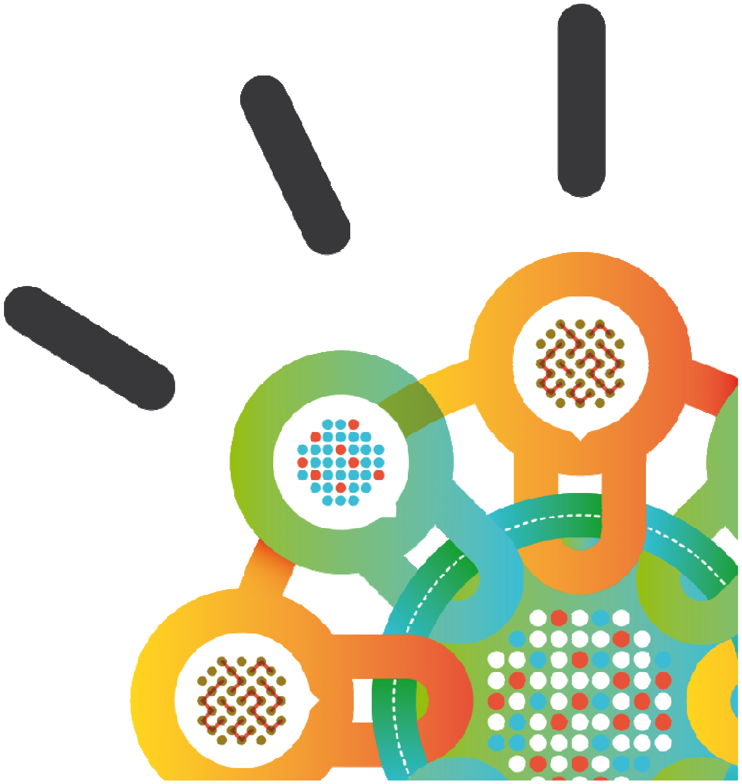
Security Intelligence.
Think Integrated.

IBM Security Trusteer Apex Advanced Malware Protection

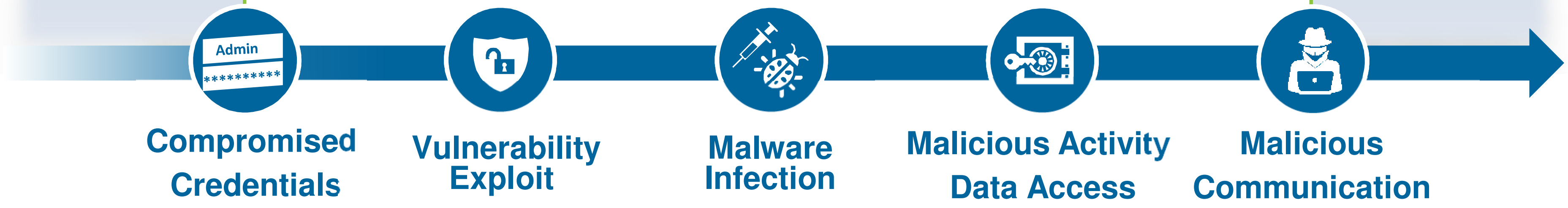
June 2015



Despite existing controls, employee endpoints are compromised and are used as pivot points into the enterprise network.

APT and Targeted Attack Methods Evolve Quickly

1. Advanced evasive malware bypasses security controls
2. Credentials are exposed through phishing and 3rd party breach
3. Compromised endpoints and stolen credentials enable access to enterprise networks, systems and data



