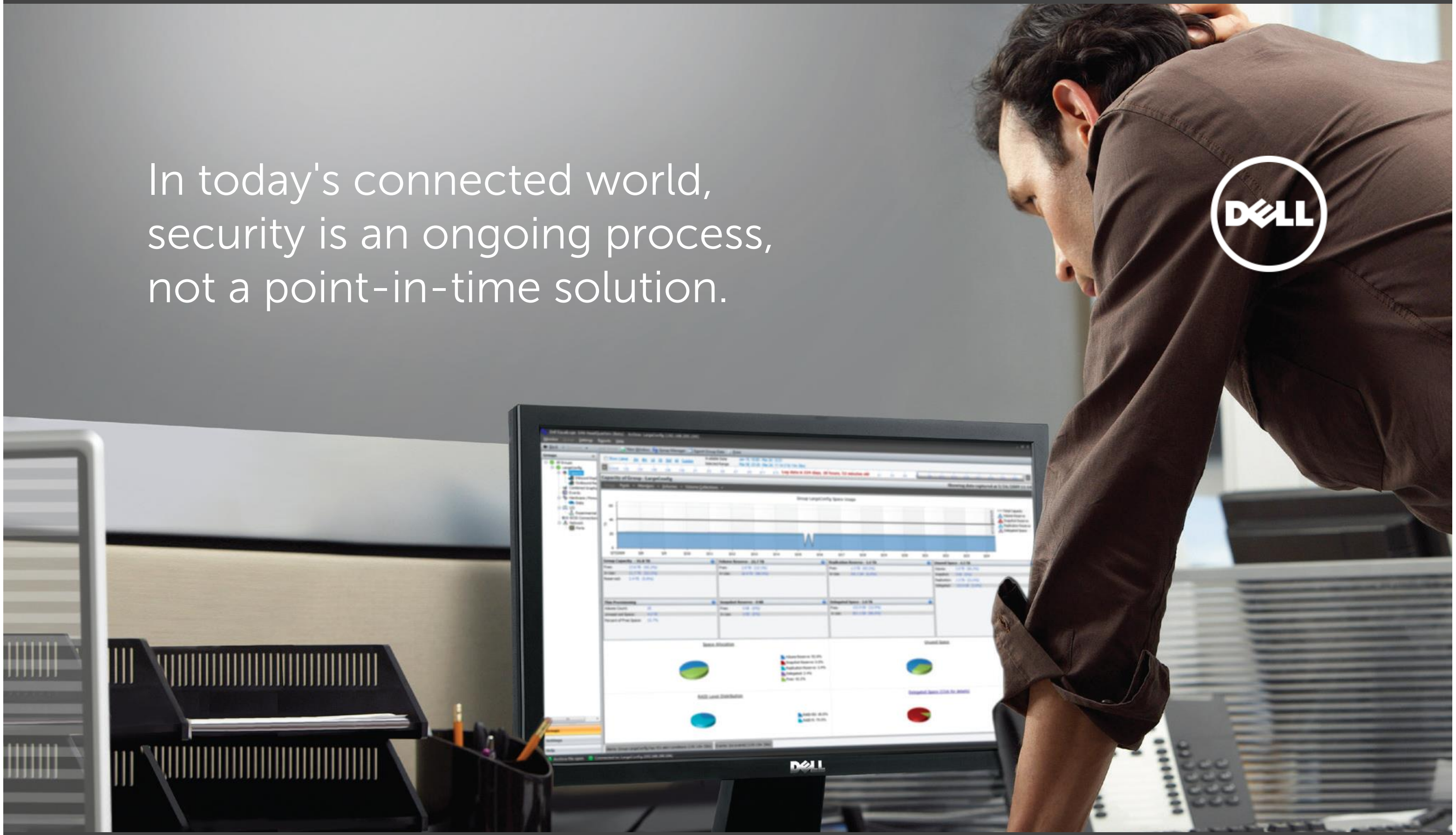

In today's connected world,
security is an ongoing process,
not a point-in-time solution.

2015 Dell Security Annual Threat Report Executive Summary

Organizations are spending more than ever on IT security, both to comply with internal and regulatory requirements and to protect their data from cyber-threats. Yet each year, high-profile data breaches continue to fill the headlines, sabotaging the reputations, relationships, and revenue of the businesses that are victimized.

