Port of Vancouver USA

Port of Vancouver USA

Hacked: Why Washington Ports Could Be Next.

CHRIS CARTER, INFORMATION SECURITY ANALYST

Intro

OSINT

Open Source Intelligence

Overshare

Are you able to provide any details about the technology environment at the Port that would be in scope of the engagement?

- Number of connected sites **6**
- Number of servers **3**
- Percentage of servers that are virtualized **100%**
- Server operating system platform in use **MS Windows Server 2012 R2 Std**
- Type of storage platform in use **All server based hard drives**
- Does the Port utilize cloud-based service providers for any critical applications? **No**
- Number of critical business applications – **Not sure, part of the goal of this project is to figure what our critical application are**
- Number of IT staff and their roles **0 – IT support is outsourced to a local vendor**
- Number of end users **+/- 40**

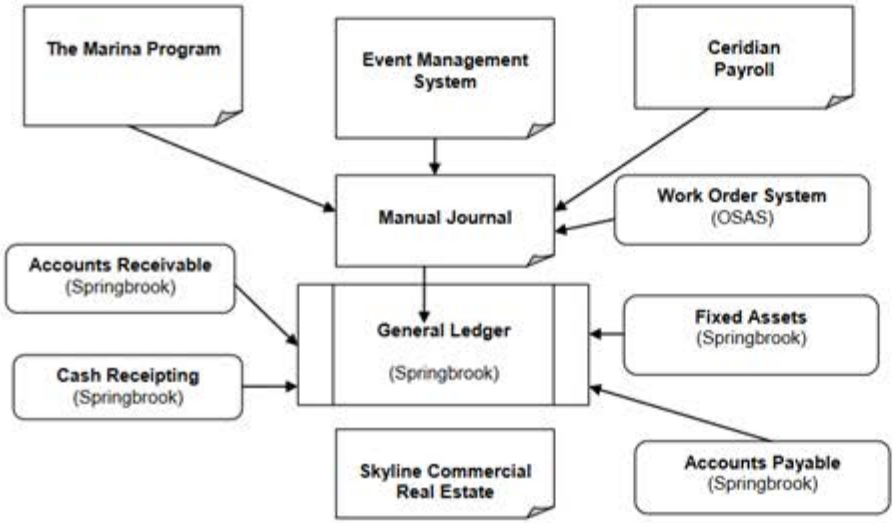
How many databases support the in-scope applications?
The primary data base is Microsoft Dynamics SL2015, plus a few other small application

No of applications that need protecting, with a brief description of each General Domain, MS Dynamics SL2015, Access/Gate control software (Topaz), camera control and recording (Milestone)

What method of authentication is required? 2 factor, single sign-on? 2 factor

What is the approximate total number of systems/functions within [redacted] that need to be evaluated? Approximately 6 – Accounting, HR, Payroll, Purchasing, Access Control, Camera Control

