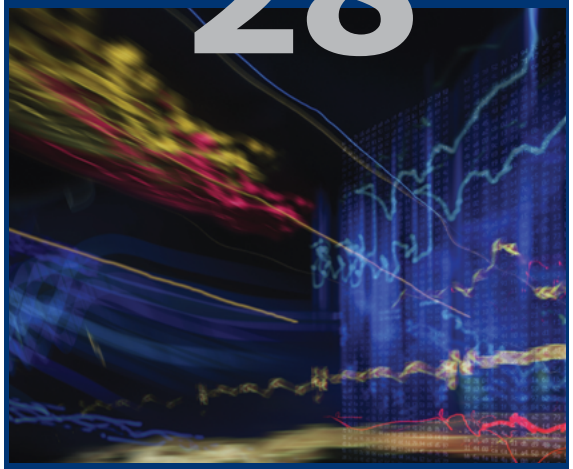
Advanced Threat Detection and Remediation:

Why it's Needed

Sponsored By 

It's estimated that in 2014, 28 distributed denial of service (DDoS) attacks occurred every hour.



Advanced Threat Detection and Remediation

Executive Summary

Newsletters, blogs and reports are loaded with news of advanced threats and targeted attacks on business and government servers. In 2014, it was estimated that 28 distributed denial of service (DDoS) attacks occurred every hour.[1] And that is just one type of attack. There are many other kinds — some detected after just a few minutes, others persisting for months or longer. These attacks can cause disruptions or outages, and the financial impact can be severe.

No business, large or small, is immune from targeted attacks. Where there is money to be made by these attacks, or political damage to be done, criminal elements will continue to create new methodologies to penetrate corporate and government networks.

J.J. Thompson, chief executive of Rook Security, perfectly summarized the digital security environment. Thompson said that even with the best information security professionals in the world,

"Sometimes it's not about the technology and it's not about whether you have the smartest staff. It's all about whether you have the right way of identifying problems and resolving those problems in a timely manner."[2]

Advanced threats have become so commonplace that it has become a matter of when — rather than if — your company will be attacked. This paper will discuss why it is absolutely necessary for organizations to pay attention to the growing problems of advanced threats and targeted attacks. It will also suggest some features that an effective solution will need.

CISO Mentality

All too often, chief information security officers (CISOs) and others charged with network and data security think their companies are sufficiently protected, believing they

Sponsored By hp

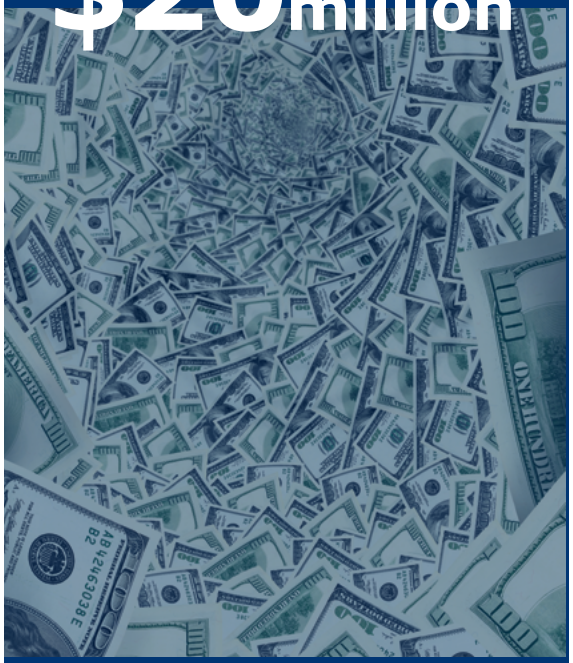
[1] Chris Preimesberger. "DDoS Attack Volume Escalates as New Methods Emerge." Eweek (May 28, 2014). Accessed May 8, 2015 at www.eweek.com/security/slideshows/ddos-attack-volume-escalates-as-new-methods-emerge.html.

[2] Leisa Richardson. "Anthem Hack Offers Big Lessons for Business, Customers." Indystar (March 1, 2015). Accessed May 8, 2015 at http://www.indystar.com/story/money/2015/03/01/anthem-hack-offers-big-lessons-business-consumers/24084979.

emedia

Financial impact to 92% of organizations: over

$20million



have implemented the right solutions to protect their environments. They ensure security is kept up to date, holes are patched, and password policies enforced.

