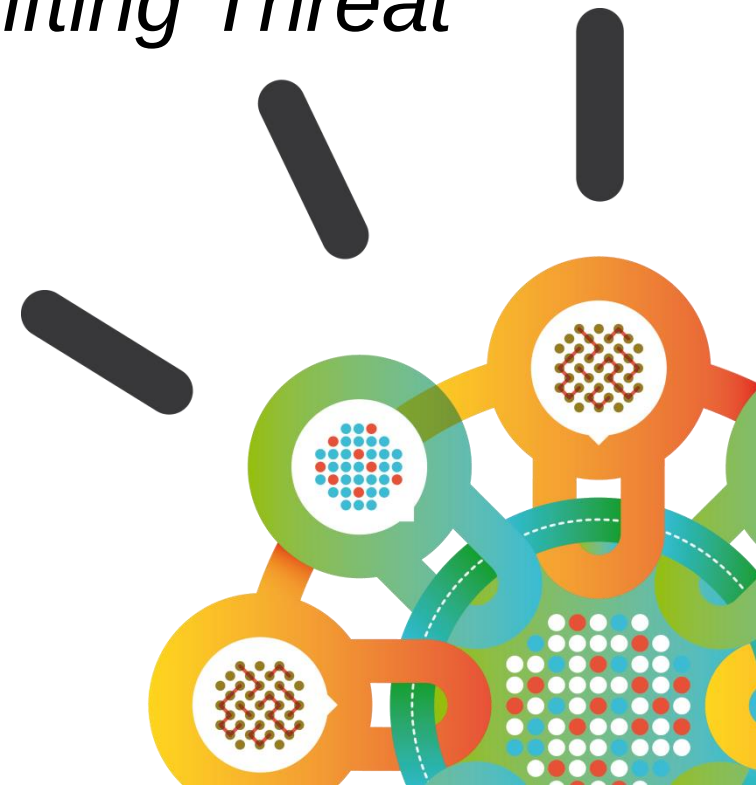
Security Intelligence.
Think Integrated.

IBM X-Force:

New Attack Vectors in the Shifting Threat Landscape

March 2015



IBM X-Force

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

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 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

