THE MONITOR

JUNE 2019

ISSUE 12

A DIGITAL NEWSLETTER BROUGHT
TO YOU BY NETWORK BOX USA, LLC

Welcome to The Monitor, a bi-monthly newsletter containing cybersecurity news and information.

It's been a while since our last installment and quite a bit has changed since then.

New look.
New content.
New direction.

One thing, however, remains the same, and that is our commitment to you.

To support and protect your network, and work towards achieving your cybersecurity goals. Always.

We hope you enjoy this June 2019 edition of The Monitor.

THE DESK

A NOTE FROM SHEELA GOH, EDITOR-IN-CHIEF

Comments? Feedback? Suggestions?

Email pr@networkboxusa.com

MAKING THE CASE FOR HAVING A CYBERSECURITY BUDGET

BY PIERLUIGI STELLA

While 15 years ago security was perceived as a nuisance (*a necessary evil even*), this view has evolved and today, security is a key business unit, right alongside marketing and sales. Today, we know that without security, companies cannot even exist.

And yet, objections remain, most frequently raised when we're discussing budgets with C-suite executive. I'd say the most common one would be something along the lines of, "*Why do you even need money if nothing has ever happened?*".

We need to change our own mindset and stop viewing security as an expense. We aren't a cost center. In a way, we're a form of insurance, but don't start the conversation in that manner because insurance is still a cost and it doesn't produce revenue.

Showing the Total Cost of Ownership (TCO) isn't good either, for 2 reasons.

Firstly, we're still talking costs, an approach already determined as being less than positive.

Secondly, in order for the actual TCO of a security solution to be properly evaluated, it must include "*your*" time.

If you don't factor that in, your CEO will.

When he does, you yourself have just become a cost. And costs always need to be reduced.

The language CEOs understand is one of ROI and profitability. And that's where our conversation needs to go.

MAKING THE CASE FOR HAVING A CYBERSECURITY BUDGET

BY PIERLUIGI STELLA

Of course, if you don't get attacked, you don’t incur the costs of an attack. Now the burden is on us to determine how much a security incident could cost the company.

For starters, 60% of small businesses that suffer a cyber-attack go out of business within 6 months. Now, THAT’s a cost!

There's actually a formula to calculate the return on security investments, as proposed by the SANS institute:-

ROSI = (ALE x Mitigation Ratio – Cost of solution)/ Cost of solution

I'll be explaining this in detail on our blog soon so keep an eye out for that.

So I ask you, what is the cost of poor security?

That depends a lot on your company and your industry.

You’ll need to consider time spent diagnosing; the time your employees spend idling because they don’t have a computer to work; loss of productivity; and cost of IT personnel to fix the issues and improve security so the incident doesn’t reoccur.

There's also the cost of new security solutions; cost of forensics analysis, specially if required by law; and let's not forget loss of image, which can often be incalculable.

MAKING THE CASE FOR HAVING A CYBERSECURITY BUDGET

BY PIERLUIGI STELLA

Cybersecurity may seem like a cost; but an attack is irrefutably a cost, and it can be a large one. Large enough to put you out of business.

Proper cybersecurity delivers ROI in the form of cost avoidance; and the avoided cost, albeit estimated, can be truly very high.

Another way of demonstrating how security contributes to the profitability of a company, and that it adds to revenue, is by understanding that in this day and age, it's impossible to do business without proper security.

Being able to show your business partners and clients that you take cybersecurity seriously has become a true business advantage.

Companies have learned to do due diligence on their vendors and partners; checking also on the strength of security postures.

Security is no longer something done grudgingly. Today, security is an important, integral part of every sound company wanting to stay in business for the long haul.

To conclude, let’s all stop thinking of ourselves as a cost center and some kind of necessary evil.

Let’s consider that cybersecurity is now a profit center, a vital business unit without which a company might not even exist.

So, no, you are NOT a nuisance.

You’re a fundamental part of the business.

