In the Boxing Ring AUG 2024

Network Box Technical News

from Mark Webb-Johnson

Chief Technology Officer, Network Box

Welcome to the August 2024 edition of In the **Boxing Ring**

This month, in the first of a series of articles covering the four key components that will form Network Box's approach to security for the rest of 2024 and beyond, we present the latest major version of our base platform operating system, **NBRS-8**. On pages 2 to 3, we outline some of the platform's key features.

Also this month, Network Box Red Team Managing Consultant - Richard Stagg, shares his view on the recent **CrowdStrike** incident, which affected innumerable systems worldwide.

On page 7, we highlight the enhancements and fixes for Network Box 5 and our cloud services that will be released in this quarter's Patch Tuesday.

In other news, Network Box Hong Kong was at the **Business GoVirtual Expo & Conference**, which took place at the HK Convention and Exhibition Centre. During the event, Network Box was presented with a **Business GoVirtual Tech Award**. Also at the event, Network Box Managing Director Michael Gazeley participated in a cybersecurity panel discussion. Finally, Network Box was interviewed by **CDO Trends** to share our insights about the *CrowdStrike* issue.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
August 2024

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 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:

NBRS

This month, in the first of a series of articles covering the four key components that will form Network Box's approach to security for the rest of 2024 and beyond, we present NBRS-8 - the latest major version of our base platform operating system.

Yearly Cycles vs. Iterative Updates

Unlike many in our industry, Network Box has never believed that the major yearly release cycle approach is suitable for Internet security. Instead, we incrementally update our products - regularly adding protection and functionality in response to the evolving threat landscape. For example, our current base platform, Network Box 5 (NBRS-5), has had more than 100 incremental firmware updates since launch, totaling more than 2,000 package updates. Furthermore, the platform has been regularly updated with hundreds of thousands of PUSH signature updates. While yearly major update cycles and Patch Tuesdays typically require reboots and intrusive network downtime, the incremental approach employed by Network Box minimizes interruption to protection services.

However, at some point, a major platform update becomes necessary. Changes to the types of threats seen, support for new types of hardware technology, or simply foundational changes requiring database migration make such platform updates inevitable. Hence, Network Box is proud to announce NBRS-8, the next iteration of our award-winning managed security platform.

NBRS-8

The goals of the NBRS-8 project are to add support for the latest hardware technologies, to run under the latest physical and virtualized environments, to support the latest protocols, to enhance our base platform toolset, and to do all this while maintaining compatibility with NBRS-5. While we cannot cover every one of the dozens of new features, we can outline some of the more important ones →

- NBRS-8 provides support for the latest networking hardware, including crypto acceleration, network acceleration, and new ethernet networking speeds (2.5G, 25G, etc). For cellular networks, the latest 5G modems, and for WIFI, the latest high-speed protocols and protection standards.
- The platform provides over 10,000 software packages on an LTS (Long Term Support) basis. All these are provided from our repositories, and we've upgraded our SSL encryption and digital signing suites for the highest level of security assurance.
- We've added support for TLS 1.3 and SSH 8.x, along with all their associated improvements (such as post-quantum cryptography, as well as the latest hashes and cipher suites). As before, this is integrated with our PCI DSS 4.0 compliant SOC services.
- The NBRS-8 platform further extends the foundation laid by NBRS-5 towards a hybrid on-premises, cloud virtual, and multi-tenanted future. To comply with geographic restriction standards such as the General Data Protection Regulation (GDPR), data can be stored on the box, in the cloud, or with a hybrid combination - while using the user and admin cloud portals to provide global access (from desktops, laptops, mobile tablets or phones).
- Support for on-premise or cloud event log collection, concentration, and a rules-based engine, integrated with NBSIEM+, NBRS-8 adds support for extending protection and policy control all the way to the endpoint devices.
- We've taken backward compatibility to the level where it is possible to have a High Availability set (or cluster) made up of NBRS-5 and NBRS-8 devices working together. Both NBRS-5 and NBRS-8 can be managed from the same security platform, and standard configurations are compatible and interchangeable.

