INFS 5115 Security Principles

Data Exfiltration

University of South Australia

School of
Information Technology
and Mathematical Sciences

Data Exfiltration

- In this module, we will review a definition of data exfiltration and consider the nature of these types of attacks.
- We will also contrast two different taxonomies that classify data exfiltration.
- The MITRE ATT&CK matrix will be used as the basis for discussion of some of the techniques used by adversaries for data exfiltration and related tactics.
- Finally, we will review a case study involving exfiltration.

Data Exfiltration

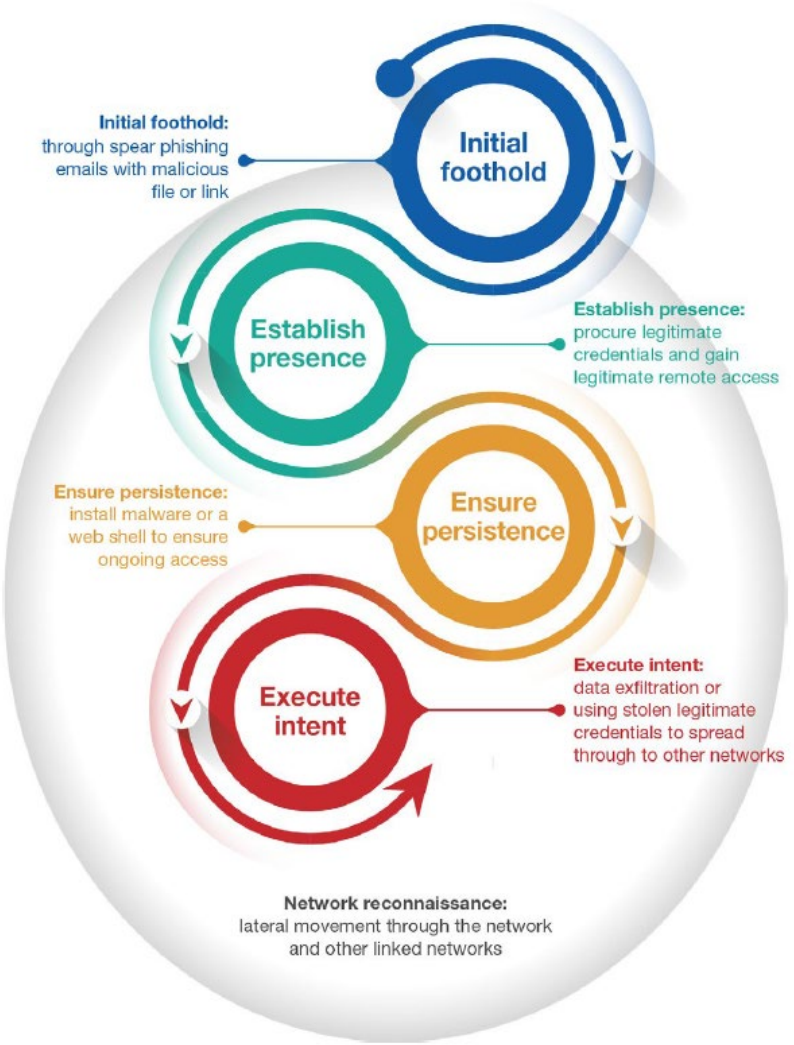
Definition

- Data Exfiltration
  - *An unauthorized transport of data from within an organization to an external recipient or destination[1].*

[1] SANS cited in Schlicher, B, MacIntyre, L, and Abercrombie, R 2016, 'Towards reducing the data exfiltration surface for the insider threat', in proceedings of 49th Hawaii International Conference on System Sciences (HICSS), IEEE, pp. 2749-2758.

ACSC 2016 Threat Report

- *Execute Intent*
  - Often includes data exfiltration.



Source: Australian Cyber Security Centre 2016, ACSC Threat Report, Commonwealth of Australia. p. 34.

Data Exfiltration

Taxonomy

In 2006, Giani, Brek and Cybenko proposed a taxonomy of exfiltration methods. The taxonomy consists of three main categories of exfiltration:

Network

The authors describe using usually benign network exfiltration methods such as HTTP and SMTP.
They also describe known malicious network attacks (e.g. malware, man-in-the-middle attacks).

Physical

Again, the authors subcategorise exfiltration techniques into those that are usually benign and known malicious in nature.

The former might include printing devices and USB storage media, while the latter might include device (e.g. laptop) theft

Cognitive

Techniques where the victim shares the data with the attacker.

