IBM Software
Thought Leadership White Paper

April 2014

What's behind a cyber attack?

Gaining insight and clarity into the what, when and how of an enterprise security incident

IBM

Contents

Introduction

Breaches happen. In today's high-value, high-stakes enterprise environments, many organizations rightly assume not only that their data and computing systems will be attacked, but that a certain number of attacks will succeed. One study found, in fact, that 97 percent of organizations have experienced malware attacks.[1]

But recognizing the problem is only the first step—because the corollary to the assumption that future attacks are coming is the recognition that past attacks have already gained entry. So now what do you do? How do you learn the what, when and how of a security incident—and what its potential damage could be? The answers to these questions are critical to remediating damage and improving defense.

When investigating a breach, organizations need better visibility and clarity into network activity. And they need it fast. A recent study by Verizon Communications found that in 66 percent of cases, discovering a breach took months,[2] during which time organizations faced potential damage to business operations, private data, intellectual property and brand image.

The challenge to avoiding damage stems from the complexity of using existing solutions for security-related data collection and breach investigation. With conventional solutions, gaining the necessary information and insight has been time consuming and difficult—if not impossible. Meanwhile, attackers employ increasingly sophisticated techniques and find surprising ease of success. Despite enterprise defenses, the Verizon study described 78 percent of initial intrusions as "low difficulty."[2]

This white paper will examine the shortcomings of conventional breach investigation approaches and present IBM® Security QRadar® Incident Forensics, a fast, simple and comprehensive solution designed to help organizations defend against advanced persistent and internal threats, including fraud and abuse.

Using QRadar Incident Forensics, organizations can reassemble raw packet traffic data back into its original form for simplified analysis, and retrace the step-by-step actions of a potential attacker to help discover and remediate security incidents and reduce the chances of data exfiltration or recurrence of past breaches.

Attackers have an advantage—but they leave a retraceable trail

Theories of warfare call it an "asymmetrical advantage"—when the power, strategies or tactics of one army differ significantly from the other's. It's an appropriate term for the state of enterprise security today. Enterprises and cyber attackers are at war. And they are operating with vastly different requirements, expertise and motivations in mind.

The typical enterprise infrastructure contains thousands of devices and applications, an untold number of increasingly complex connections, and an undetermined number of unprotected vulnerabilities. To be successful, the external attacker or rogue insider needs to exploit only one weakness. The enterprise must address them all—and if the protection measures don't work, it must find, track and remediate exploits that could be anywhere.

As a result, enterprises face an enormous task. The tracking database maintained by IBM X-Force® research and development, which has collected data on 78,000 publicly disclosed security vulnerabilities, added 8,330 new vulnerabilities in 2013 alone.[3] In the one-year period ending March 2013, malware aimed at mobile platforms became a new attack vector that grew 614 percent, nearly 450 percent faster than a year earlier.[4]

On the side of the defenders, every action on the network—whether from inside or outside the organization, authorized or unauthorized—can be captured and analyzed as part of a security incident. Following these digital impressions can potentially reveal vulnerabilities, the actions an attacker takes to exploit them and the source of the attack. Many organizations have deployed traditional solutions, such as log management and security information and event management (SIEM) applications, that give them the basic capabilities for gathering log source events and netflow data, but lack full packet captures (PCAPs), which provide richer network context.

Yet SIEM applications yield mountains of data not only from attackers but also from legitimate users—and most organizations have neither the time nor the resources to sift through it all to find specific strings of incriminating characters.

Conventional forensics solutions can be challenging to use

- **Analysts must be skilled in network security investigations.**
- **Adding point security solutions with minimal integration typically increases complexity and cost.**
- **Determining where and how to begin an investigation can lead to lost productivity.**
- **Complex queries directed at packet capture repositories can be time-intensive, consume processing and storage resources, and fail to reveal the relationships necessary for remediation.**

Advanced forensics can increase the enterprise advantage

In an enterprise attack, intrusions and defense are not the only asymmetrical elements. Events in the attack timeline typically weigh in favor of the attacker as well. Verizon has found that nearly 85 percent of such events take place in seconds, minutes or hours—with 68 percent of exfiltration occurring in the same period. Yet 62 percent of discovery occurs only after *months* have passed. And 77 percent of the remediation effort—including patching, configuration changes and intrusion blocking—requires days, weeks or months, all of it occurring *after the initial discovery*.[2]

Clearly, greater speed is a necessity in responding to a cyber attack. It can be critical to know immediately how widespread any related breach becomes. Discovering which devices or applications are affected and constructing an event timeline can tell administrators exactly where and when to apply their remediation efforts. For example: if physical devices were compromised by a person on site, locating the devices and tracking breach events can point investigators to security cameras that could identify the suspect.