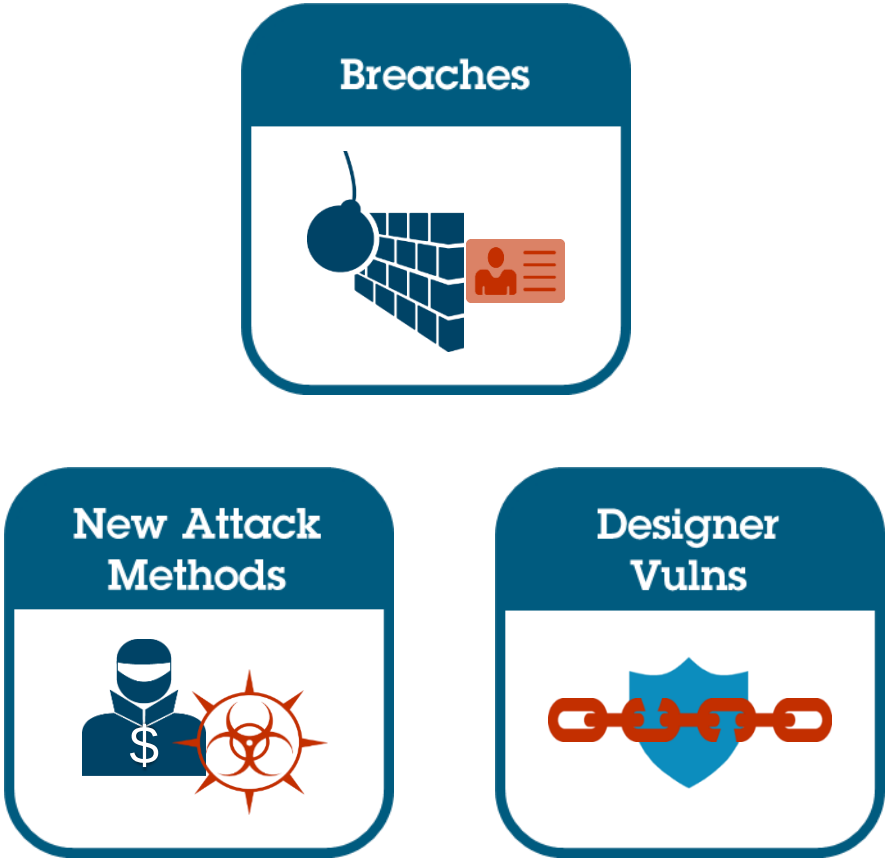
96K+ documented vulnerabilities

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

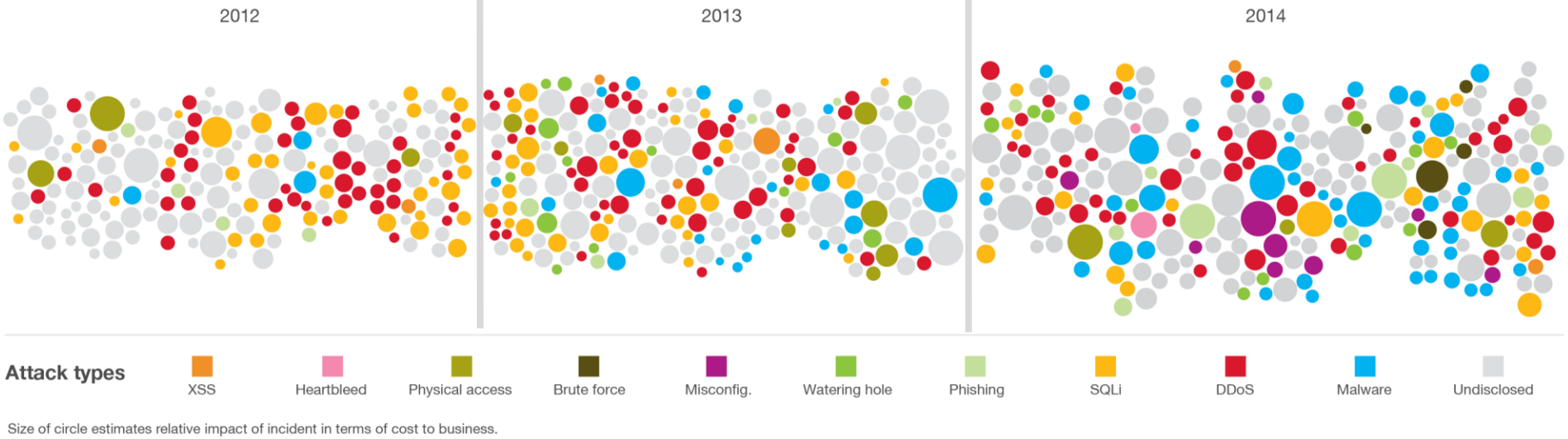
40% increase
in reported data breaches and incidents

Relentless Use of Multiple Methods

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

"Insane" Amounts of Records Breached

42% of CISOs
claim the risk from external threats increased dramatically from prior years.

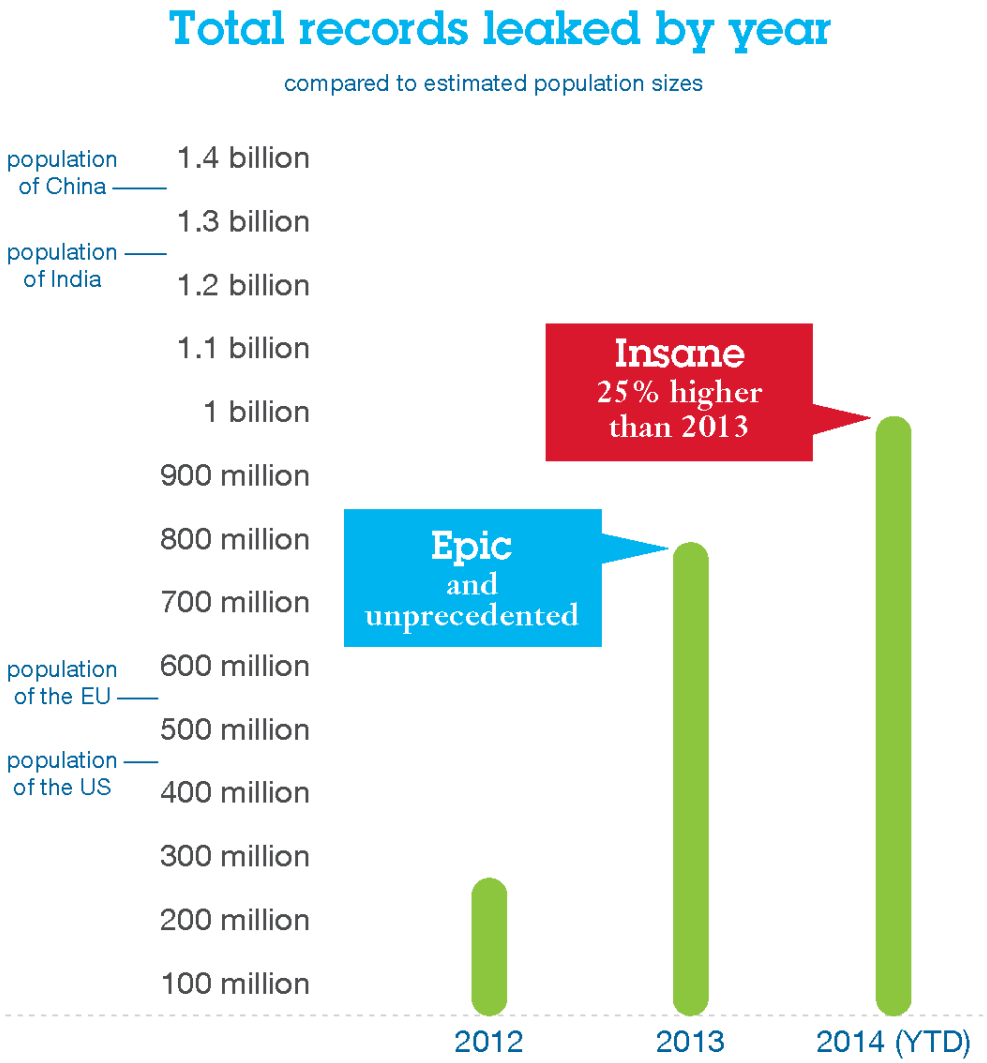


A historical look at security incidents by attack type, time and impact, 2012 through 2014

Source: IBM X-Force® Research and Development

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

Based on pure volume, the total number of records breached in 2014 was nearly 25 percent higher than in 2013



Source: *IBM X-Force Threat Intelligence Quarterly – 1Q 2015*

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

A lack of security fundamentals

- End-user password re-use
- Leaving default passwords on admin systems
- Poor challenge questions for password reset procedures

