frogworks
Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

Happy Thanksgiving!

We are deeply thankful and extend to you our best wishes for a happy and healthy Thanksgiving Day.

November 2018

Issue 11, Volume 8

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

We are excited and proud to announce that Frogworks has been recognized as one of the world's best MSPs by Channel Futures!

Channel Futures
MSP 501
2018 WINNER

THE ULTIMATE GUIDE TO THE WORLD'S BEST MSPs

Microsoft Begins Re-releasing Windows 10 October Update After Fixing File Deletion Bug

Microsoft re-released its Windows 10 October 2018 Update yesterday, following the company pulling it offline due to data deletion issues over the weekend.

The software giant says there were only a few reports of data loss, at a rate of one one-hundredth of one percent. "We have fully investigated all reports of data loss, identified and fixed all known issues in the update, and conducted internal validation," says Microsoft's John Cable, Director of Program Management for Windows Servicing and Delivery.

Microsoft is now re-releasing the Windows 10 October 2018 Update to Windows Insiders, before rolling it out more broadly to consumers. "We will carefully study the results, feedback, and diagnostic data from our Insiders before taking additional steps towards re-releasing more broadly," explains Cable.

It appears the bug that caused file deletion was related to Windows 10 users who had enabled Known Folder Redirection to redirect folders like desktop, documents, pictures, and screenshots from the default location. Microsoft introduced code in its latest update to delete the empty and duplicate known folders, but it appears they weren't always empty. Microsoft has developed fixes to address a variety of problems related to these folder moves, and these fixes are now being tested with Windows Insiders.

Speaking of Windows Insiders, Microsoft's testing community did flag some of these issues ahead of the release. Microsoft appears to acknowledge this as the company is making some changes to the feedback tool for Windows 10 to ensure testers can flag the severity of bug reports.

"We have added an ability for users to also provide an indication of impact and severity when filing User Initiated Feedback," explains Cable. "We expect this will allow us to better monitor the most impactful issues even when feedback volume is low."

Microsoft will now monitor feedback related to this re-released build of Windows 10 October 2018 Update and will officially launch it to consumers once the company is confident "that there is no further impact" to Windows 10 users. "We are committed to learning from this experience and improving our processes and notification systems to help ensure our customers have a positive experience with our update process," says Cable.

While we all hope this re-release is a positive one, Microsoft has certain come under fire with its frequent update process. I made note of this in a blog last month that discussed IT admins who are campaigning hard for Microsoft to slow their roll when it comes to their Windows 10 upgrade schedule.

Approximately 78% of more than 1,100 business professionals charged with servicing Windows for their firms said that Windows 10's feature upgrades — now released twice annually — should be issued no more than once a year.

Spectre Security Built Into New Intel Chip Hardware

By now, almost everyone has heard of the Spectre and Meltdown security flaws that have been making headlines for more than a year. They're serious flaws with dire implications for tens of millions of users around the world who have an intel-based PC.

The saga surrounding the fixes for these issues has been a long one and filled with twists and turns. Intel originally attempted to push a software fix to protect its chips, but the patch they issued was so flawed that the company requested users not install it and wait for a better, more reliable patch.

In time, that patch was issued, but unfortunately, the protection it offered carried a hefty price in the form of significant system slowdowns.

The longer-term solution was, of course, to re-engineer the chips themselves. Recently, Intel announced that some of their 9th Generation chips will come with built-in fixes to ward against both Spectre and Meltdown. Note the word "some."

Specifically, the company's new line of K-series chips, used in gaming CPU's have been re-engineered to be resistant to those security flaws. Unfortunately, the X-Series (Xeon-class chips) don't feature those security fixes.

The reason is that they're based on the older Skylake-X architecture, and given that, the company is relying solely on software updates to protect those chips.

At a recent desktop press event, the company had this to say about the matter:

"...the new desktop processors include protections for the security vulnerabilities commonly referred to as 'Spectre,' 'Meltdown,' and 'L1TF.' These protections include a combination off the hardware design changes we announced earlier this year as well as software and microcode updates."

Although Intel has been roundly criticized for its handling of the issues surrounding these flaws, this is undeniably a step in the right direction.

3 OF 12 WAYS TO PROTECT YOUR BUSINESS FROM A RANSOMWARE ATTACK!

60% OF SMALL BUSINESSES GO OUT OF BUSINESS AFTER A CYBERSECURITY ATTACK.

