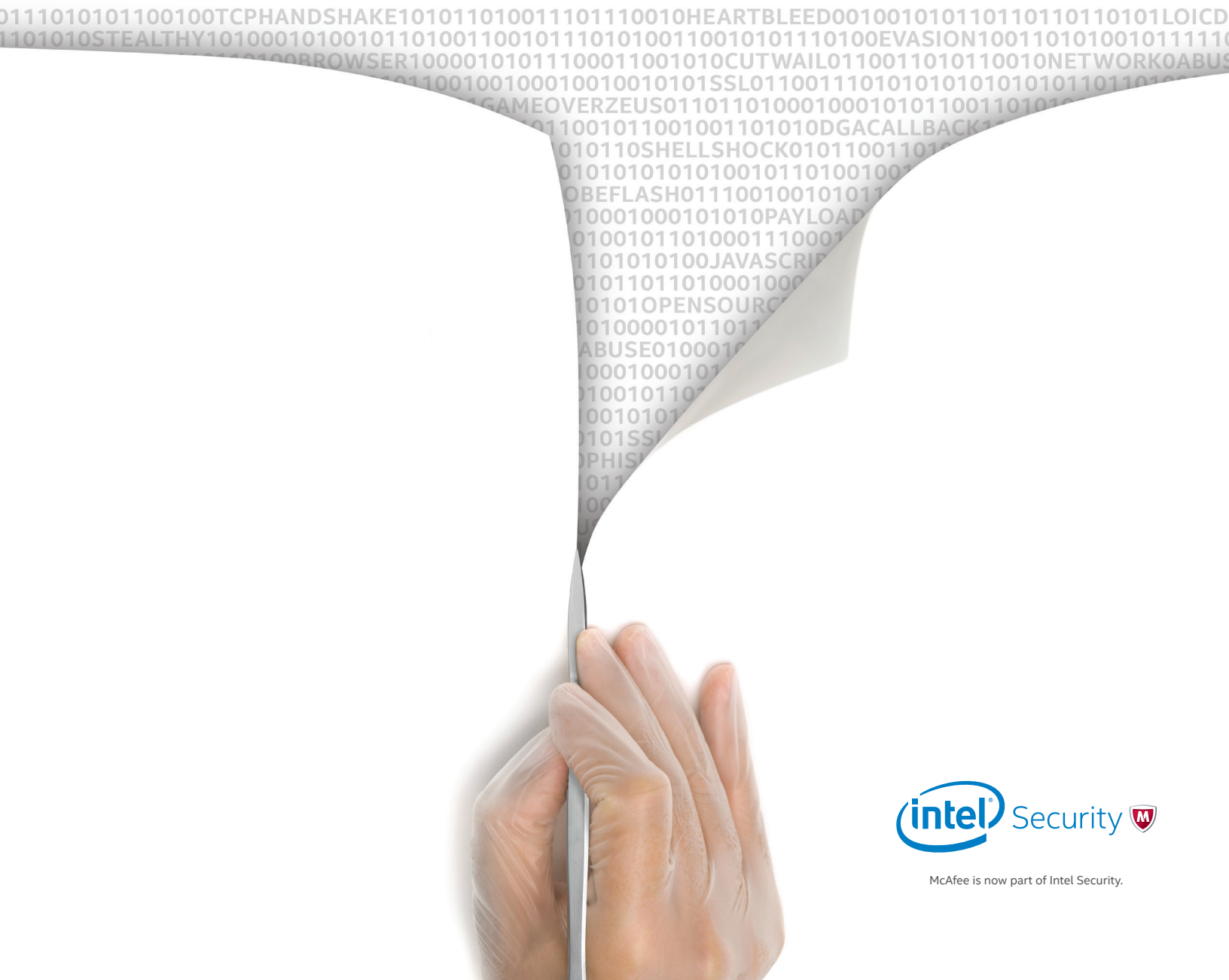
Report

Dissecting the Top Five Network Attack Methods: A Thief's Perspective.



intel Security

McAfee is now part of Intel Security.