Cracks in the foundation

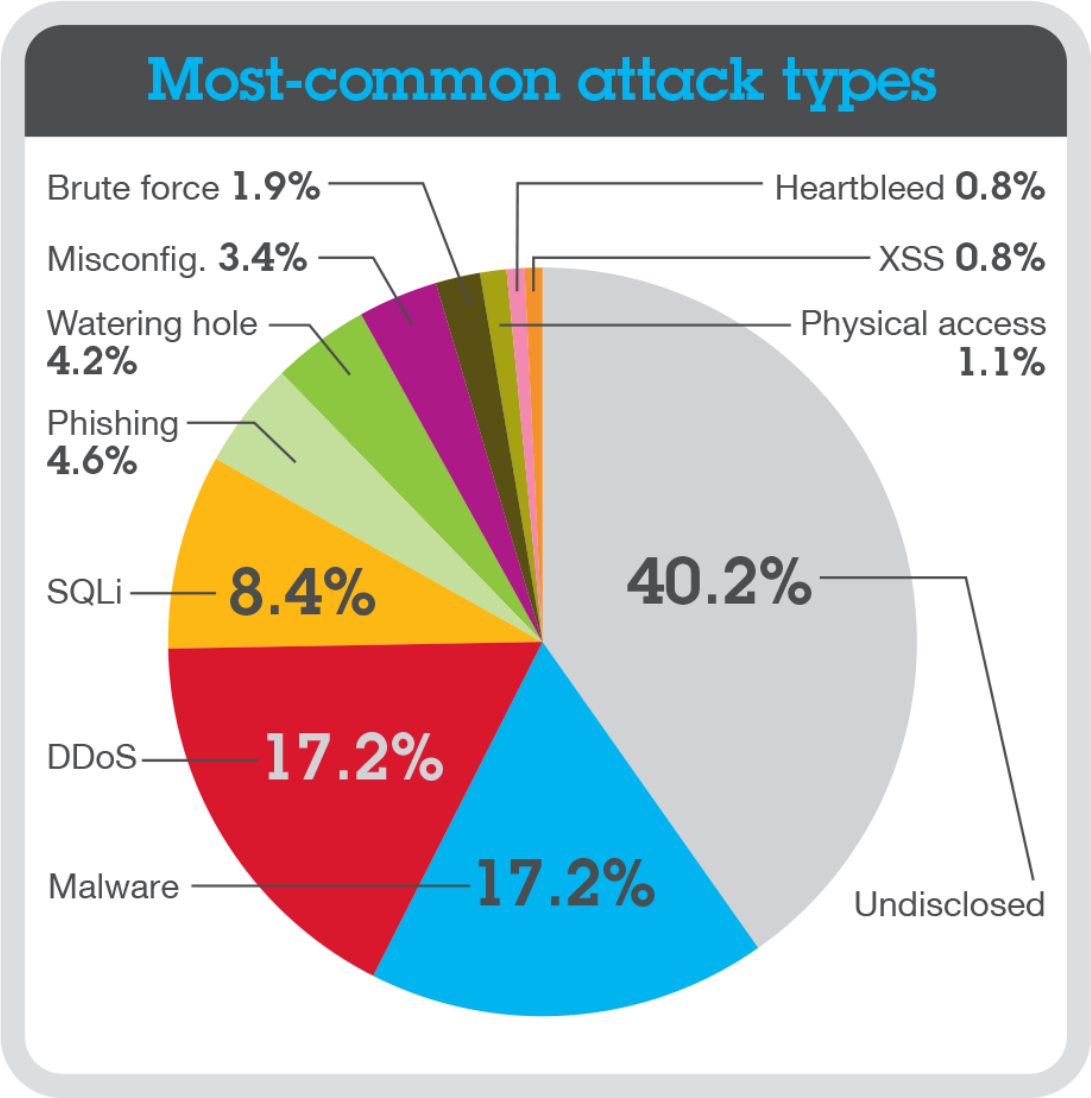
- The same operating systems, open-source libraries and CMS software are prevalent on many websites
- Several of these systems and libraries had vulnerabilities disclosed in 2014

Shrinking privacy in a digital world

- Sensitive photos stored on a cloud service were leaked due to weak passwords
- Private email communications at a major Hollywood studio were released

