

A New Era of Security for a New Era of Computing

IBM X-Force



Doron Shiloach
X-Force Product Manager

October 2015



What is X-Force?



IBM X-Force

is the foundation for advanced security and threat research across the IBM Security Framework.

IBM X-Force monitors and analyzes the changing threat landscape

Coverage

20,000+ devices
under contract

15B+ 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

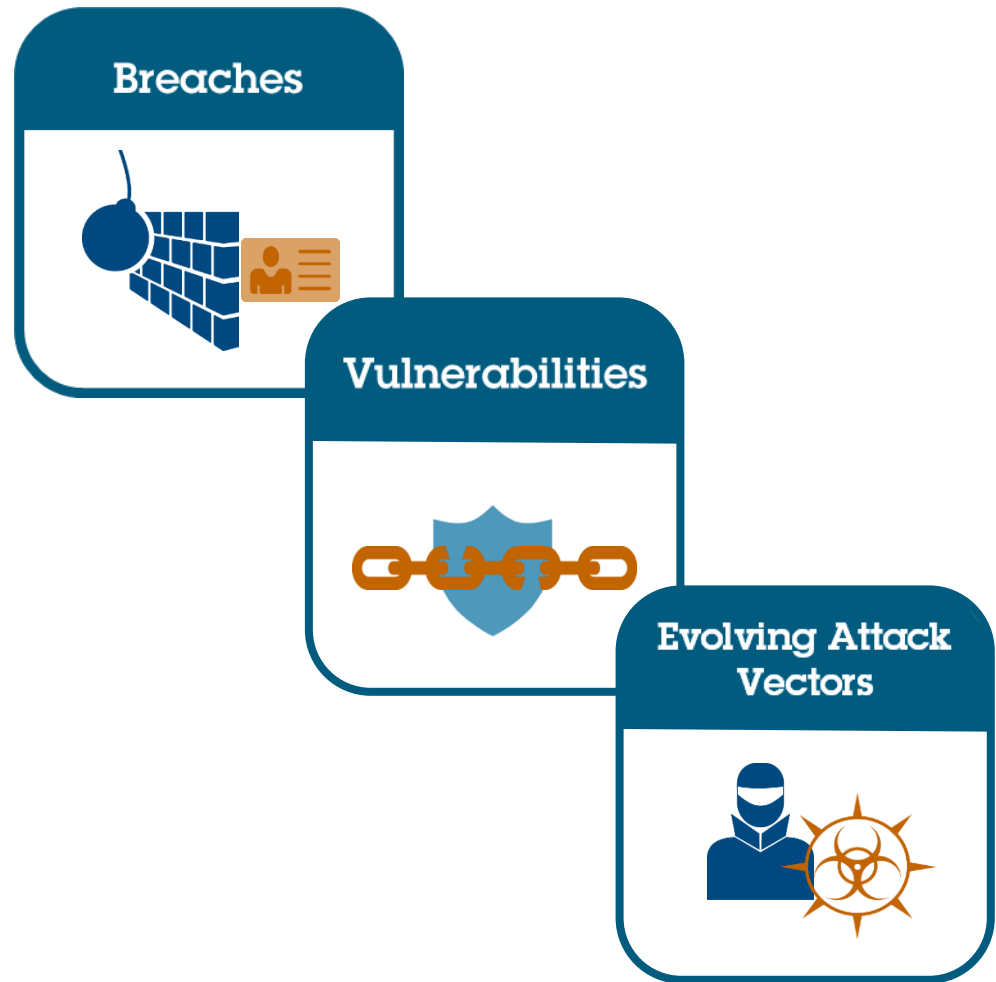
92K+ documented
vulnerabilities

860K+ malicious
IP addresses

Millions of unique
malware samples

For the vast majority of security leaders, the world has dramatically changed in the last three years

- 1 Rising over a transformed landscape
- 2 Worrying a lot about external threats
- 3 Expecting more external collaboration
- 4 Still focusing on today's technology
- 5 Uncertain about government action



Source: [2014 IBM Chief Information Security Officer Assessment](#)

83% of CISOs say that the challenge posed by external threats has increased in the last three years