606,000 SIGNATURES PUSHED OUT TO ALL CLIENT SOLUTIONS IN THE PAST 90 DAYS, WITHIN 45 SECONDS OF AVAILABILITY

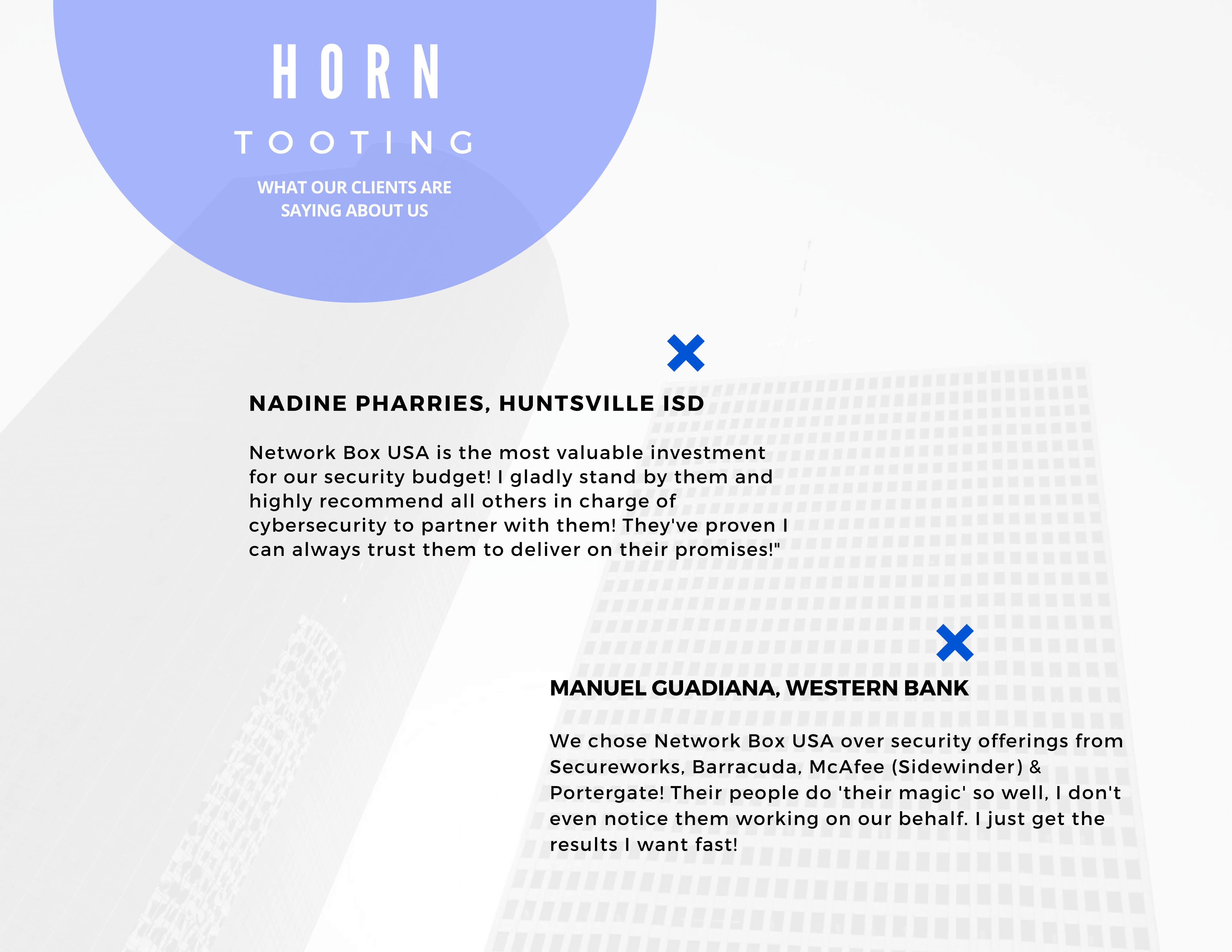
1.5M ANTI-MALWARE AND 544 ANTI-SPAM FINGERPRINTS CURRENTLY RUNNING ON OUR AWARD-WINNING Z-SCAN REAL-TIME ZERO-DAY ANTI-MALWARE ENGINE

CYBER WARFARE

WHAT WE'RE DOING BEHIND THE SCENES TO PROTECT YOUR NETWORK & KEEP IT SECURE

IT'S IMPERATIVE THAT YOUR CYBERSECURITY SOLUTIONS ARE UPDATED WITH THE LATEST THREAT PROTECTION

IMPRESSIVE SPAM DETECTION RATE OF 99.28 PERCENT



HORN

TOOTING

WHAT OUR CLIENTS ARE
SAYING ABOUT US

NADINE PHARRIES, HUNTSVILLE ISD

Network Box USA is the most valuable investment for our security budget! I gladly stand by them and highly recommend all others in charge of cybersecurity to partner with them! They've proven I can always trust them to deliver on their promises!"

MANUEL GUADIANA, WESTERN BANK

We chose Network Box USA over security offerings from Secureworks, Barracuda, McAfee (Sidewinder) & Portergate! Their people do 'their magic' so well, I don't even notice them working on our behalf. I just get the results I want fast!

