In the Boxing Ring
JUL 2019

Network Box Technical News
from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the July 2019 edition of In the **Boxing Ring**

Earlier this year, when Network Box launched our **Dark Web Monitoring Service**, we concentrated on breaches leaking passwords (both hashed and plaintext/cracked), indexed by email address for both individuals as well as domain holders. However, most breaches contain much more personal data than just passwords, and we are increasingly seeing the threat of data correlation using index types other than email address, such as site usernames, IP addresses, identity numbers, etc. This month, we will be launching **version 2** of the Network Box Dark Web Monitoring Service. On pages 2 to 3, we outline the new features and enhancements to the service.

On page 4, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5.

In other news, Network Box Managing Director, Michael Gazeley, gave a talk about the Dark Web at **ISACA China HK Chapter.** In addition, Network Box USA was at **HouSecCon 2019**. During the conference, Network Box USA's Pierluigi Stella gave a keynote on why all companies need a cybersecurity budget. Finally, Network Box was featured in various media outlets including **SC Magazine** and **Dark Reading**.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
July 2019

Stay Connected

You can contact us here at Network Box 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:

https://twitter.com/networkbox
https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse
https://www.linkedin.com/company/network-box-corporation-limited/
https://www.youtube.com/user/NetworkBox

In this month's issue:

Page 2 to 3
Dark Web Monitoring version 2

Prior to the launch of version 2 of the Network Box Dark Monitoring Service later this month, on pages 2 to 3, we highlight the new enhancements.

Including:
- Data Leakage Attributes
- Data Leakage Indexes
- Volume of Data
- Providing End-Users Access to their Data

Page 4
Network Box 5 Features

The features and fixes to be released in this month's patch Tuesday for Network Box 5.

Page 5
Network Box Highlights:

- **Network Box Hong Kong**
  ISACA China HK Chapter
- **Network Box USA**
  Houston Security Conference 2019
- **Network Box Media Coverage**
  - SC Magazine
  - Dark Reading

Dark Web Monitoring version 2

The Dark Web is the deliberately hidden part of the Internet, which is the natural habitat of hackers and cyber criminals. This 'dark side', can only be accessed with specialist knowledge, and specific software tools such as TOR (The Onion Router), Riffle, Freenet, and I2P (Invisible Internet Project). Whenever there is a data breach, the stolen personal data usually ends up on the Dark Web. There are currently over 6.5 billion sets of hacked credentials already posted on the Dark Web, and the number is growing.

The Network Box Dark Web Monitoring Service scans data breaches from the Dark Web, looking for your registered email addresses and domains. The generated report shows the breach details. As a subscriptions service, monitoring is ongoing. As new data breaches are discovered, Network Box will re-scan and keep you informed as to changes since the last report.

When Network Box launched our Dark Web Monitoring Service, we concentrated on breaches leaking passwords (both hashed and plaintext/cracked), indexed by email address for both individuals as well as domain holders. However, most breaches contain much more personal data than just passwords, and we are increasingly seeing the threat of data correlation using index types other than email address, such as site usernames, IP addresses, identity numbers, etc.

This month sees the launch of version 2 of the Network Box Dark Web Monitoring Service, and this article outlines the new features.

Data Leakage Attributes

The first major change introduced in v2 is that rather than merely storing breached passwords (hashed and plaintext/cracked), we now store many different types (attributes) of leaked data. This is dynamic, and we can add new attributes as we find them, but the list currently includes:

- General textual information
- Plaintext/cracked passwords
- Hashed passwords (either hash, or seed:hash format)
- Physical addresses
- US Social Security Numbers
- Credit card numbers
- First names
- Last names
- Unformatted names (format not known)
- Email addresses
- Last name, First names
- User IDs (number, usually internal)
- User identifiers (name, usually used for login)
- Country codes
- Genders
- IPv4 addresses
- IPv6 addresses
- Dates of birth
- URLs

As a result of this new arrangement of database storage, the formats of the dark web monitoring reports have changed; we now show this in a dynamic "attribute: count" format.

Data Leakage Indexes

We search the dark web for breached / leaked data, and can now index it in different ways. In addition to the v1 index on email address, for example we can now index on site usernames, IP addresses, identity numbers, and other such attributes. This allows us to now correlate data between breaches (in particular for those breaches that do not include email addresses).