Yet when CISOs are asked what keeps them awake at night, a common answer is, "I'm afraid of what I don't know."[3]

There is always that one patch that has not been applied, an employee bringing a flash drive from home, or someone uploading infected files from a smartphone. Any one of these can introduce problems to the corporate network. Cyber-thieves have become more creative and persistent, finding new ways to avoid detection.

Further, as these criminal elements continue to evolve, they have improved their ability to invade networks without detection, allowing theft of financial data, customer information, and other confidential details. They may even uncover trade secrets or intelligence with national security implications.

The constant challenge for CISOs and their staff has become how to proactively block intrusions and security threats and how to find other threats that may have evaded detection but are not lurking in the network.

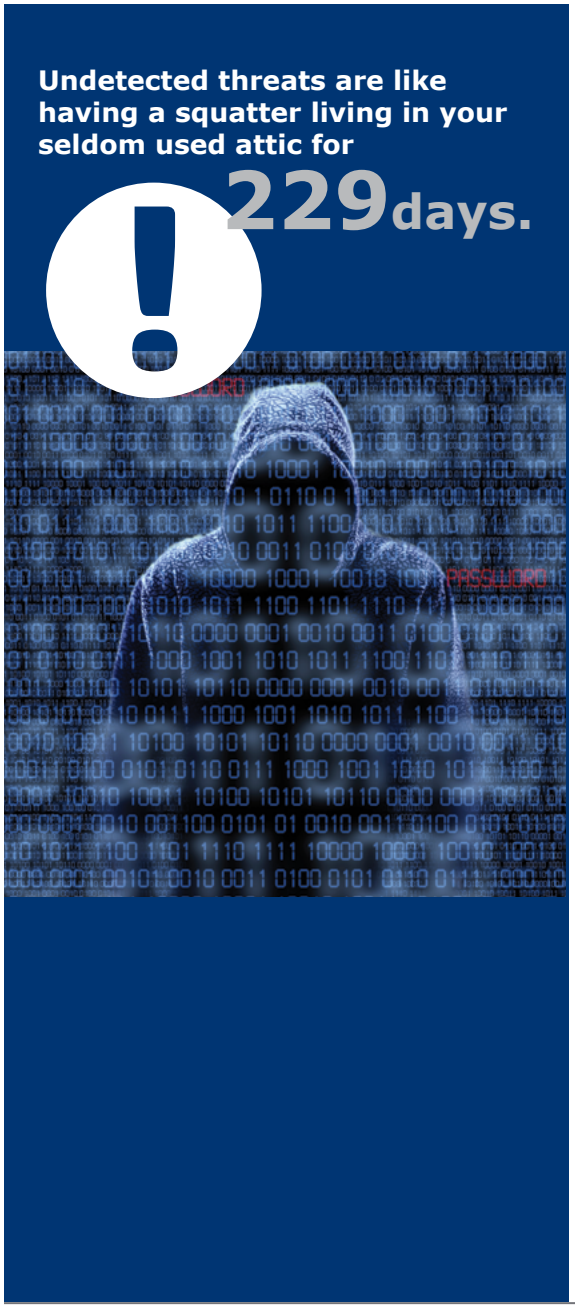
Lack of Detection

Cybercrime has been in headlines recently, and the severity and frequency is always on the rise. A 2014 survey conducted by PricewaterhouseCoopers (PwC) found that the number of detected incidents rose sharply to 42.8 million, an increase of 48 percent over the prior year. Perhaps even worse, the survey also found that the financial impact of cybercrime increased by 34 percent. Additionally, 92 percent more organizations had an impact over $20 million.[4]

Key to the effectiveness of any cybersecurity program is early detection. Some malware or viruses can reside undetected in networks or individual computers for months at a time. The average threat detection time is 229 days. During that time,

[3] Rick Tracy. "What Keeps a CSO Awake at Night?" Telos (October 7, 2014). Accessed May 8, 2015 at http://multimedia.telos.com/blog/what-keeps-a-cso-awake-at-night.

[4] "Global State of Information Security Survey 2015." Pricewaterhouse Coopers (September 30, 2014). Accessed May 8, 2015 at http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml.



threats can spread to thousands of other computers and methodically capture data. Information can be sent to outside elements or funneled to an inside perpetrator, which often makes detection even more difficult.

Undetected threats are like having a squatter living in your seldom used attic for 229 days.[5] Imagine the amount of information he could gather about you and your family, in addition to the damage he could do to your house in that time.

