Ransomware:

A 5 Step Plan to Protecting Your Business

Five Steps to Protect Your Business from Ransomware

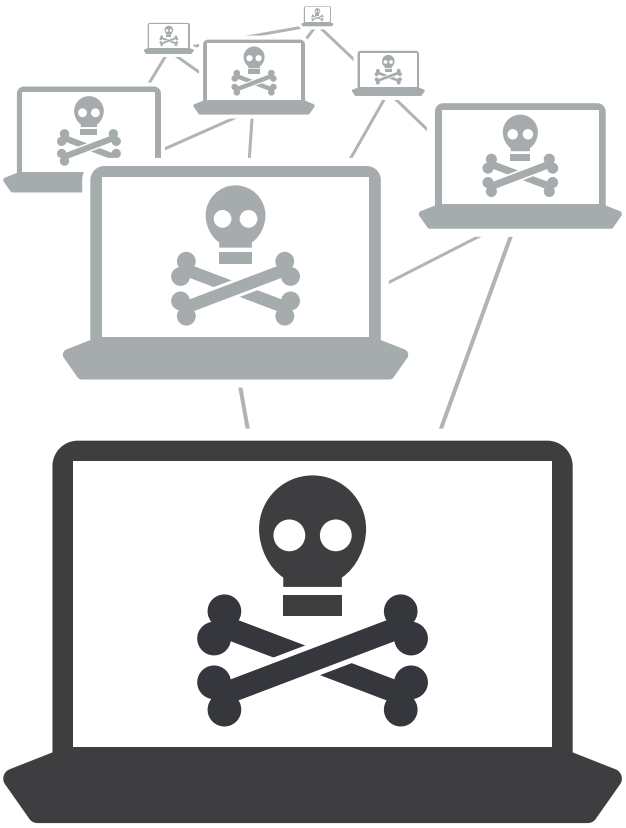
Hundreds of organisations across more than 100 countries have recently suffered as part of a ransomware epidemic that has spread across their infrastructures like wildfire. On the back of the leaked NSA 'Eternal Blue' worm, WannaCrypt0r ransomware claimed more than 200,000 endpoint scalps and was only shut down through the inadvertent actions of a security researcher.

But ransomware attacks will inevitably return.

Irrespective of your standpoint on paying criminals to get your data back, ransomware has to be one of the most heart-stopping things that can happen to an IT manager. Whilst the ransom demanded as part of WannaCrypt0r was relatively low (around $300 in bitcoins per infected host), is it a smart move to trust a criminal to hold up their end of the bargain?

The bad news, as is the case with much of security, is prevention beats cure. Post event is the worst time for organisations to try and get on top of things; the attacker is in the driving seat, staff are stressed to the limits of their capacity, jobs may be at risk and the only option left is often a risky, and potentially ineffective, one to exchange cash with the criminals.

To reduce the threat of WannaCrypt0r and other ransomware attacks, here are five key steps that your organisation can take.

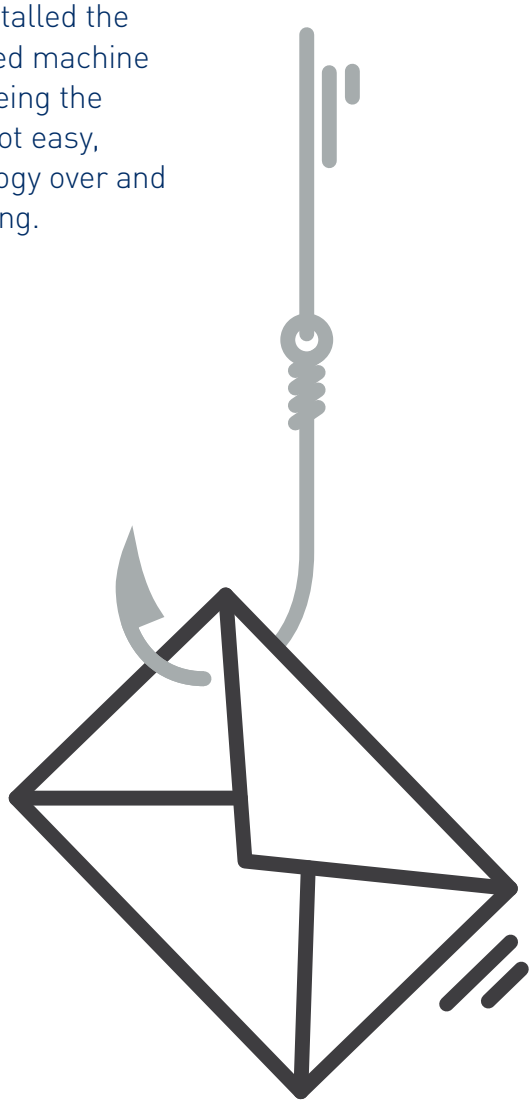


1

Teach your staff to know a phish when they see it

Most ransomware, including WannaCrypt0r, starts with phishing emails. In the WannaCrypt0r instance, the emails seemingly came from FedEx and DHL advising staff about missed deliveries, encouraging them to open files or click on links that installed the ransomware. This creates an entry point into the infected machine and what the user has access to, with network drives being the prized scalp. Knowing how to spot a phishing email is not easy, especially for staff who don't know much about technology over and above using the internet for social media or web browsing.

Furthermore, many organisations don't train their staff on how to spot unsolicited and potentially dangerous emails. People working in IT roles shouldn't expect staff to know what malware is versus what it isn't. Well-formed phishing emails are crafted to tap into human instincts and drivers. The responsibility lies with the IT department, therefore, to ensure that all staff are trained to spot and delete the emails.



