



# I AM NOT A NUMERO!

## Assessing Global Security Threat Levels

Bryan Lu, Project Manager / Researcher

Virus Bulletin Conference 2009  
21-23 September 2009  
Geneva, Switzerland

**FORTINET**®

## “Numero”

- English: “numero” or “number” or “No.” or “#”
- Spanish: “número” or “n<sup>o</sup>” or “N<sup>o</sup>”
- Portuguese: “número” or “N.<sup>o</sup>”
- French: “*numéro*”

# Agenda

- Assess The Current Threat Levels
- Varieties of Security Threat Levels
  - Virus
  - Spam
  - Vulnerability

**Assess The Current Threat Levels**

**Varieties of Security Threat Levels**

**Virus**

**Spam**

**Vulnerability**

## No Standard?

- Defined and set independently by security vendors.
- As a result, different scales and current threat condition appears.

## By The Dollar

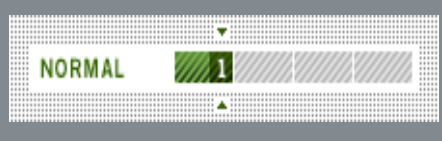


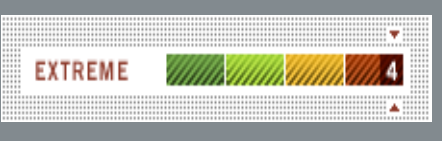
- The higher the financial impact, the higher the threat level.
- From the e-users' point of view, this makes sense.
- Remains a challenge. Regional factors, currency, etc.

## Partially Reactive

- Escalated when there is an active high-profile threat.
- Definition updates are released as soon as discovered.
- Propagation is relative to time of the day.
- Proactive threat level is worthless.

# Arbor Networks: Threat Index



 <p>NORMAL</p>	 <p>ELEVATED</p>	 <p>HIGH</p>	 <p>EXTREME</p>
<p>... no significant threats to normal Internet operations and no significant new attack or malware activity.</p>	<p>... discovered significant new threats ... not causing widespread outages.</p>	<p>... tracking major, Internet-scale issues. Major, widespread attacks ...</p>	<p>... seeing major, wide-scale disruptions in service and Internet availability and rapidly expanding attacks.</p>

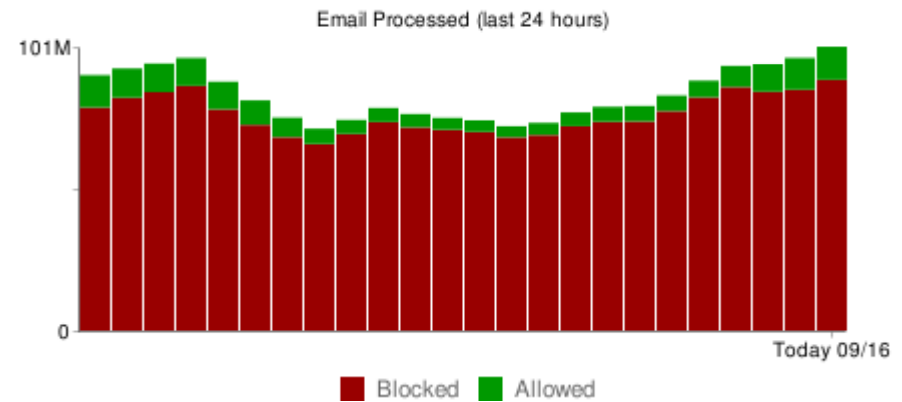
Source: <http://atlas.arbor.net/faq/threatindex>



# Barracuda Networks: Spam Data



Blocked: Spam	912,046,671
Allowed	75,243,282
Total Received	998,670,472



Source: <http://www.barracudacentral.org/data/spam>

# Cisco: Virus Threat Level



IronPort Email and Web Security

**Virus Threat Level**

Virus Outbreaks in progress

Virus Outbreaks previous 24 hours

No Outbreaks previous 24 hours

Real-Time Updates    Details

Green	Orange	Red
No Virus Outbreak In Last 24 Hours	Virus Outbreak In Last 24 Hours	Virus Outbreak In Progress

