Paul A. Strassmann

New Canaan Mens Club – January 9, 2015

- From individuals to organized groups.
- Drug cartels, mafias, terrorist cells and nation-states.

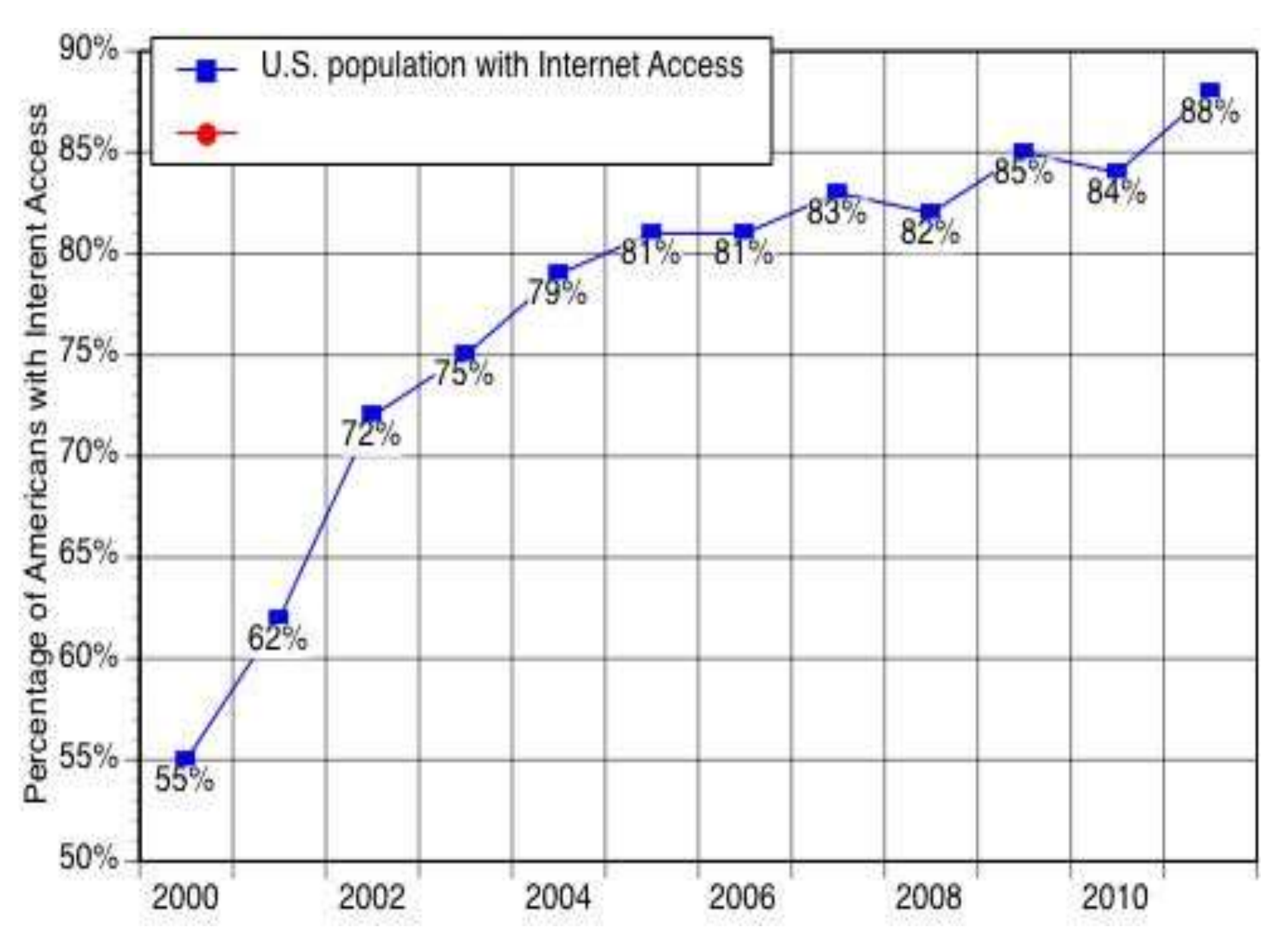
RAND Corporation. http://www.rand.org/pubs/research_reports/RR610.html

- Defenders protect 100.0%, all times.
- Espionage succeeds in 0.01% of time.

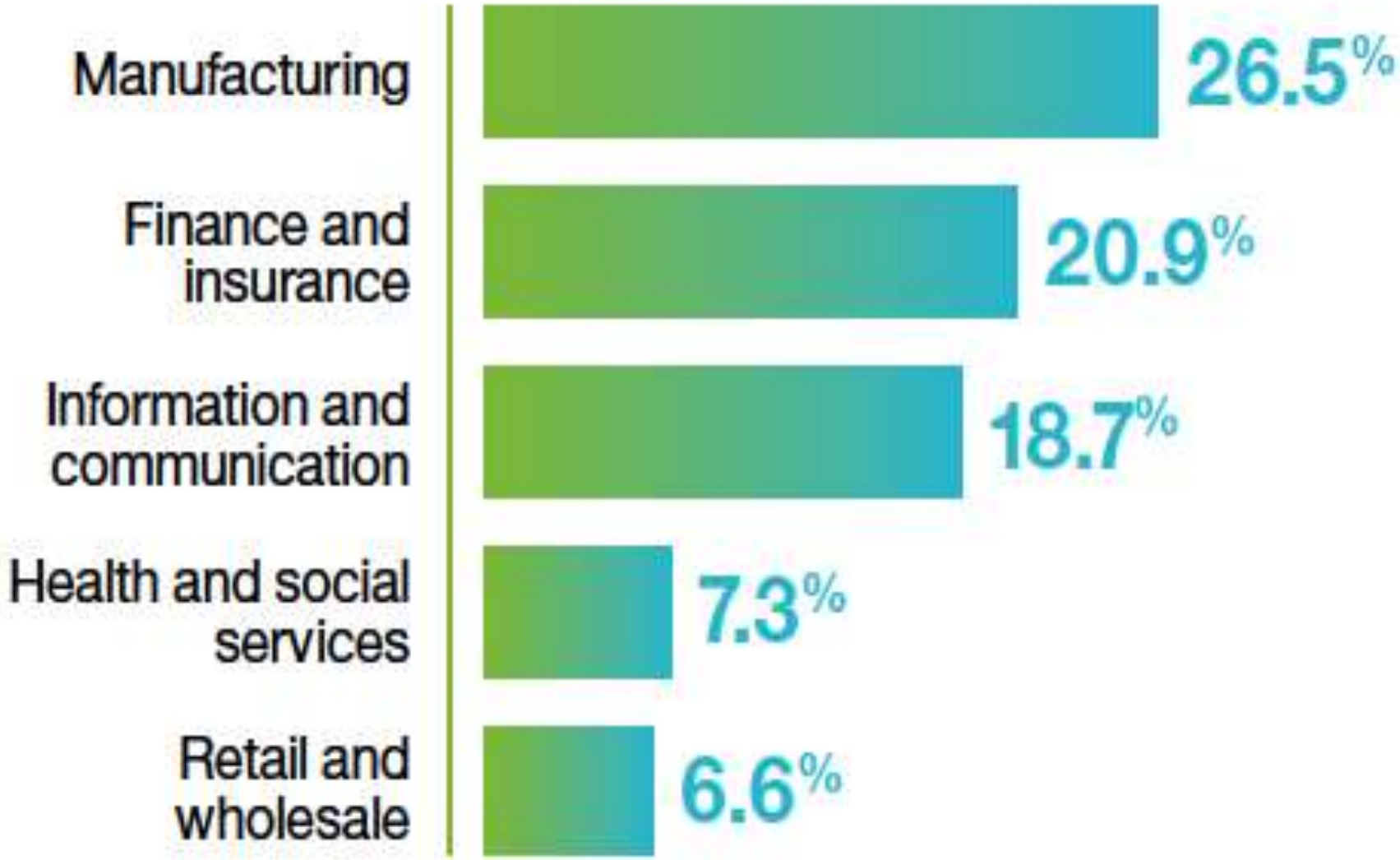
Number Internet Devices = 15+ Billions

E-mail addresses = 2
Facebook, Twitter, Linkedin = 3
Personal and work numbers = 2
Financial Accounts = 4
Health = 3
Federal, State, Municipal = 3
eBay, Amazon = 3
System ID and badges = 2

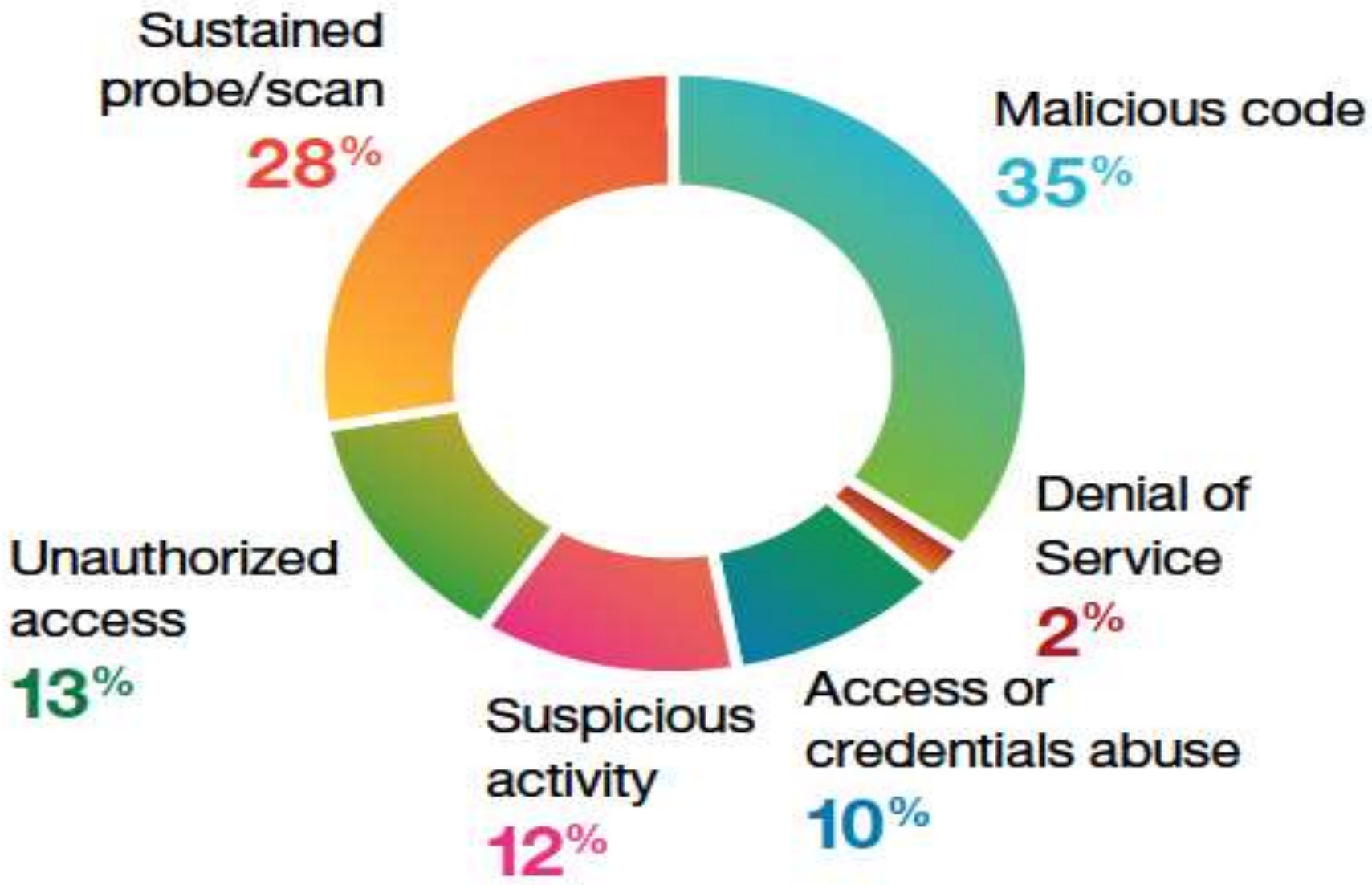
Number of Digital Identities = 50+ Billions


U.S. population with Internet Access
Percentage of Americans with Interent Access
90%
85%
80%
75%
70%
65%
60%
55%
50%
55%
62%
72%
75%
79%
81%
81%
83%
82%
85%
84%
88%
2000
2002
2004
2006
2008
2010

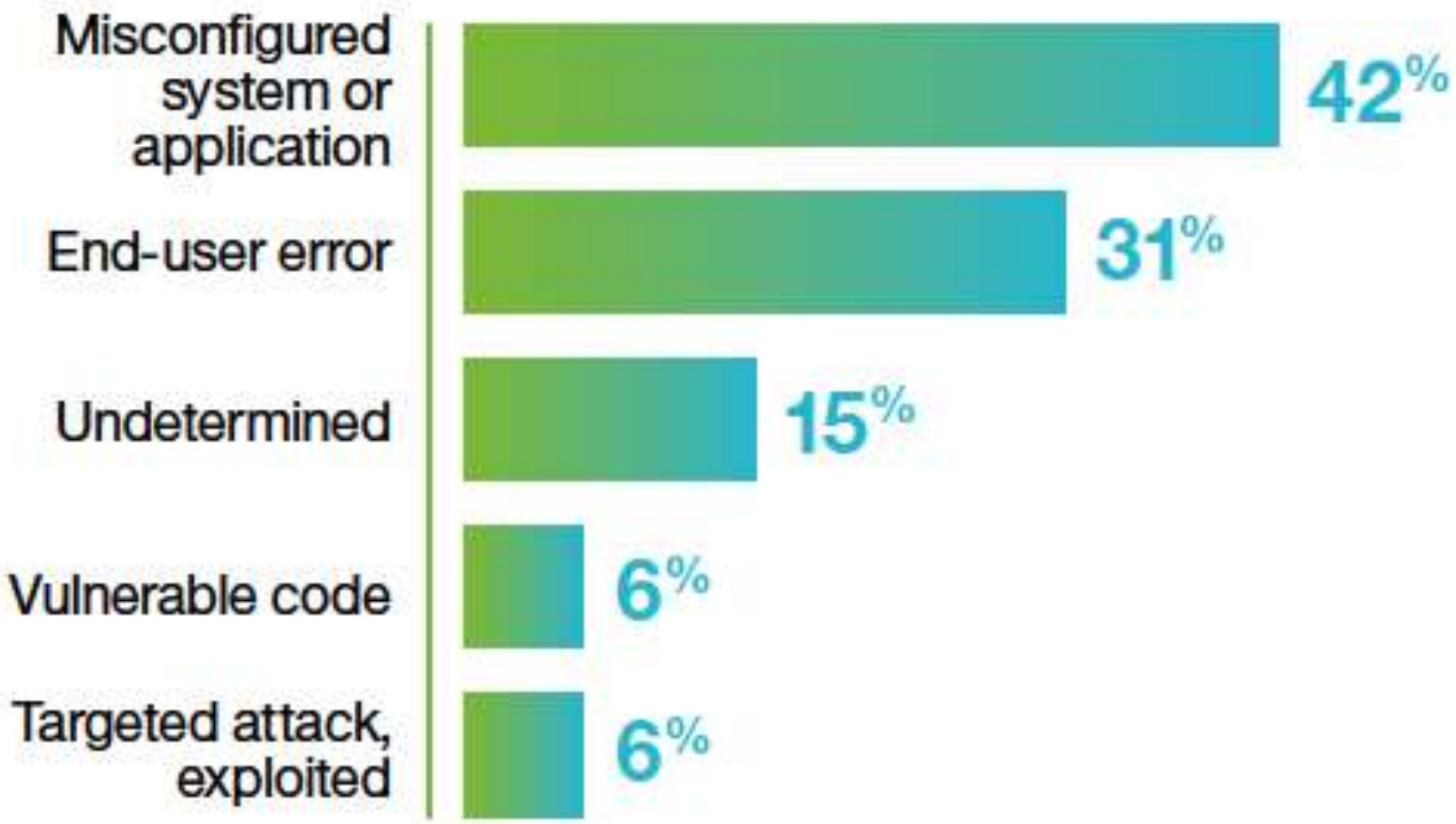
Incident rates across monitored industries