Compromised Credentials

Vulnerability Exploit

Malware Infection

Malicious Activity Data Access

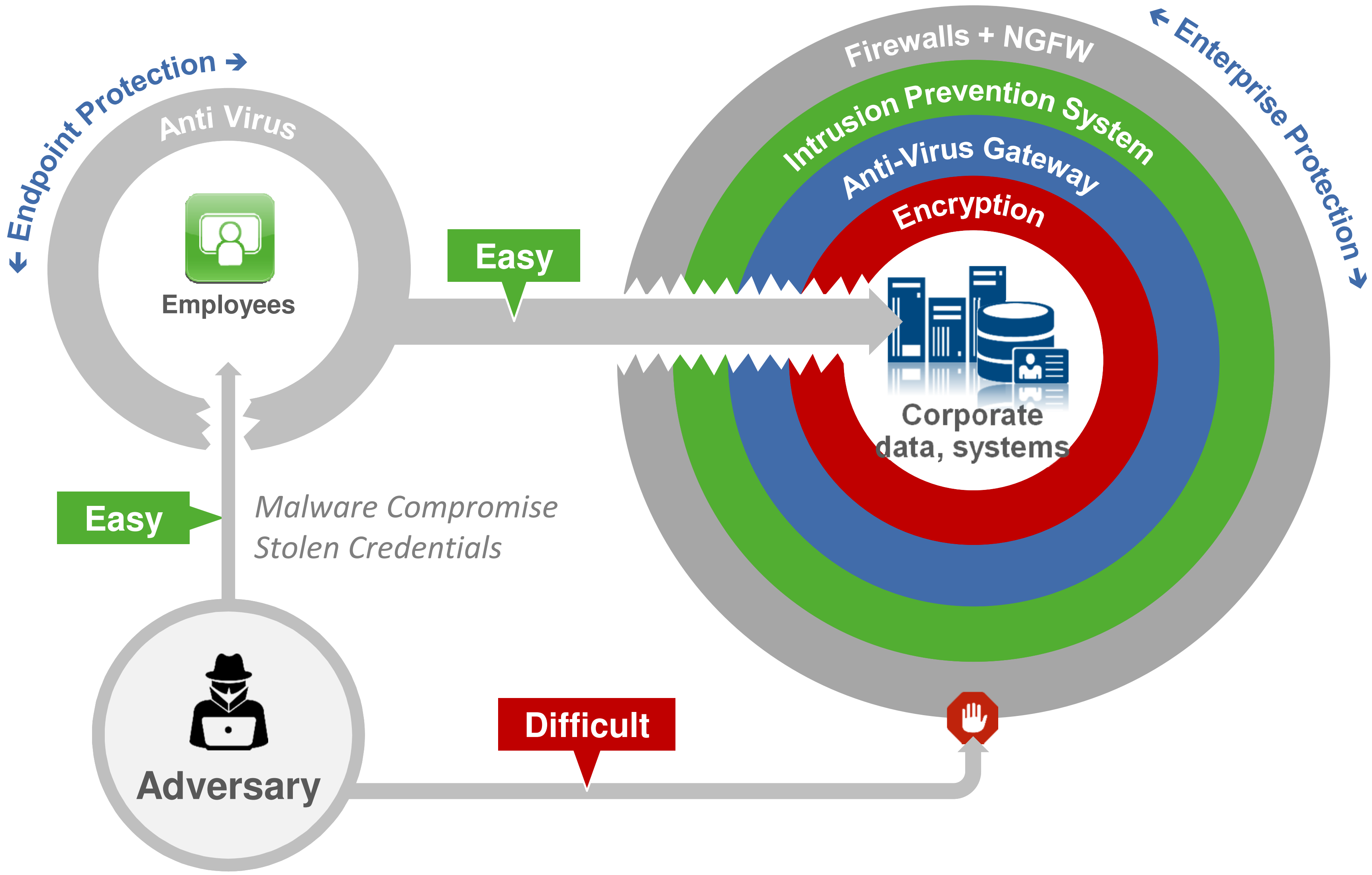
Malicious Communication

Who Hacked Sony? New Report Raises More Questions

JPMorgan Chase Breach Puts Renewed Focus on Malware A

A $1Billion APT Attack – Carbanak May Just Be the Biggest Cyber Heist Ever

The Path of Least Resistance



Corporate Credentials Theft and Exposure

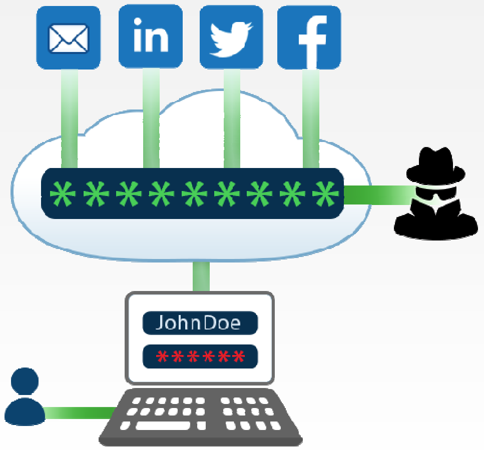
Malware: RATs, keyloggers & more

Citadel Trojan used to compromise password managers

Credentials phishing

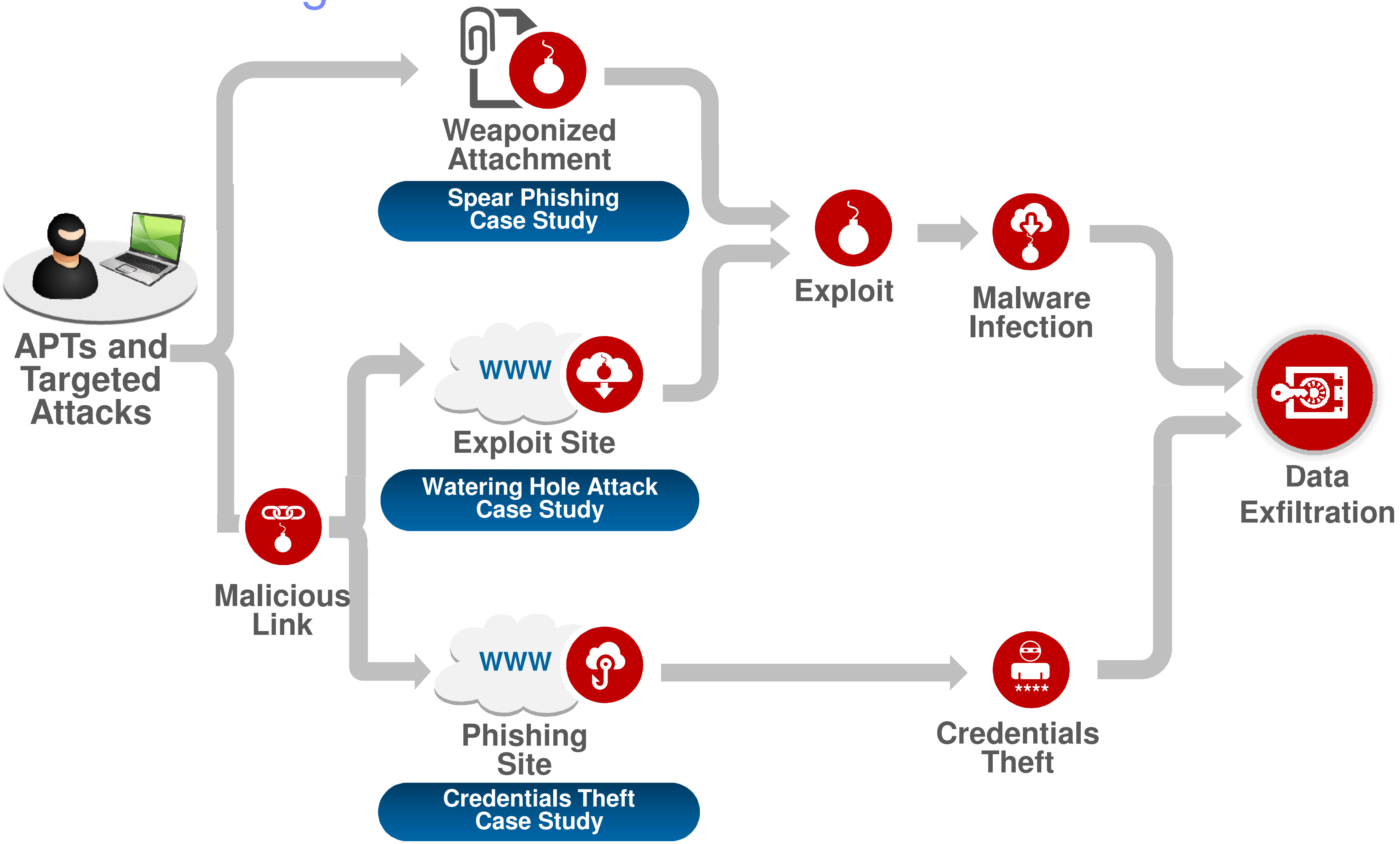
How the Syrian Electronic Army Hacked The Onion

3rd party breaches expose reused corporate credentials



Over 2 million Facebook, Google, Twitter passwords stolen - Again !

APTs and Targeted Attacks



APTs and Targeted Attacks

Weaponized Attachment

Spear Phishing Case Study

Malicious Link

Exploit Site

Watering Hole Attack Case Study

Phishing Site

Credentials Theft Case Study

Exploit

Malware Infection

Credentials Theft

Data Exfiltration

1:500 PCs infected with Advanced Evasive APT malware!

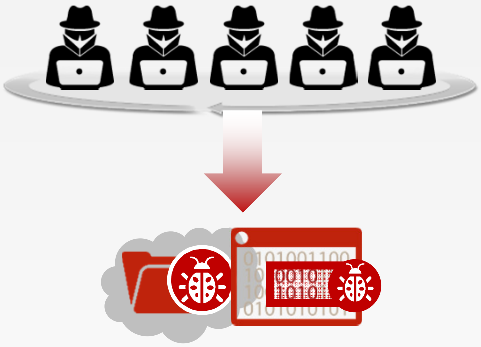
IBM Trusteer Research

Enterprise Endpoint Security Challenges

Evasive malware

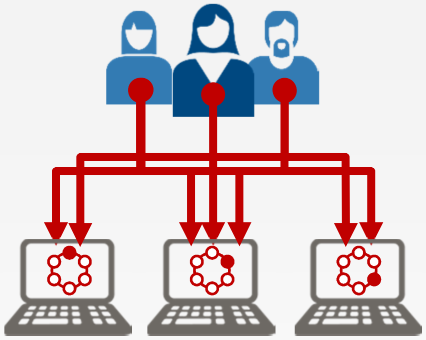
- Anti-viruses (blacklisting) cannot keep up with the high volumes of new malware
- Whitelisting processes are unmanageable
- Polymorphic engines and other techniques used for circumventing security controls
- New sophisticated evasion constantly developed

Major security control gaps



- Existing products offer no controls for major attack vectors
  - Zero-day exploits
  - Java-based attacks
  - Credentials reuse and exposure

Challenging manageability and operations



- Unpatched endpoints left due to incomplete patching processes leave the organization exposed
- Need to manage and maintain complex security controls already in place
- IT staff overloaded by number of alerts and notifications generated
- Lack of skilled professionals in the market

IBM Security Trusteer Apex Advanced Malware Protection

Preemptive, multi-layered protection against advanced malware and credentials theft

