JUL 2018

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson

Chief Technology Officer, Network Box

Welcome to the July 2018 edition of In the Boxing Ring

This month, we take a break from our usual talks about attacks that Network Box can defend against, and talk about another attack vector that does not even pass through your Network Box device, but can nevertheless be devastating in its impact: **Social Engineering**. This is an attack vector that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures. On pages 2 to 3 we discuss this in greater detail, and outline how you can protect yourself from these types of attacks.

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

Finally, Network Box Managing Director, Michael Gazeley, gave a cyber security seminar on behalf of the **ISACA** China Hong Kong Chapter. In addition, Network Box USA's CTO, Pierluigi Stella, and Network Box Germany's Managing Director, Dariush Ansari, were featured in **SC Magazine** Media and **NetzPalaver**, respectively. Furthermore, we are proud to announce that as of June 2018, **Network Box Focus** will also available in video format. Please follow the links provided to subscribe, and stay updated with the latest Network Box news.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
July 2018

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

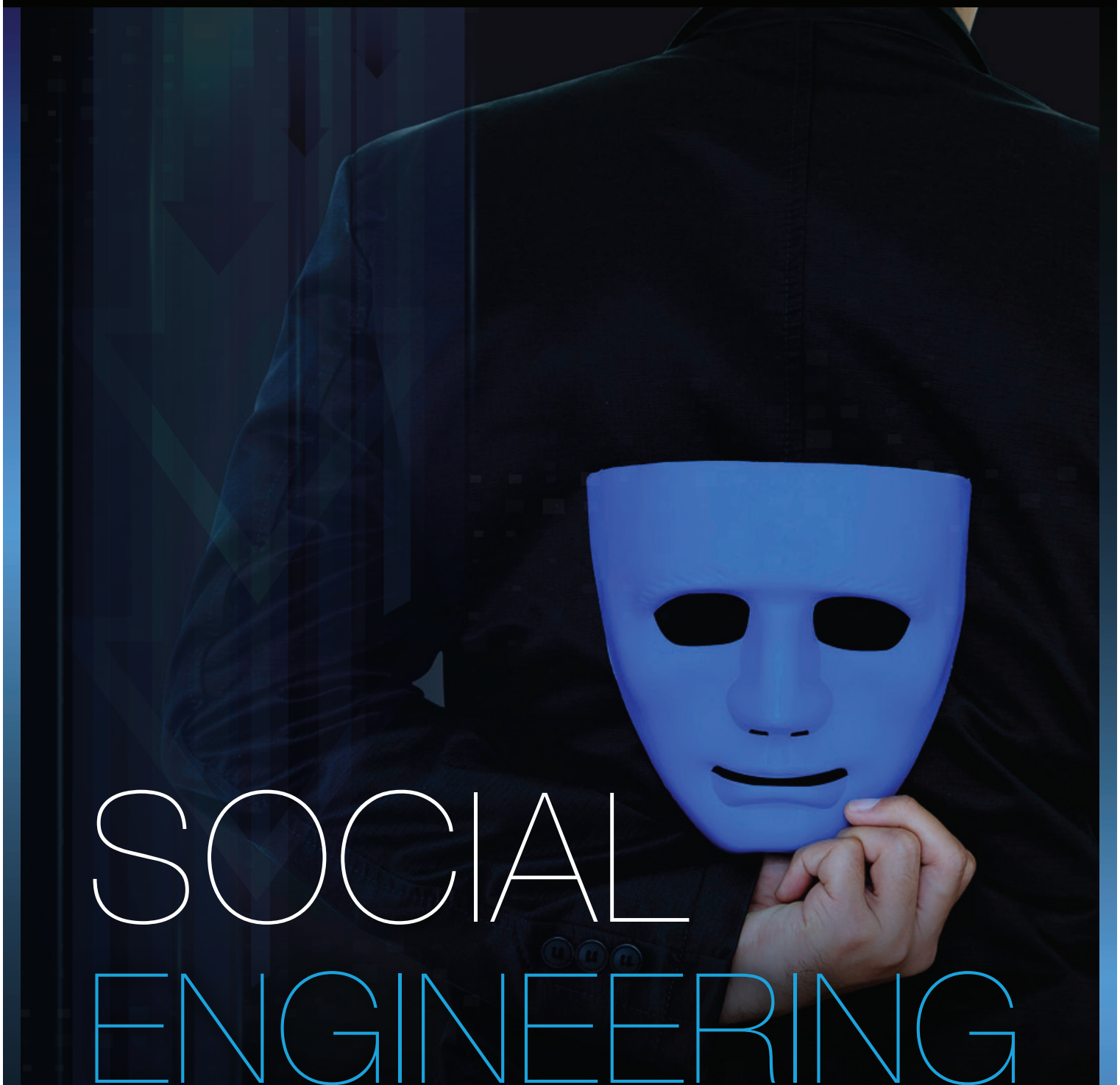
https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse

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

https://plus.google.com/u/0/107446804085109324633

In this month's issue:

NETWORK BOX



SOCIAL ENGINEERING

Each month, in these *In The Boxing Ring* articles, we usually talk about attacks that can be defended against by Network Box devices and services. This month, we'd like to take a break from that and instead talk about another attack vector. One that often doesn't even pass through the box, but that can nevertheless be devastating in its impact.