CURRENT SYSTEM DIAGRAM



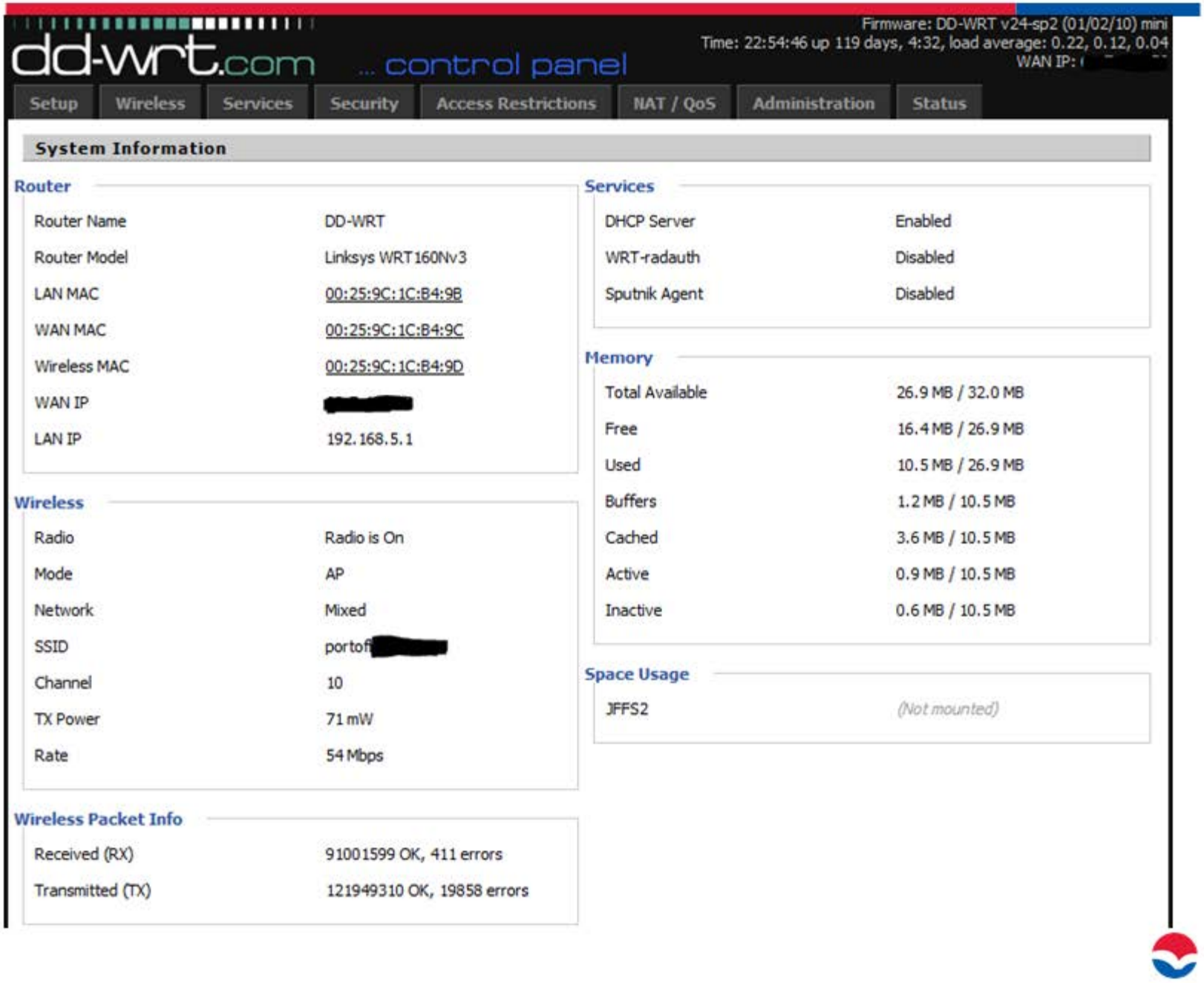
CURRENT USER PROFILE

Module	Full Access	Read Only
General Ledger	7	5
Accounts Payable	2	5
Accounts Receivable	4	5
Fixed Assets	2	5
Work Orders	30	0
Marina Management Software	21	1
Event Management Software	4	0
Skyline Property Management	5	3