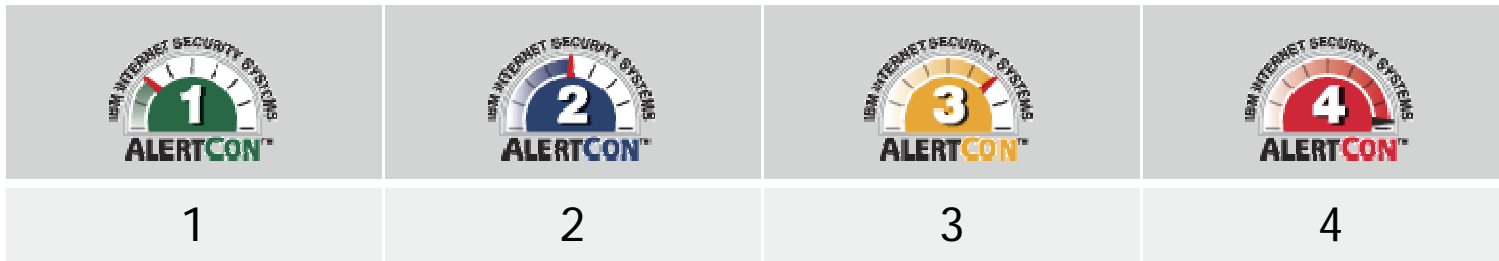
Source: <http://www.ironport.com/toc/>

# IBM ISS: Internet Threat Level

**IBM Internet Security Systems**  
**Ahead of the threat.™**

Current Internet Threat Level

The Threat Level is returning to AlertCon 1 after being raised to AlertCon 2 on Thursday, July 23.



Source: <https://webapp.iss.net/gtoc/index.html>

# McAfee: Global Threat Condition



Low	Elevated	Severe	Critical
<p>There is no direct threat to systems that have been patched.</p> <p>No new significant malware activity</p>	<p>An unpatched or recently patched vulnerability ... requires user interaction ....</p> <p>new malware activity ... not widespread.</p>	<p>An unpatched or recently patched vulnerability can be exploited by a worm, .... No worm activity</p> <p>A high incidence of new malware...</p>	<p>Systems worldwide are targeted by a worm.</p> <p>New malware ...spread globally.</p>

Source: [http://www.mcafee.com/us/threat\\_center/default.asp](http://www.mcafee.com/us/threat_center/default.asp)

# Norman: Threat Level

**NORMAN**

“You will see the current threat level as assessed by Norman at the right hand side. The date shows when the threat level was last changed.”

THREAT LEVEL (SINCE 2009-04-22)



## Low threat level

... none of these are viewed as particularly dangerous for the vast majority of the Internet community.

## Medium threat level

... a particular danger for a significant number of people ... can be malicious programs and/or vulnerabilities in widespread software.

## High threat level

... a pandemic outbreak of malicious software; published, unpatched vulnerabilities ...

Source: [http://www.norman.com/security\\_center/current\\_threat\\_level/en](http://www.norman.com/security_center/current_threat_level/en)

# Panda Security: Threat Level

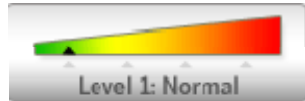


Green (Normal)	Orange (Pre-alert)	Red (Alert)
... no specific threat being massively distributed	... one or more specific threats that start to spread aggressively, or the sum of all malware in circulation constitutes an important danger.	one or more specific threats massively spread, or the combined action of all malware in circulation is extremely dangerous. Great amount of incidences worldwide.

Source: <http://www.pandasecurity.com/homeusers/security-info/gtw/#e3>

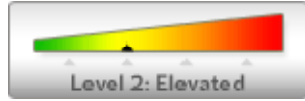
# Symantec: ThreatCon

Symantec ThreatCon



Level 1: Normal

Symantec ThreatCon



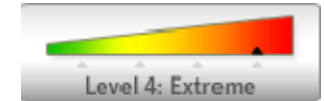
Level 2: Elevated

Symantec ThreatCon



Level 3: High

Symantec ThreatCon



Level 4: Extreme

Low : Basic network posture	Medium : Increased alertness	High : Known threat	Extreme : Full alert
...no discernible network incident activity and no malicious code activity with a moderate or severe risk rating	... when knowledge or the expectation of attack activity is present, without specific events occurring or when malicious code reaches a moderate risk rating.	... when an isolated threat to the computing infrastructure is currently underway or when malicious code reaches a severe risk rating.	... when extreme global network incident activity is in progress.