Source: IBM X-Force Threat Intelligence Quarterly – 1Q 2015

Attackers are applying fundamental attack types in creative, new ways

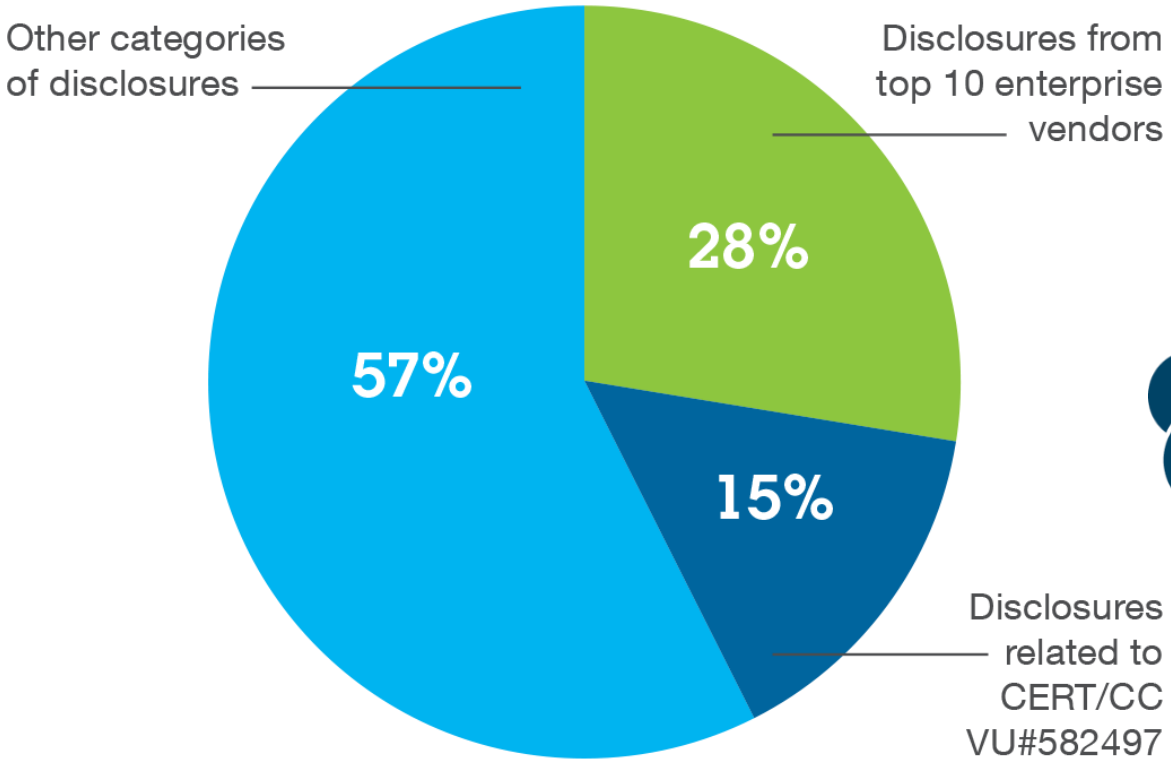


Source: *IBM X-Force Threat Intelligence Quarterly – 1Q 2015*

The 2014 vulnerability forecast shifted drastically when an automated tool identified a class of vulns affecting thousands of Android apps with improper SSL certificate validation

Vulnerability disclosures by category

as percentage of total disclosures in 2014

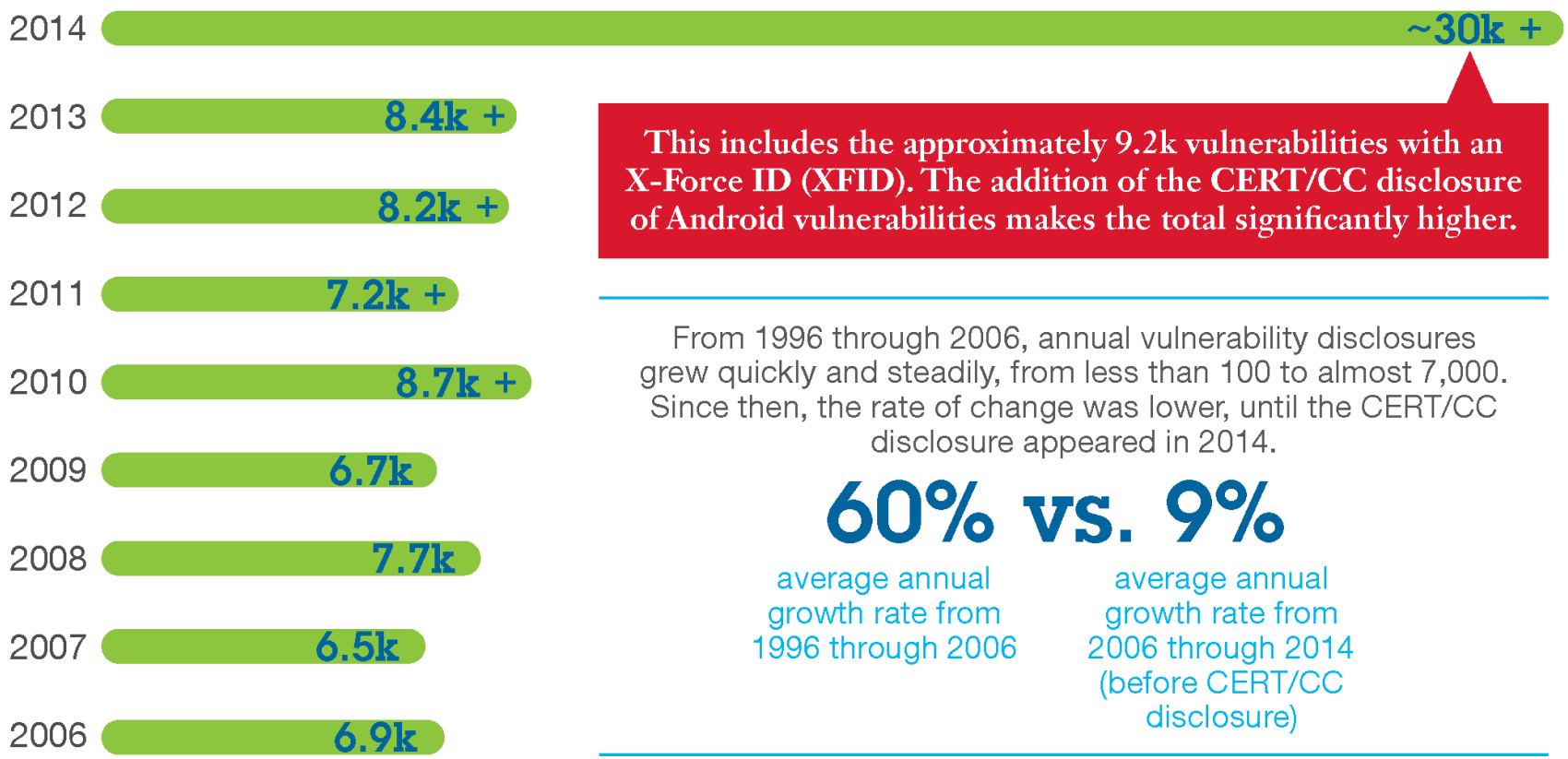


 Source: IBM X-Force Threat Intelligence Quarterly – 1Q 2015

2014 closed with 9,200 new vulns assigned XFIDs, but the total number of vulnerabilities may surge to more than 30,000

Vulnerability disclosures growth by year

1996 through 2014



This includes the approximately 9.2k vulnerabilities with an X-Force ID (XFID). The addition of the CERT/CC disclosure of Android vulnerabilities makes the total significantly higher.

