

# iDATA – Improving Defences Against Targeted Attack

## Summary

**JULY 2014**

**Disclaimer:**

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

## **iDATA – Improving Defences Against Targeted Attack**

iDATA is a CPNI cyber research programme. The programme consists of a number of projects aimed at addressing threats posed by nation states and state-sponsored actors. iDATA has resulted in a number of outputs for the cyber security community. This document provides a description of the iDATA programme and a summary of the outputs.

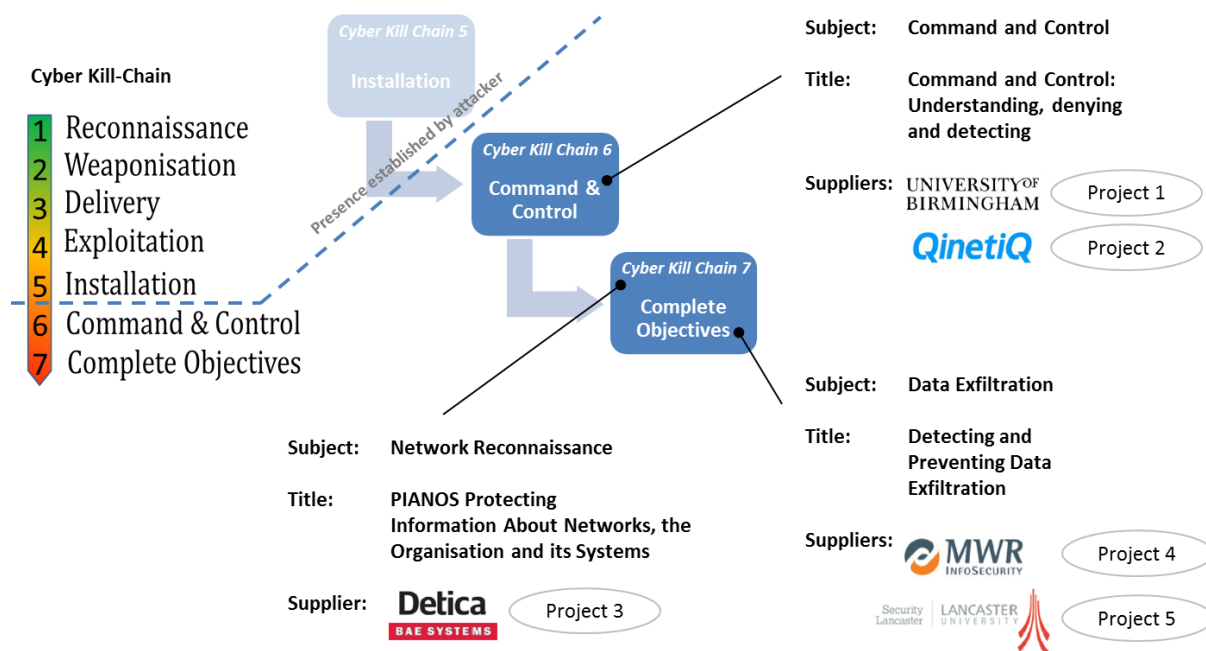
### **Background**

The corporate IT systems of UK organisations are targeted by adversaries seeking to steal information and/or disrupt business operations. iDATA is a CPNI programme of research to address cyber-attacks conducted by adversaries with significant resources and access to sophisticated tools and techniques. Such adversaries are capable of defeating most conventional cyber security measures. The Critical Controls<sup>[1]</sup> and other established advice products place emphasis on preventing attackers from penetrating IT infrastructures. iDATA assumes that infrastructures are already compromised and considers the best approaches for impeding the progress of an attack, making attacks more expensive to conduct and frustrating the efforts of an adversary. To date, iDATA has addressed remotely conducted, espionage-driven, attacks.

### **Projects**

CPNI use a Cyber Kill-Chain<sup>[3]</sup> to help describe the stages of a cyber attack and the areas at which iDATA research are aimed. A Cyber Kill Chain contains a number of stages that an attacker must complete in order to compromise a target infrastructure and achieve objectives. An attack will fail if the defenders of an infrastructure are successful at any one of the stages. As iDATA assumes that an infrastructure is already compromised, the relevant parts of the Cyber Kill Chain are stages 6 and 7.

Figure 1 shows the topics covered (mapped to the Cyber Kill Chain) and shows suppliers for the iDATA work - undertaken between July 2013 and April 2014. In order to capture different perspectives and to work with different datasets, each supplier worked independently on their topic. However, contact between suppliers was encouraged, to ensure sharing of ideas and awareness of efforts in each area.







**Figure 1: iDATA projects, with suppliers, mapped to the Cyber Kill Chain**

## Outputs



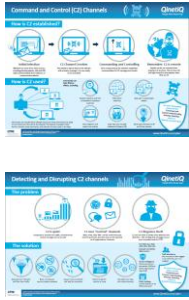
Tables 1,2,3 and 4 present the outputs of each project. In addition to these, all suppliers contributed comments on version 5 of the Critical Security Controls for Effective Cyber Defence<sup>[1]</sup>. A submission has been made to the Council on CyberSecurity<sup>[2]</sup>. All suggestions resulting from the iDATA work will be considered as part of the consensus process during the next update of the Controls.

## References


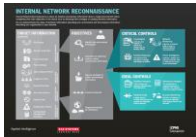

1. Critical Controls for Effective Cyber Defence, *Version 5*, ~Feb 2014, URL: <http://www.cpni.gov.uk/advice/cyber/Critical-controls/>
2. Council on CyberSecurity, *Council on CyberSecurity*, URL: <http://www.counciloncybersecurity.org/practice-areas/technology>
3. Intelligence-Driven Computer Network Defence Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, *Eric M. Hutchins, Michael J. Clopperty, Rohan M. Amin, Ph.D., Lockheed Martin Corporation, 2010*, URL: <http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>

<b>Subject:</b>	Command and Control (C2)	
<b>Title:</b>	Understanding, Denying, Detecting Command and Control	
<b>Supplier:</b>	Birmingham University	
<b>Description:</b>	A review of current cyber-attacks has been conducted and is presented in a technical report. The review highlights significant recent changes in how and why attacks are performed and provides an improved understanding of C2 techniques. This foundational work is presented in the outputs of this work and has resulted in the design of a set of effective counter-measures.	
<b>Main conclusions &amp; recommended measures:</b>	Detect known bad-network activity by monitoring DNS traffic, monitoring IP traffic and inspecting traffic content. Detect anomalous network activity by establishing traffic baselines and evaluating current network activity. Deny C2 by segmenting the network, introducing rate-limiting to slow traffic directed to disreputable or untrusted endpoints. Block unwanted / unused communications mechanisms that may be used to piggy-back C2 activity.	
<b>Outputs:</b>		
	Format	Description
Report		Detailed report including review of published literature on the topic, a round-up of C2 techniques and approaches, real-world examples, tactics to avoid detection, measures to detect and prevent C2.
Key Facts		Document to present recommended measures for detection and denial of C2 channels.
Infographic (Attack)		C2 from an attacker perspective
Infographic (Detect)		C2 from a defence perspective
Web Pages:	<ul style="list-style-type: none"> <li>• <a href="http://c2report.org/report.pdf">http://c2report.org/report.pdf</a></li> <li>• <a href="http://www.cpni.gov.uk/advice/cyber/idata/Command-and-Control-Birmingham/">http://www.cpni.gov.uk/advice/cyber/idata/Command-and-Control-Birmingham/</a></li> </ul>	



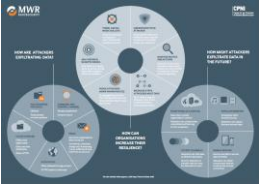

**Table 1: Birmingham University - Command and Control Outputs**

<b>Subject:</b>	Command and Control (C2)	
<b>Title:</b>	Understanding, Denying, Detecting Command and Control	
<b>Supplier:</b>	QinetiQ	
<b>Description:</b>	Research into techniques for detecting advanced attack that evades traditional defence techniques such as Antivirus, IDS, and firewalls, concentrating especially on spotting and blocking C2 (command and control) channels of malware. Detailed investigation into the ways in which advanced malware can be detected, using a combination of theoretical research and practical investigation. Amongst other things, QinetiQ have demonstrated use of Big Data analytics to spot some advanced malware that was resident on an organisation's network.	
<b>Main conclusions &amp; recommended measures:</b>	Direct detection of C2 channels is difficult and subject to change by innovative attackers. Detection is best achieved by looking at communication patters over key nodes and over an extended period rather than 'micro-examination' of specific packets.	
<b>Outputs:</b>		
	Format	Description
Report		Detailed report including C2 techniques and approaches, real-world examples, tactics to avoid detection, measures to detect and prevent C2.
Key Facts		Document to present recommended measures for detection and denial of C2 channels.
Infographics		Detection Infographic and Disruption Infographic
Web pages:	<ul style="list-style-type: none"> <li>• <a href="http://www.cpni.gov.uk/advice/cyber/idata/Command-and-Control-Qinetiq/">http://www.cpni.gov.uk/advice/cyber/idata/Command-and-Control-Qinetiq/</a></li> <li>• <a href="http://www.qinetiq.com/cpni-idata">www.qinetiq.com/cpni-idata</a></li> </ul>	

