In the Boxing Ring
NOV 2019

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

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

This month we are talking about **Sextortion Scams**. Earlier this year, Network Box Security Response started to see an increase in the volume of these particular types of spam emails. Judging by the large volume of these, and the lack of any decrease in numbers as the months go by, it seems to be an effective email scam campaign. Unfortunately, we don't see this approach stopping anytime soon - it is just too successful. We discuss this issue in greater detail on pages 2 to 3, and highlight how you can avoid being a victim of these types of threats.

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 is extremely proud to announce that the company won two **BizIT Excellence Awards** for outstanding achievement in the categories of Unified Threat Management and Managed Security Services. Additionally, Network Box Singapore has been appointed as a **Pre-Approved SMEs Go Digital Vendor** by the IMDA. Registered businesses operating in Singapore may now be entitled to receive up to 70% in subsidies if they subscribe to any Network Box UTM+ service package. Finally, Network Box's Managing Director, Michael Gazeley was interviewed by the Harbour Times; and other security news is highlighted in this month's **Security Headlines**.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
November 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:

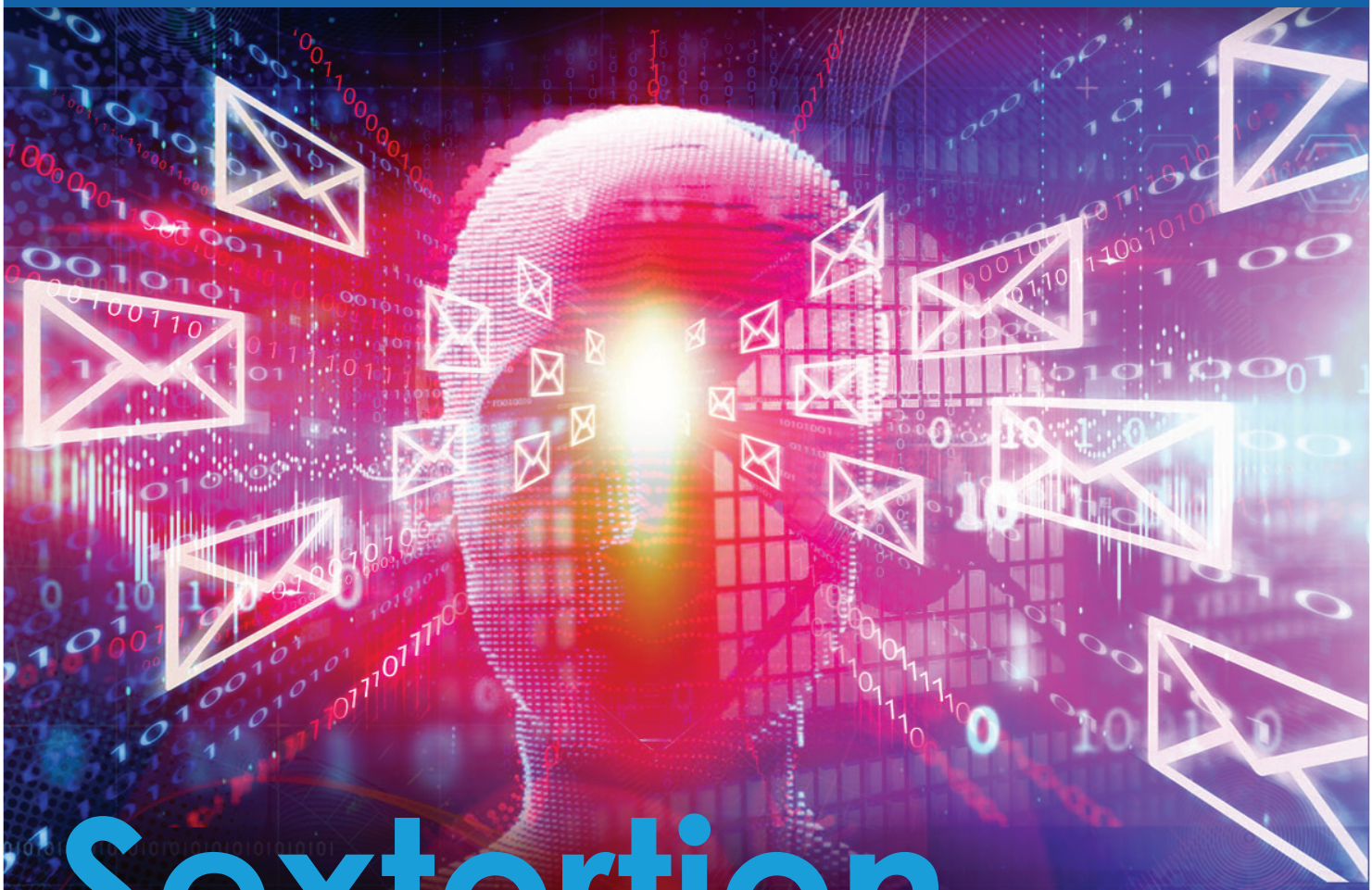
https://twitter.com/networkbox

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:



Sextortion Scams

Hackers and cyber criminals know your passwords

Earlier this year, Network Box Security Response started to see an increase in volume of a particularly nasty type of spam email. These are all part of an effective email scam campaign.

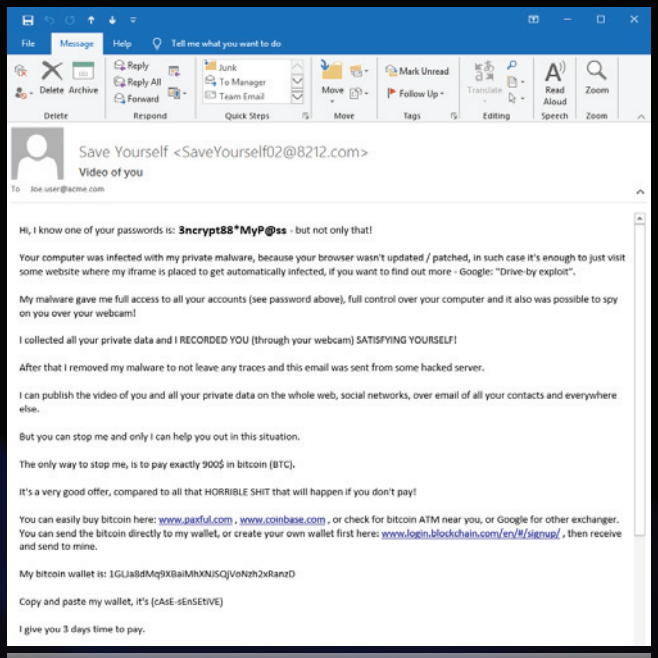