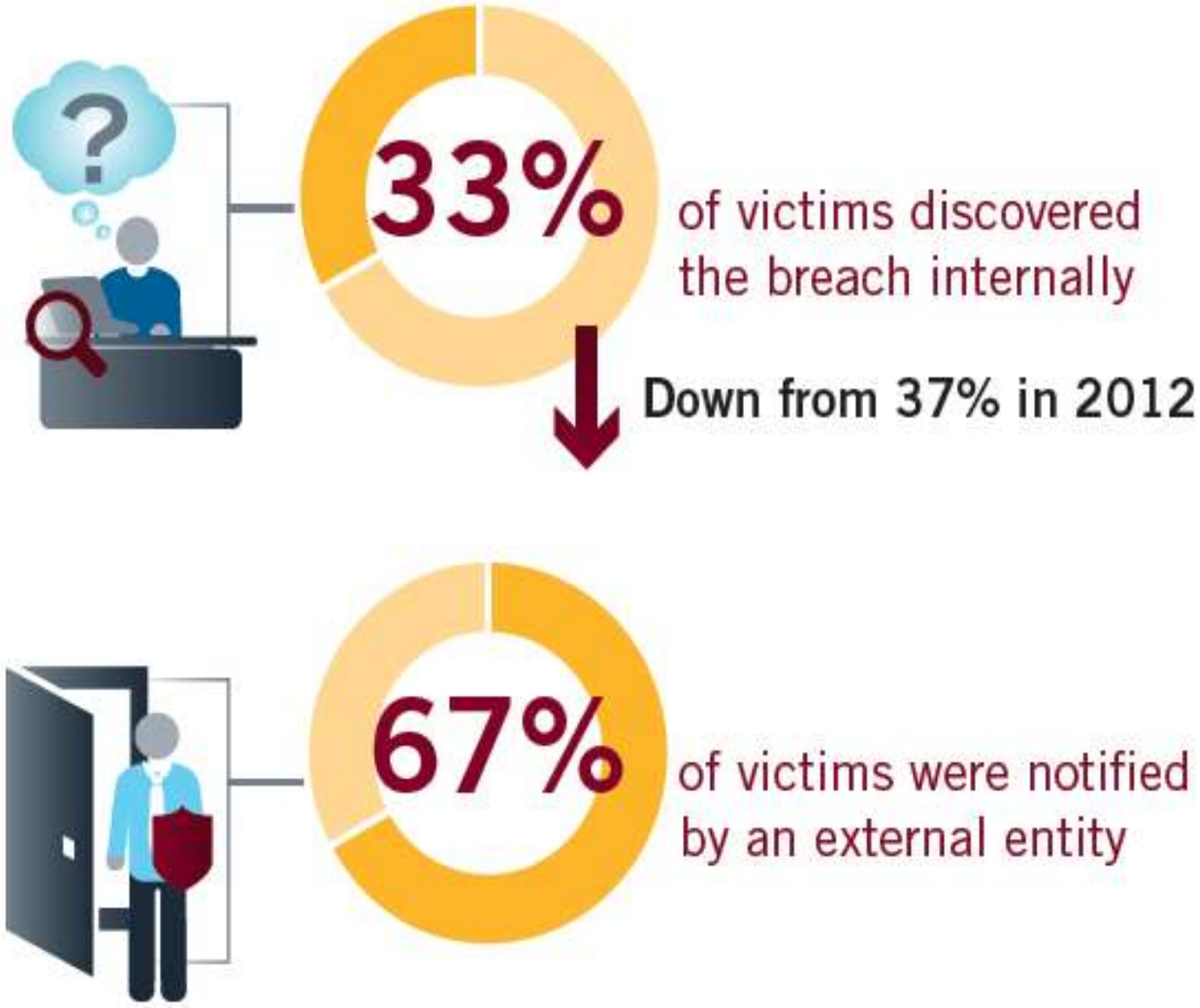


Categories of incidents



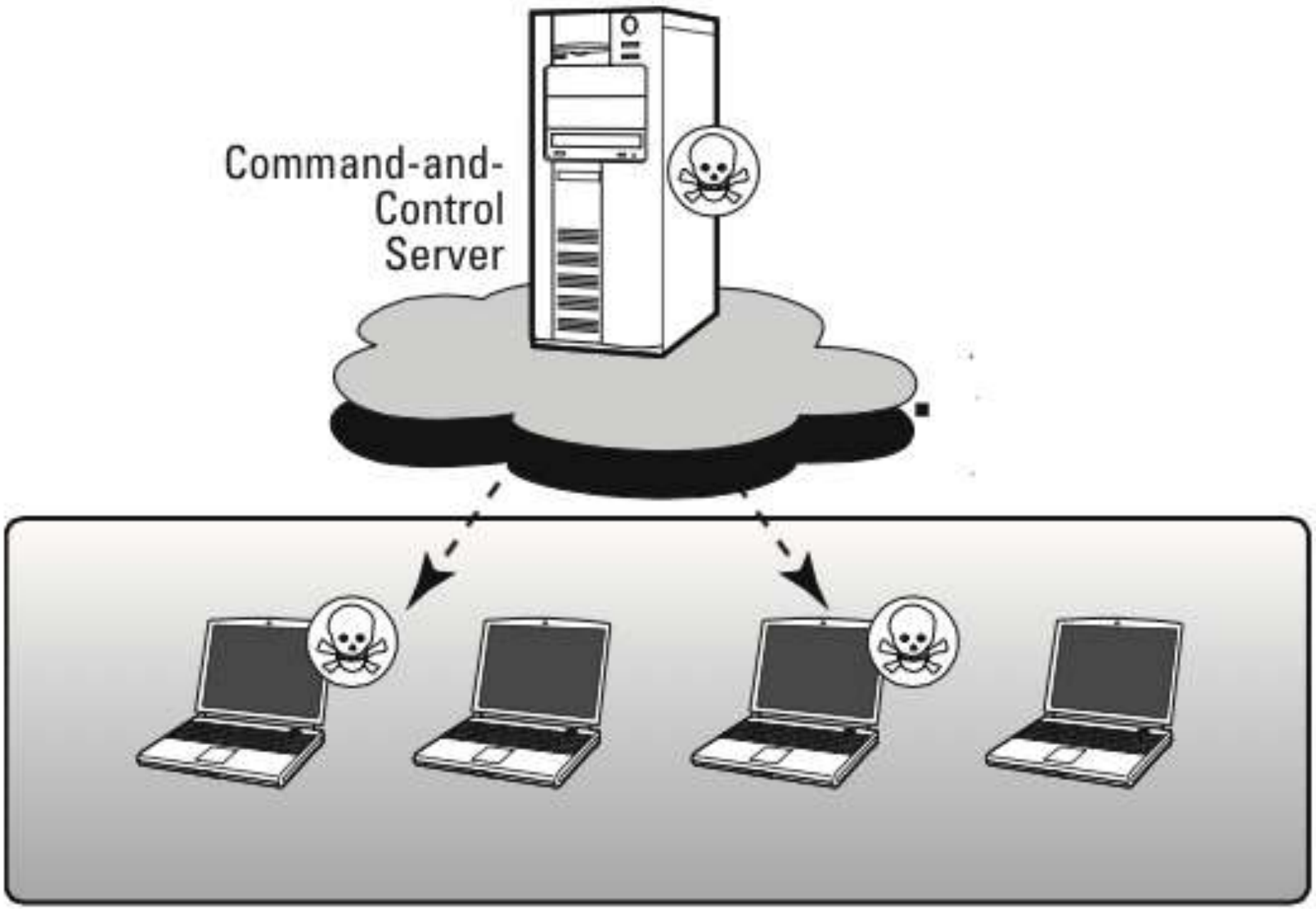
How breaches occur

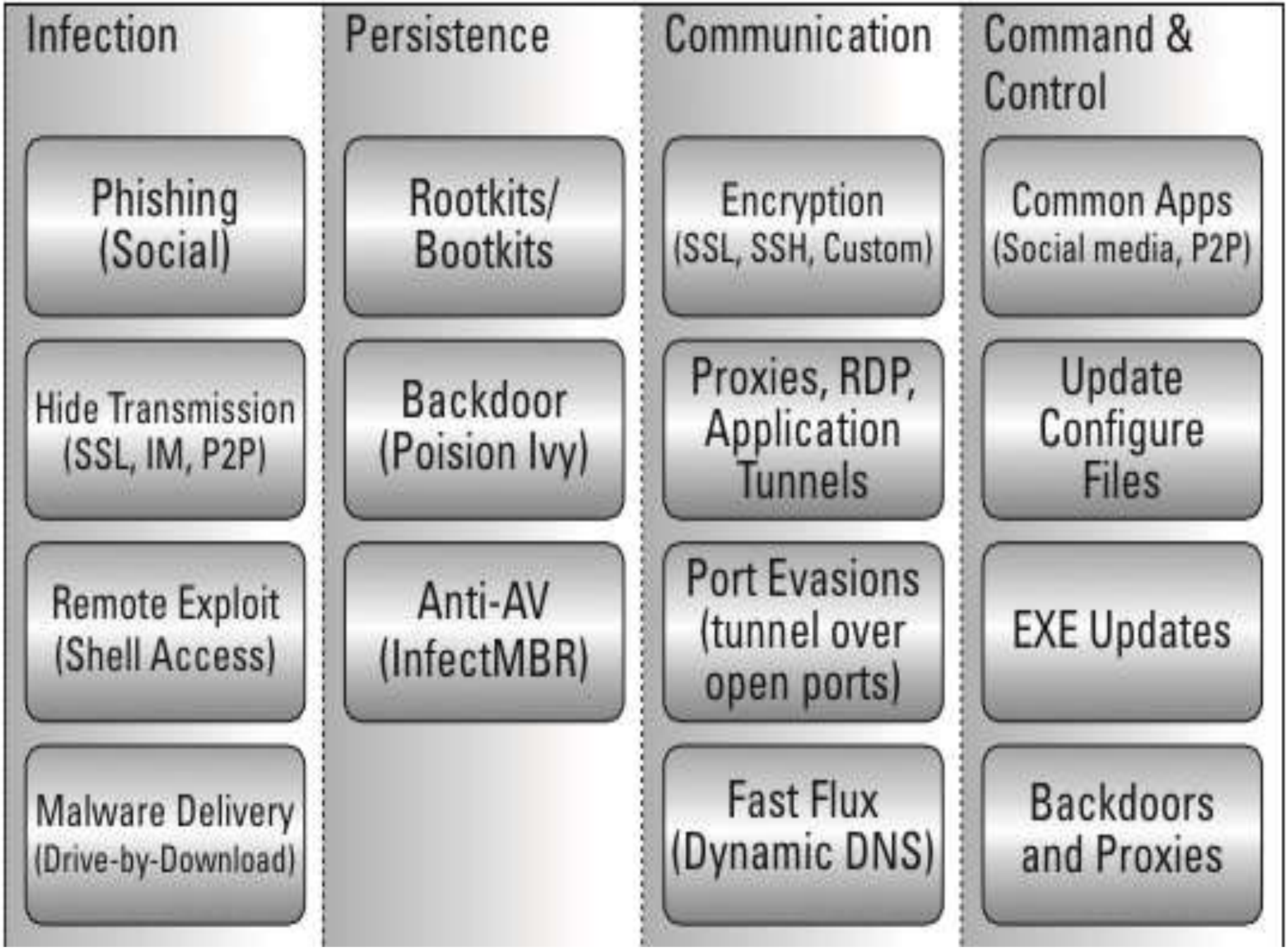




http://www.fireeye.com/blog/corporate/2014/04/annual-m-trends-report-looks-beyond-the-breach.html

http://www.fireeye.com/blog/corporate/2014/04/annual-m-trends-report-looks-beyond-the-breach.html


Command-and-
Control
Server


Infection
Persistence
Communication
Command & Control
Phishing (Social)
Rootkits/ Bootkits
Encryption (SSL, SSH, Custom)
Common Apps (Social media, P2P)
Hide Transmission (SSL, IM, P2P)
Backdoor (Poision Ivy)
Proxies, RDP, Application Tunnels
Update Configure Files
Remote Exploit (Shell Access)
Anti-AV (InfectMBR)
Port Evasions (tunnel over open ports)
EXE Updates
Malware Delivery (Drive-by-Download)
Fast Flux (Dynamic DNS)
Backdoors and Proxies

Homeland Security

Federal Bureau of Investigation

JOINT INDICATOR BULLETIN

Distributed as TLP: GREEN

Reference Number: JIB-14-20199

Destructive Malware

09 December 2014

DHS and FBI will actively update this document as more information becomes available.

Summary

This Joint Indicator Bulletin (JIB)[1] is the result of efforts between the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC)/United States Computer Emergency Readiness Team (US-CERT) and the Federal Bureau of Investigation (FBI) to highlight known cyber threat indicators.

- Typical large firm receives 50,000 intrusion/day
- Pentagon reports 10 million attempts/day
- Nuclear Security Admin: 10 million hacks/day

SOURCE (March 8, 2013):
http://www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/

- New Malicious Web Domains/day 74,000
- Web Attacks Blocked/day 247,350
- Bot Infections/day 3.4 millions
- Avg. number of stolen identities 604,826

* http://www.symantec.com/- 69 million sensors, 2013

U.S. Critical Infrastructure

- Chemicals
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Services
- Pharmaceuticals
- Public Safety
- Public Health
- Information Technology
- Nuclear Reactors
- Transportation

Source of Losses

- Cyber espionage
- Cybertheft
- Cybercrime
- Loss of sensitive business information
- Service and employment disruption
- Insurance, and recovery costs
- Competitive damage
- Reputational damage
- Loss of intellectual property
- Loss of intangible assets

Sources of Cyber Attacks

- Hactivists
- Theft by Criminals
- Organized Crime
- Insider Compromises
- Economic Espionage
- Information Warfare
  - Government
  - Government proxies

U.S. Costs of Cyber Crime

- Estimated Cost: $100 billion to $500 billion
- Loss of 500,000 jobs
- Loss to national security