Scheduled for release before the end of this year (2024), NBRS-8 will add support for the latest hardware, run under the latest physical and virtualized environments, support the latest protocols, enhance our base platform toolset, and do all this while maintaining compatibility with NBRS-5. More detailed information (including upgrade options and availability) will be made available closer to the global launch.

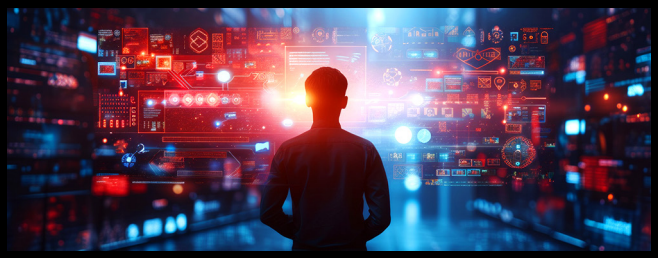
STRIKE ONE: CrowdStrike Friday in Retrospect

by Richard Stagg
Managing Consultant
Network Box Red Team

It has been a couple of weeks since the CrowdStrike incident – although people quickly stopped referring to it as an "incident"; that word isn't big enough for what transpired, and the label "Fiasco" has become immovably attached to the CrowdStrike brand now. But things move on. Fencing and McGriddles have taken over the headlines. Class-action lawsuits are starting to gain momentum. Is there still much to say about CrowdStrike?

I think: **yes**. Since the dawn of the epoch, many (including this consultant) have said that sooner or later, having an IT monoculture would lead to a catastrophic failure on an epic scale. But far from seeing the CrowdStrike meltdown as a prediction that came true, I see it as a lucky escape and a terrifying near-miss; as an early warning from which much could be learnt (but probably won't, of course). It could have been so much worse. One day, it will be.

This particular incident, while no fun for people trapped in airports or staff in IT departments (who must have been *cursing* CrowdStrike's rejection of the old maxim that you never update on a Friday), was limited in scope because it was just a silly, careless mistake, apparently void of all malicious intent. Even though the process to remediate the problem was onerous, it was not difficult: boot in safe mode, delete a file, and you're good to go. Recovery was quick.



Now re-imagine this as a nation-state pulling off a supply-chain attack against CrowdStrike (or any other third-party that has achieved a ubiquitous presence on Windows servers and workstations; there are a few). The timing would need to be aligned with a major event (a major holiday? a presidential election?), the impact would need to be far more destructive (perhaps delete, corrupt, or encrypt important files, so the recovery is non-trivial), and the resulting chaos in transport, retail, healthcare, government, banking, energy and water utilities, law enforcement, technology itself… well, it would be apocalyptic.

The eventful CrowdStrike Friday proved that nobody has a business continuity plan that includes this scenario. (Actually, that isn't true; the organisations who did have such a plan were unnoticeable, as is right and proper, because they kept running.) It also identified, for all to see, who is currently using CrowdStrike (and who isn't).

At a technical level, it demonstrated that using security tools that hook into the Windows kernel can be a pretty terrible idea. Microsoft's protestations that it's all the EU's fault and that they would never have done it otherwise are disingenuous. There *are* good technical reasons for enabling a third-party vendor to drop unsigned and arbitrary code into the kernel: as malware gets more sophisticated and stealthy, being closer to the kernel makes it easier to detect. It's also harder for attackers (or clueless staff members) to disable the protection if it's hooked into the kernel. Even so, the closer you are to the nerve centre, the greater the potential for total disruption (early adopters of Neuralink, take note), so there is a trade-off here, and security applications which stay safely in user-space are not without their benefits.

