s

Arizona State University
Center for Cybersecurity and Digital Forensics
781 Terrace Road, 4th Floor
Tempe, AZ 85281

iSecure Protector Server Edition with Biometric Signature and 5-Factor Authentication Validation Project

Objective

Determine the effectiveness of iSecure Protector Server Edition in protecting critical servers from external and internal attacks and the efficiency in bandwidth cost savings and productivities that iSecure Protector Server Edition provides.

Environment

1. Microsoft Azure Cloud running Windows Server 2016.
    a. IP Address: 52.175.232.134
    b. * Username: tpham
    c. * Password: OrangE75&jUICe

    * Username and Password was disclosed during the second phase of the test and iSecure Protector Server Edition was in protection mode.

2. iSign iSecure Protector Server Edition Management Portal
    a. https://www.isignapps.com/iSecureProtector2017/SE
    b. Username: isecureprotector
    c. Password is the administrator's biometric signature

Initial Setup

Savant WMS (www.savantwms.com) created a Microsoft Azure Cloud Server instance running Windows Server 2016 and created the credential above for an iSign Team member to access and install the iSecure Protector Server Edition. An iSign Team member was also asked to create a user on the iSecure Protector Server Edition Management Portal and to enroll his/her biometric signature.

Requirements

1. Unrestricted access to server.
2. Smart Phone with on screen signing capability

Tests and Results

Chart 1 - iSecure Protector Server Edition Basic Monitoring End Result

ISP	Domain	# of IP Addresses
Akamai Technologies Inc.	akamai.com	333
Amazon Technologies Inc.	amazon.com	16
Aoyou L.L.C	aoyouhost.com	1
Automattic Inc	wordpress.com	2
Barbarich Viacheslav Yuryevich	pinspb.ru	1
CARInet Inc.	cari.net	1
Channelnet LTD.	pinspb.ru	2
China Mobile Communications Corporation	chinamobileltd.com	1
ChinaNet Shanghai Province Network	chinatelecom.com.cn	1
CloudFlare Inc.	cloudflare.com	5
Comcast Cable Communications LLC	comcast.net	7
Digital Energy Technologies Limited	host1plus.com	2
DigitalOcean LLC	digitalocean.com	1
EdgeCast NetBlk	edgecast.com	14
Facebook Ireland Ltd	facebook.com	2
Fastly	fastly.com	2
FPT Telecom Company	fpt.com.vn	1
GitHub Inc.	github.com	1
Google Inc.	google.com	384
Highwinds Network Group Inc.	highwinds.com	5
Hostkey B.V.	hostkey.com	3
Hostspace Networks LLC	hostspaces.net	1

JSC Planetahost	eurotech.ru	1
JSC Transtelecom	intelbi.ru	1
Level 3 Communications Inc.	level3.com	11
Limelight Networks Inc.	limelightnetworks.com	2
Limited Broadcast RFC3330	-	54
LLC Server v arendy	cloudfort.com	1
Microsoft Corp	microsoft.com	15536
Microsoft Corp Singapore	microsoft.com	687
Microsoft Corporation	microsoft.com	48948
Multicast	-	5
NetUP Ltd.	netup.ru	3
New Mexico State University	nmsu.edu	1
NForce Entertainment B.V.	nforce.com	1
Online S.A.S.	free.fr	1
OVH SAS	ovh.com	2
Quantil Networks Inc.	quantilnetworks.com	15
Severen Telecom	severen.ru	1
SIA MWTV	mwtv.lv	1
Tencent Cloud Computing (Beijing) Co. Ltd.	tencent.com	1
Twitter Inc.	twitter.com	3
Verizon Communications Inc.	verizon.com	88
Viettel Corporation	viettel.com.vn	1
WestVPS LLC.	westvps.eu	1
Wonten Network Ltd.	cdnzz.net	1

According to the iSecure Protector Server Edition packet monitoring of both inbound and outbound activities, the **software detected 500 MB of data consumption from 02/15/2018 – 02/20/2018**. The reason for the high activities is due to the server being opened on all ports and there were many hacking attempts from various servers and computers throughout the Internet.

Connection to Server via RDP Test With iSecure Protector Server Edition on Basic Monitoring

Before we attempted to connect to the server, we asked the iSign Team to change the Administrator password and not disclose to anyone. Connect via RDP to attempt to use the default Administrator username: Administrator, and random password

Connections: 10 Password Attempts: 10 Success: 0

Without knowing the password and how complex it is, we were unable to break through. We were able to make the 10 connections to the server and see that it was running Windows Server 2016.

iSecure Protector Server Edition Dynamic Port Closing and Monitoring

iSecure Protector Server Edition was configured to close all ports from 1-65535 and only allow specific ports to be open when needed. As the result of dynamic port opening, iSecure Protector Server Edition detected **350 MB of data consumption from 02/20/2018 – 02/27/2018**.

Connection to server via RDP Test with iSecure Protector Server Edition in Protection Mode

