Beginning to Remediate Botted Hosts Abroad: India

Joe St Sauver, Ph.D.
MAAWG Senior Technical Advisor
joe@oregon.uoregon.edu

Messaging Anti-Abuse Working Group 21st General Meeting
3:30 PM, Tuesday Feb 22nd, 2011, Orlando, Florida

http://pages.uoregon.edu/joe/maawg-orlando-talk/

Disclaimer: all opinions expressed are my own, and do not necessarily represent the opinion of MAAWG or any other entity

I. The Problem

Bots Have Been (And Continue to Be) At The Root of the Spam Problem

- The fact that bots are at the root of the spam problem is not news – we've been talking about bots at MAAWG for a long time.
- For example, in March 2005, I delivered "Spam Zombies and Inbound Flows to Compromised Customer Systems" at the San Diego MAAWG. (see pages.uoregon.edu/joe/zombies.pdf)
- This is a good news/bad news sort of thing.
- The good news? The community **has** been making progress on the bot issue: many MAAWG members have successfully deployed strategies that allow customers avoid getting botted in the first place, or, if their customers do get botted, to at least limit the damage those botted customers can cause.
- The bad news? Just like the old days, bots are still responsible for delivering most of the spam that MAAWG participants see.

“Isn’t That Contradictory?”

- No. We **have** made progress against bots, just not **everywhere**.
- At one point, many of the bots delivering email spam were exploiting US, Canadian or Western European ISP customers. That made it easy to work on getting those hosts cleaned up: they were our problem, or the problem of people we knew.
- Now, however, the picture has changed:
  -- Most US, Canadian and Western European customers have improved their cyber security, and are less likely to become compromised by malware
  -- If a US, Canadian or Western European customer does become compromised, many ISPs are able to efficiently quarantine that host, thereby limiting their impact on the Internet as a whole.
- But the bad guys do still need compromised systems, so they’ve turned their sights elsewhere now. Now they’re compromising systems in rapidly developing economic regions of the world.

Hear “Rapidly Economically Developing,” Think “BRIC”

- We’re used to thinking about the G8 (CA, DE, FR, IT, JP, RU, UK, and US) leading the world’s economy, but there are indications that the BRIC countries (Brazil, Russia, India and China) may eventually eclipse the G8 when it comes to economic influence.
- BRIC countries collectively represent more than 25% of the world’s land area and more than 40% of the world’s population, and increasingly supply the world with both raw materials and manufactured goods. (See: http://en.wikipedia.org/wiki/BRIC)
- The BRIC countries are also increasingly well connected to the rest of the world via new high capacity undersea cables, and have an increasingly affluent population that’s been heavily investing in personal computers and other networked devices.
- Unfortunately, many of those new workstations have been infected by malware, and thus systems in the BRIC countries are now some of the world’s top apparent sources of spam.

Why Else Are Rapidly Developing Regions Targeted?

- Consumer systems in rapidly developing regions of the world are also prime targets for cyber exploitation because:
  -- While network connectivity typically has improved dramatically, it may still be expensive (relative to the US or EU), and thus is often thinly provisioned, with congested transit connections. Slow downloads mean **that large patches may seem to take "forever" to download**, thereby making it difficult (if not impossible) for users to actually download and apply patches.
  -- **Intellectual property controls may be weak** in some regions. In those areas there may be widespread trafficking in pirated software -- software that often comes larded with malware.
  -- **Regulatory regimes may be weak**: ISPs in rapidly developing economies often do not experience governmental pressure to take action to deal with compromised customer hosts.
- The end result? There are many botted systems in rapidly developing economic regions.

Getting Hard Statistics on Botted Hosts: The CBL

- Hard statistics on bot infestations are comparatively rare. The community is fortunate to have access to some publicly available hard statistics on botted hosts from the Composite Block List (or "CBL"). THANK YOU, CBL folks! The CBL lists IP addresses…

  […] exhibiting characteristics which are specific to open proxies of various sorts (HTTP, socks, AnalogX, wingate etc) and dedicated Spam BOTs which have been abused to send spam, worms/viruses that do their own direct mail transmission, or some types of trojan-horse or "stealth" spamware, dictionary mail harvesters etc. […]
  The CBL also lists certain portions of SpamBot infrastructure, such as Spam BOT/virus infector download web sites, and other web sites or name servers exclusively dedicated to the use of Spam BOTs. Considerable care is taken to avoid listing IP addresses that have are or are likely to be shared with legitimate use, except in the case of infector download websites. In other words, the CBL only lists IPs that have attempted email connections to one of our servers in such a way as to indicate that the sending IP is infected, OR, IPs specifically dedicated to the propagation/use of Spam BOTs.