We also learned that CrowdStrike's QA procedures are terrifyingly cavalier, and that they don't roll out updates in phases with caution but toss them out to all the world in one giant batch. The flaw was not a hard-to-detect edge case. It bricked every computer it touched. The most bewildering part of the whole affair was that CrowdStrike's processes let this happen at all. It will be an interesting lesson to see how the limitation-of-liability clause in their EULA stands up to the legal onslaught.

Thinking more broadly, the incident reminded us that there is an unsolvable dilemma in all these third-party security tools: in the event of a cataclysm, do we want them to fail open (exposing systems to other attacks, which might have been the bad guys' plan all along) or fail closed (rendering the world's IT unavailable for the duration)? I guess what we really want is for them not to fail at all.

CrowdStrike's drama was also bad for information security evangelism in general: companies who did not have endpoint protection, who had been slack and left the matter to fate, were rewarded: their systems did not crash. Companies who planned and invested in best-of-breed XDR were thoroughly spanked. It just got a tiny bit harder for information security professionals to sing the praises of defence-in-depth if each layer of that defence adds new failure modes.

Such single-point-of-failure scenarios are endemic and extend well beyond XDR. A threat actor inside Microsoft could stop the world. Updates to critical infrastructure on which so much depends, like Cisco firmware or Fortinet patches, are pushed over the Internet and are potentially vulnerable to supply-chain attacks. So many things now run on AWS or Google that a broad collapse of any of the major cloud platforms could bring the world to a screeching halt. ("That can't happen", they say. "We have redundant this and fail-safe that and etc etc", they say. Excuse my scepticism, but we have all heard this before.) These are occurrences which are too big for us to control, so we push them aside as "out of our hands", as if force majeure, and ignore them while focusing on the easier-to-conceptualise problems in BCP at a manageable scale (a typhoon, a power cut).

CrowdStrike showed us that BCP needs to encompass some very uncomfortable scenarios to be effective these days, because so much of our critical technology is out of our hands. And until our technology ecosystem manages to become a little less homogeneous, we should brace ourselves and think of ways to plan for and respond to the next across-the-board outage.

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 8th August 2024, 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
August 2024

This quarter, for Network Box 5, these include:

- Support for NBRS-8 SSH key types (improving management of NBRS-5 and NBRS-8 devices)
- Reliability improvements in GMS health checks
- Improved translations in Admin Portal
- Extend security module license keys
- Update IP address lists for some regional SOCs

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

CISO & Digital & Trends (CDO Trends): The Day the Kernel Panicked: How a Tiny Update Broke the Internet (and Everything Else)

In light of the recent ***CrowdStrike*** flawed kernel driver update, which affected a legion of systems worldwide, Network Box Managing Director Michael Gazeley was interviewed by **CDO Trends** to share his insights.

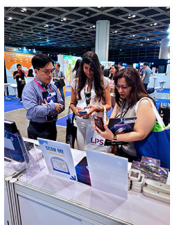
> *"From a business perspective, it is astonishing that one company was allowed to cause such a massive global IT outage. From a technical standpoint, this was possible because a kernel driver was used, which carries a risk of causing a major issue, such as the infamous BSOD (Blue Screen Of Death) seen everywhere..."*

LINK: https://www.cdotrends.com/story/4115/day-kernel-panicked-how-tiny-update-broke-internet-and-everything-else

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

Network Box Hong Kong Business GoVirtual Expo & Conference 2024

Network Box Hong Kong exhibited at the **Business GoVirtual Expo & Conference**, which took place at the HK Convention and Exhibition Centre. Several thousand visitors from across the globe attended the event, featuring AI, FinTech, MarTech, Sustainability, Retail Tech, Cybersecurity, e-commerce, and Art Tech.



Cybersecurity Panel Discussion

Network Box Managing Director Michael Gazeley, participated in a panel discussion titled, **Can AI Overtake Cybersecurity?**

Business GoVirtual Tech Awards 2024

Network Box was presented with the EXCELLENCE AWARD in **Tech Company of the Year — *Innovation Technology Application***.