IT savvy

2015 Dell Security Annual Threat Report

Table of Contents

Introduction

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

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 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 (POS) malware and attacks;
- a dramatic increase in Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encrypted Internet traffic; and
- twice the attacks on supervisory control and data acquisition (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 one 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:

1 A surge took place in POS malware variants and attacks targeting payment card infrastructures.

The retail industry was shaken to its core in 2014 after a staggering number of major retail brands experienced highly publicized POS 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.[1,2] In the case of Home Depot and Michaels, the attacks took place over several months before they were detected.[3]

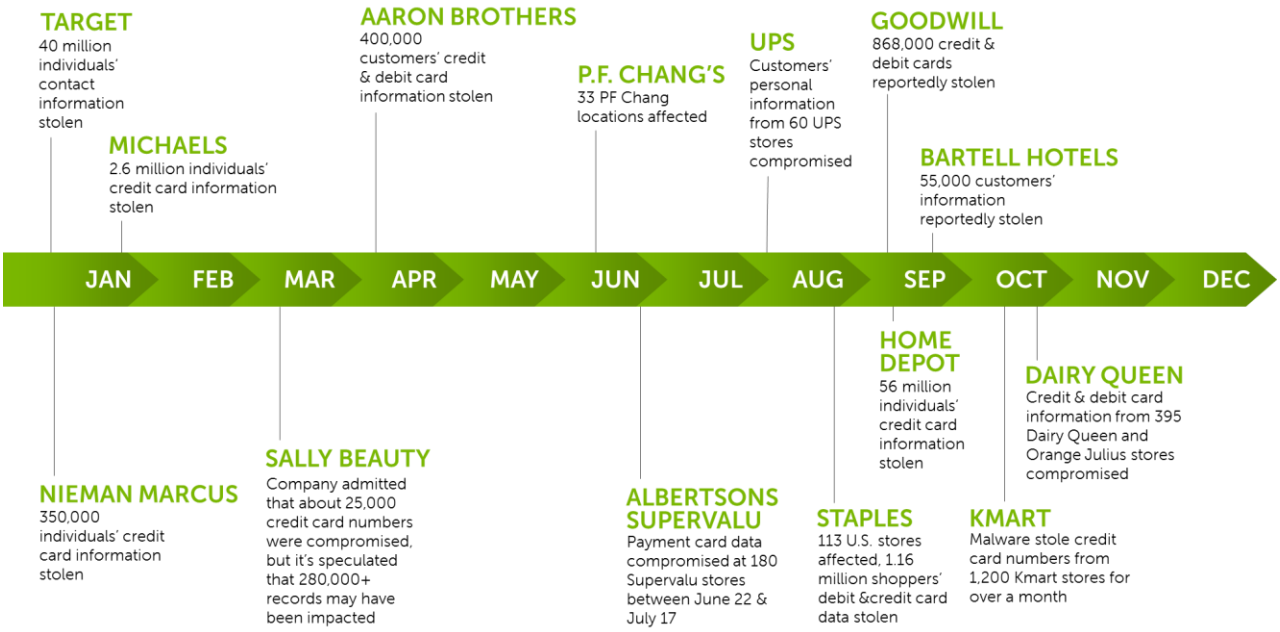
Dell saw a rise in POS attacks attempted among Dell SonicWALL customers as well.

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

- Dell SonicWALL created 13 POS malware signatures in 2014, compared with three in 2013 – a 333% increase in the number of new POS malware countermeasures 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.[1]

Timeline of High Profile Retail Breaches



To subvert the multitude of compliance regulations and corporate policies in place, cyber criminals are taking a multi-vector approach, exploiting a few key areas of concern that, if unaddressed, will lead to a continued surge in POS attacks over the coming months. Companies should consider the following approaches:

- Traditional POS applications run on terminals connected to a central computer. Often, the operating system (OS) of this central computer is not kept updated, which can make the POS system as a whole highly vulnerable. It's important to keep this OS patched and all software updated.
- Keep the POS system isolated from the rest of the network. Make sure POS systems can only communicate with valid IP addresses, so attackers cannot siphon data off to their own servers.
- Restrict activity on terminals to only POS-related activities (no web browsing).
- Install firewalls between network segments and in the B2B portal.
- Do not rely on a single layer of defense or an array of products that are not properly integrated.
- Make security training a significant part of employee onboarding and ongoing communications. Dell's recent Global Technology Adoption Index (GTAI) showed that employee security training is lacking in all industries, including retail. An astounding 56% of companies admit that not all of their employees are aware of security rules.[4]
- Think about how to truly protect your data from attackers, not just how to meet compliance regulations. Retail is the only industry in which companies are devoting more financial resources to compliance-related security concerns than to hacker-related concerns.[4] This could explain why companies like Target (and its HVAC vendor, through whom the attack was deployed) sometimes have compliant technology in place, but do not have adequate processes in place for addressing threats.
- Adopt a security policy that trusts nothing (network, resources, etc.) and nobody (vendors, franchisees, internal personnel, etc.), and then add explicit exceptions.
- Separate groups and zones to keep attackers who have gained network access from penetrating further.

- Inspect all traffic at every node on every segment, inbound and outbound, and automatically investigate anomalies.
- Enforce email security to block malware in spam and phishing attacks.
- Unify multiple technologies into a platform that protects against threats.
- Don't sacrifice security for performance.

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

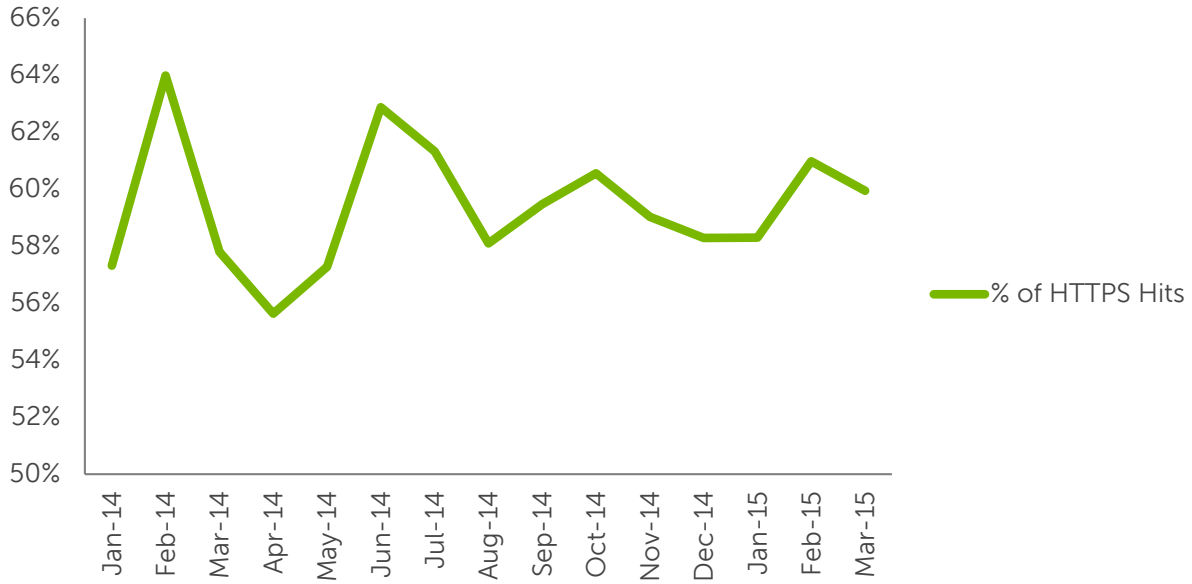
For many years, financial institutions and other companies that deal with sensitive information have opted for the secure HTTPS protocol that encrypts information being shared. Now other sites like Google, Facebook, and Twitter are adopting this practice as well in response to a growing demand for user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