Source: <http://www.symantec.com/connect/blogs/meaning-threatcon-levels>

# Trend Micro: Threat Meter



How We Calculate Threat Levels? For each indicator – web, spam, malware – current percentages and trends are compared to levels during the previous year.

GUARDED	ELEVATED	HIGH	SEVERE
No new threat activity ... little risk to recently patched and updated systems.	New threat activity puts systems with existing or new vulnerabilities at risk.	New threats and exploits are actively circulating via web and email.	Several threats and exploits are circulating rapidly via web and email.

Source: <http://us.trendmicro.com/us/about/threat-level/index.html>



## And so?

- Virus threat level be based on its spread?
- Spam threat level be replaced by its volume?
- Vulnerability threat level be based on its patch?
- Greg Young, a Gartner analyst, posted the following on his blog:
  - “The results seem so varied it really gives me low confidence in the value of these gauges.”
- For security awareness or marketing gimmicks?

# Twitter Threat Level



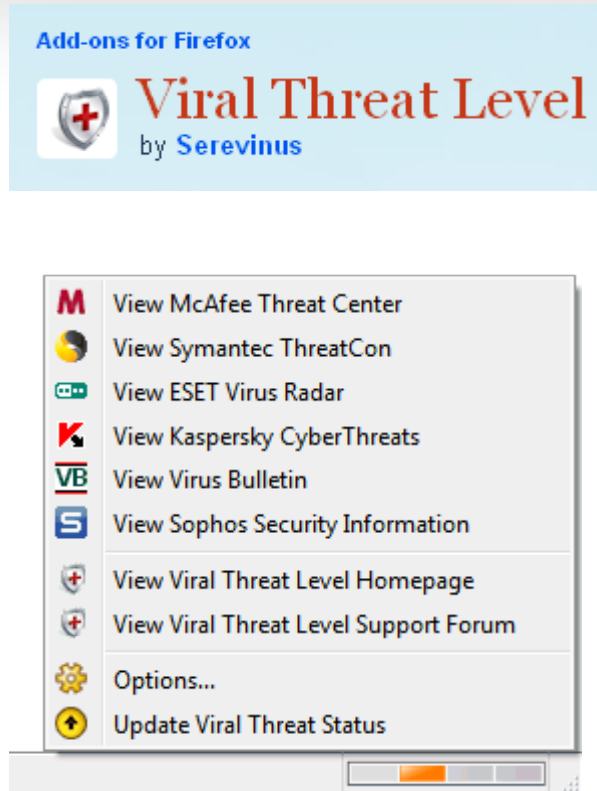
ThreatLevel

Symantec	1 (LOW)	25-Aug
Symantec	2 (MEDIUM)	22-Jul
Symantec	1 (LOW)	20-Jul
SANS ISC	Green (LOW)	14-Jul
SANS ISC	Yellow	13-Jul
Symantec	2 (MEDIUM)	5-Jul
Symantec	1 (LOW)	16-Jun
Arbor	Normal (LOW)	10-Jun
Symantec	2 (MEDIUM)	9-Jun
Symantec	1 (LOW)	4-Jun

McAfee	Elevated	1-Jun
Symantec	2 (MEDIUM)	12-May
Symantec	1 (LOW)	17-Apr
McAfee	Severe (HIGH)	10-Apr
Symantec	2 (MEDIUM)	2-Apr
Symantec	1 (LOW)	2-Apr
Symantec	2 (MEDIUM)	2-Apr
Trend Micro	Elevated	24-Mar
Trend Micro	Normal	24-Mar
McAfee	Elevated	24-Mar

Source: <http://twitter.com/threatlevel>

# Viral Threat Level extension for Mozilla Firefox



“VTL adds an image to the status bar indicating the current threat level of the internet, for example the prevalence of malware, viruses etc.

Threats could be anything from email viruses to vulnerabilities in your operating system, ...”

