Nord VPN Breach

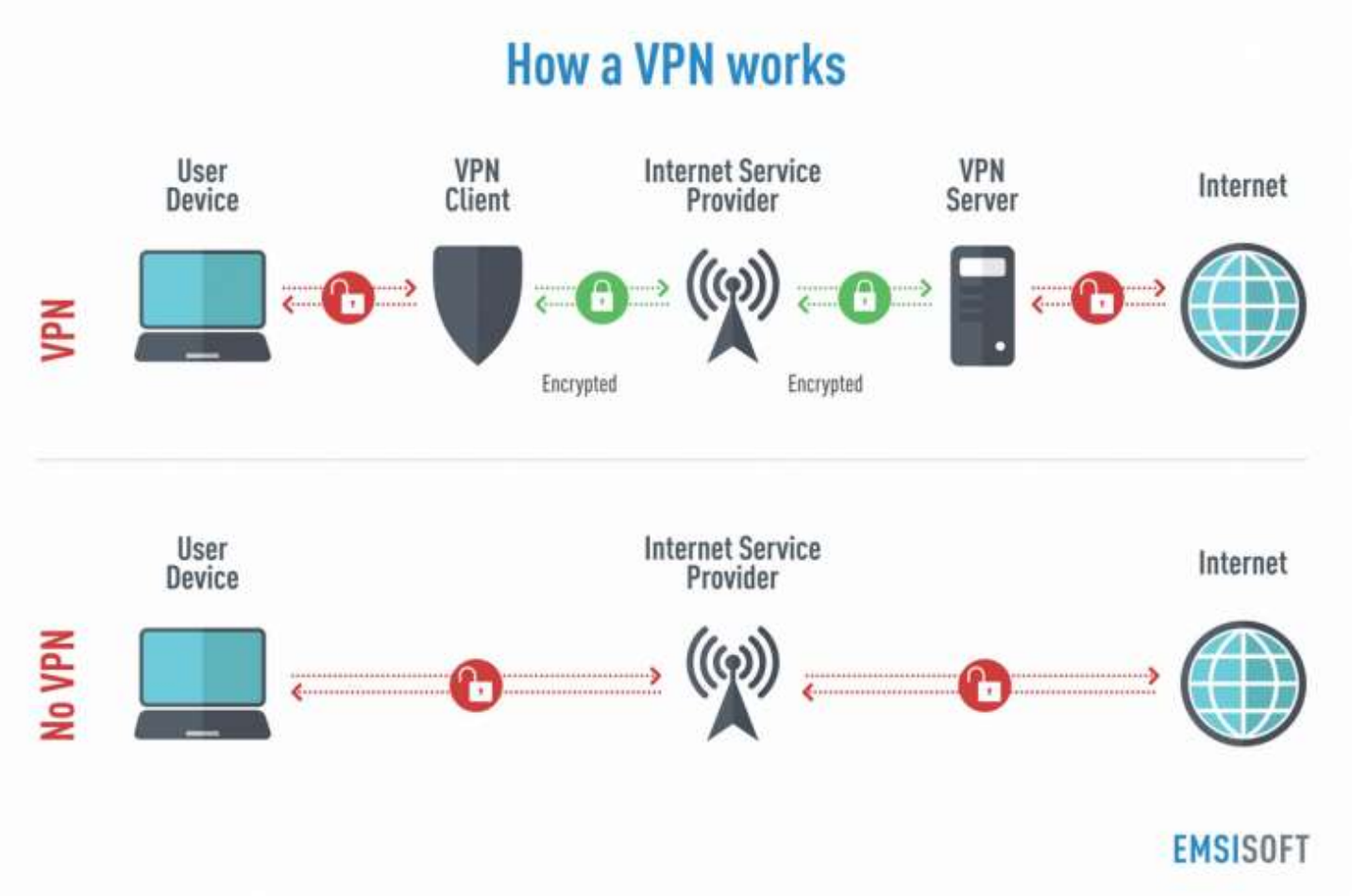
Nathan Satterfield

Who is NordVPN

- NordVPN is a personal virtual private network service provider
- Applications are available for Windows, macOS, Linux, Android and iOS, Android TV Manual setup is available for wireless routers, NAS devices and other platforms
- Was release in 2012

What is a VPN

Here’s where a VPN comes into play. It redirects your internet traffic through a specially configured remote server. This way, the VPN hides your IP address and encrypts all the data you send or receive. The encrypted data looks like gibberish to anyone who intercepts it — it is impossible to read.


