frogworks

Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

Happy New Year

A new year is equal to a blank canvas, and the paint brush is in none other than your own hands. Paint away and create a beautiful picture for yourself. Happy New Year!

January 2018

Issue 1, Volume 8

This monthly publication provided courtesy of Alex Bleam, Owner of Frogworks

*"As a business owner, you don't have time to waste on technical and operational issues. That's where we **shine**! Call us and put an end to your IT problems finally and forever!"*

- Alex Bleam, Frogworks

Ransomware Attackers Are Increasing Their Attacks On Businesses

The ransomware ecosystem is maturing. Strains are divided into "families" and the number of new families that have been discovered in 2017 is half what it was in 2016. Even so, the total number of attacks targeting businesses have risen by 26 percent over last year's totals, according to the latest statistics released by Kaspersky Lab.

Rather than inventing wholly new software strains, hackers around the world seem content to modify existing strains, with the number of modifications growing from 54,000 to an astonishing 96,000 this year.

The modifications are having impacts that extend far beyond simply allowing them to slip past a company's defenses. Last year, 29 percent of companies impacted by a ransomware attack claimed that the incident took a week or longer to recover from. This year, that percentage rose to 34 percent.

According to one of Kaspersky's senior malware analysts, Fedor Sinitsyn, "The headline attacks of 2017 are an extreme example of growing criminal interest in corporate target. We spotted this trend in 2016, it has accelerated throughout 2017, and shows no signs of slowing down.

Business victims are remarkably vulnerable, can be charged a higher ransom than individuals and are often willing to pay up in order to keep the business operational. New business-focused infection vectors, such as through remote desktop systems, are not surprisingly on the rise."

In addition to the total number of such attacks increasing, we've seen several large-scale attacks this year, and there's no reason to believe that we won't see more of that in the months and years ahead.

This represents a fundamental shift in strategy as compared to years past and is a clear indication that hacking groups around the world are increasingly coordinating their efforts and learning from one another. That's bad news for IT security professionals

PayPal-Owned Company Sees Breach Of 1.6 Million Customers

TIO Networks, a cloud-based, multi-channel bill payment platform purchased by PayPal for $233 million in 2017, was breached earlier this year, exposing PII (Personally Identifiable Information) for an estimated 1.6 million of the service's users.

TIO Networks primarily does payment processing and accounts receivables for cable, utility, wireless and telecom companies in North America. If you do business with TIO, it's possible that your company or personal information may have been compromised.

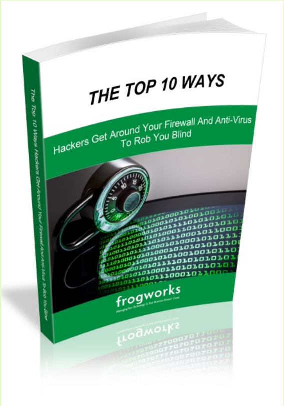
So far, neither PayPal nor TIO Networks has released any significant details about the breach, so we do not yet have any indication of how it happened, who was responsible or exactly which of their customers had their information exposed. PayPal did release a brief statement concerning the incident, which said, in part:

"The PayPal platform is not impacted in any way, as the TIO systems are completely separate from the PayPal network, and PayPal's customers' data remains secure."

The statement went on to say that as soon as PayPal identified the breach, they took action by "initiating an internal investigation of TIO and bringing in additional third-party cybersecurity expertise to review TIO's bill payment platform."

For their part, TIO Networks has suspended all operations until the investigation into the matter has been completed, and has begun notifying impacted customers. In addition to that, as is common with situations like these, they're also working with Experian to provide a year's worth of free credit monitoring for people who were affected.

Are You Protected?


THE TOP 10 WAYS
Hackers Get Around Your Firewall And Anti-Virus To Rob You Blind
frogworks

Cybercrime is so widespread that it's practically inevitable that your business – large OR small – will be attacked. However, a few small preventative measures CAN PREPARE YOU and minimize (or outright eliminate) any reputational damages, losses, litigation, embarrassment and costs.

Gain Instant Access To Our Free Report, "Top 10 Ways Hackers Get Around Your Firewall And Anti-Virus To Rob You Blind" TODAY! at https://www.getfrogworks.com/Hackers

Or call us today at (240) 880-1944

A part of TIO's statement about the incident reads as follows: "At this point, TIO cannot provide a timeline for restoring bill pay services, and continues to recommend that you contact your biller to identify alternative ways to pay your bills....We sincerely apologize for any inconvenience caused to you by the disruption of TIO's service."

The statement went on to say that as soon as PayPal identified the breach, they took action by "initiating an internal investigation of TIO and bringing in additional third-party cybersecurity expertise to review TIO's bill payment platform."

For their part, TIO Networks has suspended all operations until the investigation into the matter has been completed, and has begun notifying impacted customers. In addition to that, as is common with situations like these, they're also working with Experian to provide a year's worth of free credit monitoring for people who were affected.

