HOW TO CLOSE SECURITY GAPS TO STOP RANSOMWARE AND OTHER THREATS

CONTENTS

INTRODUCTION

Defending an enterprise against ransomware and other cyber threats gets more difficult with every passing day. Not long ago, networks had a well-defined perimeter to secure—but the rise of the Internet of Things (IoT), mobile devices, and BYOD, as well as the adoption of public and private cloud services, have all helped to create a much more diverse and dynamic attack surface.

To further complicate matters, today's threat landscape continues to evolve in both volume and sophistication of attacks. Cyber crime has matured to the level of "big business" status with eye-popping annual revenues. Just one example—ransomware exploded onto the scene in 2016, routinely filling FortiGuard Labs' weekly top-five malware list while costing businesses an estimated $850 million in ransoms paid. And that number doesn't even account for the additional costs of downtime or brand impact from negative publicity. Much of this explosion can be attributed to the maturity of the cyber crime ecosystem, as evidenced by the increase in Ransomware-as-a-Service and ransomware affiliate programs.[1] Organizations must ensure they have adequate protections across the entrie attack surface.

[1] http://blog.fortinet.com/2017/02/16/ransomware-as-a-service-rampant-in-the-underground-black-market

01 EMAIL ATTACKS

Spam is the least of your inbox worries these days. From phishing scams to malware attachments and links to a rising tide of ransomware attacks—email has long been a favorite attack vector of cyber criminals. And it's often used as an early stage for advanced threats. In fact, industry sources estimate that 66% of malware leading to incidents is installed by email, and 97% of ransomware was delivered that way in 2016.

While email security is both highly saturated and very mature, according to analysts, they note that one of the primary criteria for differentiation among secure email gateways is the capability to defend against advanced and targeted threats. If you haven't upgraded security in this area within the past 12 to 18 months, you should probably give it a close look. In addition to targeted attacks and sophisticated social engineering of business email compromise threats, continued evasion techniques (such as encrypted payloads requiring a decryption key) abound. Security

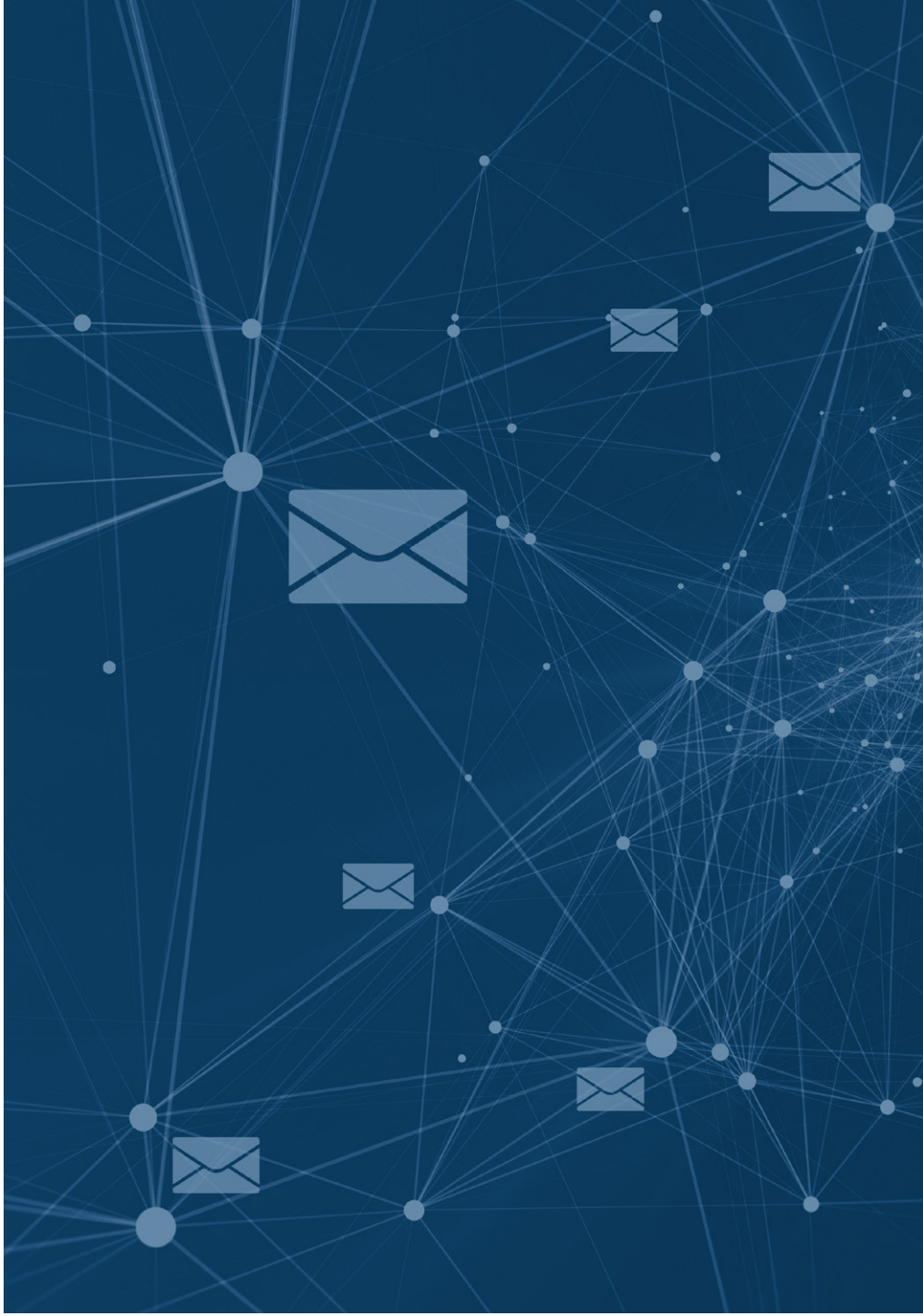
teams should ensure that their email security is routinely upgraded to address the latest cyber criminal techniques.

