Classification of attacks for efficient response

Aims

With a variety of attacks on the Internet today, it is ever more important to establish a common taxonomy to classify and categorise attacks, to enable response on a large scale. We need to classify attacks according to their scale, type, vertical affected and damage caused.

No-one has a desire to re-invent the wheel when a good wheel already exists. This paper does not propose a new taxonomy, but it does propose a discussion at CARIS2 to form an opinion on what incident categorisation method should be used for CARIS2 and for the proposed SMART RG in the IRTF. This discussion has the aim of establishing a common language for:

- describing attacks;
- understanding attacks;
- attack mitigations.

The discussion will focus on what categorisation is most helpful for researchers, responders and other stakeholders – and why. Key features of good incident categorisation will be brought out and the relevance in various situations.

The following prompts will be used to direct the conversation:

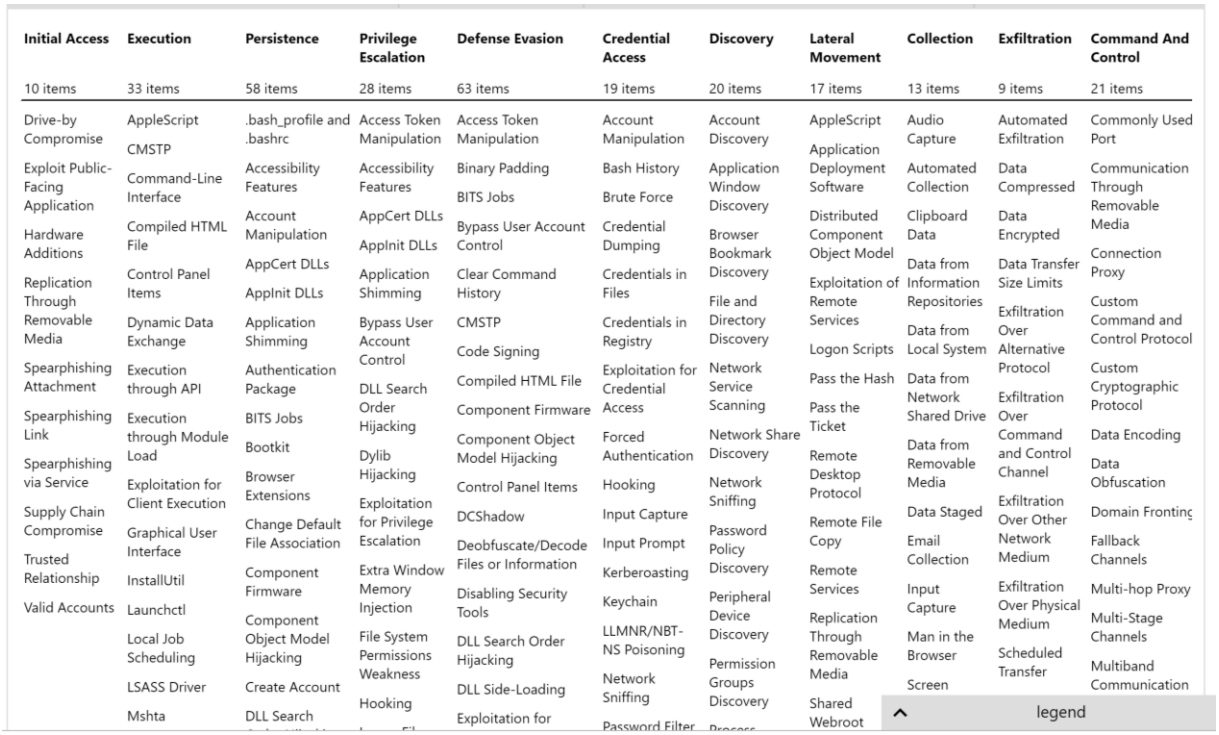
1) What existing taxonomies already exist?
2) Which existing taxonomies have participants used?
3) Do any metrics exist to find relative prevalence of such taxonomies and their usage?
4) Which taxonomies have been most helpful and why?
5) What are the features that inform the initial or developed response to an attack? (These will need to be in the taxonomy for it to be useful.)

The results of this discussion will be used to establish a common language for CARIS2 and the proposed SMART RG in the IRTF.

