Tackling the Ransomware Threat

Guidance and Recommendations for Schools and Universities

Introduction

Ransomware and malware attacks have been capturing recent headlines. Local governments and organizations in Scotland, the United States, and Japan have reportedly been targeted, with at least one case resulting in a very public, high-profile outage. These attacks are now reported to have spread across both public and private sector industries.

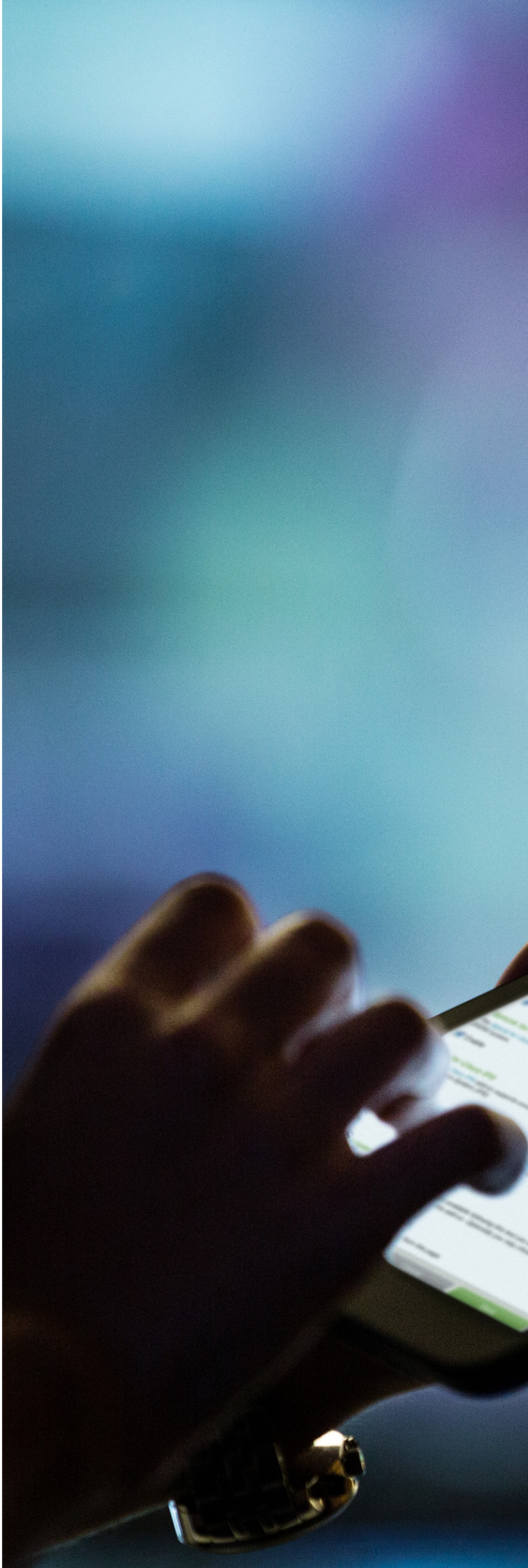
Although the exact details of each attack are still scarce, they once again highlight the operational impact that a malware outbreak can have on any organization. And the headlines support the idea that current approaches to security are failing to provide the required level of cyber protection and resilience,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

