September 2013

Combat the latest security attacks with global threat intelligence

Understand the context of attacks by leveraging insights from the IBM X-Force research and development team

Contents

Introduction

Security threats are very real, and the stakes are higher than ever on today's information-centric and interconnected world. Ever-growing numbers of attacks can affect—and originate from—any country in the world. And these attacks are becoming more dynamic, more complex and more malicious all the time.

In order to effectively combat security threats, organizations must first understand the sources of these threats. They need to know exactly what they're up against, including the origins, variations and methods of attack. But busy IT departments struggle to stay on top of the most current threat data, and to place it into a meaningful context. With today's large variety of incoming attacks, it can be extremely difficult to detect and analyze ever-changing threats, much less to turn collected data into insights that consistently identify the most dangerous threats—and then take action on those insights.

IBM offers a unique, preemptive approach to security—and at the heart of this approach is the IBM® X-Force® research and development team, one of the best-known commercial security research groups in the world. This elite team of security experts focuses on researching and evaluating the rapidly changing threat landscape, developing assessments and countermeasure technologies for IBM products, and educating users about emerging threats and trends.

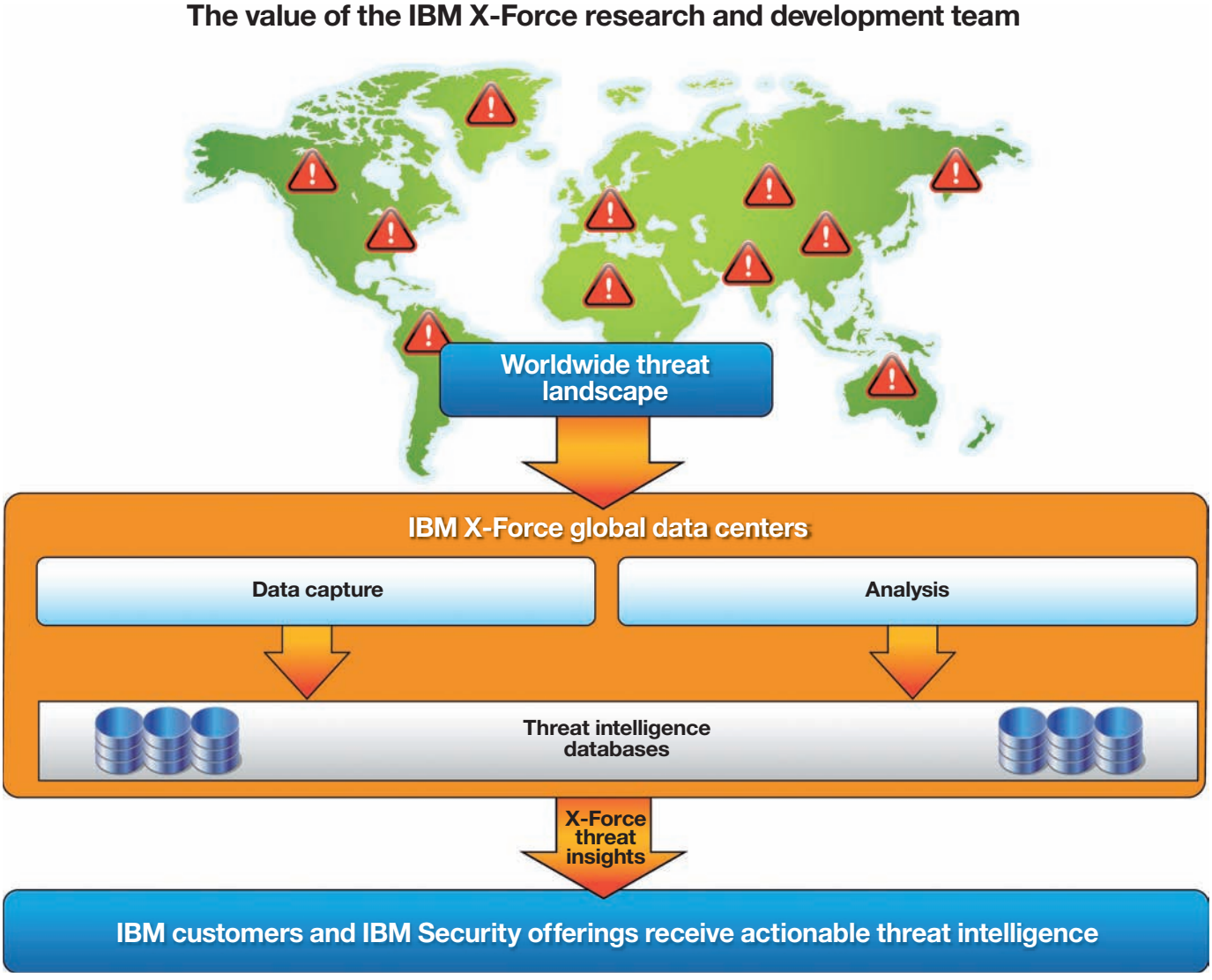
This white paper will discuss how the X-Force team collects, analyzes and distributes threat intelligence to IBM customers, as well as how this data is used to enrich the capabilities of the IBM Security portfolio. It will also describe different ways in which users can leverage this in-depth knowledge and understanding of threats to add immeasurable business value—in the form of superior threat protection—to their organizations.