2

Use what you have to stop the bad stuff getting in

Most organisations have access to a plethora of mitigation capabilities that they don't get the most out of, either through old software levels, poor configuration or a lack of understanding that certain mechanisms exist in the first place.

Looking specifically at the patching of the WannaCrypt0r outbreak, much was made of the MS17-010 patch that thousands of organisations apparently failed to deploy. However, it's worth noting that endpoint systems were still vulnerable to the ransomware delivered, the 'Eternal Blue' vulnerability merely allowed it to spread through networks like wildfire.

Patching is important of course, but there are many instances where running the latest patch is not viable (i.e. due to a piece of custom software running on the server that won't work if you patch the server). It's advisable to patch everything that your organisation can before ensuring the remaining bits are protected at the network layer, this is done by placing them behind security appliances capable of mitigating the threat.

Whilst all ransomware doesn't manifest in exactly the same way, most email-borne malware doesn't contain the complete executable. What usually happens is the initial infection, like a pathfinder, gets its teeth into an endpoint before contacting a command and control server - often via an encrypted tunnel - to download the ransomware payload.

If you have a good intrusion prevention system (IPS), or an IPS engine in your firewalls, that sits in line with your trusted and untrusted domains, along with updated signatures, then your organisation should be able to spot the command and control sessions being established. This will enable you to block them and identify the infected machines for quarantine as part of the deal.

If you don't have IPS or the necessary budget, domain reputation scoring can also be used as a means of detecting and blocking domains generated via the Mersenne Twister, or similar algorithms used to generate random domain names. Up-to-date endpoint protection also plays an important part, creating another layer through 'defence-in-depth' that gives all but the very earliest infections a good chance of being detected and stopped. However, just like with Windows, it's important to ensure IPS and endpoint antivirus/anti-malware signatures are included as part of your pathing schedule

3

Segment the network

Given that the threat of ransomware is nothing new, WannaCrypt0r emphasised the need for organisations to take a closer look at their internal network security. The fact that WannaCrypt0r could so effectively compromise other devices, moving laterally around the network on the back of the NSA-developed SMBv1 exploit, proves how desperately outdated the notion of trusted and untrusted domains with a firewall positioned between them is. Whilst the internet is still very much untrusted, so too are the internal segments of the network.

Most networks provide inter-VLAN (virtual LAN) routing that is completely open, which meant organisations that were affected by WannaCrypt0r had no network-based safeguards to restrict the internal propagation of the ransomware.

A 'Zero Trust' approach takes the intelligence found in next-generation firewalls (NGFW) and IPS, and places them in between either all, or a sub-set of, VLANs, to enforce policies based on what should and shouldn't be allowed to flow between. Given that most IPS and NGFW devices had signatures to identify and contain MS17-010 exploits, this approach would have dramatically reduced the spread of WannaCrypt0r.

As this requires architectural change and potentially some investment, this is a big step to take and is arguably one of the most resource-hungry methods of improving security posture. However, it's advisable to consider when wanting to protect the file shares, data and applications that most organisations depend on.

4

Make yourself less prone to desperation by creating backups

If your data has been encrypted by a merciless gang of cybercriminals and you don't have another copy, your options are somewhat reduced. However, if you have a backup of your data, it is much easier to close your borders to the internet, quarantine infected workstations and then re-instate your last backup for user access, a state that makes dealing with the cyberattack a little easier to deal with. Be mindful of the integrity of these backups though, malware can lie dormant for significant periods of time and might manifest in the backup as well as the live operation environment.

It's important to remember that ransomware attacks target availability, almost like a Denial of Service attack (DoS). Part of any risk assessment activity is to help visualise what loss of availability might look like. Having a regular, well-documented and well-tested backup strategy is a vital element in delivering a safety net against ransomware and many other types of attack.

5

Create a plan for when the worst happens

Unfortunately, the only way to truly protect your organisation and ensure job longevity is to assume that one of these attacks will get through. Knowing what to do and when to do it can have a significant impact on your ability to stem the effectiveness of an infection, as well as giving you the headspace to deal with things that you just wouldn't have if you were dealing with the nightmare for the first time. Model the best and worst-case impacts of an infection and work through your response strategy, ensuring you have a plan that you can follow to get back to normality.

Like end-user training, planning is a seriously undervalued part of the security cycle. It's advisable to create scenarios, model them, and then test them either in isolated parts or as full-scale 'wargames'. The benefits of doing this are significant. Whether an attack happens to your organisation or not, you will be adequately prepared to respond. You will be able to react in a calmer, more effective fashion, knowing how hard to fight and when to yield; when to invoke the backups; how to remediate systematically; and how to reduce the overall impact on your business

In Conclusion

In an increasingly digital world, there are lots of cyberthreats that go over and above WannaCrypt0r that organisations need to be wary of. The recent WannaCrypt0r attack proved that ransomware is one of the worst threats facing the IT manager/CIO/CISO, and that any investment of time and resource into prevention is well spent.

It's vital that you do the basics consistently well, optimise your threat mitigation estate (get your partners to help you) and plan for the worst-case scenario outcomes. Learn from the woes of others and give yourself as much time as possible to consider the likelihood and impact of a ransomware attack. Test your responses and refine them so that you know exactly what to do and when to do it if the worst comes to pass.

But most importantly: don't count on paying the attackers.

Next Steps

If you want to learn more about how Daisy can help your organisation, contact us at:

☎ 0344 863 3000

✉ enquiry.dcs@daisygroup.com

Or if you're an existing customer, get in touch with your account manager directly.

RW/WP/05/17

we are daisy.

www.daisygroup.com