Over the years there have been many variants, but the ones in recent months have all utilised one of more of the following attributes:

- Provide the recipient's password, as proof of 'hacking' the recipient's computer.
- Demand payment in BITCOIN, or some other crypto currency.
- Claim to have hacked the recipient's webcam, and to have recorded adult footage, pornography, or other such embarrassing details.
- Claim to have installed malware on the recipient's computer, or some website visited.
- Use mixed case letters, or international character sets, to disguise the text.
- Spoofed the sensor as the recipient themselves.
- Random sender addresses, and no URLs provided.

Judging by the volume of these, and the lack of any decrease in numbers as the months go by, it seems to be an effective campaign. Analysis of crypto currency addresses show the scams to be pulling in thousands of dollars for each address used. Many in the industry are labelling these 'sextortion scams'.

The Password (and other personal details)

It is undoubtedly the inclusion of the password in the email, as proof of the successful hacking of the recipient's computer, that is the most concerning. This raises the credibility of the scam - couple that with the spoofed sender and many will be convinced it is real. It is sad to hear the most common question from recipients is not ***'is this a scam?'***, but instead ***'how do I buy bitcoin to pay off this guy?'***. The most amusing response we have heard is '***I can't afford it, I am just a student; will they give educational discounts?'***.



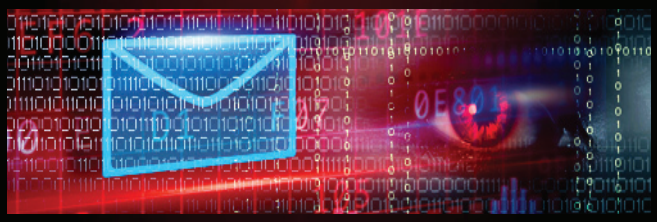
So how did the 'hacker' get the recipient's password?
The answer, of course, is data breaches on the Dark Web. These breaches contain email addresses, de-hashed (now plaintext) passwords, and a host of other personal information (including dates of birth, full names, addresses, countries of residence, etc). The 'hacker' is merely using that information as his database of who to mail, and what details to provide.

