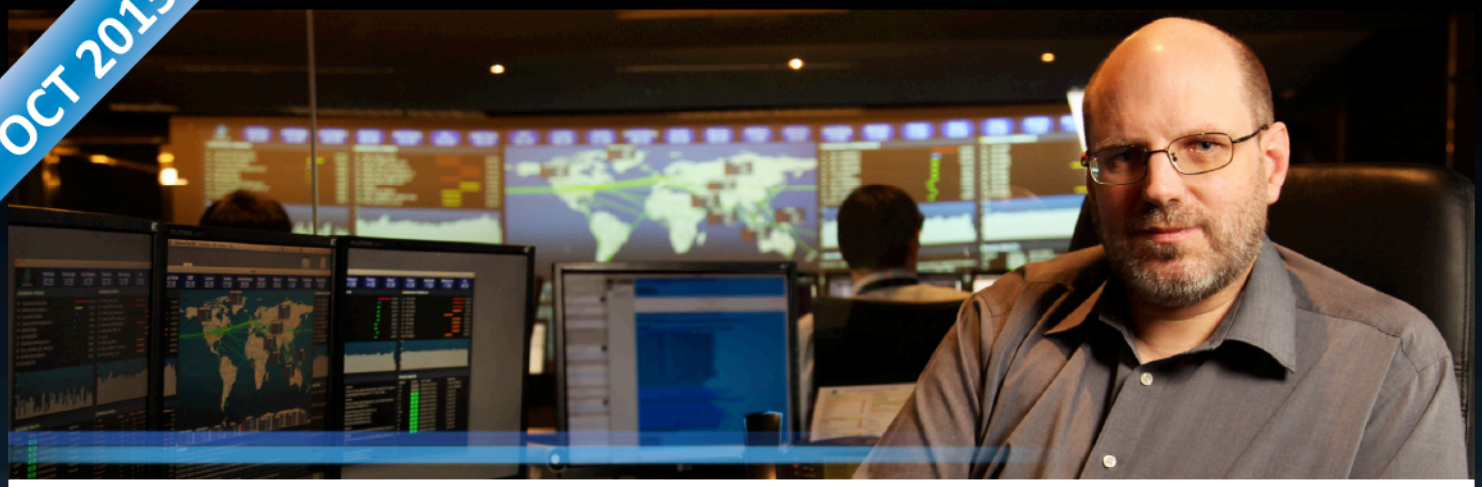
OCT 2015



Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the October 2015 edition of In the Boxing Ring

This month, in a special report conducted by Network Box USA's Pierluigi Stella (Chief Technology Officer), and Andrew Tynefield (Network Security Engineer); we analyze and discuss the type of techniques that hackers are using in a phishing email that was caught in our system on 7th July 2015. For a step-by-step breakdown of the analysis please read pages 2 to 4.

On pages 5–6, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5 and Network Box 3. Based on Sunset Policy, we will continue to support, Network Box 3 until at least late 2018.

Finally, Network Box was at the RetailEx ASEAN 2015 Expo at the IMPACT Convention and Exhibition Center, in Bangkok. We are also pleased to announce that the Network Box 5 appliance platform has been nominated for the SMBWorld Awards 2015.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
October 2015

You can contact us here at HQ by eMail (nbhq@network-box.com), or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

twitter http://twitter.com/networkbox

facebook http://www.facebook.com/networkbox
http://www.facebook.com/networkboxresponse

LinkedIn http://www.linkedin.com/company/network-box-corporation-limited

Google+ https://plus.google.com/u/0/107446804085109324633/posts

In this month's issue:

NETWORK BOX

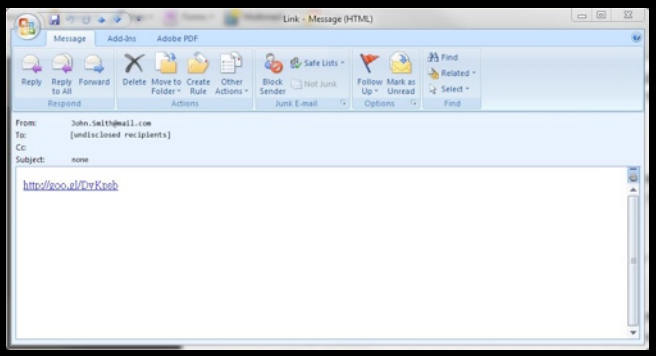
Network Box Special Report: Analysis of an email attack

Date:
7th July 2015

Analysts:
- **Pierluigi Stella**, Chief Technology Officer, *Network Box USA*
- **Andrew Tynefield**, Network Security Engineer, *Network Box USA*

Hackers are becoming increasingly clever at hiding their "products" in order to trick users into downloading malware. We all claim to know that, but to what extent do we really understand what's going on?