From 1996 through 2006, annual vulnerability disclosures grew quickly and steadily, from less than 100 to almost 7,000. Since then, the rate of change was lower, until the CERT/CC disclosure appeared in 2014.

60% vs. 9%

average annual growth rate from 1996 through 2006

average annual growth rate from 2006 through 2014 (before CERT/CC disclosure)

Source: IBM X-Force Threat Intelligence Quarterly – 1Q 2015

We had our first taste of “designer vulns” in 2014: critical vulnerabilities with clever logos and handles

Heartbleed
CVE-2014-0160

OpenSSL

Apr 2014	2 years old	CVSS 5.0

Shellshock
CVE-2014-6271/7169

Unix Bash shell

Sep 2014	25 years old	CVSS 10.0

POODLE
CVE-2014-3566/8730

SSL 3.0 Protocol

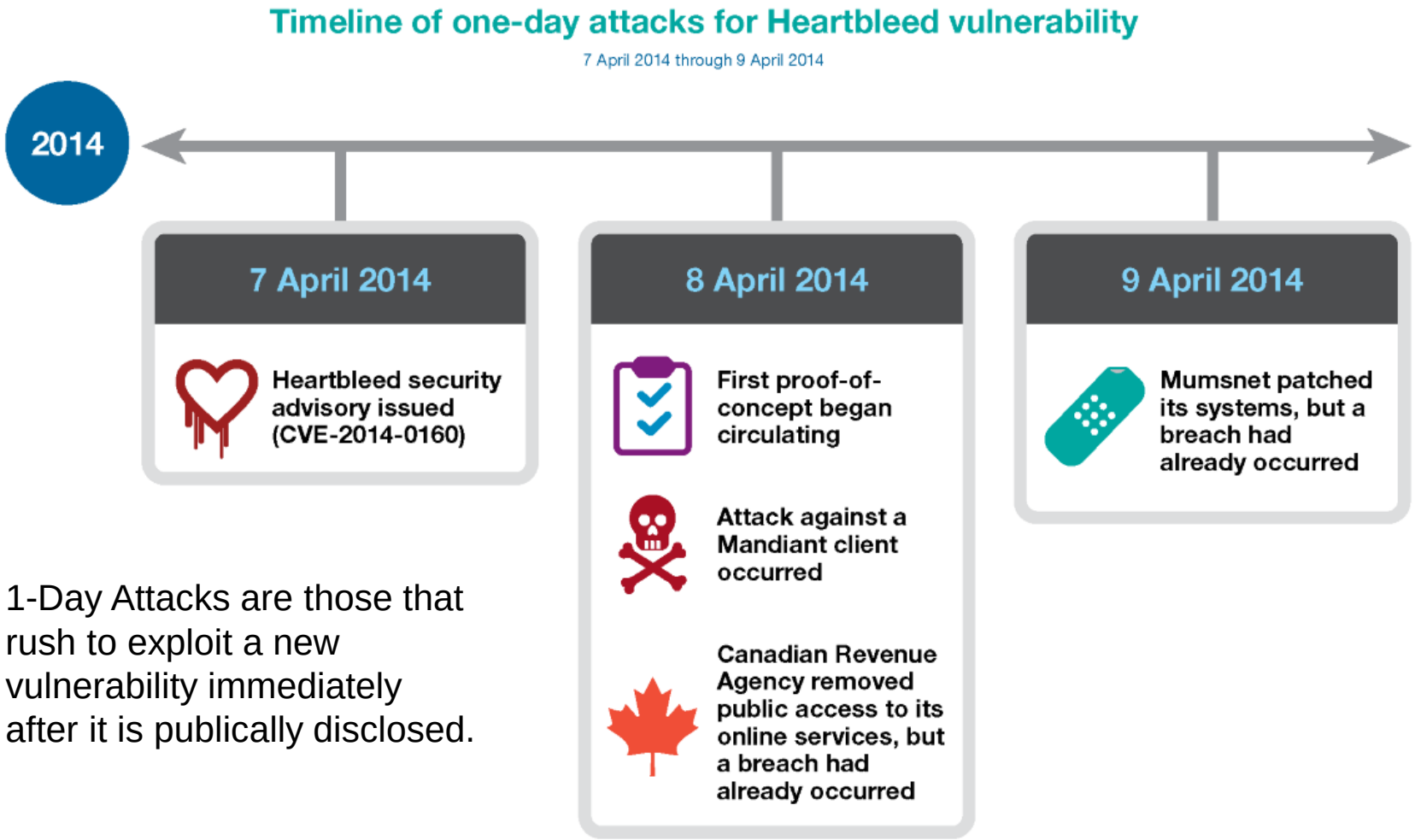
Oct 2014	15 years old	CVSS 4.3

GHOST
CVE-2015-0235

Linux GNU C Library

Jan 2015	15 years old	CVSS 10.0

One-day attack methods demonstrate how quickly attackers rush to exploit a vulnerability like Heartbleed