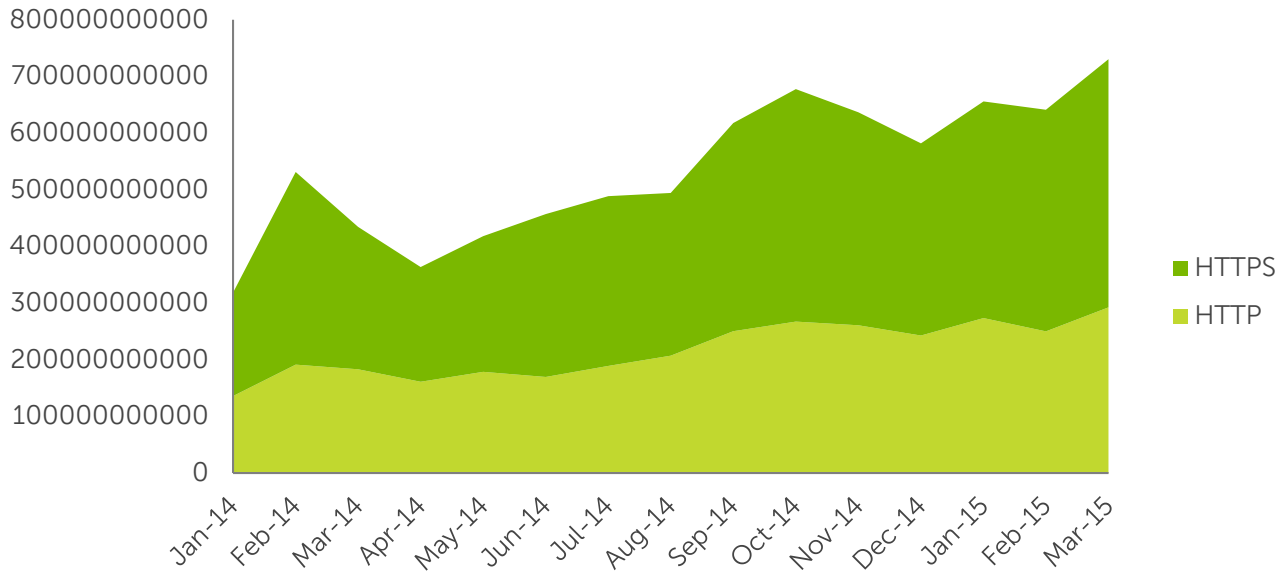
- Dell saw an increase in the volume of HTTPS web connections from 182 billion in January 2014 to 382 billion in January 2015, and this number continues to grow. As of March 2015, the number was 437 billion.

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. In early 2014, hackers successfully distributed malware to about 27,000 Europeans per hour over the course of four days, simply by infecting a group of banner advertisements on Yahoo's news site. Since Yahoo's site was encrypted, this malware was able to tunnel through users' firewalls unseen.[5]

HTTPS Hits as Percentage of Total Hits



Web Browsing Hits: HTTPs vs. HTTP



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

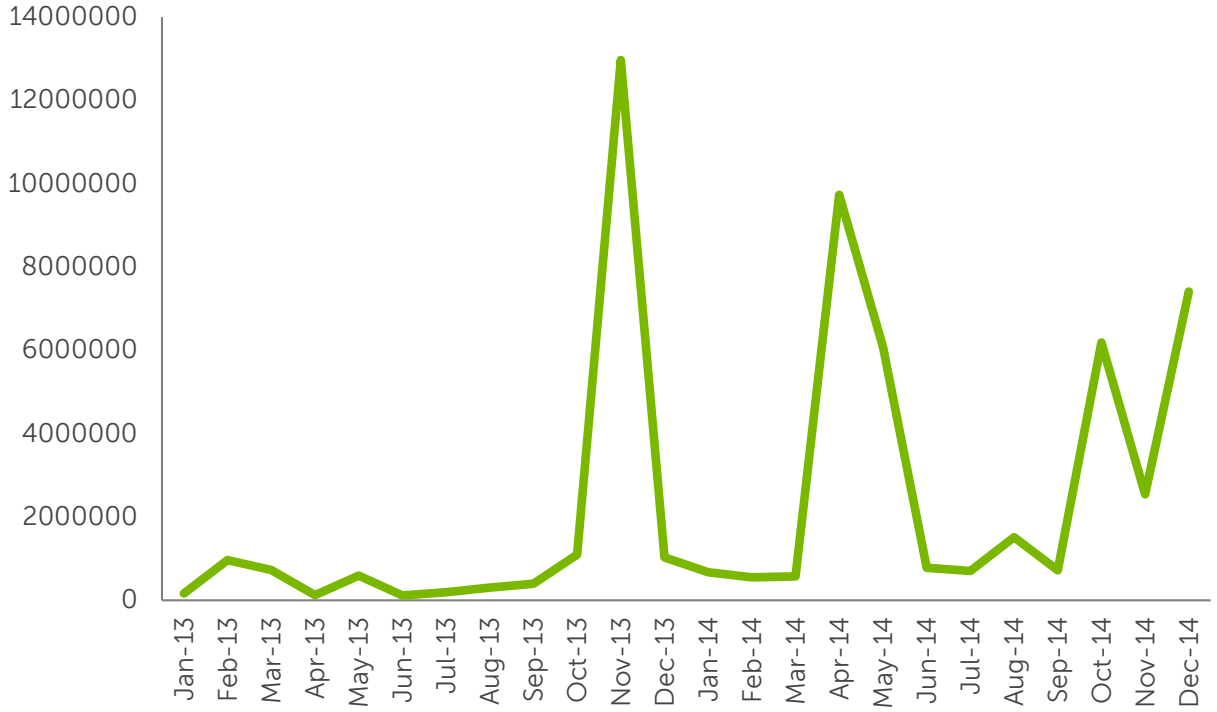
3 Attacks doubled on SCADA systems.

