NEWS
Cyber Security
Vol. 3 | Issue 1 January 2018

Back from the Desert

Happy New Year!!

Hello everyone and welcome to this year's first edition of the Cyber Security News.

For those new to DPS, or have forgotten me, I am your Cybersecurity Awareness Training Officer, Kirk Burns. I recently returned from a deployment to Afghanistan and have resumed publishing the Cyber Newsletter from Jennifer Carson who left to explore other work opportunities.

Jennifer did a great job with the newsletter during my deployment. I look forward to continuing to provide a quality newsletter which hopefully you will find helpful and informative. In my absence, Jennifer started a Crypto Challenge which apparently has become a favorite part of the newsletter. I will provide the answer to the challenge from the last newsletter as well as discuss the code later in this newsletter. I intend to incorporate something like this in each newsletter but will be calling it Cyber Challenge instead of Crypto Challenge so that I can expand the types of puzzles. I will also be changing the format slightly to better present several cyber related news events. I believe this will better educate everyone on interesting events in the cyber world and provide knowledge that will benefit the average person. Please feel free to contact me and suggest topics of interest you would like to see included in future issues of our newsletter.

I would like to thank everyone who has welcomed me back. It is good to be back home in God's Country and back to work at DPS.

Google Removes Gaming Apps

Recently Google took down 60 gaming apps from their Play Store because of pop-up porn malware being part of the app. Both Android and Apple have had issues with applications over the last few years. It is important for you to be aware of what apps are requesting access to on your electronic devices. Here is an article from Reuters about this most recent issue.

Google removes gaming apps with pop-up porn malware

(Reuters) - Alphabet Inc's (GOOGL.O) Google said on Friday it took down 60 gaming applications after security firm Check Point said it had discovered new malicious software in the apps available to both children and adults at Google Play Store.

To read more click **HERE**.

New Security Flaw Detected in Intel Hardware

The DPS IT team has taken actions to mitigate and address the flaws below to the agency.

If you have been listening to the news you have probably heard about Spectre and Meltdown. Both of these are serious computer issues plaguing computer hardware and have processor manufacturers and software companies scrambling to attempt to create patches. While these are very newly reported problems, another has just been found. That is what the next article is about.

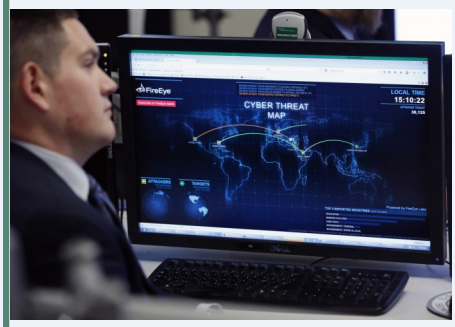
Intel AMT Security Issue Lets Attackers Bypass Login Credentials in Corporate Laptops

Helsinki, Finland – January 12, 2018: F-Secure reports a security issue affecting most corporate laptops that allows an attacker with physical access to backdoor a device in less than 30 seconds. The issue allows the attacker to bypass the need to enter credentials, including BIOS and Bitlocker passwords and TPM pins, and to gain remote access for later exploitation. It exists within Intel's Active Management Technology (AMT) and potentially affects millions of laptops globally.

To read more click **HERE**.

More Cyber News!!

Cybersecurity Showdown: Why the Military Is Preparing for a New Kind of War



The drafting, negotiation, and passage of the National Defense Authorization Act (NDAA) is an annual event that sets the annual budget for the Department of Defense. During this time Congress is able to exert control over the priorities, guiding principles, and issues that will be addressed by the department in the coming year. The 2018 incarnation of the NDAA, which has just been signed into law by the president, includes, nested in Title XVI, Subtitle C, provisions, a requirement that the White House and the DOD meaningfully investigate, consider, and establish national standards and guidance in the cybersecurity and cyber-warfare space. They must explore the development of a national posture for these issues.

To read more click **HERE**.

With WPA3, Wi-Fi security is about to get a lot tougher

At last, Wi-Fi security -- or lack of -- is about to get its day in the sun.