Below, we consider some taxonomies that are already in use. There are likely other taxonomies that have been used by CARIS2 participants to great effect, which would be welcomed as inputs to the discussion.

Existing taxonomies: MITRE

The Mitre Corporation's ATT&CK Framework (Fig.1) is a comprehensive classification of attack tactics and techniques, started around 2013 as a way to "categorize common adversary behaviour for adversary emulation and intrusion detection research". ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. According to their website, "the ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community". ATT&CK uses a matrix of multiple factors to categories attacks easily and quickly. The full matrix of attack techniques is available from Mitre's website: https://attack.mitre.org/matrices/enterprise/



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	33 items	58 items	28 items	63 items	19 items	20 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-hop Proxy
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Launchctl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot	Screen		Multiband Communication
	Local Job Scheduling	Component Object Model Hijacking		Deobfuscate/Decode Files or Information	Keychain	Remote System Discovery				
	LSASS Driver	Create Account		Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery				
	Mshta	DLL Search		DLL Search Order Hijacking	Network Sniffing	System Information Discovery				
				DLL Side-Loading	Password Filter					
				Exploitation for						

legend

Fig.1: MITRE ATT&CK Framework Navigator

Existing taxonomies: ENISA

ENISA, the EU Agency for Network and Information Security, has also published their threat taxonomy (https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view). This taxonomy begins with the threat and then describes the attacks that enable that threat, e.g. the threat is "information gathering" and the attacks that enable this are "scanning, sniffing, social engineering". This approach allows categories to link direct cause and effect. Separately, ENISA has published a web app (https://etl.enisa.europa.eu/#/) showing the evolution of the top 15 identified threats for 2015-18 in graphically pleasing bubbles (Fig.2). These bubbles are relative in size and classify common threats, though some are related to others, e.g. malware enables data breaches, botnets can lead to DDoS attacks, and so on. These broad categories allow easy classification and overlap, which may or may not be precise enough for SMART.

