Tackling the Ransomware Threat - Guidance and Recommendations from the Cisco Security Team

Introduction

In recent weeks, ransomware and malware attacks have been securing the headlines. Local authorities in both Scotland and England have reportedly been targeted, with at least one case resulting in a very public, high profile outage. These attacks have now spread to universities and even to NHS trusts.

While exact details of each attack are still scarce, they once again highlight the operational impact a malware outbreak can have on a local authority. And the headlines support the premise that current approaches to security are failing to provide the required level of cyber protection and resilience, and that further investment is necessary to identify and plug the gaps that are allowing attacks to be successful.

The Cisco UK Security Team has published this short paper to provide advice to our local government customers. It offers guiding principles to underpin security strategy, and makes five specific recommendations for implementation. While it is not possible to offer guarantees, we believe adoption of the principles and implementation of the recommendations will help local authorities to avoid potential attacks and, if they should occur, to identify and effectively mitigate them.

Three Guiding Principles

There are a number of well-respected security guides to help local authorities improve their security posture; CESG's 10-Steps to Cyber Security and the SANS Top 20 Critical Security Controls are just two of them.

Based on the advice contained in these guides, and our own practical experience, we would advance the following guiding principles to underpin a local authority's approach to security:

1. Build User Awareness

It is well recognised that the weakest link in any organisation's security posture is its staff – the user community. That is not to say that staff will behave in a malicious manner, but simply that they are human, and likely to fall for a well-crafted phishing email.

Users, therefore, need regular reminders of the need to exercise caution when opening email attachments or clicking on embedded links in emails. Regular education and awareness is required to make sure security is uppermost in the minds of staff.

2. Assume Breaches Have Taken Place

Whether a local authority will suffer a security breach is no longer a question of if, but of when.

In our experience, many organisations have already been the victims of a breach, but are simply not aware that it has happened. To address this, local authorities should consider the question, "If you knew you were going to be compromised, would you implement security differently?". By considering security in this way, authorities can begin to understand how an attack might propagate after an initial compromise and, importantly, how the attack can be detected once inside the network perimeter.

3. Prioritise Cyber Hygiene

With the industry focus on sophisticated ransomware and malware threats, it is easy to overlook the importance of fundamental security controls, such as regular software patching and rigorous password management.

According to the Verizon 2015 Data Breach Investigations Report, 99.9% of successful attacks exploited vulnerabilities that had been published for over a year on the CVE (Common Vulnerabilities and Exposures) web site.

Whether a local authority will suffer a security breach is no longer a question of if, but of when.

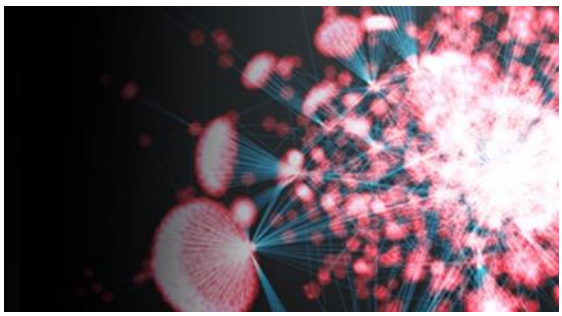
Protection across the Attack Continuum

Many recommended approaches to security focus entirely on the use of defensive technologies to block threats before they can do harm.

However, if this approach is adopted and malware does breach the defences, greater numbers of users will be exposed if there is no monitoring in place to detect the breach and no network segmentation to prevent spread.

Cisco's security strategy is based on an architecture approach that protects and remediates across the entire attack continuum; before, during and after the attack. This approach ensures that, if defensive technologies do not block a threat, additional capability is deployed within the network to quickly identify and contain the malicious activity.

Cisco security technology spans each of the three stages of the attack continuum. It has been proven to help protect against ransomware and malware threats such as those reported recently by local authorities.



Before the Attack

The initial attack vector for ransomware and malware is most often via email.

Phishing emails may not be sophisticated, or highly targeted, but can still be convincing enough to encourage an unsuspecting user to 'click' a link or open an attachment.

Blocking this type of threat requires multiple controls - to look in detail at incoming emails to see how they are constructed, to determine who is sending them, and to inspect their contents (including embedded URLs to see if they link to known malicious sites).

The Cisco Email Security Appliance (ESA) is able to apply these multiple controls, and so is ideal for mitigating potential threats from emails as they attempt to enter a local authority network.

Operation of the ESA is supported by a wealth of data and data analytics from the Cisco TALOS security intelligence and research team. That team utilise a vast cloud-based security intelligence capability that observes and analyses almost 30% of the world's email traffic.

During the Attack

To gain its initial foothold, ransomware and malware will often make use of a dropper program, designed to retrieve and install the malicious executable on the victim's machine.

If email is the attack vector, then the dropper will be part of the attachment that a victim is lured into opening. Once activated, the dropper will initiate an outbound connection to retrieve the malware executable, and this action provides another opportunity to block infection.