To complicate matters further, these kinds of threats evolve very rapidly. So inspection must be able to discover both known and zero-day types of infections. Newer technologies like sandbox analysis are being added to secure email gateways to bolster traditional defense techniques.

Because email has become a universally essential communication tool, ensuring strong protection must be a top priority for all organizations—regardless of size or industry.

***Did you know…**

- **97%** of phishing emails now deliver **ransomware**?
- Email was the delivery vehicle for **two-thirds of installed malware** in 2016, as reported by Verizon?
- A **single click** led to the biggest data breach in history?[2]



[2] http://thehackernews.com/2017/03/yahoo-data-breach-hack.html

02 WEB-BASED EXPLOITS (NETWORK/INTERNET)

Out of functional necessity, enterprise networks have become complicated beasts. Today's networks are broader and increasingly borderless thanks to trends like increasing mobility needs, the emergence of IoT devices, and adoption of private/public cloud services (e.g., Amazon Web Services and Microsoft Azure). The ever-increasing sprawl and complexity of these infrastructures make them progressively harder to defend against outside attacks.

Learn About SaaS-based INFECTIONS

In a recent survey, IT professionals name web apps they've seen infected by ransomware:

- Dropbox—70%
- Microsoft Office 365—29%
- Google Apps—12%
- Box—6%
- Salesforce—3%

With an expanding, increasingly porous, and potentially penetrable network border, the challenge becomes getting network security to follow such a dynamic perimeter as it constantly changes. And with cyber criminals consistently changing up web-based exploits to deliver malware, including ransomware, strong threat protection for this attack vector is vital. In addition to email, drive-by downloads via the web are a common ransomware delivery method, as reported by FortiGuard Labs.[3] And the use of the web to host malware allows attackers to change their payloads in an instant.

[3] https://blog.fortinet.com/2016/04/06/10-steps-for-protecting-yourself-from-ransomware

Today's businesses need to add deeper types of inspection—such as next-generation firewalling, network sandboxes, and even more sophisticated tools like network behavioral analysis and deception infrastructure. Together with email, strong protections for the web can stop 99% of the malware seeking entry. But it's important to remember that additional protections can also bring greater complexity to network security operations and can be extremely difficult to coordinate and manage.

***Did you know…**

- On average, **two-thirds** of all network traffic is **encypted**?
- The network layer encompasses **3 of the top 5 vectors** for cyber crime, as reported by Verizon?
- **87%** of CIOs feel SSL encryption puts their organizations at greater risk?
- The average enterprise uses an average of **30 different cloud services**?