  See: http://cbl.abuseat.org/

CBL Listed IP Addresses By Country

- As of Sat Feb 19th, 2011, out of 7,420,939 total IPs on the CBL:

Rank	Country	Count	%	Cumulative %
1	**India**	1,219,562	16.43%	16.43%
2	**Brazil**	732,441	9.87%	26.30%
3	**Russia**	577,307	7.78%	34.08%
4	Vietnam	443,468	5.98%	40.06%
5	Ukraine	321,380	4.33%	44.39%
6	Indonesia	249,189	3.36%	47.75%
7	Thailand	191,130	2.58%	50.32%
8	Italy	179,645	2.42%	52.74%
9	Pakistan	177,345	2.39%	55.13%
10	**China**	173,191	2.33%	57.47%

Note: just **ten** countries = nearly 60% of all known botted IPs, and **one** country, India, accounts for nearly 16.5% of all of them!

Some Other Countries For Comparison…

- Again, the number of CBL-listed IPs as of Sat Feb 19th, 2011…

Rank	Country	Count	%
13	Germany	146,076	1.97%
20	USA	91,832	1.24%
30	UK	61,409	0.83%
35	Mexico	43,012	0.58%
41	France	31,059	0.42%
51	Australia	18,496	0.25%
70	New Zealand	8,602	0.12%
71	Canada	8,318	0.11%
77	Switzerland	7,014	0.09%
83	Japan	5,473	0.07%
88	Netherlands	4,749	0.06%
149	Finland	242	<0.01%

In Fairness..

- Some countries are a lot larger than others, both in terms of their populations and the number of IP addresses they use…

- In the case of extremely large countries, infection of even a tiny percentage of all IPs can still translate to substantial address counts.

- So what do we know about the percentage of each country's IP addresses that are listed on the CBL?

  Looked at on a percentage basis, the rankings do change…

% of All IPs on the CBL, For Selected Countries

- Byelorussia 14.822% (170,869 listed IP addresses)
  Dominican Republic 10.456% (56,506 listed IP addresses)
  Ghana 9.810% (14,716 listed IP addresses)
  Cote D'Ivoire 6.443% (7,785 listed IP addresses)
  India **5.120% (1,219,562 listed IP addresses)**
  Morocco 5.012% (76,400 listed IP addresses)
  Pakistan **4.723% (177,345 listed IP addresses)**
  Vietnam **3.887% (443,468 listed IP addresses)**
  Russia **1.597% (577,307 listed IP addresses)**
  Brazil **1.389% (732,441 listed IP addresses)**
  China **0.061% (173,191 listed IP addresses)**
  Canada 0.016% (8,318 listed IP addresses)
  USA 0.007% (91,832 listed IP addresses)
  Finland 0.002% (242 listed IP addresses)

A Point For Consideration and Discussion

- Assume we want to pick **one** country where we'd work to reduce the number of botted hosts. Should we work on:

  a) Byelorussia, where roughly 15% of all their IP addresses are now listed on the CBL, or

  b) India, where "only" a little over 5% of all their IP addresses are now listed?

  From an external point of view, the 1,219,562 botted Indian IPs sure seem to "hurt" a lot more than the 170,869 botted Byelorussian hosts.

- Of the two I believe we should concentrate on India, first, even if Byelorussia is far more victimized on a percentage basis.

Digging In A Little Further

- In addition to giving us country data, the CBL also gives us data by domain. What are the top 10 Indian domains listed on the CBL?

#	Domain	Count	% of CBL	% of domain listed
1	sancharnet.in	455,829	6.15%	14.264%
3	airtel.in	277,569	3.75%	9.821%
13	vsnl.in	103,431	1.40%	2.176%
16	powersurfer.in	99,661	1.35%	13.033%
18	ddsl.in	78,071	1.05%	5.481%
28	tatatel.co.in	51,639	0.70%	7.904%
48	adityabirla.com	24,205	0.33%	11.848%
72	mtsindia.in	17,712	0.24%	24.997%
87	tpc.co.in	15,079	0.20%	1.223%
104	hutch.in	12,256	0.17%	2.886%
	Total	**1,135,452**	**15.34%**	

Looking at That Variation In Infection Rate…

- Looking at that inter-ISP variation in infection rate, clearly sancharnet.in has a far more serious problem (with 14.264% of the IPs belonging to them being CBL listed), than does tpc.co.in (with only 1.223% listed)

- Thus, even more than concentrating on one country vs. another, in this case, we may want to think about concentrating on one *ISP* first…

- But what do we want that ISP to do?

- We want them to deal with their bots, but how?

II. Beginning To Fix The Problem

We *Could* Urge Them To Just "Treat The Symptom"

- If we could convince just those ten Indian ISPs to follow MAAWG's published recommendation for **"Managing Port 25 for Residential or Dynamic IP Space"** (see http://www.maawg.org/sites/maawg/files/news/MAAWG_Port25rec0511.pdf), we could immediately knock down ~15% of the IPs on the CBL.

- I think that would be an excellent accomplishment, IF we could pull it off.

- Does the MAAWG community know anyone at those ten Indian ISPs? Is anyone willing to reach out to them? Can we invite them to a future MAAWG meeting, perhaps, such as our upcoming meeting in Paris this fall?

Or Can We/Should We "Treat The Disease?"