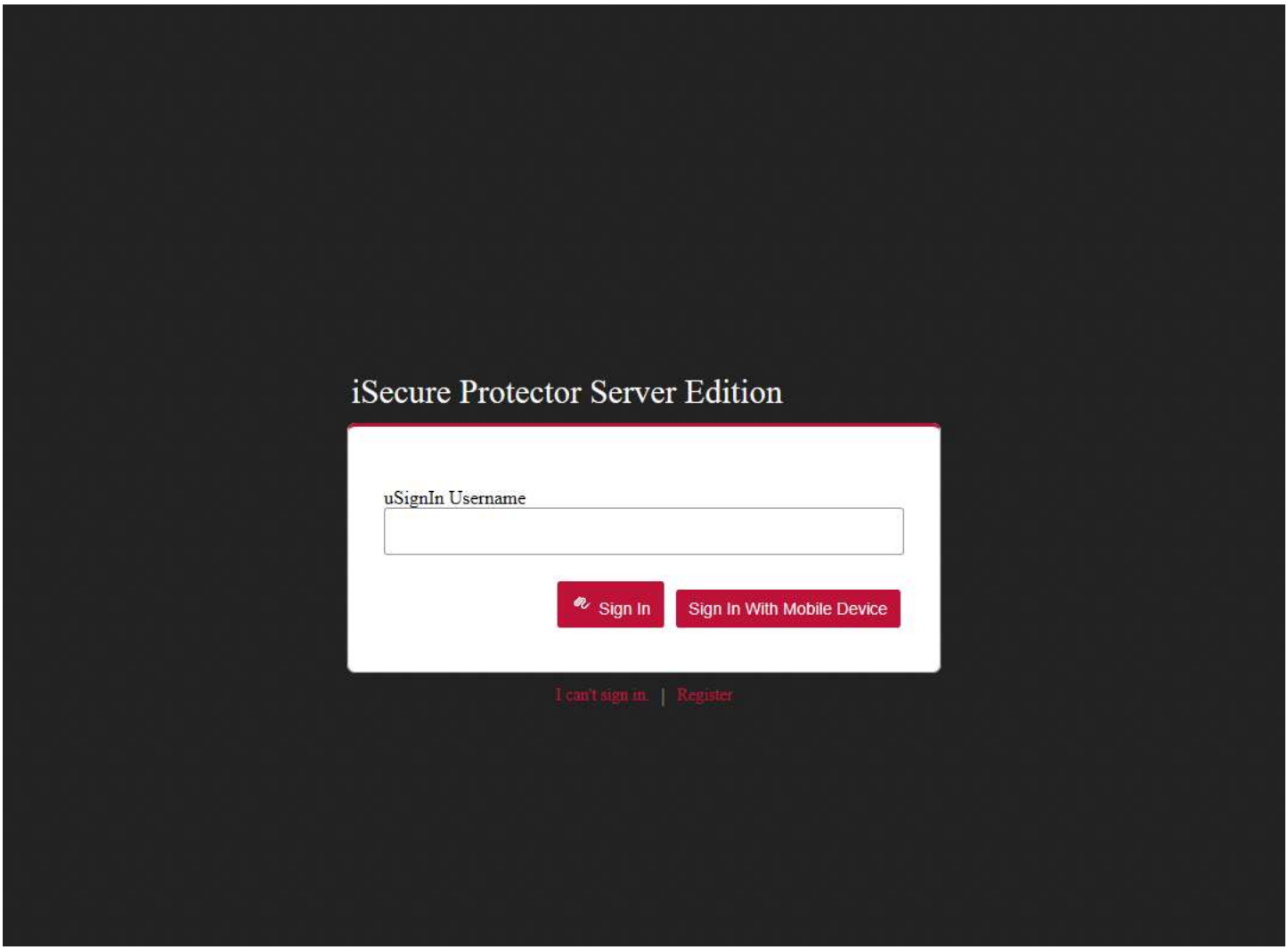
We asked the iSign Team for the username and password to connect to the server. Using the username tpham and the password set for the tpham was OrangE75&jUICe.

Connections: 0 Password Attempts: 0 Success: 0

Because iSecure Protector Server Edition closed all ports and only allow it to open to specific IP Addresses, we were unable to connect to the server to make any attempts at hacking the server.

Turning on RDP Port 3389 to allow connections to the server

A request was sent to the iSign Team to open the RDP Port 3389 and to one of their IP Addresses. We also requested the iSign Team to give us the uSignIn Username (isecureprotector). Once that has been accomplished, we proceeded to https://www.isignapps.com/iSecureProtector2017/SE and use the isecureprotector username to log into the system.



Using the provided uSignIn Username, we began to attempt to break in.

1. Enter the uSignIn Username
2. We attempted to sign using a touchscreen laptop, guessing the signatures

Signature Sign In
Attempts: 2 Failed: 2 Success: 0

After 2 failed attempts using a signature that we believed to be the signature of the uSignIn username iSecure Protector, our IP Addressed was blocked. We contacted the iSign Team to unblock the IP Address so that we can make connections to the server.

Signature Sign In with Mobile Device
Attempts: 2 Failed: 2 Success: 0

Upon signing in with mobile device, we were unable to sign in because iSecure Protector uSignIn username was already registered to another device, which we did not have possession at the time; simulating a real world situation.

Sign In with Password
Attempts: 10 Failed: 10 Success: 0
We used the Can't Sign In feature to attempt to get the passcode to log into the account and were unsuccessful because the passcode was sent to the mobile phone that was registered to the account. We did not have possession of the mobile phone that was associated to the iSecure Protector username.

Conclusion
After thorough testing and data collections, I have concluded that the iSecure Protector Server Edition reduced the bandwidth consumption from 500MB to 350MB, which is a 30% bandwidth reduction. iSecure Protector Server Edition was 100% effective in blocking unknown sources from remote desktop. Even with selective IP Address and selective port opening of 3389, the iSecure Protector Server Edition blocked all unauthorized IP Addresses.

The iSecure Protector Server Edition management portal with biometric signature and 5-Factor authentication was 100% effective in identifying unknown sources and black listed the IP Addresses immediately. Because we could not obviously reproduce the biometric signature of the iSecure Protector user, the system immediately blocked our IP Addresses after 2 failed attempts.

Trying to break in using the passcode option with a mobile device was also unsuccessful since our mobile phone was not recognized.

iSecure Protector Server Edition is certainly a great tool for both reducing bandwidth and blocking all hacking attempts.

Assistant Research Professor, Arizona State university
Title

_____
Ziming Zhao

2018/02/28
Date