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.

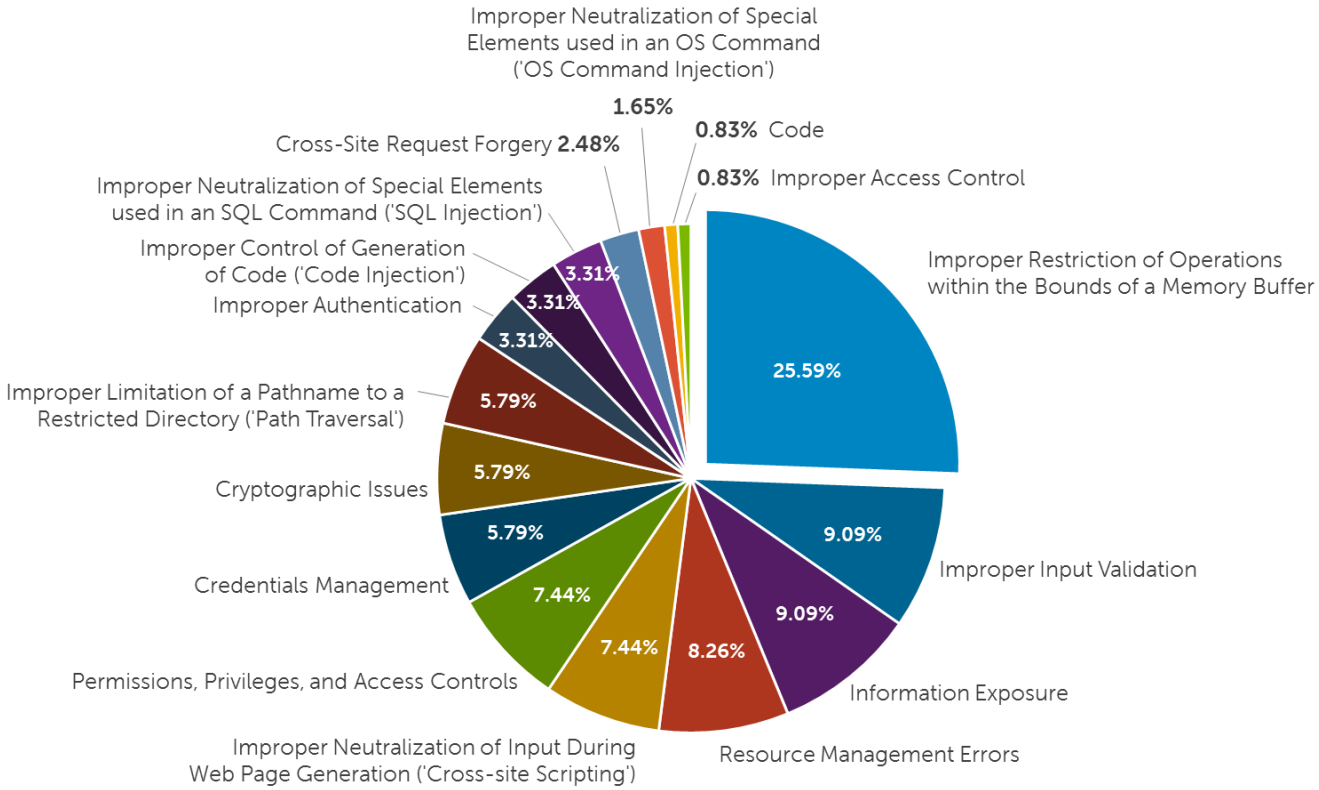
In 2014, Dell saw a 2X increase in SCADA attacks compared with 2013.

