East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Wednesday 10 June 2020

This advice has been collated by EMSOU and is intended for wider distribution within the East Midlands Region to raise awareness among businesses and the public.

Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from reputable sources.

If you require any further information, assistance or guidance please contact the EMSOU Protect Team EMSOU Protect Team **or your local Force protect team.**

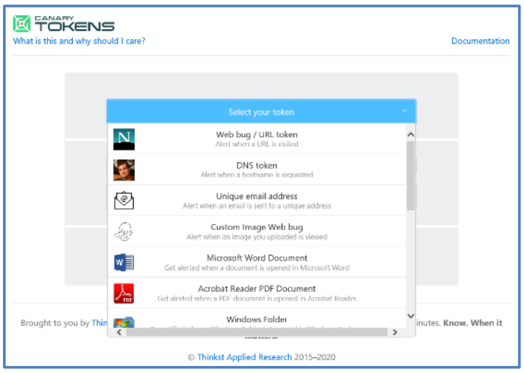
Today's topic is 'canaries and honeypots'

In the 19th century, miners brought canaries into coal mines as an early-warning signal for toxic gases. The birds, being more sensitive to carbon monoxide, would become sick before the miners, who would then have a chance to escape. Fast forward a hundred years and the concept of early warning signals is one of the fundamental aspects of defence in depth.

Canaries or honeypots on a computer network are, like the canary birds in a mine, an early warning of danger; an isolated and monitored object that detects, deflects and alerts network defenders when targeted.

Canary tokens, honey accounts, pots, hashes or nets appear to store the important data or services that an attacker would look for. When setting up a canary or honey pot, their primary purpose is to defend and gather Intel, not entrap.

Canary file: Create a Microsoft Word document and fill it with fake usernames and passwords. Save the file with a name like 'password.doc' and visit this site to create the alert. As soon as the file is opened, an email alert will be sent.



CANARY TOKENS

What is this and why should I care?

Documentation

Select your token

Web bug / URL token
Alert when a URL is visited

DNS token
Alert when a hostname is requested

Unique email address
Alert when an email is sent to a unique address

Custom Image Web bug
Alert when an image you uploaded is viewed

Microsoft Word Document
Get alerted when a document is opened in Microsoft Word

Acrobat Reader PDF Document
Get alerted when a PDF document is opened in Acrobat Reader

Windows Folder

Brought to you by Thin inutes. **Know. When it** matters.

© Thinkst Applied Research 2015–2020

A honey account: If an attacker is already in the network, they may attempt to log into user accounts, using a few common passwords. This technique avoids triggering an account lockout, but can yield valid credentials. To detect these 'password spraying' attempts, create an account so that any attempt to log will immediately alert the security team.

Honeypot: This is a computer that offers a legitimate-looking service for users. For example, a fake file server with a realistic name which suggests it is a computer that contains important research data. As soon as an attacker attempts to access this computer, an alert is generated.

For further information see Binary Defence, Cowrie and WebLayrinth.

Honey hash/token: Is a username and hashed password inserted into the memory of a running system - an entry point computer exposed to the internet. Attackers use specialised tools to tap into this memory and steal passwords. As soon as the attacker try's to use this, an alert is sent to the administrator, see here for further guidance.

Honey nets: A network of multiple honey pots set up to invite attack, so an attacker's activities and methods can be studied. The Modern Honey Network (MHN) project is an easy way to deploy, manage and monitor multiple honeypots. MHN uses scripts to automate the deployment of several different honeypot technologies.

Hot topics

Cyber-criminals have launched a new phishing scam targeting self-employed workers using the Self-Employment Income Support Scheme (SEISS). The scam begins with a text message sent to self-employed workers offering a tax rebate. The text message informs victims they are eligible for a tax refund and redirects them to a bogus website which leads to a realistic copy of the official HMRC site. Users are asked to enter their email address, postcode and HMRC log-in details, before a fake refund amount is calculated. Victims are then asked to enter personal information including card number, name on card, account number, security code and expiry date

A new Amazon phishing campaign has emerged claiming to offer recipients the chance to win a £1,000 Amazon gift card. The subject reads: *"On the occasion of overcoming the coronavirus, Amazon gives you the gift of victory."* The sender name is spoofed to read 'contact@amazon.com'. The recipient is instructed to click on a link in order to apply.

Reporting

Please report all Fraud and Cybercrime to Action Fraud by calling 0300 123 2040 or online.
Forward suspicious emails to report@phishing.gov.uk.
Report SMS scams by forwarding the original message to 7726 (spells SPAM on the keypad).

Webinar – Thursday 11th June 2020 @ 1400 – 1500 hrs

Join North West Regional Organised Crime Unit's Cyber Protect Team as they take a look at password security to protect our digital lives. In this webinar, they will discuss the need for unique and complex passwords on your online accounts, including advice on creating and storing them securely; demonstrate what a criminal may do to access your passwords and what they do with them once they have, coupling this with current trends of exploits seen in the North West region.

You'll leave this webinar with knowledge on how to create more secure passwords for each of your accounts, how to store them securely, and where to go for advice and guidance.

To register for this event click on the following link places are limited.