Source: <http://www.serevinus.com/vtl/>

**Assess The Current Threat Levels**

**Varieties of Security Threat Levels**

**Virus**

**Spam**

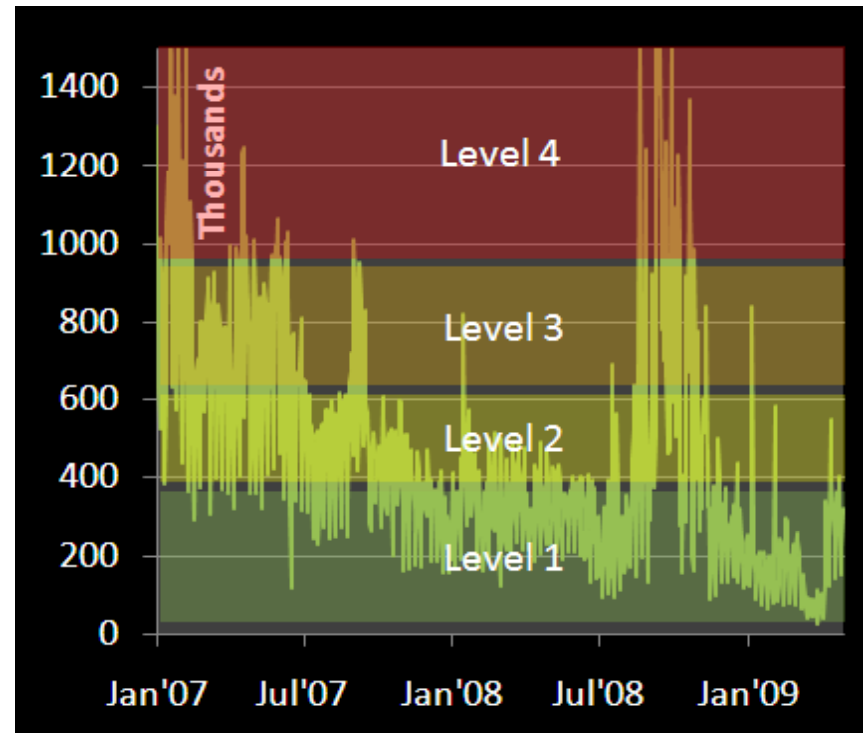
**Vulnerability**

## A Bit of History

- Began about 10 years ago as an internal process in responding to virus outbreak.
- Adapted later as a public information to inform of the present situation.
- Threat level based on the level of affected customers.

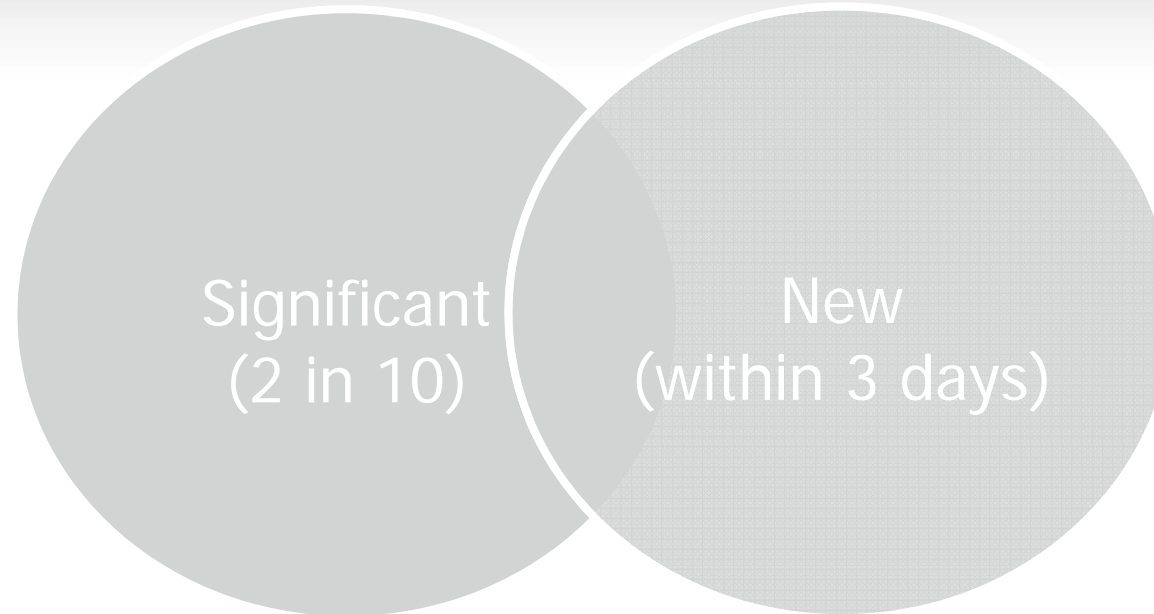
# Dependency on the Volume

- Approach #1: Set the threat level if the volume surpass a limit.
- #2: Base the threat level on the virus with the highest detection.
- #3: Apply the relative exposure of the virus to the end-users as against to the baseline.