CURRENT SYSTEM SUMMARY

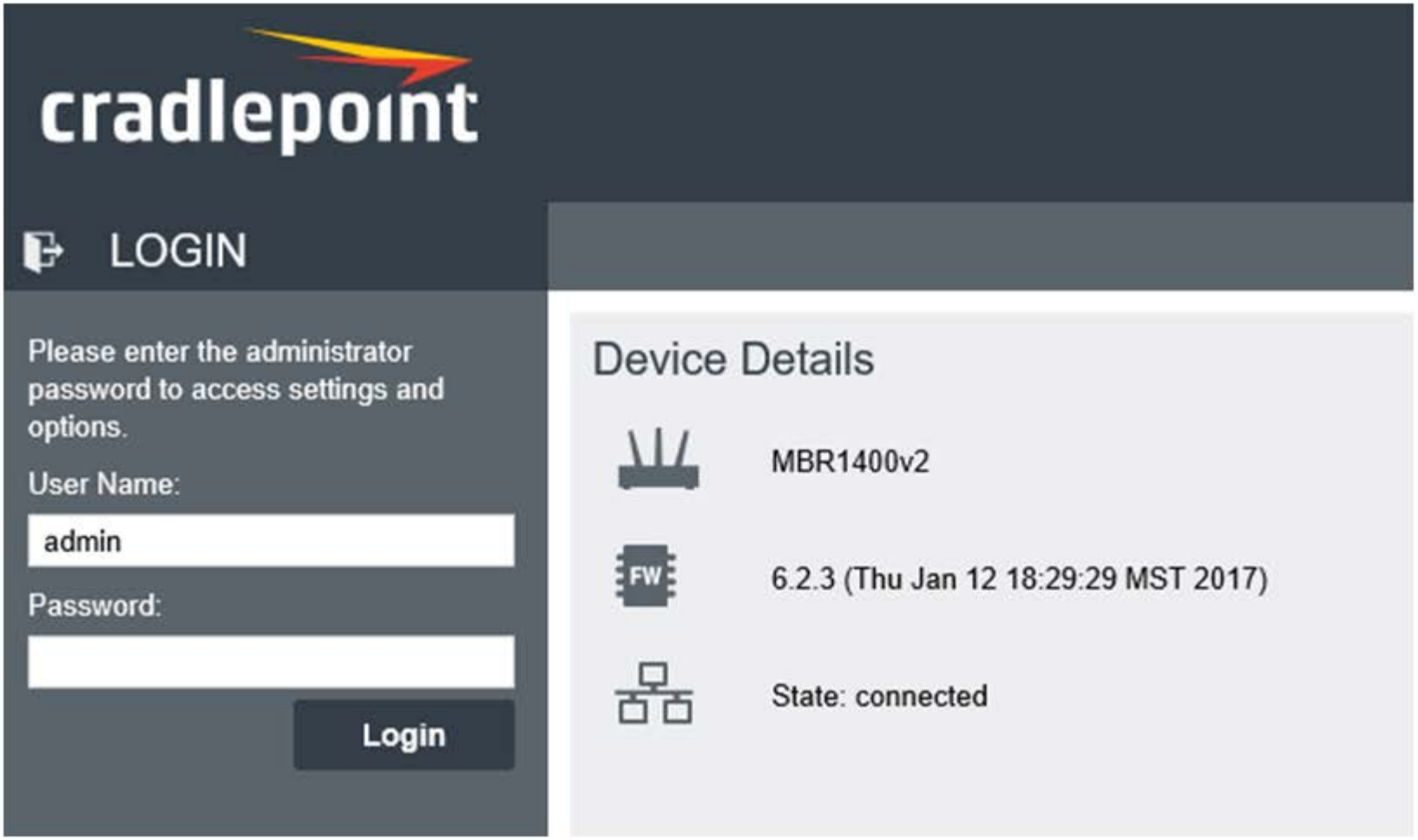
System	Database/Server	Client
Springbrook	Microsoft SQL 2000	Progress 9.1
OSAS	Proprietary	Proprietary
Marina Program	Pervasive SQL	ccMarina
PC workstations	MS Windows 7 64-Bit	N/A
Skyline	Pervasive SQL	Skyline
Event Mgmt. System	MS SQL Express	EMS 12.0
Ceridian	Web Based	Web Based

Exposed


dd-wrt.com ... control panel
Firmware: DD-WRT v24-sp2 (01/02/10) mini
Time: 22:54:46 up 119 days, 4:32, load average: 0.22, 0.12, 0.04
WAN IP: [redacted]
Setup
Wireless
Services
Security
Access Restrictions
NAT / QoS
Administration
Status
System Information
Router
Router Name DD-WRT
Router Model Linksys WRT160Nv3
LAN MAC 00:25:9C:1C:B4:9B
WAN MAC 00:25:9C:1C:B4:9C
Wireless MAC 00:25:9C:1C:B4:9D
WAN IP [redacted]
LAN IP 192.168.5.1
Wireless
Radio Radio is On
Mode AP
Network Mixed
SSID portof[redacted]
Channel 10
TX Power 71 mW
Rate 54 Mbps
Wireless Packet Info
Received (RX) 91001599 OK, 411 errors
Transmitted (TX) 121949310 OK, 19858 errors
Services
DHCP Server Enabled
WRT-radauth Disabled
Sputnik Agent Disabled
Memory
Total Available 26.9 MB / 32.0 MB
Free 16.4 MB / 26.9 MB
Used 10.5 MB / 26.9 MB
Buffers 1.2 MB / 10.5 MB
Cached 3.6 MB / 10.5 MB
Active 0.9 MB / 10.5 MB
Inactive 0.6 MB / 10.5 MB
Space Usage
JFFS2 (Not mounted)