I'll illustrate the dedication these people have to their job by analyzing an email that was caught in our email filters on 7th July 2015:



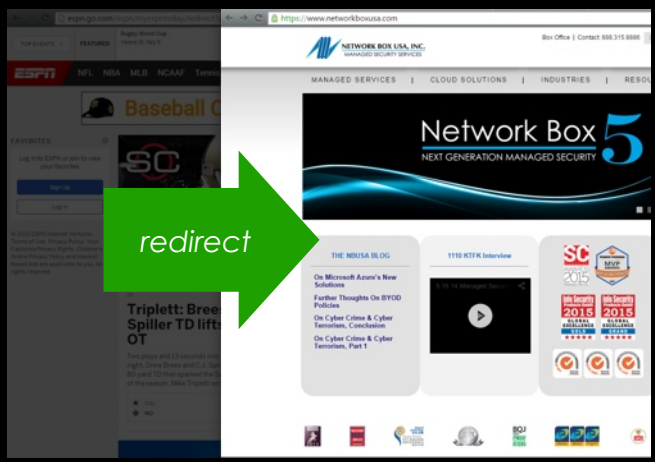
The email was basically empty, containing just an HTTP short URL. As a user, I never open links in an email unless I know the sender, I'm expecting that email, and there is some 'explanation' text in the email as to why I should click on that link. Nevertheless, users less used to security are more than likely tempted to click. So, the link was http://goo.gl/DvKpsb which expanded into:

http://espn.go.com/espn/myespntoday/redirect?url=http://www.live.com.breaking.news.bestoffer2015.info#topacuq45053

Let's analyze this long string. The URL is actually espn.go.com, a very legitimate URL; millions click on it every day to follow their beloved sports teams. There's nothing wrong with the URL per se. But, keep reading. After the first slash, you see **"redirect?url=…."**. Now, for the sake of demonstration, copy and paste the following in your browser:

http://espn.go.com/espn/myespntoday/redirect?url=http://www.networkboxusa.com/

As you do that, follow what happens by looking at the status line at the bottom of your browser. You'll see the browser go first to espn.go.com, then to www.networboxusa.com. This is what a redirect does, what it's supposed to do. That's the objective of the line above – it redirects you from the main URL to somewhere else; and, really, it can be to anywhere else.



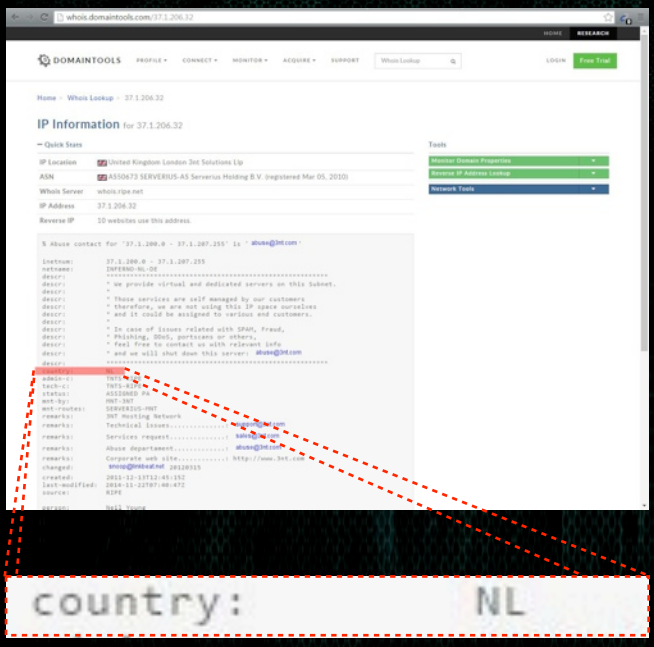
The problem is, whoever's managing espn.go.com has created a vulnerability on their website by not properly controlling the redirect. This allows hackers to exploit the redirect, sending you anywhere the hacker wants. A redirect should **not** be so exposed and publicly available like that. It should be controlled so it can be used only to send you where the webmaster of the website intended to redirect you.

That said, another trick follows. The link where you're being redirected is:

www.live.com.breaking.news.bestoffer2015.info.

