intergence
CONSULTING

Security Assessment Report for

Sample Company

Client Confidential

Powered by stratiam
Gives you Clarity

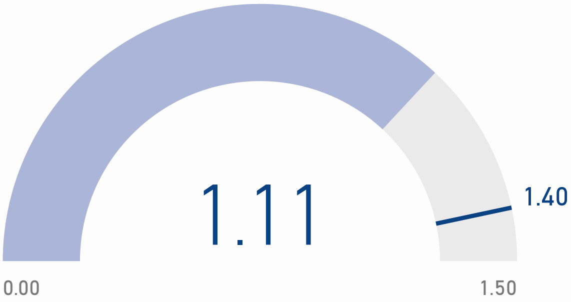
☎ +44 (0)845 226 4167 ✉ contact@intergence.com www.intergence.com

Assessment Summary

This assessment gives an insight into internal and external health. Very few companies are perfect in terms of security, therefore it is important to compare and communicate practices with other companies similar to yourselves. To help identify how your company compares with others that have had an assessment, metadata has been collected to offer analytics on both 'Threats per Device' and 'Breached Credentials'. Although this doesn't indicate a definite difference in overall security, it should help highlight a baseline which can be used a comparison.

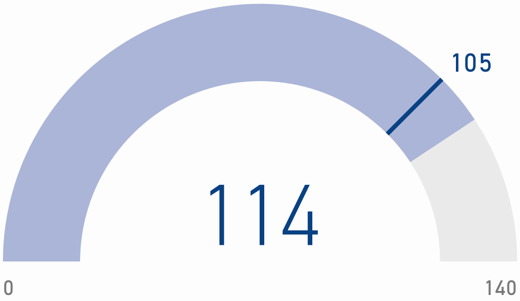
Difference from Global Averages

-0.3 Threats per Device



Sample Company Total

+9 Breached Credentials



Sample Company Total

6M
Files Scanned

65
Devices scanned

72
Threats Discovered

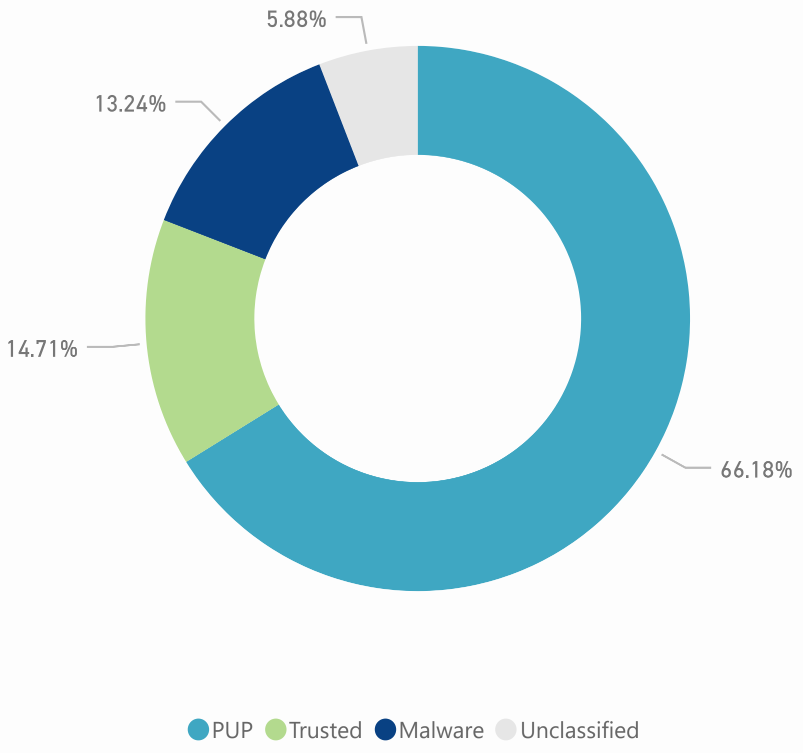
114
Credentials Discovered

stratiam
Gives you Clarity

Internal Health

During this assessment, 6256778 files were analysed by an algorithm, built using machine learning methods to accurately determine the difference between a malicious executable and a safe executable. This algorithm inspects over 6 million characteristics of a file, giving an extremely high degree of efficacy. Unclassified files have not yet received a formal classification, as they have been seen for the first time only recently.

