Ongoing Threats to Emerging Financial Entities

By: Bryce A. Lynch

Hi.

Bryce Alexander Lynch

- Chief of Security, Ripple (https://ripple.com/)
- Information Security Practitioner
  - Security research
  - Incident response
  - System architecture and engineering
  - Policy development
- Former penetration tester and red team member inside the DC Beltway
- Member, Zero State (http://zerostate.net/)
  - Nontraditional methods of group organization and direct action
  - Personal augmentation
- Advisory board, Lifeboat Foundation (http://lifeboat.com/)
- I say things that make people angry.

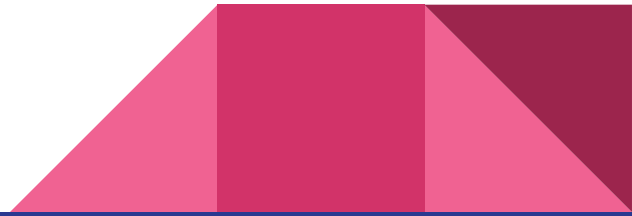
Ongoing threats to emerging financial entities

Cryptocurrency, new-generation remittance companies, and banks in emerging financial markets.

- The companies themselves
- Unscrupulous competitors
- Extortion gangs
- Nation-State Actors

The Entities Themselves

- We are our own worst enemies.
- Not enough companies carry out due diligence.
  - Hardening servers
  - Hardening endpoints
  - Installing security patches
  - Not auditing their code
- No network traffic filtering to prevent egress.
- Sensitive data is not encrypted.
- Having a security policy does NOT mean you are secure.
- Defining security metrics and building pretty dashboards does NOT mean you are secure.
- Compliance is NOT security.

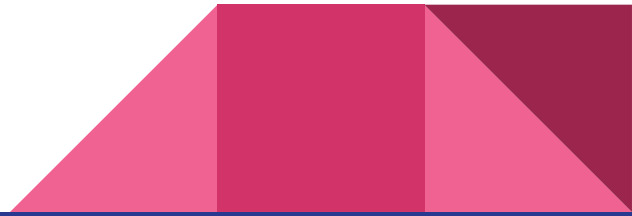


What can be done in-house?

- Set up an orchestration system to centrally manage everything.
  - Chef - https://www.chef.io/
  - Puppet - https://puppetlabs.com/
- Use it to automate the hardening of every system you set up.
- Use it to automate the installation of security patches.
- THEN start building your production and staging infrastructures.
- Use it to centrally manage your workstations.
  - Install patches in a timely manner. Boxkillers are rare. 0-days are not.
  - Antivirus software
  - Anti-malware software
- If you want to do business with multinational banks, you have to play the game like multinational banks.

Unscrupulous Competitors

- Every piece of information a company maintains is a potential target.
- Every piece of information you publish can be used to figure out the internal structure of a company.
- Every piece of information gives competitors a potential advantage.
- Leaked information can cost you money, contracts, reputation and connections.
- Surveillance malware is available on the open market and can be used to gather actionable business intelligence.
  - Skype credentials, text, audio, and video conferencing monitoring
  - Keyloggers recording credentials and discussions
  - Remote Access Tools
- Attribution of attacks is hard. If it was a competitor, chances are you couldn't prove it, anyway.



What to do?

- Watch what you publish. Ask yourself if it could be used against you.
  - Don't put your team's names, pictures, and bios on the corporate website. They make social engineering attacks significantly easier.
- Harden endpoints to make them more difficult to exploit.
- Don’t announce partnerships until the deal is signed. It will make it harder for an attacker to exploit trust relationships between personnel in aligned companies.
- Be wary of documents in email. It's very easy to hide surveillance malware in documents.
- Configure egress traffic filtering to make it difficult for malware to exfiltrate information.
- Set up multi-factor authentication on all third party services.

Extortionists

- Extortion-as-business-model has just come to the financial industry.
- DD4BC and Armada Collective
- More on the way, now that profitability of the practice has been proven.
- Modus Operandi
  - Reconnaissance on targets' infrastructures
  - Rent botnets from other gangs
    - 550 up to 775 gigabits per second spotted in the field this year.
    - Several DDoSes spiked to 1 terabit per second briefly.
  - DDoS weak points of infrastructures for a short time to show they mean business
  - Demand ransom in BTC to stop
- So far, ransoms appear to be sized to how much they think the target can pay.
- Increase the ransom and the size of the DDoS if the target doesn't pay.

Now what?

- Ask legal counsel what you should do!
- Decide how much degradation of service you are willing to accept.
- Only multi-layer response plans are going to help.
- Have a plan in place to set up additional infrastructure to spread out impact
  - Use your orchestration system to do this. You set one up earlier, didn't you?
- Reconfigure the attacked parts of your infrastructure to help mitigate the attacks using your orchestration system.
  - Network zone firewalls to absorb some of the traffic
  - Host-based firewalls to absorb more
  - Application-layer proxies elsewhere in your production network to absorb more traffic
  - Aggressive rate limiting in the applications
- Have agreements in place with your hosting providers so they'll be able to help.
- Have contracts in place with DDoS mitigation services to help.

State Level Actors

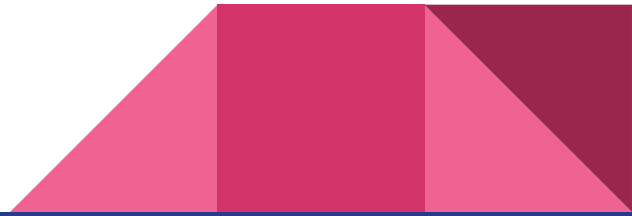
- United States
  - NSA
- United Kingdom
  - GCHQ
- Russia
  - FSB
- China
  - Unit 61398

Why?

- Good question.
- Because they want in.
- Because they think they can gather useful intelligence.
- Strategic clandestine access might be useful later.
- Tactical purposes, to achieve specific, in-theater short term goals.
- Potentially economic and industrial espionage.

How?

- 0-day vulnerabilities
- Custom hardware implants
  - Generally, only if you've done something to draw their attention.
- Privileged access to network backbones
  - This should be assumed in your threat model.
- Custom malware
  - Just about every attacker has access to this, though.
- Physical attacks
  - Generally, only if you've done something to REALLY draw their attention.
- National Security Letters (or the local equivalent)



Mitigation

- There isn’t a whole lot that can be done. We’re all outclassed.
- If you think you're paranoid enough, you're not paranoid enough.
- Don't give them a reason to target you specifically.
  - Follow applicable laws to keep them from deciding you’re a threat.
- Decide how much data needs to be kept online.
  - Encrypted or not?
- Keep the most sensitive operations and data offline.
  - Key generation on physically isolated machines.
  - Most sensitive data should be split up into multiple pieces before it leaves isolation.
  - Kept on encrypted storage media which is kept offline as much as possible.
  - Move most sensitive data via offline means.
    - Personal visits
    - Bonded couriers
    - Generation of secrets/keys on-site

Comments or questions?

How to contact me

- E-mail
  - drwho@virtadpt.net
    - PGP: 0x807B17C1 / 7960 1CDC 85C9 0B63 8D9F DD89 3BD8 FF2B 807B 17C1
  - bryce@ripple.com
    - PGP: 0xA4364248 / A177 A590 2869 32AC E2E1 946A FAD8 98D6 A436 4248
- Web
  - http://drwho.virtadpt.net/
- Twitter
  - @virtadpt
- Facebook
  - virtual.adept

Thank you!
I hope you enjoyed the conference!