Corptek LLC SOLUTIONS

Security Assessment

Outbound Security Report

Scan Date: 4/1/2014

Prepared for
Company AAA

Prepared by
Corptek Solutions, LLC

3/26/2016

Table of Contents

1 - Summary

This report is designed to point out issues that were detected while performing the security assessment. This includes issues found in the areas of system leakage, system control, and user control.

Assessment Summary	
# End-points in Data Collection	3
System Leakage	
# End-points with protocol leaks	3
# Protocols leaked by all tested end-points	15
System Controls	
# Partially restricted protocols	0
# Unrestricted protocols	0
User Controls	
# Partially restricted sites	0
# Unrestricted sites	13

2 - System Leakage

Users inside your network are able to access and transmit to the following ports and protocols:

Windows Protocols

Internal Windows protocols in most cases should not be allowed to leave the local network

Protocol	Common Name	End Point(s)
135 / TCP	MS RPC	DC01 UTIL01
135 / UDP	MS RPC	DC01 UTIL01
137 / TCP	NetBIOS/IP	DC01 UTIL01
137 / UDP	NetBIOS/IP	DC01 UTIL01
138 / TCP	NetBIOS/IP	DC01 UTIL01
139 / TCP	NetBIOS/IP	DC01 UTIL01
139 / UDP	NetBIOS/IP	DC01 UTIL01

System Management Protocols

The following protocols can be leaked externally to an unknown source on the Internet. These protocols can convey security related information regarding network devices and be used to export configuration information.

Protocol	Common Name	End Point(s)
No issues detected		

Exploitable Protocols

The following protocols have been known to leak information or can be used to create “phone home” scenarios that may permit access to your internal network.

Protocol	Common Name	End Point(s)
6661 / TCP	Internet Relay Chat (IRC)	DC01 SE-Dresden UTIL01
6662 / TCP	Internet Relay Chat (IRC)	DC01 SE-Dresden UTIL01
6663 / TCP	Internet Relay Chat (IRC)	DC01 SE-Dresden UTIL01
6664 / TCP	Internet Relay Chat (IRC)	DC01 SE-Dresden UTIL01
6665 / TCP	Internet Relay Chat (IRC)	DC01

Protocol	Common Name	End Point(s)
		SE-Dresden UTIL01
6666 / TCP	Internet Relay Chat (IRC)	DC01 SE-Dresden UTIL01
6667 / TCP	Internet Relay Chat (IRC)	DC01 SE-Dresden UTIL01
6668 / TCP	Internet Relay Chat (IRC)	DC01 SE-Dresden UTIL01

3 - System Controls

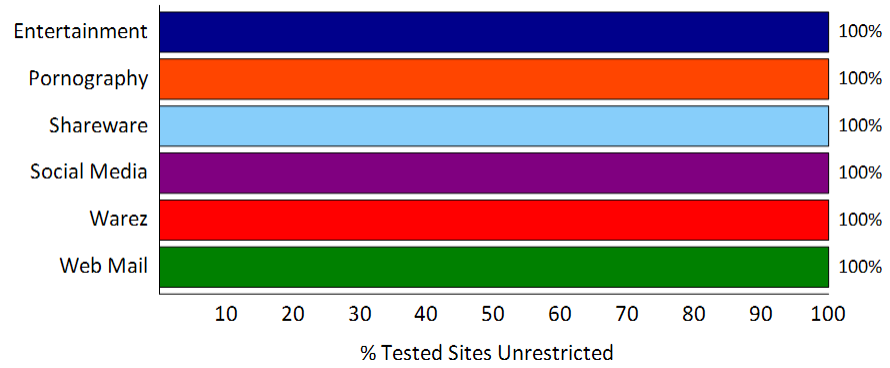
Some protocols should be highly restricted to systems which rely on them for their operation. Granting access to more than one system (unless specifically designated to require the protocol) is not recommended. The following table shows Internet-based protocols and highlights if these "allow, but limit" protocols are pervasive.

Protocol	Common Name	End Point(s)	Analysis
No issues detected			

4 - User Controls

An analysis of user controls indicates if content-filtering and access filtering has been implemented to prevent users from accessing potentially harmful websites and other Internet resources.

The following site categories were found to be accessible from various end-points:



URL	Category	Unrestricted End Point(s)	Analysis
ESPN	Entertainment	DC01 SE-Dresden UTIL01	**Unrestricted**
Playboy	Pornography	DC01 SE-Dresden UTIL01	**Unrestricted**
YouPorn	Pornography	DC01 SE-Dresden UTIL01	**Unrestricted**
Download.com	Shareware	DC01 SE-Dresden UTIL01	**Unrestricted**
Tucows.com	Shareware	DC01 SE-Dresden UTIL01	**Unrestricted**
Facebook	Social Media	DC01 SE-Dresden UTIL01	**Unrestricted**
Google+	Social Media	DC01 SE-Dresden UTIL01	**Unrestricted**
MySpace	Social Media	DC01 SE-Dresden UTIL01	**Unrestricted**
YouTube	Social Media	DC01 SE-Dresden UTIL01	**Unrestricted**
Isohunt.com	Warez	DC01 SE-Dresden UTIL01	**Unrestricted**
Pirate Bay	Warez	DC01	**Unrestricted**

URL	Category	Unrestricted End Point(s)	Analysis
		SE-Dresden UTIL01	
Gmail	Web Mail	DC01 SE-Dresden UTIL01	**Unrestricted**
Yahoo Mail	Web Mail	DC01 SE-Dresden UTIL01	**Unrestricted**

5 - Wireless Access

Providing wireless access enables greater freedom within the workplace, but can also pose potential security risks. The following table shows detected wireless networks and has any possible security issues highlighted. Some access points which are detected may not be a part of your network and their use should be discouraged as there is an inherent risk in connecting to foreign networks.

SSID	Secured	Security	Risk Level
<blank>	Yes	RSNA	Low
202Xnet	Yes	WPA_PSK	Low
Belkin_G_Wireless_B976AF	**Yes**	**IEEE80211_Open**	**High**
clear	**No**	**IEEE80211_Open**	**High**
clear-guest	**No**	**IEEE80211_Open**	**High**
CLIENT	Yes	RSNA_PSK	Low
HP8A74CE	**No**	**IEEE80211_Open**	**High**
Kristie	Yes	RSNA_PSK	Low
SPLS-CORP	Yes	RSNA	Low