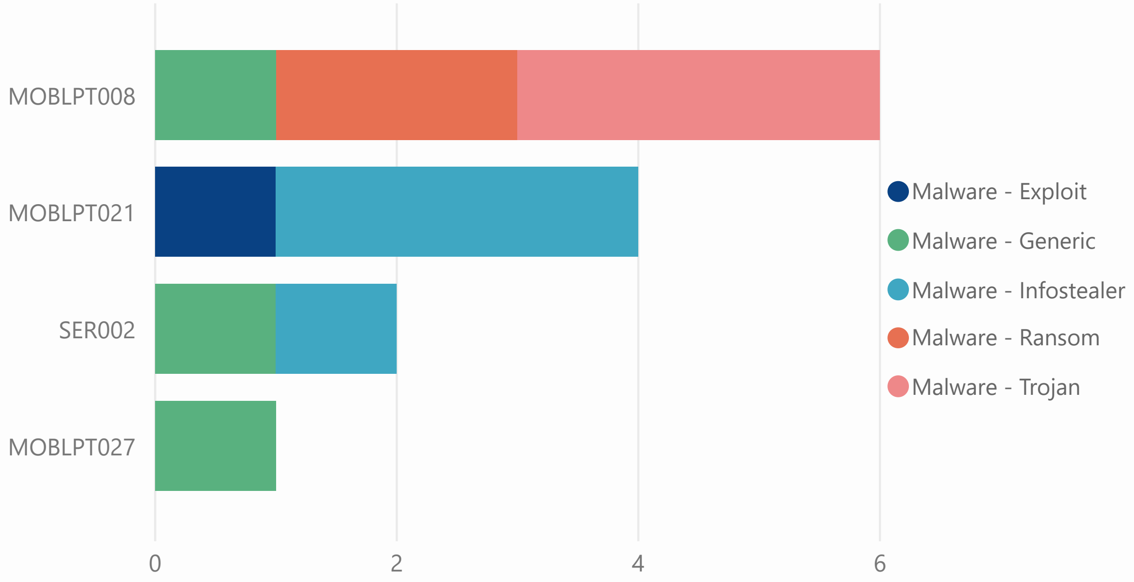
4	45	9
Unclassified	Potentially Unwanted Applications	Classified Malware



Internal Health - Malware

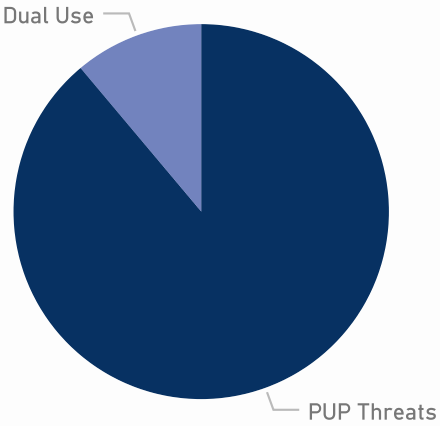
Malware is an executable which can cause your machine damage. These files may not have run, but please contact your sales representative if you feel you have been breached and would like to start identifying and reversing damage caused. The Trojan classification identifies a more generic threat, which hides itself behind the facade of a genuine file.

Count	Malware Group
3	Malware - Trojan
2	Malware - Ransom
4	Malware - Infostealer
3	Malware - Generic
1	Malware - Exploit
13	