Volume of virus infections per day

## Suggested Approach



Then, match the highest significant and new percentage with a given threshold set for the different levels. (e.g. Escalated starts at 20%; High at 50%; Severe at 90%).

**Assess The Current Threat Levels**

**Varieties of Security Threat Levels**

**Virus**

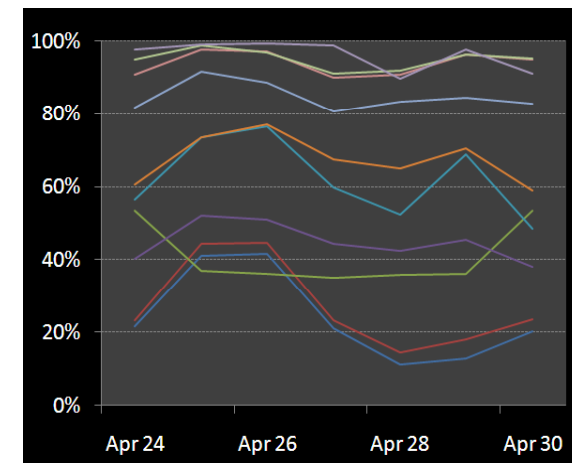
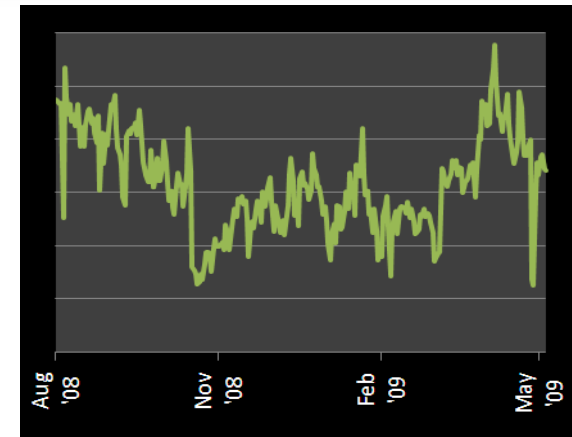
**Spam**