Effective Real-Time Protection

Using multiple layers of defense to break the threat lifecycle

Zero-day Threat Protection

Leveraging a positive behavior-based model of trusted application execution

Security Analysis and Management Services

provided by IBM Trusteer security experts

Apex multi-layered defense architecture

Threat and Risk Reporting

Vulnerability Mapping and Critical Event Reporting

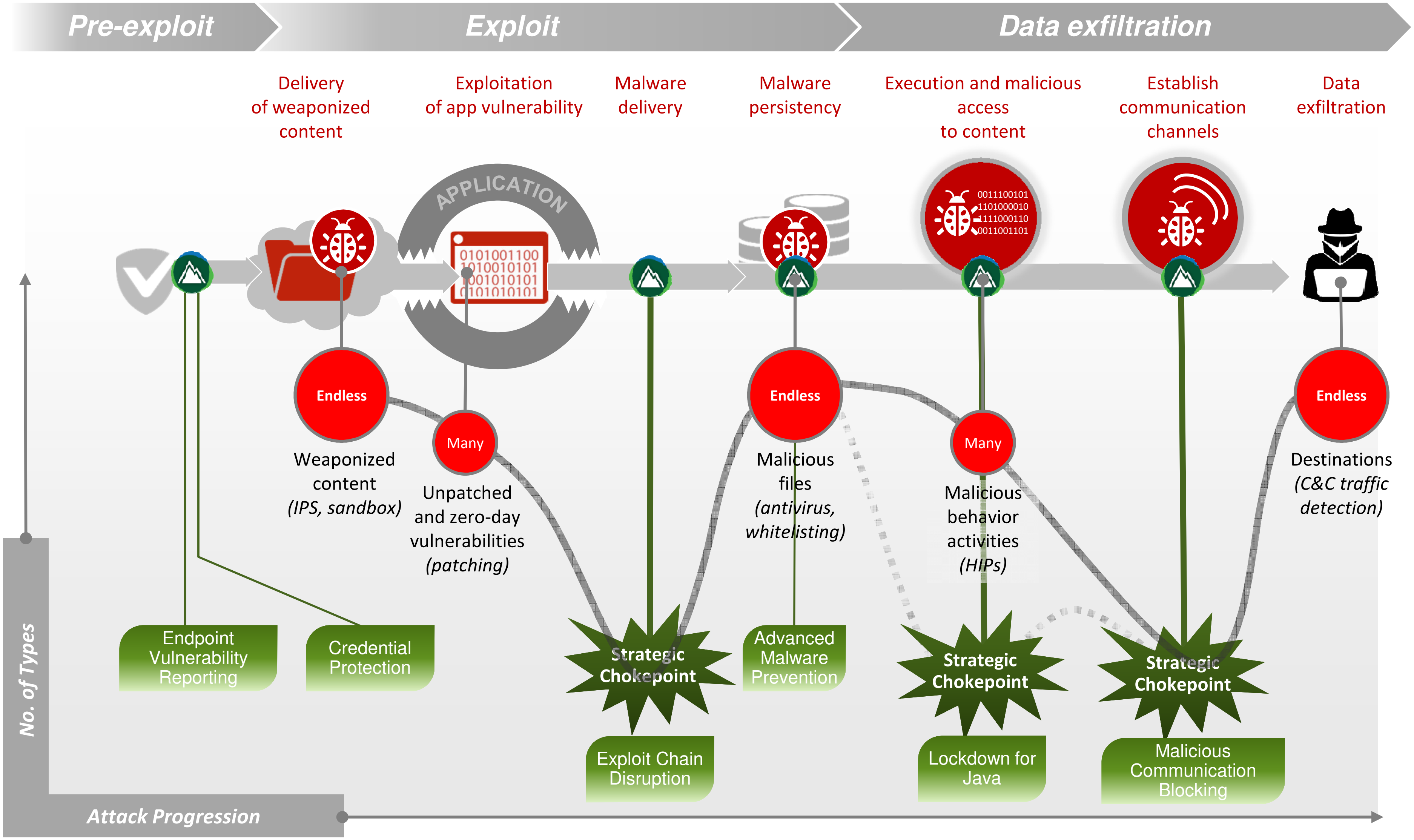
Advanced Threat Analysis and Turnkey Service

Credential Protection	Exploit Chain Disruption	Advanced Malware Detection and Mitigation	Lockdown for Java	Malicious Communication Prevention
• Alert and prevent phishing and reuse on non-corporate sites	• Prevent infections via exploits • Zero-day defense by controlling exploit-chain choke point	• Mitigates mass-distributed advanced malware infections • Cloud based file inspection for legacy threats	• Prevent high-risk actions by malicious Java applications	• Block malware communication • Disrupt C&C control • Prevent data exfiltration

Global Threat Research and Intelligence

Global threat intelligence delivered in near-real time from the cloud

Breaking the Threat LifeCycle



Pre-exploit

Exploit

Data exfiltration

Delivery of weaponized content

Exploitation of app vulnerability

Malware delivery

Malware persistency

Execution and malicious access to content

Establish communication channels

Data exfiltration

Endless
Weaponized content *(IPS, sandbox)*

Many
Unpatched and zero-day vulnerabilities *(patching)*

Endless
Malicious files *(antivirus, whitelisting)*

Many
Malicious behavior activities *(HIPs)*

Endless
Destinations *(C&C traffic detection)*

Endpoint Vulnerability Reporting

Credential Protection

Strategic Chokepoint
Exploit Chain Disruption

Advanced Malware Prevention

Strategic Chokepoint
Lockdown for Java

Strategic Chokepoint
Malicious Communication Blocking

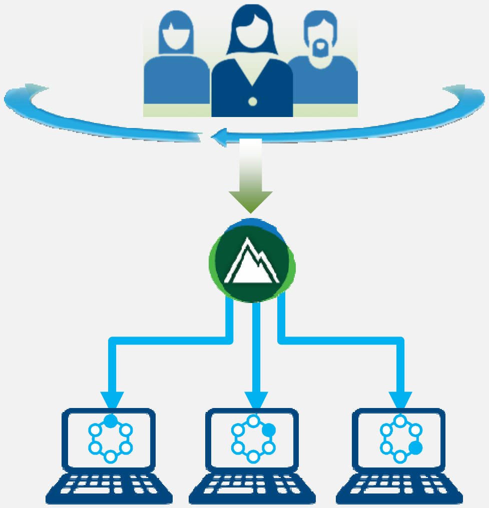
No. of Types

Attack Progression

Low operational impact

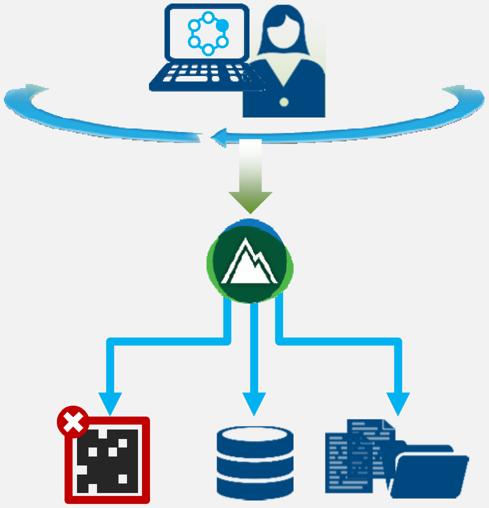
Advanced threat analysis and turnkey service

Low impact to IT security team



Eliminate the traditional security team approach (detect, notify, and manually resolve)