- We saw worldwide SCADA attacks increase from 91,676 in January 2012 to 163,228 in January 2013, and 675,186 in January 2014.
- 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. In 2014, Dell saw 202,322 SCADA attacks in Finland, 69,656 in the UK, and 51,258 in the US.
- Buffer overflow vulnerabilities continue to be the primary attack method, accounting for 25% of the attacks.

SCADA Hits Monthly



Key SCADA Attack Methods



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.

There are a few general ways to protect against SCADA attacks:

- Make sure all software and systems are up to date. Too often with industrial companies, systems that are not used every day remain installed and untouched as long as they are not actively causing problems. However, should an employee one day connect that system to the Internet, it could become a threat vector for SCADA attacks.
- Make sure your network only allows connections with approved IPs.
- Follow operational best practices for limiting exposure, such as restricting USB ports if they aren't necessary and ensuring Bluetooth is disabled.
- In addition, reporting and sharing information about SCADA attacks can help ensure the industrial community as a whole is appropriately aware of emerging threats.

4 More organizations will enforce security policies that include two-factor authentication (2FA).

When a data breach happens, cyber criminals don't always utilize the information or access they gained right away. Sometimes, they wait for a calculated opportunity.

As a result of 2014's numerous data breaches, a large number of user credentials, such as credit cards and Social Security numbers, were stolen and sold in underground markets. Understanding that these credentials might be used at any time, many financial institutions, such as Citibank, have begun to enforce 2FA.

With 2FA, when a user attempts to log into Citibank's site for the first time, he or she will not be authorized based on username and password alone. Citibank will send a verification code to the user's cell phone number on file, and only that code in combination with the username and password will allow the user access to his or her online banking.

Typically 2FA, which is more broadly called multi-factor authentication (MFA), requires two of the following authentication factors:

- *Knowledge* factors ("things only the user *knows*"), such as a password
- *Possession* factors ("things only the user *has*"), such as an ATM card or cell phone
- *Inherence* factors ("things only the user *is*"), such as a thumbprint

In addition to online banking or other user logins, companies will likely implement 2FA in a few key places, including access points for mobile workforce authentication, virtual private networks (VPN), virtual desktop infrastructure (VDI), cloud servers, networks, and single-sign-on for web-based apps.

Companies can take additional steps to reinforce the value of 2FA, including:

- requiring all employees to use different passwords for every online service the company uses. This is easier to implement if employees use a password management app;
- having detailed and well-communicated procedures in place for when a mobile device is lost or stolen; and
- educating employees on basic security measures, such as password protection.

5 Sophisticated, new techniques will thwart Android malware researchers and users, and more highly targeted smartphone malware will emerge. In connection, the first wave of malware targeting wearable devices via smartphones will emerge.

Smartphone attacks have been a security concern since mobile devices began to reach widespread adoption, but it wasn't until 2014 that smartphone malware began to look and act like its desktop predecessors.