This includes social engineering and shoulder surfing attacks.

Giani, A, Berk, V, and Cybenko, G 2006, 'Data exfiltration and covert channels' in proceedings of Defense and Security Symposium, International Society for Optics and Photonics, pp. 620103-1-620103-11.

Data Exfiltration

Taxonomy

A contrasting taxonomy, based upon the communication channel mechanism, was proposed by Schlicher, MacIntyre and Abercrombie in 2016.

Overt

Authorised communication that is observable and identifiable.

Encryption (e.g. TLS) may be used to preserve privacy.

Tunnelled

Unauthorised communication that would ordinarily be blocked.

Exfiltration is achieved via an overt channel, but the data is intentionally cloaked to masquerade as legitimate.

Covert

Encoded in the payload of overt channel communications.

May be embedded in parts of the network or application protocol.

Steganographic techniques may be used to hide the data being exfiltrated

Schlicher, B, MacIntyre, L, and Abercrombie, R 2016, 'Towards reducing the data exfiltration surface for the insider threat', in proceedings of 49th Hawaii International Conference on System Sciences (HICSS), IEEE, pp. 2749-2758.

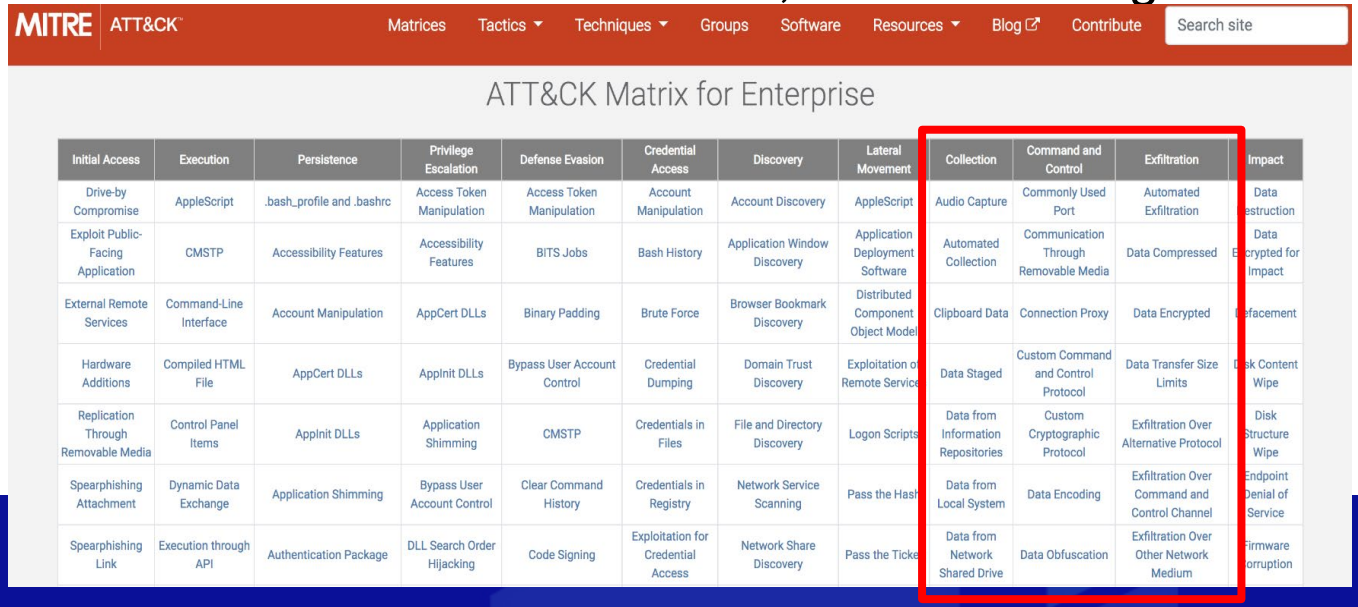
Data Exfiltration Process

- Sood and Enbody describe data exfiltration within the context of two phases:
  1. Data Gathering
  2. Data Transmission

Sood, A, and Enbody, R 2014, 'Targeted cyber attacks: multi-staged attacks driven by exploits and malware', Syngress.

Data Exfiltration Process

- We will focus on the **Collection** and **Exfiltration** tactics, with a brief discussion of Command and Control, in the following slides.



