National Cyber Security Centre
a part of GCHQ

Telecoms Breaches & Attacks (or how advanced is APT?)

Adrian Moss – NCSC Deputy Telecoms Lead

16th November 2021

National Cyber Security Centre
a part of GCHQ

Government Health Warnings

Government Documents can be boring…
All comments are mine; not official policy
Be warned, I can talk for England

National Cyber Security Centre
a part of GCHQ

Plenty of "public" attacks…

- Florida Water
- Ukraine Power
- French TV
- USA Pipeline

National Cyber Security Centre
a part of GCHQ

Advanced Persistent Threat

Phrase “APT” well known in security
- Used to classify threat groups
- APT1 – specific Chinese group
- APT28 – Fancy Bear (Russia)
- APT37 – North Korea
- APT40 – “Periscope”, more recent Chine

Visions similar to attached

Conjures up “invincible”

“It’s not our fault, it was an APT”

National Cyber Security Centre
a part of GCHQ

Advanced Persistent Threat?

Dr Levy translation "**A**dequate **P**ernicious **T**oerags"

Hostile Threat actors **can** use Advanced tools…

- But why use a Cruise Missile at ~$7M a pop when a rifle (35 cents for the bullet and re-usable) will do the same?

And there are millions of "cyber vandals"

- WannaCry wasn't "Advanced" and didn't target NHS
- NHS (and others) were vulnerable
- Security researcher "accidentally" launched WC2
  - "I mean it's not very well designed, look, even I can improve … oh"

National Cyber Security Centre
a part of GCHQ

Advanced? Persistent Threat

- Florida Water
  - Commercial (and insecure) remote desktop access
- Ukraine Power
  - Targeted – but not “Advanced”
  - “Phishing” email
- French TV
  - Open ports & default passwords – modify config files (and wipe backup)
- USA Pipeline
  - Remote access as engineers “working at home”

National Cyber Security Centre
a part of GCHQ

~~APT~~ (What should we do?)

- That's where the TSR's come in! Try and stop the **easy** stuff
- Passwords
  - Reset to complex before connecting to network (and check old one has gone)
  - NCSC guidance – Change is not always better
  - 2FA will help (and **any** 2FA is better than none)

National Cyber Security Centre
a part of GCHQ

~~APT~~ (What should we do?)

- Patching
  - Keep things (fairly) up to date
- Users / Machines
  - Enough rights to do their job, and no more
  - If checking Gmail from Admin Account – you deserve it
- Segregated networks (Data, Management, Office)
- Ports and Services
  - If not in use, close down

National Cyber Security Centre
a part of GCHQ

Real APT's (that you may encounter)

- In and out like a thief in the night
- They don't want you to know they were ever there…
- Meticulous long term planning by the bad guys…
- … and entering by the one route you thought was safe
- For example Solarwinds…

National Cyber Security Centre
a part of GCHQ

Real APT's – SOLARWINDS

- Attack a supplier – delicately modify their code
- Which in turn attacks **your** supplier (say FireEye)
- And pick a vector which ends up with an insecure security product
  - What better attack than through a trusted security service?

SOLARWINDS HACK

SolarWinds attack explained: And why it was so hard to detect

A group believed to be Russia's Cozy Bear gained access to government and other systems through a compromised update to SolarWinds' Orion software. Most organizations aren't prepared for this sort of software supply chain attack.

By Lucian Constantin

CSO Senior Writer, CSO | 15 DECEMBER 2020 11:44 GMT

National Cyber Security Centre
a part of GCHQ

(Feel I should mention NICC)

NICC and NCSC are complimentary, not competitive

- NCSC view of SIP – “If you’re not using it, close the SIP port”
- NICC view of SIP – “if you’re going to use it, here’s how”
- NCSC view of SIP – “Here’s some guidance on passwords”
- NICC view of SIP – “Here’s some guidance on packet retries”
- Alt view of SIP- “Did you know ‘INVITE’ goes weird with товарищ”?

National Cyber Security Centre
a part of GCHQ

Questions ?

Adrian.M@ncsc.gov.uk

NICC Open Forum – 16th November 2021