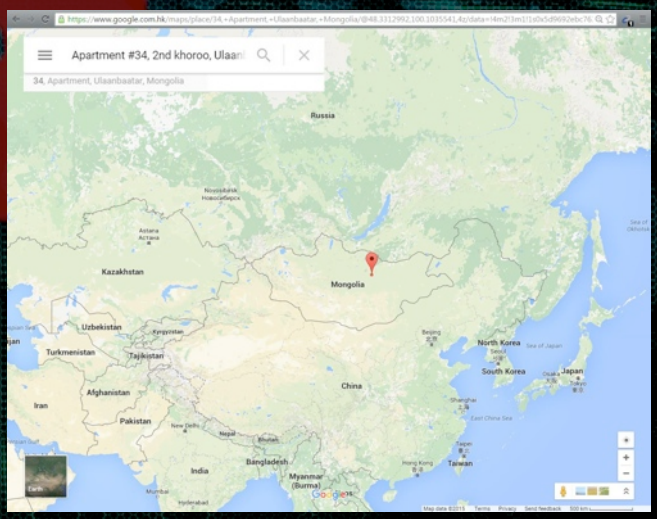
Within that link, you're being sent to tag **topacuq45053**.

Now, to the non-expert eye, this might look like a Microsoft link (www.live.com) but that's not how domain names work. You should always read them from right to left, meaning the actual domain name here is bestoffer2015.info. This domain resolves to **IP 37.1.206.32** (which is assigned to the Netherlands) and belongs to a company called 3NT Hosting Network, which is likely legitimate, and completely unaware of what's going on with this link hosted on their server. The DNS servers for the domain are, instead, hosted in the Russian Federation.



Looking at the HTML content of the www.live.....info link, we find a java script. At this juncture, the hacker could choose to do many things but he chooses to hide another redirect into the script. In fact, the script creates random URLs, all within the domain com-1sv.net. We won't go into the details of the java script; suffice to say it merely generates random names but the actual domain does **not** change – it's always com-1sv.net.

This domain resolves to 3 IP addresses, assigned to Japan. But a "whois" of the IPS reveals that the IP is actually reassigned to a company called iTools LLC, located at "Apartment #34, 2nd khoroo, Ulaanbaatar Bayangol 16050 in Mongolia. We took the time to check Google maps; the address **actually** exists. Whether there's truly an iTools LCC at that address or not remains to be seen. It isn't unlikely though that they too are unknowingly hosting this link on their servers.



Finally, the final page, randomly generated by the java script, in reality always points to a phishing page with images of Rachel Rays and promises of fast weight loss. We didn't analyze what happens if you actually click on links within that page, believing that at this point the lesson is learned.

What's the lesson, you ask?

Let's recap – a short Google URL, pointing to espn.go.com, exploiting an error on that website to point to another link in the Netherlands, wherein a java script points to a server in Mongolia. The hacker who put all this together had to:

- Register the 2 domains in the Netherlands and Mongolia
- Hack his way into those servers or, somehow, find a way to host a redirect link on those servers
- Put the phish pages on the final server; the page looks very legitimate and well done, so time was spent to create it
- Register the short link on Google
- Create the emails, instruct the botnet to send out the spam emails to distribute the link in the hopes that someone would click

This is a **lot** of work that took a great deal of patience. Granted, purchasing those domains, of course, was done with a stolen credit card. Of that, we have no doubt but still, it takes a fair bit of dedication and commitment to undertake this entire process simply to cloak a link so AVs can't catch it.

The reason why hackers are doing this now is because it's virtually impossible for any AV to follow this maze of URL links to the end, to reveal the phish or malware. If we tried following every link in every email, email delivery would come to a screeching halt. Instead, AV companies hunt for the final pages so that even if you do click on the initial link, they hope to block your browser from completing the chain of redirects. But, clearly, they can't keep up with the onslaught of chains of links. The final page, typically done by the hacker, took time to develop, and the chain of links is manipulated to change so many times that it becomes impossible to follow. And while the end link goes to the same page; that page may be hosted on several servers, and the paths left by the hacker to get you there will likely be millions, each different.

How, you might ask, how is Network Box protecting me from this threat?

In a case such as this, every aspect of the Network Box protection toolkit may come handy. As the email is received, we may be able to recognize the originating IP as blacklisted. If that is not yet the case, we may be able to recognize the URL as being blacklisted as well. Therefore, the email scanner, with its many engines, may pick up this email and quarantine it (in actuality, that **is** truly what happened – we picked up this email for the study from our quarantine).

It also doesn't help that the first redirect in this case was actually linked to espn.go.com, which is legitimate. It **would** be nice if sites like them would check their codes and remove such vulnerabilities. Hackers already have enough tools in their arsenal. We don't need to provide them with even more launching platforms, do we?

However, assuming none of that happens for some reason, and assuming the user clicks on the link, our web filtering and browser AV protection would analyze the content of the page and, if it contains malware, your Network Box will block the page from even loading. One caveat though; if the landing page is encrypted, this may not happen on our 3.2 platform – and this is a **VERY** important reason to encourage all of you, once more, to migrate to 5.0 and adopt HTTPS decoding, to allow the Network Box to scan encrypted content and enhance the protection of your network.

