Security: You Ain’t Seen Nothing Yet: New Attacks and How to Prepare for Them

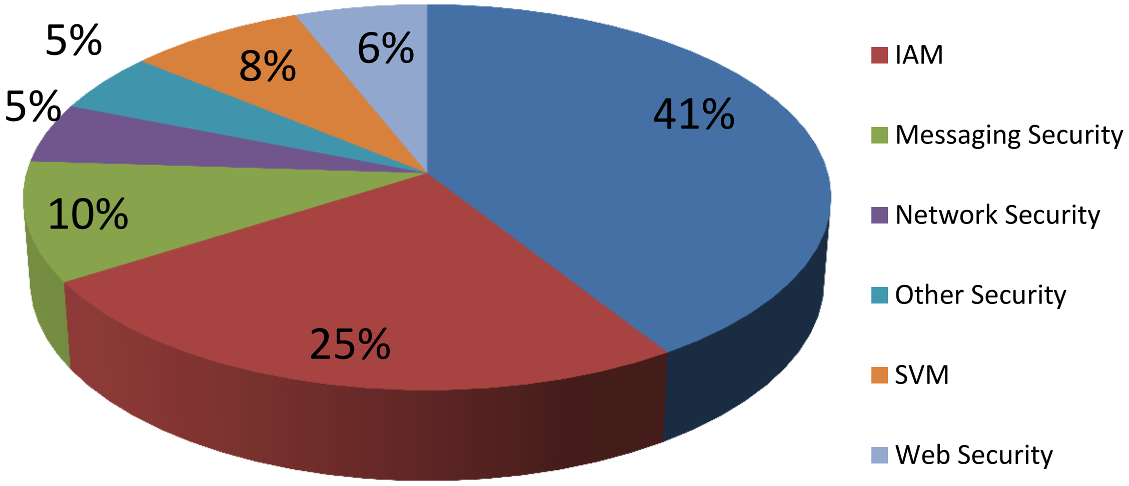
Dustin Kehoe

Associate Research Director

IDC ANZ

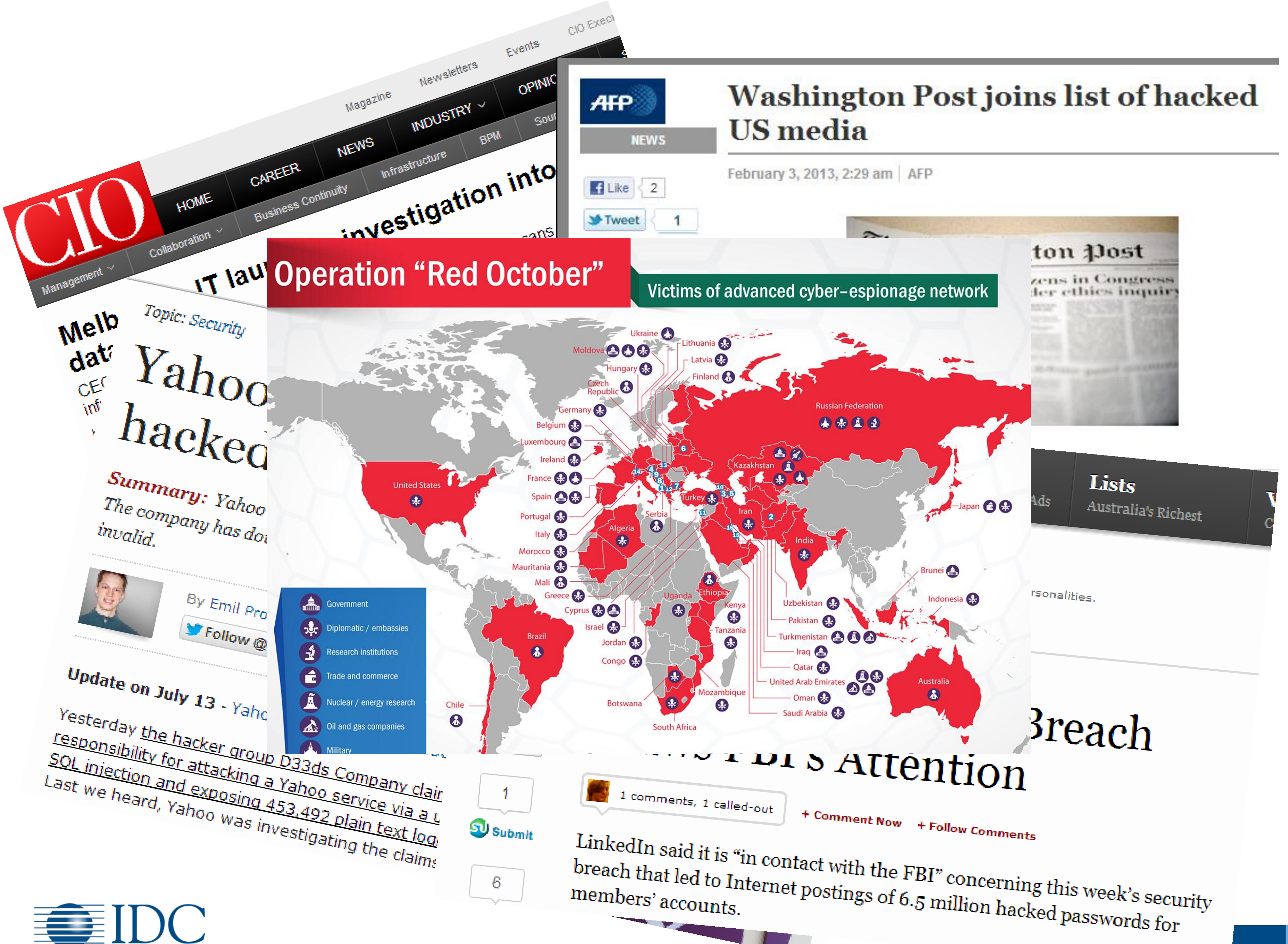
APeJ – Fastest Growth Region World Wide 13% Y-on-Y Growth from 2011