Low-footprint threat prevention



Minimize impact by blocking only the most sensitive actions

Exceptional turnkey service

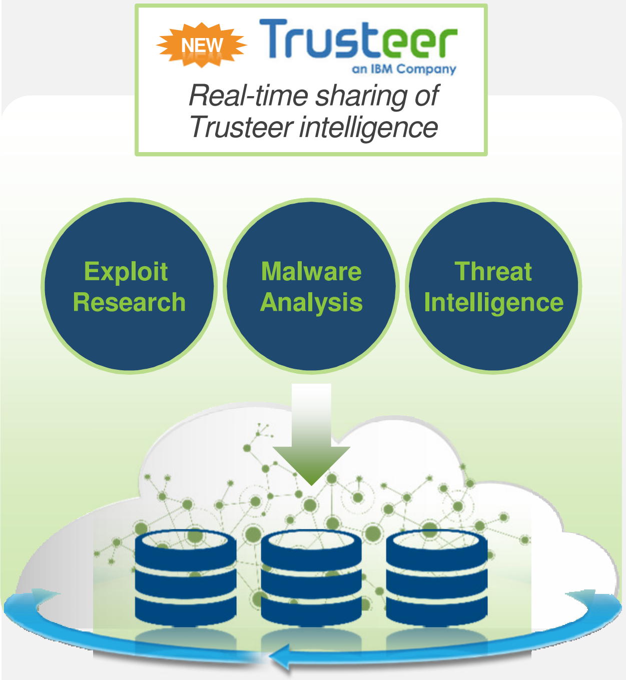
Centralized risk assessment service

Directly update endpoint users

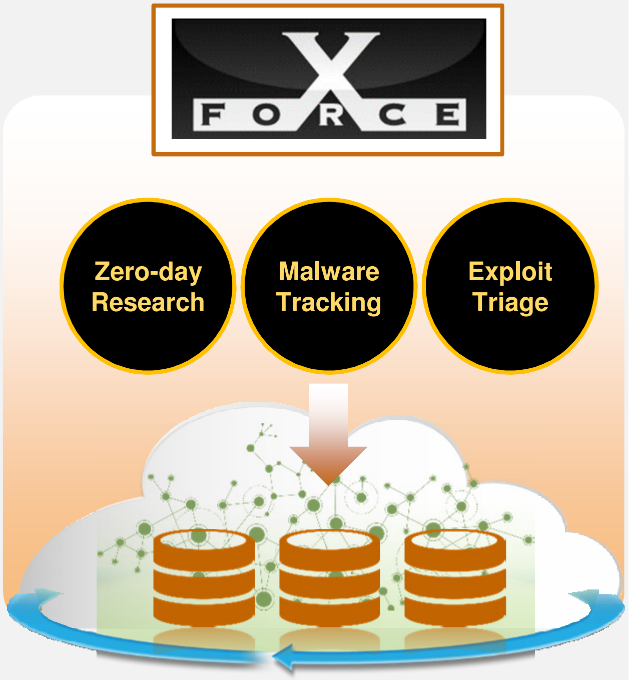
Dynamic intelligence

Crowd-sourced expertise in threat research and dynamic intelligence

Global Threat Research and Intelligence



- Combines the renowned expertise of X-Force with Trusteer malware research
- Catalog of 70K+ vulnerabilities,17B+ web pages, and data from 100M+ endpoints
- Intelligence databases dynamically updated on a minute-by-minute basis



Apex Blocks Threats that Bypass Other Security Controls!

Healthcare Provider – 30,000 users (Live, Blocking)

- Aepx blocked over 200 high risk infections over the first weeks
- Apex blocked 4 unknown (never reported before) malicious downloaders

Shipping – 15,000 users (Live, Blocking)

- Blocked “Viking” on PoS
- Apex blocked Ransomeware (CTB-Locker), Keyloggers,
- Apex blocked multiple Trojans and malware downloaders

Technology – 2,000 users (PoC, Monitoring)

- Apex identified an attempt to exploit MS Word that tried to install RAT
- 3 Malicious files that bypassed other security controls

PoC – 200 users (Monitoring)

- Apex prevented attempt to run malicious attachment (spear-phishing) that tried to download Gamarue (RAT)
- Blocked exploit attempt that tried to download unknown Trojan

Malware Protection on the Endpoint…Differentiating from True Zero Day Advanced Threat Protection

Legacy Anti Virus

New marketing, some enhancements, but core approach is still not enough:

- Blacklisting – based on what we 'know'. Not a 0-Day solution
- Relies on frequent updates that are reactive
- Must scan filesystem frequently
- Advanced Heuristics are just 'looser' signatures.
- Still require updates, system scanning and attack identification

Endpoint Malware Protection

Malware Protection vendors are bundling in many suites of products

- Layered approach is validated (no silver bullet)
- Loose integration – higher performance and administrative overhead

IBM is uniquely positioned to offer integrated protection

- A dynamic, integrated system to disrupt the lifecycle of advanced attacks and prevent loss

Smarter Prevention

Trusteer Apex Endpoint Malware Protection

Trusteer an IBM Company

- Prevent malware installation and disrupt malware communications

IBM Security Network Protection XGS

- Prevent remote network exploits and limit the use of risky web applications

IBM Guardium Data Activity Monitoring

- Prevent remote network exploits and limit the use of risky web applications

Security Intelligence

IBM Security QRadar Security Intelligence

QRadar

- Discover and prioritize vulnerabilities
- Correlate enterprise-wide threats and detect suspicious behavior

Continuous Response

IBM Security QRadar Incident Forensics

QRadar

- Retrace full attack activity, Search for breach indicators and guide defense hardening

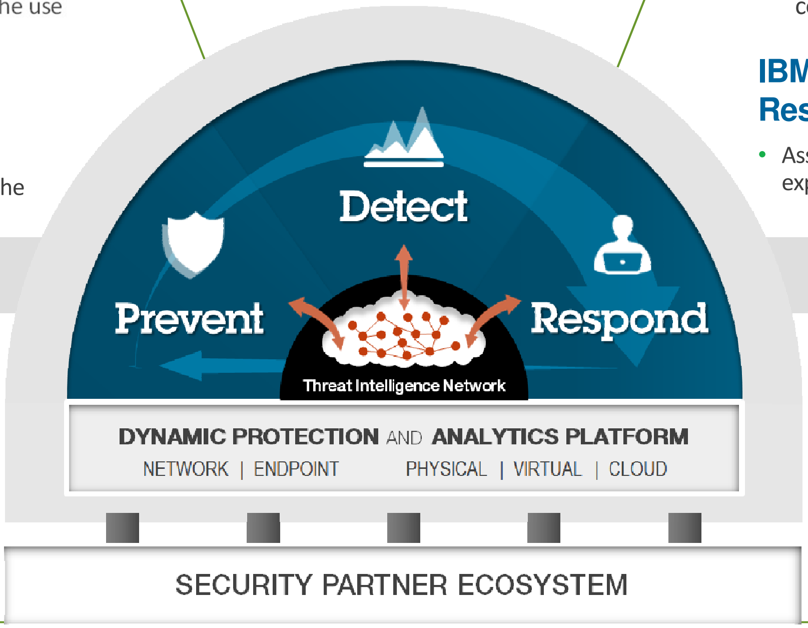
IBM Endpoint Manager

- Automate and manage continuous security configuration policy compliance

IBM Emergency Response Services

24x7

- Assess impact and plan strategically and leverage experts to analyze data and contain threats



DYNAMIC PROTECTION AND ANALYTICS PLATFORM

NETWORK | ENDPOINT PHYSICAL | VIRTUAL | CLOUD

SECURITY PARTNER ECOSYSTEM

Open Integrations

Ready for IBM Security Intelligence Ecosystem

- Share security context across multiple products
- 100+ vendors, 400+ products

Global Threat Intelligence

IBM X-Force Threat Intelligence

- Leverage threat intelligence from multiple expert sources

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 or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a 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 SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security

Optional Slides

How Apex improves the security posture thru integration

IBM QRadar

- Apex protects against Advanced Threats and APTs, which are not covered by traditional security technologies (such as AV).
- Apex provides increased threat visibility and endpoint intelligence, which will reduce the time to research and remediate attack vectors.
- Apex actually prevents attacks, which reduces false alerts so that the IT staff can focus on real security threats.