Near Daily Leaks of Sensitive Data

40% increase in reported data breaches and incidents

2012

Relentless Use of Multiple Methods

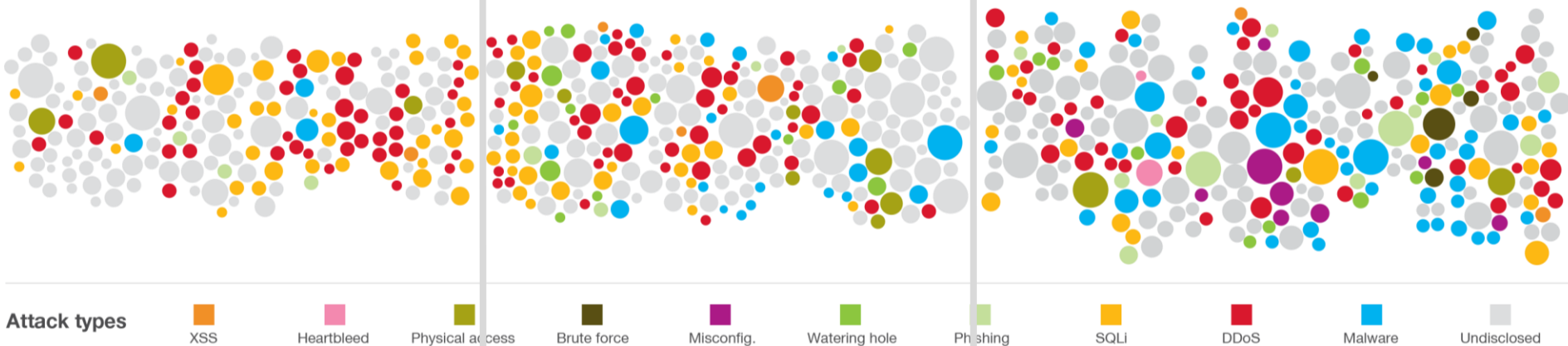
800,000,000+ records were leaked, while the future shows no sign of change

2013

“Insane” Amounts of Records Breached

1,000,000,000 records were breached with 42% of CISOs reporting the risk from external threats increased dramatically.

2014



Size of circle estimates relative impact of incident in terms of cost to business.

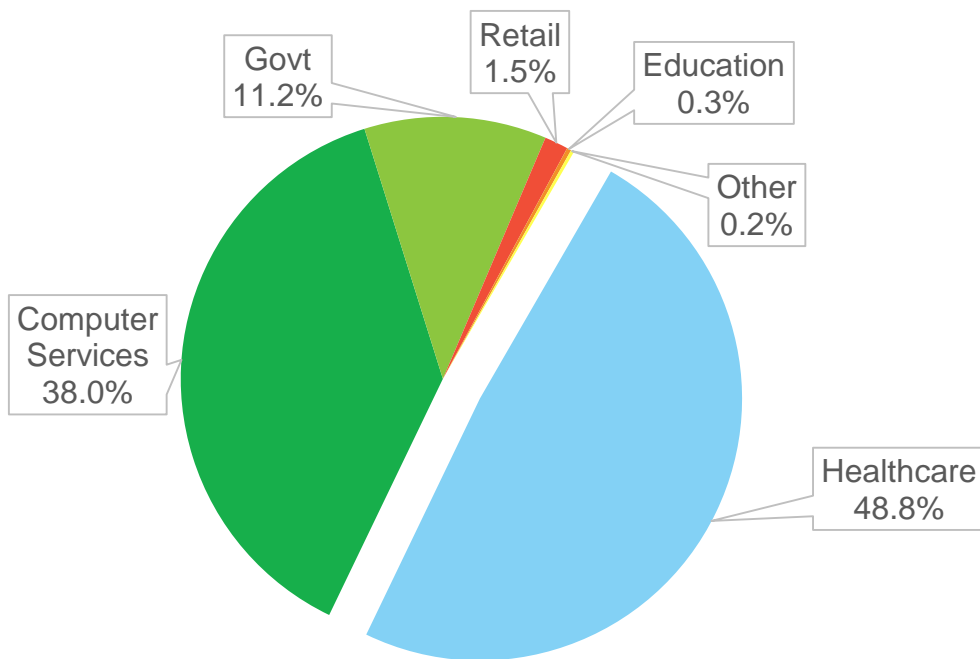
A historical look at security incidents by attack type, time and impact, 2012 through 2014

Source: IBM X-Force® Research and Development

Source: [IBM X-Force Threat Intelligence Quarterly – 1Q 2015](#) and [2014 IBM Chief Information Security Officer Assessment](#)

IBM Managed Security Services declares 2015 the “Year of the Healthcare Breach”

Top 5 Industries per Count of Records Compromised
1H 2015



100,000,000

Number of healthcare records compromised in the first half of 2015

\$363

Average cost per lost or stolen record in a healthcare org; 136% higher than average cost per record of a data breach.

The tone of breaches has shifted, revealing disturbing flaws in the fundamentals of both systems and security practices

A lack of security fundamentals

- Password reuse between enterprise and personal accounts
- Leaving default admin passwords on systems
- Poor challenge questions for password reset procedures

Cracks in the foundation

- The same operating systems, open-source libraries and CMS software are prevalent on many websites
- 2014 saw several of the systems and libraries suffer public vulnerability disclosures