- While ISPs **can** block spam from botted hosts by managing port 25 traffic, that doesn't cure the underlying condition – even if we block port 25 direct-to-MX traffic, those hosts **are** still botted.
- As long as those hosts remain botted, even if they **aren't** able to send email spam, they **can** still be used for DDoS attacks, click fraud, fast flux hosting, and many other abusive network behaviors. I'd like to eliminate all **those** possibilities, **too**.
- Therefore **my** preference would be to actually help those ISPs get their customer systems **cleaned up and hardened**.
- Don't get me wrong, I'd be delighted even if those hosts were simply no longer channeling spam, but I'd be a lot happier still if all those hosts were fully disinfected and hardened!

- What would cleaning and hardening those systems entail?

Microsoft's Classic Recipe for Home PC Security

- I've been tremendously impressed by the simplicity and historical effectiveness of Microsoft's classic recipe for home PC security:

  -- Install a trustworthy antivirus and antispyware program
  -- Update software regularly
  -- Never turn off your firewall

- More recently, they've augmented those recommendations:

  -- Use strong passwords and keep them secret
  -- Use flash drives cautiously

  See www.microsoft.com/security/pc-security/protect-pc.aspx

- Those *are* all great recommendations.

"But Joe…" (An Aside on The What to Do Question)

- In talking with security experts about those recommendations, security experts will often immediately flag ways that those recommendations are imperfect or inadequate, including:

  -- it is hard for end-users to accurately track and patch out-of-date software (unless they know about tools such as Secunia PSI)
  -- signature-based antivirus software misses many threats today
  -- many firewalls only block inbound threats, and pay no attention to outbound traffic
  -- what about securing home wireless networks?
  -- shouldn't we be telling users to backup their systems, too?

- All true. But the key point is that there's a limit to what a non-technical audience can absorb and do. Five major general items may be about it. More than that, and you risk overwhelming folks

So Why Are We Seeing So Many Problems In India?

- Shouldn't the classic Microsoft recipe work there, just as it has worked in the United States, Canada and Western Europe? Maybe not.
- For example, is that magic security recipe even available in all the **languages** actually used in India?
- After all, users are more likely to secure their systems if you talk with them about system security in a language they understand! I know that I'd sure have a hard time understanding and following security advice offered to me only in Greek or Thai, neither of which I speak, rather than in English…
- Our counterparts in the Anti-Phishing Working Group are currently offering localized basic phishing education as a redirection link for users who attempt to visit an identified (and taken-down) phishing site. One version of that page looks like…

Velkommen til vr opplringsside om phishing

http://education.apwg.org/r/no/

Google

APWG

www.antiphishing.org

Committed to wiping out Internet scams and fraud

Carnegie Mellon CyLab

Supporting Trust Decisions Project

cups.cs.cmu.edu/trust

ADVARSEL!

Nettsiden du forsøkte å besøke kan ha forsøkt å stjele dine personopplysninger. Nettsiden er fjernet da den er identifisert som en "phishing"-side. En phishing-side forsøker å lure informasjon som bankkontonummer, passord og annen personlig informasjon fra deg.

Hvordan du ble lurt

Hvordan beskytte deg selv

1 Ikke stol på lenker i e-post.

ADVARSEL! http://www.amazon.com/update

2 Oppgi aldri personlig informasjon ut fra forespørsel i e-post.

ADVARSEL! Navn: Kari Nordmann

Kredittkort: 1234 5678 9101 1213

3 Sjekk adressen til nettsiden grundig.

5 Ikke ring til telefonnummer oppgitt i e-post eller i hurtigmeldinger. Slå opp i en mer pålitelig kilde, som telefonkatalogen eller kredittkortfaktura.