DHCP Clients

Host Name	IP Address	MAC Address	Client Lease Time
*	192.168.5.125	xx:xx:xx:xx:21:0A	1 day 00:00:00
iPad	192.168.5.119	xx:xx:xx:xx:BA:E7	1 day 00:00:00
*	192.168.5.146	xx:xx:xx:xx:93:D3	1 day 00:00:00
iPad-3	192.168.5.118	xx:xx:xx:xx:B0:A9	1 day 00:00:00
Zen	192.168.5.101	xx:xx:xx:xx:0F:72	1 day 00:00:00
Casshole	192.168.5.128	xx:xx:xx:xx:EE:E8	1 day 00:00:00
jennifersiPhone	192.168.5.126	xx:xx:xx:xx:98:DC	1 day 00:00:00
Lindas-iPhone	192.168.5.127	xx:xx:xx:xx:86:CC	1 day 00:00:00
EE-5590-1SW84Q2	192.168.5.111	xx:xx:xx:xx:1F:D7	1 day 00:00:00
iPhone	192.168.5.149	xx:xx:xx:xx:9A:89	1 day 00:00:00
Tiff	192.168.5.123	xx:xx:xx:xx:5C:E9	1 day 00:00:00
android-f0eff6eae676ccd7	192.168.5.110	xx:xx:xx:xx:4F:01	1 day 00:00:00
DESKTOP-3HFIBEJ	192.168.5.129	xx:xx:xx:xx:D5:A4	1 day 00:00:00
[redacted]	192.168.5.138	xx:xx:xx:xx:ED:D2	1 day 00:00:00
[redacted]	192.168.5.135	xx:xx:xx:xx:69:79	1 day 00:00:00


cradlepoint
LOGIN
Please enter the administrator password to access settings and options.
User Name:
admin
Password:
Login
Device Details
MBR1400v2
FW
6.2.3 (Thu Jan 12 18:29:29 MST 2017)
State: connected

Port of [redacted]

Terminal Operations

Home Page

JMT Web App

Secure Jade Internal Page

JMT Web App

Secure Jade External Page

JMT Web App

Remote Desktop

RCS-3100

ALX Technology

LOG IN


WebCTRL®
Licensed to Port of [redacted] for use at [redacted] Regional Airport.
Serial Number ([redacted])
Name:
Password:
Log in

Product Information

Printer Information

Status Device Needs Attention

HP ENVY 7640 e-All-in-One Printer series

Status Log

Out of Paper

Your connection is not secure

The owner of pay.port[redacted].com has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more...

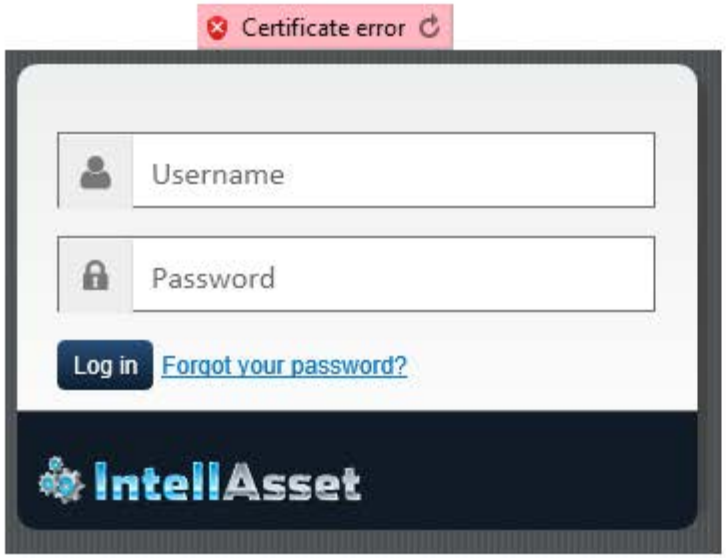
☐ Report errors like this to help Mozilla identify and block malicious sites