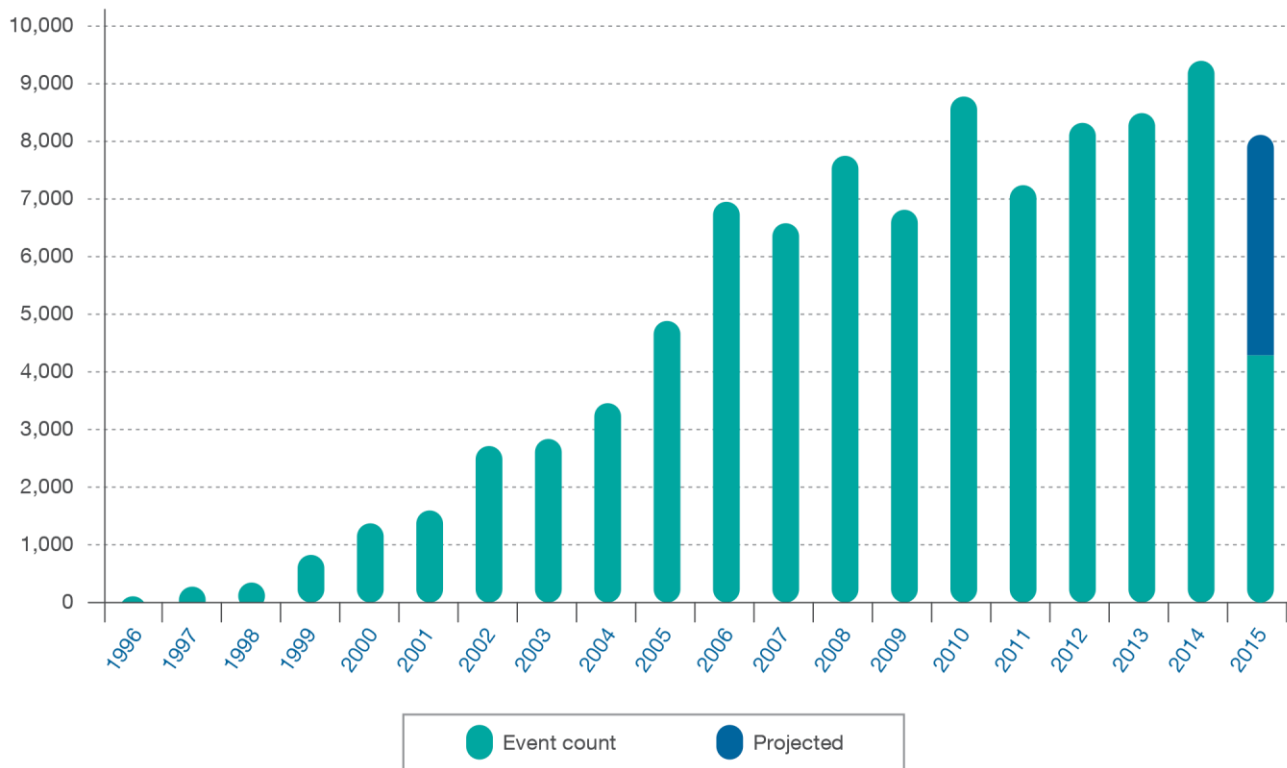
Shrinking privacy in a digital world

- Healthcare record leaks surged in 1H 2015
- Weak passwords make it easy for attackers to compromise cloud-based storage services

Under current trends, X-Force projects about 8,000 disclosures in 2015, which would be the lowest since 2011

Vulnerability disclosures growth by year

1996 through 2015 (projected)



In the first half of 2015, we recorded just over 4,000 new security vulnerabilities.

Figure 4. Vulnerability disclosures growth by year, 1996 through 2015 (projected)

Source: IBM X-Force® Research and Development

CVSS v3 more accurately reflects the scope and impact of modern vulnerabilities

Comparison of DNS Kaminsky Bug (CVE-2008-1447)

