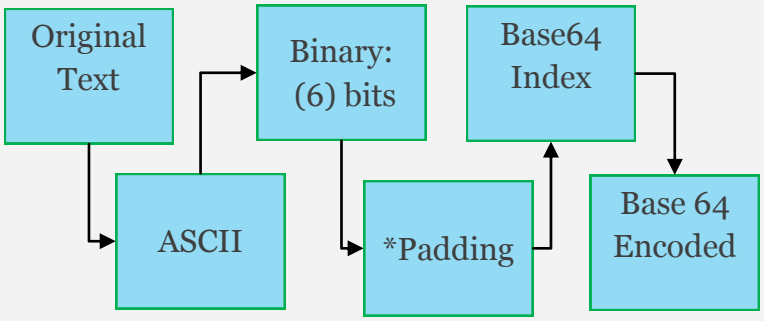
NEWS
Cyber Security
Vol. 2 | Issue 4 May 2017

Under Review
Crypto Challenge 2.0

Welcome to another Crypto Challenge review! Last month's challenge was difficult, but you rose to the occasion. Getting down to business, the challenge was obfuscated using Base64 encoding. This encoding type is very common and has many purposes. Email and web applications use it to convert binary files into text. However, this process is also maliciously used to hide malware code, and evade security measures.

Base64 Encryption: Overview

1. Convert each character to ASCII
2. Convert ASCII values to binary
3. Separate binary sequences into groups of 6 bits
4. Insert zeros when necessary—Padding
5. Reference each group to the Base64 Index,



Consider this only a primer on base64 encoding, but here is a fabulous base64 tutorial. Working it out by hand can be a long process, but honestly, it is not too difficult. Once you get the hang of it, decoding base-64 is surprisingly satisfying. For those checking their work or seeking instant gratification, you may want to use a "Text-to-Base64" encryption tool. Feel free to contact me if you ever get discouraged. I have some great tutorials and will gladly walk you through the process. Trust me, doing good Cyber isn't always easy, but it sure is fun!

Champions: April 2017

D.Wright| B.Means| R.Dodson
P.Vanney | D.Barber |W.Nichols
B.Pasmore |B.Shields | J.Norris
T.Kingsley | K.Schofield | J.Crouse
T.Hatch |D.Wade |E.Neumann
F.Krueger |S.Flores | M.Lesko
J.Carrillo |R.Maguire |J.Taylor
A.Shoop |J.Kimbler |J.Lavender
R.Hess| D.Evans |T.Siegmund
M.Millan| F.Carmichael |D.Curtin

RANSOMWARE

Most of us have heard of the WannaCry ransomware outbreak by now. Discovered around 4:00 AM EDT May 12, 2017, the WannaCry attack is still affecting various organizations around the world. Read the full United States Computer Emergency Readiness Team (US-CERT) analysis report here.

Ransomware is malicious software that encrypts critical system data and holds it for ransom – payable only in Bitcoins. This is a cruel method of criminal extortion when leveraged against vulnerable industries such as hospitals, telecommunications, and local law enforcement. Although the outbreak is most definitely newsworthy, the Department responded quickly and took actions to secure our network from WannaCry. Cyber Security wanted to take this time to highlight what really matters to us and our families: prevention. It is important we learn from this event and get serious about preventing ransomware.

Prevention

Keep software up-to-date

Maintain external backups of critical data

Do not click email links or attachments from unknown sources

WannaCry was effective because it indiscriminately 'wormed' to massive proportions by attacking any professional and private Windows workstations it touched. Here's the kicker, Microsoft had previously released a solution to protect against the exploits used by the WannaCry ransomware. The entire event could have been avoided if organizations and people had kept their software up-to-date and practiced good cyber 'hygiene'.

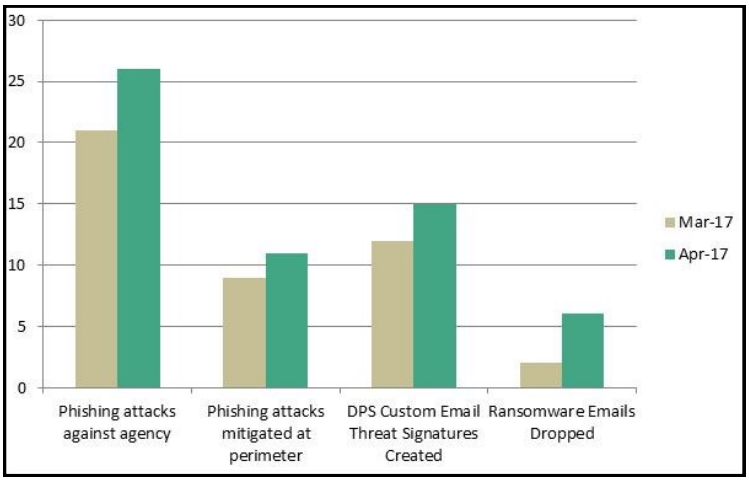
What's the moral of the story? Keep your software up-to-date. If you haven't already, here is how to update your windows systems.