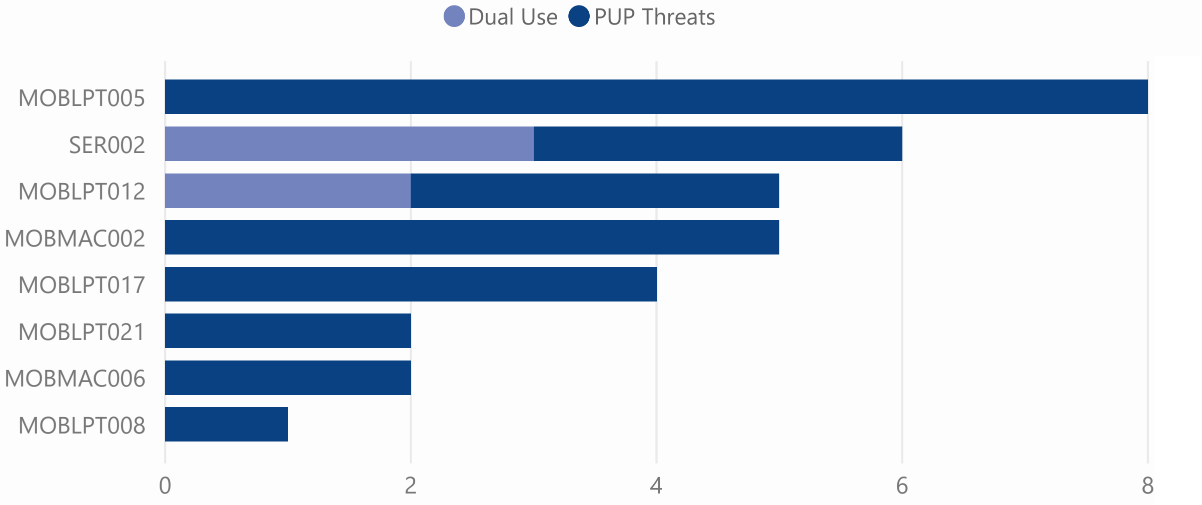


Internal Health - PUPs

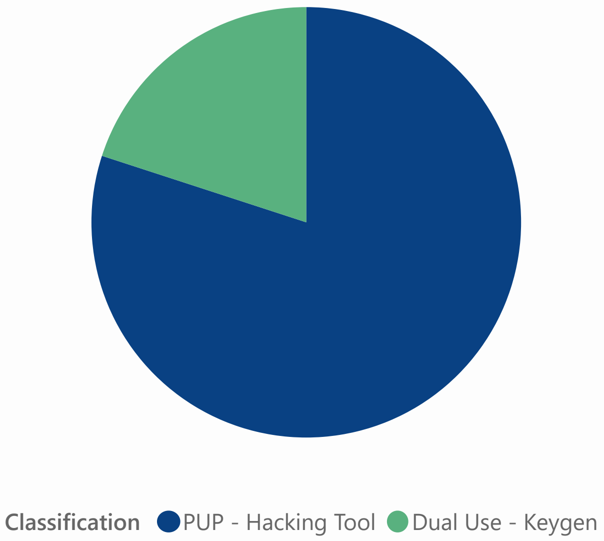
A PUP, or potentially unwanted program consists of executable files which may not seem immediately like a threat, but often in the wrong hands could be used maliciously, or others which may escalate to become a more serious threat. The most common PUP type is adware. Adware is seen as a gateway to malware, due to its untrusted communication with unknown external sources which could easily be compromised. This report highlights dual use tools which may be used legitimately to assist IT admins perform their job but could also be used by an attacker, so knowing what type of devices they reside upon is essential.