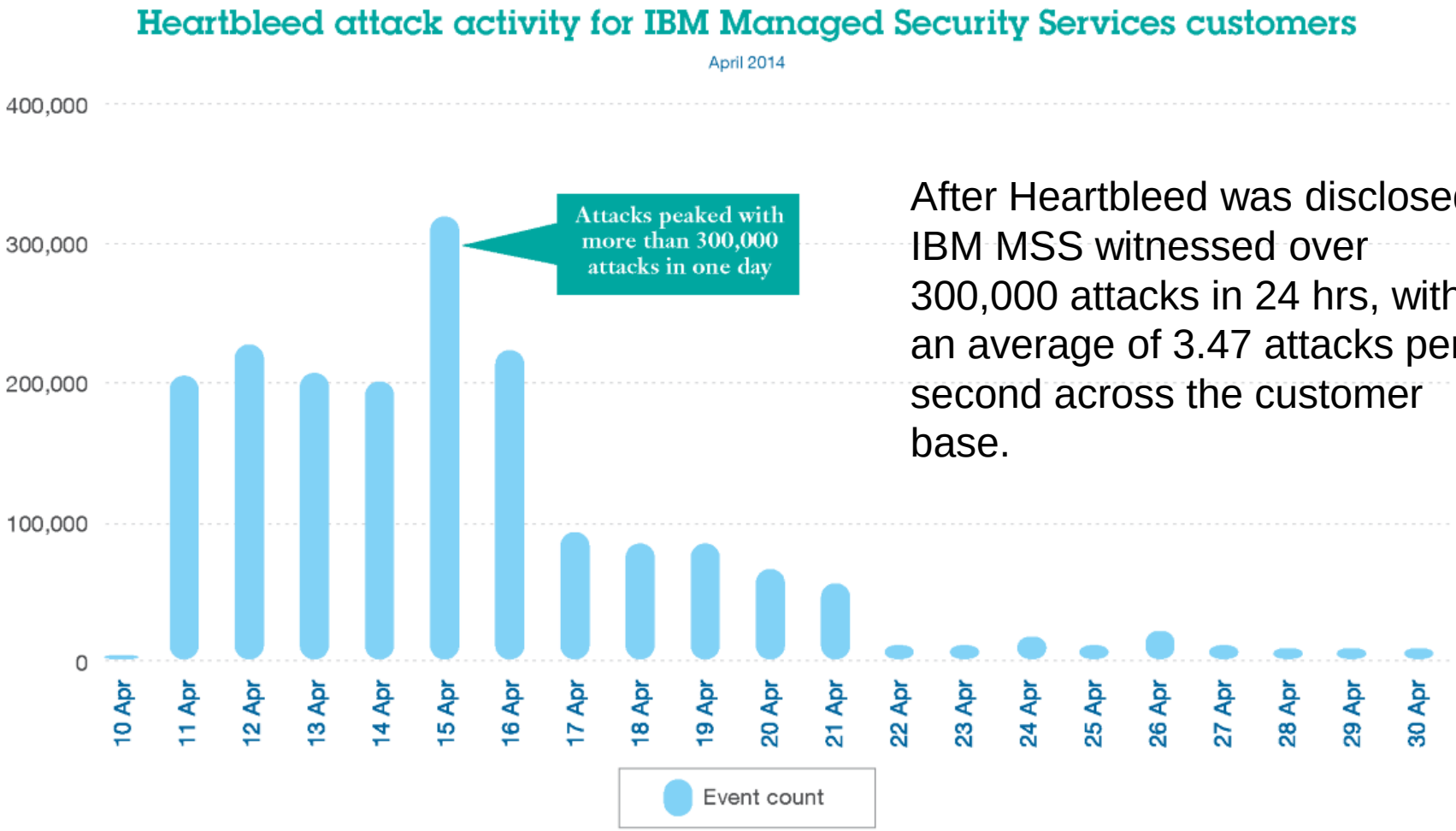


1-Day Attacks are those that rush to exploit a new vulnerability immediately after it is publically disclosed.

Figure 4. Timeline of one-day attacks for Heartbleed vulnerability (CVE-2014-0160), 7 April 2014 through 9 April 2014

Source: IBM X-Force Threat Intelligence Quarterly – 3Q 2014

Heartbleed attacks surged to 3.47 attacks per second after the vulnerability disclosure



After Heartbleed was disclosed, IBM MSS witnessed over 300,000 attacks in 24 hrs, with an average of 3.47 attacks per second across the customer base.

Figure 1. Attack activity related to the Heartbleed vulnerability, as noted for IBM Managed Security Services customers, in April 2014

Source: IBM X-Force® Research and Development

 Source: IBM X-Force Threat Intelligence Quarterly – 3Q 2014

The disclosure of the Shellshock bug in September brought immediate exploit attempts

Patching the original vulnerability was complicated by the development of additional exploit techniques, resulting in additional CVE numbers created

1992 ⟷ 2014

1992

Vulnerability in Bash shell introduced in Linux v1.14

24 Sep 2014

Shellshock vulnerability disclosed in CVE 2014-6271

Vendor patch for CVE 2014-6271 found insufficient. Add'l CVE 2014-7169 created.

25 Sep 2014

X-Force elevates AlertCon level to a 3

Additional CVEs created to document Shellshock

27 Sep 2014

IBM MSS observes 1000% increase above average of the attack signature Command_Shell_ Injection across customer base

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

IBM X-Force and Trusteer researchers uncovered several new attack methods in 2014.

Source: 2014 IBM Chief Information Security Officer Assessment

Massively Distributed APT malware is being used to target industries beyond traditional financial targets

Massively Distributed

- Off the shelf malware, not custom designed
- Using mass distribution campaigns
- Millions of machines already infected!