CVSS scoring from version 2 to version 3

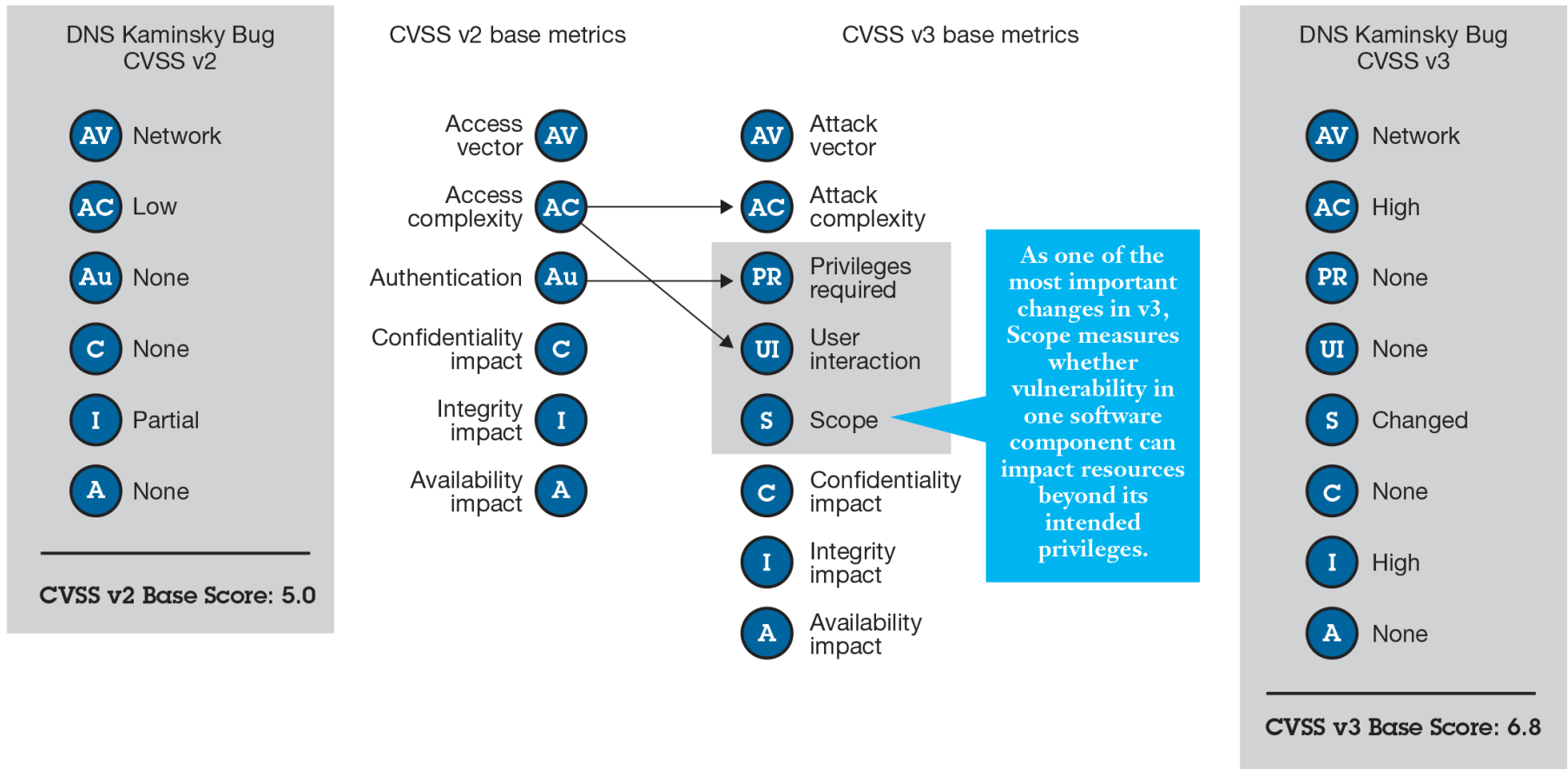



Figure 5. Comparison of DNS Kaminsky Bug (CVE-2008-1447); CVSS scoring from version 2 to version 3


Source: IBM X-Force® Research and Development

New CVSSv3 scoring more accurately reflects vulnerability impact


Heartbleed
CVE-2014-0160




OpenSSL

CVSS v2 5.0	CVSS v3 7.5	
----------------	----------------	---


Shellshock
CVE-2014-6271/7169




Unix Bash shell

CVSS v2 10.0	CVSS v3 9.8	
-----------------	----------------	---

POODLE
CVE-2014-3566/8730



SSL 3.0 Protocol

CVSS v2 4.3	CVSS v3 3.1	
----------------	----------------	---

59% of CISOs strongly agree that the sophistication of attackers is outstripping the sophistication of their organization's defenses