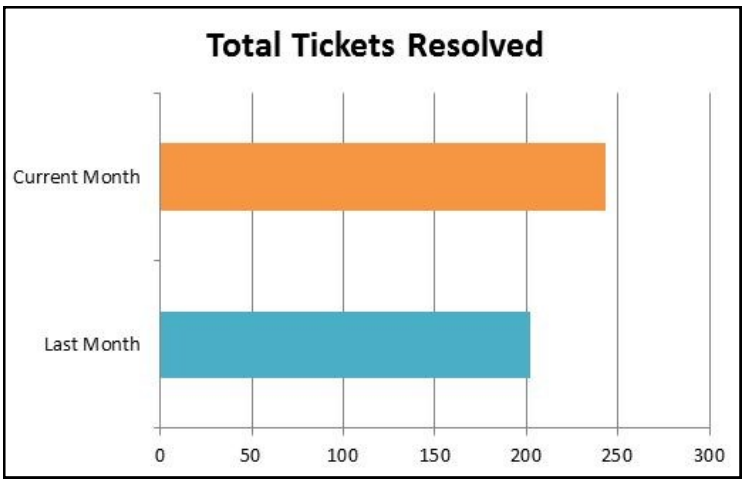
Windows Updates

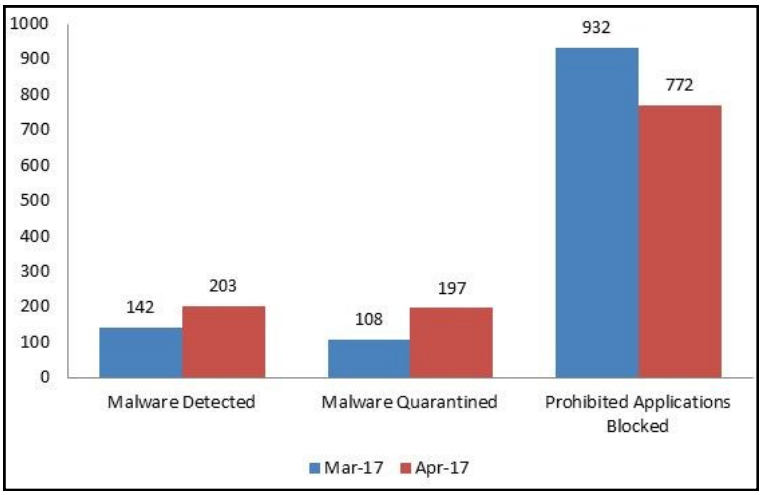
1. **Select the Start button**
2. **Go to Settings > Update & security > Windows Update**
3. **Select Check for updates.**

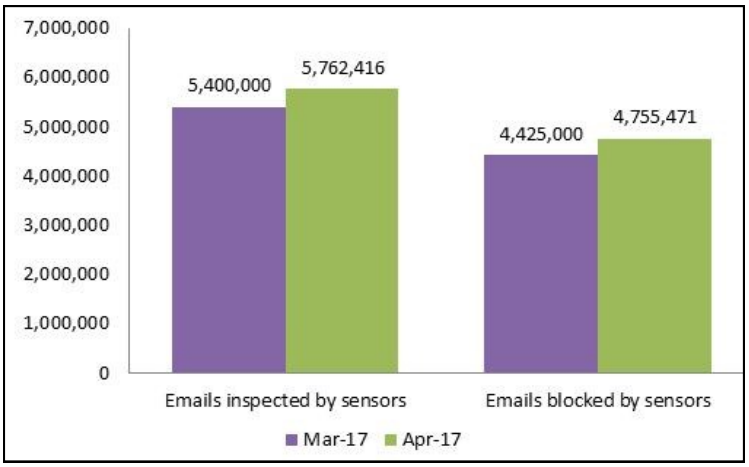
Secure.
Protect.
Inform.

<Cyber Stats />









New Cyber Twitter!

Introducing the new and super official Cyber Security Twitter account. Follow us for security news, updates, and threat intelligence. Check out our page here!

Newsletter Support

Jennifer.Carson@dps.texas.gov

Connect & Share

Website | Twitter