It's clear that cyber-crimes are alive and well on the global stage and will only continue to be pervasive as long as organizations delay taking the necessary defense measures to stop threats from slipping through the cracks. In the 2015 Dell Security Annual Threat Report, we'll present the most common attacks that were observed by the Dell SonicWALL Threat Research Team in 2014 and the ways we expect emergent threats to affect businesses of all sizes throughout 2015. Our goal is not to frighten, but to inform and provide organizations of all sizes with practical advice that will help them adjust their practices to more effectively prepare for and prevent attacks, even from threat sources that have yet to emerge.

1.7 trillion IPS attacks blocked

4.2 billion malware attacks blocked

In 2014, we collected 37 million unique malware samples, almost double the 19.5 million from 2013. Put another way, every day in 2014, attackers launched twice as many unique attacks on your systems with malicious code. We saw 88 trillion hits for application traffic and 45 billion hits for post-infection malware activity.

Key findings include:

- A surge in point-of-sale malware and attacks
- A dramatic increase in SSL and TLS encrypted Internet traffic
- Twice the attacks on SCADA systems

The data was gathered by the Dell Global Response Intelligence Defense (GRID) Network, which sources information from a number of devices and resources including:

- More than 1 million security sensors in more than 200 countries;
- Activity from honeypots in Dell's threat centers;
- Malware/IP reputation data from tens of thousands of firewalls and email security devices around the globe;
- Shared threat intelligence from more than 50 industry collaboration groups and research organizations;
- Intelligence from freelance security researchers; and
- Spam alerts from millions of computer users protected by Dell SonicWALL email security devices.

Threat Findings for 2014

One of the best ways to predict and prepare for emergent threats is to analyze information about recent breaches. Dell's predictions and security recommendations for 2015 revolve around eight key findings, including three of particular note:

1 A surge took place in point-of-sale (POS) malware variants and attacks targeting payment card infrastructures.

The retail industry was shaken to its core in 2014 after a staggering four major retail brands experienced highly publicized breaches. Home Depot, Target, Michaels, and Staples all became targets of credit card data theft, with each breach exposing millions of consumers to potential fraudulent purchases and/or identity theft. Target's was considered the largest breach in the history of U.S. retail, with 40 million card numbers stolen, until Home Depot's breach compromised 56 million card numbers just a few months later. In the case of Home Depot and Michaels, the attacks took place over several months before they were detected.

Dell saw a rise in POS attacks attempted among Dell SonicWALL customers as well.

In 2014, we developed and deployed more than 3X the new POS malware countermeasures than the previous year.

- Dell SonicWALL created 13 POS malware signatures in 2014, compared to three signatures in 2013 – a 333% increase in the number of new POS malware countermeasure developed and deployed.
- The majority of these POS hits targeted the U.S. retail industry.
- We saw POS malware tactics evolve in 2014, with new trends including memory scraping and the use of encryption to avoid detection from firewalls.

It begs the question: In a modern retail environment, where compliance to payment card industry (PCI) standards is mandatory, how does this happen? The most common causes include inadequately trained employees, lax firewall policies between network segments and in the B2B portal, and reliance on a single layer of defense or an array of poorly integrated products. Or in Target's case, the attack came indirectly through the company's HVAC vendor, who likely received deeper user permissions than needed.

2 More companies were exposed to attackers hiding in plain sight as a result of SSL/TLS encrypted traffic.

For many years, financial institutions and other companies that deal with sensitive information have opted for the secure https protocol that encrypts information being shared. Now other sites like Google, Facebook, and Twitter are adopting this practice as well in response to a growing demand for user privacy and security.

Dell saw a 109% increase in the volume of HTTPS web connections from the start of 2014 to the start of 2015.

Although there are many benefits to using more Internet encryption, we are seeing a less positive trend emerge as hackers exploit this encryption as a way of "hiding" malware from corporate firewalls.

While managing against this threat is complicated, organizations can provide threat protection for encrypted traffic by implementing SSL inspection.

3 Attacks doubled on supervisory control and data acquisition (SCADA) systems.

Industrial operations often use SCADA systems to control remote equipment and collect data on that equipment's performance. Whereas the motive behind POS and secure web browser attacks is typically financial, SCADA attacks tend to be political in nature, since they target operational capabilities within power plants, factories, and refineries, rather than credit card information.

In 2014, Dell saw a 2X increase in SCADA attacks compared to 2013.

- The majority of these attacks targeted Finland, the United Kingdom, and the United States, likely because SCADA systems are more common in these regions and more likely to be connected to the Internet.
- Buffer overflow vulnerabilities continue to be the primary attack method.

Because companies are only required to report data breaches that involve personal or payment information, SCADA attacks often go unreported. As a result, other industrial companies within the space might not even know a SCADA threat exists until they are targeted themselves. This lack of information sharing combined with the vulnerability of industrial machinery due to its advanced age means that we can likely expect more SCADA attacks to occur in the coming months and years.