Go Back | Advanced

pay.port[redacted].com uses an invalid security certificate.

The certificate expired on Friday, December 7, 2018, 8:58:39 AM. The current time is March 25, 2019, 12:16 PM.

Error code: SEC_ERROR_EXPIRED_CERTIFICATE



Public Downloads

Sorted by name

<address>Apache/2.4.18 (Ubuntu) Server at [redacted].terminalsystems.com Port 443</address>

Cameras

http://[redacted]myfoscam.org:88/CGIProxy.fcgi?cmd=snapPicture2&usr=Guest&pwd=Port 18&t=

http://[redacted]myfoscam.org:88/CGIProxy.fcgi?cmd=snapPicture2&usr=port[redacted]&pwd=1988Sn2001!&t=

US to reportedly blacklist Chinese surveillance camera giant Hikvision

Server 5.20.2

Banner: 220 AXIS Q1755 Network Camera 5.20.2 (Aug 24 2012) ready.

We use a vendor for that

<h3>This web service is using http://tempuri.org/ as its default namespace.</h3>
<h3>Recommendation: Change the default namespace before the XML Web service is made public.</h3>

[redacted] BidData

The following operations are supported. For a formal definition, please review the Service Description.

- AddProjectNotice
- AddUserPrintCenter
- DeleteAnnouncement
- DeleteBidder
- DeleteCompanyLogo
- DeleteMsg
- DeletePrintMsg
- DeleteProjectAdmin
- DeleteProjectNotice
- DeleteRfi
- DeleteUserPrintCenter
- GetAllCities
- GetAllCompanies
- GetAllCompaniesByProjectRole

You protected the data but what about the vendor?

Snoco-Asset_Schema_022613-traffic.mdb	28-Feb-2013 10:39	944K
Snoco-Asset_Schema_031413.mdb	13-Mar-2013 15:12	7.6M
Snoco-Asset_Schema_040213.mdb	02-Apr-2013 09:42	476K
Snoco-Asset_Schema_060713.mdb	10-Jun-2013 13:58	3.7M
Snoco-Asset_Schema_070113.mdb	01-Jul-2013 17:00	1.0M
Snoco-BMS_060713 (2).xls	01-Jul-2013 17:00	730K
Snoco-BMS_060713.xls	07-Jun-2013 11:23	1.2M
Snoco-Bridges_042913.mdb	29-Apr-2013 14:22	804K
Snoco-Bridges_050813.mdb	08-May-2013 10:10	708K
Snoco-Bridges_052013.mdb	20-May-2013 14:05	3.0M
Snoco-Drainage_Facilities.mdb	23-May-2013 12:06	22M
Snoco-Road AssetsAMMS_Schema_022112.mdb	21-Feb-2013 14:23	4.0M
Snoco-Road_Asset.mdb	12-Apr-2013 08:31	3.5M
Snoco-Road_Asset_041513.mdb	16-Apr-2013 08:35	8.3M
Snoco-SignPlates_053013.mdb	31-May-2013 09:06	912K
Snoco-guard-rails-Asset_Schema_021112.mdb	19-Feb-2013 08:35	1.3M
Snoco-spot_post_schema_020513.mdb	05-Feb-2013 09:01	432K
Snoqualmie 2014 Parks List.xlsx	08-May-2017 12:56	17K
SnoqualmieAddresses.zip	09-May-2017 09:46	506K
SnoqualmieBillableRates.zip	22-Feb-2017 15:10	74K
Snoqualmie Contractor List.xlsx	06-Mar-2017 07:52	213K
Snoqualmie Contractor List ABBREVIATED VENDOR NAME-mod.xlsx	22-Mar-2017 13:17	234K
Snoqualmie Contractor List ABBREVIATED VENDOR NAME.xlsx	16-Mar-2017 08:39	216K
SnoqualmieParks.zip	31-Jan-2017 11:22	778K
SnoqualmieParksUpdate.gdb.zip	03-Mar-2017 14:48	47K
SnoqualmieVehicleAndEquipmentRatesInventory - Jan 2017.zip	31-Jan-2017 11:28	55K
Snoqualmie Vehicle Inventory - Jan 2017.xls	08-May-2017 12:56	70K
StateLicenseInfo Missing.png	26-Apr-2019 09:21	148K