Comprehensive Menu of Advanced Capabilities

- Keylogging and screen capturing
- Remote code execution
- Full remote control

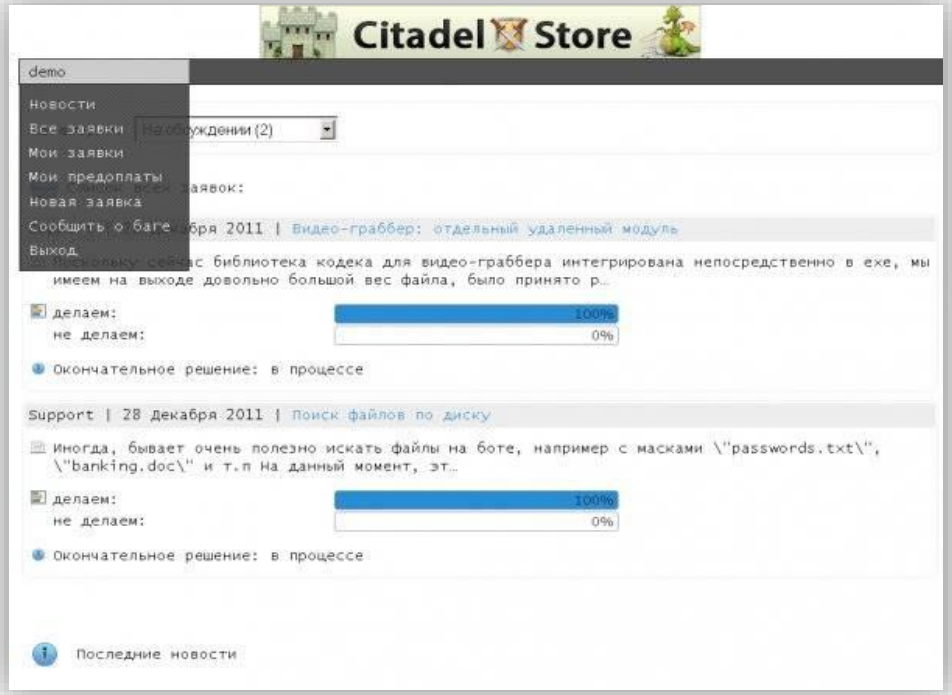
Able to be Repurposed

- Communicates with a C&C
- Receives operational instructions via config file
- Config file can be updated with new operational instructions

Highly Evasive

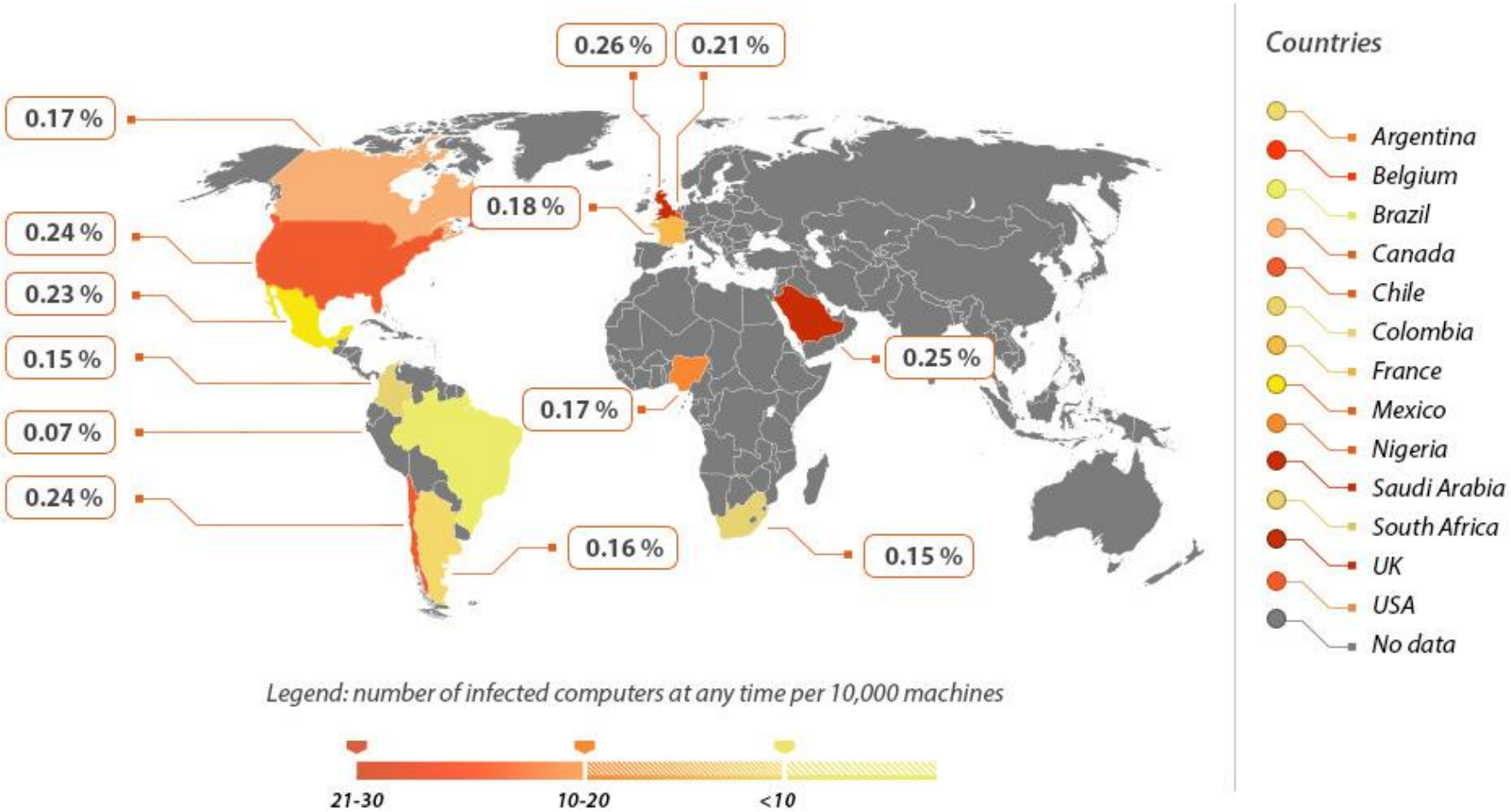
- Sophisticated evasion techniques used to bypass detection
- Can remain stealthy on the machine for lengthy periods of time