Kredittkortfaktura

For kundeservice ring:
+47 11 xx xx xx

6 Ikke åpne uventede vedlegg i e-post eller lenker i hurtigmeldinger (IM).

The Challenging Reality of Languages In India

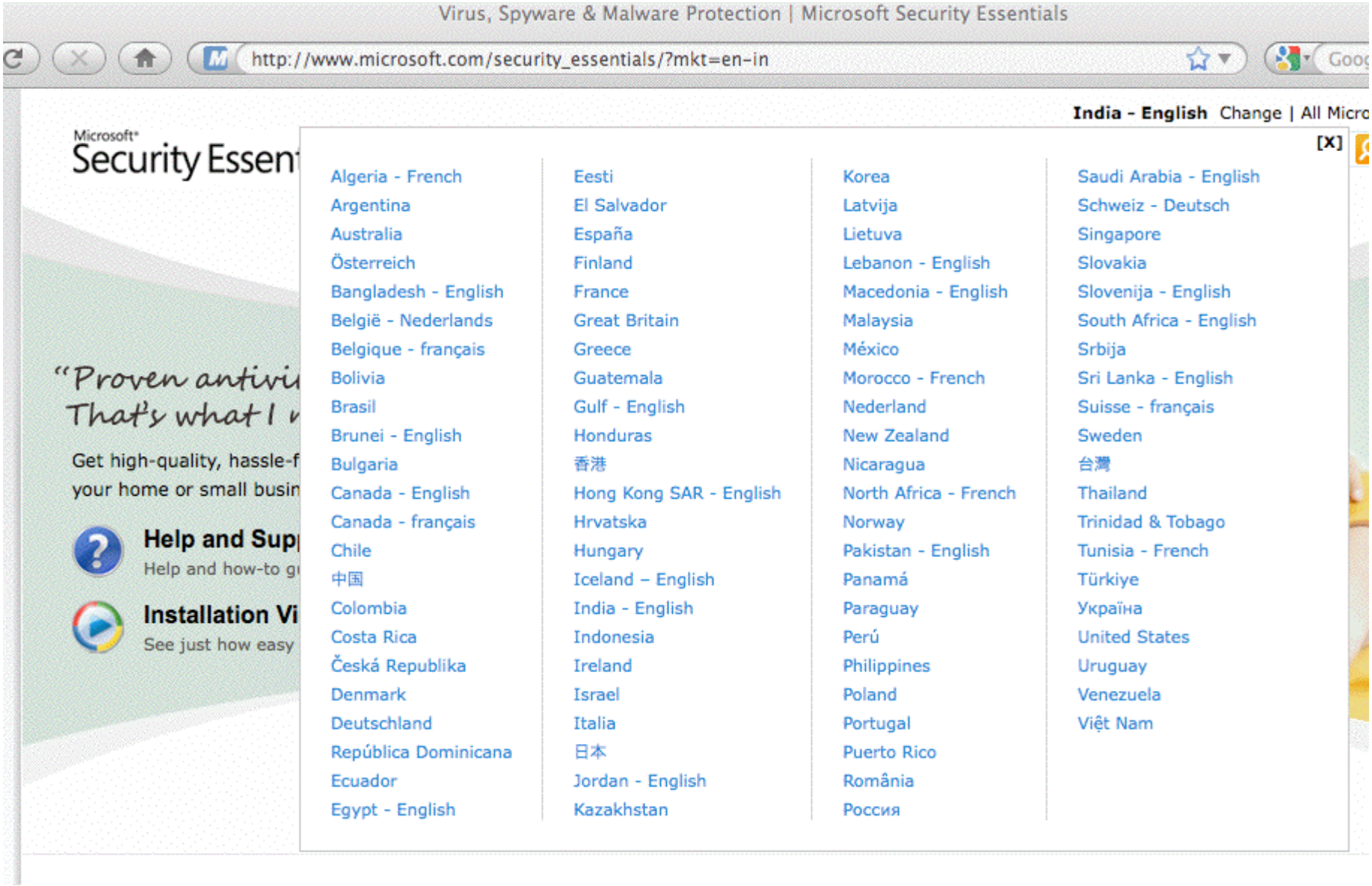
- The (incorrect) stereotype is that most Indians speak Hindi (more accurate estimates peg that only at around 40%) or English (only a few percent of Indians are believed to actually use English, see for example http://news.bbc.co.uk/2/hi/8365631.stm).
- Many Indians use other, less-well-known, South Asian languages such Assamese (1.3%), Bengali (8.1%), Gujarati (4.5%), Kannada (3.7%), Maithili (1.2%), Malayalam (3.2%), Marathi (7%), Oriya (3.2%), Punjabi (2.8%), Tamil (5.9%), Telugu (7.2%), or Urdu (5%). (See: http://www.cia.gov/library/publications/the-world-factbook/geos/in.html). Of course, even a language that's used by "just" 1% of India's population still represents a language used by nearly 12 million people!
- For comparison, there were a little over 28 million Spanish-speaking people in the United States in 2000, and there are just under 7 million Canadians who speak French.

So Is Microsoft's Basic Security Info Available In The Languages Actually Used in India?

