East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

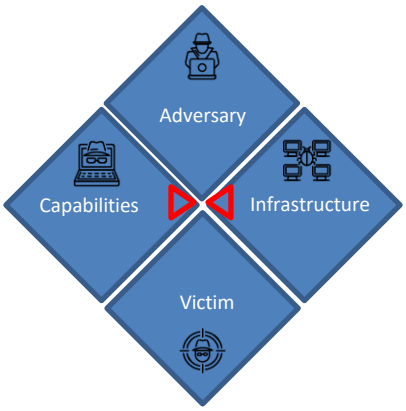
Friday 24 July 2020

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: Using the Diamond Model for Intrusion Analysis



Threat intelligence is useful when trying to get to grips with the anatomy of a security incident. The more information we have, the better able we are to identify the problem and make informed decisions about how we should deal with it. Intelligence is also useful when developing strategies to prevent a reoccurrence.

The Diamond model identifies the key elements of an incident. Depending on the audience, it can be used to present a simple and non-technical summary or a very detailed breakdown of what has occurred.

In 2013, the retail giant Target suffered a data breach which exposed over 40 million credit and debit card details and the personal information of 70 million customers from over 2000 stores.

The breach can be used to illustrate the Diamond Model:

- **Adversary**: is the '**who**' behind an incident. This may be an IP address, a domain name or an email address. In the Target data breach, the person responsible was thought to be the Ukrainian hacker, Andrey Hodirevski.
- **Victim**: is the '**where**'. Some victims are purposefully selected by an attacker, others merely a victim of opportunity. The 'where' could be anything from the local comprehensive school to a multi-million pound enterprise such as Target.
- **Capability**: is the '**how**' and highlights the adversary's knowledge of tactics and techniques. The attacker must have some level of capability such as hacking skills, or access to capabilities such as paying a 3rd party to use ransomware. In the Target data breach, Hodirevski knew how to create phishing emails, as well as how to traverse networks and deploy malware.
- **Infrastructure**: is 'by **what** means' or the hardware / software chain between the attacker and the victim. Hodirevski was able to pivot from the network of Fazio Mechanical Services (an air conditioning supplier to Target) to get onto the retail giant's network and from there, attack cash tills used by the store.

There are also two axis in the model (seen in red above):

- **Social-Political**: is the '**why**' behind an attack such as a grudge attack, economic espionage, politically motivated, or in the case of Target, financially driven.
- **Technology**: ties the '**how**' and the '**what**' together.

Finally, there are optional 'meta-features' that add further detail to mapping out the incident:

- **Timestamp**: is the '**when**', and records the chronology of events
- **Phases**: cover which steps of the 'Kill Chain' have been accomplished which describes well known steps hackers use when launching a cyber-attack. It often starts with gathering intelligence on the victim and ends with delivering a malicious payload or data exfiltration.
- **Result**: this centres on whether an attacker was able to compromise the confidentiality, integrity, or availability of data. Results are recorded as; 'success', 'failure', or 'unknown'.
- **Methodology**: is a general classification of the type of attack that took place such as phishing or denial of service. In the Target data breach, the attack initially began using a phishing email loaded with the Citadel Trojan. This gave Hodirevski a backdoor onto Fazio's systems and from there onto Target's network.
- **Resources:** cover assets, used to accomplish the incident e.g. hardware, software, funds, knowledge, information, access to facilities etc.

When completing the Diamond Model, it is important to think about how reliable your intelligence is. Is the information from a reliable source? Is the data likely to be an accurate representation of what has happened? Use a scale from 1 to 6, with 6 being 'difficult to say'.

When recording information there is no specific order to the Diamond Model - just 'paint the picture'. Some incidents may require multiple models focusing on each step of the attack, others just one or two. Either way, the Diamond model is a powerful and flexible tool for intrusion analyst.

Today's Hot Topic is: Attacks on Twitter

On Thursday evening, various Twitter accounts belonging to high profile US celebrities and brands were hacked to post tweets that linked to a cryptocurrency investment scam.

Twitter posted a thread saying that hackers compromised its internal systems and tools to carry out this attack. To mitigate the impact, Twitter locked the verified accounts that were compromised, although full access has now been restored.

While this appeared to be an attack on Twitter, rather than individual users, make sure that you

- Are always wary of requests for money or sensitive information
- Minimise the amount of sensitive data you share online
- Always use a strong password and two factor authentication.

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).