These defense operations are complex, however, and cannot be undertaken manually. Instead, organizations need comprehensive, automated tools for converting their network packet captures into indexed, searchable information. Security teams can then use this information to rapidly determine threats and their characteristics, distinguish true attacks from false positives, and formulate proactive best practices for future actions based on a clearer understanding of the attack.

Using an advanced network forensics solution, investigators can have a fuller view of the trail of events in an attack, with identifying components such as IP and MAC addresses, application protocols, webhosts, user queries and SSL certificates. They can identify stolen data, such as Social Security or credit card numbers. And they can gather information that can help identify the source of the breach—whether an external attacker or an insider using proper authority for malicious purposes.

Emerging threats require clarity to detect and resolve

An advanced network forensics solution can give security analysts clarity of content, relationships and event sequence to resolve incidents. For example:

- **Network security—A retailer needed to detect unauthorized duplication of customer payment data from point-of-sale (POS) systems to compromised internal systems.**
- **Fraud and abuse—A financial firm needed to uncover a sophisticated money-laundering scheme involving multiple seemingly unconnected interactions.**
- **Insider threat—A manufacturing firm needed to find the perpetrator, identify collaborators, and pinpoint the systems and data involved in stolen intellectual property.**
- **Evidence gathering—A security research firm needed to compile evidence against a malicious entity involved in breaching a secure system and stealing data.**

Advanced forensics can enable a comprehensive security approach

In an effort to stop attacks and breaches, as well as comply with government and industry security regulations, many organizations have deployed network forensics solutions. In many cases, however, the security solutions they choose are point products that provide insights and responses that are dependent upon the skills of technically trained analysts.

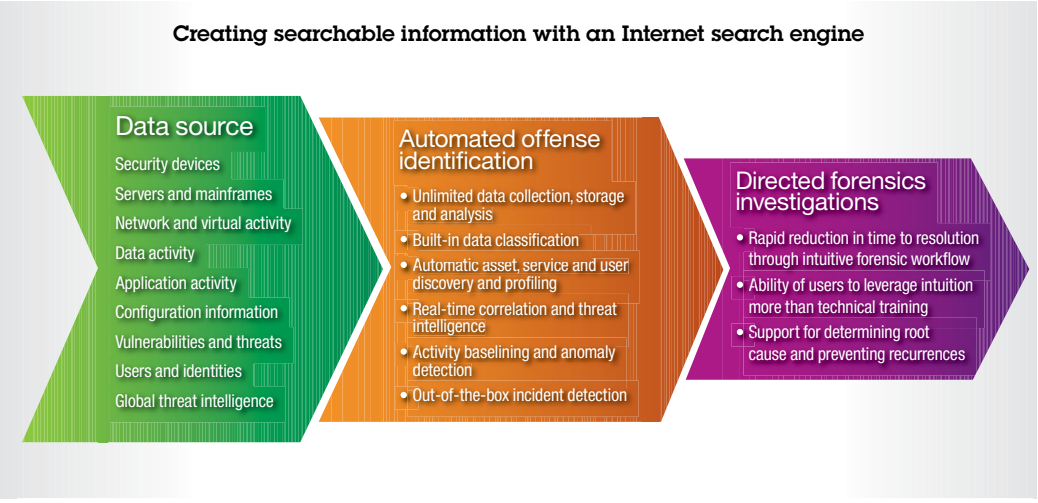
Such an approach treats network forensics as a job for simple PCAP searches. But the serial deployments that result—layering one point solution on top of another as new capabilities become necessary—can obscure the organization's true network security posture with unnecessary complexity. A better approach is to deploy a comprehensive forensics solution that can investigate not only PCAP data in motion, but also documents, databases and other data at rest.

Using the advanced, comprehensive network forensics solution from IBM, QRadar Incident Forensics, investigators can not only gather network information, they can also proactively search for possible breaches based on alerts issued by the X-Force threat intelligence feed. They can find network relationships and help identify incident sources. Then, using security incident-related network data and insights to understand why certain attacks succeeded, they can more effectively eradicate malicious activities associated with a breach. Administrators can facilitate the production of evidence to support legal actions or fulfill compliance audits.

Ultimately, the IT security team can use information and insights from QRadar Incident Forensics to help develop effective countermeasures and security best practices—updating perimeter defenses such as firewalls, endpoint patches and applications, frequently tuning anomaly detection capabilities, and writing multilevel SIEM correlation rules and proactive measures that reduce false positives and better identify attacks.

Creating searchable information with QRadar Security Intelligence Platform

So how does QRadar Incident Forensics work? In a nutshell: It begins after a security incident when a security analyst defines a search or a case, retrieving all associated PCAP data, reconstructing each embedded file, and then creating multiple indexes using the file contents and metadata. These steps produce searchable information that security teams can retain for long-term investigations of the incident.



Based on its core extraction and correlation capabilities, QRadar Incident Forensics can support the three principal operations of network security investigations:

Security incident response

Once a security breach is discovered, QRadar Incident Forensics can enable investigators to follow the attacker's step-by-step actions in real time and develop a profile known as a *digital impression*—which traces a threat actor's previous and current activity. The resulting insights can help the security team quickly remediate the incident and develop countermeasures against further damage.

Alert triage

SIEM solutions normally generate a limited number of suspected security offenses and then correlate them with other available security data. QRadar Incident Forensics, however, enables the security team to further investigate each potential offense to determine whether it is an actual attack or a false positive result. With conventional forensics solutions, these investigations can take weeks to resolve, depending upon analyst skill levels and responses from identified users. But by automatically combining information from the SIEM reports with historical information from the investigation and resolution of previous incidents, QRadar Incident Forensics can help dramatically reduce the time required to complete each investigation.

Proactive, defensive data exploration

From time to time, security teams search their network to determine its security posture. These searches could be based on an alert received from a threat intelligence organization such as X-Force or an internal policy of planned security activities. In any case, a search can be streamlined and made more effective with the advanced QRadar Incident Forensics solution's simplified, search engine-like interface; categorization and filtering capabilities to reduce the volume of data returned; and pivot capabilities that enable a variety of search views.

Investigations can be more comprehensive and productive

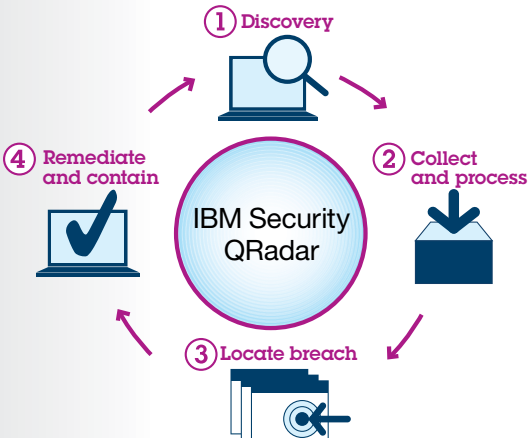
QRadar Incident Forensics is designed to help organizations rapidly and thoroughly investigate malicious network activity by providing visibility and clarity into network security incidents.

Available either as software or as a hardware appliance with software built in, the solution integrates seamlessly with IBM Security QRadar SIEM and IBM QRadar Security Intelligence Platform, as well as with most available third-party packet capture formats. The comprehensive approach gives IT security teams the ability to more easily and productively conduct investigations; make smarter, faster decisions by analyzing security data in the network context; and support effective remediation.

Using a search engine-like interface to handle data within or flowing through the network, QRadar Incident Forensics supports both incident-driven and threat intelligence-directed investigations to provide security teams with the underlying evidence that retraces digital impressions, categorizes external content and labels suspect content.