IBM Endpoint Manager

- Apex protects against Advanced Threats and APTs, which are not covered by traditional security technologies (such as AV).
- Apex provides protection during the time-window from before a vulnerability is published to when a patch is applied.
- Endpoint Manger is integrated with Trusteer Apex to support rapid deployment.

A large international bank

Protecting employee endpoints against advanced threats and malware

Advanced Threat Protection

One of the largest international banks concerned that compromised endpoints enable a breach:

- Concerned that **compromised** employee endpoints will **enable a breach**
- Existing security controls (AV, FW, etc) **aren't effective** against advanced threats

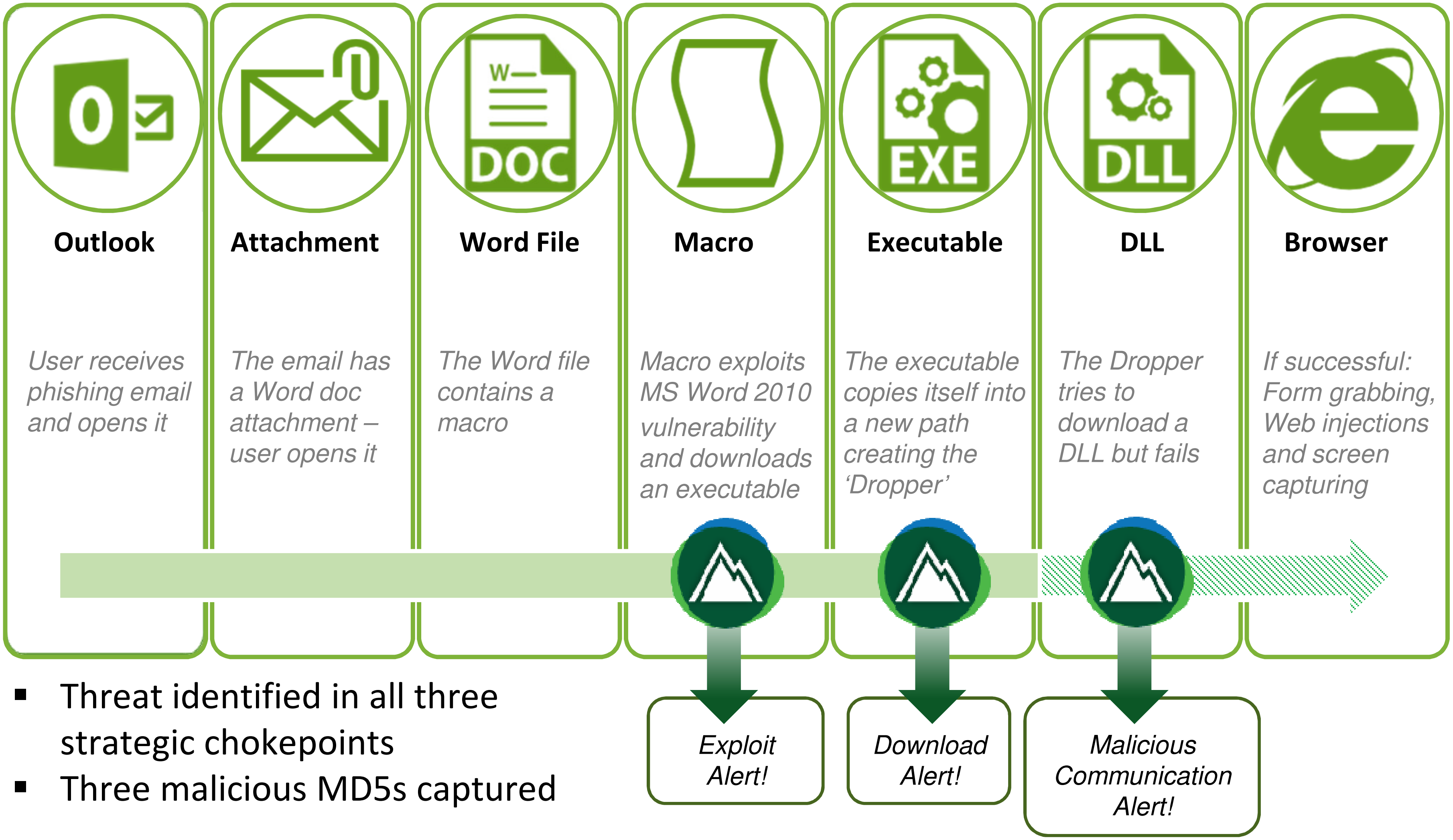
IBM Trusteer Apex installed on employee endpoints in 'Monitor' mode:

Identified an employee that was a victim on a **spear-phishing campaign**:

- Weaponized attachment contained an **exploit** that tried to infect the endpoint with a variant to the **Bugat Trojan**
- IBM Trusteer Apex alerted in **real-time** on **multiple phases** of the threat lifecycle
- Captured **three** malicious files that **bypassed** other security controls

IBM Trusteer Apex Identifies Trojan in Real-time

Dridex Banking Trojan Distributed Through Phishing Campaigns



Outlook

User receives phishing email and opens it

Attachment

The email has a Word doc attachment – user opens it

Word File

The Word file contains a macro

Macro

Macro exploits MS Word 2010 vulnerability and downloads an executable

Executable

The executable copies itself into a new path creating the 'Dropper'

DLL

The Dropper tries to download a DLL but fails

Browser

If successful: Form grabbing, Web injections and screen capturing

Exploit Alert!

Download Alert!

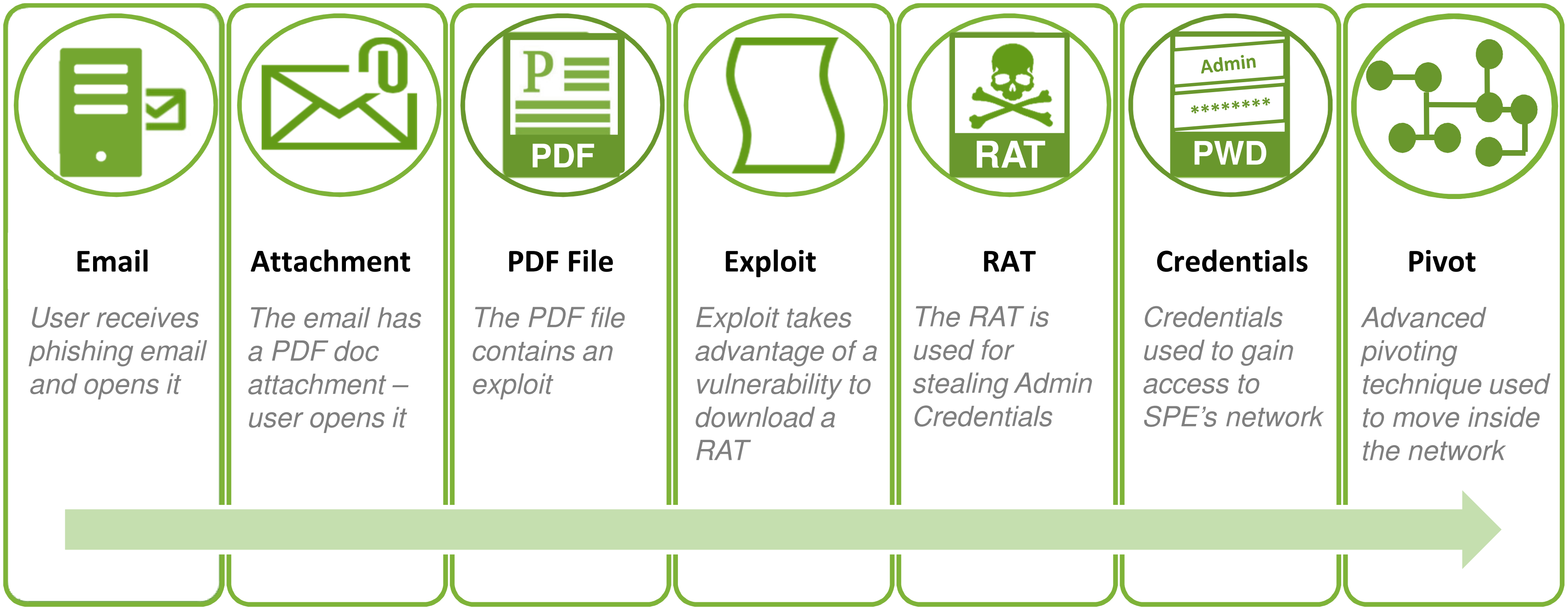
Malicious Communication Alert!

