CareCERT Advisory

NHS Digital is aware of a ransomware attack affecting organisations in Europe however we can confirm that this is not known to have affected any NHS system. We ask that health organisations remain vigilant but this broadcast is to reassure organisations of the status of the incident and that there is no specific action to take.

NHS Digital issued guidance relating to an old exploit in March 2017 (see below) which should be followed and there is no need to switch any systems off or take any additional action as a precaution. Updated antivirus software will prevent systems from being impacted.

If you're an IT manager and you believe your organisation is affected and require support or further information, please contact NHS Digital on carecert@nhsdigital.nhs.uk or by calling 0800 085 6653.

PetrWrap Ransomware (CC-1287)

Published to the CareCERT Information Sharing Portal 22/03/2017

A new ransomware has been identified called PetrWrap that is based on Petya, a ransomware family offered as a service (RaaS).

The authors of Petya created a number of mechanisms to prevent other attackers using their code without paying for the service. These obstacles have been mitigated by the authors suggesting that they possess advanced technical capability.

PetrWrap is distributed after first penetrating a target network through unprotected RDP access. After gaining a foothold on the network, the ransomware uses PsExec to execute copies of itself on target machines.

Other tools such as Mimikatz are used in order to obtain the necessary account credentials for privilege escalation in order to traverse the target network.

After a successful attack, PetrWrap displays a ransom note directing the affected user to a payment website.

Affected Platforms

Microsoft Windows – all versions

Remediation

If a computer on your network becomes infected with Ransomware report it to your

AV vendor for analysis and patching.

Typically Ransomware will begin encrypting local machine files, mapped network drives and files on any shared network storage the logged-in user has permission to access. For system administration accounts this may include backup storage locations.

To avoid becoming infected with ransomware, ensure that:

- A robust program of education and awareness training is delivered to users to ensure they don’t open attachments or follow links within unsolicited emails.
- All operating systems, antivirus and other security products are kept up to date.
- All day to day computer activities such as email and internet are performed using non-administrative accounts and that permissions are always assigned on the basis of least privilege.
- Your organisation adopts a holistic all round approach to Cyber Security as advocated by the 10 Steps To Cyber Security.

Identifying the source of infection:

- Identifying the infected machine and unplugging / disconnecting or quarantining it from the network is essential to damage limitation.
- Users should immediately report infections to their IT support provider, disconnect their network cable and power the computer down.
- File auditing should be enabled and file server logs should be monitored to detect signs of unauthorised encryption and allow the source of encryption to be identified (i.e. the infected PC).

To limit the damage of ransomware and enable recovery:

- All critical data must be backed up, and these backups must be sufficiently protected/kept out of reach of ransomware.
- Multiple backups should be created including at least one off-network backup (e.g. to tape).
- The only guaranteed way to recover from a ransomware infection is to restore all affected files from their most recent backup.