**Vulnerability**



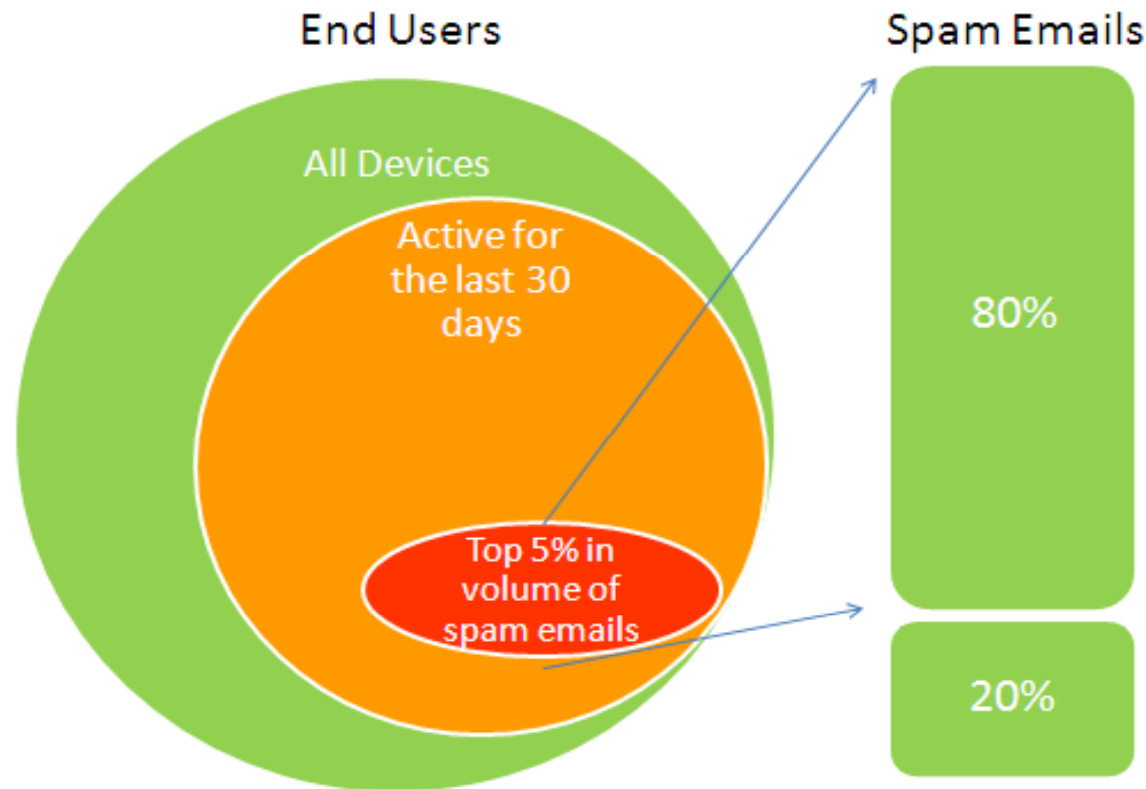
# Challenge

- How to convert the billions of spam per day to a threat level.
  - A million more spam is barely noticeable
  - Internet users are ever increasing.
  - Favorable effect of large-scale mitigation on the source of spam.
  - Source of stats.
  - Do not even use the clean emails (i.e. spam rate).



# Suggested Approach

1. Pick a sampling group; compile a list of end-users that have been active and in top tier in volume.



## Suggested Approach

2. For each end-users, compare the current last 24-hour volume with the previous 10 weeks of the same day and hour.
3. Get the percentage of end-users that have surpassed the previous maximum volume.
4. Match the percentage with a given threshold set for the different levels. (e.g. Escalated starts at 20%; High at 50%; Severe at 90%).

**Assess The Current Threat Levels**

**Varieties of Security Threat Levels**

**Virus**

**Spam**

**Vulnerability**

# Challenges

- The lifespan can be several years.
- May have (or w/out) any protection in place yet.
- Vulnerabilities have severity ratings.
- A million attempts on DoS vs a single attempt on a PDF exploit.
- Effect of false negative detection.

## Suggested Approach

1. Extract the active vulnerabilities.
2. Only include those vulnerabilities that have reached the e-users threshold (e.g. 1% of the active e-users).
3. Use the window of activity (e.g. 7-day). Any prior escalation should be removed.

## Suggested Approach

4. Manually confirm that the vulnerability is not a false positive.
5. Cross-check the vulnerabilities with their severity weighed value to get the total value of the vulnerabilities. (e.g. Critical is 40, High is 8, Medium is 2, Low is 1).
6. Compare the total value with the threat level threshold. (e.g. Severe is “ $\geq 160$ ”; High is “ $\geq 80$ ”; Escalated is “ $\geq 40$ ”; Normal).

## Summary

- Distinct threats. Distinct levels.
- Sophisticated approach yet simple to understand.



# Fortinet Threat Level

## VIRUS, SPYWARE, AND OTHER MALWARE THREATS

The antivirus threat indicator measures the outbreak of new threats (virus, spyware, and other malware) with an average that includes a 14-day, 5-day, and 3-day trend. Previously identified threats protected against by new updates are excluded from the measurement. Threats are verified by the FortiGuard Global Threat Research

Normal

event. E  
antivirus.

Elevate

High ind  
Network  
affected

Severe

event. In  
end-use  
encoura

## VULNERABILITIES

The vulnerabilities threat indicator measures the outbreak of new intrusion-type threats over a 14-day period. The indicator levels are weighted based on severity. For new intrusions and vulnerabilities, the FortiGuard Global Threat Research assigns a severity level of 1 (low), 2 (medium), 8 (high), and 40 (critical). Threats are confirmed by the Vulnerability Watch organization to identify and eliminate false positives.

