ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

CERT Specialist Journey

(ISC)2 “Show me the way”, 30 March 2021

Martijn van der Heide, ThaiCERT Specialist
Electronic Transactions Development Agency, Thailand

Simpler times: 1996

Internet for consumers was just getting started in The Netherlands.

There were 3 ISPs, I worked for one of them as the only admin (imagine that now!)

- ❑ Server infrastructure was 5 desktops (Sun Sparkstations)…
- ❑ Around 30,000 customers.
- ❑ Dial-in only, so speeds measured in kbps.
- ❑ Total upstream for the entire ISP: 2 Mbps.
- ❑ All tech could be understood completely.

Technical people like to play

- Not much to do yet on the Internet, limited reach of social media (mostly 1-on-1, e-mail, ICQ, AOL instant messenger).
- Almost only technical people were customers.
- Forum = USENET (newsgroups).

So one day in 1996, a thread started in the newsgroups:

Can we crash the ISP servers together?

Indeed they could. At 20:00 that night, they launched a DDoS on the POP3 service and e-mail went down.

Fix quickly

They announced to do this fun thing again the next evening…

My management asked if this could be stopped. So I rewrote the POP3 server to add connection rate limiting (max 2 connections per IP address).

- This didn't exist yet, so I designed and wrote it from scratch in 1 day.

New job at Royal Dutch Telecom

Move from consumer ISP to business ISP.

- ❑ At that time, everything was clear text, SSL did not exist yet.
- ❑ No IDS, no Firewalls, not much in the way of security at all.
- ❑ Talk to customers, see what they need and how we can help.

Let’s set up a security team!

- ❑ Organize training, become a trainer too.
- ❑ In 2002 this was restarted as a formal CERT (KPN-CERT).

Rapid growth

- ❑ IT landscape growing to several hundred tools at each organization (you can't understand everything about all of them, plus keeping them up-to-date is hard).
- ❑ Increasing bandwidth, more sharing, hacking tools can be downloaded for free.

We needed national cooperation, share threat intelligence and help/learn from each other.

- Incident handlers group established in 2004.
- Mailing-list and physical meetings once a month.
- Soon joined by banks, hospitals and industrial sector.

Patching

Patching, or the lack thereof, is a big problem.

- ❑ Patching often causes downtime for reboots and may break applications, so this requires thorough testing first, which takes time.
- ❑ Many vulnerable systems worldwide.

And if you do always patch? You can get hit by supply-chain attacks such as **NotPetya** and **SolarWinds Orion**.

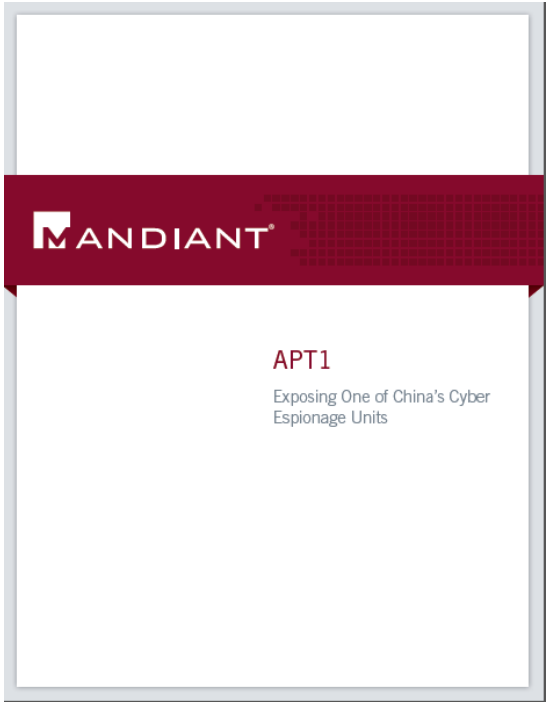
APTs

Reports about sophisticated attacks were published by security researchers. This kind of attack was given a name by the US Air Force: Advanced Persistent Threat (APT).

- Only 1 per year or so – now daily.

APT1, or Comment Crew, was active since 2006, also in our region, and were arrested and jailed as a result of the investigation.

The first APT attack has since been traced back to 1996: **Moonlight Maze**, by **Turla**.



Thailand (OSINT)

Thailand has been a target for APTs since at least 2007

- **GhostNet** (China) – Ministry of foreign affairs, ASEAN (Association of Southeast Asian Nations) Secretariat and various others.
  - Spying for anything related to Tibet.
- **Dark Caracal** (Lebanon) – Military personnel, enterprises, medical professionals, activists, journalists, lawyers and educational institutions.
  - Hundreds of gigabytes of exfiltrated data, in 21+ countries, across thousands of victims. Stolen data includes enterprise intellectual property and personally identifiable information.

2007	2
2009	2
2010	5
2011	1
2012	1
2013	1
2014	3
2015	3
2016	4
2017	3
2018	5
2019	6
2020	3
Total	**39**

Thailand (OSINT)

- Malware and operations only seen in Thailand:
  - **Bookworm** (2015, China) – Defense and government.
    - Spying.
  - **Lazarus Group** (2014, North Korea)
    - The legendary breach of Sony Pictures Entertainment was performed from a hotel in Bangkok and the exfiltrated data sent to a hacked server also in Bangkok.
- Sometimes not aimed at Thailand
  - Spying on specific groups, such as Americans or Iranians, or minorities such as Uyghurs or Tibetans, who happen to be in Thailand.
- More information on APTs: https://apt.thaicert.or.th

Trends

- ❑ Move to always online, everything online, internet activities growing throughout the country.
  - This is why our agency is called Electronic Transactions Development Agency.
- ❑ COVID-19 massively accelerated this with WFH.
  - Change of security perimeter.
  - COVID-19 related phishing, scams and attacks.
- ❑ New laws, including to protect CII.
- ❑ We need many more security people!

Do it together

- ❑ Work together and learn from each other. This way, I have worked with National CERTs, Law Enforcement, the military and other sectors.
  - They may have some specific tools for their sector, but otherwise face exactly the same IT security challenges.
- ❑ Join forums such as FIRST or the COVID-19 CTI League.
  - Be active as much as you can. Work on your reputation, as security is trust based.
  - Physical meetings are best when possible, building trust does not work well at all online.

Thank You

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

WWW.ETDA.OR.TH : ETDA THAILAND
ETDA