Volume of Data

To give you some idea of volume, in the past month alone we've found 77 new breaches, adding close to half a terabyte of breached data to our existing database. Today we store data from 13,574 breaches, and that number continues to grow.

Providing End-Users Access to their Data

As a matter of policy and to protect the sensitivity and security of this data, Network Box does not provide breached personal data to anyone except for the authenticated and confirmed end-users at the breached email address, as well as authorized Network Box staff. IT managers, in particular, do not have access to this data.

We are now finalizing a facility to provide end-users direct access to their data. This will be a public website into which an end user email address is entered:

- If the email address, or its domain, is subscribed to the Dark Web Monitoring Service, a report will be emailed directly to the end user, detailing all the information on that user that we have found to be breached and leaked.
- Without a subscription, a short summary report will be emailed directly to the end user. This does not contain the breached information itself - merely an indication of the amount and type of breached data discovered.

We anticipate being able to launch this facility during July 2019.

Quite apart from the direct threats offered by breached leaked personal data, administrators can consider using this as an opportunity for end-user education concerning such phishing activity (and general Internet trust) - not just for these users, but also other high level and high risk staff. Users should be encouraged NOT to use their work email address for non-work related websites (it is estimated that about 30% of people, reuse the passwords on multiple sites). It would be prudent to force a password reset on internal systems for breached accounts.

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 2nd July 2019, 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 14 days.

Network Box 5 Features
July 2019

This month, for Network Box 5, these include:

- Support for S-80i box model
- Support for Telit LTE modem modules
- Performance and reliability improvements for NBSIEM logging
- Enhancements and improvements in IPSEC stack (in particular for IKE v2)
- Fixes to admin portal display of activity overview by entity
- Enhancement to generic proxy holistic log to record port usage
- Enhancements to firewall event log display in admin portal
- Introduction of new string comparison operators (notcontains, nostartswith, and notendswith)
- Introduction of support for ECDSA SSL certificate offload
- Improved logging of summary message for bypassed SSL traffic
- Improvements to WAF signature reload mechanism
- Introduction of a rescan command for quarantined emails

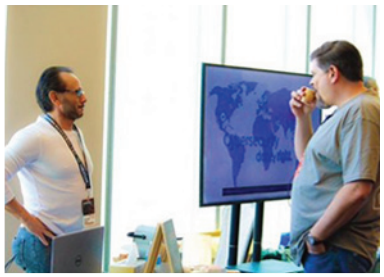
In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

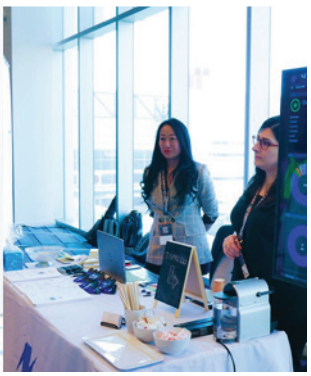
Should you need any further information on any of the above, please contact your local SOC. They will be arranging deployment and liaison.

Network Box HIGHLIGHTS

Network Box USA
HouSecCon 2019

Network Box USA was at this year's Houston Security Conference (**HouSecCon 2019**), which was held at the Marriott Marquis Houston. During the event, Network Box USA's CTO, Pierluigi Stella, gave a keynote titled, "Making A Case For Having a Cybersecurity Budget."



Network Box Hong Kong
ISACA China HK Chapter

Network Box Managing Director, Michael Gazeley, gave a Continuing Professional Development Seminar titled, "The Dark Web: The Dark Side of the Internet." Many aspects of the Dark Web were covered, including Advanced Identity Theft, Augmented Blackmail, Email Hoaxes, Criminal Big Data, and Dark Web Monitoring.



Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Kevin Hla
Production Support

Network Box HQ
Network Box USA
Contributors

Subscription

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 Media Coveage

SC Magazine
GandCrab ransomware operators put in retirement papers
LINK: https://bit.ly/31XBAfQ

Dark Reading
Federal Photos Filched in Contractor Breach
LINK: https://ubm.io/2IU1w4l