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data estruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data crypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	efacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Service	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	sk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware orruption

MITRE, 'Adversarial Tactics, Techniques & Common Knowledge', The MITRE Corporation, https://attack.mitre.org/wiki/Main_Page.

MITRE ATT&CK

Collection

- Before data can be exfiltrated from within an organisation, it is necessary for the adversary to collect the data.
- MITRE describes the Collection tactic as consisting of *techniques used to* ***identify and gather information, such as sensitive files, from a target network prior to exfiltration****. This category also covers locations on a system or network where the adversary may look for information to exfiltrate.*

See Activity - Data Exfiltration Demo in Week 11

MITRE, 'Collection', The MITRE Corporation, https://attack.mitre.org/wiki/Collection.

MITRE ATT&CK

Exfiltration

A summary of the adversary techniques utilised during the Exfiltration phase outlined in ATT&CK follow:

Data Compressed	Data compression can aid exfiltration by helping to reduce the amount of data transferred and make a multitude of files more portable. Custom libraries can be used, however it is also common to utilise standard compression utilities. Compression can also act as a weak form of obfuscation, preventing plain text analysis by network security tools.
Data Encrypted	Data encryption provides a much stronger form of obfuscation as defenders, and the security technologies operating on their behalf, are generally unable to view the data being transferred without access to the encryption keys.
Data Transfer Size Limits	Adversaries may try to limit exfiltrated data to fixed size chunks to avoid triggering detection thresholds.

MITRE, 'Exfiltration', The MITRE Corporation, https://attack.mitre.org/wiki/Exfiltration.

MITRE ATT&CK

Exfiltration

Automated Exfiltration

- Similar to automated collection, automated exfiltration commonly relies upon scripts to trigger the exfiltration of data that has been collected.
- It may be used in combination with other exfiltration techniques.

Scheduled Transfer

- Exfiltration performed at certain times of the day or intervals.
- May help to blend with regular traffic patterns.
- May also be combined with other exfiltration techniques.

Exfiltration Over Physical Medium

Physical media may be particularly useful when attempting to exfiltrate data from air-gapped systems.
Physical media can include devices introduced by a user.
For example, USB media, mobile phones and other removable storage and/or processing devices.
The physical media may be used as the final exfiltration point or a ‘hop’ to other disconnected systems.

MITRE, ‘Exfiltration’, The MITRE Corporation, https://attack.mitre.org/wiki/Exfiltration.

MITRE ATT&CK

Exfiltration

Exfiltration Over Other Network Medium

- Utilising a separate network connection from the main enterprise network may be a more viable exfiltration medium for an adversary.
- Examples include local Wi-Fi or Bluetooth networks, if the adversary is within a suitable physical proximity.
- Other network paths, such as 4G mobile network connections, may also be used if available (e.g. if a mobile device is connected).

Exfiltration Over Command and Control (C&C) Channel

- Data exfiltration may be orchestrated via the C&C channel being used by the adversary to control the malware or other toolkit they are utilising for the exfiltration.
- More detail regarding C&C will be provided on the following slides.

Exfiltration Over Alternative Protocol

Exfiltration may also be conducted over an entirely different protocol to that being used for C&C.
This secondary protocol would likely be used to communicate with a different remote server to the C&C host.
Other channels may include using a cloud service as the exfiltration target.

MITRE, 'Exfiltration', The MITRE Corporation, https://attack.mitre.org/wiki/Exfiltration.

MITRE ATT&CK

Command and Control

- Remotely controlling data exfiltration can be achieved via Command and Control (C&C) infrastructure.
- MITRE notes that the Command and Control *tactic represents* ***how adversaries communicate with systems under their control*** *within a target network.*
- The following slides address some of the C&C techniques used, with a focus on those relating to exfiltration.

MITRE, 'Command and Control', The MITRE Corporation, https://attack.mitre.org/wiki/Command and Control.

MITRE ATT&CK

- Commonly Used vs Uncommonly Used Ports
  - Adversaries may seek to conduct C&C activities over commonly used ports to avoid firewall rules and detection systems.
  - Commonly used ports may include standard ports for HTTP, HTTPS, SMTP and DNS.
  - Internal connections may also be established using standard ports for protocols such as RPC, SSH and RDP.
  - Conversely, attackers may also try to use uncommon ports, in the hope that the network security infrastructure is misconfigured and allows this traffic to reach the internet.

MITRE, 'Command and Control', The MITRE Corporation, https://attack.mitre.org/wiki/Command and Control.