Malware executables are very often retrieved from websites that are known to be bad. The Cisco OpenDNS Umbrella solution utilises DNS techniques to prevent the retrieval of malicious executables over any port or protocol - simply by blocking DNS responses associated with malicious domains. The intelligence behind the decision to block DNS responses comes, like with Cisco ESA, from the collection and analysis of over 80 billion DNS queries a day by the Cisco TALOS team. The OpenDNS Umbrella solution uses data mining and advanced classification techniques that result in very rapid identification and blocking of domains with new and emergent threats.

After the Attack

Cisco Network as a Sensor (NaaS) provides full visibility of network activity, through the use of NetFlow behavioural monitoring. Cisco NetFlow captures metadata about every conversation on the network; who is talking to who, over which protocol, and for how long. Once aggregated and analysed, this information can provide insight into normal behaviour. It also allows identification of questionable patterns of activity, such as malware spreading across the network, which might otherwise go unnoticed.

Utilising NetFlow in this way transforms the entire network into a security sensor, offering insight that simply cannot be achieved with traditional security appliances deployed in spot locations. NetFlow is supported on a wide range of standard Cisco Catalyst and Nexus switches, as well as the entire Cisco router portfolio, so NaaS is not, in any way, network topology dependent.

A companion solution, Cisco Network as an Enforcer (NaaE) utilises Cisco TrustSec and the Cisco Identity Services Engine (ISE) to deliver software defined network segmentation. TrustSec uses Security Group Tags (SGTs) to enforce role-based, topology-independent access control. This means that network segmentation can be implemented far more easily than relying on IP address or VLAN based segmentation, and can be automated.

NaaE uses SGTs to respond dynamically to threats. For example, a user may join the network and be allocated a tag associated with their role e.g. finance. The tag is used to enforce agreed access policies – for example the user may only be able to access those services available to members of the finance department. If that users' device is infected with malware and starts to exhibit questionable network behaviour (reported by the NaaS solution), the user tag can be changed dynamically to a 'quarantine' tag. Access control policies could already be pre-defined within the network to limit access for devices with the tag 'quarantine', resulting in the potential malware outbreak being rapidly contained without any manual administrative intervention.

Cisco NetFlow captures metadata about every conversation on the network; who is talking to who, over which protocol, and for how long.

Summary and Recommendations

A successful approach to security requires a local authority to prioritise a number of key actions.

First and foremost, the basics must be taken care of – user education and awareness, and cyber hygiene through patch management and password protection. But secondly, and equally important, is taking an architectural approach to security that spans the full attack continuum.

Local authorities can begin to adopt such an architectural approach by implementing the following five recommendations;

1. **Build a Security Culture** - User education and awareness is a core security principle and fundamental to developing a strong security culture. However, security culture extends beyond just routine security training and should instead be woven in to the day-to-day life of users. Like all things in the world of security, it should be tested and, in the context of ransomware and malware, local authorities should run test phishing campaigns to measure the effectiveness of user education.

   Cisco's own security culture has developed over many years, and is now based on a mature, structured program that operates across the whole business. The Cisco team responsible for the program have shared some of their experience here.

2. **Security as an Architecture** – All too often, security is applied at a project level, or in response to a security incident. This approach can lead to deployment of a multitude of point technologies with limited integration, resulting in gaps in visibility and protection. We recommend that local authorities adopt an architectural approach to security by considering how security controls should be applied across the environment, and how they can function together to mitigate risk. This approach ensures a more integrated and effective security capability that can be better aligned to managing business risk and impact.

3. **Review Network Segmentation** – Most networks are still built with a flat security model. While segmentation may be implemented for operational convenience, there is often only limited security policy enforcement between segments. Lack of policy enforcement between segments allows attacks that breach defensive perimeter technology to easily exploit an initial foothold and propagate across an entire network. Local authorities should review current network segmentation, and explore opportunities to implement strong security policies between segments.

4. **Improve Network Traffic Visibility** – Within the network perimeter, few organisations have a clear insight into patterns of traffic flow. By enabling and capturing NetFlow data, valuable insight can be provided into normal network behaviour, allowing incidents to be rapidly identified and threats to be contained.

5. **Develop Security Operations Capability** –Building and operating a full-time Security Operations Centre is costly, but essential if incidents are to be quickly identified and contained. There is a significant trend towards the use of skilled, third party suppliers to deliver fully managed security operations capability. Local authorities should audit their current operational capability and explore whether it should be augmented by third party resource and expertise.

Contact Cisco

We would be delighted to discuss the contents of this paper with you. Or, take that opportunity to review your wider security needs and the benefits of a defence-in-depth security strategy.

If that is the case, please contact your Cisco account manager, or email the team at lgovuk@cisco.com. And you can find out more about Cisco and Local Government by visiting our UK Local Government web site.

Authors

This paper has been written by the Cisco Local Government and Security teams. The teams have over 20 years' experience of working with local authorities on their technology programmes. Their aim is to work with you to develop secure technology environments which enable efficient and cost-effective business, which support high quality, accessible digital services, and which can provide the foundation for digital cities and communities.

Disclaimer