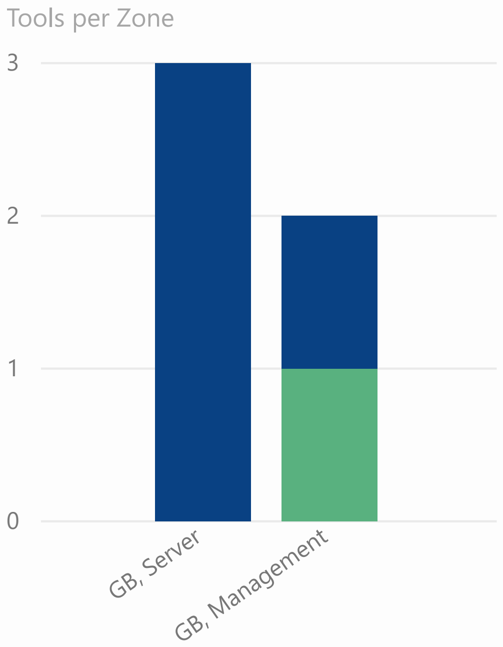


Count of PUP Grouping	PUP Grouping ▲
5	Dual Use
40	PUP Threats
45	



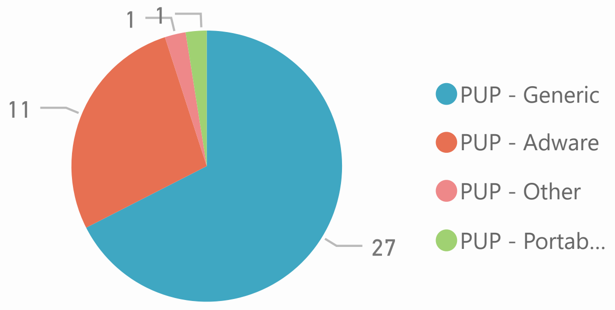
Internal Health - Dual Use Tools

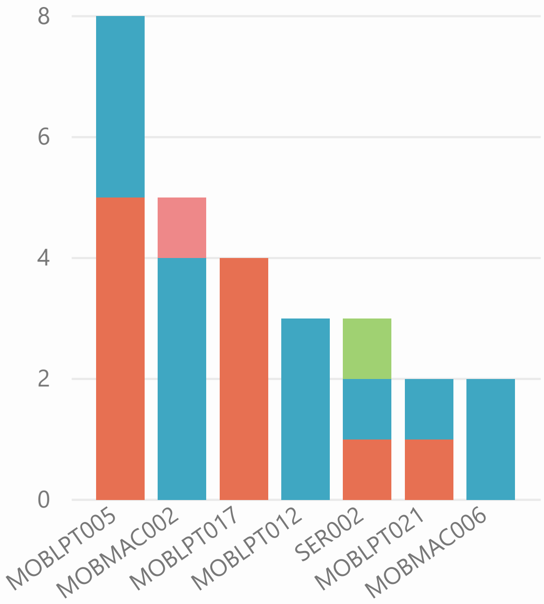




Classification	File Name	DeviceName	Zones
Dual Use - Keygen	E8FBEC25DB4F9D95B5E8F41CCA51A4B32BE8674A4DEA7A45B6F7AEB22DBC38DB	MOBLPT012	GB, Management
PUP - Hacking Tool	netcat.exe	MOBLPT012	GB, Management
PUP - Hacking Tool	mysql (deleted b'eca73dddd34847f245d45f6fdacff8ef').exe	SER002	GB, Server
PUP - Hacking Tool	netcat (deleted b'1c226f535c355de68179f42f681995b4').exe	SER002	GB, Server
PUP - Hacking Tool	netpass (deleted b'afd71236f1820ee77a0035de8a198207').exe	SER002	GB, Server

Internal Health - PUP Threats





Device Name	Last Reported User	PUP Count
MOBLPT005	Williemae Mangrum	8
MOBMAC002	Miss Pierre	5
MOBLPT017	Deloris Choice	4
MOBLPT012	Eduardo Skoglund	3
SER002	ADMINISTRATOR	3
MOBLPT021	Kurt Perryman	2
MOBMAC006	Carmelina Albanese	2
MOBLPT008	ADMINISTRATOR	1
MOBLPT014	Cruz Crosson	1
MOBMAC004	Leisa Bushnell	1
MOBMAC005	Venus Nevin	1
MOBMAC007	Loriann Hague	1
MOBMAC008	Deirdre In	1

Device Risk

Devices listed below have threats which show deceptive and data loss capabilities, respectively. Deception could indicate improper labeling, hidden sections or running invisibly, while destruction could include files which delete files, terminate processes or registry manipulation.

Device Name	Deception Risk
MOBLPT005	3 - High
MOBLPT008	3 - High
MOBLPT012	3 - High
MOBLPT014	3 - High
MOBLPT021	3 - High
SER002	3 - High
MOBLPT017	2 - Medium
MOBMAC002	2 - Medium
MOBLPT024	1 - Low
MOBLPT027	1 - Low

Device Name	Destruction Risk
MOBLPT005	3 - High
MOBLPT008	3 - High
MOBLPT012	3 - High
MOBLPT014	3 - High
MOBLPT017	3 - High
MOBLPT021	3 - High
SER002	3 - High
MOBMAC002	2 - Medium
MOBLPT024	1 - Low
MOBLPT027	1 - Low

Devices listed below have threats which show collection and data loss capabilities, respectively. Collection risk indicates files present of capabilities which could potentially collect data, while data loss risk represents characteristics which seem to indicate exfiltration of this data.

