ProtonMail

DDoS Attack – Lessons Learned

Zurich, April 7, 2016

Dr. Andy Yen, co-founder and CEO

ATTACK BACKGROUND

November 4th, 2015, ProtonMail was attacked

- Largest and most high profile DDoS attack to hit Switzerland.
- Made headlines around the world.
- In total, nearly 60 hours of downtime spread out over 4 days.
- Was really a life or death situation for the business.


sign in search more International

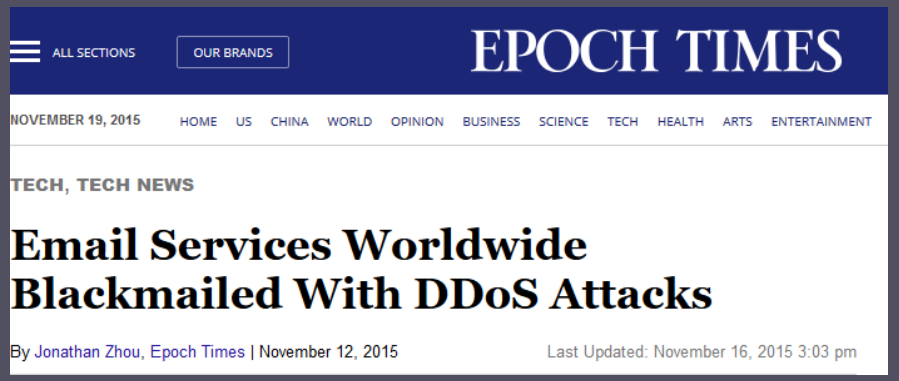
theguardian

home › tech UK world sport football opinion culture business lifestyle all

Hacking

ProtonMail: encrypted email provider held ransom by hackers

Email provider based in Switzerland has internet connection cut off by hackers who did not cease attack even after $6,000 ransom was paid


ALL SECTIONS OUR BRANDS EPOCH TIMES

NOVEMBER 19, 2015 HOME US CHINA WORLD OPINION BUSINESS SCIENCE TECH HEALTH ARTS ENTERTAINMENT

TECH, TECH NEWS

Email Services Worldwide Blackmailed With DDoS Attacks

By Jonathan Zhou, Epoch Times | November 12, 2015 Last Updated: November 16, 2015 3:03 pm

COMPANY BACKGROUND

PROTON TECHNOLOGIES AG

- The world's largest encrypted email provider.
- One of the largest email providers in Switzerland.
- Over 1 million customers from 150+ countries

Key Facts:

- Founded in August 2013 by CERN scientists
- Headquartered in Geneva, Switzerland with a research center in San Francisco, CA
- In 2015, ranked by Business Insider as the hottest startup in Switzerland

> "ProtonMail Bids for Google's Crown with fully encrypted email for everyone."
>
> Forbes