Normal

Intrusion

Elevate

High ind

Severe

## SPAM

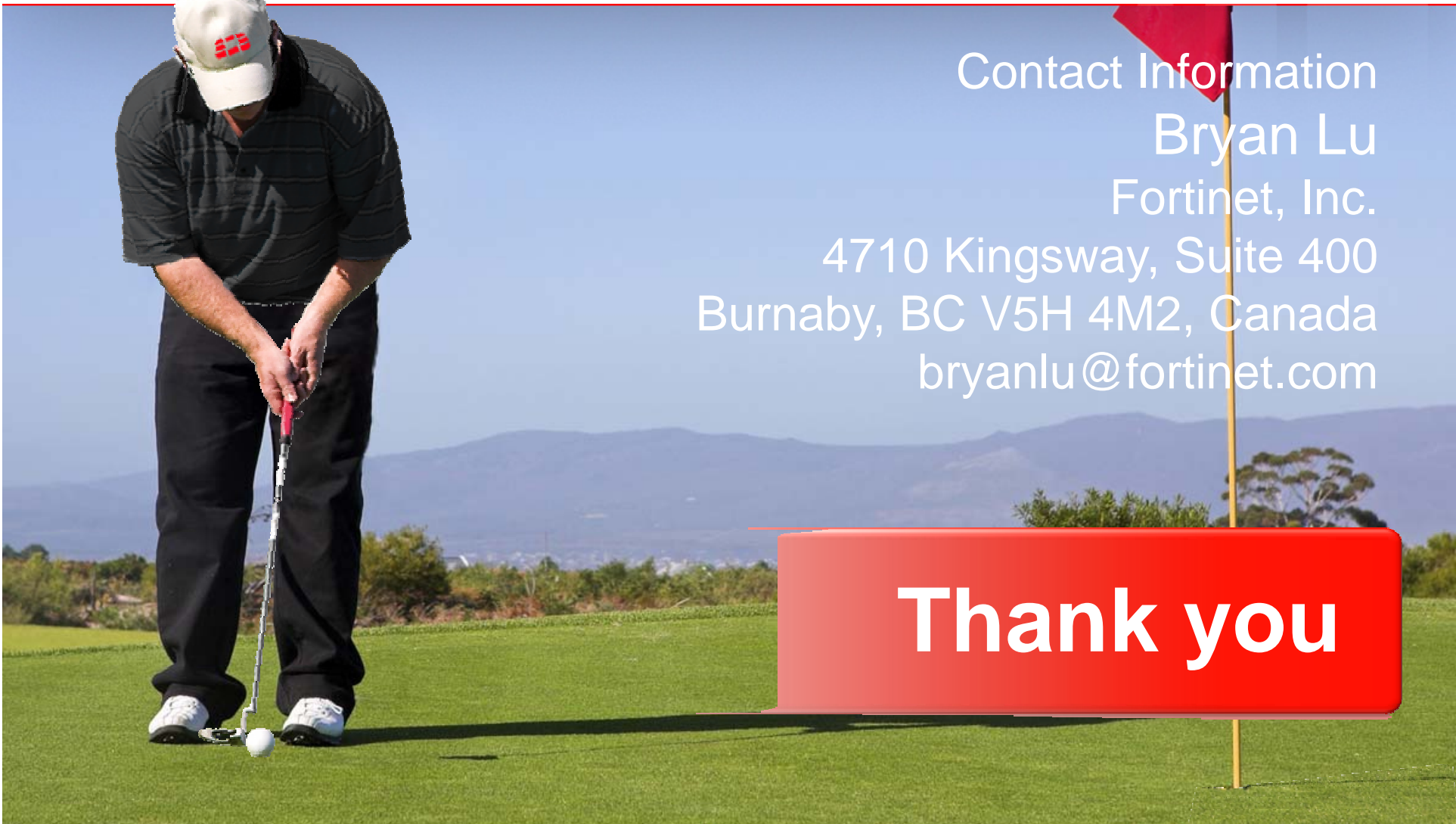
The Spam threat level indicator measures both the rising/falling trend and the impact of spam on a running average (median) for the prior 10 weeks. This indicator reports on amount of spam across sampled Fortinet systems. Network security managers can use the threat indicator to determine when antispam controls should be deployed. The threat levels are:

Normal indicates that spam levels are remaining constant and antispam controls are necessary.

Source: <http://www.fortiguard.com/resources/glossary.html>



Questions ?



Contact Information  
Bryan Lu  
Fortinet, Inc.  
4710 Kingsway, Suite 400  
Burnaby, BC V5H 4M2, Canada  
[bryanlu@fortinet.com](mailto:bryanlu@fortinet.com)

**Thank you**