97% OF ALL BREACHES COULD HAVE BEEN PREVENTED WITH BEST PRACTICES IN IT SECURITY.

1. COMPUTER UPDATES

Keep Microsoft, Adobe and Java products updated for better security.

2. ENCRYPTION

Whenever possible, the goal is to encrypt files at rest, in motion (think email) and especially on mobile devices.

3. FIREWALL

Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM.

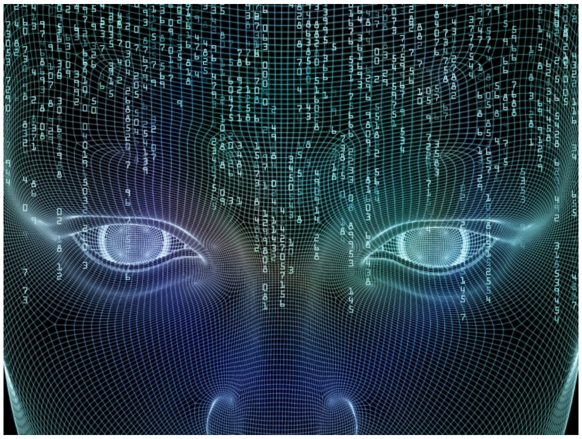
frogworks
Managing Your Technology So Your Business Doesn't Croak.

WWW.GETFROGWORKS.COM/PROTECTMYBUSINESS

An A.I. Breed of Malware

The past 100 years or so have seen an incredible advancement in technology, and the new found age of Artificial Intelligence is certainly no small part of it. Everything and everyone uses Machine Learning concepts to make life easier, like Siri or Alexa, but the dark side of the same can definitely be used to make life a living hell.

At the Black Hat USA 2018 conference a couple of weeks ago, security researchers at IBM considered a very likely scenario in the near future and created DeepLocker – a new generation malware which can fly under the radar and go undetected by way of carrier applications (like video conferencing software) until its target is reached. It uses an A.I. model to identify its target using indicators like facial recognition, geolocation and voice recognition — all of which are easily available on the web. Weaponized A.I. appears to be here for the long haul and could target anyone. Scary.



DeepLocker is just an experiment by IBM to show how open-source A.I. tools can be combined with straightforward evasion techniques to build a targeted and highly effective malware. As the world of cybersecurity is constantly evolving, security professionals will now have to up their game to combat hybrid malware attacks. Experiments like this allow researchers to stay one step ahead of hackers.

According to Marc Ph. Stoecklin, principal research scientist at IBM Research, “The security community needs to prepare to face a new level of A.I.-powered attacks. We can’t, as an industry, simply wait until the attacks are found in the wild to start preparing our defenses. To borrow an analogy from the medical field, we need to examine the virus to create the ‘vaccine.’”

But back to DeepLocker…

DeepLocker’s Deep Neural Network model provides “trigger conditions” that need to be met for malware to be executed. In case the target is not found, the virus stays blurred inside the app, which makes reverse-engineering for experts an almost impossible task.

To prove the efficiency and precision of A.I.-based malware, security engineers demonstrated the attack using the notorious WannaCry virus. They created a proof-of-concept situation where the payload was hidden inside a video conferencing program. None of the anti-virus engines or sandboxes managed to detect the malware, which resulted in this conclusion by researchers:

Imagine that this video conferencing application is distributed and downloaded by millions of people, which is a plausible scenario nowadays on many public platforms. When launched, the app would surreptitiously feed camera snapshots into the embedded A.I. model, but otherwise behave normally for all users except the intended target.

What is more, applications like Social Mapper can be implemented inside the malware which would make the detection of a potential target an even more manageable task.

Indeed, the power of Artificial Intelligence is probably limitless, but the experiment proves that security researchers still have a lot of work to do when it comes to cybersecurity. The examination of various apps should be taken into consideration, and any unexpected actions should be flagged immediately.

Microsoft Is Changing How Searches Will Work

Change is coming to the way Microsoft handles search across its ecosystem. If you use the home edition of Office, you're not likely to notice, but if you use Office 365, the changes will be significant.

Here's what's happening:

First of all, the search bar will get bigger, taking a more prominent and visible place on your screen's real estate.