Additional predictions:

- More organizations enforce security policies that include two-factor authentication.
- Sophisticated, new techniques thwart Android malware researchers and users, and more highly targeted Android malware emerges.
- More Android malware emerges targeting specific apps, banks, user demographics, and specific technologies.
- The first wave of malware targeting wearable devices emerges.
- Digital currencies including Bitcoin continue to be targets of mining attacks; Botnet involved.
- Home routers and home network utilities become targets and are used to assist large DDoS attacks.
- Electric vehicles and their operating systems are targeted.

Key Industry Observations of 2014

The business world saw a number of breaches throughout the year involving companies who overlooked one or more of these basic threat vectors:

Outdated, unpatched software

Under-restricted contractor access to networks

Under-secured network access for mobile or distributed workers

Under-regulated Internet access for all employees

Some of these threat vectors have posed security challenges for years, while others are emerging as a result of today's highly mobile, consumer-tech-empowered workforce. As always, cyber-criminals remain adept at finding new ways to exploit common blind spots and, as we'll discuss, even use companies' best security intentions against them.

Other key vulnerabilities and attacks from 2014:

The Common Vulnerabilities and Exposures (CVE) system reported about **9,400 NEW VULNERABILITIES** and **more than 2/3** of them were related to **network attacks.**

The POODLE man-in-the-middle vulnerability was disclosed in September 2014.

We released **13 ADVISORIES** addressing **Microsoft security bulletins,** including out-of-band zero-day advisories.

The **HEARTBLEED buffer over-read vulnerability,** disclosed in April 2014, potentially affected about **17%** (about 1/2 million) of the Internet's secure web servers.

The **Nuclear, Angler and Magnitude** together forms **almost 90%** of the **"in the wild"** exploit kits.

The **Angler** exploit kit is **most prevalent** – accounting for around **60%** of all exploit kits.

Multiple NTP-based and **DNS-based DDoS** attacks were observed.

FOURTEEN well-known **zero-day vulnerabilities** were released.

SHELLSHOCK vulnerabilities were **exploited by attackers within hours** of the initial disclosure on September 24, 2014. By the next week, **millions of attacks and probes per day** were observed.

Final Takeaways

Clearly, network security remains a top priority and a major challenge as companies combat today's more organized, highly skilled and well-financed cyber criminals. 2014 brought new, innovative techniques for gaining elevated rights and access to corporate networks in ways that were both unpredictable and almost impossible to detect and prevent by traditional security defense systems.

The most effective approach companies can take today is to establish multiple layers of security and threat intelligence that provide numerous methods for preventing and responding to attacks on their network. These layers, together comprising a defense-in-depth program, include all of the following:

1. Continuous security awareness training for employees.

2. Vigorous endpoint defense, as most network infiltrations begin with a compromised user device.

    a. Deploy secure mobile access technology that checks the security posture of user devices before granting network access and enforces policy that grants VPN access only to trusted users, mobile apps and devices
    b. Deploy secure workspace technology to establish and enforce on-device data protection policies and app management
    c. Implement two factor authentication for both administrators and users
    d. Protect the privileged accounts.
    e. Manage contractors, partners, interns, patients, and vendors access differently than internal resources. Control and monitor access rights regularly.

3. Replacing traditional or legacy firewalls with a Next-Generation Firewall (NGFW).

4. Investment in a capable intrusion prevention system.

5. Addition of an SSL/TLS inspection capability to detect and block malware that is hidden in SSL/TLS-encrypted traffic.

6. Ensuring there is around-the-clock threat counter-intelligence feeding security updates to NGFWs and intrusion prevention systems.

7. Deployment of an email security solution.

8. Consistent software updates.

9. Securing remote work environments by segmenting router access.

10. Providing the same level of defense throughout a distributed enterprise's locations, including kiosks, executive homes, and remote offices.

In today's world, security may seem like an insurmountable challenge, but overall protection simply requires a mix of the right technology, the right planning, and the right training. Stay vigilant over what's happening in your infrastructure. Get knowledgeable about other breaches happening in the industry. Be communicative with your team. And be prepared and ready to act when a threat inevitably arises.

As a global leader in network security, it is Dell's mission to help companies proactively protect their data from common and emergent threats. We hope this Executive Summary, and the complete Dell Security Annual Threat Report, empowers organizations of all sizes to become more prepared, informed, vigilant, and successful in preventing attacks throughout 2015.

The complete Dell Annual Threat Report is available online at
http://software.dell.com/whitepaper/dell-network-security-threat-report-2014874708