1H 2012



$870 million

Region	5 Years CAGR through 2016
Asia Pacific	12.0%
CEMA	11.7%
Latin America	8.2%
USA	7.1%
Canada	5.4%
W. Europe	5.4%
Japan	3.9%
World Wide	7.0%



IT lau... investigation into

Melb... dat...

CE... inf...

Topic: Security

Yahoo hacked

Summary: Yahoo... The company has do... invalid.

By Emil Pro...

Update on July 13 - Yaho...

Yesterday the hacker group D33ds Company clai... responsibility for attacking a Yahoo service via a ... SQL injection and exposing 453,492 plain text log... Last we heard, Yahoo was investigating the claims

Washington Post joins list of hacked US media

February 3, 2013, 2:29 am | AFP

Operation "Red October"

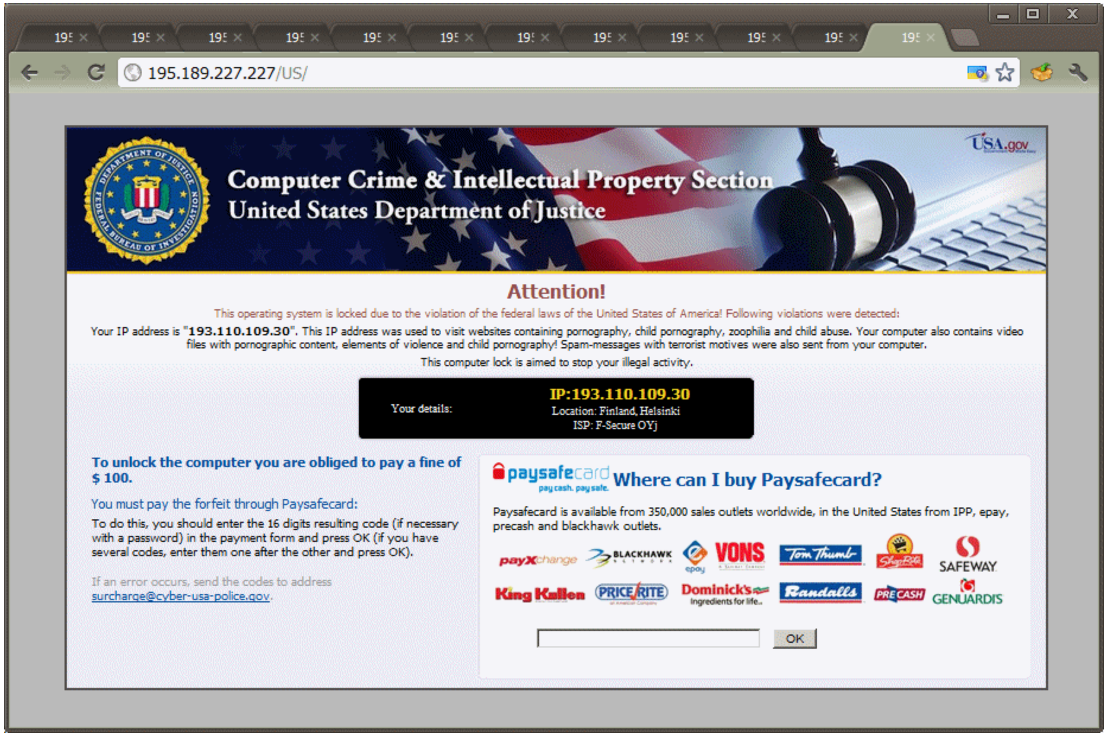
Victims of advanced cyber-espionage network

...Breach ... FBI's Attention

LinkedIn said it is "in contact with the FBI" concerning this week's security breach that led to Internet postings of 6.5 million hacked passwords for members' accounts.

IDC
Analyze the Future

Anatomy of a Ransomware



Computer Crime & Intellectual Property Section
United States Department of Justice

Attention!