Device Name	Collection Risk
MOBLPT005	3 - High
MOBLPT008	3 - High
MOBLPT012	3 - High
MOBLPT014	3 - High
MOBLPT017	3 - High
MOBLPT021	3 - High
SER002	3 - High
MOBMAC002	2 - Medium
MOBLPT024	1 - Low
MOBLPT027	1 - Low

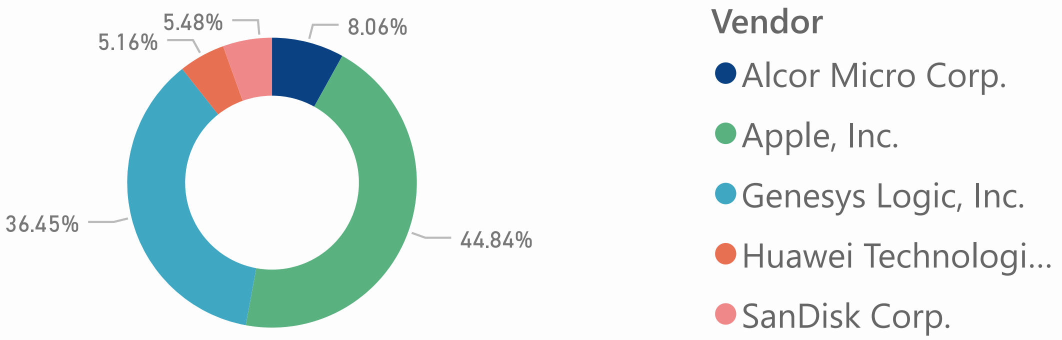
Device Name	Data Loss Risk
MOBLPT005	3 - High
MOBLPT012	3 - High
MOBLPT021	3 - High
SER002	3 - High
MOBLPT008	2 - Medium
MOBLPT014	2 - Medium
MOBLPT017	2 - Medium
MOBMAC002	2 - Medium
MOBLPT024	1 - Low
MOBLPT027	1 - Low

Removable USB Devices

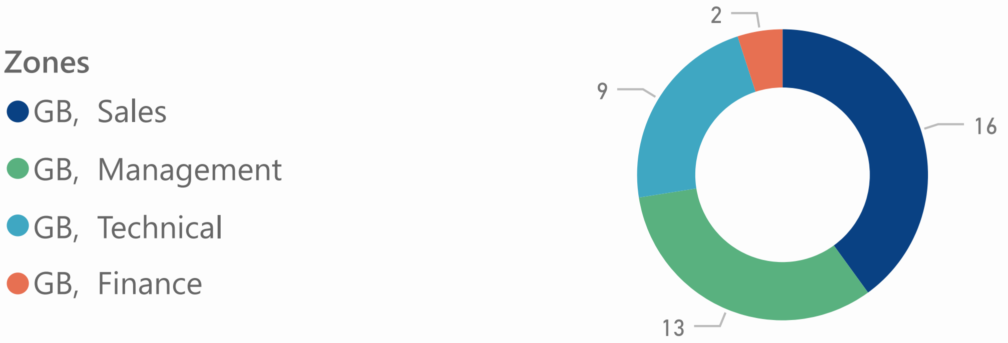
During this assessment, input of USB storage devices were tracked. Storage devices could both be seen as a security threat if they were to contain malware and/or portable applications, while also being a method to exfiltrate data by attackers with access to the physical target machines. If company intelectual property is stored within a computer system and access through USB devices is allowed, it is recommended that a USB control system , or a data loss prevention system to cover multiple exfiltration methods is investigated.

Devices which had USB Input	Unique USB Storage Devices	Total USB Storage Devices Tracked
14	30	353