Time to Understand What—and Who—You're Dealing With

According to our analysis, data breaches and their aftermath are commonplace, with no signs of slowing. The threats you face today are created by savvy criminals leveraging advanced techniques to surgically target network openings you may not know you have. And while the situation is serious, with certain smart network changes and a healthy-dose of 'knowing your enemy,' the prognosis is quite good.

The More You Know, the Stronger You Grow

This report offers forensic insight into five of the most common network attack methods that data thieves love to use. It also provides practical guidance on how criminals view your network, how to use that information to maintain a dynamic security profile, and ways to minimize the likelihood of a breach and its injurious repercussions.

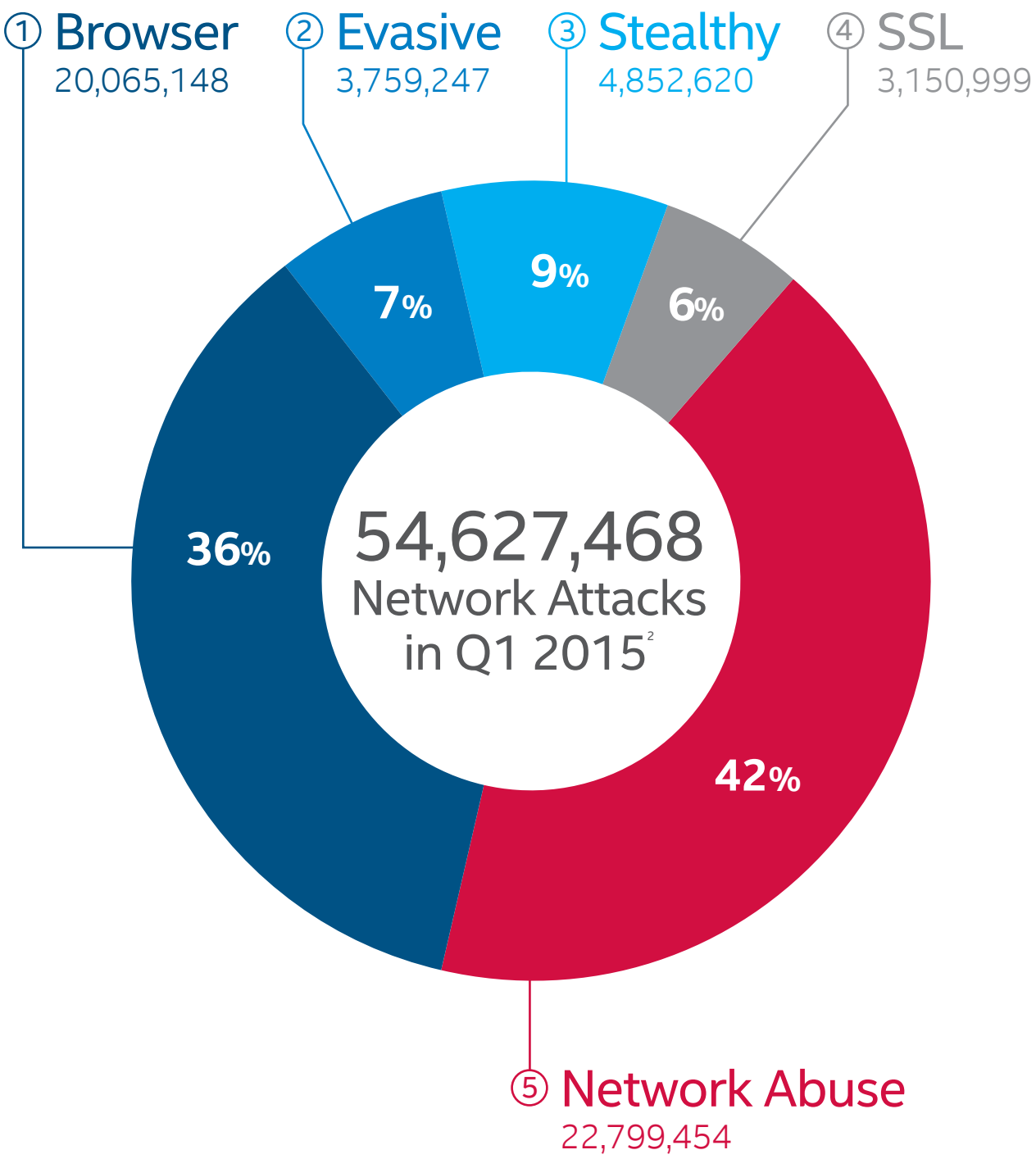
Big Numbers That Don't Add Up

76% of Black Hat attendees see advanced malware as a big or huge problem.[1]