QRadar Incident Forensics indexes everything contained within the captured network traffic—ranging from documents to website images, and including the metadata and contents of both structured and unstructured data—to help reduce the time required to investigate offenses, in many cases from days to hours or even minutes. To enhance data intelligence and insights, the solution enables a powerful data pivoting capability for discovering and displaying extended relationships for searchable variables such as IP addresses, MAC addresses, email addresses, application protocols, SSL certificates and more.

Investigating security incidents with IBM Security QRadar solutions



1. IBM Security QRadar SIEM discovers an offense.
2. IBM Security QRadar Incident Forensics reassembles and indexes the data.
3. Administrators can use this data to construct digital impressions leading them to the incident location.
4. IT security teams can then assess the credibility of a true threat and use appropriate means to block the communication, patch the vulnerabilities, contain critical data in the event of an incident and remediate malicious actions to prevent a recurrence.

The result is a richer, big-data view of network data, application and malicious user relationships than is provided by traditional network forensic tools that can use only processed PCAPs. With the help of electronic breadcrumbs, investigators can follow the path of malware or attackers and retrace the chronological interactions of incident events, helping investigators understand how to remediate breaches to reverse actions and prevent recurrences. Organizations can also document regulatory compliance.

Security investigations can be faster and easier

Conventional security solutions require extensive training—in some cases, even the ability to write code—to navigate collected PCAP data, understand the data's meaning, and know what to do with it in order to remediate an attack and prevent future incursions.

QRadar Incident Forensics, on the other hand, gives virtually any member of the security team—even junior members without extensive knowledge of security data—the ability to determine the full network context of a security incident.

An intuitive, free-form query interface built into QRadar Incident Forensics means that a search for network security incidents is as easy to formulate as looking for sports memorabilia using any popular Internet search engine. With the forensics solution integrated into the single-console management interface of QRadar Security Intelligence Platform, access to the full set of forensics capabilities is only a point and click away. And full network searches, in many cases, take only minutes or hours due to extensive indexing, rather than the days or weeks required by other solutions.

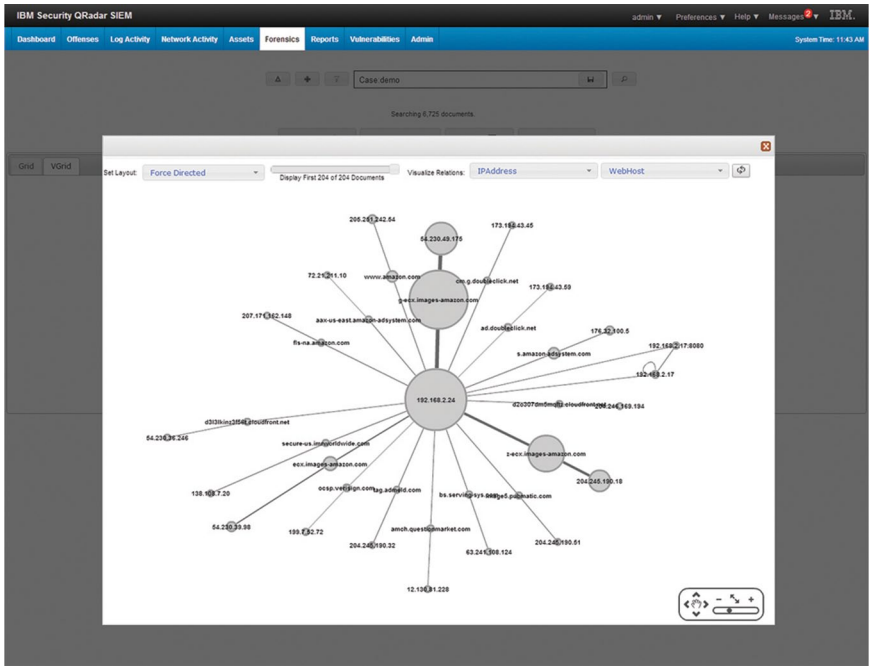
In many cases, QRadar Incident Forensics searches can make investigations faster and more comprehensive—helping identify data that may have been missed. Once the solution has retrieved and processed the raw PCAPs into rich document files, its search

engine uses network, file and personal metadata indexes to return fast keyword searches of structured and unstructured data. It can even search stored network documents. The solution's ability to provide information in context helps reveal threat levels and vulnerabilities. It generates multiple views of data that show relationships, timelines, and source and threat categories. And it enables users to refine searches with intelligent filtering for information such as IP and MAC addresses, application protocols or email addresses.