How a VPN works
VPN
User Device
VPN Client
Internet Service Provider
VPN Server
Internet
Encrypted
Encrypted
No VPN
User Device
Internet Service Provider
Internet
EMSISOFT

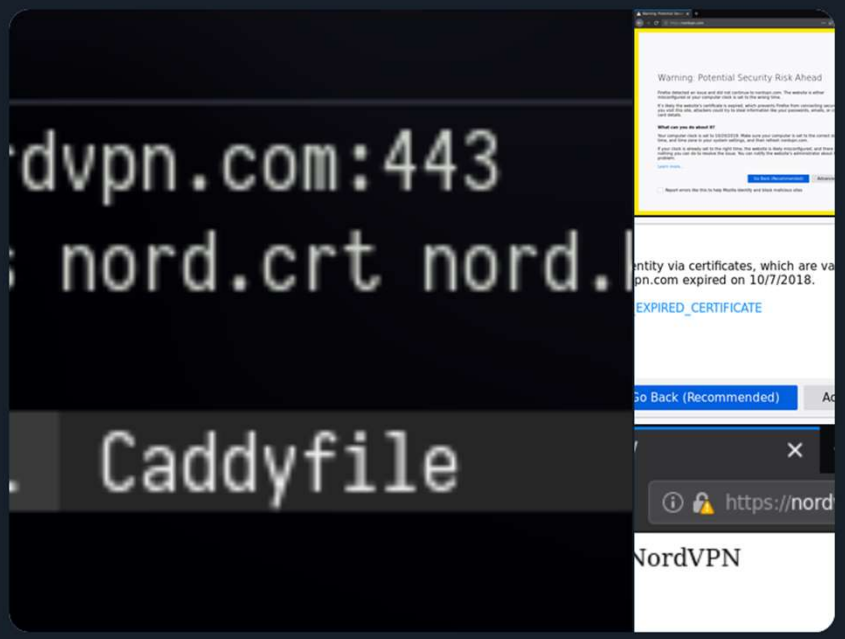
Nord VPN Breach

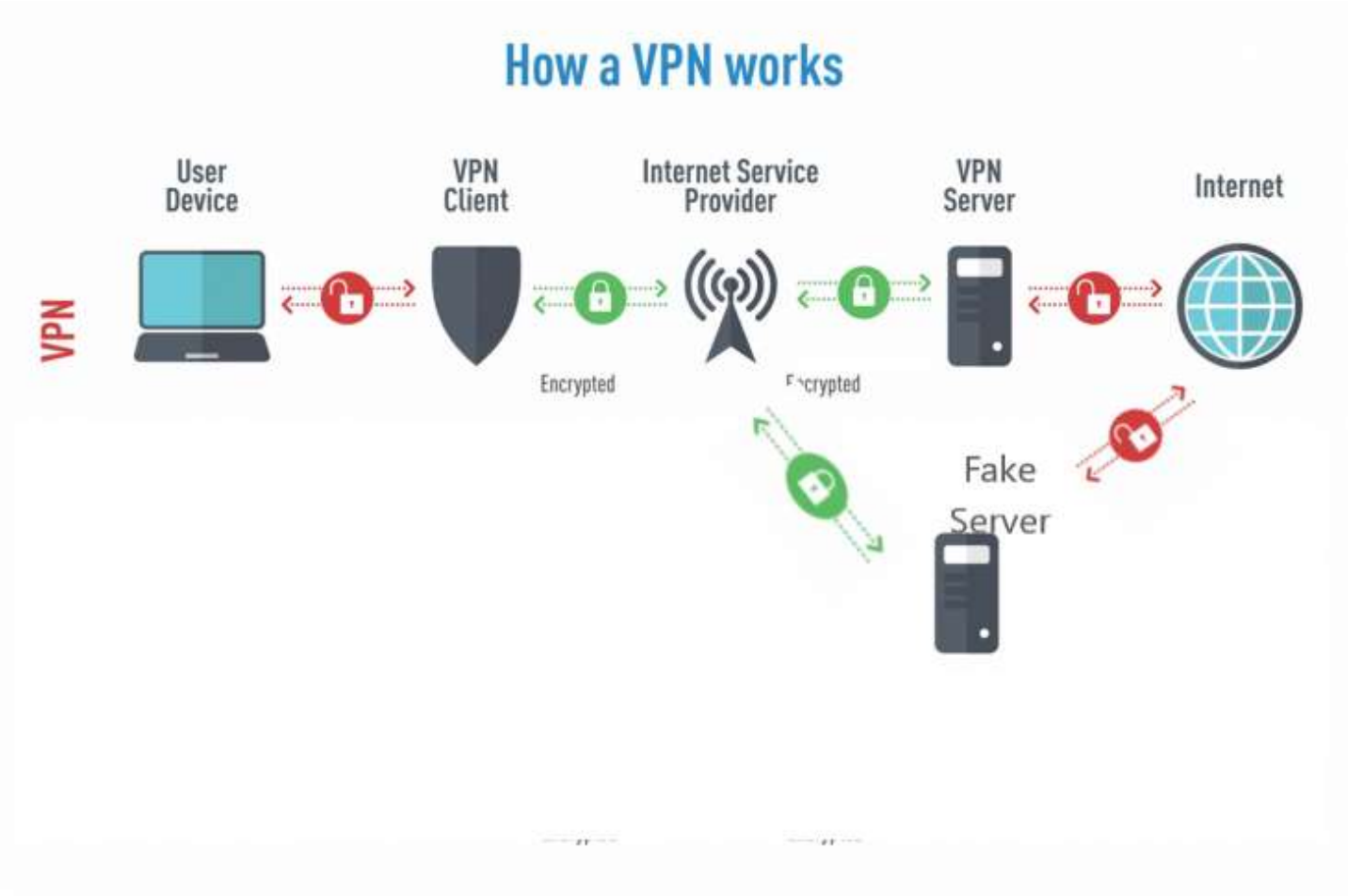
- Happened in March 2018
- Happened at a data center in Finland
- Nord claims that the data center did not disclose the hack
- Techs at the Nord found an account of the data breach a few months ago, which led to a security audit which ended in Nord canceling their contract with the data center

How It Happened

- The attacker gained access by exploiting an insecure remote management system left by the data center provider
- With a properly configured firewall or removing this remote management software this breach could have been avoided

So apparently NordVPN was compromised at some point. Their (expired) private keys have been leaked, meaning anyone can just set up a server with those keys...




How a VPN works
VPN
User Device
VPN Client
Internet Service Provider
VPN Server
Internet
Encrypted
Fake Server

What damage did it cause?

- By waiting for over a year after the breach occurred to make a statement they lost a lot of trust

How could it be prevented?

- More intense security auditing of third party servers
- Nord previously did not encrypt their sever hard drives

What Nord is doing in the future

- Partnering with cybersecurity consulting firms
- This firm will assist in penatration testing
- Intrusion handling
- Vendor risk assessment
- Source code analysis
- Setting the groundwork for a full-scale third-party independent security audit in 2020.

What Nord is doing in the future

- Vendor security assessment and higher security standards
- Diskless RAM servers which will allow Nord to create a centrally controlled network where nothing is stored locally Everything they need to run will be provided by NordVPN’s secure central infrastructure

Links

- https://www.youtube.com/watch?v=-SINytnyOdM
- https://nordvpn.com/blog/security-plan/
- https://twitter.com/hexdefined/status/1185864801261477891