Web Management
inter@ctive technologies
We don't Design the Web, We Manage it!

AN INVITATION TO JOIN A WORLD WIDE PROTECTED NETWORK

WEB MANAGEMENT PRESENTS....

THE PROTECTED NETWORK

A FIRST LINE OF DEFENCE IN AN UNCERTAIN AND NETWORK CONNECTED WORLD

A Policy Discussion Paper - to Governments around the World

Draft 7.1 – 31st October 2011

Executive Summary

Cybercrime has grown into a worldwide 388 billion dollar a year industry globally based on financial losses and time lost. 14 adults fall victim to Cybercrime every second of every day. Viruses, malware, online scams and phishing dominate the Internet. Thus far, attempts by governments and law enforcement agencies to stem the tide have had little to no effect. (http://norton.com/cybercrimereport)

There are literally Millions upon Millions of Internet connections around the World. Of these connections, less than half have adequate protection, and an even smaller fraction of these are kept up to date. Many devices don't have an option of protection at this time. Those most at risk are of course those least able to defend themselves. (http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0/)

Web Management is proposing that your Internet users are given the choice of using The Protected Network as their first line of defence. The purpose of the Protected Network is the safeguarding of internet connected devices and the defence of the personal security of internet users. The Protected Network will achieve this end by blocking access to sites that harbour documented technical threats. Once they are blocked, it goes further to educate users about the dangers, and assisting users with the improvement of their online security. (www.protectednetwork.org/)

This approach differs from others in many ways. It is completely optional, transparent in operation and works alongside the Net Surfer. It does NOT monitor their connection. All data is derived externally to the ISP. By default, everyone is connected to the Protected Network, but they are able to change their level of protection at any time, right down to disconnecting entirely. ISPs join the network under whatever mechanism works best in your country. An Industry Code, a recommendation, whatever works for you. As far as what equipment, software, etc is used, that is entirely up to the ISP. The actual lists are provided by the Protected Network free to the ISP, and the service is free to the user.

There is a Cyber Criminal problem - Blocking Cyber Criminals will work

Phase one of implementation is already completed in Australia, with the Australian Protected Network deployed at ISP, Business and Home locations. During Stage Two implementation, The Australian Protected Network will be expanded to include all Internet Access points in Australia. It will prevent known cyber criminal locations on the net from interacting (scamming, infecting, etc) Australian Internet users. It will do it optionally, transparently, and purely as a tool for the Australian Internet user to make use of. This same protection needs to be rolled out around the world, forming a protective network.

Furthermore, it will provide education and direction towards Anti-Virus and support software that Internet users need to prevent further danger. Instead of a user getting a Phishing website when they click on a dangerous link in an email, they receive the education they need to prevent them doing it again, and links to Anti-Virus protection software that will help protect them.

Mikko Hypponen, Chief Research Officer at F-Secure Corporation believes, “We need to improve security, educate people and most importantly, we need to work internationally to catch and prosecute online criminals.” Mikko has been fighting online crime for over 20 years, and states that the problem has never been worse than it is today.

Mark Garlipp is Managing Director of ECN Internet. He has over 20 years experience and has taken part in every step of the development of the Australian Protected Network. His experiences as an Internet Service Provider have been invaluable in proving that the very real threat of Cyber Crime can be overcome.

Brian Hay from the Qld Police Fraud squad is the top police officer in this area. He believes the Protected Network would make a valuable contribution to the security of our nation.

Bob Gurnett from CITEC is Queensland’s Chief Technology officer, and he commends the contribution that the Protected Network will make to Cyber Security.

Bev Robb is from Teksquisite, Internet security & privacy experts. Bev states that there is a serious cybercrime problem globally, and that the Protected Network Phase Two is the next step on the road to a more secure online future.

Julio Canto is a Security Analyst from Virus Total/Hispasec Sistemas. He has many years experience in the Internet Security arena and recommends that a strong blocking regime is a very important first step in the fight against cyber criminals.

Peter Coroneos, as CEO of the Internet Industry Association, at the last Cyber Security Taskforce meeting stated that James Collins has something in the Protected Network. Peter has firsthand experience that there is a problem with Cyber Crime and that the APN can make a difference.

Matt Tett from Enex Test Labs has extensive knowledge of Cyber Criminal behaviour in many years of work in this field. He knows that the Cyber Criminals can and should be blocked.