Second, anywhere the company utilizes a search box (from their Bing search engine, to the OS itself, to Teams, Office and more), the plan is to provide a unified and consistent look that is intended to improve the overall user experience.

The box itself is getting a makeover and will soon start offering suggestions based on your previous search behaviors. For instance, it may present you with a list of frequently used email contacts or documents that you've recently edited, with the list updating dynamically as you begin typing a term into the search field.

In addition to that, you'll soon be able to search for commands within a given application, so instead of hunting around on the menu bar for the function you're looking for, the search box will take you right to it, showing it among the search results.

If you're signed into your Office 365 account, the search results will also include any documents you have saved in OneDrive or SharePoint and relevant conversations in Yammer and Teams if you use those. It also may feature contacts from your company directory.

Most significantly, since the Bing search engine is itself a search box, those results will be displayed alongside relevant webpages.

If you're curious to see it in action, it is currently available today as an opt-in beta/preview mode for corporate users. It's also available in both Outlook and SharePoint mobile apps. The general public will be able to see it in action as soon as the second quarter of 2019, when the new functionality will be expended to Office Home, Office Desktop and Windows 10 itself.

Payment Pages Are Being Compromised To Steal Data

Symantec's most recent statistics have revealed a disturbing trend. Malware designed to compromise checkout pages is seeing a big spike in use, with the company reporting a staggering 248,000 attempts since August 13th of this year, with more than a third of them (36 percent) between September 13th through September 20th. As disturbing as those numbers are, that's just the tip of the iceberg.

As Symantec notes on their website:

"If we compare the week of September 13 to 20 to the same week in August, the number of instances of formjacking attacks blocked by Symantec more than doubled, jumping from just over 41,000 to almost 88.500 - a percentage increase of 117 percent."

Leading the surge is a particularly nasty strain of malware known as "Magecart." Magecart campaigns are quite robust that begin by breaching the target website, then injecting malicious scripts into it that are designed to scrape card details and other customer information provided during the checkout process. This is an attack that's alternately known as formjacking, payment card scraping, and web-based skimming.

Symantec isn't the only company to take note of the trend. RiskIQ has been sink holing domains associated with Magecart infrastructure for much of the month and alerting companies compromised by Magecart attacks as they find them.

Kevin Beaumont, an independent security researcher, had this to say via Twitter:
"#TrackingMagecart I've updated the IoCs to double the number of domains, now tracking over 1000 objects - some of the domains have now been sink holed. Recommend InfoSec vendors block/flag domains."

Magecart isn't new. Security researchers have been tracking it since 2015, and independent researcher Willem de Groot has created a malware scanning website called MageReport, which allows business owners to check to see if their Magento-based webshop is vulnerable to this type of attack. If you think you might be, it certainly bears making use of.

At present, the one thing that's not known is the reason behind the sudden spike. Only that it's happening.

Firefox Adds Data Breach Monitoring Service

Firefox is upping the ante where digital security is concerned, having just announced the release of a new, free service called 'Firefox Monitor.' The new service is designed with one specific goal in mind: To assist users in finding out if their accounts were exposed via a data breach.

It was developed in partnership with Troy Hunt, whose website, "Have I Been Pwned" is one of the most popular destinations on the web for security-minded individuals. This website, in fact, is the driving force behind Mozilla's new service.

People will be able to engage with the service in two different ways. First, by making a direct inquiry to check the status of their various accounts, passwords, and email addresses that may have been compromised. Or second, by configuring the new subsystem to notify them when their information has been detected by the system.

Nick Nguyen, of Mozilla, had this to say about the new feature:

"It can be hard to keep track of when your information has been stolen, so we're going to help by launching Firefox Monitor, a free service that notifies people when they've been part of a data breach. After testing this summer, the results and positive attention gave us the confidence we needed to know this was a feature we wanted to give to all of our users."

If you find out via active polling or receive a notification that one of your accounts was compromised, you should take action immediately. You should change the password and audit the account to address instances where you may have used the same password associated with the compromised account in order to minimize your risks.

This is great news, and a fantastic addition by Mozilla. While it's not a magic bullet that will solve all your security woes, it should help give users greater peace of mind, and it puts a powerful new tool in their hands to monitor the integrity of their own accounts. Kudos to Mozilla!