CREATING A SECURITY SUB-CULTURE

TO CHANGE THE CORPORATE CULTURE

BY MICHAEL FARNUM

In her Cultural Theory, Dame Mary Douglas, a British anthropologist, maintained that individuals often associate harm with actions that are outside the norm of a culture.

This means that cultures often actively resist change because of the risks that are perceived to be created with change.

And while Douglas was speaking more from the perspective of large national cultures that have developed over hundreds or thousands of years, her theory is often applied to the culture of corporations that have existed for a significantly smaller amount of time.

When viewed from the perspective of cybersecurity, this can be a very discouraging theory.

Changing corporate culture to take cybersecurity into consideration is a task that CISOs and cybersecurity groups are faced with every day.

Yet if cultures actively resist change, especially cultures that developed over time with little to no intention (*most corporate cultures fit that description*), how is that job supposed to get done?

A key comes from one of Douglas' quotes, "*If you want to change the culture, you will have to start by changing the organization.*" The organization itself must be changed in some fundamental ways that can allow cybersecurity to become an integral part of the culture.

This kind of culture change has to happen from the top down to be ultimately successful, but it can start from a grassroots effort if done correctly.

The CISO can start with creating a "*subculture*" of security that shows the more immediate results of implementing controls.

CREATING A SECURITY SUB-CULTURE

TO CHANGE THE CORPORATE CULTURE

BY MICHAEL FARNUM

Making that subculture rewarding to business and individuals can show the larger organization that security, while inherently disruptive in many ways, can affect change for the better.

One method for building a rewarding system is to create a deliberate plan that works with the larger IT operations team.

Building out a method for automating security into the creation of applications and/or workloads can cut down issues such as “shadow IT”, which can have a very significant impact on security posture.

If groups like marketing (*which are often the worst offenders in creating shadow IT*) see the IT and security groups as easy to work with, then they will see them as their primary provider of IT services.

This effort can be used to create success stories for employees, which can help in their career. If they can show their management that they were successful in their project AND they built security into the final product, they will be lauded for their efforts.

This is only part of a reward system that can be implemented that helps build a partnership between employees and security.

Armed with evidence that risk can be lowered by partnering with security, the CISO can start to make headway into changing the organization from the top down. Though not an easy effort, building those subcultures can show that change can be beneficial.

That is how the larger culture will see change.

GLOBETROTTING

STATS & STORIES, TRENDS & TALES

RANSOMWARE

Ransomware continues to be a hot topic when it comes to cybercrime. The FBI received reports of 1,493 ransomware victims via the Internet Crimes Complaint Center (IC3) in 2018 and it doesn't look like it's slowing down. Ransomware activity is up by 195% in Q1 2019 compared to Q4 2018 with a good portion of it being targeted at businesses, as opposed to consumers.

TROJANS

Aside from ransomware, we're also seeing an uptick in the use of Trojans, especially Emotet, to gain access to sensitive data. Emotet was initially a banking Trojan often delivered via a malicious URL in a document, such as an invoice, but it's now being used to target the healthcare industry as well. In fact, Trojans are the most common malware (80%) found in the healthcare industry with Emotet topping the list.

HOT TOPICS

195%

Ransomware is up by 195% in Q1 2019 compared to Q4 2018.

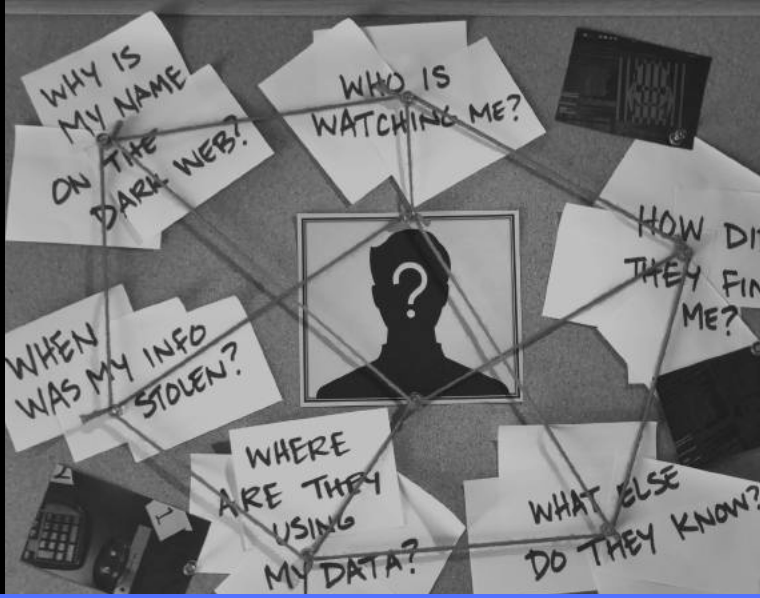
1493

.The FBI received reports of 1,493 ransomware victims via the Internet Crimes Complaint Center (IC3) in 2018.