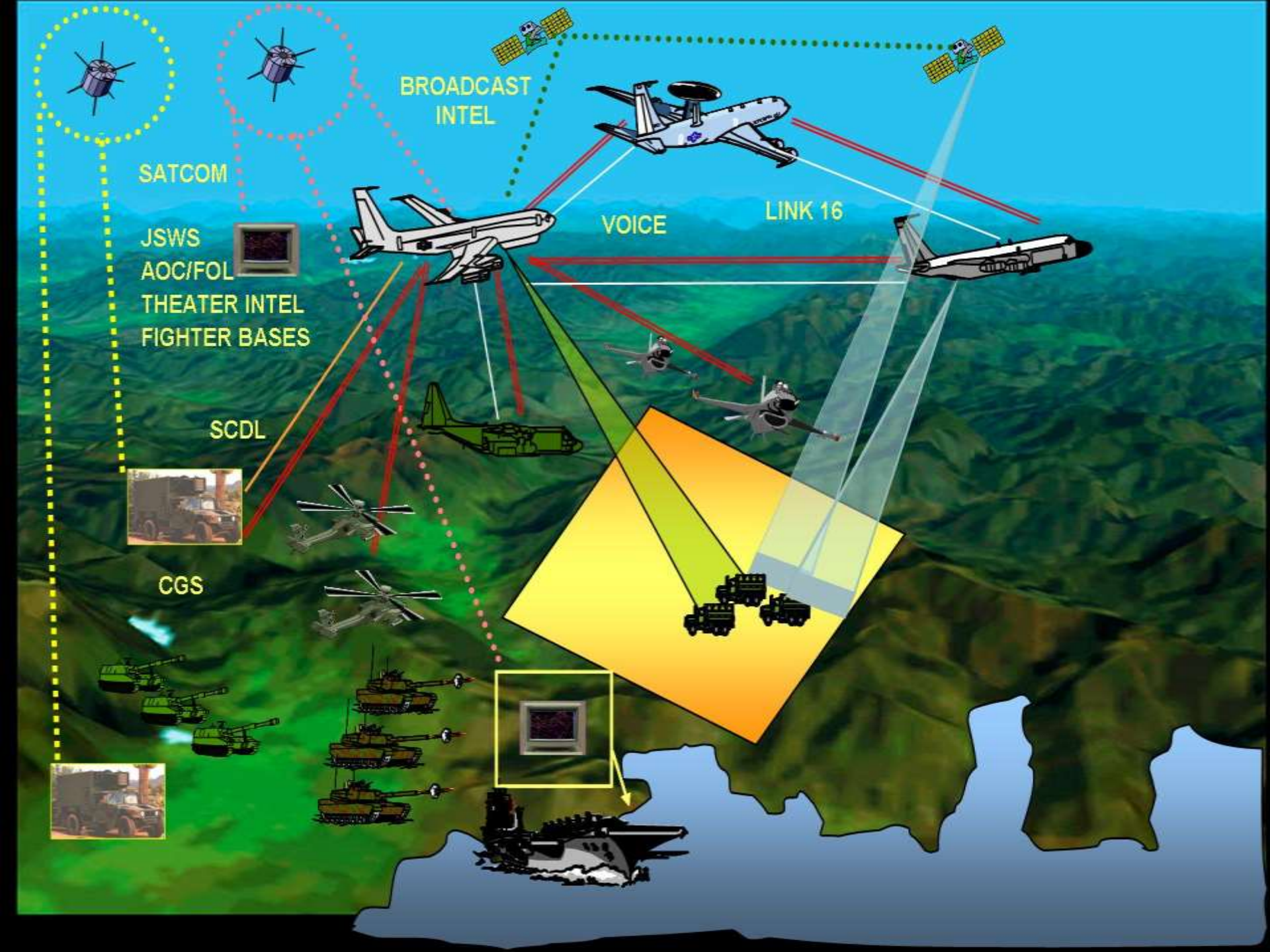
SOURCE: https://csis.org/event/estimating-cost-cyber-crime-and-cyber-espionage

Pixel Tracker Bug Advertised (November 15, 2014)

- Available for private database of 140,000.
- Delivers e-mails, passwords, usernames and private messages of all the members.
- Price: $90 via BitCoin.

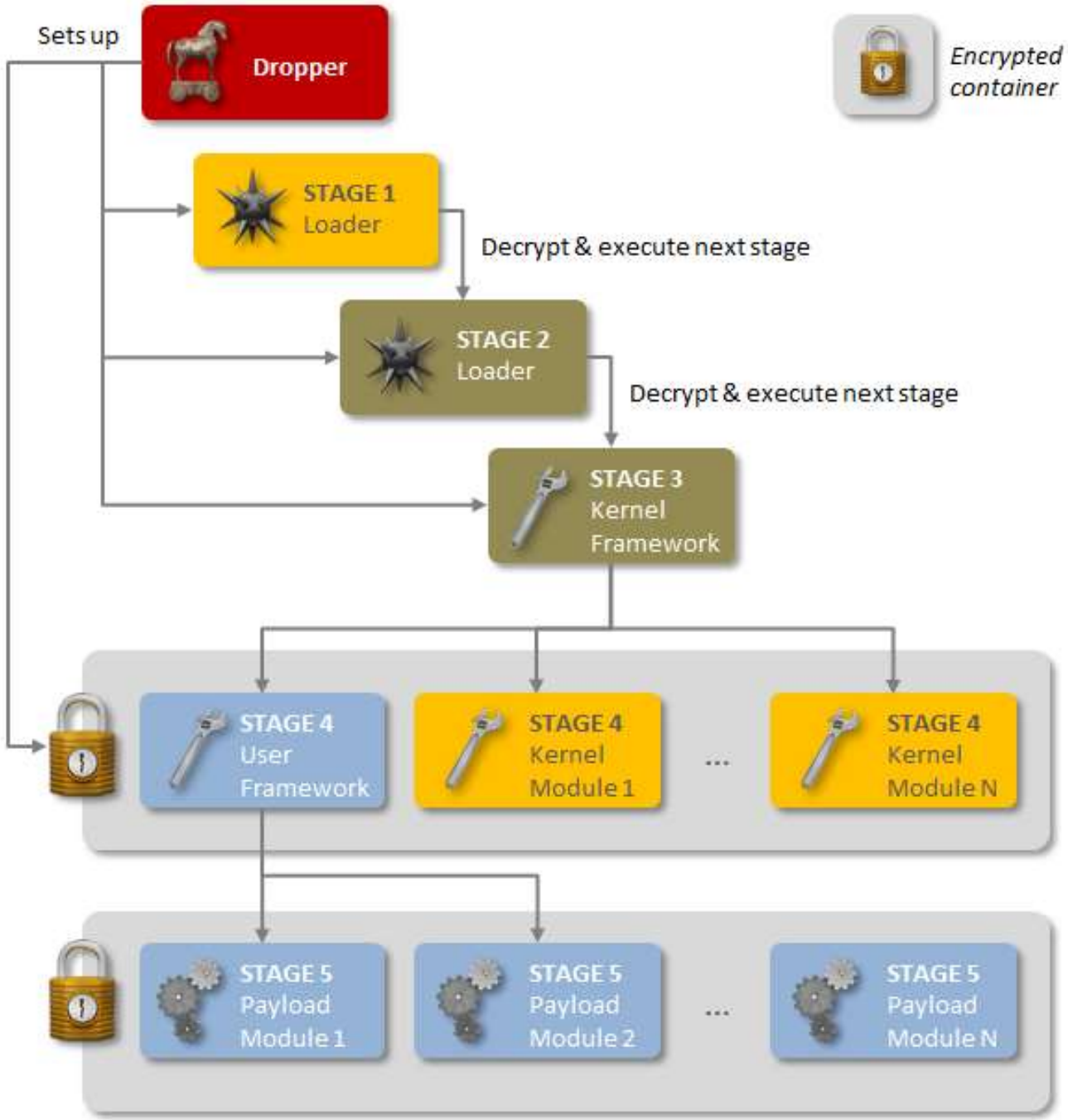
- *Countermeasures: Disable Browser Feature*