Attacks from the Dark Web



Ransomweb / Ransomware as a Service



Aggressive Financial Malware

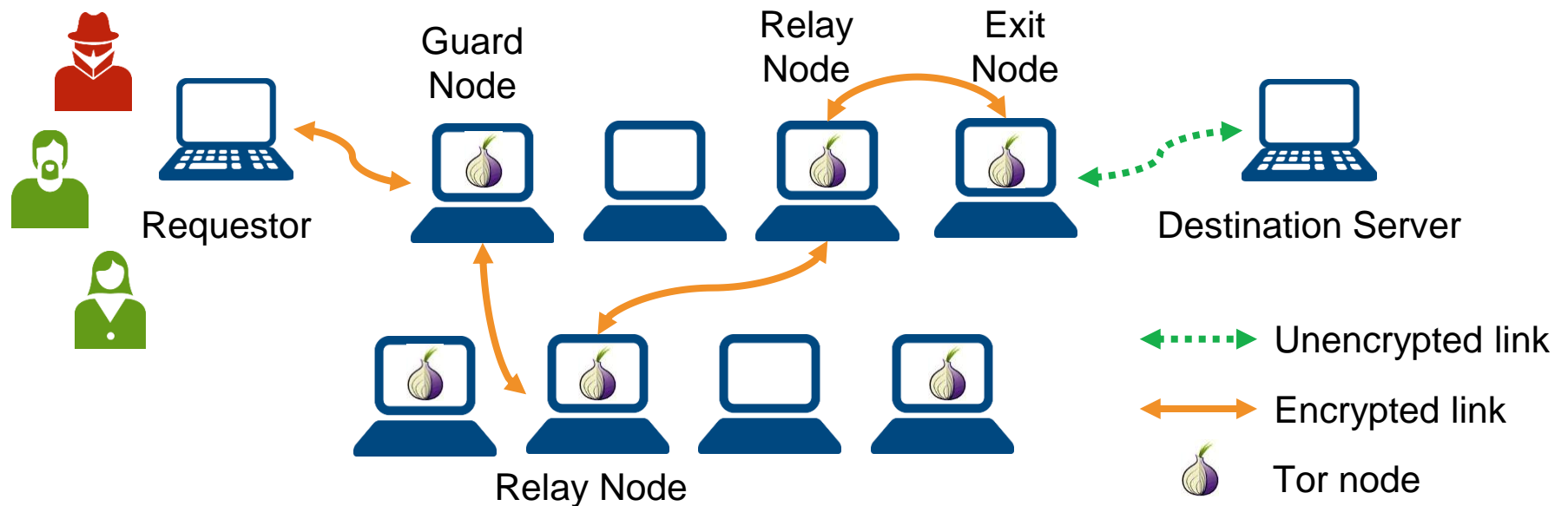


Source: [2014 IBM Chief Information Security Officer Assessment](#)

The Dark Web is comprised of individuals and organizations participating in host-to-host anonymous encrypted communications to execute illicit or illegal activity

Tor was originally designed, implemented and deployed in 2004 as a third-generation onion routing project of the US Naval Research Laboratory to protect government communications.

Because it allows private, encrypted communication, it's now used for nefarious purposes.



Tor provides infrastructure allowing anonymous attackers to operate malicious botnets within the network or transport their nefarious traffic



SQL Injection

SQLi makes up the majority of attacks originating from Tor exit nodes



Vulnerability Scanning

Vulnerability scanning often represents the early stages of an attack

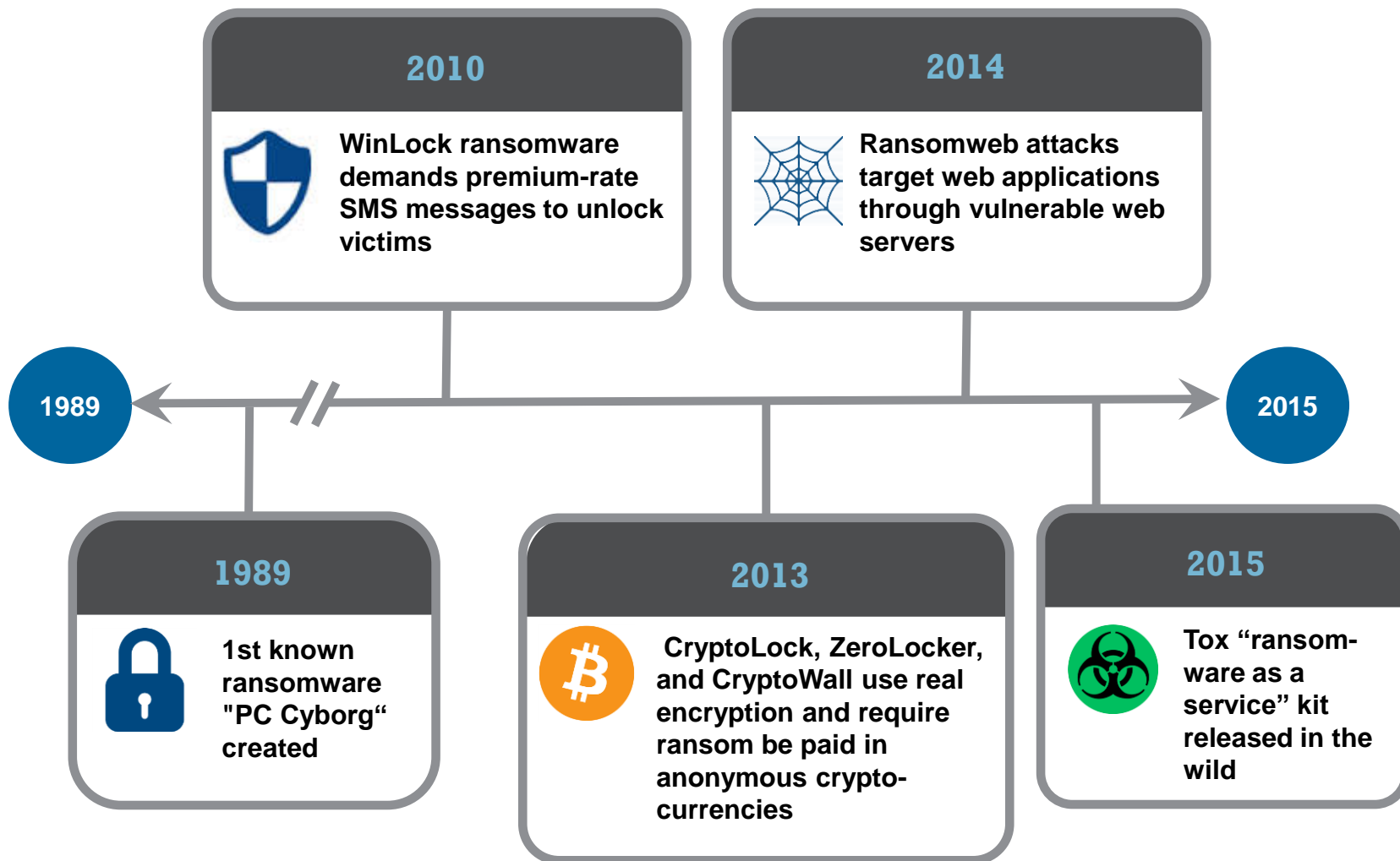


DDoS

DDoS attacks combine Tor-commanded botnets with a sheaf of Tor exit nodes.