80%

Trojans are the most common malware in the healthcare industry with Emotet topping the list.

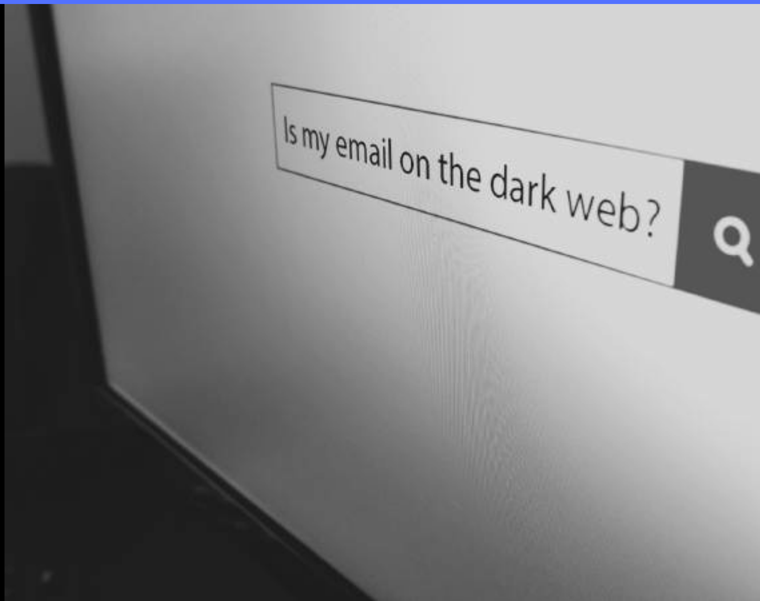
DO YOU KNOW IF YOUR EMAIL ADDRESSES OR PASSWORDS HAVE BEEN STOLEN?



DARK WEB MONITORING

How can you find out if someone is using your company's identity? Where do you even begin looking, be it the deep web or the dark web? And given all the mess that could potentially ensue, businesses need to not only protect against hackers, and breaches they must also regularly check if their name (or domain, IP addresses, etc.) pop up on the dark web.

HAVE YOUR DOMAIN NAMES OR PERHAPS IP ADDRESSES BEEN COMPROMISED?



WHY OUTSOURCE TO AN MSSP?

that is the question

IMPROVE SECURITY WITHOUT INCREASING COSTS

AVOID TECHNOLOGY OBSOLESCENCE

MIGRATE FROM CAPITAL TO OPERATIONAL EXPENDITURE

SHARE OR TRANSFER RISK MANAGEMENT & SECURITY RESPONSIBILITIES

COMPLY WITH GOVERNMENT OR INDUSTRY REGULATIONS

ACCESS SECURITY EXPERTISE UNAVAILABLE IN-HOUSE

01

EMAIL ADDRESSES CAN BE SPOOFED. DON'T ASSUME AN EMAIL IS LEGITIMATE SIMPLY BECAUSE IT'S COMING FROM SOMEONE YOU KNOW.

02

BLOG POST - COSTS OF HAVING YOUR DATA FOR SALE ON THE DARK WEB

BLOG POST - HOW TO EASILY HARDEN YOUR EMAIL CONFIGURATION

03

ON APRIL 8TH & 9TH, WE WERE A PROUD SPONSOR OF Hou.Sec.Con2019.

HELD AT THE MARRIOT MARQUIS HOUSTON, THIS YEAR WITNESSED INFAMOUS PLANE HACKER CHRIS ROBERTS DELIVERING THE OPENING KEYNOTE, WHILE AWARENESS CRUSADER, IRA WINKLER WAS ON HAND TO CLOSE THE 2-DAY EVENT.

04

OUR VERY OWN PIERLUIGI ALSO PRESENTED ON THE NOTEWORTHY TOPIC OF BUILDING THE CASE FOR A CYBERSECURITY BUDGET TO A VERY ATTENTIVE AND ENGAGED AUDIENCE.

JUDGING BY THE NUMBER OF QUESTIONS POSED, A SEQUEL IS DEFINITELY IN THE WORKS.