INFORMATION WARFARE

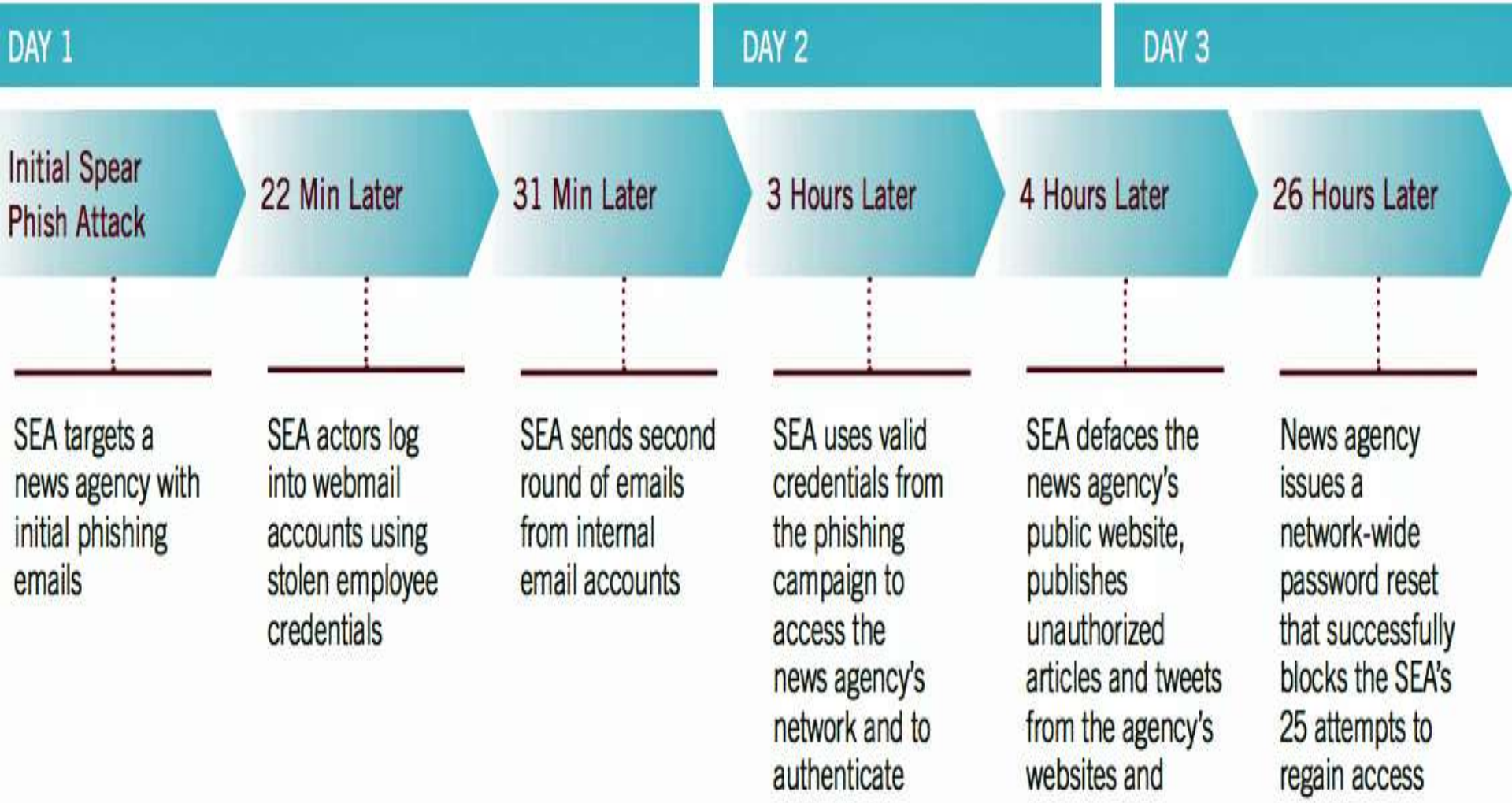

BROADCAST
INTEL
SATCOM
JSWS
AOC/FOL
THEATER INTEL
FIGHTER BASES
VOICE
LINK 16
SCDL
CGS

Major Information Warfare Programs

Year Discovered	Spy Ware
2010	Stuxnet
2010	Aurora
2012	Flame
2013	Red October
2014	DarkHotel
2014	Uroburos
2014	The Mask
2014	Regin


Sets up
Dropper
Encrypted container
STAGE 1 Loader
Decrypt & execute next stage
STAGE 2 Loader
Decrypt & execute next stage
STAGE 3 Kernel Framework
STAGE 4 User Framework
STAGE 4 Kernel Module 1
...
STAGE 4 Kernel Module N
STAGE 5 Payload Module 1
STAGE 5 Payload Module 2
...
STAGE 5 Payload Module N