How security teams view information is important to success

Significantly, nothing on the network escapes the view of a directed QRadar Incident Forensics search case. A simple search for the word "confidential," for example, can not only locate all documents labeled as such, but it can also uncover all events that involve an externally leaked document, identify paths where a copy may have been sent, and reveal the individual who initiated those actions. Equally important, the solution can present information in a number of ways, allowing investigators to create the view that is best suited for the insights they need.

The interface allows security staff to simply click on metadata to locate related information. It further enables investigators to pivot searchable variables and change the metadata field to see extended and perhaps unsuspected relationships. Beginning with an email address, for example, an investigator can discover the associated IP address and Internet login ID, then use the combined information to achieve clarity on who the attacker is and the trail of the attacker's actions on the network.



Via IBM Security QRadar Incident Forensics, security teams can easily visualize relationships between suspect entities using IP addresses, email addresses, chat IDs and more.

The visibility and clarity provided by QRadar Incident Forensics is fundamental to an organization's efforts to eliminate and remediate security incidents. With more limited solutions, attacks can recur and malware can re-infect the infrastructure—because the security team missed an artifact of the attack.

Anatomy of an attack—and an intelligent response

Arriving at work, the enterprise security team discovers that its SIEM application found a number of new offenses overnight. Instead of working their way through the SIEM data manually, however, the team launches a QRadar Incident Forensics session with a simple click on the solution's tab on the QRadar Security Intelligence Platform console, which assembles all the relevant packet captures, performs extensive indexing, and returns detailed, multi-level search results quickly, in most cases in minutes—if not seconds.

From an extensive array of data, ranging from the IP address that originated the incident to a mailbox ID and a MAC address, the solution reveals metadata categories that provide identifying data for the attacker and the trail of events that the attack left on the enterprise network. Utilizing elements of the larger network context, the security team is able to determine whether the SIEM data reveals an actual attack or whether it is a false positive for an explainable event mistaken as an attack.

If the event is a false positive, the team knows to tune its SIEM correlation rules so similar incorrect results are not returned in the future. If the attack is real, the team can take immediate actions to remediate the threat and help avoid future incidents that use the same source or the same techniques.

Building intelligence can help in navigating investigations

Attackers and breaches grow smarter and more sophisticated daily. Organizations, in response, need smart defenses, made even smarter by the intelligence in their networks.

By finding and reconstructing security incidents on the network and presenting them in ways that support deeper interpretations, insight into root causes and support for remediation, QRadar Incident Forensics builds new intelligence for the defense organizations need. The solution follows electronic breadcrumbs left by attackers, identifies code injections or rogue asset additions, sees device configuration and firewall rule changes—and more. It achieves these defenses with three principal techniques: creation of digital impressions, identification of suspect content and categorization of network content.

Digital impressions

A digital impression is a powerful index of metadata that can help an organization identify suspected attackers or rogue insiders by following malicious user trails. In building these relationships, QRadar Incident Forensics can draw data from network sources such as IP addresses, MAC addresses and TCP ports and protocols. It can find information such as chat IDs, and it can read information such as author identification from word processing or spreadsheet applications.

A digital impression can not only help the organization discover the identity of an entity who attacked the network one time, but it can also help uncover associations by linking the entity's identity to identifying information for other users or entities, potentially revealing additional attacks.