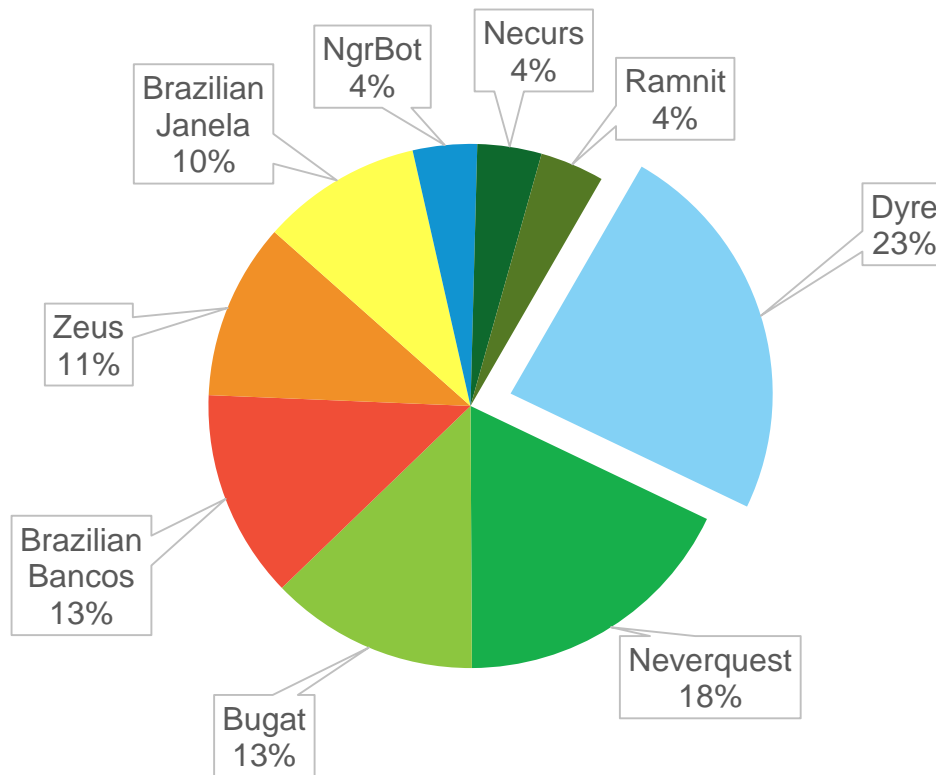


Ransomware reaches a broader range of attackers through "infection as a service" kits



Malware is being developed as a campaign, backed by complex crime methodologies and organizations.