Example of a Simple Attack



Commercial Attack Tools Available for $10 to $50,000

Zeus: Cybercrime Suppliers in Russia

SpyEye: From Malaysia

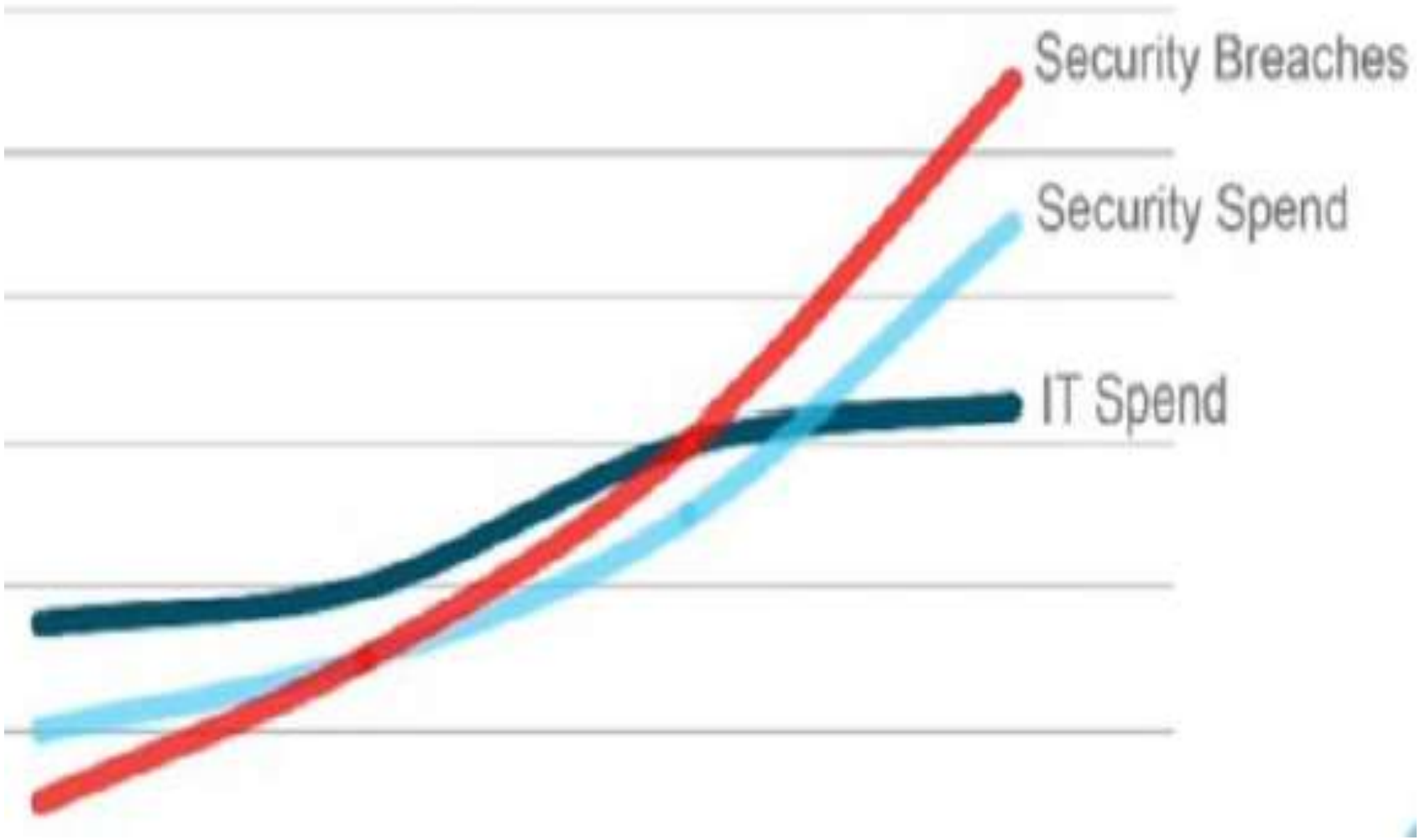
Bugat v2: Origin unknown

Gozi Prinimalka Blitzkrieg: Russian

Carberp: Priced up to $40,000 for kit

CYBER DEFENSES

Costs of Security Exceed the Costs of Risks



Distribution of Malware

Malware

- Certified Definitions* 23,847,280
- Additions During August 2013 136,051

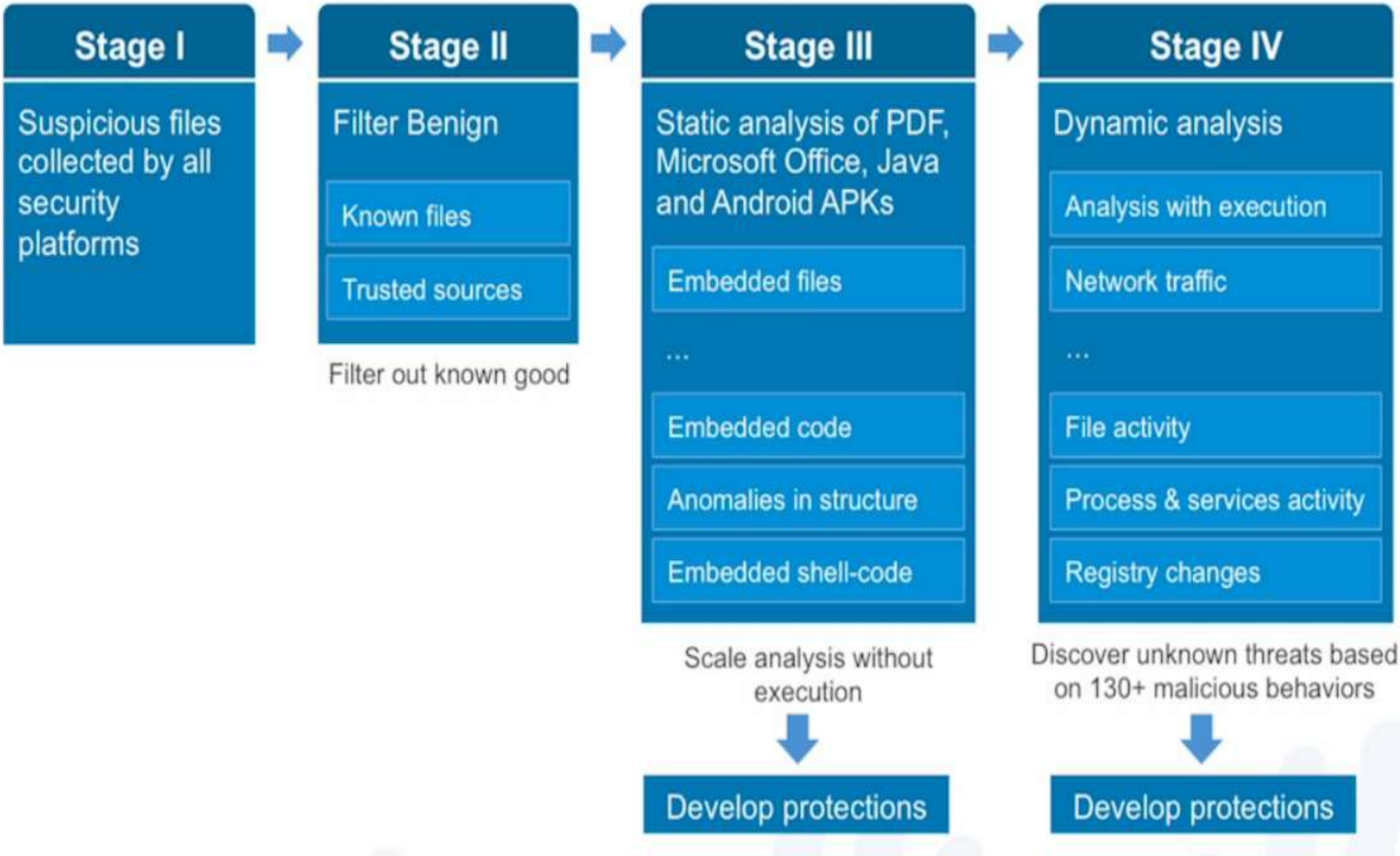
* http://www.symantec.com/security_response/definitions/certified/ - 8/17/2013
** IDC #242346

U.S. Computer Emergency Readiness Team

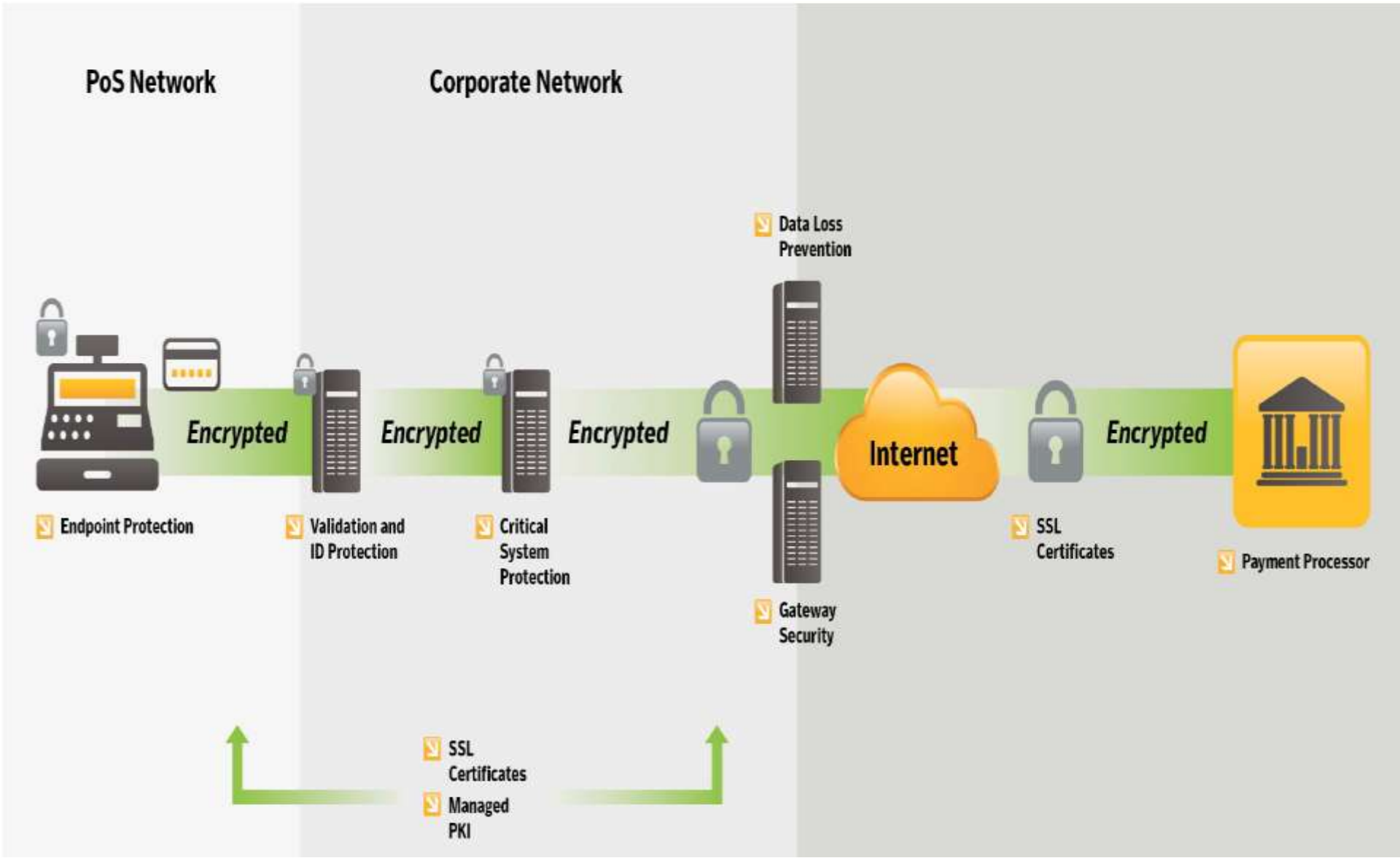
National Vulnerability Database

62,829 Vulnerabilities, June 2014

Wildfire Core Detection Techniques



How to Defend a Point-of-Sale System



PERSONAL PROTECTION

E-mail: Strassmann to Hollstein and Messert

for 11/14 introduction

Paul Strassmann <paul@strassmann.com> Nov 11

to Bchollstein, jtmessert, econgleton

Would appreciate posting the attached.