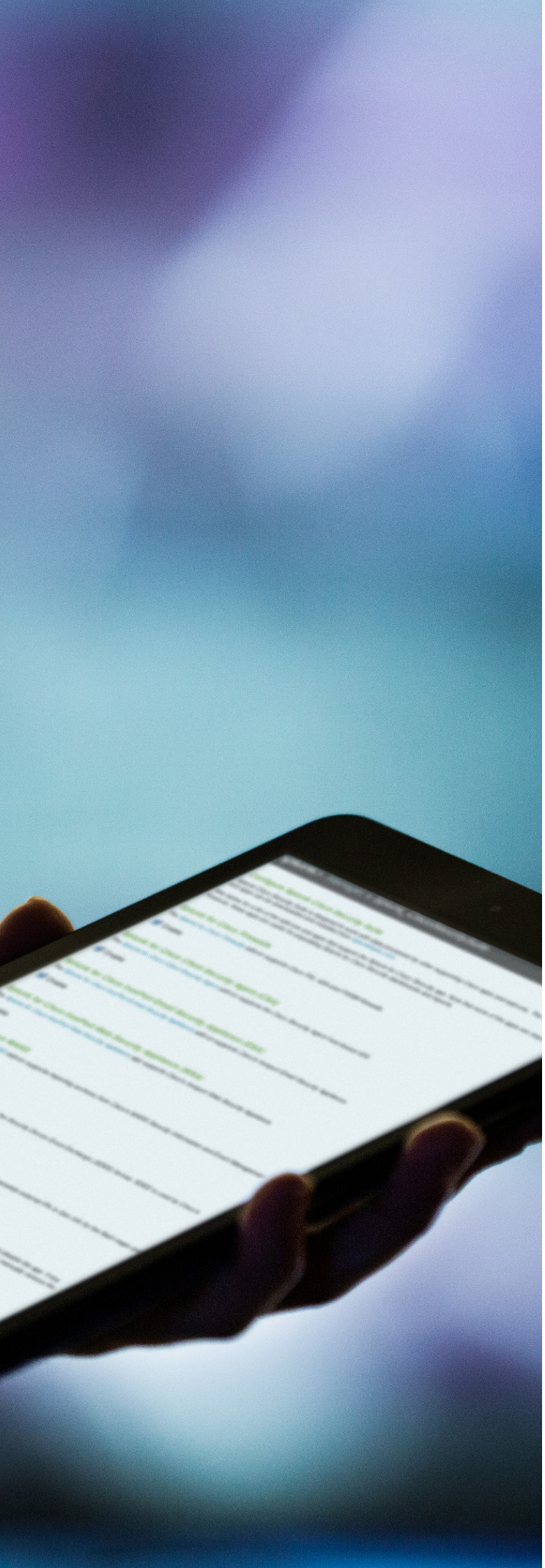
This paper offers guiding principles to underpin a security strategy and makes five specific recommendations for implementation. It is not possible to offer guarantees, but we believe adopting the principles and implementing the recommendations will help institutions to avoid potential attacks and, if they should occur, to identify and mitigate them effectively.

Three Guiding Principles

A number of well-respected security guides and frameworks are available to help organizations improve their security posture. The Cybersecurity Framework issued by the National Institute of Standards and Technology (NIST), the "10 Steps to Cyber Security" summary from the Communications Electronics Security Group (CESG), and the SANS Institute's top 20 critical security controls are just three notable examples of available resources.

Tapping the advice contained in these resources and our own practical experience, we advance the following principles to underpin an institution's approach to security:





1. Build User Awareness

The weakest link in any organization's security posture is its staff–the user community. That is not to say that staff members 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 embedded links in emails. Regular education is required to make sure security is uppermost in the minds of staff.

2. Assume That Breaches Have Taken Place

Whether an institution will suffer a security breach is no longer a question of "if" but "when."

In our experience, many organizations have already been the victims of a breach and are simply unaware that it has happened. To address this, organizations should consider the question, If you knew you were going to be compromised, would you implement security differently? By considering security in this way, institutions can begin to understand how an attack might propagate after an initial compromise and, importantly, how the attack can be detected when it's inside the network perimeter.

3. Prioritize cyber-hygiene

As the industry focuses 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 percent of successful attacks exploited vulnerabilities that had been published for more than a year on the CVE (Common Vulnerabilities and Exposures) website.

Organizations must therefore take an effective and integrated approach to their security.

Cisco and our partners can explain the value of a digital strategy, help you to develop your own strategy, and, of course, help you to execute it. Please see the section of the paper which explains how we can help. We look forward to that opportunity. To find out more, or to arrange a visit to Cisco to see some of our digital technology in action, please contact your local Cisco account manager.

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.

Even if this approach is adopted, however, malware can still breach the defenses. Then, if there is no monitoring in place to detect the breach and no network segmentation to prevent the threat from spreading, greater numbers of users are exposed.

Cisco's security strategy is based on an architectural approach that protects and remediates across the entire attack continuum: before, during, and after an attack. 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 like those recently reported.

Before the Attack

The initial attack vector for ransomware and malware is most often email. Phishing emails may not be sophisticated or highly targeted, but they can be convincing enough to encourage an unsuspecting user to click a link or open an attachment.

Blocking this type of threat requires multiple controls. A security solution must see how incoming emails are constructed, determine who is sending them, and inspect their contents (including embedded URLs to determine whether they link to known malicious sites).

The Cisco Email Security Appliance is able to apply these multiple controls. It is ideal for mitigating potential threats from emails as they attempt to enter an institution's network.