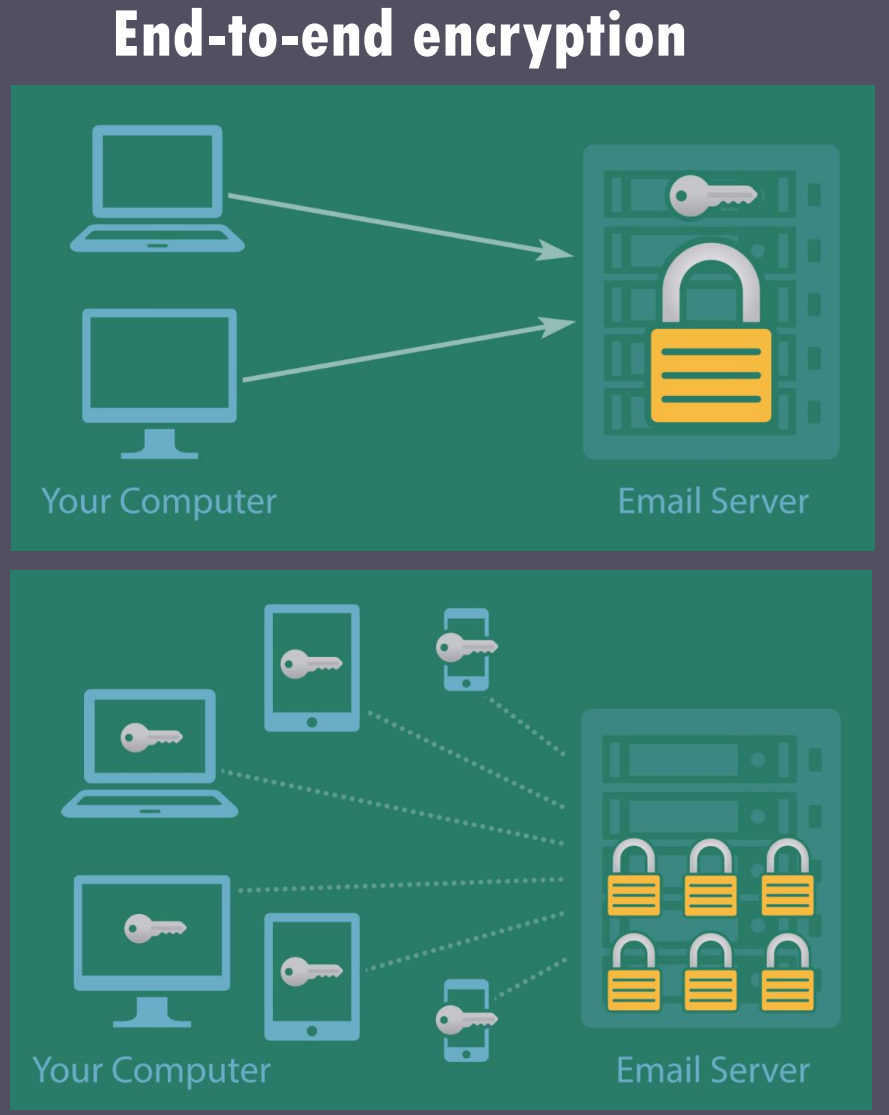
ENCRYPTED EMAIL

PROTONMAIL

- The best way to protect data is to not have data
- Encrypt data before it reaches the server
- Encryption is transparent to the user

ADVANTAGES

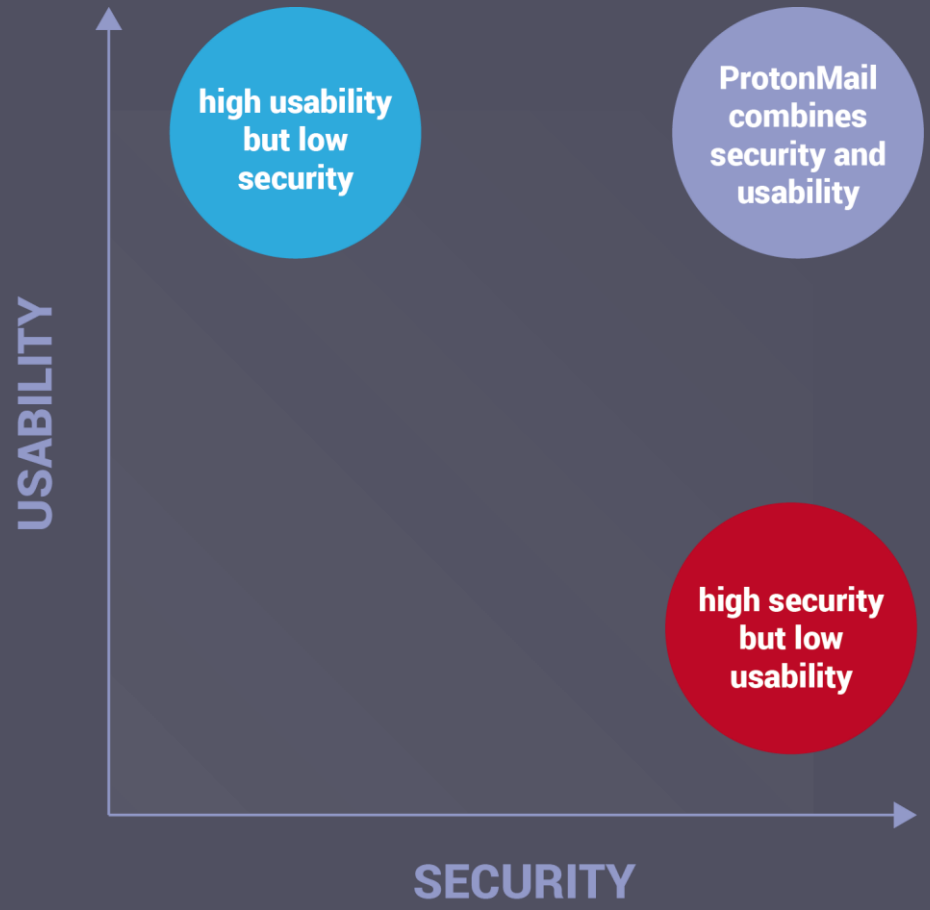
- Service provider can’t access your data
- Better protection in case of server compromise