MITRE ATT&CK

Command and Control

- In addition to common and uncommon ports, adversaries may leverage both common and custom protocols for C&C purposes.
- This includes application layer protocols (e.g. HTTP, FTP) and Non-Application Layer Protocols (e.g. ICMP, UDP).
- Data Obfuscation and Encoding are also commonly used as part of C&C channels (e.g. Base64 encoding).

MITRE, 'Command and Control', The MITRE Corporation, https://attack.mitre.org/wiki/Command and Control.

Index	Binary	Char	Index	Binary	Char	Index	Binary	Char	Index	Binary	Char
0	000000	A	16	010000	Q	32	100000	g	48	110000	w
1	000001	B	17	010001	R	33	100001	h	49	110001	x
2	000010	C	18	010010	S	34	100010	i	50	110010	y
3	000011	D	19	010011	T	35	100011	j	51	110011	z
4	000100	E	20	010100	U	36	100100	k	52	110100	0
5	000101	F	21	010101	V	37	100101	l	53	110101	1
6	000110	G	22	010110	W	38	100110	m	54	110110	2
7	000111	H	23	010111	X	39	100111	n	55	110111	3
8	001000	I	24	011000	Y	40	101000	o	56	111000	4
9	001001	J	25	011001	Z	41	101001	p	57	111001	5
10	001010	K	26	011010	a	42	101010	q	58	111010	6
11	001011	L	27	011011	b	43	101011	r	59	111011	7
12	001100	M	28	011100	c	44	101100	s	60	111100	8
13	001101	N	29	011101	d	45	101101	t	61	111101	9
14	001110	O	30	011110	e	46	101110	u	62	111110	+
15	001111	P	31	011111	f	47	101111	v	63	111111	/
Padding		=									

Base64 Encoding

How would the following three bytes be encoded using Base64?

00111101 00100101 10000011

001111 01 0010 0101 10 000011

P S W D

Source:
https://en.wikipedia.org/wiki/Base64

MITRE, 'Command and Control', The MITRE Corporation, https://attack.mitre.org/wiki/Command and Control.

Data exfiltration example

- Many organisations employ intrusion detection and prevention systems that analyse network traffic to detect patterns that may represent malicious activity, including data exfiltration.
- Often, these security tools focus on more commonly used techniques and protocols for data transfer (e.g. HTTP, FTP and SMB).
- Jakober discusses the operation of Domain Name Service (DNS)-based data exfiltration.
- This exfiltration method utilises DNS requests to exfiltrate data, which is often possible from devices within secured network segments.

Jakober, L 2017, '20 Years of DNS Data Exfiltration: Why, How, and What's Next?', Akamai, https://blogs.akamai.com/2017/06/-20-years-of-dns-data-exfiltration-why-how-and-whats-next.html.

Data exfiltration example

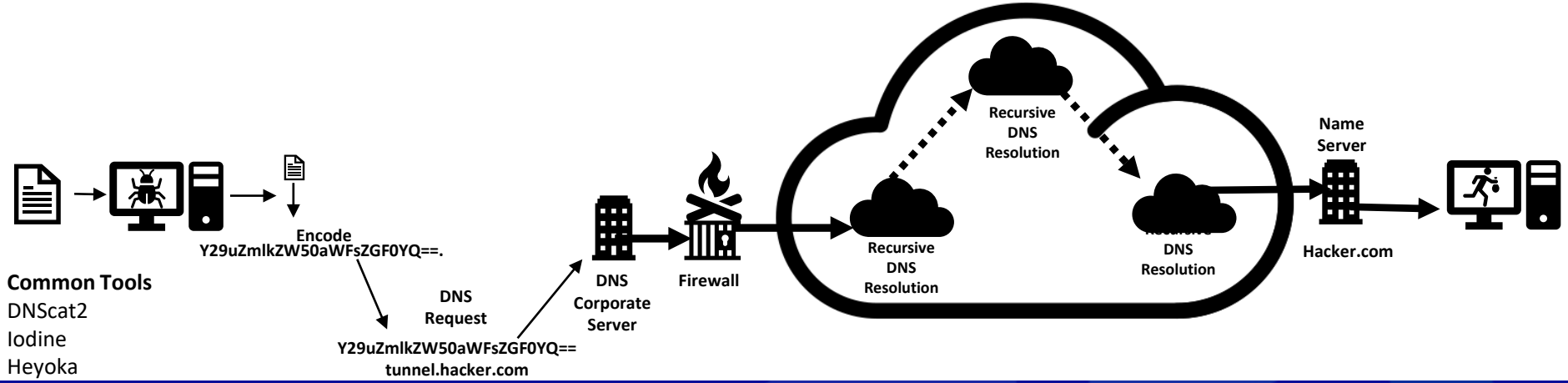
- Many core functions of contemporary operating systems rely upon DNS, particularly in enterprise environments.
- For example, it is often used to facilitate authentication, updates and network services sharing.
- DNS has a number of purposes, however one of its core purposes is to translate (domain) names to IP addresses.
- DNS is often available in some form to every network connected device within an enterprise.