The Wi-Fi Alliance, an industry body made up of device makers including Apple, Microsoft, and Qualcomm, announced Monday its next-generation wireless network security standard, WPA3. The standard will replace WPA2, a near-two decades-old security protocol that's built in to protect almost every wireless device today -- including phones, laptops, and the Internet of Things.

To read more click **HERE**.

Crypto-Miner Botnet Spreads over SSH

A recently discovered Linux crypto-miner botnet spreading over the SSH protocol is based on the Python scripting language, which makes it difficult to detect, F5 Networks has discovered.

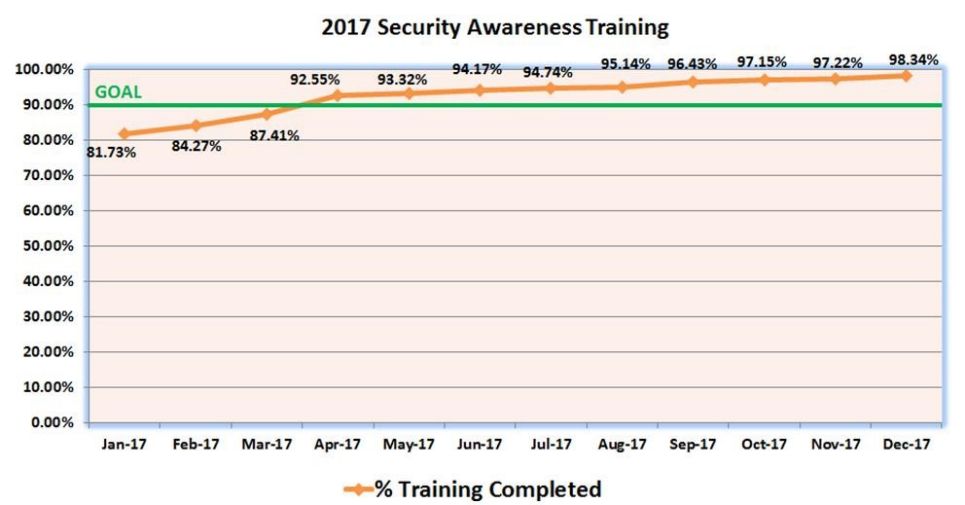
Dubbed *PyCryptoMiner*, the botnet is using Pastebin to receive new command and control server (C&C) assignments when the original C&C isn't available. Under active development, the botnet recently added scanner functionality hunting for vulnerable JBoss servers (exploiting CVE-2017-12149), F5 says.

To read more click **HERE**.

<Cyber Stats - Nov and Dec />

Starting next month I hope to incorporate more statistics so that everyone is aware of cyber events happening here at DPS.

Below I have added a graph showing completion percentages for the Sans Securing the Human online cyber training. As an agency we are doing well with the training, but we aren't at 100% yet. If you have not completed the training please do so. I will be sending out reminders to individuals and possibly supervisors soon for those who still need to complete the training.