Understanding today's global threats

Each day, tens of thousands of malware variants are created, with new classes of threats continually added and improved upon. Savvy attackers use polymorphic programs to alter malware into new form factors after each delivery. And all of this is exacerbated by the proliferation of mobile devices, cloud computing and virtualization—in fact, the intersection of these technologies provides fertile new ground for threats and malware.

Today's attacks are often not random, but targeted for maximum financial gain and impact. Rogue individuals and groups are constantly innovating new ways to attack organizations' critical data. As a result, traditional methods of dealing with threats are no longer enough. Organizations require visibility into a much wider range of threat data than ever before in order to effectively protect themselves. IBM X-Force Threat Intelligence can provide the additional insight organizations need to take on these modern-day threats.

The value of the IBM X-Force research and development team



Leveraging threat intelligence technologies

By monitoring global threats around the clock, understanding the latest vulnerabilities and exploit techniques, and updating the IBM Alert Condition (AlertCon) resource center in real time, the X-Force team works hard to keep IBM users abreast of the current global threat level at all times—delivering unequaled security research and threat mitigation technology.

URL/web reputation

While traditional web-filtering methods depend on manually compiled lists of sites to be blocked or individual ratings or algorithms that apply a set of rules based on experience, security has long since outgrown these methods. That's why the X-Force team uses a more comprehensive reputation process that automatically scans the entire web and categorizes each site using a combination of intelligent text classification, image recognition, linkage analysis and structural analysis. In addition, the categorization process handles multiple languages, and can sort URLs into multiple categories depending on subpages and instances of multiple hosts on the same domain.

Fully automated web crawlers inspect millions of new and updated sites every day. All sites are categorized automatically using advanced technologies and an infrastructure that provides the power necessary for this process. The result is a database that is continually updated—reflecting well in excess of 100,000 changes every day. In addition, web content in the database is sorted into 69 different categories. X-Force users have access to this global URL reputation database, which contains well over a hundred million entries resulting from the inspection of tens of billions of web pages and images.

IP reputation

X-Force Threat Intelligence leverages the X-Force team's skills and infrastructure to provide users with additional insight into and context for security situations that involve IP addresses of a suspicious nature. IP reputation data uses threat data collected from myriad sources to categorize IP addresses into separate threat categories, including:

- Malware hosts
- Spam sources
- Dynamic IPs
- Anonymous proxies
- Botnet command-and-control servers
- Scanning IPs

Individual IP addresses are then assigned a reputation score to help determine the risk level for malicious activity. This score is designed to help users prioritize threats and determine which to address first. They can also use IP reputation data to look up IP addresses for security events affecting the traffic coming across the network; next-generation products can block any traffic, filtered by category and by user-defined thresholds. IP reputation data is updated every five minutes to provide IBM users with the most current data available.

In addition to data collected by the X-Force team, IBM also leverages third-party sources to augment its threat-intelligence capabilities. And because IBM recognizes that no single entity can be the paramount source of threat data, it continues to build an ecosystem of partners that can help provide clients with the most trusted, dynamic and up-to-date information.

Application categorization

With web applications becoming the most prevalent method with which to access the Internet, send and receive data, and communicate on social networks, it is imperative that organizations maintain an awareness of threats that originate with this software. By categorizing these applications, the X-Force team enables customers to apply appropriate security controls within

IBM security products. The X-Force team can detect a wide variety of web applications—and the actions that users take via those applications—including:

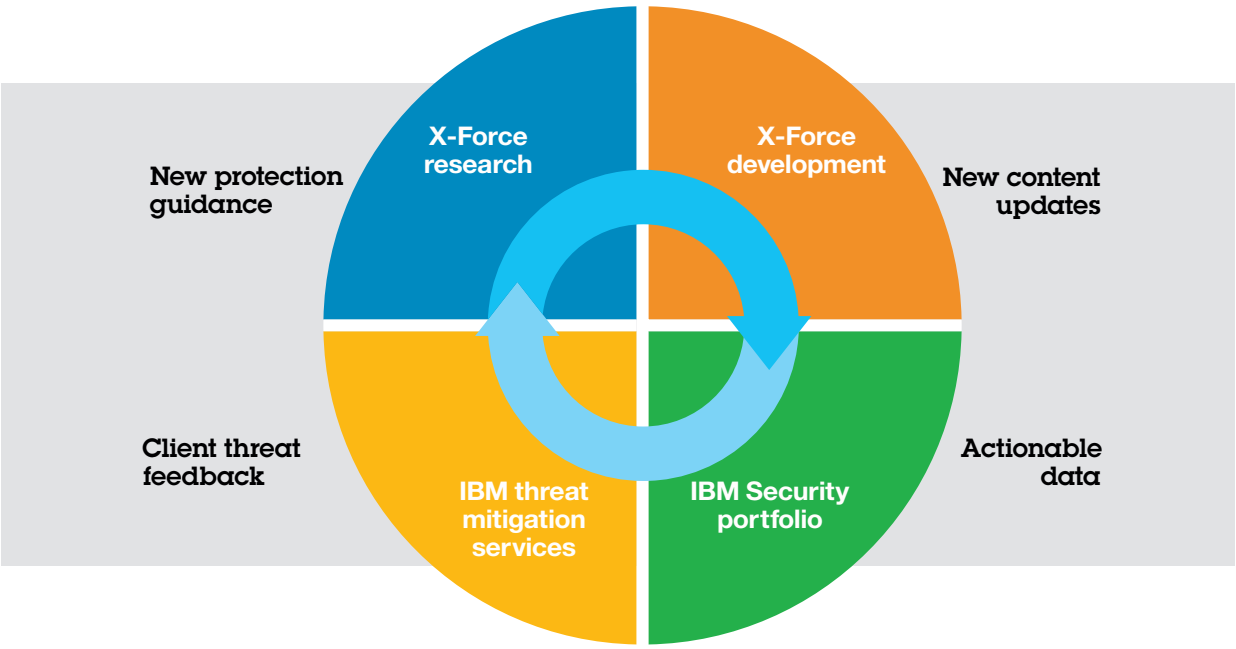
- Communicating via audio/video (A/V)
- Sharing items such as files, A/V streams or email attachments
- Starting third-party applications
- Streaming A/V
- Viewing, saving or downloading email attachments
- Writing, posting or chatting

The X-Force team can adapt to changes in actions for relevant applications in a matter of hours—an essential capability for handling the dynamic nature of Web 2.0 applications, which can release new software versions much more frequently.

Vulnerability tracking

The X-Force team is instrumental in protecting users against the threat of attack because their knowledge base and data-collection methods are unmatched in the industry. From a vulnerability perspective, the team maintains and analyzes one of the world's most comprehensive databases of known security vulnerabilities, with more than 75,000 entries, including detailed analyses of every notable public vulnerability disclosure since 1994. The team collects vulnerabilities from a variety of private and public research sources, including long-standing partnerships with leading software vendors. Overall, this effort enables IBM to understand and prioritize these vulnerabilities and apply the information to provide valuable product enhancements.

IBM X-Force intelligence lifecycle



Battling advanced persistent threats with X-Force insights

To address the types of threats encountered today, it's not enough to rely only on the security information gathered from a single organization. Nowhere is this more evident than with the class of attacks known as advanced persistent threats. These threats, while encompassing a wide range of techniques, have certain traits that can often be countered with global threat intelligence from the X-Force team.

For example, attacks of this type often utilize spear-phishing (email spoofing fraud attempts) as a point of access to targeted networks; once accessed, the goal is to connect the target to a malware host. X-Force Threat Intelligence can help preemptively stop this technique by:

- Blocking access to certain classes of URLs, based on web-filtering data
- Limiting access to the applications most likely to lead to a malware-infected site, using application control
- Helping to prevent the initial exploit from being effective, using vulnerability-based technology from an IBM network security appliance

The culprits behind these attacks are often working toward specific goals, potentially over long periods of time. After gaining a foothold in a targeted network, attackers often look to communicate with the compromised endpoint as well as to exfiltrate the data of interest. If communication occurs with a command-and-control server or an anonymous proxy, X-Force IP reputation data can provide intelligence to detect this communication and help prevent data loss.

Another common technique of advanced persistent threats is to attack other systems on the same network. X-Force Threat Intelligence, incorporated into IBM access management tools, can aid in denying attackers access to resources—such as code from the targeted network—based on the overall risk factor of the user.