PROTONMAIL

Cloud Security

- Cyberattacks – not a matter of if, but a matter of when
- Unfortunately, companies (and people) are “lazy”
- Securing your own infrastructure is expensive
- Cloud solutions like ProtonMail can actually be more secure
- At the same time, also more cost effective
- E2EE mitigates privacy concerns of the “cloud”



PROTONMAIL

November 2015 DDoS Attack

- ProtonMail is not an appealing target for conventional hacking attacks.
- If you can’t steal the data, making it unavailable is the next best alternative.
- ProtonMail is an appealing target for several reasons
  - Well known international brand
  - Smaller company, probably fewer resources to resist large scale attack
  - Service interruptions are costly for the business
- Initial attacks will invite further attacks (we know of at least two separate attackers)

ProtonMail

FIRST ATTACKER

ARMADA COLLECTIVE

Background

- Either originating from DD4BC or acting as copy cat and using their methods.
- Focused on hosting providers, e-commerce, financial services primarily in Europe.
- Mostly financially motivated.

Strategy

- Customers will receive a ransom mail, asking for 15-30 bitcoins (5.600 € – 8.400 €).
- Warning attack follows within minutes. If payment refused, threatened with further attacks
- Targeted - Emails sent to dedicated and named internal recipients
- Do their homework – if victim has strong DDoS protection, they will not go after it.

Attack Methods

- Current vectors are amplification attacks (NTP, RIP Reflection Amplification)
- Warning attacks up to 20GB

Risk

- Effected organizations have short time to act and prepare
- Very high risk – aggressive and professional attackers
- Proven results with high volume and taking down companies

ProtonMail

SECOND ATTACKER

Identity Unknown

- Second attacker was extremely powerful.
- Attacks reached 100 Gbps
  - Targeted entire datacenter
  - Attacked upstream ISPs
  - Impact felt as far away as Moscow
- Attack against ISPs serving ProtonMail was a coordinated strike, simultaneously hitting routers in London, Paris, Zurich, Geneva, Frankfurt and Moscow.
- May have been a nation state actor (We have a contentious relationship with several countries)

PROTONMAIL DDoS ATTACK

TIMELINE


TechRepublic. CXO Innovation Cloud Security Big Data More

SECURITY

Exclusive: Inside the ProtonMail siege: how two small companies fought off one of Europe's largest DDoS attacks

What started as a simple digital ransom quickly escalated into a trans-continental networking battle.

By Dan Patterson | November 13, 2015, 11:46 AM PST

ProtonMail

Nov. 3 2015	Nov. 4 2015	Nov. 5-7 2015	Nov. 8 2015	Nov. 9-15 2015
Ransom email received from The Armada Collective, followed by DDoS attack that took site offline for 15 mins	Next DDoS attacks hits in the morning and by afternoon reached over 100G directly attacking the datacenter and ISP infrastructure.	ProtonMail continues to suffer from ongoing high volume, complex attacks from a second, unknown source	Radware's Emergency Response Team brought in to help mitigate attack. Service restored shortly afterwards.	Attacks continue at high volume of 30-60G at peaks during these days. Attacks are mitigated successfully by Radware

- Considered to be one of the largest attacks in Europe
- Bulk of the damage caused by the second, unidentified attacker, which made no demands.