- Threat identified in all three strategic chokepoints
- Three malicious MD5s captured

** IBM Trusteer Apex running in 'Monitor' mode*

Alleged Russian hack into Sony’s network

Spear-phishing email sent to employees in Russia, India and other parts of Asia



Email

User receives phishing email and opens it

Attachment

The email has a PDF doc attachment – user opens it

PDF File

The PDF file contains an exploit

Exploit

Exploit takes advantage of a vulnerability to download a RAT

RAT

The RAT is used for stealing Admin Credentials

Credentials

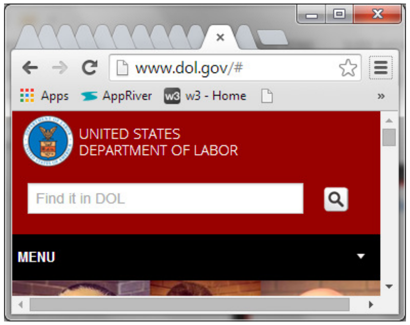
Credentials used to gain access to SPE’s network

Pivot

Advanced pivoting technique used to move inside the network

- Russian cybercriminals claim they successfully breached Sony during 2014 using spear-phishing attacks.
- It is not clear if this group is responsible for the infamous breach in which Sony movies were stolen and systems were shut down.

DoL Watering-hole Attack: Targeting Lab Employees



1. DoL website compromised

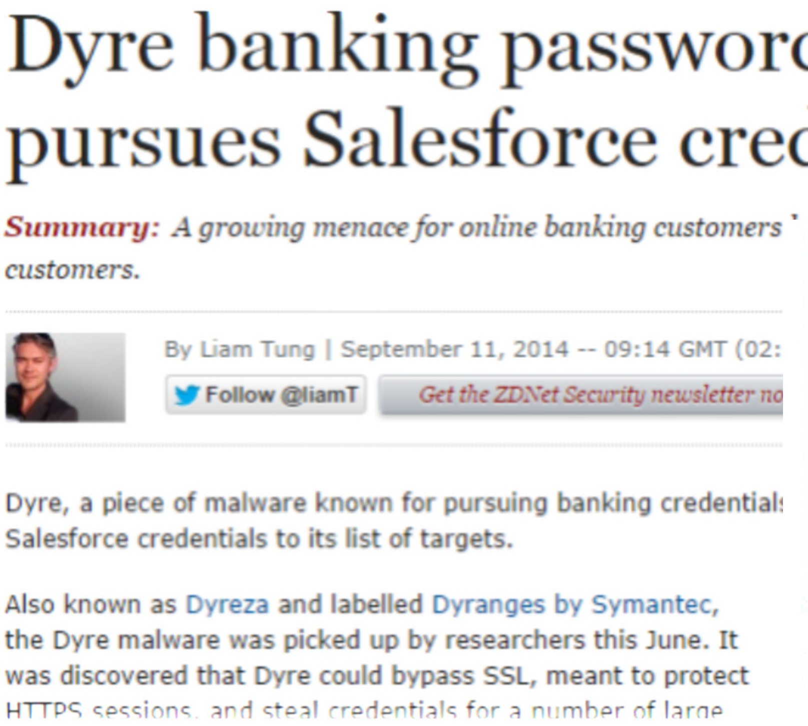
3. Redirected to exploit site

4. Exploited an IE zero-day remote code execution vulnerability to download the ***Poison-ivy Trojan***

2. Website Visitors

5. User machine compromised

Dyre Malware Steals Employee Credentials to Salesforce.com



Dyre banking password stealer pursues Salesforce credentials

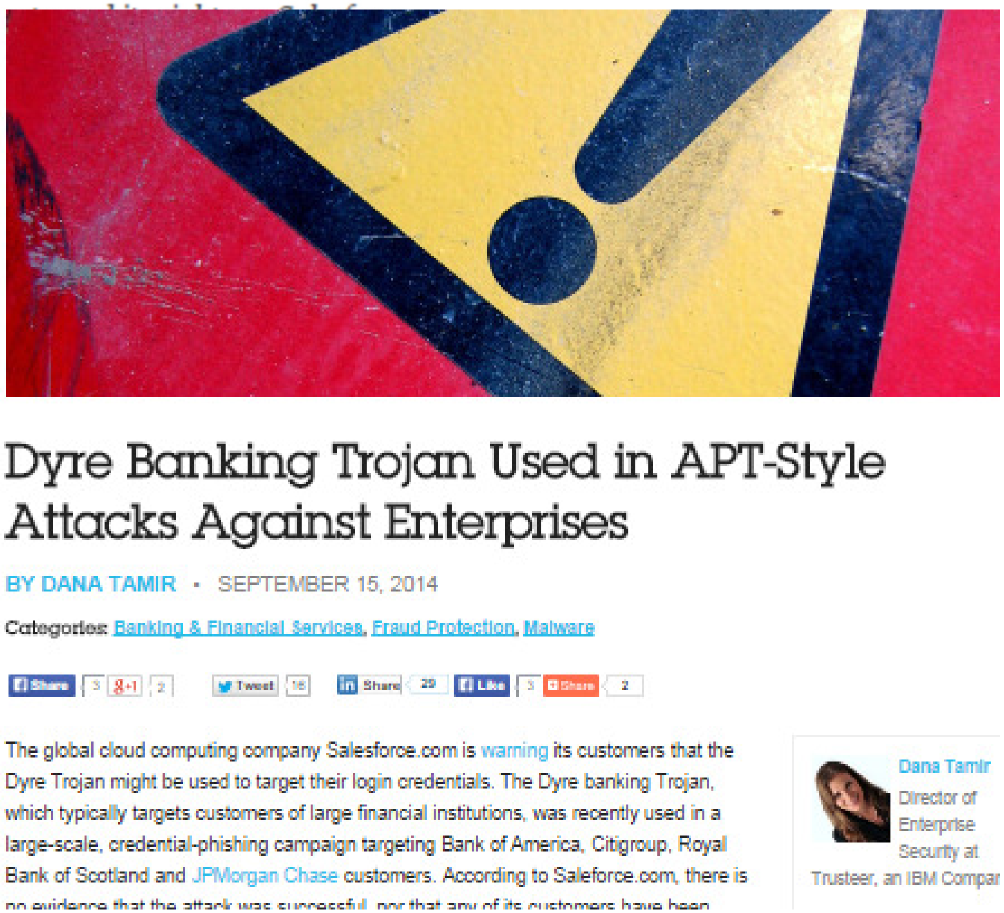
Summary: A growing menace for online banking customers'

customers.

By Liam Tung | September 11, 2014 -- 09:14 GMT (02:

Dyre, a piece of malware known for pursuing banking credential
Salesforce credentials to its list of targets.