In one recent attack of particular notoriety, hackers penetrated the corporate networks of a well-known international casino company in Las Vegas, resulting in loss of data and destruction of thousands of computers and servers. An investigation uncovered that the threat penetrated the network months before through a relatively small — and lightly guarded — location in Bethlehem, Penn. The cyber-thieves searched for the door into the corporate domain for several months without being detected until they found a workable entrance.[6]

Many businesses only use internal resources and technicians to determine the security levels that meet their needs for the evaluation, selection and implementation of chosen solutions. Often this results in a patchwork of non-interrelated combinations of firewalls, IPS, antivirus software, malware detection, and security appliances. Each of these components may require installation and setup, training, updates and monitoring.

Businesses of all sizes as well as government agencies are increasingly becoming aware that this is not enough. They need to detect intrusions of all kinds accurately and quickly. The longer the intrusions go undetected, the more the eventual remediation will cost and the more painful it will be.

Ability to Move Freely Within a System

Because more security is stacked at the point of entry, once advanced threats or targeted attacks get into the network, threats can usually move freely across the network,

[5] T.J. Alldridge, interview by Charles D. Beard and Annika Mitic, February 12, 2015.
[6] Swati Khandelwal. "Las Vegas Sands' Casino Network Hit by Destructive Malware." The Hacker News (December 12, 2014). Accessed May 8, 2015 at thehackernews.com/2014/12/las-vegas-casino-hacked.html.

The average cost of a data breach incident is now estimated at

$5.9million

propagating at will onto multiple servers — both local and remote — potentially gaining access to thousands of computers or servers. With access to these resources, advanced threats can exfiltrate or destroy information.

When a threat is able to move freely within a system, it puts a significant amount of information at risk, including:

- Confidential company information like business plans and financial or marketing strategies
- Client information like contact names, products purchased and sales history
- Vendor information, pricing and purchase volumes
- Employee information: names, addresses, Social Security numbers and salaries

Attacks on retailers can severely damage their reputation with customers, causing them to take their business to competitors. Freedom of movement within corporate systems require retailers to deal with the financial impacts of data recovery, purchase of credit monitoring services for customers, pay for the reissuance of credit cards and so forth. The 2013 attack on Target comes to mind as a recent example.[7]

Healthcare industries are another prime target for hackers. Anthem, a major insurance provider providing coverage for millions of individuals, recently saw cybercriminals compromise some 80 million customer records. Because hackers could poke around Anthem's system until they found something, sources have estimated the cost of the breach at more than $100 million.[8]

It's not just major companies that spend millions of dollars remediating penetration by advanced threats. The *average* cost of a data breach incident for a large organization is now estimated at $5.9 million.[9]

All of this highlights the importance of scanning the east-west traffic for threats moving laterally across the network and a layered security solution that works together.

[7] Rich Hein. "12 Biggest Data Breaches of the Last 12 Months." Networkworld (April 1, 2014). Accessed May 8, 2015 at http://www.networkworld.com/article/2285949/security/146856-12-Biggest-Data-Breaches-of-the-Last-12-Months.html.

[8] "Report: Cost of Anthem Breach Could Cross $100M." HealthcareDIVE (February 17, 2015). Accessed May 8, 2015 at www.healthcaredive.com/news/report-cost-of-anthem-breach-could-cross-100m/364814.

[9] "Global State of Information Security Survey 2015." Pricewaterhouse Coopers (September 30, 2014). Accessed May 8, 2015 at http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml.

Security systems should communicate with each other to streamline protection.

Features needed for an effective solution

When considering options that will provide the highest level of security for your environment, it's critical to evaluate the features offered by each solution. High on the list of those features will be:

