Powered by

BlackBerry | CYLANCE

intergence

Intergence

Security Assessment

DATASHEET

Benefits

- Validation of existing endpoint security controls.
- Identification of impacted systems and any changes the malware may have made to them, enabling a more effective response and containment.
- Early indication of darknet activity that could lead to future breach.

Contact Intergence to discuss an assessment of your malware status.

Security Assessment

Today's malware is highly sophisticated, targeted and complex and is the root cause of many damaging security breaches.

A Security Assessment is a vital component of effective IT risk management and incident response programs. It helps to understand the extent of malware infection and incidents to rapidly identify additional hosts or systems that could be affected.

Intergence Security Assessment efficiently aids the identification of malware in environments as well as providing strategic and tactical recommendations to provide guidance and help reduce risk.

Service Overview

The primary focus of the Security Assessment is to provide a point-in-time report into the current end-point estate with a view to understanding if existing technical controls are providing adequate visibility and protection.

In addition to the desktop insight, we will also provide an indication of any Darknet activity associated with the domain of the organisation.

Delverables

The deliverables of the assessment include:

- Full report, including visibility of both internal and external health
- View of Administrator Tools, and where they are located within the environment
- Based on the threats that are discovered, visibility of the highest 'at risk' devices
- Visibility of USB storage devices plugged-in throughout the duration of the service
- Visibility of any classified malware
- Visibility of any full credentials found upon the Darkweb for the customer's domain (Max. 5)
- Insights into the breaches which have affected users within the primary domain

Depending on findings during the assessment, we can offer additional services ranging from remediation, incident response and managed services.

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

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

Powered by

BlackBerry | CYLANCE

intergence

Intergence

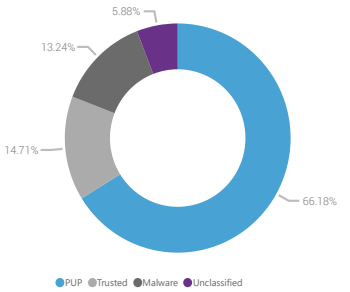
Security Assessment

DATASHEET

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.

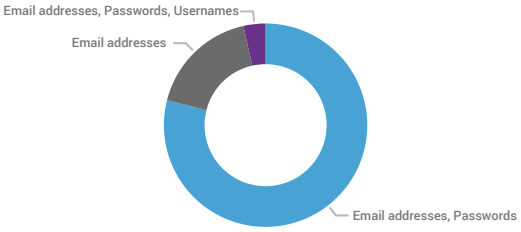
4	45	9
Unclassified	Classified Malware	Potentially Unwanted Applications



External Health

These credentials are an example of what were found within the external health report.

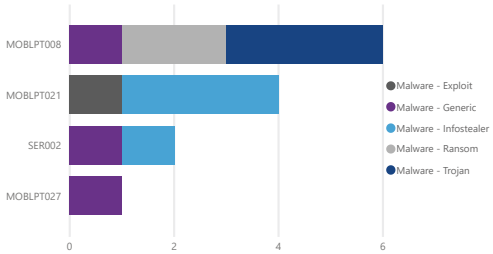
Breach	Email Address	Password	Compromised Data
LinkedIn	realdata02@sample.com	breakm3!	Email addresses, Passwords
	realdata01@sample.com	chelsea123	Email addresses, Passwords
TalkTalk	realdata06@sample.com	H3isenburg	Email addresses, Passwords, Usernames
Secure-It	realdata04@sample.com	K01carp99!	Email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



Internal Health - Malware

Malware is an executable which can cause your machine damage.

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

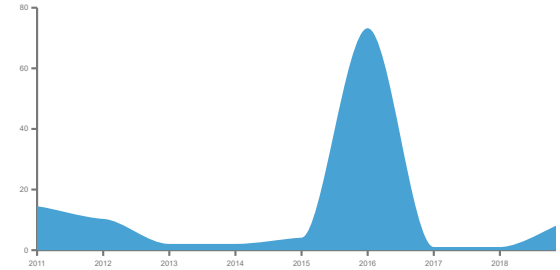


External Health

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.

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

Credentials Exposure over Time



+44 (0)845 226 4167

contact@intergence.com

www.intergence.com