A part of TIO's statement about the incident reads as follows: "At this point, TIO cannot provide a timeline for restoring bill pay services, and continues to recommend that you contact your biller to identify alternative ways to pay your bills....We sincerely apologize for any inconvenience caused to you by the disruption of TIO's service."

Many Consumers Would Withdraw Business From Companies If Data Breached

You've probably heard the phrase "the customer is always right" a thousand times. It's a truism in the business world, except when it isn't. A recent survey released by Gemalto reveals a dismaying dichotomy that's costing businesses around the world big money.

Only 27 percent of consumers surveyed feel that businesses do enough to protect customer data, and an overwhelming 70 percent of them say that they'd take their business elsewhere if a company suffered a data breach.

Unfortunately, most consumers have exceedingly poor data security habits, with 56 percent admitting to using the same password across multiple web properties and 41 percent failing to take advantage of stronger security measures like two-factor authentication, even when offered by companies.

That puts businesses, rather unfairly, in the crosshairs. They cannot make their customers take advantage of the added security offered, and given the statistics above, they are forced to have to spend even more money since most consumers won't take significant action to protect themselves or their own data.

Windows 10 Now Installed On Over 600M Machines

When Microsoft first released Windows 10, the company boasted that it would try to get its new OS running on a billion devices by 2018.

Time and circumstance have conspired to make that lofty goal unlikely, and the company has since retreated from it. However, according to statistics released at a recent shareholder's meeting, there are now more than 600 million devices utilizing it, including PCs, tablets, HoloLens headsets, Surface Hubs and Xbox One consoles.

It's an impressive number, but two things contributed to dramatically slowing the overall rate of adoption.

First and foremost, the company recently ended its free Windows 10 upgrade offer, which had been the driving force behind the rapid adoption since the initial release of the OS. Secondly, Microsoft gave up on the Windows Phone, making it unlikely in the extreme that smartphones will ever contribute in any significant way to the total number of installed devices.

Earlier this year, Microsoft found itself in hot water when it was discovered that the company was quietly pushing the new OS onto Windows 7 and Windows 8 machines. This move ate up a whopping six gigabytes of hard disk space and drew a considerable amount of fire from a variety of user and industry groups.

Some of the other tactics used by the company have also been found to be overly aggressive, and in some cases, downright coercive. The worst of these have since been abandoned, but not before considerable damage had been done to the company's image.

As things stand now, Windows 10 is the second most widely used desktop OS, behind only Windows 7, which has a market share of 52.37 percent according to the latest statistics by Netmarketshare. Even if Microsoft never quite reaches its initial 1 billion-device goal, 600 million devices is nothing to sneeze at.

Jason Hart, Gemalto's CTO, had this to say on the matter:

"In the face of upcoming data regulations such as GDPR, it's now up to businesses to ensure they are forcing security protocols on their customers to keep data secure. It's no longer enough to offer these solutions as an option. These protocols must be mandatory from the start - otherwise, businesses will face not only financial consequences, but also potentially legal action from consumers."

Digging more deeply into the details of the survey, we find that consumers trust social media sites the least when it comes to safeguarding their data, with 58 percent of respondents citing these companies as their biggest worry in terms of data security.

Curiously, 33 percent of those surveyed say they trust banks with their personal data, in spite of the fact that banks and other financial institutions are frequent targets and have suffered a

of high profile breaches in recent years.

Regardless, no matter what industry you're in, if you get breached, your customers are likely to punish you for it, even if you offer them means to make their data more secure.

Former Employees Pose Serious Risk To Security

The Department of Health and Human Services' Office for Civil Rights (OCR) has reminded those who deal with PHI and PII of the dangers that terminated employees can pose to system security in their monthly cybersecurity newsletter. Their advice is as timely as it is excellent, and includes the following:

"Making sure that user accounts are terminated so that former workforce members don't have access to data is one important way Identity and Access Management can help reduce risks posed by insider threats.

IAM can include many processes, but most commonly would include the processes by which appropriate access to data is granted, and eventually terminated, by creating and managing user accounts."

Kate Borten, President of The Marblehead Group, agrees, citing Verizon's 2017 Data Breach Investigations Report, which was released earlier this year and named health care as the industry with the highest number of insider breaches.

OCR has published an extensive list of recommendations, which include:

- The creation and maintenance of user access logs used to determine when a user's access levels are increased, or new equipment is assigned. These logs can also be used to track and trace precisely who is accessing what data, when, and using what locations, creating an audit trail.
- Establishing processes designed to terminate an employee's access as soon as employment ends. These processes should also refer back to the aforementioned access logs to ensure that all equipment has been returned.
- Changing all administrative passwords on termination of an employee with access to those accounts, so that they will be unable to access them post-employment.
- The creation of alerts that call attention to accounts that have not been utilized in some predefined number of days in order to identify accounts that may be ripe for purging from the system.
- And developing a robust auditing procedure designed to ensure that all IAM-related policies are being followed, and that the system is working as intended.

It's an excellent piece, and if your firm is in any way involved with the handling of protected health information, you owe it to yourself to head to OCR's website and read it in its entirety.