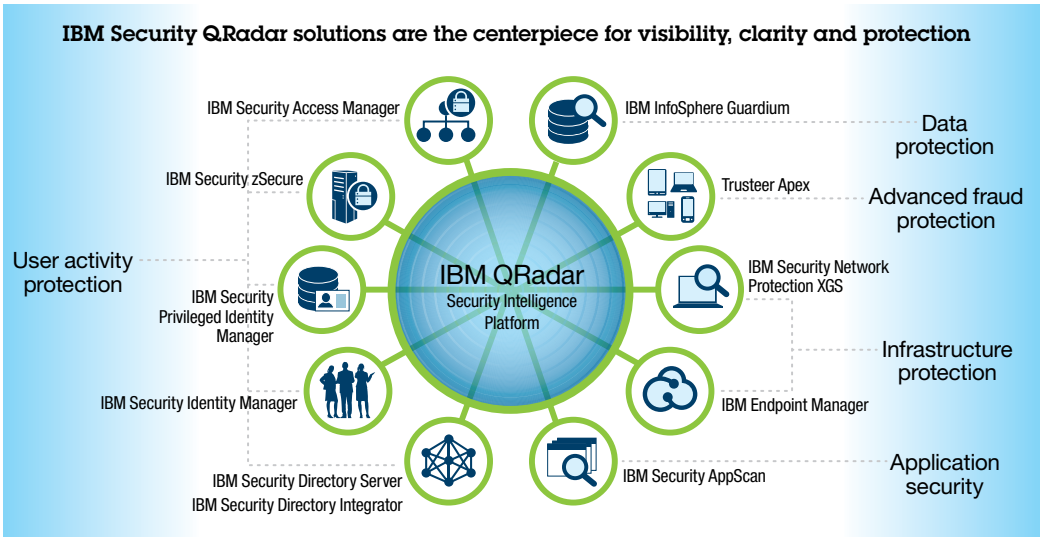
Content categorization

Categorizing where network traffic comes from and distinguishing between legitimate and malicious sources is key to protecting against breaches. Security research organizations such as X-Force maintain databases of URLs that track a location's reputation so that organizations can tell whether it might be the source of an attack it has suffered—or of a potential attack in the future.

Filtering and labeling data by category—for example, asking whether an attempt at network access is coming from a trusted business or a criminal organization—as well as limiting access based on metadata and correlating relationships between organizations can all play a role in keeping malware and harmful actions from breaching the network.

Suspect content

A data breach typically targets specific types of information—Social Security numbers, credit card numbers, medical IDs or intellectual property labeled "confidential," for example. QRadar Incident Forensics can help recognize those patterns of information (simply query "confidential" in the search engine) to quickly reveal theft, malicious damage or other activities that can harm the organization. The security team can then remediate the action and put into place measures designed to prevent its recurrence.



Conclusion

Today's sophisticated cyber attacks require a rapid and effective response based on all available intelligence about the what, when and how of the attack. The comprehensive and easy-to-use capabilities of IBM Security QRadar Incident Forensics can provide the visibility and clarity into a network security incident as well as insight into the extent of breach activities that the security team needs in order to remediate and prevent recurrences. Using QRadar Incident Forensics, organizations can also strengthen their documentation of regulatory compliance.

With insights gained through QRadar Incident Forensics, an IT security team can be well positioned to craft an action plan that leverages network intelligence and the organization's full security resources for a next-generation approach to security incident forensics that supports network security, insider threat analysis—including fraud and abuse—and the documentation of incident-related evidence.

For more information

To learn more about IBM Security QRadar Incident Forensics, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/services/us/en/it-services/security-intelligence.html

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
April 2014

Please Recycle

[1] Ponemon Institute, "2013 Cost of Cyber Crime Study: United States," October 2013. http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf

[2] Verizon RISK Team, "2013 Data Breach Investigations Report," *Verizon Communications*, April 2013. http://www.verizonenterprise.com/DBIR/2013/

[3] IBM X-Force, "IBM X-Force Threat Intelligence Quarterly – 1Q 2014," *IBM Security Systems*, February 2014. https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-WW_Security_Organic&S_PKG=ov21294

[4] Juniper Networks Mobile Threat Center, "Third Annual Mobile Threats Report: March 2012 through March 2013," *Juniper Networks*, 2013. http://www.juniper.net/us/en/local/pdf/additional-resources/3rd-jnpr-mobile-threats-report-exec-summary.pdf

WGW03056-USEN-00