Brian Krebs of KrebsonSecurity is one of the most highly respected leaders in this field. He not only helps with the discovery of Cyber Criminals, he works with the industry. Brian says that Cyber Criminal activity can and must be blocked.

LeaseWeb is one of the twenty largest providers in the world. It is their belief that they have a responsibility to ensure a “clean and safe internet”, so they have taken steps to “block malicious and hacked websites”.

http://vrritti.com/2010/08/24/leaseweb-to-monitor-cybercriminals/

The Norton 2011 Cyber Crime Report is an extensive source of data on this topic. It includes data showing the global cost of cyber crime right down to discussion about the need to prevent access to cyber criminals.
http://norton.com/cybercrimereport

Alastair MacGibbon is director of the Centre for Internet Safety at the University of Canberra. He is the former director of the AFP's High tech Crime Centre. Alistair states that governments need to take more responsibility for online security as more services are being offered online.
http://www.abc.net.au/am/content/2011/s3312727.htm

We also have commendations from the Mayor of Redland City, the local State Member of Parliament and our Premier, Anna Bligh, who believes this paper is a “Solid Start”. And that’s what we need! A starting point towards a global solution.

Ken Mihill from Scripture Union Queensland has been involved with Phase One of the Australian Protected Network, and has been using it to protect his family from a myriad of threats for many years. His experience and remarks are attached.

The Web Management Solution

In the face of a withering assault from the many attack vectors of the Cyber Criminals, Web Management proposes creating a default layer of protection for all Internet connected devices. For the first time, all Internet users, everywhere, will have a choice of being protected online, and educated about the dangers they face.

Tablets, mobile phones, game stations, medical equipment, and of course the many desktop and laptop computers on the market, will all have the option of a “First Line of Defence”. There is no default level of protection currently available for these devices, and for many of them, there is no available protection against the cyber criminals. The Protected Network gives them a “Choice”.

The proliferation of mobile devices of varying types is fuelling a proliferation in cyber Criminal activity that targets the use of these devices. We are moving further and further away from standard desktop hardware and relying more and more on mobile devices which are inherently insecure.

Under the Australian Protected Network, all Australian internet connection points are provided with an APN relay box. In Australia alone, 104 ISPs service a total 10,446,000 internet users, as of the end of 2010. A relay box at each ISP provides up to date amalgamated lists of sites that are currently causing trouble. The Internet Service Provider hardware is then updated with this data and therefore, users are protected from documented technical threats to the security of their devices.

APN relay boxes are in turn connected to the central processing equipment at Web Management, which collates the lists and provides the updates. In your country, a central agency will provide the same function.

Our proposal at this time is to continue the roll out of the Protected Network in further stages, initially only drawing on existing reliable public sources to determine the location of cyber criminal activity. Once the network is fully rolled out, we can improve on that functionality by using the unique technologies available through Web Management to make advanced protection methods available, expanding the choices for users. But it will always be their choice.

Problems of Cyber Crime are also bringing up problems of Privacy. Big Brother has arrived, but he wasn’t the Government conspiracy we all expected; he *is* a cyber criminal with designs on gaining access to every part of your online, and offline, life.

There are special considerations when designing a National protection system. That’s why the Protected Network does *not* monitor users and does *not* make use of any user activity or transfer logs. The Protected Network users’ privacy is assured at all times; indeed it is improved by the protection from cyber criminals provided.

It is completely optional, transparent in operation and works alongside the Net Surfer. By default, everyone is connected to the Protected Network, but they are able to change their level of protection at any time, right down to disconnecting entirely.

Corporate Information

Web Management InterActive Technologies Pty Ltd is a Queensland, Australia owned company that has been in operation since October 2002.

The Principal of Web Management, James Collins, has been in the industry since 1984 and has extensive experience with computer communications. He is one of the original members of the Internet Industry Association of Australia and has become recognised by the IIA for his knowledge and experience in the field of National Cyber Crime protection. (www.iia.net.au)

Web Management is involved with the iCode compliant, Family Friendly, and Responsible Internet Business programs, as well as being on the E-Security and Classification Taskforces. (www.icode.net.au)

Web Management is a member of the International Cyber Threat Task Force. (www.icttf.org)

Research and development of the APN has been the primary focus for the past 9 years and represents a significant investment. During that time, Web Management has been providing protection to businesses and families in Brisbane, Qld while continuing to hone the network. It has been in use at ISPs (e.g. Mark Garlipp - ECN Internet), Businesses (e.g. Ian Renton – Renton Dental), and families (e.g. Ken Mihill).