Last year, a variety of Android attacks arose that mimicked the functionalities of PC-based ransomwares. The first such malware was detected by Dell SonicWALL in May 2014. Called AndroidLocker, it locked down users' mobile devices, displaying what claimed to be a warning from the FBI for viewing, storage, and/or dissemination of banned pornography. The ransom note demanded the user pay a "fine" within a certain time frame to avoid criminal charges. If the user paid, the phone was unlocked.[6]

The next evolution came just a few weeks later. Called Simplelocker, it used the same scareware language as AndroidLocker (pornography distribution), but also incorporated two new features:

1. It encrypted all user files stored on the mobile device's SD card, including documents, images, and videos.
2. It used the Tor anonymity network for its Command and Control communication. This was the first-ever Android malware family to perform file encryption and use Tor for its communication.[7]

Meanwhile, we also began to see the first Android Remote Administration Tools (RAT) attacks, AndroRAT and Dendroid.[8]

Android and iOS malware also began to target specific populations and types of devices. In June 2014, Dell SonicWALL detected an Android Trojan targeting Korean banks. When users would download the malware, it would appear in their app drawer as "googl app stoy." If opened, it would show an error message, shut down, and seemingly uninstall itself. However, it was secretly still running in the background, specifically monitoring Korean financial apps.[9] A similar malware variant emerged the following month.[10]

ANDROID ATTACKS OF 2014

AndroidLocker
SimpleLocker
AndroRAT
Dendroid
Windseeker
Wirelurker

"**WireLurker** and similar apps point to a **trend we can expect to emerge in 2015 —** malware targeting wearables, TVs, and other ancillary devices."

The Chinese were also specifically targeted by smartphone attacks, first with an instant messenger app called Windseeker[11] and then with iOS malware called WireLurker.[12]

WireLurker was packaged with desktop Mac applications downloaded from Chinese third-party app store Maiyadi. When an iOS device was connected by a USB cable, WireLurker would infiltrate the mobile device and steal call logs, contacts, and other personal data. Another version of the malware would copy certain apps from jailbroken iPhones onto their paired Macs in order to infect those apps with the malware and then copy it back to the smartphone.

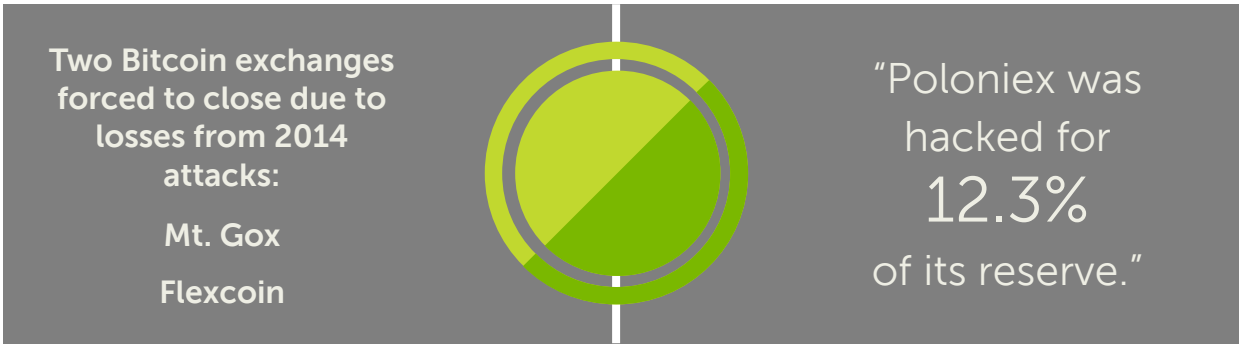
WireLurker and similar apps point to a trend we can expect to emerge in 2015—malware targeting wearables, TVs, and other ancillary devices. The pairing of these devices to laptops and smartphones will give hackers an easy attack vector, and these devices will become much more enticing as the market grows in the coming months.

6 Digital currencies including Bitcoin will continue to be targets of mining attacks.

In February 2014, Tokyo-based Mt. Gox, the world's largest Bitcoin exchange, suddenly went dark, shutting down its website and deleting its Twitter feed. As the dust settled, the company revealed that about 850,000 Bitcoins, worth $450 million, had gone missing and were likely stolen. 200,000 Bitcoins were later recovered, but Mt. Gox was forced to liquidate its remaining assets and close.[13]

Mt. Gox wasn't the only Bitcoin exchange targeted in 2014. Poloniex was hacked for 12.3% of its reserve, while Flexcoin was hit so hard that, like Mt. Gox, it had to close.[14] The hacks have continued into 2015, with Bitstamp temporarily suspending service to investigate a breach in January.[15]

The difficulty of tracing a Bitcoin mining attack is what makes it so enticing for cyber thieves. Bitcoin is a cryptocurrency that has built its demand on the foundation of being untraceable and anonymous, so victims don't always come forward when a breach occurs. In addition, traditional currency stolen from a bank account typically has to be transferred to another registered bank account, whereas Bitcoin theft requires no such digital trail.



