Ransomware as a Service (RaaS)

Police Scotland Cybercrime Harm Prevention Team.
05.10.2023.

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Ransomware as a Service (RaaS)

Organisations and individuals have been getting better at preparing, responding to and recovering from cyberattacks. At the same time however, cyber criminals are also improving their methods of cyberattack.

Cyber criminals crave money as well as information but also the desire to cause widespread disruption and panic to the organisation or individuals they attack. These attacks mostly carry threats of publicising exfiltrated data or placing pressure on their victims to respond within short deadlines to particular demands.

The impact of these attacks will be immediate and particularly when organisations are unprepared, there are often long term effects. For some, recovery is often lengthy and costly, if at all possible in some cases. In the case of the victim being an individual, it can be an extremely anxious time with perhaps not knowing how to get support.

The message we want to bring to the organisational environment is that Cyber resilience is key to operational resilience and business continuity and the same applies to individuals, so it is vitally important that;

1. **People recognise the cyber risks and are well prepared to manage them.**
2. **Businesses and organisations recognise the cyber risks and are well prepared to manage them.**
3. **Digital public services are secure and cyber resilient.**
4. **National cyber incident response arrangements are effective.**

In terms of cyber risks, Ransomware as a Service (RaaS) can be regarded as the monetisation of cyber vulnerabilities. Indeed this particular attack method has, year on year, been the biggest development in cybercrime since the NCSC (National Cyber Security Centre) published its 2017 report on online criminal activity.

Most ransomware incidents are not sophisticated attacks, but are usually the result of poor cyber hygiene. That’s not to say that victims did not take cyber security seriously.

Poor cyber hygiene can include not updating devices with the latest software updates, unpatched devices, poor password protection on devices and accounts, or lack of 2 step verification (2sv).

Introducing these elements in your cyber security, whilst not a complete guarantee, would interrupt the majority of ransomware attacks. 2sv in particular is often not in place, which is in itself an enabler for the Cybercriminal to be successful against organisations and individuals.

Lastly and just as important, back up your data. We take for granted that we will always have access to our data however, Ransomware malware will lock down your devices and access to your data. Having a current and virus scanned back up of your data will be major part of the recovery from a Ransomware attack – make this one of the first changes you make.

The most effective response is prevention and that aspect of being prepared. We can strive to achieve this by investing in staff and individual awareness which in turn improves Cyber Resilience, Operational Resilience, Business Continuity and of course recovery.

From an organisations perspective, staff play a hugely important additional role - it should be recognised they have an increased accountability and responsibility towards organisational security in the online space.

Cyber security is not solely the responsibility of your IT team, so we need to have a collective resilient capacity to respond to cyberattacks. Being able therefore to detect, deter, disrupt and recover from cyberattacks are key objectives which awareness and training will bring.

To assist and further support you in being more cyber resilient, we have included the links to guidance from our colleagues at the NCSC

A guide to ransomware - NCSC.GOV.UK

Where to report a cyber incident - GOV.UK (signpost-cyber-incident.service.gov.uk)

Password managers: using browsers and apps to safely store... - NCSC.GOV.UK

Install the latest software and app updates - NCSC.GOV.UK

Turn on 2-step verification (2SV) - NCSC.GOV.UK

Backing up your data - NCSC.GOV.UK

If you have been a victim of crime, and it is not an ongoing emergency, you can report this to Police Scotland on 101.

This alert was sent out for your information by
Police Scotland Cybercrime Harm Prevention Team -
All information was correct at time of distribution. 05/10/2023.