Data Exfiltration example

Step 1 - The attacker purchases a domain name such as hacker.com

Step 2 - The attacker configures the domain's name servers to his own DNS server.

Step 3 - The attacker delegates a subdomain, such as "tunnel.hacker.com" and configures his machine as the subdomain's authoritative DNS server.



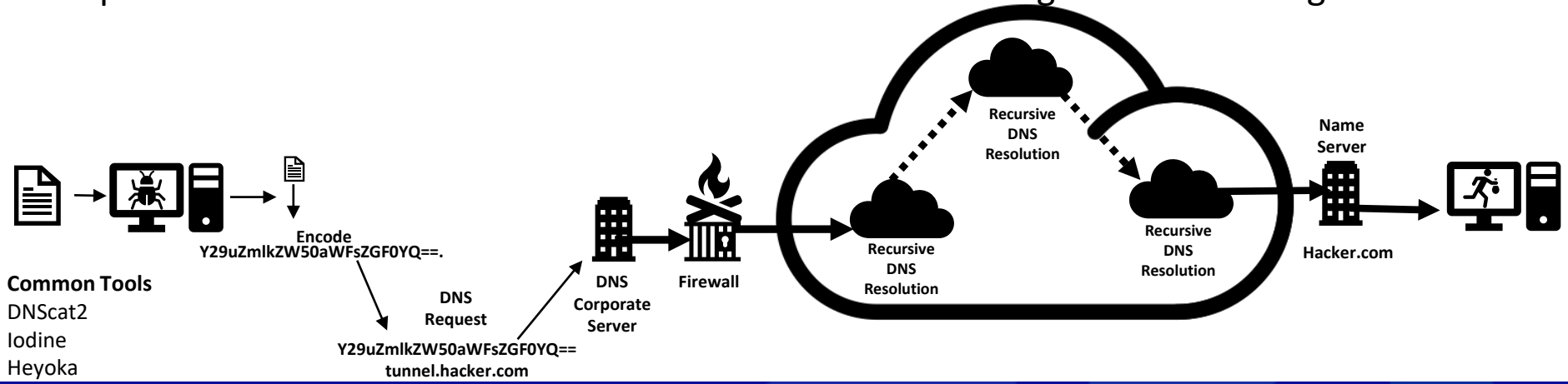
Jakober, L 2017, '20 Years of DNS Data Exfiltration: Why, How, and What's Next?', Akamai, https://blogs.akamai.com/2017/06/-20-years-of-dns-data-exfiltration-why-how-and-whats-next.html.

Data Exfiltration example

Step 4 - Any DNS request made by the victim to “{data}.tunnel.hacker.com” will end up reaching the attacker’s machine.

Step 5 - The attacker’s machine encodes a response that will get routed back to the victim’s machine.

Step 6 - A bidirectional data transfer channel is achieved using a DNS tunneling tool.



Jakober, L 2017, ‘20 Years of DNS Data Exfiltration: Why, How, and What's Next?’, Akamai, https://blogs.akamai.com/2017/06/-20-years-of-dns-data-exfiltration-why-how-and-whats-next.html.

Discussion (CA #4)

Answer the following question in relation to the article by Crozier & Corner (2017):

- Describe the techniques and tools used by the attackers to exfiltrate data, with reference to the categories described in the seminar.
- What lessons can organisations learn from this incident?
- Identify at least five tactic-specific recommendations from the MITRE ATT&CK framework for mitigating data exfiltration.

Crozier, R, Corner, S 2017, 'Hacked Aussie Defence firm lost fighter jet, bomb, ship plans', *itnews*, Oct 12, <https://www.itnews.com.au/news/hacked-aussie-defence-firm-lost-fighter-jet-bomb-ship-plans-475211>