MAR 2015

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the March 2015 edition of In the Boxing Ring

This month, Network Box USA's co-founder and Chief Technology Officer, Pierluigi Stella, talks about the virtues of adopting an Intrusion Prevention System (IPS), in the article titled **Data Breaches: *Identify and Remediate***. Today, there are still many large-scale security vendors that still offer the 'classify and remediate' approach, where they will monitor traffic and alert customers if there is an attack. In this day and age of zero-day threats and exploits, this concept is not only out-dated but leaves you vulnerable to attacks. This issue is discussed in further detail on pages 2–3.

On pages 3–4, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5 and Network Box 3. We continue to develop, and will continue to support, Network Box 3 for the foreseeable future (several years).

Finally, Network Box is proud to announce that Network Box 5 has been named a finalist in ten categories for the 11th Annual 2015 Info Security Global Excellence Awards. In addition, Network Box has also made it to the finals of the INNOVATIONSPREIS-IT 2015, in Germany.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
March 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

Data Breaches: Identify and Remediate

by Pierluigi Stella

When I started delving into security, two of the first words I learned were **identify** and **remediate**, a phrase to mean that you'd identify a problem and fix it. That said, what does "identify a problem" mean? Typically, it'd encapsulate things such as running a vulnerability assessment (or, better yet, a true penetration test), finding all the pain points, and making a plan to fix them (remediation).

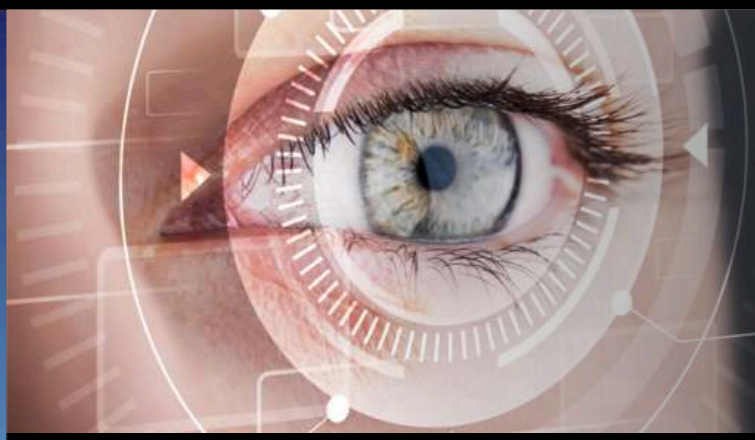
Most of the literature I've found on this topic still refers to classify and remediate in these terms. In the meantime though, I've noticed that some companies are using these terms in a very different way and making lots of strides in marketing their products with scare tactics, using big terms.

Many years ago, we used to install IDS, which would produce hundreds of pages of reports and, once each day, we'd pore over those pages to find correlations and identify possible threats. After that, we'd make configuration changes, mostly to the firewall, to block those threats.

With the passing of time, we've built tools that no longer require such human intervention, for many reasons. Aside from being inconvenient and demeaning for someone to spend his or her life poring over hundreds of pages of logs on a daily basis, it's also incredibly inefficient and easily plays into the hands of hackers. With modern hacking counting on automated tools that change the threat at a speed beyond human comprehension (let alone capability), relying on human analysis is, to say the least, obsolete (I'd venture further and call it obscene at this point).

As such, we've created tools that identify threats in true real time and block them, automatically. These are called IPS – intrusion PREVENTION systems. Prevention is key here; you want to block the attempt at intrusion as it starts. You want to change the paradigm from having a camera that gives you a picture of the thief, to a guard that blocks the thief at the doorstep. If a packet can be malicious, block it.

NETWORK BOX



Network Box Intrusion Detection and Prevention (IDP):

- Scans network traffic at the application level, and seamlessly blocks malicious behavior with zero latency
- **3 Engines:**
  Front-Line IPS, Passive/Active IDS, Inline IPS
- 16,005 Signatures
- **Active** (blocks network traffic)
  Passive (logs intrusion attempts)

An evolution of this concept consists of integrating the IPS with the firewall; allowing the firewall to do most of the work as it's faster and much more accurate. Then scan the traffic that passes through with the IPS and, if the IPS determines that a packet is a threat, tell the firewall to drop that connection, so no further threat packets can pass through from that sender. This is what many are calling the NextGen Firewalls, which, incidentally, are old news now. Network Box has had this concept since 2000; only relatively recently has the industry has caught up with it and given it a formal name.

Since this approach makes a lot of sense, you'd expect that the entire security industry would move in that direction and abandon the concept of IDS. In a way though, IDS still has merit within a LAN; it can identify malicious traffic within the LAN and provide alerts on local activity.

Enter the concept of 'classify and remediate'. I've run into this more than once lately. There are companies that make a fortune telling their customers that they'll monitor the traffic and alert them if something's trying to come in. And I've even seen such "alerts". One of them went like this "IP address *xyz* is sending a PHP exploit to your web server; please make sure your server is patched".