A few Bitcoin-targeted malwares emerged throughout 2014, including a ransomware called Bitcrypt and a Trojan called Coinstealer. Although each of the year's attacks, particularly the one on Mt. Gox, crippled Bitcoin prices, the number of Bitcoin wallets has continued to grow and is expected to reach 12 million by the end of 2015. By that time, the number of vendors accepting Bitcoin is expected to be more than 140,000.[16] Where there's demand, there are cyber thieves, so we can expect attacks on exchanges and individual Bitcoin wallets to continue throughout 2015.

7 Home routers and home network utilities will become targets and will be used to assist large distributed denial-of-service (DDoS) attacks.

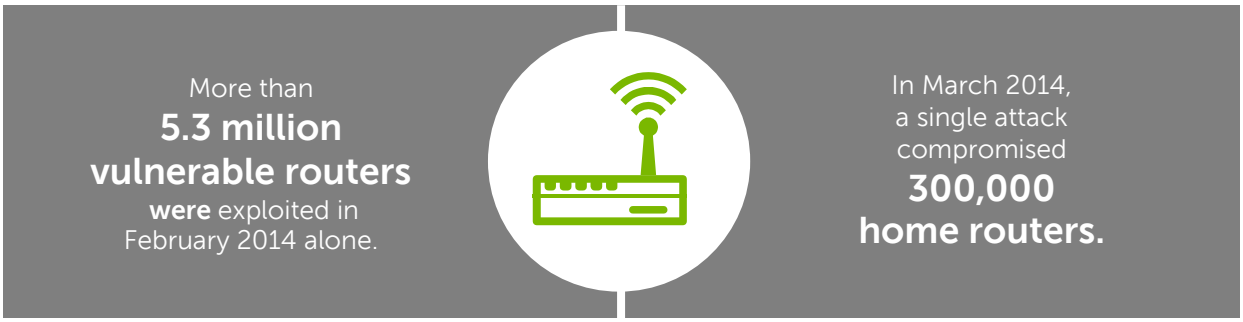
Domain-name-system-based (DNS) DDoS amplification attacks increased significantly in 2014, with more than 5.3 million vulnerable routers exploited in February 2014 alone. DNS applications provider Nominum estimates that 24 million routers have open DNS proxies, exposing Internet service providers (ISPs) to further DDoS attacks in the future.[17]

DNS amplification attacks are growing in popularity, largely because they're so easy to execute. Home routers mask the attack target, making it difficult for ISPs to trace the attack to its final destination.

In March 2014, a single attack compromised 300,000 home routers, many of which had administrative interfaces that were accessible from the Internet.[18] Consumers and businesses with home offices need to take a few steps to protect home routers against attacks like these:

- Set your own password, as default passwords can make it easy for thieves to compromise your router along with others of the same model.

- Check your router manufacturer's website for any firmware updates.
- Disable remote management of your router over the Internet or restrict remote access to certain, trusted IPs.
- Do not use a LAN's default IP address ranges.
- Log out every time you access the router interface.
- Check the router's DNS settings frequently to make sure they haven't been modified.
- Use SSL to access the router's Web interface, if possible.[18]



8 Electric vehicles and their operating systems are targeted.

The electric vehicle market may not be growing by leaps and bounds yet, but with more automakers entering the field each year, an electric future still feels imminent.

As we've seen with other technologies that gained widespread adoption, this means electric cars will inevitably be targeted by hackers, especially as Apple and Android operating systems are integrated into their dashboards.

Apple's iOS-based CarPlay standard and Google's competing Android Auto standard (and soon a version of Android that can be built directly into cars) are paving the way for automakers to offer more sophisticated in-vehicle connectivity. Just as smartphone malware has begun to mimic desktop variants, we can expect to see attacks on electric vehicles start simply, but evolve over time.