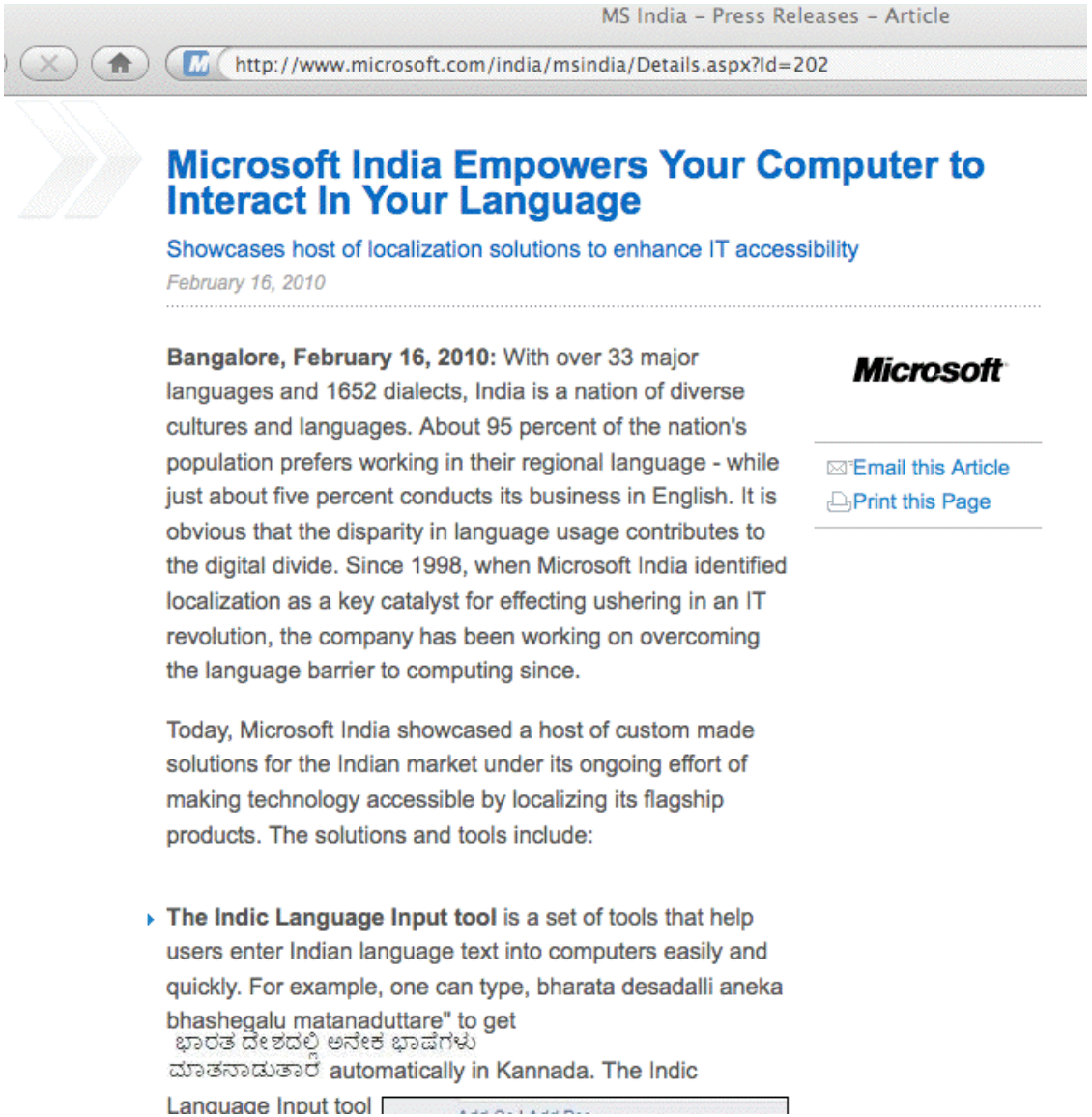
- It may be, but if so, I'm having trouble finding it.

- Microsoft offers some basic security information in *89* different languages or dialects, by my count, however the available options shown on the following screen shot do not appear to include any Indian languages except for "India – English" (and as we've mentioned, that only covers a few percent of all Indian people).

- See the next slide…


Virus, Spyware & Malware Protection | Microsoft Security Essentials
http://www.microsoft.com/security_essentials/?mkt=en-in
India - English Change | All Micro
Microsoft
Security Essen
[X]
Algeria - French
Argentina
Australia
Österreich
Bangladesh - English
België - Nederlands
Belgique - français
Bolivia
Brasil
Brunei - English
Bulgaria
Canada - English
Canada - français
Chile
中国
Colombia
Costa Rica
Česká Republika
Denmark
Deutschland
República Dominicana
Ecuador
Egypt - English
Eesti
El Salvador
España
Finland
France
Great Britain
Greece
Guatemala
Gulf - English
Honduras
香港
Hong Kong SAR - English
Hrvatska
Hungary
Iceland – English
India - English
Indonesia
Ireland
Israel
Italia
日本
Jordan - English
Kazakhstan
Korea
Latvija
Lietuva
Lebanon - English
Macedonia - English
Malaysia
México
Morocco - French
Nederland
New Zealand
Nicaragua
North Africa - French
Norway
Pakistan - English
Panamá
Paraguay
Perú
Philippines
Poland
Portugal
Puerto Rico
România
Россия
Saudi Arabia - English
Schweiz - Deutsch
Singapore
Slovakia
Slovenija - English
South Africa - English
Srbija
Sri Lanka - English
Suisse - français
Sweden
台灣
Thailand
Trinidad & Tobago
Tunisia - French
Türkiye
Україна
United States
Uruguay
Venezuela
Việt Nam
"Proven antivi
That's what I
Get high-quality, hassle-f
your home or small busin
Help and Sup
Help and how-to g
Installation Vi
See just how easy

Does Microsoft Not “Get” The Indian Language Issue? No, They Appear To Understand The Issue…



MS India – Press Releases – Article

http://www.microsoft.com/india/msindia/Details.aspx?Id=202

Microsoft India Empowers Your Computer to Interact In Your Language

Showcases host of localization solutions to enhance IT accessibility

February 16, 2010

Bangalore, February 16, 2010: With over 33 major languages and 1652 dialects, India is a nation of diverse cultures and languages. About 95 percent of the nation's population prefers working in their regional language - while just about five percent conducts its business in English. It is obvious that the disparity in language usage contributes to the digital divide. Since 1998, when Microsoft India identified localization as a key catalyst for effecting ushering in an IT revolution, the company has been working on overcoming the language barrier to computing since.