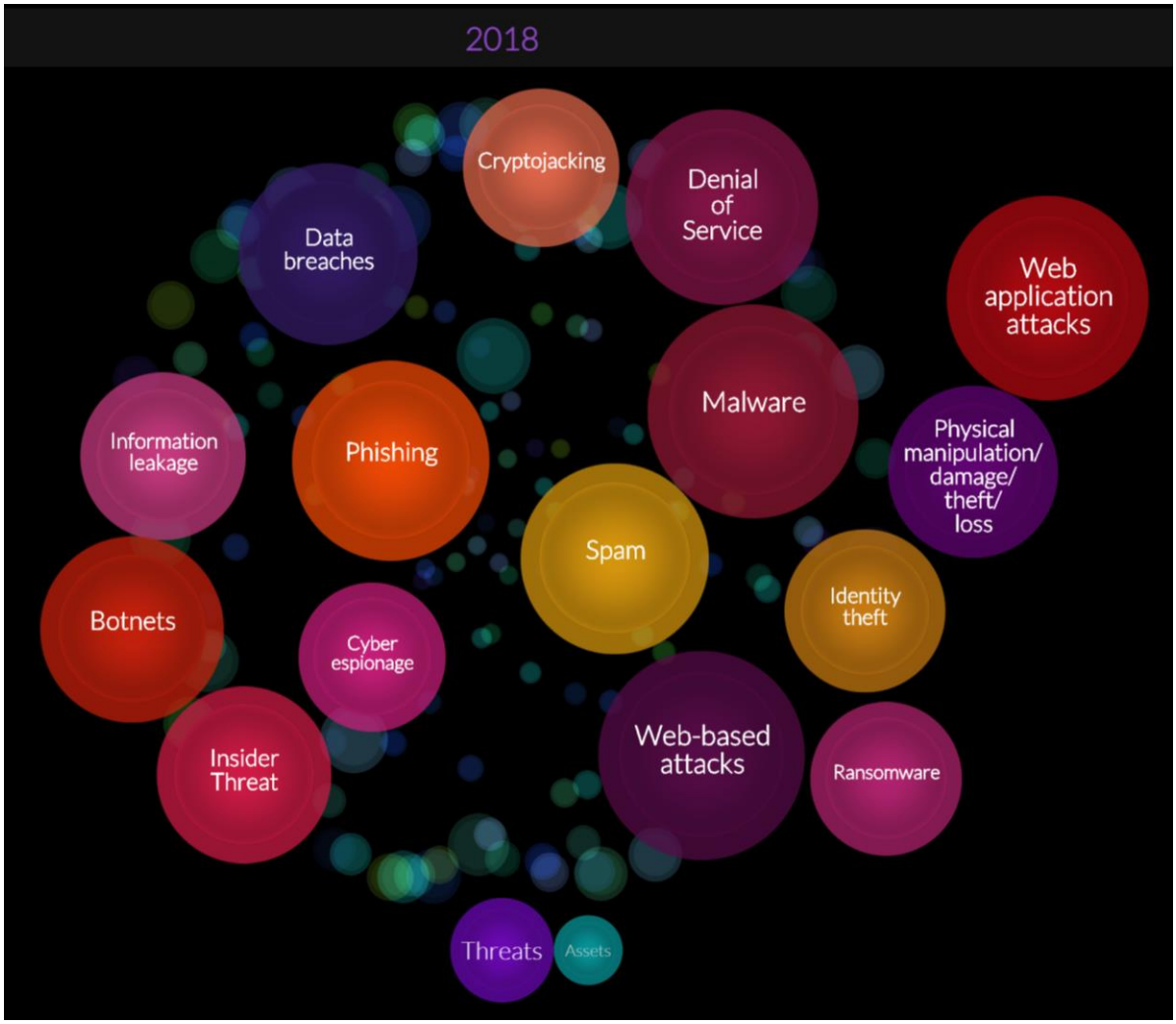


Fig.2: ENISA Threat Landscape web app

Existing taxonomies: NCSC

NCSC, the UK's National Cyber Security Centre, has its own way of classifying incidents for prioritisation (Fig.3). An incident is placed into a category based on its scale and the affected parties, rather than by the attack technique. More information can be found here: https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents

	Category definition	Who responds?	What do they do?
Category 1 National cyber emergency	A cyber attack which causes sustained disruption of UK essential services or affects UK national security, leading to severe economic or social consequences or to loss of life.	Immediate, rapid and coordinated cross-government response. Strategic leadership from Ministers / Cabinet Office (COBR), tactical cross-government coordination by NCSC, working closely with Law Enforcement	Coordinated on-site presence for evidence gathering, forensic acquisition and support. Collocation of NCSC, Law Enforcement, Lead Government Departments and others where possible for enhanced response.
Category 2 Highly significant incident	A cyber attack which has a serious impact on central government, UK essential services, a large proportion of the UK population, or the UK economy.	Response typically led by NCSC (escalated to COBR if necessary), working closely with Law Enforcement (typically NCA) as required. Cross-government response coordinated by NCSC.	NCSC will often provide on-site response, investigation and analysis, aligned with Law Enforcement criminal investigation activities.
Category 3 Significant incident	A cyber attack which has a serious impact on a large organisation or on wider / local government, or which poses a considerable risk to central government or UK essential services.	Response typically led by NCSC, working with Law Enforcement (typically NCA) as required.	NCSC will provide remote support and analysis, standard guidance; on-site NCSC or NCA support may be provided.
Category 4 Substantial incident	A cyber attack which has a serious impact on a medium-sized organisation, or which poses a considerable risk to a large organisation or wider / local government.	Response led either by NCSC or by Law Enforcement (NCA or ROCU), dependent on the incident.	NCSC or Law Enforcement will provide remote support and standard guidance, or on-site support by exception.
Category 5 Moderate incident	A cyber attack on a small organisation, or which poses a considerable risk to a medium-sized organisation, or preliminary indications of cyber activity against a large organisation or the government.	Response led by Law Enforcement (likely ROCU or local Police Force), with NCA input as required.	Law Enforcement will provide remote support and standard guidance, with on-site response by exception.
Category 6 Localised incident	A cyber attack on an individual, or preliminary indications of cyber activity against a small or medium-sized organisation.	Automated Protect advice or local response led by Law Enforcement (likely local Police Force).	Remote support and provision of standard advice. On-site response by exception.

Fig.3: NCSC cyber attack categories