How can we better secure our systems

Dovid Bender
https://github.com/dovi5988/cluecon/2021

About me

Dovid Bender
Phone freak by day Firefighter by night.

Overview

- Who is this for?
- What has changed in the last few years?
- What kind of attacks are we seeing?
- What can we do about it?

Recent attacks

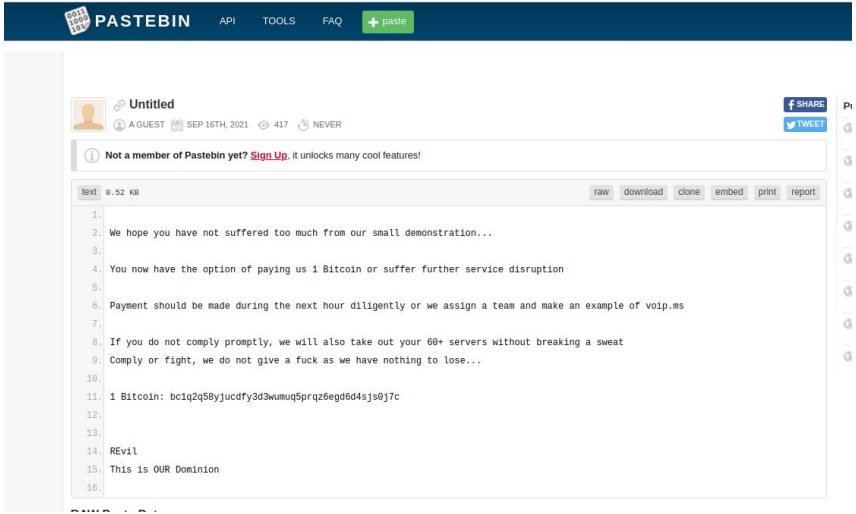
UK VOIP company

- Not much known about attack(s)

Recent attacks

VoIP.MS

- - Was done for profit
- - Started as an attack on their DNS servers.
- - Pivoted to volumetric and I assume SIP as well



Recent attacks

Bandwidth

- As with VoIP.MS was done for profit.
- Started as volumetric attack.
- Attacks seemed to have targeted the US 9-5 work day
- BGP showed all routes dropped except ISP that does DDOS scrubbing.
- A day or two later issues started again. I was told attackers pivoted to attacking with SIP packets.
- BGP then showed all traffic going through cloudflare.

DDOS mitigation & protection

CloudFlare

- Not cheap but is the gold standard.
- They say they have 100TB of capacity.
- Auto mitigation in 3 seconds.
- At the very least SSH/WEB/DNS behind them. It won’t break the bank.
- Many other services

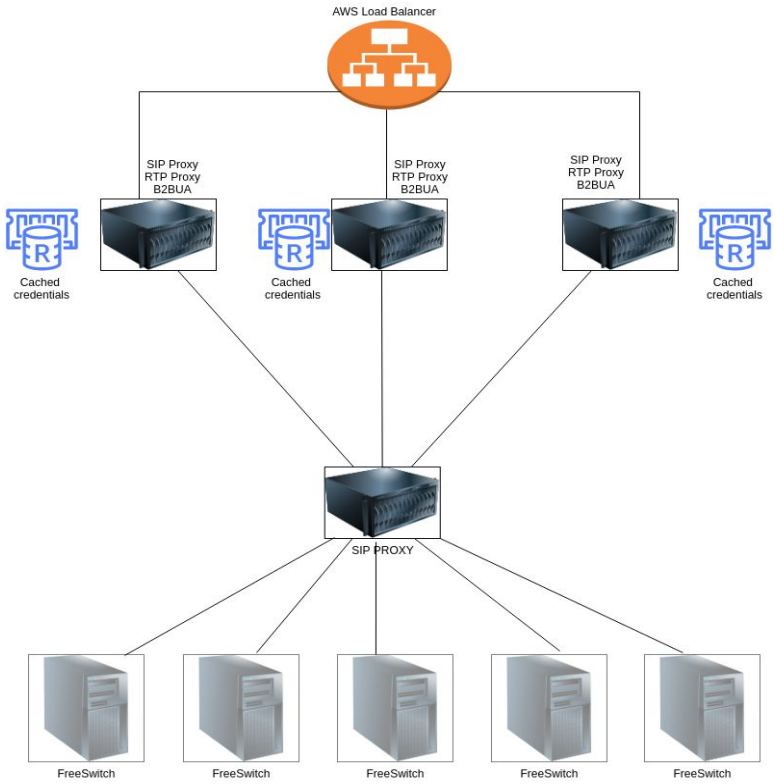
DDOS mitigation & protection

Do it yourself. (AWS as an example).