Social Engineering (in the context of information security, at least) is an attack vector that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations, or for financial gain. Such attacks can be initiated either in person, via postal mail, via telephone calls, via email, or other such mechanisms.

So how can you defend yourself against these sorts of attacks?

As a start, we have five specific recommendations:

1. Educate

Your staff has to care about information security, and be aware that social engineering attacks are real. Train them how to right-click on an email sender name to show the hidden email address. Train them to verify the address when replying to emails. Train them to be suspicious, and to report suspicious activity, and verify if at all uncertain. Above all, train them to be skeptical of any and all interactions and data requests or instructions.

2. Test

Don't simply rely on the training, but actively and regularly engage in penetration testing social engineering exercises. Send in spoofed emails and try to solicit a response. Call and try to get information you shouldn't have access to. If a problem is found, do not address it with a culture of blame, but rather go back to point #1 and re-train again and again until they get it right. If you don't have the expertise in-house to do education and/or testing, then consider engaging a professional penetration tester to help.

3. Limit

It is common to have an 'Our Team' page on your public website, complete with names, bios, and contact details; but consider how that information could be used in social engineering. When your staff speaks at public events, consider what is in their published bios, contact points, and information revealed in the talk itself. Limiting the public disclosure of information (particularly regarding personnel, roles, and responsibilities) makes a social engineer's job significantly harder. Be aware that even if you limit what information you release, your customers may not do the same (and as such, customer information may be available to social engineers).

4. Verify

Institute callback and other such verification procedures. Instill a culture of, and procedural guidelines for, verification. If someone calls in with an instruction / request, have your staff call back to confirm (with the callback being on the registered number / email address of the requestor). Names, email addresses and telephone numbers are all trivially spoofed/forged, and callbacks help detect such issues. Consider the use of pre-arranged challenge/response questions. Dual Factor mechanisms can also be used to verify.

5. Visitors

Implement physical security for visitors. People already in your office are often trusted more than external callers, even though they may be visitors (and that includes contractors and temporary on-site workers). Consider instituting procedures to log all visitors, require a staff sign-off, and make dated visitor badges and escorts mandatory. Verify the identity of all visitors, at the point they are registered.

Implementing these five recommendations will go a long way towards improving your security posture, and defending against social engineering attacks.

NETWORK BOX

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 3rd July 2018, 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 2018

This month, for Network Box 5, these include:

- System security ACL updates to reflect new Network Box Security Response infrastructure arrangements
- New HTTP ACL types now available in Admin Web Portal
- Improvements to DKIM signing and verification
- Performance improvements in Global Monitoring System
- Various miscellaneous improvements to Admin and User Web Portals

In addition, the following functionality is being released as an open BETA release to regional Security Operations Centres:

- Fine-grained security policy support for SSL certificate checking
- Improved caching of SSL CRLs and intermediate CA certificates
- POP3: Support optional client and server keepalive messages during scanning
- POP3: STLS support (in addition to existing pop3s protocol support)
- IMAP4: Support optional client and server keepalive messages during scanning
- IMAP4: STARTTLS support (in addition to existing POP3s protocol support)

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 Hong Kong
ISACA Cyber Security Seminar

Network Box Managing Director, Michael Gazeley, gave a seminar entitled, '**10 Cyber Security Facts *(that you need to know)***,' on behalf of the ISACA China Hong Kong Chapter. The seminar covered everything from Advanced Persistent Threats, to cyber-security inside Hotels, to PCI-DSS v3.2 compliance, to protecting yourself in the age of Smart Devices.

ISACA (Information Systems Audit and Control Association) is an independent, nonprofit, global association that engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems.

Newsletter Staff	Subscription
Mark Webb-Johnson Editor **Michael Gazeley** **Kevin Hla** Production Support **Network Box HQ** **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
SC Magazine Article

Network Box USA's Chief Technology Officer, Pierluigi Stella, had an article on Two-Factor Authentication published in **SC Magazine's** media outlet.

LINK: https://www.scmagazine.com/two-factor-authentication-is-hackable-so-what-everything-is/article/765571/

Network Box *Focus*

As of June 2018, Network Box *Focus*, will be provided on video format. To keep up-to-date with the latest news, please click '*Subscribe*' from the link below.

LINK: https://youtu.be/YQZqDZKq_iM

Network Box Germany
NetzPalaver Interview

Network Box Germany's Managing Director, Dariush Ansari, was interviewed by **NetzPalaver** to talk about how MSSPs solve resource problems for IT departments.

LINK: https://netzpalaver.de/2018/06/15/koelner-mssp-entlastet-kmus-beim-eu-datenschutz/