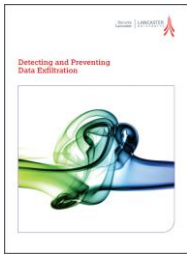

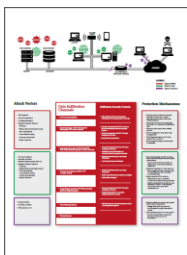

**Table 2: QinetiQ - Command and Control Outputs**

<b>Subject:</b>	Network Reconnaissance	
<b>Title:</b>	PIANOS Protecting Information About Networks, the Organisation and its Systems	
<b>Supplier:</b>	BAE Systems Applied Intelligence (Previously Detica)	
<b>Description:</b>	An insight into the network reconnaissance activities of intruders following successful compromise of a target network. Work includes a look at emerging threats and a number of case studies.	
<b>Main conclusions &amp; recommended measures:</b>	Attackers predominately use legitimate system tools and applications to perform internal network reconnaissance. It's difficult for organisations to restrict use of these tools without hampering legitimate and essential use. Log analysis, network monitoring, and incident response, are highlighted amongst the most important controls to detect and deal with network reconnaissance. Network diodes and software inventories are presented as effective ways of impeding the progress of an attack.	
<b>Outputs:</b>		
	Output	Description
Report		Detailed report including Network reconnaissance techniques and approaches, real-world examples, tactics to avoid detection, measures to impede progress of an attacker.
Infographic		High level view of target technical information within an organisation and what controls can protect it.
Checklist		Advisory checklist to help an organisation assess the strengths and weaknesses of current security measures with respect to defending against network reconnaissance activities.
Web pages:	<ul style="list-style-type: none"> <li>• <a href="http://www.cpni.gov.uk/advice/cyber/idata/PIANOS/">http://www.cpni.gov.uk/advice/cyber/idata/PIANOS/</a></li> <li>• <a href="http://www.baesystems.com/solutions-rai/cyber-security/prepare">http://www.baesystems.com/solutions-rai/cyber-security/prepare</a></li> </ul>	

**Table 3: BAE Systems Applied Intelligence – Network Reconnaissance Outputs**

<b>Subject:</b>	Data Exfiltration	
<b>Title:</b>	Detecting and Deterring Data Exfiltration	
<b>Supplier:</b>	MWR InfoSecurity	
<b>Description:</b>	Current and future exfiltration tactics are covered within this work. Defensive measures are discussed, with the most important measures presented, in order to increase organisational resilience. To illustrate the problem and highlight the solutions, a day in the life of an attacker and a defender is provided. Case studies and further reading are given.	
<b>Main conclusions &amp; recommended measures:</b>	Given the motivation and resources of some attackers and the complexity of modern organisations, protection of digital assets cannot be guaranteed. A comprehensive defence-in-depth strategy is needed to detect and deter data exfiltration. Such defences can be expensive and the need for such a strategy must be understood by top layers of management. A successful strategy will increase costs for the attacker and minimise potential impact on an organisation. Defensive measures include; ensuring a network is manageable, logging throughout an organisation, auditing accounts, using data loss prevention, using anti-virus, using intrusion detection systems, host hardening and honeypots.	
<b>Outputs:</b>		
	Download	Intended Audience
Technical Report		Detailed report including Data Exfiltration techniques and approaches (current and future), real-world examples, tactics to avoid detection, measures to detect and prevent Data Exfiltration.
Executive Report		High level report explaining the topic, and the importance of implementing measures to prevent Data Exfiltration.
Infographic		Graphics on Data Exfiltration and measures to prevent it.
Animation		3 minute animation to present the topic of Data Exfiltration to a non-technical audience. Designed to promote other guidance products.
Web pages:	<ul style="list-style-type: none"> <li>• <a href="http://www.cpni.gov.uk/advice/cyber/idata/Data-Exfiltration-MWR/">http://www.cpni.gov.uk/advice/cyber/idata/Data-Exfiltration-MWR/</a></li> <li>• <a href="https://www.mwrinfosecurity.com/practice-areas/cyber-defence/">https://www.mwrinfosecurity.com/practice-areas/cyber-defence/</a></li> </ul>	

**Table 4: MWR InfoSecurity – Data Exfiltration Outputs**

<b>Subject:</b>	Data Exfiltration	
<b>Title:</b>	Detecting and Preventing Data Exfiltration	
<b>Supplier:</b>	Lancaster University	
<b>Description:</b>	A systematic review of relevant literature, collection of case-studies and production of incident trees have all been completed in order to improve understanding of the topic of data exfiltration. The consequences of new and emerging technologies and business practices have been considered with respect to the impact on data exfiltration modes.	
<b>Main conclusions &amp; recommended measures:</b>	Areas for increased effort include; post exfiltration recovery, defensive measures in relation to business needs, and the need for data exfiltration detection and prevention as opposed to information protection.	
<b>Outputs:</b>		
	Format	Description
Technical Report		Detailed report including Data Exfiltration techniques and approaches (current and future), real-world examples, tactics to avoid detection, measures to detect and prevent Data Exfiltration.
Executive Report		High level report explaining the topic, and the importance of implementing measures to prevent Data Exfiltration.
Infographic		Graphics on Data Exfiltration and measures to prevent it.
Cyber-Wheel		Tool to suggest approaches to detection and prevention of data exfiltration.
	Intended Audience	
		Technical / Academic
		Executive / Technical Management
		Executive / Non technical
		Technical

**Table 5: Lancaster University – Data Exfiltration Outputs**