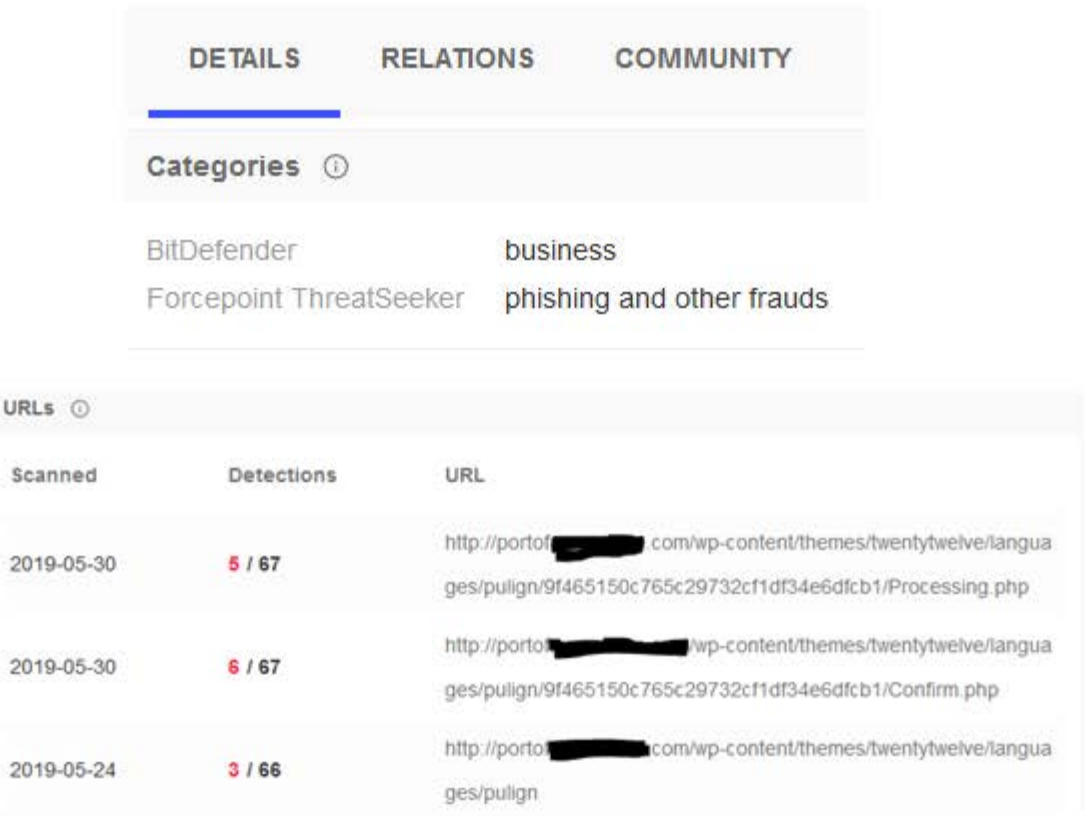
<tr class="rgRow" id="ctl01_TemplateBody_WebPartManager1_gwpciNewQueryMenuCommon_ciNewQueryMenuCo
<td>Mr. Jerry Allender</td><td>Canaveral Port Authority</td><td>Port Commissioner</td><td>(32
</tr><tr class="rgAltRow" id="ctl01_TemplateBody_WebPartManager1_gwpciNewQueryMenuCommon_ciNewQue
<td>Mr. Pat Anderson</td><td>Port of Beaumont</td><td>Vice President, Board of Commissioners<
</tr><tr class="rgRow" id="ctl01_TemplateBody_WebPartManager1_gwpciNewQueryMenuCommon_ciNewQueryM
<td>Mr. Glen Bachman</td><td>Port of Everett</td><td>Commissioner</td><td>(425) 388-0625</td>
</tr><tr class="rgAltRow" id="ctl01_TemplateBody_WebPartManager1_gwpciNewQueryMenuCommon_ciNewQue
<td>Ms. Elizabeth Beeton</td><td>Port of Galveston</td><td>Board of Trustees of the Galveston
</tr><tr class="rgRow" id="ctl01_TemplateBody_WebPartManager1_gwpciNewQueryMenuCommon_ciNewQueryM
<td>Mr. Harold Bistline</td><td>Canaveral Port Authority</td><td>Port Attorney</td><td>(321)
</tr><tr class="rgAltRow" id="ctl01_TemplateBody_WebPartManager1_gwpciNewQueryMenuCommon_ciNewQue
<td>Mr. Richie Blink</td><td>Plaquemines Port, Harbor and Terminal District</td><td>Commissio
</tr><tr class="rgRow" id="ctl01_TemplateBody_WebPartManager1_gwpciNewQueryMenuCommon_ciNewQueryM
<td>Mr. Patrick Boyle</td><td>Duluth Seaway Port Authority</td><td>Commissioner</td><td>(218)
</tr><tr class="rgAltRow" id="ctl01_TemplateBody_WebPartManager1_gwpciNewQueryMenuCommon_ciNewQue
<td>Mrs. Melanie Bradford</td><td>Canaveral Port Authority</td><td>Special Assistant/Liaison
</tr><tr class="rgRow" id="ctl01_TemplateBody_WebPartManager1_gwpciNewQueryMenuCommon_ciNewQueryM