Microsoft

Email this Article

Print this Page

Today, Microsoft India showcased a host of custom made solutions for the Indian market under its ongoing effort of making technology accessible by localizing its flagship products. The solutions and tools include:

- **The Indic Language Input tool** is a set of tools that help users enter Indian language text into computers easily and quickly. For example, one can type, bharata desadalli aneka bhashegalu matanaduttare" to get ಭಾರತ ದೇಶದಲ್ಲಿ ಅನೇಕ ಭಾಷೆಗಳು ಮಾತನಾಡುತಾರೆ automatically in Kannada. The Indic Language Input tool

It's Good That Microsoft "Gets" the Indian Language Challenge Because Microsoft Will Likely Need To Play A Key Role In Cleaning Up Infected Indian Systems

- Realistically, we probably can't clean up bots in India without Microsoft.
- Many (most?) of the botted hosts in India are running Windows. Microsoft, as the vendor of that operating system, is the natural/ de facto trusted source for security help for those users (any other intervener would need to devote a substantial amount of effort toward simply establishing their security bona fides)
- **Critically important: Microsoft has excellent direct access to users' systems via Microsoft Update (including the ability to run the MS Malicious Software Removal Tool as part of that process)**
- By implication: **ANY <u>scalable</u> program to clean up botted Indian systems most likely <u>MUST</u> involve Microsoft**.

Thinking About The Problem of Scale in India

- How long would it take to manually clean up and secure all of India's current 1,219,562 CBL-listed IP addresses?
- Let's assume that:
  -- each listed IP represents a single botted system
  -- it only takes an hour to clean and harden each of those hosts
  (that's wildly low, but let's give folks the benefit of the doubt)
  -- there will be no newly-botted/repeatedly re-infected systems
- 1,219,562 systems @ (1 hr/per system)
  ---------- = 30,489 person weeks
  40 hrs/per person per week

  30,489/(50 work weeks per person year) = 609 person work years
- But, of course, in reality, even as we might be cleaning some hosts, other hosts will be getting newly infected…
- Bottom line: automation is essential.

A Methodological Aside: The Assumption That 1 Listed IP == 1 Botted Host

- On the previous page I mentioned the assumption that 1 CBL listed IP equals 1 botted host. That assumption is only an approximation, and may be too high or too low.
- A single botted host could result in multiple IP addresses being listed (imagine that single host repeatedly spewing spam while receiving a sequence of different IP addresses from a DHCP pool)
- On the other hand, multiple botted hosts might be "hidden" behind a single shared IP address if users are dialing in, or the user is using network address translation (e.g., they're running a home network that's sharing one public IP address, and multiple hosts behind that home gateway device are infected)
- For now, we'll assume those two phenomena offset each other, but recognize that the infected machine count MIGHT actually be far larger (or smaller) than we currently believe.

Considerations If We Do Need To Rely on Microsoft

- If infected users are running **pirated** copies of Windows, those users may be reluctant to permit Microsoft to access or update their systems, perhaps worrying that doing so might somehow result in their identity being disclosed, or that Microsoft might disable or remove infringing Microsoft products outright.
- Microsoft may not be disposed to undertake a Secunia-PSI-like scan for out-of-date **third party software** applications (such as out-of-date Adobe or Apple software, old versions of Java, etc.)
- If part of what we want as a hardening strategy is for users to use some non-Microsoft products, such as Firefox instead of IE, it would be unrealistic to expect Microsoft to offer users that option
- Microsoft **may not be interested** in investing time and effort in this sort of Indian initiative (or they'd already have done it, right?)
- Lastly, if we do succeed in getting users' attention, will we have the localized security tools they'll need, ready for them to use?

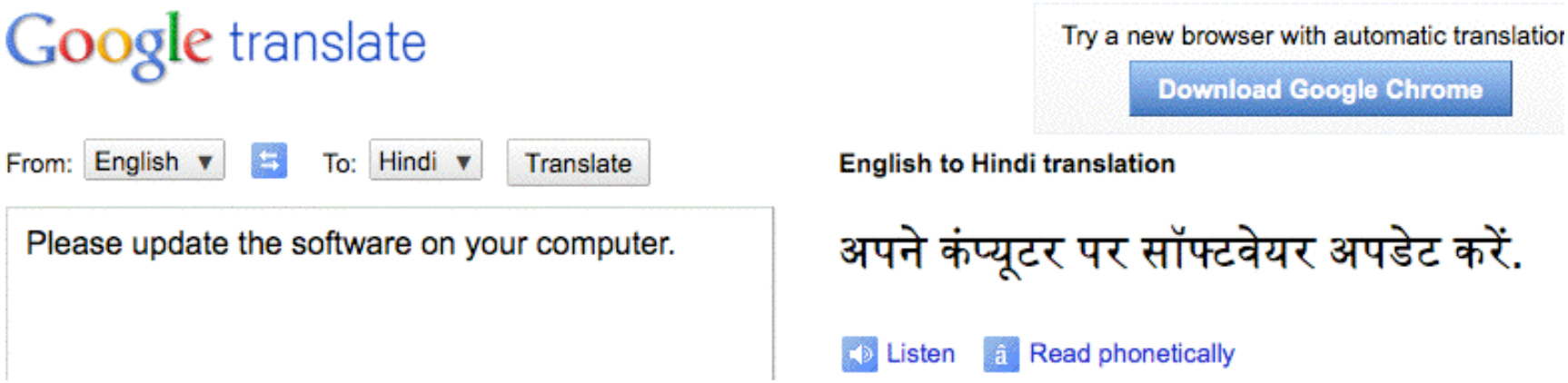
Offering Localized Security Advice Is One Thing, Localized Security Software's Something Else