Also known as Dyreza and labelled Dyranges by Symantec, the Dyre malware was picked up by researchers this June. It was discovered that Dyre could bypass SSL, meant to protect HTTPS sessions, and steal credentials for a number of large



Dyre Banking Trojan Used in APT-Style Attacks Against Enterprises

BY DANA TAMIR • SEPTEMBER 15, 2014

Categories: Banking & Financial Services, Fraud Protection, Malware

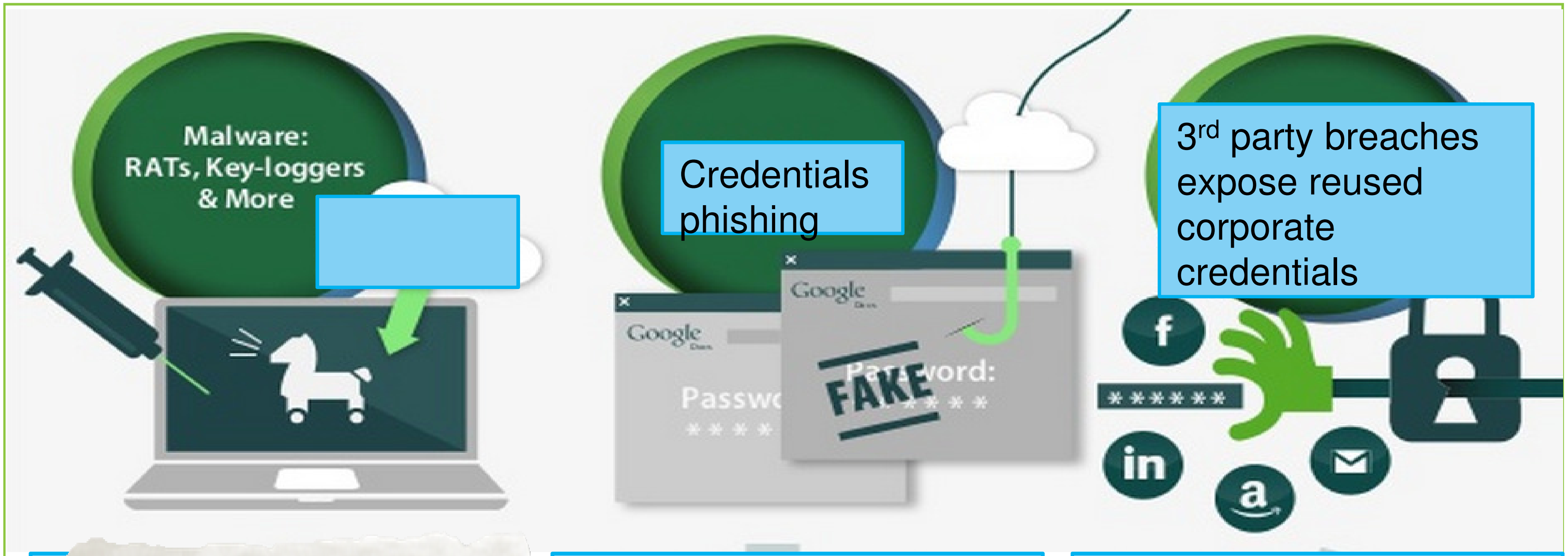
The global cloud computing company Salesforce.com is warning its customers that the Dyre Trojan might be used to target their login credentials. The Dyre banking Trojan, which typically targets customers of large financial institutions, was recently used in a large-scale, credential-phishing campaign targeting Bank of America, Citigroup, Royal Bank of Scotland and JPMorgan Chase customers. According to Saleforce.com, there is no evidence that the attack was successful, nor that any of its customers have been

Dana Tamir
Director of Enterprise Security at Trusteer, an IBM Compar

IBM Security Trusteer Apex Advanced Threat Protection

Large International Bank	Existing security controls aren’t effective against advanced threats	Identified the exploit in real time and captured 3 malicious files
Large Multinational Technology Company	Concerned about advanced threats bypass existing security controls	Identified an unknown Trojan that bypassed AV and tried to communicate with a C&C
A Leading Technology Company	Concerned that compromised PCs will enable a Breach	Prevented a spear-phishing attachment from compromising employee endpoints
A Healthcare Organization	Concerned that stolen credentials will enable unauthorized access	Detected >200 dangerous infections on employee PCs > 4 unknown Trojans identified

Corporate Credentials Theft and Exposure



Credentials phishing

3rd party breaches expose reused corporate credentials

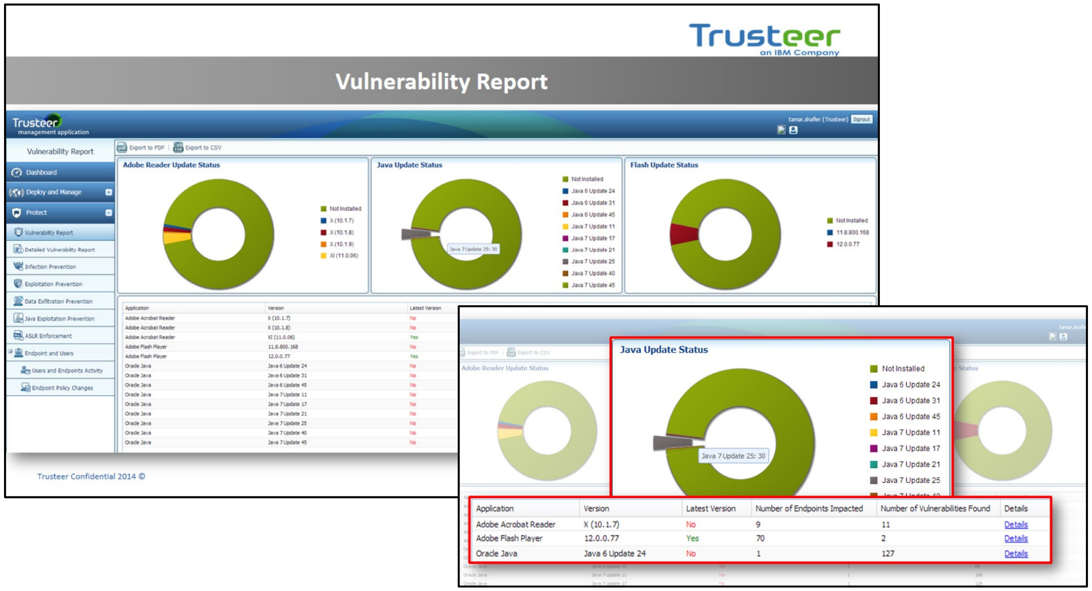
‘The Onion’ explains how SEA hijacked its Twitter account

Yahoo email account passwords stolen

Lockhead martin

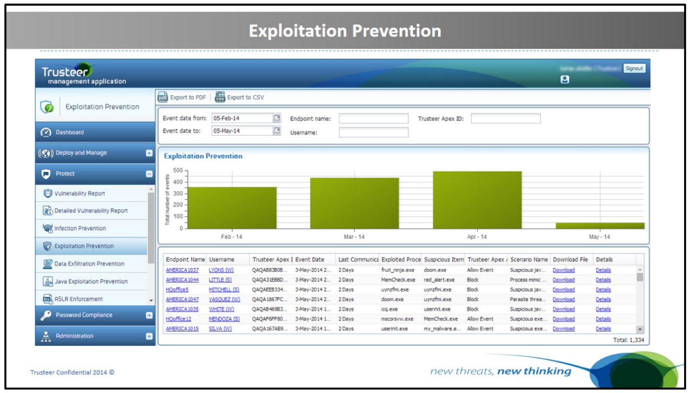
Threat and risk reporting: Vulnerability mapping and critical event reporting

