East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Thursday 13th August 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: MITRE ATT&CK

The Mitre ATT&CK (adversarial tactics, techniques, & common knowledge) framework is a free resource which will help your IT Team to:

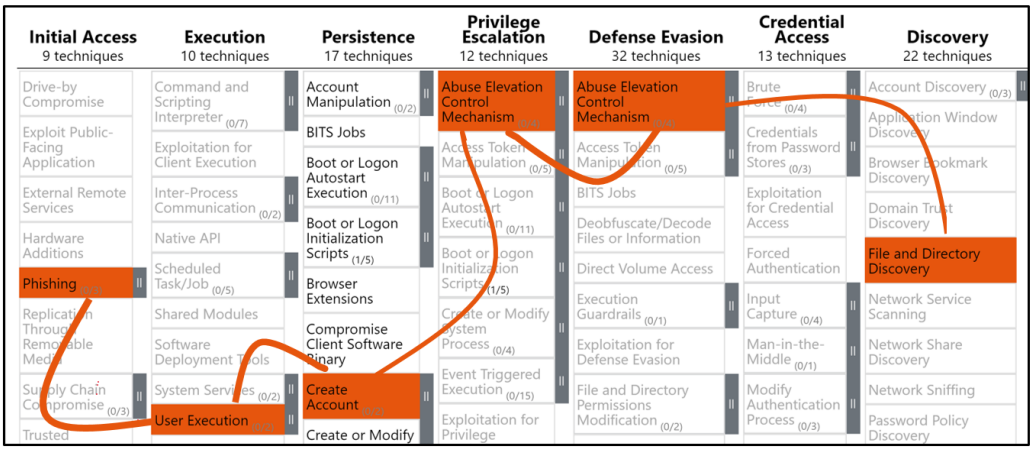
- Understand how a cyberattack will play out in order to stop them.
- Identify gaps in enterprise security defences, which can be prioritised and acted upon.
- Use a common language to clearly communicate the exact details of a threat and current security controls and processes.

The framework focuses on attacker behaviour which is important if you want to stop an ongoing attack before data exfiltration or destructive behaviour occurs. It allows security teams to clearly identify the nature of a threat, map that threat back to the security controls that should protect against them and then ultimately determine whether or not these controls are effective. The framework covers 12 tactics, which an attacker is trying to achieve:

Tactic / Goal	**The attacker is trying to**
Initial Access	. . . get into your network.
Execution	. . . run malicious code.
Persistence	. . . maintain his or her foothold.
Privilege Escalation	. . . gain higher-level permissions.
Defence Evasion	. . . avoid being detected.
Credential Access	. . . steal account names and passwords.
Discovery	. . . figure out your environment.
Lateral Movement	. . . move through your environment.
Collection	. . . gather data of interest
Command and Control	. . . communicate with compromised systems to control them.
Exfiltration	. . . steal data.
Impact	. . . manipulate, interrupt or destroy your systems and data

T**echniques:** Describe the different ways that attackers can achieve these tactics or goals. Using the online matrix tool, you can drill into each technique by double-clicking it. This gives

you a more detailed explanation of the technique, how to mitigate it and malware commonly associated with the use of the technique.



Attackers move from technique to technique

Mitre ATT&CK also includes something called 'Groups'. There are 91 groups at present and these represents high profile attackers whose techniques and modus operandi are known. These attackers often go by different aliases, but the Groups descriptors identify them. If threat intelligence prompts senior leadership to question whether the organisation is adequately protected against a particular group or attack, the MITRE framework will help you to give a confident response.

How can I get started with Mitre ATT&CK

Start by selecting the security controls used in the current environment and then map them back to the framework. From here, it is possible to immediately identify gaps, assess risk and then act to improve defences.

For Red Teams, it is also possible to model real-world attackers, both by the techniques they use and the sequence in which they deploy them, as well as the specific software tools that they deploy. Ultimately, this gives a clear, objective way to explain to senior management what the security strategy needs to be outlining:

- Which threats we should be most concerned about.
- What security controls we need to acquire.
- Which security controls provide the necessary protection.

Vendor products vary widely in their effectiveness but the framework provides security teams with the ability to compare and contrast products to see how they address the risks that the organization faces.

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).