It should now be crystal clear, the critically vital multilayer protection your Network Box offers. It is not always possible to block something with only one tool, and that is why our solution is comprised of such an extensive suite of tools. The synergy between all these tools allows us to provide a much stronger, far more robust level of protection.

Undeniably, the best defense against these threats is user awareness - so educate, and keep educating, your users about these threats, explain how they work, what they do, the potential dangers they pose, and make sure they don't click. Clearly, if the user does not click, the whole argument becomes moot because the threat disappears. Because, for as much as AV companies may be striving to find those "final landing pages" and create protection against them, hackers have become increasingly savvy at cloaking them, cleverly developing these long chains of redirect.

For years, we have been recommending to our clients, the idea that security spending **must** include a large portion dedicated to educating users to think in terms of safety. To teach them what threats may look like, ensure they understand what lurks behind a link, and establish a mindset of thinking not once, not twice, but thrice (at least) before clicking on any link. Because if they do not click, the threat cannot come in. So please, think before you click!

Stay safe.

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 6th October 2015, Network Box will release our patch Tuesday set of enhancements and fixes. Due to the extensive number of enhancements made, we have increased the rollout window beyond the normal 7 days. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

Network Box 5 Features
October 2015

This month, for Network Box 5, these include:

- Improvements to Network Address Translation, related to internal services
- Enhanced admin console trace capability
- Support for PPTP protocol through generic proxy
- Improved transparent UDP support for generic proxy
- Introduction of Real Time summaries for periodic mail utilisation statistics
- Introduction of Real Time summaries for firewall utilisation statistics
- Support for SNI domain and category in web client (HTTPS) policy rules
- Support for magic file identification in web client, and associated policy rules
- Support for web client policy rule regarding non-SSL traffic over SSL ports
- Support for ECDSA in SSL proxy
- Improvements to logging and reporting of mail server deliveries
- Support configuration of SSL on mail server outbound eMail
- Addition of fine-grained control over user portal report generation
- Compatibility improvements to MIME structure of mail portal reports
- Improvements to scrolling stop/resume in transactional log reports
- Support for localised translations on CSV report export
- Increased font sizes in user and admin web portals via screens bigger than 1,850 pixels wide
- Explicit support in user and admin web portals for screen width "1250px-1849px" into "1250px-1549px" and "1550px-1849px"
- Restructuring of Web Client Activity in admin web portal
- Support for SSL termination of virtual hosts (certificate selection via SNI)
- Introduction of a facility to rename an entity
- Enhanced support for automatic IP entity learning
- Support for clustered NOC servers
- Introduce configurability for the number of mail scanning engines
- Improved support for suppressing TLS for SMTP mail where server doesn't provide TLS option
- Defer envelope scan results from HELLO and MAILFROM stages to RCPT stage (to improve logging and control)
- Performance improvements when scanning large complex emails
- Policy support added for strict enforcement of MIME structure in eMails
- Support for fine-grained engine-level controls in scanning modules framework
- Introduction of fine-grained engine-level controls in mail scanning modules
- Enhanced support for automatic discovery of embedded base64 encoded blocks in eMails
- Support for V-95, V-395, V-1000, V-2000, V-4000 and V-8000 virtual Network Box models

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

Should you need any further information on any of the above, please contact your local SOC. They will be arranging deployment and liaison.

NETWORK BOX

Network Box 3 Features October 2015

On Tuesday, 6th October 2015, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, for Network Box 3, these include:

- Enhancements to Box Office and Response web sites.
- Compatibility improvements to MIME structure of mail portal reports
- Various (mostly internal) enhancements to several internal support systems

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

Newsletter Staff	Subscription
Mark Webb-Johnson Editor	Network Box Corporation nbhq@network-box.com or via mail at:
Michael Gazeley **Nick Jones** **Kevin Hla** Production Support	**Network Box Corporation** 16th Floor, Metro Loft, 38 Kwai Hei Street, Kwai Chung, Hong Kong
Network Box HQ **Network Box UK** **Network Box USA** Contributors	Tel: +852 2736-2083 Fax: +852 2736-2778 www.network-box.com

Network Box Thailand RetailEx ASEAN 2015

Network Box Thailand exhibited at the RetailEX ASEAN 2015 expo, held at the IMPACT Exhibition & Convention Center, Bangkok. During the expo, Network Box Thailand's Director, Andrew MacGregor, gave a talk titled, 'The Vulnerability of Everything,' which highlighted the security flaws and vulnerabilities found in most web facing smart devices.

Network Box SMBWorld Awards 2015

The Network Box 5 appliance platform, has been nominated for the SMBWorld Awards 2015. This highly prestigious annual competition, relies on a dynamic selection process, involving SMBWorld readers and the members of SMBWorld's supporting organizations. The final result will be announced on the 20th November, 2015.