Trends in Ransomware

Gavin Willis NCSC

Technical trends

- Growth. All the signs over the last few years suggest that there will be more and more ransomware brands.
- Ransomware as a service. Costs varying between $50 and $400
- Criminal groups having different preferences for cryptocurrencies. Some are aware of transaction fees and degree of anonymization.
- Delivery methods. Email remains the most common delivery method. We are also aware of automated brute force attacks to drop ransomware onto critical servers.
- Targeted attacks. Difficult to generalize, we feel that most attacks are not targeted but some sectors are more vulnerable than others due to the use of old technology. Even if an attack is targeted, control may soon break down.

Policy trends

- High profile. Ransomware has been a fact of life in the technical community, Wannacry brought ransomware to the attention of the highest levels of government in the UK. The UK NHS is a sensitive political subject in its own right, the impact of Wannacry was magnified by that political sensitivity. The NCSC and its assistance and published guidance was central to the response. Rarely have we been so central to the government

- Scrutiny. After the impact, there was a very serious look at what happened and what could have been done better. In particular, the National Audit Office, a very thorough and unemotional body examined how Wannacry affected the NHS. It published a detailed report.

- A UK minister made a public attribution of the Wannacry attack

Communications

- NCSC published or refreshed its guidance several times during the WannaCry incident.

- Tailored messages for different communities.

- But consistency across them all, including statements by senior ministers.

Guidance updates

- Wannacry ransomware:guidance updates
- Ransomware: Wannacry guidance for enterprise administators
- Ransomware:WannaCry guidance for home users and small businesses
- Ransomware:Latest NCSC Guidance
- All were wrapped up into ‘Mitigating Malware’

Policy trends

- **Obsolete Platforms Security Guidance**
- In the real world, we know that not everybody can migrate from obsolete systems.
- We do not offer a way to achieve risk-free use of obsolete products
- We offer advice on how to reduce the risks

Wannacry and the NHS

- “The WannaCry cyber attack had potentially serious implications for the NHS and its ability to provide care to patients. It was a relatively unsophisticated attack and could have been prevented by the NHS following basic IT security best practice. There are more sophisticated cyber threats out there than WannaCry so the Department and the NHS need to get their act together to ensure the NHS is better protected against future attacks.”

Amyas Morse, head of the National Audit Office, 27 October 2017

Wannacry and the NHS

- 1.9 NHS organisations did not report any cases of harm to patients or of data being compromised or stolen. If the WannaCry ransomware attack had led to any patient harm or loss of data then NHS England told us that it would expect trusts to report cases through existing reporting channels, such as reporting data loss direct to the Information Commissioner’s Office (ICO) in line with existing policy and guidance on information governance. NHS Digital also told us that analysis of the WannaCry ransomware suggested that the cyber attack was not aimed at accessing or stealing data, although it does not know for certain that this is the case.

Wannacry attribution

Foreign Office Minister for Cyber, Lord Ahmad said:

The UK’s National Cyber Security Centre assesses it is highly likely that North Korean actors known as the Lazarus Group were behind the WannaCry ransomware campaign – one of the most significant to hit the UK in terms of scale and disruption.

NCSC Guidance -openly available www.ncsc.gov.uk

- **Mitigating Malware** –ransomware is a class of malware, and the broad guidance for mitigating malware applies.
- Much of the guidance is ‘classic’. Use supported operating systems, patch promptly, segment networks, back important files up in an appropriate manner, use AV

Don’t pay a ransom

- there is no guarantee that you will get access to your data/device
- your computer will still be infected unless you complete extensive clean-up activities
- attackers may assume that you would be open to paying ransoms in the future
- you will be funding criminal groups

Thank You

Further information is available from

UK National Cyber Security Centre

www.ncsc.gov.uk