We recommend that you educate your users about this threat. You can also subscribe to the Network Box Dark Web Monitoring service to pro-actively inform your users of the issue. We even have a portal (***https://darkweb.network-box.com/***), that subscribed users can visit and enter their email address, to receive an individual report showing all the breached information we have discovered on them.

Spoofed Sender

It is trivial to spoof sender addresses with SMTP email, and hard to defend against. In particular, the 'from' header sender address is often not protected at all (and that is the address shown to the recipient in his email client).

We continue to see customers requesting to whitelist their own domain, and we continue to recommend against that. We also continue to see this in policies of customers that migrate to Network Box protection services. Gmail's use of sender address to decide whether an email was 'sent' or 'received' continues to be a problem. Typically, 1% to 2% of spam on the Internet nowadays uses the sender spoofed as the recipient's domain (either the recipient themselves, or somebody else in the same domain). We recommend that you consider the use of policy controls such as DKIM and SPF to limit the impact of sender spoofing, and never whitelist your own addresses / domains.



Crypto Currencies and Bitcoin

We continue to see crypto currencies (and bitcoin in particular) used in these and other scams. Again, you can educate your users that whenever they see an email demanding BITCOIN, or other crypto currency, it is most likely a scam and they should report to their IT support for assistance.

The Future

We don't see this approach stopping anytime soon - it is just too successful. Of particular concern to us is that many data breaches contain far more information than simply passwords. For example, the recent Malindo / Lion Air breach includes passport numbers, identity numbers, and a host of other very private and hard to change information. But more importantly, it includes relationships between travellers travelling together; and that opens the door to spoofing of email addresses from people you have a relationship with, for example; only adding to the credibility of the scam.

So, take care, and please continue to be distrustful of anything coming in from the Internet. The bad guys may know your password, but NO - you most likely were not hacked!

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 5th November 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
November 2019

This month, for Network Box 5, these include:

- New GMS sensor "AGENT" (to monitor the GMS system on the box itself)
- Change to GMS reporting protocol (including host and port)
- Add support for multiple configurable GMS servers
- Performance improvement for sender correlation in web portals display of email record
- Support configuration option for sender correlation in web portals
- Add Mail Top Threats (total, incoming, and outgoing) KPIs to default reporting template
- Enhancements to application identification (including support for 500+ new applications)
- Enhanced support for configurability of test points for GMS DNS client sensor
- Performance improvements to signature download (PUSH) system
- Minor housekeeping release of Kaspersky scanning engine update

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 Singapore
SMEs GO DIGITAL Pre-Approved Vendor

Network Box Singapore has been appointed as a **Pre-Approved SMEs Go Digital Vendor** by the Singapore Info-communications Media Development Authority (IMDA). Thus, if you are a registered business operating in Singapore and subscribe to any Network Box UTM+ service package, you may be entitled to receive up to 70% in subsidies from the Productivity Solutions Grant (PSG).

For more details on how to apply for the grant:
https://www.businessgrants.gov.sg



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:

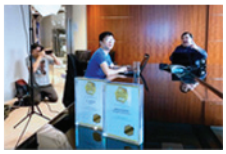
Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong

Tel: +852 2736-2083
Fax: +852 2736-2778

www.network-box.com

BizIT Excellence Awards 2019
Outstanding Performance

Network Box is pleased to announce that the company won two **BizIT Excellence Awards** for outstanding performance, in the categories of ***Unified Threat Management*** and ***Managed Security Services***. Network Box's UTM+ has been significantly augmented with cloud-based NBSIEM+ (Network Box Security Incident and Event Management Plus) technologies this year, while Network Box's Managed Security Services have been notably strengthened by enhanced Dark Web Monitoring capabilities.

Securirty Headlines

Harbour Times
Cybersecurity not a priority in Hong Kong – but it should be
LINK: https://bit.ly/2qiMVIW

SC Magazine
Adobe leaves Creative Cloud database open, 7.5 million users exposed
LINK: https://bit.ly/339WCIe

CPO Magazine
DDoS Attack on Amazon Web Services Raises Cloud Safety Concerns
LINK: https://bit.ly/36xxai4