This operating system is locked due to the violation of the federal laws of the United States of America! Following violations were detected:

Your IP address is "**193.110.109.30**". This IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

Your details: IP:193.110.109.30
Location: Finland, Helsinki
ISP: F-Secure OYj

To unlock the computer you are obliged to pay a fine of $ 100.

You must pay the forfeit through Paysafecard:

To do this, you should enter the 16 digits resulting code (if necessary with a password) in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address surcharge@cyber-usa-police.gov.

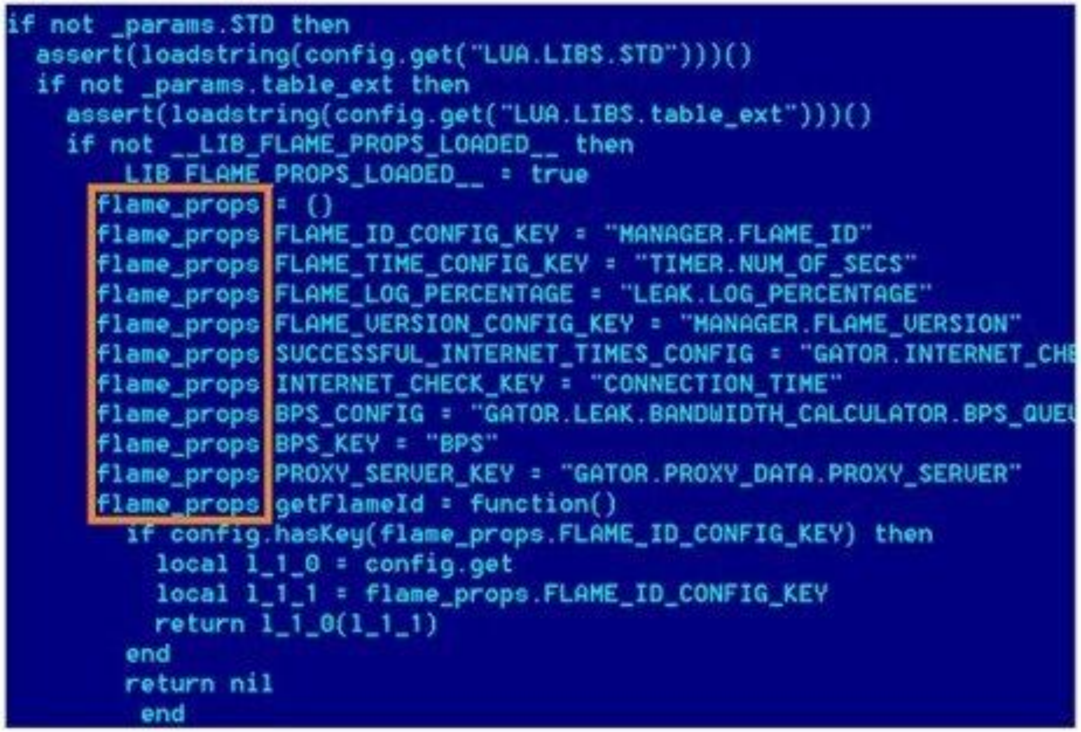
Where can I buy Paysafecard?

Paysafecard is available from 350,000 sales outlets worldwide, in the United States from IPP, epay, precash and blackhawk outlets.

- Freezes computer
- Virus not deleted even after ransom paid
- Keystroke loggers and other viruses inserted

- Masquerades as a law enforcement or software vendors
- Scammers then demand for ransom be paid in order to unfreeze screen
- Drive-by virus, infected by merely surfing sites – most commonly porn sites.
- Highly adaptive – location aware. Morphs information to suit locality of attack

Anatomy of an Advance Persistent Threat



```
if not _params.STD then
  assert(loadstring(config.get("LUA.LIBS.STD")))()
  if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS.table_ext")))()
    if not __LIB_FLAME_PROPS_LOADED__ then
        LIB_FLAME_PROPS_LOADED__ = true
      flame_props = ()
      flame_props FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
      flame_props FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
      flame_props FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
      flame_props FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
      flame_props SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CHE
      flame_props INTERNET_CHECK_KEY = "CONNECTION_TIME"
      flame_props BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUEU
      flame_props BPS_KEY = "BPS"
      flame_props PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
      flame_props getFlameId = function()
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
          local l_1_0 = config.get
          local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
          return l_1_0(l_1_1)
        end
        return nil
         end
```

- Siphons information over protracted periods
- Advanced versions focuses on gaining control of critical infrastructure
- Run by nation states and cyber cartels

- Military and intelligence origins
- Persistent in nature. Highly targeted. Utilises combination of attacks – malware, social engineering
- Can be “primitive” by using known vulnerabilities. Can also be stealthy
- Highly elusive. Codes can be polymorphous to avoid detection

Panel Discussion !!

Dustin Kehoe

Associate Research Director,
Telecommunications
IDC ANZ

Email:	dkehoe@idc.com