Attendees who spend 10 hours or more a week fighting threats.[1] **37%**

Top Network Attack Methods

There were over 54 million network attacks in Q1 2015 alone.[2]



1 Browser Attacks

You See a Browser, They See a Door

Thieves know that when your employees use the web, security decisions shift away from IT. That's why they use lots of phishing emails, social engineering, and drive-by browser downloads aimed at tricking less-savvy employees into divulging data. It's a numbers game—sooner or later, somebody succumbs to it.

So instead of buying more static, bolt-on security solutions, embrace a security solution that's dynamic. One that can grow as security needs change, and can get stronger by learning what needs protecting and why.

87% Growth

Suspect URLs skyrocketed between 2013 and 2014.[3]

82 Million

new suspect URLs were found in 2014.[3]

A Thief's Perspective

"Seems I can always get through the next new product that is supposed to stop me. It's often not about the technology but the user. They're just so easy to trick."

Hacker Profile:
Crafty

Skillset:
JavaScript, Flash, and Social Engineering

Attack Method:
Browser

Motivation:
Building Bot Armies

What You Need to Know

The Hallmarks of a Browser Attack

- **The Less-Savvy, the Better**
  Hackers know that your web users—not necessarily security pros—come in direct contact with malicious web content.
- **The Malware is Well Hidden**
  Browsers discretely cache files and other content to improve the user experience, meaning malware is rarely obvious to the uninitiated.
- **The Unaware Get Exploited**
  Attackers leverage this reality to covertly transfer malicious payloads and execute malware scripts.

Save Your Employees from Themselves

- **Minimize Wrong Turns**
  Start with web content and URL filtering. It keeps users safe from the darker corners of the web—and helps you set policy, too.
- **Go Deep on Analysis**
  Stay ahead of the latest attacks by intelligently finding malware that hides in feature-rich browser content like JavaScript and Adobe Flash.
- **Understand Intent**
  For maximum protection, embrace simulated browser environments called emulation. These technologies allow immediate understanding of an inbound file's intent.
- **Shift the Big Picture Paradigm**
  Minimize reactionary spending. Future-proof your security by embracing a next-generation solution that grows with your needs.

2 Evasive Attacks

If There's a Crack, They'll Find It

No doubt, security solutions are more sophisticated and intelligent than ever. Unfortunately, attackers are too. Wiley thieves use evasion techniques that challenge network security like never before, exploiting weaknesses at every level of the infrastructure.

Criminals and their evasive techniques confuse network devices, bypass inspection, or cloak their existence. Data thieves have an insatiable appetite for evasive innovation, and they know the best way to defeat security defenses is to not fight them at all.

22%
of CIOs and security managers say their networks were breached in the last 12 months.

40%
of those breached think AETs played a key role.

YET[4]

63%
have trouble convincing top managment that AETs exist and are costly.

39%
lack methods to detect and track AETs.

A Thief's Perspective

"Most of my targets don't believe evasions are a concern. Out of sight, out of mind—just like my attacks. Their mistake is my gain."

Hacker Profile:
Innovator

Attack Method:
Evasive

Skillset:
Networking, Malware Creation

Motivation:
Endpoint Control or Botnet Creation

How Attackers Evade Your Security

- **They Hide During Network Delivery**
  Using advanced evasion techniques (AETs), crafty attackers avoid network detection by breaking up file (malware) packets into hard-to-inspect patterns.
- **They Go Dormant During Analysis**
  To evade sandboxes—closed security environments that closely analyze the behavior of a suspect file—malicious files know when they're in one, and remain silent.
- **They Stay Covert During Callback**
  Once on the endpoint, sophisticated malware avoids abnormal behavior or uses randomized callback connections to evade security devices and continue malicious activity.

