcoin account,*** *we will send solution file and all the problems caused. My team has stopped all traffic to your site now, thanks to this vulnerability.*

*https://t.me/****** My Telegram*

********@gmail.com My Mail.*

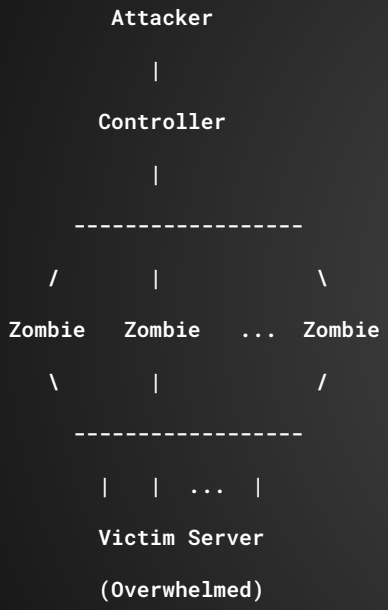
OnePageCRM

Response

- 5:44pm Broadcast update for whole team on the company-wide WhatsApp channel
- 5:45pm Call in incident response (IR) meeting room opened
- 5:52pm 1 DevOps joined the call
- 5:53pm Confirmed that we have DDoS attack
- 6:03pm 2 DevOps joined the incident room (just after 1 pint) on the walk back to office

OnePageCRM

Distributed Denial-of-Service Attack (DDoS)



OnePageCRM

Response

- Quick decisions was made
  - do not communicate with hacker / do not pay
  - face the problem
  - find a solution

OnePageCRM

OnePageCRM

Solutions vectors

- Buy and deploy AWS shield service DDoS protection
- Block by IP with Linux iptables
- Enhance infrastructure with ALB, WAF and try to block DDoS with WAF firewall rules
- Ask AWS support to help
- Buy and deploy Cloudflare DDoS protection

OnePageCRM

AWS shield service with DDoS protection / AWS support service

- $3000 per month
- Minimum commitment of 12 months
- $36,000 budget decision to make

- AWS support costs for us $469.73 with 6 months commitment
- They return to us in 1 hour with suggestion to use AWS Shield

OnePageCRM

Cloudflare DDoS protection

- Perfect and well known solution, widely used
- DNS zones management had to move to Cloudflare to be fully protected
- Big infrastructure decision to apply in short amount of time

$469.73
$469.73

OnePageCRM

Enhance infrastructure with ALB, WAF

- With terraform tool enhance our infrastructure around SSO
  - Application load balancer (ALB)
  - Web application firewall (WAF)
- Feed the ip addresses to block from measuring frequency of requests from logs
- 2 hours 30 min of WAF works burns $450
- $130k per months 🤯🤯🤯

Block by IP with Linux iptables

- Block ip address on Linux

  sudo iptables -A INPUT -s IP_ADDRESS -j DROP

- Try ban 1-2 ip addresses, saw that new Zombie addresses jump into attack
- Ask ChatGPT

  Could you please ***create parser in bash and accumulate all ip addresses used in ddos (first column):***

  10.23.72.110 - - [08/Dec/2023:18:15:45 +0000] "GET / HTTP/2.0" 503 190 "/" "Mozilla/5.0 (Nintendo Switch; WebApplet) AppleWebKit/606.4 (KHTML, like Gecko) NF/6.0.1.16.10 NintendoBrowser/5.1.0.20923" "10.101.121.159" "-" req 0.065 upstream 0.064

  10.23.72.110 - - [08/Dec/2023:18:15:45 +0000] "GET / HTTP/2.0" 503 190 "/" "Mozilla/5.0 (Nintendo Switch; WebApplet) AppleWebKit/606.4 (KHTML, like Gecko) NF/6.0.1.16.10 NintendoBrowser/5.1.0.20923" "10.101.121.159" "-" req 0.065 upstream 0.064

Block by IP with Linux iptables

```
#!/bin/bash

LOG_FILE=$1

# Extract IP addresses and count occurrences

awk '{print $1}' "$LOG_FILE" | sort | uniq -c | sort -nr
```

26981 10.19.208.175

24440 10.41.143.117

23904 10.63.72.110

23080 10.80.39.89

OnePageCRM

Block by IP with Linux iptables

- Ask ChatGPT to enhance filter by the first column number to filter more than 100

```
# Extract the first column (IP Address), count occurrences, and filter by count
awk '{print $1}' "$LOG_FILE" | sort | uniq -c | sort -nr | awk '$1 > 100' | awk '{print $2}'
```

10.19.208.175

10.41.143.117

10.63.72.110

10.80.39.89

Block by IP with Linux iptables

- Next script from ChatGPT read ip addresses and filter with iptables:

```
#!/bin/bash

IP_LIST_FILE=$1

# Read each IP address

while IFS= read -r ip_address

do

    # Add a rule to iptables ipfw to block the IP address

    sudo iptables -A INPUT -s "$ip_address" -j DROP

done < "$IP_LIST_FILE"
```

Block by IP with Linux iptables

- Ask ChatGPT to write a cycle script to parse and rotate logs

```
#!/bin/bash
NUM_CYCLES=10000
for (( i=1; i<=NUM_CYCLES; i++ ))
do
  ./parse_and_rotate_logs.sh "$1" > "cycle_ip_addr_$i_block"
  ./block.sh "cycle_ip_addr_${i}_block"
  wc -l "cycle_ip_addr_${i}_block"
  sleep 10
done
```

End of story

- 02:07am 1 Devops suggested the sso is stable now and a good idea is to leave it as it is till 9am or 10am in the morning.
- 02:09am 3 Devops is suggesting that cloudflare may be a good solution to go for
- 02:16am End of the day and will start in the morning with lessons learned session