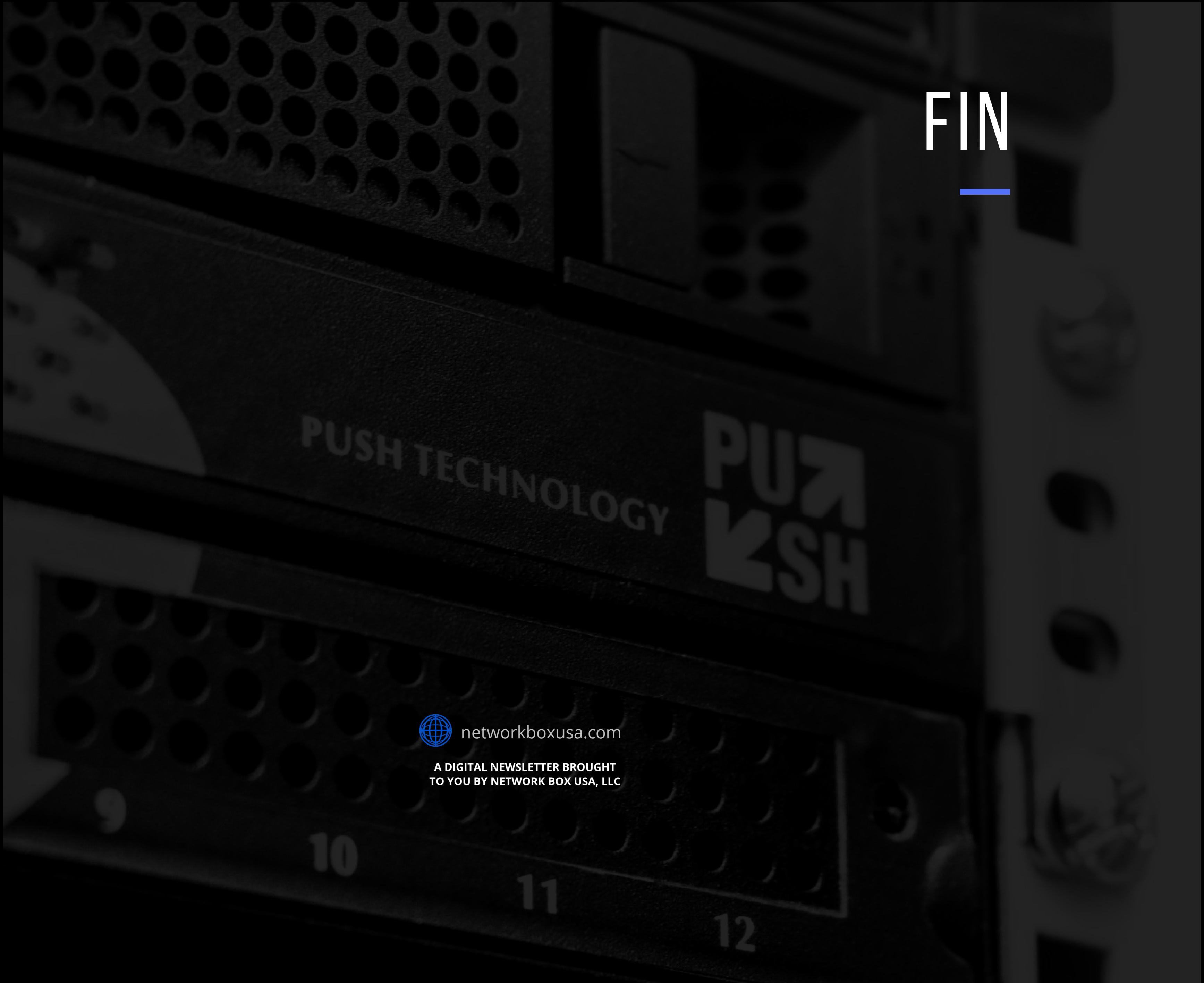
05

WANT TO KNOW WHY WE'RE DIFFERENT FROM OTHER MSSPS & CYBERSECURITY PROVIDERS OUT THERE?

TAKE A LOOK AT OUR LATEST YOUTUBE VIDEO http://bit.ly/2Kr0kXq

06

WE'RE IN THE NEWS. WELL, OUR CTO PIERLUIGI STELLA IS, SHARING HIS VIEWS ON SC MAGAZINE ABOUT GANDCRAB'S IMPENDING RETIREMENT FROM THE RANSOMWARE SCENE.



FIN

networkboxusa.com

A DIGITAL NEWSLETTER BROUGHT
TO YOU BY NETWORK BOX USA, LLC