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

Ribb"IT" Review

"Rise above the storm and you will find the sunshine."

-Mario Fernandez

August 2019

Issue 8, Volume 9

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

Keeping up with BlueKeep

Remote Desktop Services (RDS) benefit employees and IT administrators alike. With employees often working from anywhere, remote desktop reduces the physical burden of carrying a work laptop home. It also makes updating and managing systems easier, which can alleviate the administrative burden when handling a large network.

Unfortunately, a vulnerability recently discovered in RDS has the potential to let hackers remotely wreak havoc on computers or servers running RDS — and their networks — if the issue isn't patched.

What is BlueKeep?

During Windows' May 2019 patch cycle, Microsoft released a patch for a remote code execution bug in their Remote Desktop Services software. If left unpatched, this vulnerability could allow remote, unauthenticated attackers to execute payloads with administrative privileges and spread to other computers/servers within a network.

Errata Security CEO, Robert Graham, scanned all externally facing IP addresses on May 28th, 2019 for systems susceptible to BlueKeep.

In his blog, Robert estimated nearly one million computers, laptops, and servers may be vulnerable and Microsoft noted that if an attacker is able to gain access into the system, they could then "install programs; view, change, or delete data; or create new accounts with full user rights."

Exploiting the Vulnerability

Offensive security researchers have worked around the clock to prove the BlueKeep vulnerability could be exploited by malicious hackers. On June 3rd 2019, Ryan Hanson showcased his success on Twitter despite having "very little experience with kernel exploitation".

Considering previous wormable attacks like WannaCry, it is highly probable that hackers will start attacking unpatched computers and servers in the very near future. Microsoft, NSA, and dozens of fellow security vendors have made similar conclusions and advise IT departments to immediately patch affected systems.

How Do I Fix This Vulnerability?

Due to the severity of BlueKeep, Microsoft has released patches for all actively supported versions of Windows and the old/busted versions from yesteryear. Installing the appropriate patch via your tried and tested patching process will fix this vulnerability.

What is the Risk of Not Fixing the Vulnerability?

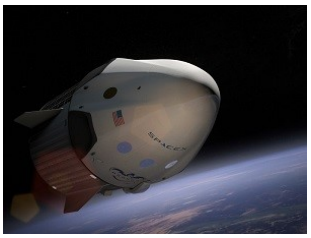
Vulnerable hosts are extremely likely to be remotely compromised by an attacker which could lead to data theft or encryption of all files using ransomware.

Considering this has the potential to be a wormable exploit, not only would the exploited host be affected but an entire network could be impacted as well.

You can find links to the necessary patches on our website at : **https://www.getfrogworks.com/keepingupwithbluekeep**

Also, feel free to call our office at 240 - 880 - 1944 if you have any questions about your network security.

NASA Suffers Data Breach With Device Connected To Network



Not even NASA is immune to hacking. Recently, the American space agency announced that they traced a breach back to April of 2018.

That was when a group described as an APT (Advanced, Persistent Threat) breached the Jet Propulsion Laboratory's network via a 'Raspberry-Pi' device that was improperly connected to the network.

The hackers made off with more than 500MB worth of data in 23 files. Two of the files contained sensitive information relating to international Traffic in Arms Regulations relating to the Mars Science Laboratory mission.

According to investigators, the reason the hackers were able to burrow so deeply into the agency's networks from a third-party device was that the agency did not have their network properly segmented. Once the hackers gained access, they could go pretty much anywhere they wanted.

"We also found that security problem log tickets, created in the TISB when a potential or actual IT system security vulnerability is identified, were not resolved for extended periods of time - sometimes longer than 18 days." The investigators from the OIG said.

Late last year, the US Department of Justice charged a pair of Chinese nationals for hacking cloud providers, the US Navy, and NASA. The DOJ's filings identified the pair as part of one of the Chinese government's elite hacking corps known as APT10.

Given that, it is entirely possible that APT10 was behind the Raspberry Pi incident. They certainly have the skills, means and motive. Especially given Chinese interest in US technology in general and their recent big push for space exploration.

Clearly, NASA has some work to do to shore up their security, and the hope is that now that these events have come to light, the agency will take decisive steps to do just that. Good luck, NASA.

Update Your Browser To Fix New Firefox Security Vulnerability

Are you a Firefox user? If so, you'll want to update to version 67.0.4 as soon as possible. Just last week, Mozilla released Firefox 67.0.3 to address a critical remote code execution vulnerability that was being used in the wild to selectively target vulnerable systems.

Unfortunately, that proved to be just the tip of the iceberg.

Since then, the company discovered that the vulnerability they initially addressed was merely the second part in a chained pair of security flaws. The pair worked in tandem to drop and execute malicious code onto vulnerable systems.

In response, the company quickly released the latest version, 67.0.4, which addresses both links in the chain. The issue, initially reported by Coinbase Security, is being tracked as CVE-2019-11708.

Its description reads as follows:

"Insufficient vetting of parameters passed with the Prompt: Open IPC message between child and parent processes can result in the non-sandboxed parent process opening web content chosen by a compromised child process. When combined with additional vulnerabilities, this could result in executing arbitrary code on the user's computer."

Obviously, this is a serious issue indeed, especially since it's one that's already being actively exploited by hackers around the world. If you're not sure what version you're running, open Firefox, go to the help menu, and click on "About Firefox." The software will take it from there and scan for a new version. If one is available, it will let you know, and you can download and install it.