Identify risks from vulnerabilities and user behavior, help ensure compliance



Application	Version	Latest Version
Adobe Acrobat Reader	X (10.1.7)	No
Adobe Acrobat Reader	X (10.1.8)	No
Adobe Acrobat Reader	XI (11.0.06)	Yes
Adobe Flash Player	11.8.800.168	No
Adobe Flash Player	12.0.0.77	Yes
Oracle Java	Java 6 Update 24	No
Oracle Java	Java 6 Update 31	No
Oracle Java	Java 6 Update 45	No
Oracle Java	Java 7 Update 11	No
Oracle Java	Java 7 Update 17	No
Oracle Java	Java 7 Update 21	No
Oracle Java	Java 7 Update 25	No
Oracle Java	Java 7 Update 40	No
Oracle Java	Java 7 Update 45	No

Application	Version	Latest Version	Number of Endpoints Impacted	Number of Vulnerabilities Found	Details
Adobe Acrobat Reader	X (10.1.7)	No	9	11	Details
Adobe Flash Player	12.0.0.77	Yes	70	2	Details
Oracle Java	Java 6 Update 24	No	1	127	Details
Oracle Java	Java 6 Update 45	No	1	69	
Oracle Java	Java 7 Update 11	No	1	166	
Oracle Java	Java 7 Update 17	No	1	129	



Event date from: 05-Feb-14
Event date to: 05-May-14
Endpoint name:
Username:
Trusteer Apex ID:

Endpoint Name	Username	Trusteer Apex I	Event Date	Last Communica	Exploited Proce	Suspicious Item	Trusteer Apex /	Scenario Name	Download File	Details
AMERICA1037	LYONS (W)	QAQAB83B0B...	3-May-2014 2...	2 Days	fruit_ninja.exe	doom.exe	Allow Event	Suspicious jav...	Download	Details
AMERICA1044	LITTLE (S)	QAQA31EBBD...	3-May-2014 2...	2 Days	MemCheck.exe	red_alert.exe	Block	Process mimic ...	Download	Details
HQoffice5	MITCHELL (S)	QAQAEEB334...	3-May-2014 2...	2 Days	uynzfmi.exe	uynzfmi.exe	Block	Suspicious jav...	Download	Details
AMERICA1047	VASQUEZ (W)	QAQA1867FC...	3-May-2014 2...	2 Days	doom.exe	uynzfmi.exe	Block	Parasite threa...	Download	Details
AMERICA1035	WHITE (W)	QAQAB469B3...	3-May-2014 1...	2 Days	icq.exe	userinit.exe	Block	Suspicious jav...	Download	Details
HQoffice12	MENDOZA (S)	QAQAF6FF80...	3-May-2014 1...	2 Days	mscorsvw.exe	MemCheck.exe	Allow Event	Suspicious exe...	Download	Details
AMERICA1015	SILVA (W)	QAQA167AB9...	3-May-2014 1...	2 Days	userinit.exe	my_malware.e...	Allow Event	Suspicious exe...	Download	Details

Total: 1,334

Vulnerability reports

Detailed reporting to visualize and understand which endpoints and apps are vulnerable to exploits

Corporate credential reports

Reporting on which users are re-using credentials, out of policy guidelines

Incident reports

Reporting on security incidents – exploits, suspicious communication, infections

Why Apex

Apex is re-defining endpoint protection for advanced threats with a holistic approach:

Advanced Multi-Layered Defense

- ✓ Credential Protections
- ✓ Exploit Chain Disruption
- ✓ Lockdown for Java
- ✓ Malicious Communication Blocking
- ✓ Cloud-Based File Inspection

Low Operational Impact

- ✓ Low impact to IT security team
- ✓ Low-footprint threat prevention
- ✓ Exceptional turnkey service

Dynamic Intelligence

- ✓ Combines the renowned expertise of X-Force with Trusteer malware research
- ✓ >100 million endpoints collecting intelligence
- ✓ Protections dynamically updated near real-time

And the cost of a data breach is on the rise, with customers at risk

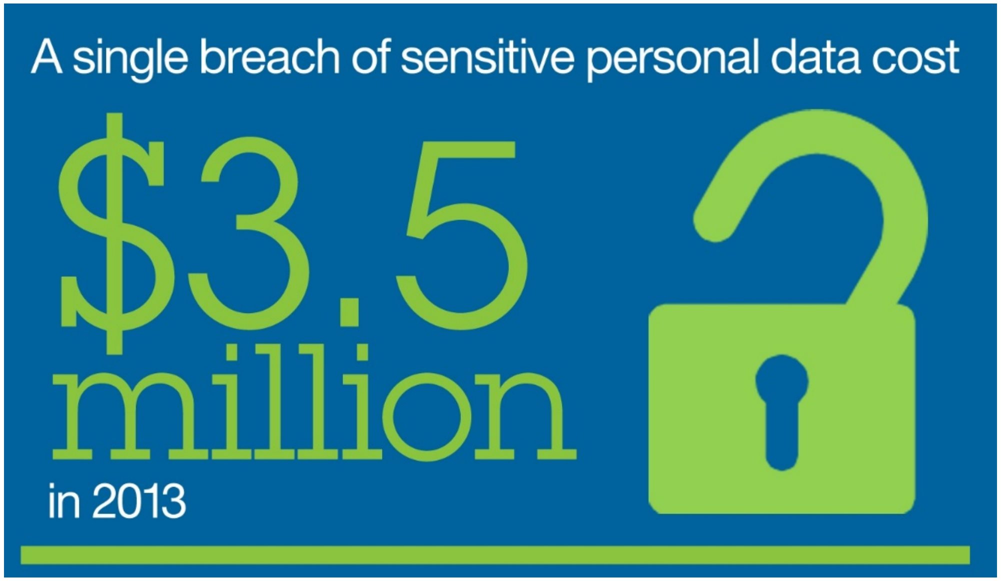
The average cost of a data breach increased

15%

in 2013

A single lost or stolen data record cost on average

$145 in 2013

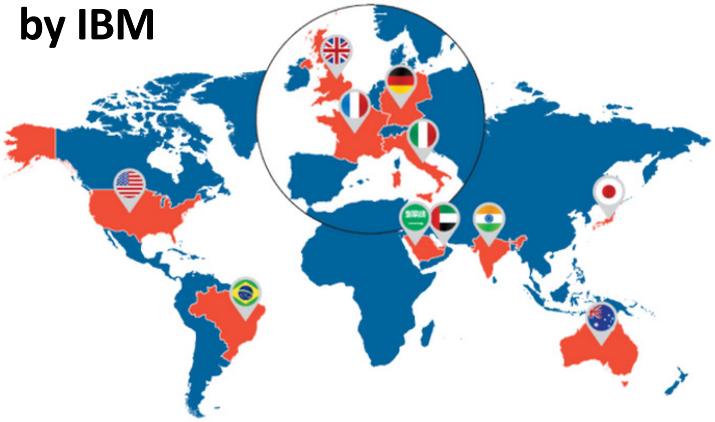


A single breach of sensitive personal data cost

$3.5 million

in 2013

2014 Cost of Data Breach Study From Ponemon Institute, sponsored by IBM



Security is a board room discussion, and security leaders are more accountable than ever before

CEO	CFO/COO	CIO	CHRO	CMO
Loss of market share and reputation Legal exposure	Audit failure Fines and criminal charges Financial loss	Loss of data confidentiality, integrity and/or availability	Violation of employee privacy	Loss of customer trust Loss of brand reputation

Your Board and CEO demand a strategy

Source: Discussions with more than 13,000 C-suite executives as part of the IBM C-suite Study Series

Advanced Malware Compromises Employee Endpoints

Exploits

- Weaponized attachments
- Drive-by downloads
- Watering holes
- Malvertising

Evasive Malware

- Bypassing detection controls (AV, etc)
- Evading native controls (Java, EMET)
- Hiding malicious communications

Zero-Day Threats

- Exploitation of unknown vulnerabilities
- New, never seen before malware