<td>Ms. Kimberly Brandon</td><td>Port of San Francisco</td><td>President, San Francisco Port
</tr><tr class="rgAltRow" id="ctl01_TemplateBody_WebPartManager1_gwpciNewQueryMenuCommon_ciNewQue
<td>Mr. C. Michael Callais</td><td>Port Fourchon</td><td>Port Commissioner</td><td>(985) 632-
</tr><tr class="rgRow" id="ctl01_TemplateBody_WebPartManager1_gwpciNewQueryMenuCommon_ciNewQueryM
<td>Mr. John Comeaux</td><td>Port of Port Arthur Navigation District</td><td>Commissioner</td
</tr><tr class="rgAltRow" id="ctl01_TemplateBody_WebPartManager1_gwpciNewQueryMenuCommon_ciNewQue


We just have a website


HACKED


HACKED
Joomla!™

Web Reputation



DETAILS | RELATIONS | COMMUNITY

Categories

BitDefender	business
Forcepoint ThreatSeeker	phishing and other frauds

URLs

Scanned	Detections	URL
2019-05-30	5 / 67	http://portof[redacted].com/wp-content/themes/twentytwelve/languages/pulign/9f465150c765c29732cf1df34e6dfcb1/Processing.php
2019-05-30	6 / 67	http://porto[redacted]/wp-content/themes/twentytwelve/languages/pulign/9f465150c765c29732cf1df34e6dfcb1/Confirm.php
2019-05-24	3 / 66	http://porto[redacted].com/wp-content/themes/twentytwelve/languages/pulign

275

Malware
view all

180

Malware
view all

149

Malware
view all

Risk
5.7

Risk
4.3

The most dangerous phrase in the language is "we've always done it this way."

Rear admiral Grace Hopper


A collection of companies working together to collect and share intelligence will always have better visibility into the threat landscape than one organization on its own.
– Ken Xie, CEO and Founder, Fortinet

Thank You

Chris Carter
Information Security Analyst
Chris.Carter@portvanusa.com
https://www.linkedin.com/in/chrishcarter/
360-693-3611