Web Management has provided written and oral submissions to Cyber Crime and Cyber Safety committees. In June 2010 we appeared in the “Emerging Technical Measures to Combat Cyber Crime” section of the Hackers, Fraudsters and Botnets publication, and in June 2011, under the "New Technologies" section of the High-Wire Act publication.

Appendix Index

1) Technical Documentation
    a. Phase Two rollout – Technical Summary
    b. Later Phases – Technical Summary

2) Supporting Documentation
    a. Mikko Hypponen, Chief Research Officer, F-Secure Corporation - the leader in research in this area
    b. Brian Hay, Detective Superintendent, Fraud and Corporate Crime Group, Qld State Crime Operations Command.
    c. Bob Gurnett, Qld Chief Technology Officer.
    d. Bev Robb, Teksquisite
    e. Julio Canto, Virus Total, Hispasec Sistemas Lab
    f. Matt Tett, Enex Test Labs
    g. Ken Mihill, Scripture Union Qld
    h. Melva Hobson, Mayor of Redland City
    i. Michael Choi MP, Member for Capalaba

Phase Two Rollout – Technical Summary

Cyber Criminals base their phishing attacks around compromised websites that they use as jumping off points for the hosting of forms that trick innocent users into entering their personal credentials. The locations of these compromised websites are collated by bodies such as “Phishtank”. To quote their website, “Phishtank is a collaborative clearing house for data and information about phishing on the Internet”. Phishtank is one of many such databases created specifically for the purpose of protecting users.

We are using periodic exports from these known, reliable databases to populate the database tables at Web Management. In the case of Phishtank, a program running on the WMIT server transfers the XML output from their service into the WMIT database. This data is then disseminated throughout the rest of the Protected Network by means of periodic requests from the Protected Network relay nodes at the ISPs.

The Web Management server receives periodic requests from the ISP based nodes on the network and delivers updates to add or delete data from the node’s database.

Based on the ISP’s requirements, the node exports to a formatted list, the current database of dangerous sites and any associated, derivable, control file information such as Proxy configuration lines to match their equipment.

When the ISP equipment receives an attempt to connect with one of these compromised websites, it responds by instead showing a site report page built by the WMIT servers, based on the ISP that is making the request, and the site that they were trying to access. No user identifiable information is transferred.

The WMIT reporting system uses this information to build a customised response to the threat that they were nearly exposed to. This page includes tips on how to avoid the dangers and provides educational and anti-viral links that can assist with their protection in future. This page also includes ISP specific information such as information on activating and deactivating the Protected Network functions on their Internet connection.

Later Phases – Technical Summary

Once the Protected Network is rolled out and bedded in, we can start to provide additional, far more effective options, ramping up to a World Wide system which engages with law enforcement and neutralises emerging threats.

Options will assist in the areas of solving the problem of copyright, giving problem gamblers a choice, and other currently unsolvable problems. The Protected Network is all about giving users a choice to be protected, or not. It does not, will not, and can not work in an environment of enforcement. This is a Cooperative Network.

The servers at Web Management have, for the past 9 years, been scanning and profiling the Internet. Patterns are stored in a vast knowledge engine of quadrillions upon quadrillions of patterns of profile points. These patterns are largely unexploited at this time, but as users become available to provide input, more accurate results in the search for online criminals will result from the exploitation of this system.

Users of the Protected Network will have the option of taking part in the fight by adding their input to the equation. We can draw on the vast “Crowd” of the Internet to discover newly linked cyber criminal locations. Together, we can all step forward into a more secure, more transparent, tomorrow...

James Collins

From: Mikko H. Hypponen [mikko.hypponen@f-secure.com]
Sent: Friday, 9 September 2011 9:37 PM
To: jamesc@au.wmit.net
Subject: Re: Expert quote needed.

My name is Mikko Hypponen.

I've been fighting online crime for over 20 years, and the problem has never been worse than it is today. Organized criminal gangs are stealing massive amounts of money with backdoors, banking trojans and password stealers.

We need to improve security, educate people and most importantly, we need work internationally to catch and prosecute online criminals.

James is right in drawing attention to this urgent topic.

Mikko Hypponen
Chief Research Officer
F-Secure Corporation

James Collins

From: Hay.BrianJ@police.qld.gov.au
Sent: Wednesday, 11 May 2011 3:59 PM
To: jamesc@australianprotectednetwork.com.au
Subject: RE: Australian Protected Network

Hi James

I am happy to acknowledge the willingness of effort you display in the fight against cyber crime and the protection of communities from adverse cyber influences.