03 UNPROTECTED WEB APPLICATIONS

Unprotected web applications are the easiest point of entry for hackers, and they're vulnerable to numerous sorts of attacks. The use of websites, web-based applications, and infrastructure tools (both on-premises and as an IaaS form) present well-documented vulnerabilities that have led to breaches. Attackers exploit these weaknessses (via XSS, SQL injection, etc.) to gain entry to networks.

In 2017, the year opened with key vulnerability disclosures responsibly made by FortiGuard Labs in common open source code used by WordPress, Drupal, Joomla, and more.[4] This was followed by vulnerabilities disclosed in Apache web infrastructure and others. Cyber criminals can exploit vulnerable web infrastructure for many purposes, such as to gain entry and move laterally through the network or to steal information from back-end databases. In 2016, there were also cases of compromise for the purpose of encrypting websites for ransom.[5]

[4] http://blog.fortinet.com/2017/01/05/analysis-of-phpmailer-remote-code-execution-vulnerability-cve-2016-10033
[5] http://sensorstechforum.com/drupal-ransomware-uses-sql-injection-lock-drupal-websites/

Organizations with extensive or critical web-based systems—especially those that are exposed for public use—should close this attack vector with the use of a web application firewall and network sandbox, in addition to rigorous code review during development. This includes anyone doing ecommerce, government agencies (e.g., tax departments), and professional staffing services.

***Did you know…**

- Web application attacks are the **#1 source** of data breaches?[6]
- A number of recent attack incidents have exposed vulnerabilities in both **Apache and WordPress**?
- **Financial, public, and information** industries were especially hard hit by web app attacks in 2016?

[6] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

04 WEAKNESSES AT THE ENDPOINT

Cyber criminals constantly seek to exploit any and all weaknesses across an organization's attack surface. But endpoints are the ultimate destination, given that's where data is stored—so a final line of defense is needed to secure them, following protections across other attack vectors.

End-users themselves can be the root of a range of endpoint vulnerabilities that are difficult to defend. People are often fooled by clever, socially engineered malware. These sorts of attacks constantly shift tactics to exploit a momentary lapse in judgment or errant click.

All of the various devices that end-users connect to the network also present security issues. Most employees need both on- and off-site corporate network access—but corporate data policies must be enforced at all times to make these endpoints as secure as possible at all times.