Operation of the Email Security Appliance is supported by a wealth of data and data analytics from the Cisco Talos threat intelligence team. Team members use a vast cloud-based security intelligence capability that observes and analyzes almost 30 percent of the world's email traffic. From this wealth of data, they're able to detect new threats

and feed their insights into Cisco security products.

During the Attack

To gain an initial foothold, ransomware and malware will often make use of a dropper program. These programs retrieve a malicious executable and install it 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. When it is activated, the dropper initiates an outbound connection to retrieve the malware executable. This action provides an opportunity to block infection.

Malware executables are very often retrieved from websites that are known to be bad. The Cisco OpenDNS Umbrella solution uses DNS techniques to prevent the retrieval of malicious executables over any port or protocol. It simply blocks DNS responses associated with malicious domains. The intelligence behind the decision to block DNS responses comes, as it does with the Email Security Appliance, from the collection and analysis of more than 80 billion DNS queries a day. The OpenDNS Umbrella solution uses data mining and advanced classification techniques. It can rapidly identify and block domains with new and emergent threats.

After the Attack

Using the network as a sensor, you gain full visibility of network activity through NetFlow behavioral monitoring. Cisco NetFlow captures metadata about every conversation on the network: who is talking to whom, over which protocol, and for how long. When it is aggregated and analyzed, this information can provide insight into what is normal behavior. It also helps IT staff identify questionable patterns of activity, such as malware spreading across the network, which might otherwise go unnoticed.

Using NetFlow in this way transforms the entire network into a security sensor. You get 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 Cisco Nexus® switches, as well as the Cisco router portfolio.

A companion architecture, the network as an enforcer, uses Cisco TrustSec® technology and the Cisco Identity Services Engine (ISE) to deliver software-defined network segmentation. Cisco TrustSec security group tags (SGTs) enforce role-based, topology-independent access control. Network segmentation can be implemented far more easily than relying on IP addresses or VLAN-based segmentation and can be automated.

When the network is used as an enforcer, SGTs respond dynamically to threats. For example, a user may join the network and be allocated a tag associated with a role (for example, finance). The tag is used to enforce agreed-upon access policies. The user may be able to access only those services available to members of the finance department. If that user's device is infected with malware and starts to exhibit questionable network behavior (reported by the network as a sensor), the user tag can be changed dynamically to a "quarantine" tag. Access control policies could already be predefined within the network to limit access for devices with the tag "quarantine." The potential malware outbreak will thus be rapidly contained without any manual administrative intervention.

Summary and Recommendations:

A successful approach to security requires an institution to prioritize a number of 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 second, and equally important, is taking an architectural approach to security that spans the full attack continuum.

Organizations can begin to adopt such an architectural approach by implementing the following five recommendations.

1. Build a security culture.

User education is a core security principle and fundamental to developing a strong security culture. However, security culture extends beyond routine security training. It should instead be woven into 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, institutions should run test phishing campaigns to measure the effectiveness of user education. Cisco's own security culture has developed over many years. It is now based on a mature, structured program that operates across the whole business.

2. Consider 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 the deployment of a multitude of point technologies with limited integration, resulting in gaps in visibility and protection. We recommend that organizations adopt an architectural approach to security. They should consider 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. Although segmentation may be implemented for operational convenience, there is often only limited security policy enforcement between segments. A 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. Organizations should review their current network segmentation and explore opportunities to implement strong security policies between segments.

4. Improve network traffic visibility.

Within the network perimeter, few organizations have a clear insight into patterns of traffic flow. By capturing NetFlow data, organizations can gain valuable insight into normal network behavior. Incidents can be rapidly identified and threats contained.

5. Develop a security operations capability.

Building and operating a full-time Security Operations Center is costly, but it's essential if incidents are to be quickly identified and contained. There is a significant trend toward the use of skilled third-party suppliers to deliver a fully managed security operations capability. Organizations should audit their current operational capability and explore whether it should be augmented by third-party resources and expertise.

Not sure where to begin? Cisco security services provide access to network and security experts along with continuous monitoring and management support.

Authors

This paper was written by the Cisco UK Education and Security teams. The teams have over 20 years' experience of working with education institutions on their technology programs. Their aim is to develop secure technology environments that enable efficient and cost-effective business; that support high-quality teaching, learning, and research; and that can provide the foundation for digital campuses to support the student journey.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.