If you don't want to go that route, just head to Mozilla's website and grab the latest direct from there.

Kudos to the sharp-eyed researchers at Coinbase Security for spotting the issue, and to Mozilla for their rapid response. Don't take any chances. Install the latest update today.

We now have an E-newsletter!

… but we might not have your email address! If you would like to receive our newsletter though email please visit us at **www.getfrogworks.com/newsletter** and sign up.

Large Percentage Of Mobile Apps Have Security Flaws

How many apps do you have on your phone?If you're like most people, you've likely got dozens or more. Considering how much storage is available on mobile devices these days, people tend to install apps and when they no longer want them, they don't bother to uninstall them. Whatever your number is, the statistics recently published by Positive Technologies in their report "Vulnerabilities and Threats in Mobile Applications 2019" will alarm you.

Here are a few of the key findings:

35 percent of all mobile apps tested had vulnerabilities relating to the insecure transmission of sensitive data.

35 percent had issues with the incorrect implementation of session expiration

20 percent had problems relating to sensitive data being stored in the app source code and insufficient protection against cyber attacks using brute-force techniques

29 percent of tested apps contained vulnerabilities relating to insecure inter-process communications, which are classed as high risk

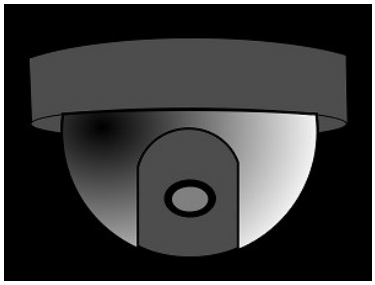
Overall, high-risk vulnerabilities were found in 38 percent of tested iOS apps, and 43 percent of Android apps. Even worse, 89 percent of the vulnerabilities that were discovered could be exploited via malware. The hacker targeting the device would never even need to take physical control of the device.

Leigh-Anne Galloway (one of the people responsible for the report) said:

"Developers pay painstaking attention to software design in order to give us a smooth and convenient experience and people gladly install mobile apps and provide personal information. However, an alarming number of apps are critically insecure, and far less developer attention is spent on solving that issue. We recommend that users take a close look when applications request access to phone functions or data. If you doubt that an application needs access to perform its job correctly, decline the request."

Wise words, and very good advice. So back to the initial question, and with the statistics above in mind, how many apps do you have on your phone?

IP Camera Hacking Attempts Are Rising



Recently, Trend Micro published some statistics that just about everyone should find disturbing. According to their latest statistics, the security company has blocked more than five million cyber-attacks against IP cameras, just in the past five months. Worse, IP cameras don't tend to have great security in place to begin with, making it relatively easy for hackers to control them remotely.

IP cameras send video directly to the internet as it is captured, and are typically used for surveillance. They're among the vast crop of 'low hanging fruit' of web-connected devices these days. The company found that of the attacks, fully 75 percent relied on simple brute-force tactics.

Oscar Chang, of Trend Micro, had this to say about the findings:

"More verticals are seeking connected, AI-powered video surveillance applications, causing a clear paradigm shift from a relatively closed-off network to a more interconnected network operated heavily by cloud-based

technologies. Due to this shift in the landscape, manufacturers and users must pay attention to the security of these IoT devices. While the industry has known about cyber-risks, manufacturers have been unable to properly address the risk without knowing the root cause and attack methods."

Those are wise words. There is explosive growth of the number of smart devices in recent years, and hackers have gleefully appointed them by the tens of thousands and turned them into botnet armies for hire. Given those circumstances, one would think that every smart device manufacturer would make increased security of the devices they sell a top priority.

To date, however, that simply hasn't been the case. Until that changes, we can expect to see the numbers Trend Micro and other security companies report increase until we finally reach a tipping point.

The sad thing is, it doesn't have to come to that. If the industry were to start getting serious about IoT security and standards put in place, we could, at the very least, diminish the magnitude of the problem. At present,

Researchers Recently Discovered A New Mysterious Malware Strain

Researchers at the cybersecurity firm Anomali have discovered a completely new type of malware that's disturbing on several levels.

Worse is the fact that the researchers aren't quite sure what it does.

The new strain has been dubbed 'IPStorm' by its creators, who at this point, remain unknown.

Of interest is the fact that it is the first malware found in the wild that makes use of the IPFS P2P network for its command and control communication. By doing so, it can hide its network activity amid legitimate streams of P2P network traffic, making it virtually undetectable. IPFS is an open source P2P file sharing network used to store and share files. Among other things, it's currently being used to host a version of Wikipedia that can be accessed in countries where access to the website proper is blocked.

The malware has been written in the Go programming language, but researchers haven't been able to ascertain at this point how it begins its initial infection cycle. They have discovered that the malware package itself has been split into a number of parts, which is an indication that the group responsible for its initial development knows what they're doing.

The researchers added: "By breaking functionality out into different Go packages, the codebase is easier to maintain. Also, the threat actor can break out things into modules to make it easier to swap out or reuse functionality."

On top of that, IPStorm comes with a number of antivirus-evasion techniques built-in. When it copies itself onto a target system, it uses folder names that relate to Microsoft or Adobe systems, making it unlikely that even a savvy, observant user would notice it right away.

The researchers estimate that right now, the IPStorm botnet consists of some 3,000 machines, which is a surprisingly small number and a clear indication that the malware is in a very early stage of development. Keep this one on your radar. It's not a big threat at the moment, but it certainly has the potential to be a major problem in the months ahead.