Combating cyber crime requires a holistic approach from police, government, industry and community perspectives. The Australian Protected Network provides a valuable contribution to achieving those goals and I applaud you for your efforts.

Thank you

Brian Hay
Detective Superintendent
Fraud & Corporate Crime Group
STATE CRIME OPERATIONS COMMAND

' (07) 3364 4441
' 0438264564
7 (07) 3364 6549
* Hay.BrianJ@police.qld.gov.au
* P.O. Box 1440, Brisbane, Qld 4001
F *Police Headquarters, 200 Roma Street, Brisbane

James Collins

From: Bev Robb [teksquisite@gmail.com]
Sent: Monday, 12 September 2011 6:27 PM
To: jamesc@au.wmit.net
Subject: Australian Protected Network

James,

I looked at your proposal with great interest. There is a serious cybercrime problem (globally) and the Australian Protected Network Phase two is the first step towards fighting online criminals. Technology that can block cyber criminal activity, would be a tremeandous asset to your country and to the world at large in the fight against cybercrime.

My expertise is in the area of Internet security & privacy - anyone can google Teksquisite or Bev Robb and get a pretty good idea regarding my knowledgebase.

Though Phase two is not the complete solution, it's just the start of the solution - you will need backing and resources in order to achieve this. Hopefully your country will be supportive of this new technology and find ways to share it with other countries (after it has matured a bit more.)

Best Wishes,

Bev Robb
Teksquisite
541.727.1966

James Collins

From: Julio Canto [jcanto@hispasec.com]
Sent: Monday, 12 September 2011 7:36 PM
To: jamesc@au.wmit.net
Subject: Re: about the questions

I'm Julio Canto and I work at Virustotal.com, a site dedicated to analyze malware. I've also worked in my company fighting various forms of cybercrime (phishing, crimeware, etc) for customers like banks and big companies in the EMEA and LATAM zones.
Online crime is a problem since many years ago, but the problem is that by now, most of its victims are average people, therefore there's not much reaction from governments about it. You only need to check reports from FBI, APWG or other respected entities to corroborate it. Blocking _fast_ that kind of phenomena is a very importante first step to do something in a field where almost nothing effective is being done.

--

Regards,

Julio Canto | VirusTotal.com | Hispasec Sistemas Lab | Tlf: +34.902.161.025 | Fax: +34.952.028.694 | PGP Key ID: EF618D2B | jcanto@hispasec.com

just my humble opinion, after spending some years in antifraud activities :/

James Collins

From: Matt Tett [matt@testlab.com.au]
Sent: Tuesday, 13 September 2011 10:04 AM
To: jamesc@au.wmit.net
Subject: Enex TestLab opinion on cyber-crime

Dear James,

Thank you very much for your recent call in relation to my thoughts on cyber-crime.

Do I personally consider that cyber-crime exists, and is a significant global problem ?

Yes, indeed, there is absolutely no question that Cyber-crime exists, I have been a practising cyber-security professional for over fifteen years now, I hold current CISSP, CISA, CISM and CSEPS certifications in good standing. And that is not just my personal opinion, but one shared by our organisation, Enex TestLab. We work at the forefront of independent professional testing, globally and one of the key areas is security testing.

Is there something that can be done about cyber-crime ?

Absolutely, exactly what however, is the billion dollar question. Cyber-crime is a global issue, spanning jurisdictional, legislative, cultural and political boundaries. Enabling the criminal organisations behind these threats to obscure their tracks and evade law enforcement. The very nature of electronic networking systems and electronic data and records means technology is an enabler for fraud and theft. Radical changes and solutions are needed. Critical national infrastructure, financial institutions, Government departments and agencies worldwide have been coming to terms with this over the recent years, but as in most illegal activities the criminals have the upper hand in the fact that they are generally well funded from their proceeds and are not tied by rules and regulations, so as the net tightens so to speak they jump to the next option striving to remain one step ahead.

Regards,

Matt Tett
Managing Director
CISSP, CISM, CISA, CSEPS

Enex TestLab
RMIT University Bundoora East Campus
Building 253 Room 21
Plenty Road Bundoora VIC 3083
P: +61 3 9436 7454 (ext 101)
M: +61 (0) 417 399 280
W: www.testlab.com.au

Mr Ken Mihill
33 Granby St
Upper Mt Gravatt
Qld 4122

5 May 2011-05-05

Mr James Collins
P.O. Box 1073
Capalaba, Qld, 4157

Letter of Recommendation – Australian Protected Network

To whom it may concern,

I am writing to recommend the internet protection system created by Mr James Collins of Web Management Interactive Technologies and known as the Australian Protected Network.

My family and I have been under the protective umbrella of a system created by Mr Collins for a number of years now. As a father of two teenage daughters I am able to comfortably allow them internet access knowing that they and my household system are covered. Media and criminal activity reports identify that girls are consistently the target of predators and there is a need to provide a sound level of protection for those who are vulnerable.
As a former detective I know that the people who seek to harm others show levels of determination and resourcefulness that the average person does not have the time or awareness to counter. It is incumbent upon those who have the capacity to do all within their power to actively provide protection against those who would harm. I know that Mr Collins has dedicated his personal time and resources into this cause around the internet.
It is said that evil flourishes when good men do nothing and with regards to the internet this is a true saying.

I could not even fathom the financial savings that could flow to the community by having an effective internet protection system but I am aware that internet related crime is significant in our country. To stem the victimisation from this crime and to be able to direct valuable resources towards the detection and prevention of other crimes must be a significant benefit to our society.

The Australian culture has been an attractive one to all in other countries and part of that is the opportunity to relax and enjoy our leisure activities without fear of victimisation or offensive material. The internet is an important part of our life now and our leisure. When people can't safely use it part of our culture is threatened. Nobody likes to live in fear, yet that is how some feel for want of an effective protective system.

I hear the government is making moves towards internet security, but it would be far more significant to see things implemented. And so I encourage the Government to recognise that the Australian Protected Network meets a need of Australians, and ask that they seriously consider investigating its implementation.

Kind regards,

Ken Mihill

From the Mayor's Office
Melva E Hobson
Mayor of Redland City

21 April 2011

Our Ref: MH:hs
DW: 5449390
Contact: Mayor's Office
3829 8235

TO WHOM IT MAY CONCERN

It is encouraging to hear that progress is being made regarding the Federal Government recognizing the benefits of the Australian Protected Network. The purpose of this dialogue is to indicate that I commend Web Management's work towards providing a first line of defence for the more vulnerable members of our community.

I realize that if implemented successfully, the Australian Protected Network could provide inestimable financial savings to the community, not to mention saving countless lives being negatively affected by the criminal elements of the online world.

Therefore I encourage the Government to recognize that the Australian Protected Network meets a need of Australians, and ask that they seriously consider investigating its implementation.

Yours sincerely

Melva E Hobson

Melva E. Hobson PSM
Mayor of Redland City
Queensland's Sustainable City for 2010

Redland City Council
ABN 86 058 929 428

Cnr Bloomfield & Middle Sts.
Cleveland Qld 4163

PO Box 21,
Cleveland Qld 4163

Telephone 07 3829 8623
Facsimile 07 3829 8781

Email mayor@redland.qld.gov.au
www.redland.qld.gov.au

Electorate Office
Shop 60
Capalaba Park Shopping Centre
Redland Bay Rd
CAPALABA QLD 4157

Postal Address
PO Box 50
CAPALABA QLD 4157

Phone: (07) 3245 6950
Fax: (07) 3245 4871
E-mail: capalaba@parliament.qld.gov.au

MICHAEL CHOI MP
MEMBER FOR CAPALABA
ALEXANDRA HILLS - CAPALABA
THORNESIDE - BIRKDALE

27 April 2011

OUR REF: 11/04GEN/mc:mw

To whom it may concern

I've known James Collins of Web Management Interactive Technologies for over 5 years. I've found him to be totally dedicated to creating a secure internet network environment to protect our community, including young people and our business sector.

Not being an expert in this field I am not au fait on how his system will work but one thing I do know, we need to have better protection from criminal elements in cyberspace.

I commend Web Management's work towards providing a first line of defence for the more vulnerable members of our community.

I realise that if implemented successfully, the Australian Protected Network could provide inestimable financial savings to the community, not to mention saving countless lives being negatively affected by the criminal elements of the online world.

James is an honest and dedicated person. He has devoted a good part of his life for this cause at great personal and financial expense.

I seek your support in giving him the best possible assistance and consideration to his proposal accordingly.

Yours sincerely

MICHAEL CHOI MP
MEMBER FOR CAPALABA