

Security Information View in Relation to New Technologies

SECURITY FOR A NEW ERA OF COMPUTING

Jeff Crume, CISSP-ISSAP

Distinguished Engineer IBM Master Inventor IT Security Architect crume@us.ibm.com Blog: InsideInternetSecurity.com



Today's security drivers



Three key security technology trends

Risk Based Access

Security Information Sharing

Cognitive Security



Landscape of Identity & Access Management market is evolving

By 2020,



of enterprises will use attribute-based access control as the dominant mechanism to protect critical assets ...



... and 80%

of user access will be shaped by **new mobile and non-PC architectures** that service all identity types regardless of origin.¹

1 Gartner, Predicts 2014: Identity and Access Management, November 26, 2013

2 Gartner, MarketScope for Web Access Management, November 15, 2013

3 Forrester, Predictions 2014: Identity and Access Management, January 7, 2014

With the growing adoption of mobile, adaptive authentication & fine-grained authorization, traditional Web Access Management is being replaced by a broader "access management."¹

A clear need exists in the market for a converged solution² that is able to provide or integrate with MDM, authentication, federation, and fraud detection solutions.³

Can we leverage this trend for better security?

Multi-Factor Authentication and Risk Based Access

Authentication options*

* Stronger authentication may be effective in mitigating userid/password credential compromise; advanced malware/RAT can circumvent many in-band multi-factor mechanisms







Code Generation



Password

Security Information Sharing

IBM X-Force monitors and analyzes the changing threat landscape

Coverage 20,000+ devices under contract 35B+ events managed per day 133 monitored countries (MSS) 3,000+ security related patents 270M+ endpoints reporting malware



Depth

25B+ analyzed web pages and images

12M+ spam and phishing attacks daily

89K+ documented vulnerabilities

860K+ malicious IP addresses

Millions of unique malware samples

IBM X-Force® Research and Development

Expert analysis and data sharing on the global threat landscape



The IBM X-Force Mission

- Monitor and evaluate the rapidly changing threat landscape
- **Research** new attack techniques and develop protection for tomorrow's security challenges
- Educate our customers and the general public
- Integrate and distribute Threat Protection and Intelligence to make IBM solutions smarter

IBM X-Force Exchange



A new platform to consume, share, and act on threat intelligence

IBM X-Force Exchange is:

TRUSTED

a robust and secure platform built by one of the most trusted global brands

SOCIAL

a collaborative platform for sharing threat intelligence

ACTIONABLE

an integrated solution to help quickly stop threats

Backed by the reputation and scale of one of the most recognized security research teams in the world

Collaboration

Crowd-sourced information sharing based on 700+TB of threat intelligence

Search				AlertCon™ Thre	at Level (1)						
Search by Application name, IP, URL, Vulnerability, MD6							0,	Activity	Collections		
Current Threat Activit	y II 186.3.44.230 Ecuador Spam, Dynamic IPs	190.253.187.144 Colombia Spam, Dynamic IPs	197.27.87.111 Tanisia Spam, Dynamic IPs	41.143.58.200 Morocco Spam, Dynamic IPs	186.56.134.65 Argentina Sparn, Dynamic IPs	77.2 Rus Spa		Timoline Vulnerability research Vulnerability research litiwmt WMF file buffer overflow PCRE regular expression buffer overflow Security Intelligence Blog Organizations Ramp Up on NSSGL Databases, But What About Security? Comparing Free Online Malware Analysis Sandboxes Business Continuity: The Unsung Hero of Security intelligence	My Collections + New collection + New collection Vulnerability research Vulnerability research Shared with me There are no collections shared with you yet Public Conto this 5 min		
Malicious IP addresses in 1,606	the last hour	Command and Control 1	spam 1,266	Natvare 47	sea 55	nning 5	_		Posadar Web Exploit presentation presentation Bill Gales Bothet		

https://exchange.xforce.ibmcloud.com

Cognitive Security

The next era of security



Moats, Castles



Intelligence, Integration

Cloud, Collaboration, Cognitive

A tremendous amount of security knowledge is created for human consumption, but most of it is untapped



Threat and vulnerability feeds

A universe of security knowledge Dark to your defenses

User and network activity

Typical organizations leverage only 8% of this content*

Examples include:

- Research documents
- Industry publications
- Forensic information
- Threat intelligence commentary
- Conference presentations
- Analyst reports

- Webpages
- Wikis
- Blogs
- News sources
- Newsletters
- Tweets



Cognitive systems bridge this gap and unlock a new partnership between security analysts and their technology



Cognitive Security

- Unstructured analysis
- Natural language
- · Question and answer
- Machine learning
- Bias elimination
- Tradeoff analytics

Cognitive: Revolutionizing how security analysts work

Natural language processing with security that understands, reasons, and learns

E IBM QRada	ar Security Intelligence Offenses Log Ac	e tivity Net	work Activity Assets	Reports Risks Vi	ulnerabilities A	Advisor Admin			admin∨ Heip∨ wiessages∨			
Filters Deservables File File File File File File File File	< Back 10 9 3 24 1 15 4	CReader ha epperer to 130 IF Ad	Offense: 832/ as determined melware family or of the affected. ORdate has also but arreader, T Calographice, 8 file k1/A Xyubagmidwwyyd	ampalan may be related to the offer to these additional indicators possi- tive scorpena.com/865/40/b.exe uput 20.132.23.12 20.1 20.132.23.11 20.132.23.12 20.1 prvvid	Se and 3 other hosts in by related to the incident	your networks nt containing 14 Domains,	20	10. (0. 20.30 Looky 178.212.252.32	Verview Sources Attack Campaigns Matson Insights Watson Insights ORadar has determin and 3 other hosts in 1 these additional india 130 IP Addresses, 7 di	24 Dus Action from D (1) Destinations (1) Documents Found Documents Found Documents Found and A Documents Found and A and A	Notes (0) Wa Domains Implicated 14 ampaign may be relate to be affected. QRadar to the incident containi Hes	× Send to Resilient > Itson Hosts Involved Q 4 Explore Insights ed to the offense has also found ng 14 Domains,
Watson determines the specific campaign (Locky), discovers more infected endpoints, and sends results to the incident response team							Name	Created Mar 23, 2016 4:22 P	Da	ta Sources Reporting		



THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- 🥑 @ibmsecurity
- > youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