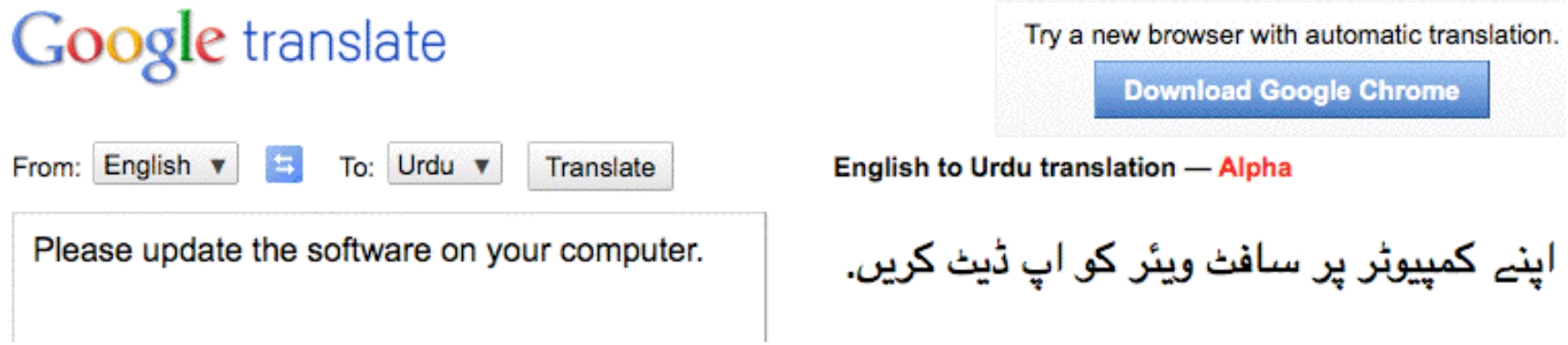
- It's one thing to offer simple security advice in appropriate local languages, but are there alternative web browsers, antivirus products, and other critical security software available in fully internationalized formats to actually implement that advice?
- For example, checking www.mozilla.com/en-US/firefox/all.html I notice that Firefox is available in Assamese, Bengali, Gujarati, Hindi, Kannada, Malayalam, Marathi, Punjabi, and Telugu. Obviously that's not every major Indian language, but it's still a very nice start.
- On the other hand, if you want to get depressed, pick a major Indian language and try to find a commercial (or free) PC antivirus product that's fully internationalized for that language. (Hint: some of the few products you may find may actually be malware, not anti-malware, so be careful out there!)

Many Key Languages Are Uncommon in the US; It May Be Expensive To Obtain Language Expertise

- While many Americans learn world languages such as French, German, Italian or Spanish in high school and college, less common languages are still not studied by enough students.
- The US government, in particular, experiences problems as a result of this shortage, and they've been working hard (and paying premium prices!) to attract American citizens fluent in critical need (CNLs) or super critical need languages (SCNLs).
- An excellent per-agency summary of what languages the government is looking for is available at www2.ed.gov/about/offices/list/ope/iegps/consultation-2011.doc
- Why does this matter to us? If you're trying to internationalize system and network security products, you'll be competing with the government for a limited number of candidates who are fluent in those languages. SCNL's (unfortunately) include Hindi

What About Google Translate?
Yes, It Does Do Hindi (and Now Even Urdu)





Question: any native Hindi or Urdu speakers in the audience? What do you think?

Looking at That Translated Text, Part of the Issue May Be A Matter of Alphabets/Font Support

- Supporting different languages in software products can be tough, but it can be doubly tough when the languages you're trying to support don't use the usual Latin alphabet we're used to in the West.
- For example, standard Hindi uses Devanagari script – if you're developing a piece of security software, you may internationalize it for "easy" foreign languages (such as French, German, Italian or Spanish), but are you going to make the effort for languages that don't even use a Western alphabet? Empirically, we know that many companies don't do so.