ProtonMail

PROTONMAIL DDoS ATTACK

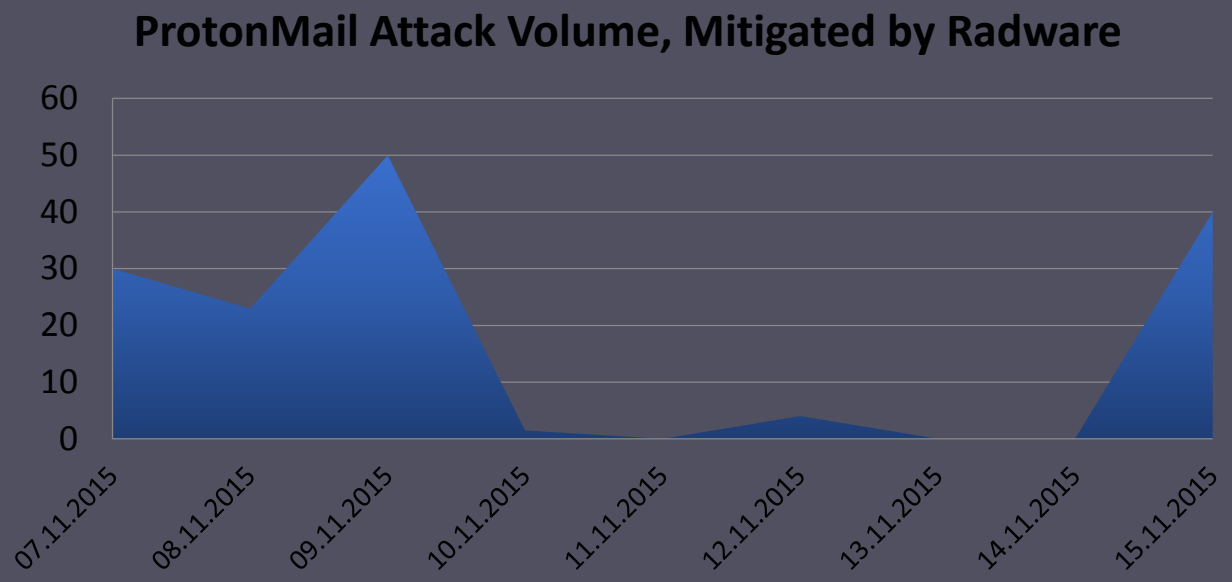
Evolution of Attack Vectors

Nov 8th	Nov 9th	Nov 10th	Nov 11th
• UDP flood • SYN flood • DDoS-NTP-reflection • DDoS-DNS-reflection • SYN-ACK Flood • DDoS-TCP-urgent • DDoS-TCP-zero-seq • DDoS-chargen-reflected events	• UDP Flood – Reflective DNS • TCP RST Flood • ICMP Flood • SYN Flood – HTTPS • SYN Flood – HTTP	• UDP Flood – SSDP & NTP Reflection • ICMP Flood • TCP SYN Flood • TCP Out-of-State Flood	• UDP flood DDoS-SSL • TCP Out-of-Stat DDoS-udp-fragmented • DDoS-NTP-reflection DDoS-DNS-reflection • SYN-ACK Flood Minor ICMP flood/RST flood • SYN flood

- Sign of a highly sophisticated attacker.
- Repeatedly trying new strategies to break through Radware.

PROTONMAIL DDoS ATTACK

Persistent DDoS Attacks



Network	Application
UDP Flood	DNS Reflection
TCP RST Flood	NTP Reflection
TCP-SYN	SSDP
TCP Out-of-State	HTTP/S SYN Flood
SYN-ACK	
ICMP	

- Attackers are extremely persistent, seeing attacks on an almost weekly basis, even now.
- DDoS protection needs to be permanently implemented.

EVALUATING SOLUTIONS

THERE ARE MANY TYPES OF DDoS PROTECTION...

- It is critical to understand your legitimate traffic. As an ESP, we literally have every type (http/https/smtp/dns, etc)

- Two main types of solutions exist today:
  - DNS based solutions (point DNS records to scrubbing centers)
  - BGP solutions

- In our experience, BGP solutions are more effective and have more capabilities.

EVALUATING SOLUTIONS

KEY CONSIDERATIONS

- How fast can the solution be implemented?
- Can it protect all legitimate traffic types? False positives?
- Does the solution compromise the security/privacy of your infrastructure?
- Does the solution compromise the usability of your product?
- How quickly can the solution adapt and respond?

- In ProtonMail’s case, Radware was able to meet these requirements.

ProtonMail

LESSONS LEARNED

A FEW NOT SO OBVIOUS POINTS...

- You are vulnerable if your datacenter and upstream bandwidth providers are vulnerable.
  - We saw attacks against our PTP and upstream routers
- Collateral damage matters
  - If your DC or ISP is suffering, they will probably disconnect you.
- Solution: Isolate your infrastructure
  - Need to get to the state where you only rely on your datacenter for power and cooling

LESSONS LEARNED

PROTECTION DOES COME AT A COST

- Isolating infrastructure is not trivial
  - ProtonMail now connects directly from our DC to the main Swiss POP in Zurich 114 km away (using SBB dark fibre)
  - We use a dedicated IP-transit provided by a Tier 1 carrier.
  - We are a RIPE LIR, have our own ASN and own IPv4 /22
- Need to have networking experts to manage the infrastructure
  - IP-Max SA is the best in Switzerland
- Relative to our size, we have an insanely sophisticated/resilient infrastructure.
- Large fixed and re-occurring costs for the business.
- This is partially offset by more customers.

THANK YOU

Proton Technologies AG
Dr. Andy Yen
andy@protonmail.ch
protonmail.com