East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Monday 08 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 the "Kill Chain"

The term kill chain was originally used by the military to describe the structure of an attack which begins with identifying a target and ends with its destruction. The term was later adopted by Lockheed Martin to describe how an organisation's network might be attacked.

Reconnaissance: Assess the organisation from the outside-in, to identify targets and tactics. Tactics used may include scanning networks for known vulnerabilities and using open source intelligence (corporate websites, news reports and social media profiles).

Intrusion & Exploitation: Attackers can exploit identified vulnerabilities to penetrate the network and/or use what has been discovered to socially engineer an attack - manipulating staff to; click a link, download malware, visit an infected website, or plug in a malicious USB.

Expansion & Entrenchment: Once access had been gained, the attackers move laterally to other systems and accounts (privilege escalation), to obtain access to high value data or better control of the network. Purpose built penetration tools are 'noisy' so many attackers will 'live off the land' and use inbuilt functions, such as PowerShell, and tap into file systems (NFS and SMB) which pass information over the network unencrypted.

Exfiltration & Damage: Attackers will; steal data piecemeal or en masse, deploy a payload such as ransomware or a logic bomb, biding their time for maximum effect.

Covering your tracks: Attackers will purge log files, delete temporary files and software, plant 'false flags' and encrypt drives to confuse and delay any form of forensic investigation.

Why it matters?

The Kill Chain emphasises the need for defence in depth employing a multi layered approach involving technical, procedural and physical controls:

- Logical controls (vulnerability scanning; host hardening, segmentation, anti-malware)
- Administrative controls (policies; procedures, standards, training)
- Physical controls (gates, doors, badges, signage, equipment disposal etc.)

The kill chain illustrates how large the attack surface is for an organisation and the time and commitment a cybercriminal will invest in attacking your organisation.

Crucially, the average amount of time an adversary will spend in the network before launching an attack - known as the dwell time - is 6 months.

East Midlands Special Operations Unit

When preventative controls fail, an organisation's survival will depend on:

- Detective controls: to identify, flag and trace intrusions.
- Recovery controls: to contain, sanitize, restore or recover the network.

Table top sessions are a key element in the defence of any organisation against a cyber event.

Gathering critical team members, to discuss ways to; identify, study and respond to different types of cyber incidents and maintain business operations will ensure survival.

"Failing to prepare means preparing to fail."

Hot Topics

The NCSC is continuing to see **ongoing active compromises** of a number of VPN vulnerabilities, detailed in an NCSC Alert published here, The NCSC strongly recommends UK organisations check that all security updates are installed.

The CISA Alert from April 2020 can be found here: **It provides new detection methods for this activity, including a tool to help identify associated Indicators of Compromise (IOC's).** It also warns that if a victim organisation previously compromised **has not reset its passwords**, an actor could still regain access even after the vulnerability has been patched.

There is expected to be a spike in ransomware attacks as employees return to their physical workspaces. Due to the short amount of time to prepare employees for remote working, security protocols and procedures were relaxed in some organisations. Ransomware on potentially compromised devices are expected to be activated when returned to the workspace.

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.