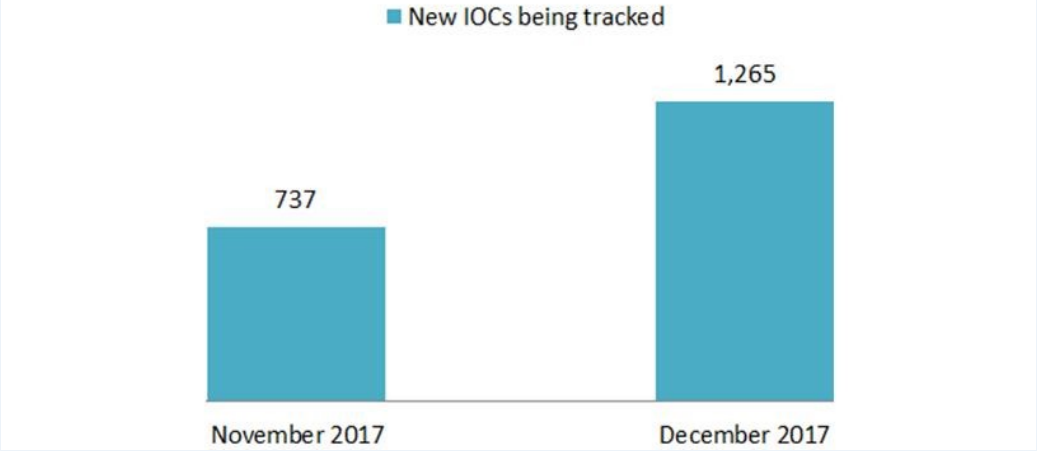


Other Statis- tics

There were 10 phishing attacks against DPS for the month of November and 12 during December. While impossible to prevent all phishing attacks, we have increased the Threat Signatures by 16 in November and 29 in December to help try to protect the Agency as well as all employees.

The graph on the right shows Indicators of Compromise (IOC). As you can see, DPS had 737 new IOCs for the month of November and a huge jump to 1,265 for the month of December. That is an almost 72% increase in incidents between the two months. While IT and Cyber do a great job of protecting against these incidents, every employee can assist by notifying cyber as soon as you observe anything strange and by remembering your online security training.

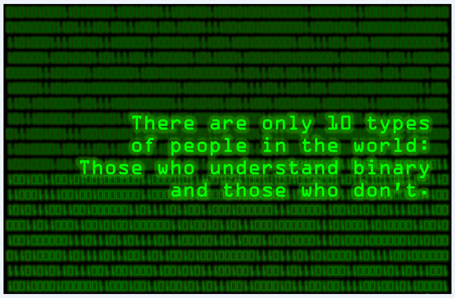
New IOCs being tracked	737	71.64%	1,265



Crypto Challenge

01010011011001010110001101110101011100100110100101110100011110010010000001101000011000010111001100100000011011100110111100100000011011000110100101101101011010010111010001110011001000000110111101101110011011000111100100100000011000100110000101110010011100100110100101100101011100100111001101110011

Above is the code that Jennifer included in the last newsletter. For those of you who don't know, this is called BINARY. For a detailed explanation of what Binary is, you can click **HERE**. For the Readers Digest version, you can think of it as a code that computers use at the hardware level to communicate with other computers and execute programs. Binary is not an encryption. It is an encoding. The main difference being you do not have to have a key to convert the binary code back to its original form.



A quick Google search will provide you with several websites that will convert the binary code to text. When you put the code above into any of them you will see that the encoded message that Jennifer put in the last newsletter says "Security has no limits only barriers".

Below you will find this month's Cyber Challenge. Next month's Challenge will be better thought out.

00110011 00110100 00100000 00110110 01100110 00100000 00110100 00110011 00100000 00110110 00110011 00100000 00110101 00110011 00100000 00110101 00110111
00100000 00110101 00111001 00100000 00110110 00110111 00100000 00110110 00110101 00100000 00110101 00110111 00100000 00110011 00111001 00100000 00110011
00110001 00100000 00110100 00111001 00100000 00110100 00111000 00100000 00110100 01100101 00100000 00110111 00110111 00100000 00110101 01100001 00100000
00110101 00110111 00100000 00110011 00110101 00100000 00110110 01100010 00100000 00110100 00111001 00100000 00110100 00110111 00100000 00110011 00110001
00100000 00110111 00110110 00100000 00110110 00110011 00100000 00110110 01100100 00100000 00110101 00110101 00100000 00110110 00110111 00100000 00110110
00110010 00100000 00110011 00110010 00100000 00110011 00110100 00100000 00110110 00110111 00100000 00110101 00111001 00100000 00110011 00110010 00100000
00110011 00111001 00100000 00110110 01100100 00100000 00110101 01100001 00100000 00110110 01100100 00100000 00110101 00110110 00100000 00110110 01100011
00100000 00110100 00111001 00100000 00110100 00111000 00100000 00110101 00110010 00100000 00110110 01100110 00100000 00110101 00111001 00100000 00110101
00110111 00100000 00110011 00110100 00100000 00110110 00110111 00100000 00110110 00110010 00100000 00110011 00110010 00100000 00110011 00110100 00100000
00110110 00110111 00100000 00110101 00110011 00100000 00110101 00110110 00100000 00110101 00110001 00100000 00110110 00110111 00100000 00110110 00110011
00100000 00110011 00110010 00100000 00110101 00110110 00100000 00110110 01100001 00100000 00110110 00110100 00100000 00110101 00111000 00100000 00110100
01100001 00100000 00110111 00110000 00100000 00110110 00110100 00100000 00110100 00111000 00100000 00110110 01100010 00100000 00110111 00110011 00100000
00110100 00111001 00100000 00110100 00111000 00100000 00110110 01100011 00100000 00110111 00110110 00100000 00110110 00110100 00100000 00110101 00110011
00100000 00110100 00110010 00100000 00110011 00110011 00100000 00110110 00110001 00100000 00110101 00110111 00100000 00110111 00111000 00100000 00110111
00110011 00100000 00110100 00111001 00100000 00110100 00110111 00100000 00110100 01100001 00100000 00110110 01100011 00100000 00110100 00111001 00100000
00110100 00110111 00100000 00110110 00111000 00100000 00110110 00111000 00100000 00110101 00111001 00100000 00110011 00110010 00100000 00110111 00110100
00100000 00110110 01100011 00100000 00110101 01100001 00100000 00110100 00110011 00100000 00110011 00110100 00100000 00110110 00110111 00100000 00110101
00110110 00100000 00110011 00110010 00100000 00110110 00111000 00100000 00110110 00111000 00100000 00110110 00110100 00100000 00110100 00110011 00100000
00110110 00110100 00100000 00110111 01100001 00100000 00110100 00111001 00100000 00110100 00110111 00100000 00110011 00110001 00100000 00110111 00110110
00100000 00110110 00110011 00100000 00110110 01100100 00100000 00110101 00110101 00100000 00110111 00110011 00100000 00110100 00111001 00100000 00110100
00111000 00100000 00110110 01100011 00100000 00110111 00110110 00100000 00110110 00110100 00100000 00110101 00110011 00100000 00110100 00110010 00100000
00110110 01100010 00100000 00110101 01100001 00100000 00110101 00111000 00100000 00110100 01100101 00100000 00110110 01100011 00100000 00110110 00110011
00100000 00110110 01100101 00100000 00110101 01100001 00100000 00110110 01100011 00100000 00110100 00111001 00100000 00110100 00111000 00100000 00110101
00110010 00100000 00110111 00110110 00100000 00110100 00111001 00100000 00110100 00110111 00100000 00110100 01100001 00100000 00110110 01100011 00100000
00110100 00111001 00100000 00110100 00110111 00100000 00110110 00111000 00100000 00110110 00111000 00100000 00110101 00111001 00100000 00110011 00110010
00100000 00110111 00110100 00100000 00110110 01100011 00100000 00110101 01100001 00100000 00110100 01100110 00100000 00110100 01100010 00100000 00110100
00110001 00100000 00110110 01100101 00100000 00110101 00110011 00100000 00110100 00110001 00100000 00110100 01100010 00100000 00110011 00110100 00100000
00110110 01100110 00100000 00110100 00110011 00100000 00110101 00110110 00100000 00110100 00111001 00100000 00110100 00110110 00100000 00110100 01100001
00100000 00110111 00110000 00100000 00110101 00111001 00100000 00110011 00110010 00100000 00110110 00111000 00100000 00110110 00111000 00100000 00110110
00110011 00100000 00110110 01100100 00100000 00110101 00110001 00100000 00110110 00110111 00100000 00110101 00110001 00100000 00110011 00110010 00100000
00110111 00111000 00100000 00110110 00111000 00100000 00110110 00110011 00100000 00110110 01100100 00100000 00110111 00110100 00100000 00110110 01100011
00100000 00110100 00111001 00100000 00110100 00110001 00100000 00110011 01100100 00100000 00110011 01100100

Newsletter Support

GRP_Cyber_Risk@dps.texas.gov

Connect & Share

Website | Twitter