Top 5 USB Storage Vendors



Count of Serial Number by Zones

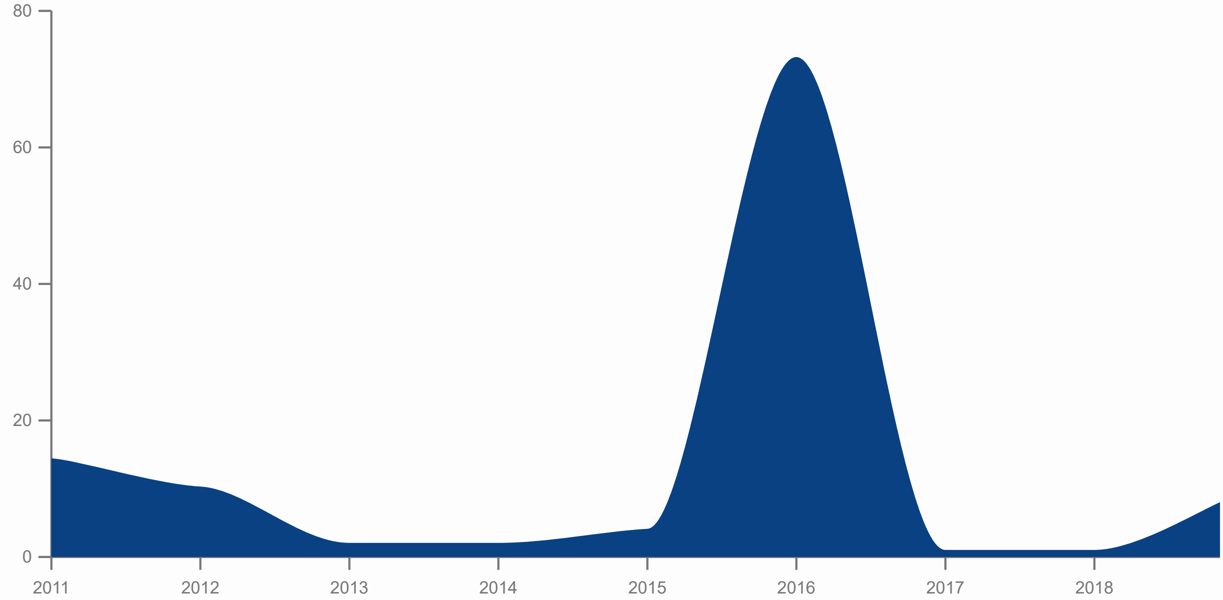


External Health

Using detailed dark web analysis, Sample Company's domain was investigated using a combination of HUMINT and automation, which discovered how many compromised data types existed upon the dark web. The data types could exist as credentials or PII data, and leaves both the company and employee vulnerable to the potential of further breach. Good password policy should be enforced to reduce the risk of breached credentials being reused for company logins, or a secure single sign-on solution to remove the password requirements.

Identified Breaches	Total Compromised Accounts	Unique Compromised Accounts	Identified Passwords
3	114	99	94

Credentials Exposure over Time

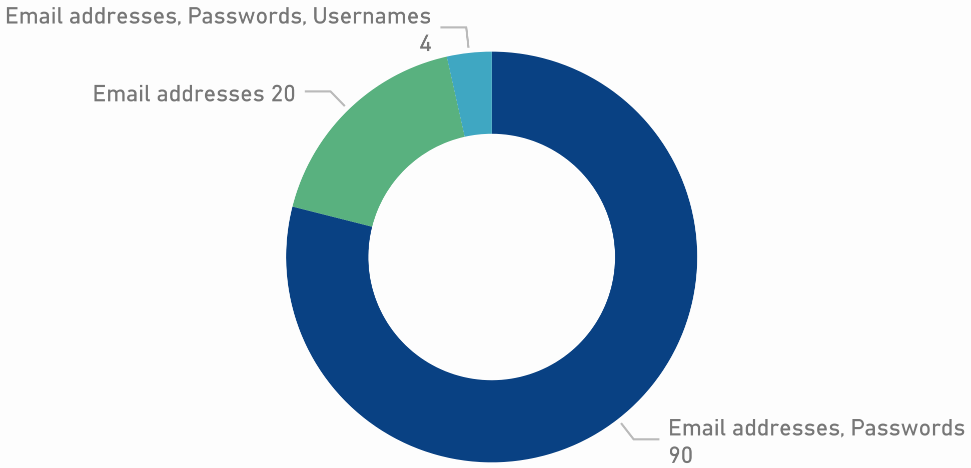


External Health

These credentials are an example of what were found within the external health report. If you would like the full data, please contact your sales representative. By being a recipient of this report, you commit to the responsibility of not using this data maliciously, and handling it with care.

Breach	Email Address	Password	Compromised Data
LinkedIn	realdata02@sample.com	breakm3!	Email addresses, Passwords
LinkedIn	realdata01@sample.com	chelsea123	Email addresses, Passwords
TalkTalk	realdata06@sample.com	H3isenburg	Email addresses, Passwords, Usernames
Secure-It	realdata04@sample.com	K01carp99!	Email addresses, Passwords, Usernames
Secure-It	realdata05@sample.com	password	Email addresses, Passwords, Usernames

...109 others found, contact your sales rep. for details on acquiring the full list.


Email addresses, Passwords, Usernames 4
Email addresses 20
Email addresses, Passwords 90