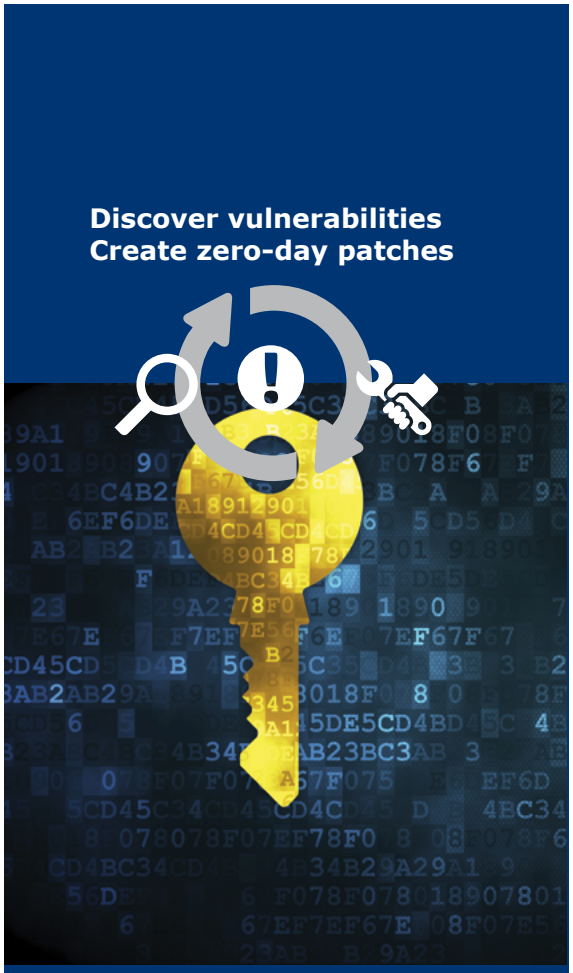
- **Zero-day detection:** Don't let that squatter into your attic in the first place.
- **Advanced threat protection:** Detect and analyze advanced threats that may have slipped past other security systems.
- **Integration with other security solutions:** Security systems should communicate with each other to streamline protection.
- **Lateral detection:** Many concentrate their security efforts on what comes in and out of your network but you can't ignore the lateral movement of the threat once it gets in.
- **Shut out threats after remediation:** Incorporate next generation firewalls and Intrusion Prevention System (IPS) to shut out the threat immediately.
- **Threat intelligence:** Block future vulnerabilities before they can be exploited.

Solutions

The PwC study found that regardless of the publicity and media attention to significant attacks on businesses, many organizations have not approached information security decisions at the board level.[10] This level of commitment is vital to a successful defense and ongoing security solution.

HP offers the TippingPoint Advanced Threat Appliance (ATA). TippingPoint ATA can detect and analyze targeted attacks and advanced threats to your systems in minutes. By working with the TippingPoint Next-Generation Firewall (NGFW) and IPS, it will shut down all points of access to prevent the same attack from reentering or moving laterally across the same

[10] "Global State of Information Security Survey 2015." Pricewaterhouse Coopers (September 30, 2014). Accessed May 8, 2015 at http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml.



network. The TippingPoint ATA will also send threat information to HP ArcSight, an industry-leading Security Information and Event Management (SIEM) solution from HP, for further investigation. ArcSight will give you a view of how the threat got in, who was responsible, and what it was attempting to do.

TippingPoint is a complete family of solutions that combine to address today's next generation security threats for business. It is the only next generation security solution that delivers a simple, effective and reliable suite of products that protect against known and unknown vulnerabilities — not just the exploits.

HP TippingPoint pioneered the Intrusion Prevention System (IPS), which resides in-line, blocking known, unknown, and zero-day vulnerabilities in real time. HP Security Research (HPSR) and the Zero-Day Initiative program discover more vulnerabilities, and the TippingPoint DVLabs team creates more zero-day patches to provide real-time protection for the IPS and NGFW platforms than any other vendor. To date, we have created more than 9,000 Digital Vaccine filters (virtual patches). TippingPoint's security coverage focuses on the root cause of the security threat — the actual software vulnerability — rather than merely identifying and blocking an exploit aimed at that vulnerability.

HP TippingPoint protects the data and the applications that matter anywhere in the network — data center, campus networks and bank offices. Your network and organization are protected, while still keeping your employees productive. Through the use of HP TippingPoint's unique set of security components, companies are protected from cyber-threats and advanced persistent threats.

Security for you and your company

How Do You Get Started?

It's time to ensure that your network is safe from advanced malware attacks. HP is an industry leader in technology and security, providing business with the technology and tools required to protect networks, data assets and intellectual property. HP is ready to assist you in protecting your environment and data from cybercriminals.

Contact HP today to discuss how its threat prevention family of solutions can provide security for you and your company.

Learn more at
Network Security Management System TippingPoint SMS | HP® Official Site

Talk with an expert:
1-877-686-9637

emedia | www.emedia.com | inquiries@emedia.com
800-782-6167 or 312-754-6355