Don't Let the Cheaters Prosper

- **Find the Hidden Delivery Patterns**
  Continuous tracking and inspection of network sessions from beginning to end allow the complex patterns of evasive connections to be found and blocked.
- **Step-Up the Analysis**
  Inspection of latent file code in malware empowers a sandbox to find hidden malicious behaviors and strengthen detection rates.
- **Call-Out the Callback**
  Intelligent connection tracking allows covert callback patterns to be learned and blocked. Connecting network traffic to originating endpoint processes helps pinpoint malicious connections typically missed by less-intelligent approaches.
- **Look for Proven Expertise**
  As you plan your defense, implement technology and solutions with a proven, quantifiable track-record in thwarting evasive attacks. There really is no substitute for experience.

3 Stealthy Attacks

Getting to Know All about You

Last year, hackers made an estimated $2.5 billion in revenue from online criminal activity.[5] With that kind of payoff, the incentive to breach your network has never been higher.

As a result, extremely complex, advanced threats have cropped up that seemingly overcome any siloed solution you can throw at them. They know your weaknesses, understand every aspect of your security posture, and expertly conceal their identity. Stopping them requires a coordinated effort across your entire security network.

1,367
confirmed security breaches in 2013.[6]

Lost Intellectual Property
Almost four companies a day lose their intellectual property.[6]

A Thief's Perspective

"I love breaching a company that spends tons of money on gear but can't get it working together. I know I leave traces, but by the time the admins connect all the dots, I'm long gone."

Hacker Profile:
Revenue

Attack Method:
Stealthy

Skillset:
Breach Planning and Development

Motivation:
Your Intellectual Property

Signs of a Stealthy Attack

- **Deception Is Commonplace**
  Stealthy attacks masquerade their intent until reaching the endpoint target.
- **They Do Their Homework**
  Months of research give the attackers a thorough knowledge of the network and infrastructure.
- **Beware the Personal Device**
  Attackers leverage BYOD (because they're less protected) to penetrate the protected network from the inside.
- **They Count on Info Overload and Siloed Security**
  Breaches are allowed to fester as overworked IT staff often miss the faint signals of these targeted attacks.

The Shut-Down Strategy

- **Find the Unknown Attack**
  Sandbox technology helps understand intent of inbound files to help find unknown and stealthy malware.
- **Correlation is Critical**
  All perimeter network security devices need to communicate with sandboxing technologies to close the gaps.
- **Create a Cohesive Protection System**
  All security devices should break down data silos by sharing and learning from each other in real time.
- **Think Beyond the Box**
  While individual technologies can identify attacks, only a connected approach that shares and learns context will help stop advanced threats and breaches.

4 SSL Attacks

Sometimes, They Hide in Plain Sight

When it comes to stopping attacks, visibility is everything. While SSL and encryption have been the basis of secure communications, they have also enabled new avenues for attackers.

The way the thief sees it, using existing encrypted channels already available within your network is a great way to obscure attacks from detection. So hackers essentially turn your defenses against you. Stoppable? Yes. But you need to strike a balance between proper inspection capabilities and network performance, which can be tricky.

24 Million

SSL attacks detected by McAfee in 2014 alone.
SSL attacks sky-rocketed in Q3 and Q4 of 2014 most likely due to the massive Heartbleed outbreak.[7]

A Thief's Perspective

"Why not hide in encrypted traffic? Most companies don't have the right equipment to inspect it. Since they can't see it, I can even use easy attacks."

Hacker Profile:
Efficient

Skillset:
Encryption, Application Vulnerabilities

Attack Method:
SSL/Encrypted

Motivation:
Financial Gain

A Survey of the SSL Landscape

- **The Problem is Growing**
  As more business applications (cloud, social media) embrace encryption, hackers have plenty of places to hide.
- **They Sidestep On-Premises Inspection**
  Malicious files and payloads can be delivered via encryption, thereby bypassing on-premises inspection.
- **You Get a Wolf in a Sheep Suit**
  Attackers become more efficient as simple, rudimentary attacks gain new life when delivered over SSL connections that can't be inspected.