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 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 the **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 policies that grant 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 2FA for both administrators and users.
    d. Protect privileged accounts.
    e. Manage contractor, partner, intern, patient, and vendor access differently than internal resources. Control and monitor access rights regularly.
3. Replacement of 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. Implementation of an 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 of remote work environments by segmenting router access.
10. Implementation of 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. Seek knowledge 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 Dell Security Annual Threat Report empowers organizations of all sizes to become more prepared, informed, vigilant, and successful in preventing attacks throughout 2015.

Resources

1 Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It, "Bloomberg Businessweek, March 13, 2014, http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

2 Gene Marks, "Why The Home Depot Breach Is Worse Than You Think," Forbes, September 22, 2014, http://www.forbes.com/sites/quickerbettertech/2014/09/22/why-the-home-depot-breach-is-worse-than-you-think/

3 Katie Lobosco, "Michaels Hack Hit 3 Million," CNN Money, April 18, 2014, http://money.cnn.com/2014/04/17/news/companies/michaels-security-breach/

4 Dell, "2014 Global Technology Adoption Index 2014," November 2014, http://www.dell.com/learn/us/en/uscorp1/corporate~secure~en/documents~gtai-executive-summary.pdf

5 Douglas Macmillan, "Yahoo Ads Are Targeted in Malware Attack," Wall Street Journal Blog, January 6, 2014, http://blogs.wsj.com/digits/2014/01/06/yahoo-ads-are-targeted-in-malware-attack/

6 "AndroidLocker ransomware targeting Android phones," SonicWALL Security Center, May 15, 2014, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=679

7 "First TOR-based file encrypting Android Ransomware," SonicWALL Security Center, June 10, 2014, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=688

8 "Source Code leaks for Android RAT Dendroid," SonicWALL Security Center, August 29, 2014, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=718

9 "Android banking Trojan targets Korean users," SonicWALL Security Center, June 30, 2014, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=697

10 "Another Android Trojan targeting Korean banks," SonicWALL Security Center, July 18, 2014, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=702

11 "Android Windseeker with injection and hooking mechanisms," SonicWALL Security Center, October 3, 2014, https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=734

12 Jeremy Kirk, "Chinese iOS devices fall prey to invasive WireLurker malware," PC World, November 6, 2014, http://www.pcworld.com/article/2844292/apple-mobile-devices-in-china-targeted-by-wirelurker-malware.html

13 "Mt. Gox," Wikipedia entry, various sources, http://en.wikipedia.org/wiki/Mt._Gox

14 Alex Hern, "Bitcoin bank Flexcoin closes after hack attack," The Guardian, March 4, 2014, http://www.theguardian.com/technology/2014/mar/04/bitcoin-bank-flexcoin-closes-after-hack-attack

15 Ms. Smith, "Beginning 2015 with a bang of 3 breaches: Bitstamp, Morgan Stanley, Chick-fil-A," Network World, January 5, 2015, http://www.networkworld.com/article/2864856/microsoft-subnet/beginning-2015-with-a-bang-of-3-breaches-bitstamp-morgan-stanley-chick-fil-a

16 "State of Bitcoin 2015: Ecosystem Grows Despite Price Decline," CoinDesk, January 7, 2015, http://www.coindesk.com/state-bitcoin-2015-ecosystem-grows-despite-price-decline/

17 "24 million home routers expose ISPs to massive DNS-based DDoS attacks," Nominum, April 2, 2014, http://nominum.com/news-post/24m-home-routers-expose-ddos/

18 Lucian Constantin, "Attack campaign compromises 300,000 home routers, alters DNS settings," PC World, March 4, 2014, http://www.pcworld.com/article/2104380/attack-campaign-compromises-300000-home-routers-alters-dns-settings.html

For More Information

About Dell

Dell Inc. listens to customers and delivers innovative technology and services that give them the power to do more. For more information, visit www.dell.com.

If you have any questions regarding your potential use of this material, contact:

Dell
1 Dell Way
Round Rock, TX 78682
www.dell.com

Refer to our Web site for regional and international office information.