Global Financial-based Malware
Infection Rates
1Q 2015



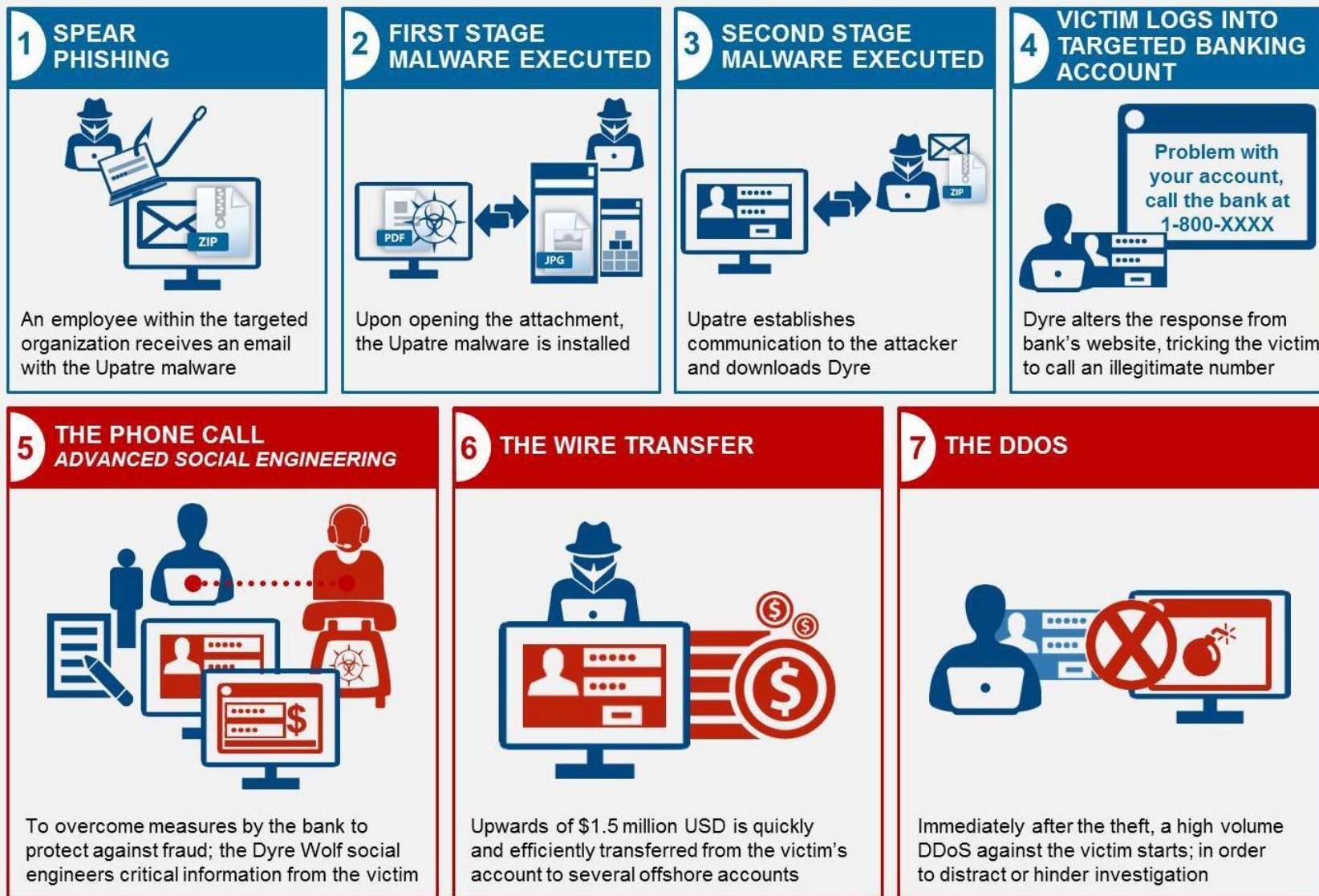
In October 2014, the IBM X-Force malware researchers tracked a very large increase in the infection rate of the Dyre malware, from 500 instances to almost 3,500.

Although always prominent, this spike in infection represented an advancement in the malware:

- Advanced social engineering to steal banking credentials
- Complex process injections
- Added layer of DDoS sprees

Source: IBM MSS, ["Inside the Dyre Wolf malware campaign"](#)

The Dyre Wolf campaign is run by a ring of unusually well-funded, experienced and intelligent people



Source: IBM MSS, "Inside the Dyre Wolf malware campaign"

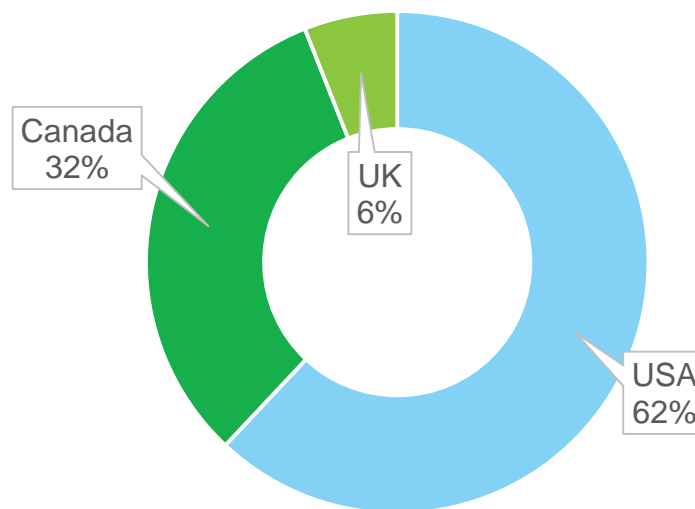
Malware is evolving quicker than ever

CoreBot was discovered by IBM researchers in late August. Within days, evolved samples of the modular CoreBot Trojan took on capabilities of a full-fledged banking Trojan.

Capabilities now include:

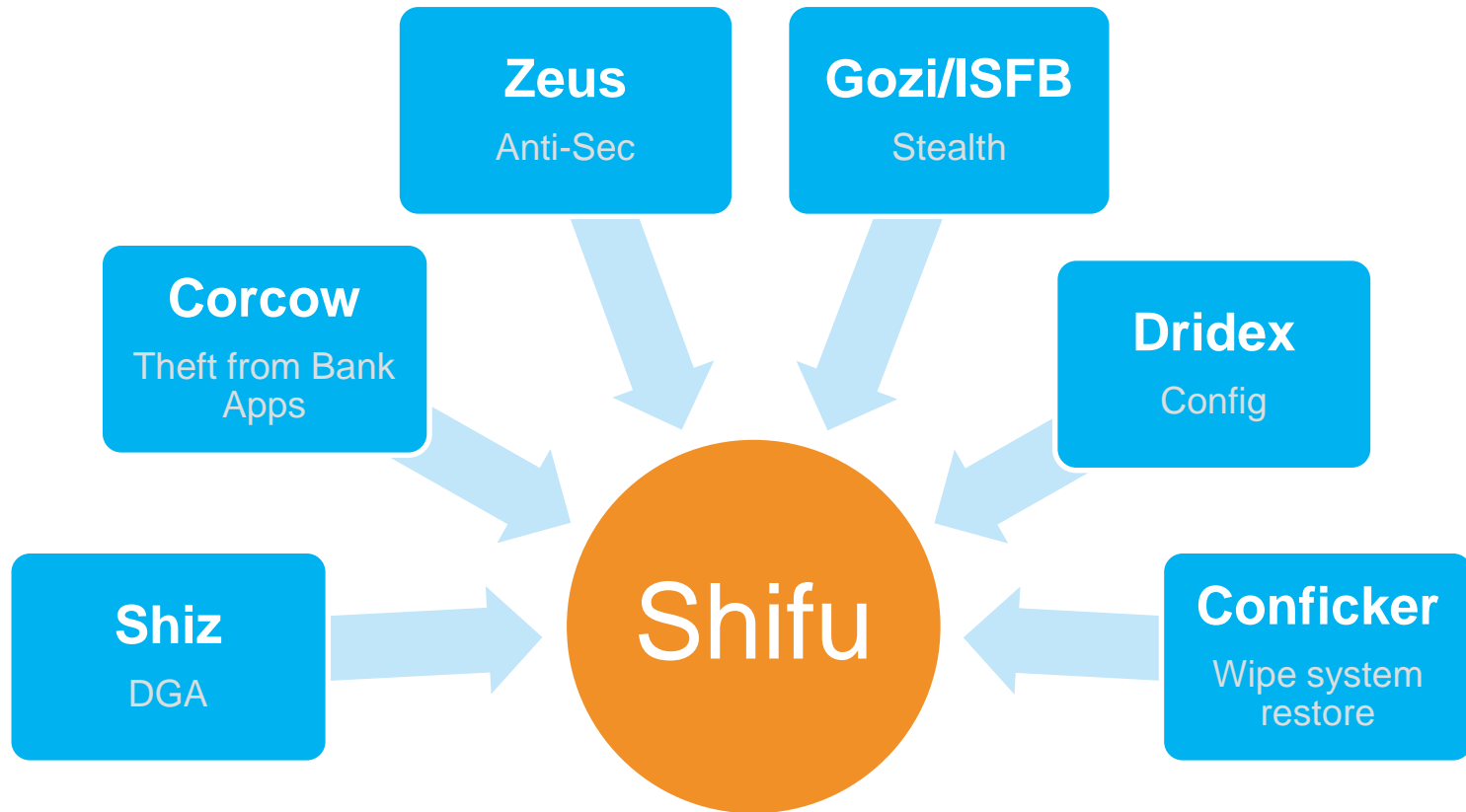
- Browser hooking for IE, Firefox and Chrome
- Generic real-time form-grabbing
- VNC module for remote control
- MitM capabilities for session takeover
- 55 preconfigured URL triggers to target banks
- Custom web-injection mechanism
- On-the-fly web-injections from a remote server

CoreBot Target Countries
As of September 2015



Source: IBM X-Force malware research, "[Watch Out for CoreBot, New Stealer in the Wild](#)" and "[An Overnight Sensation — CoreBot Returns as a Full-Fledged Financial Malware](#)"

The Shifu Trojan took “best of breed” elements from infamous crimeware that preceded it, and now locks them out of Shifu’s territory.



This is the first time we are seeing malware build prevention “rules” for suspicious files, to make sure that the endpoint it’s on remains in its exclusive control from the moment of infection.

What can you do to mitigate these threats?

Preparedness is Key

- Create and practice a broad incident response plan.
- Maintain a current and accurate asset inventory.

Manage your operations

- Keep up with threat intelligence.
- Have a patching solution that covers your entire infrastructure.
- Implement mitigating controls.
- Instrument your environment with effective detection.

Protect your data from ransomware

- Maintain at least one copy of your data not directly mapped visibly as a drive on your computer.
- Technologies that prevent “phone home” operations can help stop earlier iterations of certain ransomware.

Block threats from the dark web

- Apply wholesale blocking at the firewall of Tor nodes identified by frequently-updated directories
- Formulate and issue a comprehensive corporate policy for acceptable use to protect against Tor relays on your own network



IBM Security

- TOP 3** enterprise security software vendor in total revenue
- 20** industry analyst reports rank IBM Security as a **LEADER**
- 133** countries where IBM delivers managed security services
- 10K** clients protected *including...*
- 24** of the top 33 banks in Japan, North America, and Australia



Visit our web page
[IBM.com/security/xforce](https://www.ibm.com/security/xforce)



Watch our videos
[IBM Security YouTube Channel](#)



View upcoming webinars & blogs
[SecurityIntelligence.com](https://www.ibm.com/security/intelligence)



Follow us on Twitter
[@ibmsecurity](#) and [@IBMXforce](#)

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.

THANK YOU

www.ibm.com/security



IBM Security

Intelligence. Integration. Expertise.

© Copyright IBM Corporation 2015. 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. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. 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.