By integrating X-Force threat intelligence across the security portfolio, IBM provides enterprise security technologies with an external vantage point, helping identify sophisticated attackers. Using continually updated global threat information in areas such as the latest phishing domains, command-and-control servers and anonymous proxies, attacker technologies can be quickly identified and remediated. Moreover, the combination of X-Force content with broader prevention and analytic capabilities builds a formidable defense against today's most advanced adversaries.

Making the most of X-Force Threat Intelligence

There are different methods through which IBM users can leverage X-Force Threat Intelligence to better protect their organizations.

Cloud-delivered threat updates

By subscribing to X-Force Threat Intelligence, users receive automatic X-Force threat updates delivered via the cloud. This method of delivery helps ensure that IBM users have access to the most up-to-date threat intelligence available—without affecting or slowing business operations.

IBM Security users can also opt to have unknown URLs reported back to the IBM Security global filter database anonymously, helping to increase threat coverage even further for IBM Security and its customers. Feeding these URLs directly into the web-crawling process helps to categorize previously unknown websites, or to add more granularity to currently categorized sites. Feedback on IP reputation statistics can also be reported back to the IBM Security servers.

IBM Security product integration

Products within the IBM Security portfolio have been optimized to integrate or incorporate X-Force capabilities—helping to ensure that IBM users receive the greatest benefits from this advanced threat data with the least amount of effort. Some examples include:

Security intelligence

To help organizations detect and defend against today's growing variety and volume of threats, IBM offers a robust security intelligence platform that applies sophisticated analytics to many types of data. The platform provides comprehensive analytics through security information and event management, log management, anomaly detection, and configuration and vulnerability management capabilities—and these capabilities can be extended even further by adding worldwide threat intelligence from X-Force.

Users can easily incorporate X-Force IP reputation data into the platform's rules and captured offenses and events—extending the value of its standard, open-source intelligence feeds. This enables users to capture events quickly and accurately, as well as to capture them in a way that provides additional insight for further analysis. The data from these intelligence sources is incorporated into the platform's correlation and analysis functions and serves to greatly enrich its threat-detection capabilities with up-to-the-minute data on threats.

Adding X-Force Threat Intelligence to this security intelligence platform provides users with additional context on security incidents, which helps improve incident prioritization—and ultimately, helps to prevent or minimize damaging attacks.

Intrusion prevention and web application control

As more and more applications are being accessed through the cloud—including social network, messaging, business and storage applications—network protection and web application control grow more critical. A next-generation IBM intrusion prevention appliance—designed to help mitigate risk, increase network visibility and awareness, and monitor and control application activity—integrates with X-Force Threat Intelligence to provide superior protection. This network-protection appliance provides application-action control, IP event information, URL filtering, and protocol analysis-based intrusion prevention, which includes injection logic protection, shellcode heuristics technology and content-analysis capabilities.

Integration with X-Force Threat Intelligence provides advanced application control and web content filtering capabilities. Being able to more specifically identify—and prioritize—threats gives organizations more control over the types of traditional and web applications employees should or should not access. To help minimize risk, organizations can leverage X-Force data to manage access to websites that meet specific policy requirements—and to prevent access to malicious websites.

Security access

Ensuring the right level of user access and privileges is a top security priority for organizations. IBM offers leading access-control solutions—that draw upon X-Force Threat Intelligence data—to help organizations enforce established access rights, password policies and information management policies. The incorporation of threat data, such as IP reputation, into the risk factor algorithms allows for a more accurate and comprehensive calculation of whether to grant or deny access to a resource.

These solutions also contribute to compliance efforts by maintaining centralized audit trails for access requests and preventing unauthorized access—all while enabling administrators and users to be more productive.

IBM Security access management software provides a single point of authorization for web, cloud-based, mobile and enterprise applications, helping to smooth the implementation of security policies across a wide range of web and application resources.

Conclusion

A preemptive security approach requires market-leading research, a keen eye for attack trends and techniques, and the ability to process and act upon this threat intelligence. Because the X-Force research and development team collects and analyzes threat information from thousands of customers around the world, it is able to identify new threats before customers could without the aid of X-Force Threat Intelligence. X-Force creates value by providing much broader—and higher quality—threat information than organizations can obtain on their own. Organizations can leverage this data to help prevent security incidents and/or to minimize the impact of security attacks.

Today, accessing X-Force Threat Intelligence is easier than ever, thanks to widespread integration with IBM Security solutions, including IBM QRadar® Security Intelligence Platform, IBM Security Network Protection appliances, IBM Security Access Manager and more.

For more information

To learn more about the value provided by the IBM X-Force research and development team, and about X-Force integration with IBM Security offerings, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security/xforce

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 the world-renowned X-Force research and development team, 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 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
September 2013

Please Recycle

WGW03034-USEN-00