The Strategy to Stay Safer

- **Combine Visibility and Integration**
  Bottom line—you need greater visibility into encrypted traffic.
- **Take a Balanced Approach**
  Being able to inspect encrypted traffic shouldn't come at the price of network performance. Throughput on important network segments should not suffer.
- **You Need to Mix It Up**
  SSL inspection integrated with other security technologies provides advanced inspection of hidden attacks.

5 Network Abuse

They Like to Hit You Where It Hurts

Odds are, a good portion of your day-to-day operations rely on the Internet to pump data and drive business. So if your website disappeared today, how much of an impact would that have?

Significant pain? Sure. Thieves know it, too. That's why Network and Resource Abuse remains one of the most common types of network attack. Additionally, proper detection can become a challenge. Since an attacker uses standard traffic in a malicious way, there's nothing abnormal about the traffic itself. You've got to keep your eyes peeled.

109 Million

DDoS attacks were detected in 2014.[8]

62 Million

abusive Brute Force attacks were detected in 2014.[9]

A Thief's Perspective

"For $6 in Bitcoin, I can rent time on a DDoS tool and bring down most websites. Better yet, if I send just the right type of packet to their web servers, I can crash the site for free."

Hacker Profile:
Smash and Grab

Attack Method:
Network Abuse

Skillset:
Networking and Webservers

Motivation:
Hactivisim or Distraction

Signs of Abuse

- **The Unwelcomed Guest**
  In a DDoS attack, a server receives a flood of connect requests or specially crafted connection requests.
- **You Get Spread Thin**
  Resources on the server are overwhelmed or completely fail, rendering it unable to handle normal traffic.
- **The Real Motivation**
  DDoS attacks can often be used by hackers to distract IT administrators as they slip in the back door.
- **You Get Held Hostage**
  Usually criminal in nature, DDoS attacks can sometimes come with an accompanying ransom request.

Protect Yourself

- **Understand Your Traffic**
  On-premises, deep-packet inspection is needed to completely understand the abusive traffic hitting your web server.
- **Pay Attention to the Volume**
  You need volumetric analysis to see small and often disguised changes in traffic patterns.
- **Get Complete Visibility**
  You need SSL visibility as attacks often hide in encrypted traffic.
- **Be Efficient and Smart**
  Combine the power of abuse traffic filtering with top-end inspection technologies to deliver the best protection solution.

We're All in This Together

With new breaches announced regularly, the current security reality is that organizations are struggling for answers. It's time to shift your perspective and rethink network security, period.

What's New Isn't Always What's Best

At the very least, we all need to participate in the discussion. Understanding what we're facing and how we can combat these five attack methods is key. What doesn't work is getting caught in the 'shiny new toy' syndrome. Adding more gear won't reduce the number of threat vectors. You're much better off developing communication and coordination among the security solutions you already have.

We Can Thwart the Thieves

Since threats are constantly changing, you need to embrace a platform that supports growth with your needs. And when you shop for that platform, be sure to choose a vendor that invests in technology and has a proven track record of success.

Learn More

To see what kind of innovation is going on at Intel Security, we urge you to check us out at www.intelsecurity.com/network. Or at the very least, use the information here to begin the very necessary discussions among your business constituents. Join the discussion #ThiefsPerspective.

Follow Network Security

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world.

www.intelsecurity.com

1. Based on an Intel® Security survey of 2014 Black Hat conference attendees.
2. McAfee Labs Q1 2015 Threat Report.
3. McAfee Labs Q4 2014 Threat Report.
4. http://www.mcafee.com/us/resources/reports/rp-security-industry-dirty-little-secret.pdf
5. http://www.darkreading.com/russian-hackers-made-$25b-over-the-last-12-months-/d/d-id/1316631
6. Verizon Data Breach Report 2014.
7. McAfee Labs Q4 2014 Threat Report.
8. Ibid.
9. McAfee Labs Attack Data, Q1-Q4, 2014.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com