- Thus, it's not surprising to see that many of the top ranked countries listed on the CBL use non-Latin alphabets…

Alphabets Used By The Top Ten Countries on the CBL

1	**India**	**Devanagari and others Brahmic scripts**
2	Brazil	Variant of the Latin alphabet
3	**Russia**	**Cyrillic**
4	Vietnam	Variant of the Latin alphabet
5	**Ukraine**	**Cyrillic**
6	Indonesia	Variant of the Latin alphabet
7	**Thailand**	**Thai script**
8	Italy	Variant of the Latin alphabet
9	**Pakistan**	**Pashto alphabet, Urdu alphabet**
10	**China**	**Simplified Chinese**

- Obviously not all alphabets are not equally problematic. There are some top notch security products (such as Kaspersky's antivirus product) which are available in Cyrillic, yet Russia and the Ukraine are both CBL "Top 10" states. And what of BR, VN, IN, and IT, all of which use some variation of a Latin alphabet?

The Indian Government's TDIL Program: A Possible Partner For Localized Security Tool Development?

Making Patching Faster and More Efficient

- The other factor that will facilitate people getting patched would be making the patching process faster and more efficient. Patches cannot be something that will take hours or days to download. Patches need to be available in just a matter of minutes, or perhaps an hour at the most.
- Bandwidth issues implies that fast patch downloads probably requires creation of **local** low latency "patch repositories" (or local "patch caches") for all major vendors.
- The natural location for these sort of repositories would probably be at Internet exchange points, so the traffic doesn't need to come from North America or Western Europe, etc.
- Checking http://www.ep.net/ I see only one exchange point operator in India, http://www.nixi.in/ , with locations in Mumbai, Delhi, Chennai, Kolkata, Bangalore, and Hyderabad.

Antivirus Software and Patches on Physical Media

- Another possibility would be making antivirus software and patches (where permitted) available on physical media – CD-ROMs, DVDs or even inexpensive thumb drives.
- In some cases, this may be the most expeditious way of sharing critical patch information with "thinly networked" users, but it is still not without potential issues:
  -- generally, vendors are reluctant to allow 3rd parties to deliver patches via physical media
  -- if you charge for media, even a small charge may be too much for economically struggling individuals; if you don't charge, you may be subject to frivolous requests for media
  -- how do users know that the CD-ROM or DVD or thumb drive they receive is genuine, and not tainted with malware? (Yes, the contents can be digitally signed, but many users might not reject inappropriately signed or completely unsigned media)

III. Who?
(or “WHO”?)

Who Will Help Fix Bots in Developing Countries?

- We've talked a little about how ISPs could take action to mitigate the impact of bots, and we've also talked about how Microsoft (and other software vendors) could play a role in helping to fix bots in rapidly developing countries.
- But if it turns out that we can't do this at a commercial level, do we need a full blown program of foreign assistance by governmental or non-governmental organizations?
- Many more fortunate nations recognize their humanitarian obligations to their less fortunate neighbors when conventional disasters strike, providing food, clothing, temporary shelter, medical assistance and help rebuilding. Has the time come for us to also create an international cyber outreach effort, a cyber **"world health organization,"** to help the world better cope with cyber disasters, such as large scale bot infestations?

The Cyber World Health Organization Idea Isn't New

- For example, I talked about it at the Anti-Phishing Working Group's E-Crime Summit held in San Francisco in May 2007, see "We Need a Cyber CDC or Cyber World Health Organization," pages.uoregon.edu/joe/ecrime-summit/ecrime-summit.pdf
- More recently, APWG, along with the IEEE, held an invitation-only e-Crime Response and Management Roundtable meant to rekindle interest in public health approaches to cyber threats at the end of their 2010 General Meeting in Dallas, Texas.
- Senior Microsoft staff members have also publicly advocated for a public health approach to infected computers, most notably Scott Charney, Microsoft's VP for Trustworthy Computing, as part of his recent RSA keynote ("Fight computer viruses like epidemics: Microsoft," http://tinyurl.com/microsoft-public-health)
- Does this approach finally have "legs?"

There Are Some Existing Efforts to Help Network Operators In Developing Nations

- As an example, the National Science Foundation and many generous sponsors from the commercial sector currently support the Network Startup Resource Center (NSRC), which is homed at the University of Oregon in Eugene, see http://www.nsrc.org/

- While the NSRC works in many developing countries in Africa, Asia and South America, their focus really isn't primarily on end-user security or preventing spam, and they certainly aren't staffed or funded to handle outreach to end-users who may be botted or who may need help hardening their systems.

- However, their efforts could serve as a model for some other organization that IS appropriately focused on botted hosts.

Is There A Role for MAAWG in This Area?

- Does MAAWG have leadership responsibilities when it comes to dealing with the problem of bots in rapidly developing countries?
- We can certainly draw attention to the problem -- IF we want to do so -- and sometimes publicizing a problem can be an important first step toward fixing a major problem.
- Can we translate some of our current best practices into languages that are relevant to rapidly developing regions?
- Can we evangelize the importance (and the business value!) of running clean networks, and sell that message to our international ISP counterparts? Will they be willing to help push that message to their customers?
- Or is the problem of botted hosts abroad simply not our problem, even if that's where we're seeing much spam originate today? Can we continue to just "block and forget"? I sure hope not…

Thanks For The Chance to Talk Today

- Are there any questions?