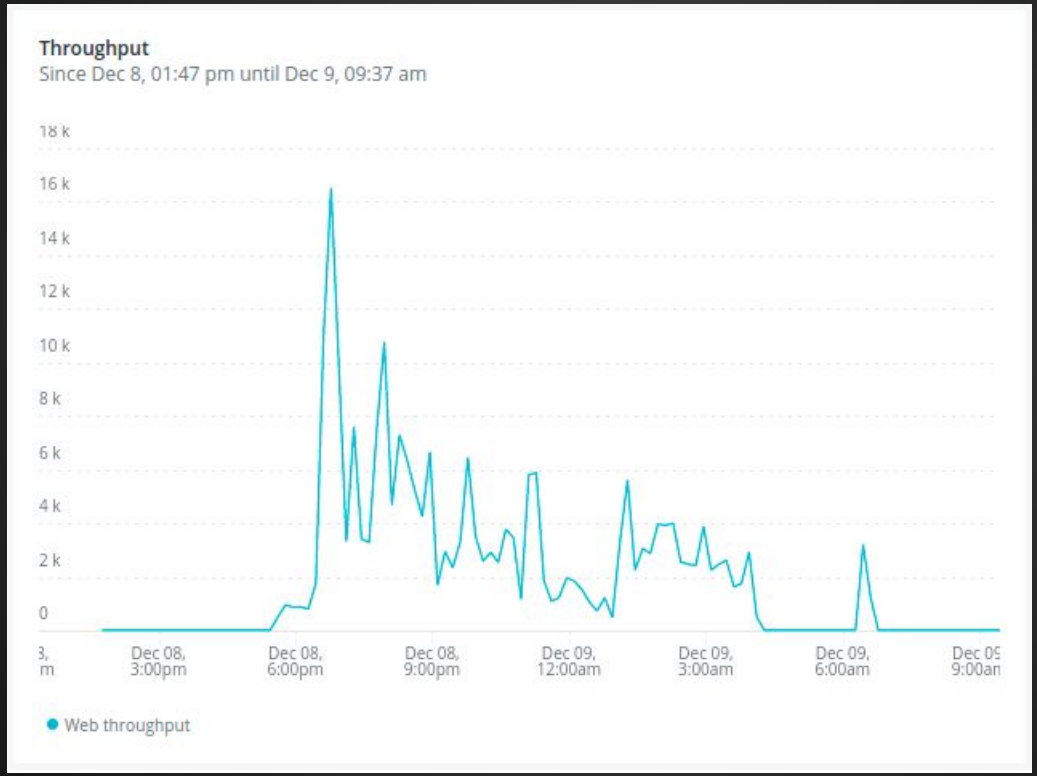
OnePageCRM

Summary

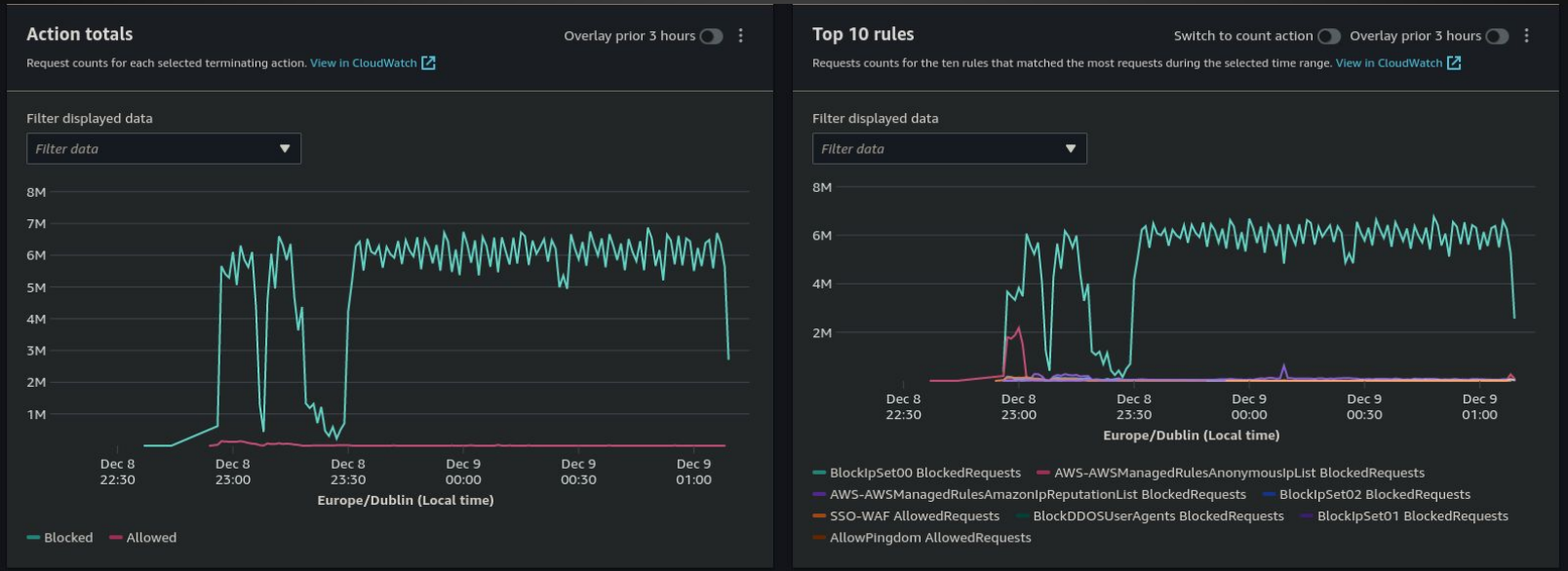
- Botnet total IP address blocked 6454
- DDoS attack continues for 11 hours
  - 5:40pm - 4:10am
  - Retry 6:10 am - 6:40 am
- SSO downtime 2 hours, 28 outages
- Simple solution works well
  - linux, iptables, bash, unix pipes, unix commands: awk, sort, uniq
  - ChatGPT boost reduced time to deliver
  - 0 extra costs

Attack timeline Pingdom measurements

New Relic Throughput measurements



WAF measurements



OnePageCRM

Afterthoughts

- IRP incident response plan
- IRT incident response team
- Training: communication, roles, games
- Timeline
- Post incident session
- Background skills
- Improvisation

Thank you


Join us
https://www.onepagecrm.com/careers/