- AWS has a DDOS solution (not cheap).
- Load Balancer (hashed based srcIP:port dstIP:port) so no issues with UDP.
- Use OpenSIPS/Kamailio to scale out as needed. Let these instances take the brunt of the traffic.
- Use the pike module to rate limit traffic, if there is too much ban the IP in iptables
- Validate all packets to make sure they are valid SIP packets, if they aren't ban them with iptables.

https://opensips.org/html/docs/modules/3.3.x/sipmsgops.html#func_sipmsg_validate
https://www.fredposner.com/2367/handling-sip-flood-attacks-using-kamailio/
https://www.fredposner.com/handling-non-sip-kamailio/

DDOS mitigation & protection



DDOS mitigation & protection

In addition

- Lots of other DDOS mitigation providers out there. Do your homework.
- Ban known bad IP's for instance https://github.com/trick77/ipset-blacklist
  - TOR Exit nodes
  - Known bad/compromised hosts
- API BAN - https://apiban.org/
- Don't forget about IPv6.
- Hide from Shodan [1]

[1] https://www.kwancro.com/post/hide-from-shodan/

DDOS mitigation & protection

- Whatever solution you go with TEST, TEST, TEST! DON'T ASSUME! A solution is worthless if not tested periodically.
- Find a LEGITIMATE company that can stress test your system. [1] [2]
- Many large telecom companies were shocked with their limits when stress testing their systems.
- Self preserve. If your max is 50k CPS don't let OpenSiPS/Kamailio take more. Drop the excess traffic rather than go down.
- These are general rules. As you go through your dev cycle you should re-test and evaluate.

[1] https://www.enablesecurity.com/ - SIP, RTP, Web, XMPP and various others (volumetric coming)
[2] https://www.red-button.net/ - AWS Authorized DDOS test partner

Back to basics

Things to watch

- Sign up with your vendors to find out about latest security issues. Most software vendors and lot's of open source projects have a dedicated security email group for notifications.
- Telegram can be a great resource. I follow
  - Hacker News https://t.me/hackernewslive
  - Cybersecurity & Privacy News - https://t.me/cibsecurity - Great for all CVE's
  - The Hacker News - https://t.me/thehackernews
  - Cyber Security News - https://t.me/Cyber_Security_Channel
- Podcasts
  - CyberWire-X
  - Security In Five Podcast
  - The Tripwire Cybersecurity Podcast
  - Defensive Security Podcast - Malware, Hacking, Cyber Security & Infosec
  - Beers with Talos Podcast
- Twitter - The list is every long….

Back to basics

- Just because you can’t do it all, it doesn’t mean you should not do any of it.
- Have your system audited by a **reputable organization**.
- Have a backup plan, and test it. Best if backups are:
  - Preferably stored off site, if on the cloud in a different account.
  - Stored with immutable storage.
  - If you have bare metal look at solutions like Veeam or N-Able.
- Attackers like to linger.
- Test periodically. You **must validate** your backups otherwise do you really have backups?
- selinux/apparmor is there for a reason. Use it!

Back to basics

- Principle of Least Privilege [1]
  - Does the SQL server need SSH access to the NFS server?
  - If using AWS or other cloud providers don't use the same API keys for all systems.
  - Credentials should only have access to what they need to. (e.g. cdr's collector should only have sql access to the cdrs table).
- Segment your network. Put stops between systems. Don't let an attacker move laterally.
- SSH
  - Only leave open to known hosts or at the very least use a service like CloudFlare [2]
  - SSH KEYS ONLY **with** passphrases. Passwords should be for console access **only**.
- 2FA is a must and as much as we love SMS it can be less than secure.

[1] https://en.wikipedia.org/wiki/Principle_of_least_privilege
[2] https://www.cloudflare.com/products/cloudflare-spectrum/ssh/

Back to basics

- Cycle through passwords regularly.
- The only secure password is the one you don’t know, use password managers.
- Have a schedule to update your systems periodically.
- Provisioning
  - If you provision handsets, mutual TLS is a must.
  - Reduce the attack surface area (e.g. by customer or phone moel).
- Don’t rely on one method (e.g. use Fail2Ban with mutual TLS)
- Look at my talk from 2018 [1]

[1] https://www.youtube.com/watch?v=9Wzzlo1kfTQ

Thank you

Evan Mcgee from Signal Wire @startledmarmot
Fred Posner from LOD @fredposner
Sandro Gauci from Enable Security @sandrogauci
David Duffett from Let The Geek speak @dduffett
SignalWire crew!

Questions?