Thanks, Paul

Sent to Hollstein and Messert

```
<!DOCTYPE html><html><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>Strassmann.com Mail</title><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="google"
value="notranslate"><meta name="application-name" content="Strassmann.com Mail"><meta name="description"
content="Google&#39;s approach to email"><meta name="application-url"
content="https://mail.google.com/mail/u/0"><meta name="google" content="notranslate"><link rel="canonical"
href="https://mail.google.com/mail/" /><link rel="shortcut icon"
href="https://www.google.com/a/strassmann.com/images/favicon.ico" type="image/x-icon"><link rel="alternate"
type="application/atom+xml" title="Strassmann.com Mail Atom Feed" href="feed/atom"><script
type="text/javascript">// <![CDATA[
var GM_START_TIME=(new Date).getTime();var GM_SUPPORTED_IE_VERSION="8.0";var
GM_SUPPORTED_GECKO_VERSION="2.0.0";var GM_MOOSE_URL="?ui\x3dhtml\x26zy\x3db";var GM_NO_COOKIE_URL="?
view\x3dnocookies";var GM_NO_ACTIVEX_URL="?view\x3dnoactivex";var GM_APP_NAME="Strassmann.com Mail";var
GM_ACTION_TOKEN="AF6bupN1EEy0n9dJVLJaDSzn6aroz4sJbA";
// ]]></script><script type="text/javascript">// <![CDATA[
(function(){try{var d=this,e=function(a){var b=typeof a;if("object"==b)if(a){if(a instanceof
Array)return"array";if(a instanceof Object)return b;var c=Object.prototype.toString.call(a);if("[object
Window]"==c)return"object";if("[object Array]"==c||"number"==typeof a.length&&"undefined"!=typeof
a.splice&&"undefined"!=typeof a.propertyIsEnumerable&&!a.propertyIsEnumerable("splice"))return"array";if("
[object Function]"==c||"undefined"!=typeof a.call&&"undefined"!=typeof
a.propertyIsEnumerable&&!a.propertyIsEnumerable("call"))return"function"}else return"null";
else if("function"==b&&"undefined"==typeof a.call)return"object";return b},h=Date.now||function(){return+new
Date};var k=String.prototype.trim?function(a){return a.trim()}:function(a){return a.replace(/^[\s\xa0]+|
[\s\xa0]+$/g,"")},m=function(a,b){return a<b?-1:a>b?1:0};var p;e:{var q=d.navigator;if(q){var
r=q.userAgent;if(r){p=r;break e}}p=""}var
t=-1!=p.indexOf("Opera")||-1!=p.indexOf("OPR"),u=-1!=p.indexOf("Trident")||-1!=p.indexOf("MSIE"),v=-1!=p.inde
xOf("Gecko")&&-1==p.toLowerCase().indexOf("webkit")&&
!(-1!=p.indexOf("Trident")||-1!=p.indexOf("MSIE")),w=-1!=p.toLowerCase().indexOf("webkit"),x=function(){var
a="",b;if(t&&d.opera)return a=d.opera.version,"function"==e(a)?a():a;v?b=/rv\:([^\);]+)(\)|;)/:u?
b=/\b(?:MSIE|rv)[: ]([^\);]+)(\)|;)/:w&&(b=/WebKit\/(\S+)/);b&&(a=(a=b.exec(p))?a[1]:"");return u&&(b=
(b=d.document)?b.documentMode:void 0,b>parseFloat(a))?String(b):a}(),y={},z=function(a){var b;if(!(b=y[a]))
{b=0;for(var c=k(String(x)).split("."),n=k(String(a)).split("."),A=Math.max(c.length,n.length),
```

Walgreens

Your Order Can Ship Today

Hello Paul,

Order # 1436797168 has been placed on a brief hold until we hear from you.

Verify here and your order will be shipped

We will send you a tracking number once you confirm.

This is in regards to your Black Friday Perk Deals

Please Proceed to the Walgreens Activation Center HERE

CryptoLocker

Your Personal files are encrypted!

Private key will be destroyed on

1/6/2015 12:53:45 PM

Time left

71:53:30

Checking wallet.

Received: 0.00 BTC

Your personal files **encryption** produced on this computer: photos, videos, documents, etc. Encryption was produced using a **unique** public key RSA-2048 generated for this computer.

To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **1.00 bitcoin** (~299 USD).

You can easily delete this software, but know that without it, you will never be able to get your original files back.

Disable your antivirus to prevent the removal of this software.

For more information on how to buy and send bitcoins, click "Pay with Bitcoin"
To open a list of encoded files, click "Show files"

Do not delete this list, it will be used for decryption. And do not move your files.

Show files

Pay with Bitcoin

What to Do for Partial Protection

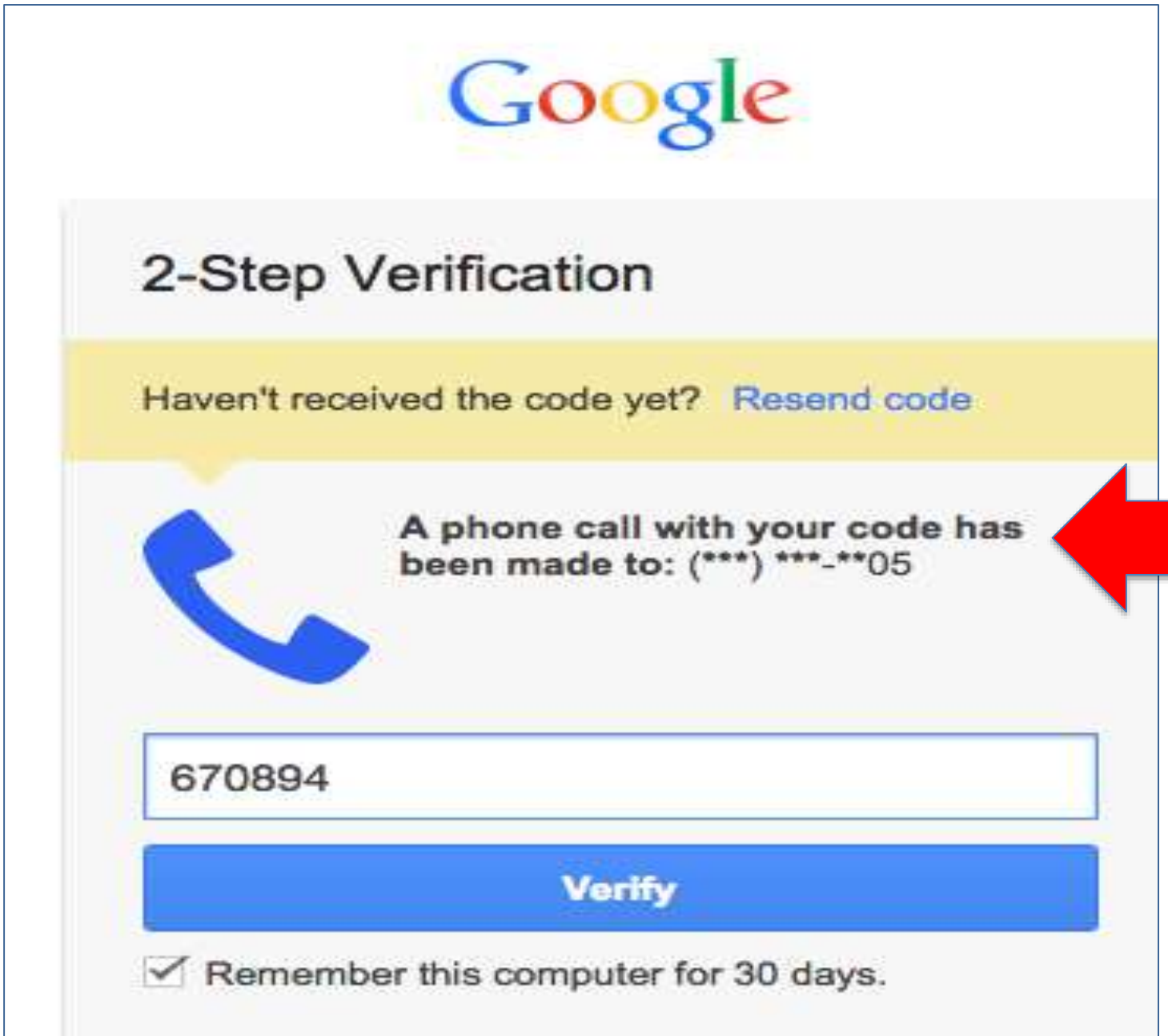
What to Do

- Never click on unknown e-mail attachment
- Never download application from uncertified source
- Never accept offers from unverified senders
- Always back up your systems

Optional:

- *Switch to G-mail for two factor authentication*
- *Switch to Apple*

Gmail Two Factor Authentication



Advice

- INTERNET is vulnerable
- You may be “hacked”
- Self-protection: set up backup computer
- Security services available