Citadel is available for sale on the Russian underground, with new features prioritized by crowdsourcing to target new industries

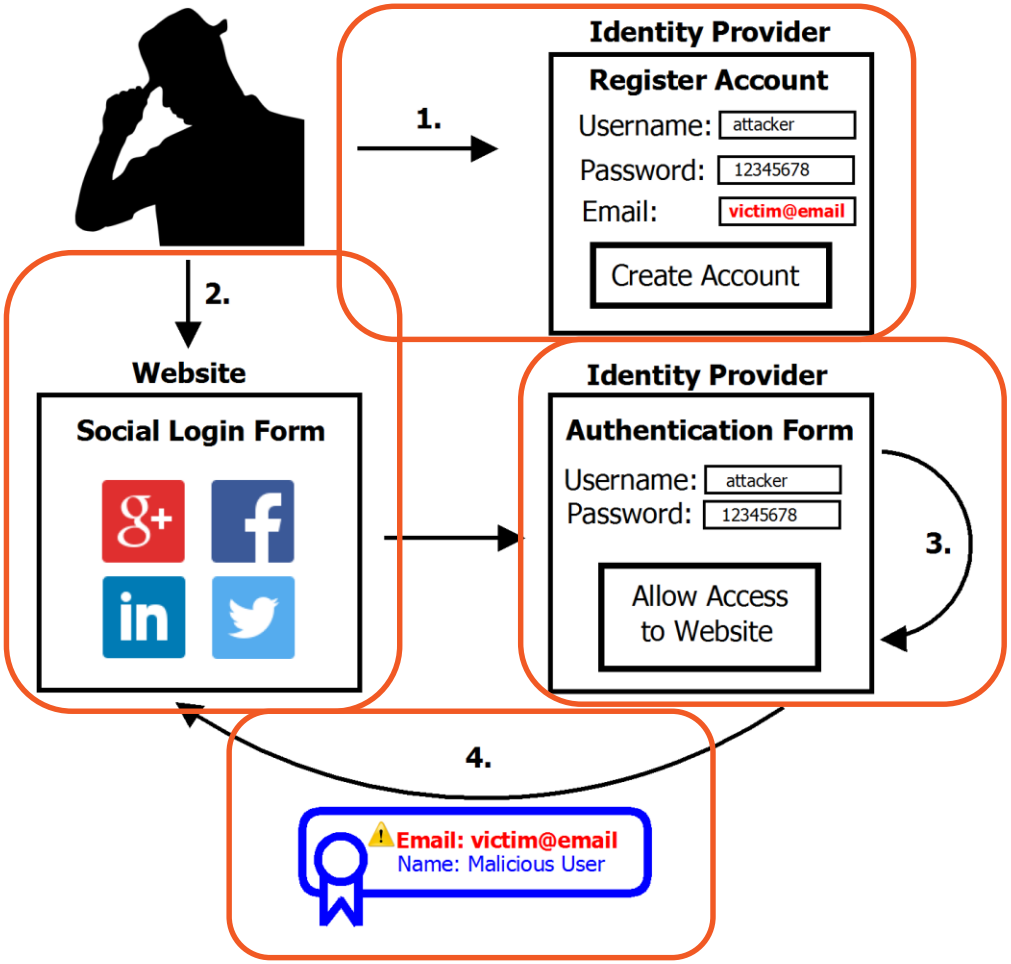


An average of 1 in 500 machines is infected with a Mad APT at any point in time

Infection Rates for Massively Distributed APT Malware by Country



The "SpoofedMe" attack takes advantage of vulnerabilities in social login identity providers and design issues in relying websites to gain user credentials



1. The attacker registers a new account with LinkedIn using the email from the victim's Slashdot

2. The attacker surfs to Slashdot and chooses "Sign In With LinkedIn". The attacker is redirected to the authentication

3. On LinkedIn, the attacker enters the new credentials (from Step 1) and agrees to pass

4. If successful, one of these happens:

- Slashdot logs the attacker in to the victim's account.
- Slashdot links the attacker's account with the victim's existing one.

IBM Security Trusteer researchers discovered the KL-Remote remote overlay toolkit that performs a “virtual mugging” of an end user’s computer

KL-Remote can bypass traditional protection methods:

1. Username/ Password
2. Two-Factor Authentication
3. Device Identification

What can you do to mitigate these threats?

- **Keep up with threat intelligence.**
- **Maintain a current and accurate asset inventory.**
- **Have a patching solution that covers your entire infrastructure.**
- **Implement mitigating controls.**
- **Instrument your environment with effective detection.**
- **Create and practice a broad incident response plan.**

Connect with IBM X-Force Research & Development

Twitter
@ibmsecurity and @ibmxforce

IBM X-Force Threat Intelligence
Quarterly and other research reports:
http://www.ibm.com/security/xforce/

IBM X-Force Security Insights Blog
www.SecurityIntelligence.com/topics/x-force

Find more on SecurityIntelligence.com

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