Janet Network Security Incident Classification Scheme

The statistics provided by Jisc's Janet network CSIRT require a degree of interpretation. Often the numbers are influenced more by the team's activities than they are by external influences. For example: an increase in the number of malware incidents may indicate increasing infections, but it is just as likely to be due to increased detection rates by CSIRT.

Each incident receives a single classification when it is created. In most cases we will not go back and change the initial classification - seeking perfect classification can prove to be a large distraction from the work of handling incidents, and no system will be 100% perfect.

Compromise
The more "traditional" security incidents get placed here. Systems that have been compromised through network service vulnerabilities, insecure passwords or web defacements usually end up in this category if one of the others is not more appropriate. These systems are often used to host illegal material, relay further attacks and access other systems, or to distribute malware. A judgment and distinction is made by the incident handler with systems that have been compromised through automated malware.

Copyright
Reports of copyright infringement. Since the studios send most of these in a standard format we are able to handle them automatically.

Denial of Service
Attacks aimed at denying legitimate access to a network or service. These range from simply overwhelming a connection with greater traffic than it has capacity, to traffic especially crafted to consume CPU and memory resources on the target system. Since October 2016 we have been running a DDoS mitigation platform, which has greatly increased our visibility of attacks on the network and provides more granular metrics. The number here relates to the number of incidents rather than the number of attacks, which the mitigation platform measures, and as a single incident may consist of multiple attacks the numbers referred to here will be lower than that reported elsewhere.

General Query
An enquiry from a customer, usually related to the provision of services by CSIRT.

LEA Query
Enquiries from the police, or other law enforcement agency. The typical incident is a request to obtain communications data from a Janet-connected customer under RIPA Section 22. Where appropriate these requests are passed to the customer to action.

Legal/Policy Query
An enquiry from a customer on a legal or policy issue.

Malware

An incident that primarily involves a system being infected with malicious software without the user's consent. The overwhelming majority of these incidents will naturally be due to large outbreaks of malware, but they can range form targeted attacks to banking Trojans. A large amount of these tickets are from automated systems.

Network Security Query
An enquiry from a customer about best practices in network or information security.

Other
Anything that does not fall into one of the other categories.

Phishing

Incidents involving phishing emails being sent to or received from a Jisc customer. The overwhelming majority of these are low level unsophisticated phishing attacks designed to capture email account details for use in advance-fee fraud. More sophisticated attacks often cross into the malware category.

Scanning
A system on the Janet network sending probes for network services on other systems. Most of these are detected by our own systems. We consider network scanning directed at Janet network systems to be a "normal" part of Internet background activity and do not report on it.

Social Engineering
Attacks where information or access to systems is obtained through the deception of people. Since we split phishing from this category, very few incidents are now classified here.

Unauthorised Use
Misuse of the Janet network, not covered by other categories, as defined by the Janet network AUP and Security Policy.

Unclassified
This classification can only occur if the incident handler fails to set an incident classification. It should almost always be 0 in every report.

Undetermined
This category is used when the incident handler is not yet sure of the incident classification, but wishes to come back and set one later.

Unsolicited Bulk Email
Spam sent from systems reported on the Janet network. This used to be mostly email sent from open relays but is now largely sent through legitimate email accounts on systems compromised with malware.