Seriously? That's their take on security? Please, make sure your server is patched?

I was (and still am) flabbergasted at such daring. I'm not talking about small companies who are trying to make a living creating unneeded panic. I'm talking about large security companies that instead of blocking the traffic and protecting their customers using an IPS, use an IDS to alert and ask the customer to 'remediate'. I feel as though we've gone back 15 years and found a way to market an old concept. We're using the concept of classify and remediate as a viable protection from Internet threats.

Well, I've news for all of you attempting to do this – it does NOT work, and it's the reason why so many companies are falling victim of hackers left and right. You cannot "remediate"; you need to block before the issue even starts. Having the ability to identify a threat floating inside a LAN is important. But if you truly want to be protected from Internet threats, stop thinking in terms of classify and remediate, and start thinking in terms of active protection, real time blocks, a barricade against each and every threat that the Internet is going to throw at you.

Knowing that IP *xyz* is scanning your ports is irrelevant and unnecessary. It makes for a nice graph you can present to the board of directors, but nothing more. What you really need to have is a system that will BLOCK such threats; so that IP *xyz* can knock at your door as many times as it wants; if you've configured things properly, the door will never open and those "threats" will continue to be caught, and blocked at the edge of your network, unfailingly, like only an automated system can do.

If you're still relying on human intervention for your protection because these companies have convinced you that it's the way modern security works, it's time you look around and get yourself some **REAL** security.

Pierluigi Stella
Network Box USA, CTO

With his extensive knowledge of security issues in the financial, banking, healthcare, education and hospitality and travel sectors; Pierluigi is frequently quoted by IT and security industry press, and is a sought-after writer and speaker. He has received numerous industry recognitions for notable career achievements in addition to being the recipient of excellence awards for innovative design.

NETWORK BOX

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 3rd March 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.

Network Box 5 Features
March 2015

This month, for Network Box 5, these include:

- Change default mode to anomaly scoring, in Web Application Firewall
- Support specification of source NAT selected source IP, in directed web client proxy mode
- Enhanced options for basic authentication over LDAP
- Improvements to KPI reporting, related to complex KPIs reported over long time periods
- Performance improvements to display of holistic record details in all administrative interfaces
- Support for direct download of SSL proxy certificate authority certificates, from admin portal login screen
- Enhanced support for Sender Policy Framework (SPF) enforcement in mail scanning
- Release of nbms-mail-server - an on-the-box mail server capable of store-and-forward routing
- General improvements to the administrative notification system
- New Global Monitoring System (GMS) sensor for mail scanner
- New Global Monitoring System (GMS) sensor for file scanner
- New Global Monitoring System (GMS) sensor for authentication scanner
- New Global Monitoring System (GMS) sensor for reporting subsystem
- Improved new top-level domain support during mail scanning
- improvements to logging of packet flags in IPv6 firewall blocks
- Performance improvements in quarantine mail release via slow mail servers
- Improvements to mail spam blacklisting
- Addition of 'date' header to report, and other, eMails generated by the Network Box appliance
- Support for multiple client certificate groups, in SSL VPN servers
- Change to network firewall logging, to log INVALID packets (from connection tracking) specifically as such
- Improved support for Internet Explorer 11 in HTTPS web administrative and user portals

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 ISO 9001 / ISO 20000 / ISO 27001 certified Security Operations Centre, ensures that customers' networks are protected against cyber threats, 24x7x365.

Network Box 3 Features March 2015

On Tuesday, 3rd March 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 related to signature release notification
- 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 **Michael Gazeley** **Nick Jones** **Kevin Hla** Production Support **Network Box HQ** **Network Box UK** **Network Box USA** Contributors	Network Box Corporation nbhq@network-box.com or via mail at: **Network Box Corporation** 16th Floor, Metro Loft, 38 Kwai Hei Street, Kwai Chung, Hong Kong Tel: +852 2736-2083 Fax: +852 2736-2778 www.network-box.com

Network Box USA
Silicon Valley Communications

Network Box is extremely proud to announce that Network Box 5 has been named a FINALIST in a total of TEN CATEGORIES, for the upcoming 11th Annual 2015 Info Security's Global Excellence Awards, which are being held on the 20th April, in San Francisco, USA.

LINK:
http://www.infosecurityproductsguide.com/world/

Network Box
Triple ISO Certification

Recently, Network Box's ISO/IEC certifications were renewed and upgraded to the latest standards, by ISO auditors. This highlights Network Box's continued commitment to excellence.

ISO 9001:2008
ISO/IEC 20000:2011
ISO/IEC 27001:2013

Network Box Germany
INNOVATIONSPREIS-IT 2015

Network Box has made it to the final round of, INNOVATIONSPREIS-IT 2015, of the 'innitiative mittelstand' in Germany. This is an Award for Innovative IT Solutions in the field of SME businesses. Network Box is nominated in the category IT Security. The winner will be announced during CeBit 2015, in Hannover, later this month.