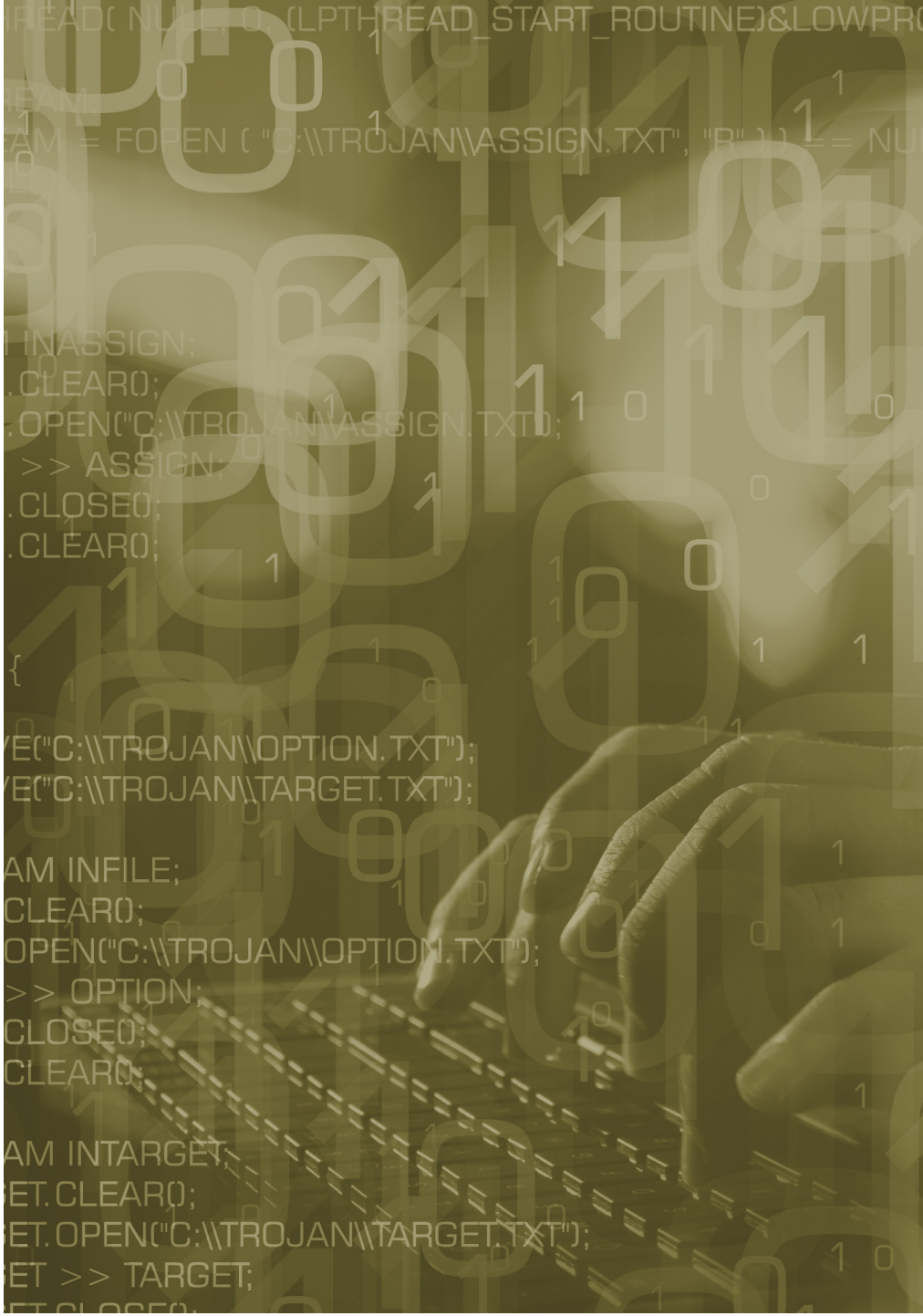
Securing your endpoints against sophisticated threats on myriad devices can be very challenging:

- Endpoints that store data are not always properly identified and secured.
- Critical endpoint systems are often untouched for availability reasons, to the detriment of security.
- A decreasing number of end-user devices are corporate standard as a result of BYOD, hiring of contractors, etc.
- The sheer number of connected devices to keep secure can be overwhelming.
- Most devices are at some point exposed by accessing public Internet outside the corporate network.

As challenging as it can be, it is the last and in some cases the only line of defense, so advanced protections are essential.

***Did you know…**

- **$850M** in ransoms were paid in an attempt to recover encrypted systems in 2016?
- And that ransomware infects **30-50K** devices per month?
- The average organization has **four active malware/bots**?



CONCLUSION

As Gartner recently noted, “All organizations should now assume that they are in a state of continuous compromise.”[7] And the data points on ransomware, ransoms, and other incidents discussed above clearly demonstrate why. In response, companies should be actively improving protection, detection, and mitigation within their broader security strategy.

Effectively protecting your enterprise starts with ensuring coverage across all of these different attack vectors through coordinated Advanced Threat Protection (ATP). Security must be able to inspect traffic, objects, and user activity from the endpoint (including IoT) and access layers to the network edge and core, all the way out to applications and the public cloud—without bogging down business operations. Security must cover the entire attack surface.

Furthermore, it’s critical to have powerful security components that share global threat intelligence (what’s seen in the wild by a research lab) as well as local intelligence (what’s happening in real time within the organization). This enables them to work as a single, cohesive system.

If components operate independently, then there will be gaps through which cyber criminals can slip and silos that will slow down response and mitigation times. Automation of all deployed components presents the strongest, most unified defense.

Implementing a seamless, end-to-end security strategy for Advanced Threat Protection, even across components from multiple vendors, offers the most promising approach to addressing advanced threats to cover the entire attack surface of today’s organizations.

[7] http://www.gartner.com/smarterwithgartner/security-at-the-speed-of-digital-business/

FORTINET®

www.fortinet.com