West Midlands | Regional Cyber Crime Unit

ISSUE 1, 27TH MAY 2020

WM ROCU
Cyber Crime Sentinel

This newsletter has been collated by West Midlands Regional Cyber Crime Unit and is intended for wider distribution within the West Midlands Region to raise awareness among businesses and members of 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 West Midlands RCCU team. Any reports of cyber crime still need to be made to Action Fraud.

IN THE NEWS

A hoax copy of the NHS website has been discovered. The website includes harmful links to COVID-19 related health tips. Once these links are clicked on, a pop-up box appears asking visitors to save a file called 'COVID19'. If saved, the malware it contains steals passwords, credit card data, cookies from browsers, crypto wallets, files and screenshots.

Criminals are following a familiar pattern shown during and after disasters – sending out phishing emails and malware with a humanitarian edge, asking for donations from the unsuspecting public to aid those most affected.

Phishing emails, advertising face masks which play on the rumours being reported in the media that the public may be asked to wear face masks outside.

Attackers have deployed a phishing campaign against remote workers using Skype, luring them with phishing emails that fake notifications from the service. The social engineering in this campaign is refined enough to make victims access the fraudulent login page and provide their credentials. Furthermore, the username is automatically filled in, which only helps clear any suspicion. All the victim has to do is type in their password and the attacker gets it automatically.

USEFUL INFORMATION

Slido Webinar - Q&A Session

You will be able to join us at Sli.do every Wednesday 10-11am to ask us questions and advice about cyber security and how to stay safe online. You can ask a question any time and we will answer during this time. Enter the event code wmrccu.

Suspicious Email Reporting Service (SERS)

Spotted something suspicious in your inbox? You can now forward phishing emails to the NCSC's new Suspicious Email Reporting Service, helping to protect the UK from email scams!

Read more about how the service is automating the takedown of malicious infrastructure at www.ncsc.gov.uk/information/report-suspicious-emails

Shade Ransomware (Troldesh) ransomware shuts down and releases decryption keys

The Shade ransomware gang have published more than 750,000 decryption keys on GitHub.

Find out more at https://www.zdnet.com/article/shade-troldesh-ransomware-shuts-down-and-releases-all-decryption-keys

No More Ransom

The No More Ransom project is an initiative between law enforcement and the private sector with the goal of helping victims of ransomware retrieve their encrypted data without having to pay criminals.

Find out more at https://www.nomoreransom.org

Please report all Fraud and Cybercrime to Action Fraud by calling 0300 123 2040 or online. Forward suspicious emails to report@phishing.gov.uk.

Join West Midlands and Tarian Regional Cyber Crime Teams, as they host a free webinar on how to plan and prepare for a cyber incident.
Monday 1st June 2-3pm
Book your space now at eventbrite
https://www.eventbrite.co.uk/e/cyber-response-planning-to-prepare-tickets-105367856094?fbclid=IwAR0Aw1engovrenfJansLRzEe0MNsLhx5A_xdHRAM5u8KXSL-bNYwQFznOdc

Microsoft Warns of COVID-19 Phishing Emails Spreading RAT

In a series of tweets, Microsoft detailed a massive campaign that delivers a remote access tool using emails with attachments containing malicious Excel macros. Read more at https://twitter.com/MsftSecIntel/status/1262504864694726656

EasyJet Cyber Incident

EasyJet revealed that they suffered a breach including the personal, and in some cases financial, details of thousands of customers. We recommend changing passwords for any accounts which could have been affected, and we would urge people to be extra cautious around any correspondence related to this, as attackers may look to exploit the story in phishing attacks. Find out more at https://www.ncsc.gov.uk/news/easyjet-incident

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk