An April Fool’s Treasurehunt

01
APR

An April Fool’s Treasurehunt

April 1, 2016 / Ryan Nolette / Advanced Threat Protection, Detection and Response, Endpoint and Server Security, Prevention, Response, Tech Toolbox

It's once again April Fool's day and some tech news online reads like a bad prank. For example, a few days ago, we saw a new point-of-sales (POS) malware in the wild.

I'm not kidding.

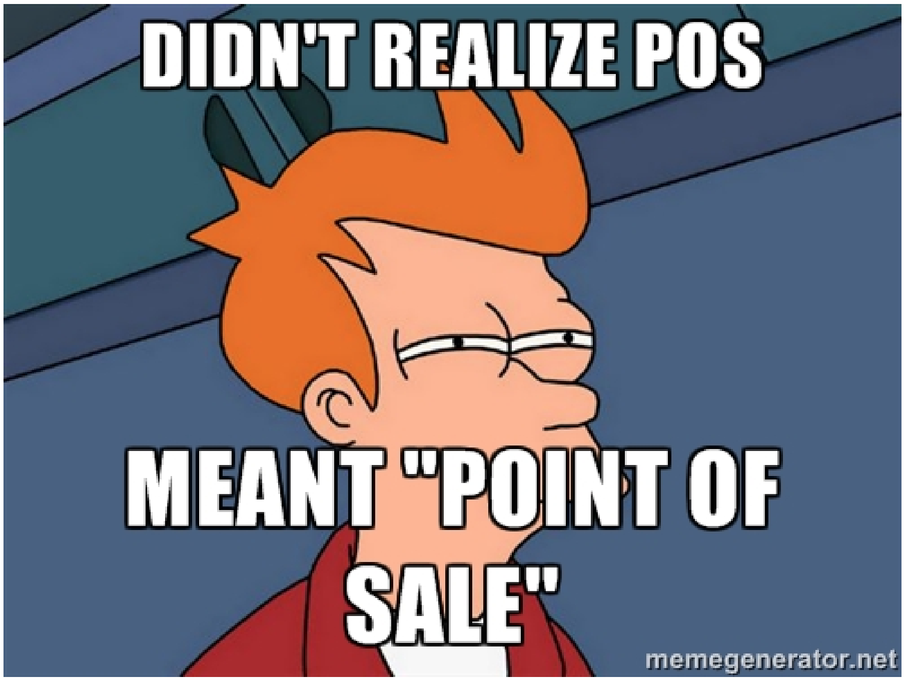
When I originally read the article about Treasurehunt on Threatpost's website, I thought it was an early April Fool's prank. I just couldn't believe that POS malware is still as large of a threat as it still is.

POS systems are single-function appliances, and a large amount of these appliances run a stripped down version of Windows XP called "XPembedded."

What does embedded mean?

"An embedded system is a dedicated computer system designed for one or two specific functions. This system is embedded as a part of a complete device system that includes hardware…The embedded system is unlike the general-purpose computer, which is engineered to manage a wide range of processing tasks. Because an embedded system is engineered to perform certain tasks only, design engineers may optimize size, cost, power consumption, reliability and performance."

Sounds a lot like the description of a POS system right?

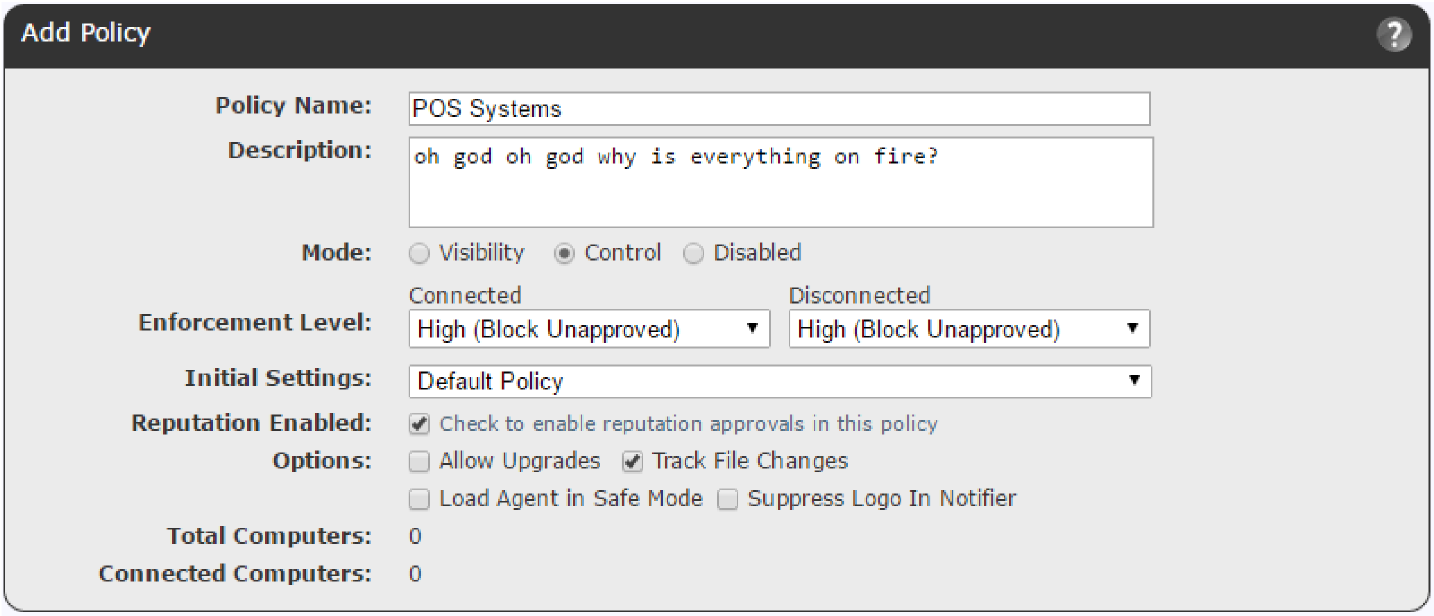


The very name of the OS contains the word embedded. This means that only very limited software is installed on them and they're rarely updated. If this is the case, why are these systems not using whitelisting and authenticated access?

So, in the spirit of helping you avoid the worst prank ever, a breach, I am going to show you how to first defend against POS malware using Carbon Black Enterprise Protection and then how to alert on unauthorized interactive logins on your POS systems using Carbon Black Enterprise Response.

Carbon Black Enterprise Protection

1. Install Carbon Black Enterprise Protection on all POS systems
2. Create a new policy called "POS Systems"

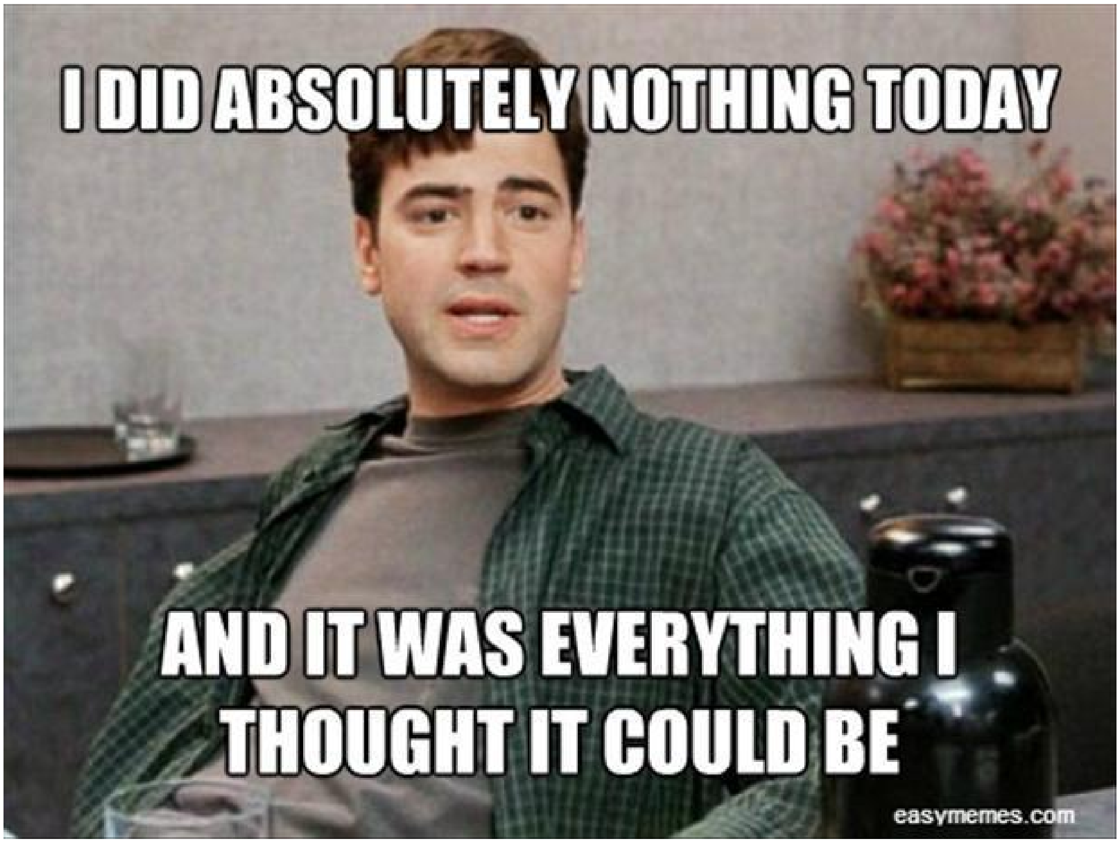


Add Policy

Policy Name:	POS Systems	
Description:	oh god oh god why is everything on fire?	
Mode:	○ Visibility ● Control ○ Disabled	
	Connected	Disconnected
Enforcement Level:	High (Block Unapproved)	High (Block Unapproved)
Initial Settings:	Default Policy	
Reputation Enabled:	☑ Check to enable reputation approvals in this policy	
Options:	□ Allow Upgrades ☑ Track File Changes	
	□ Load Agent in Safe Mode □ Suppress Logo In Notifier	
Total Computers:	0	
Connected Computers:	0	

3. Put all your POS systems into this policy

4. Go tell management this was harder than it actually was and go hide in the server room to browse Reddit like a civilized person. You get a gold star today.


I DID ABSOLUTELY NOTHING TODAY
AND IT WAS EVERYTHING I THOUGHT IT COULD BE
easymemes.com

Carbon Black Enterprise Response

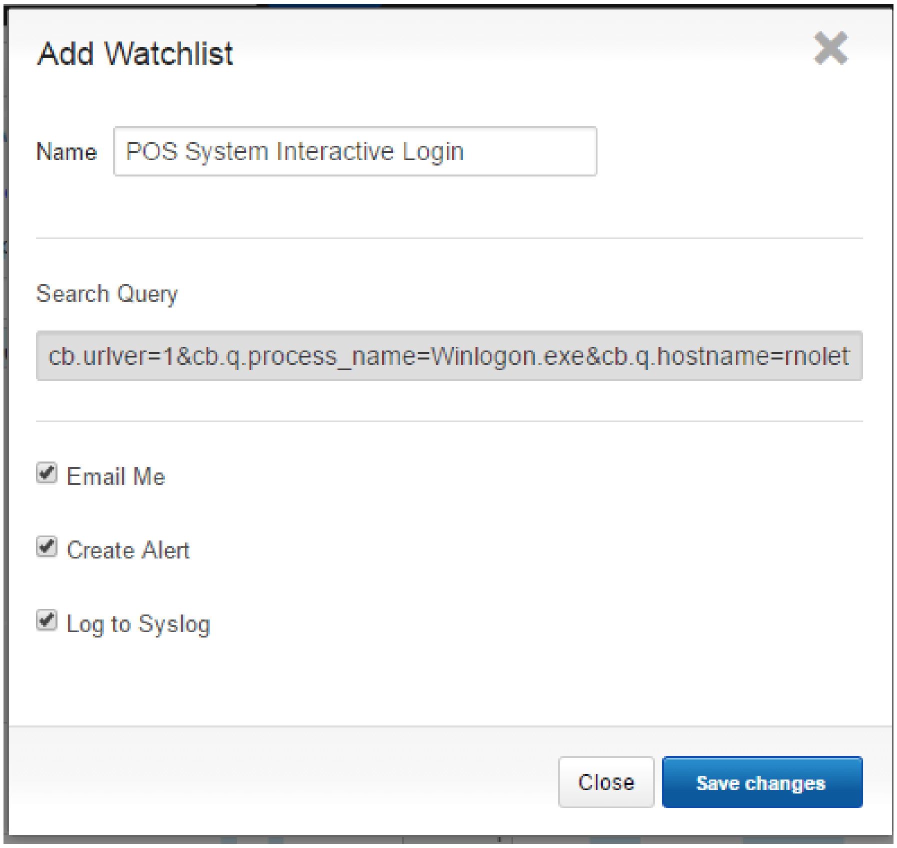
For this example we are going to look at execution of the winlogon.exe process which is executed during the interactive logon process of a windows system. The Windows subsystem starts Winlogon.exe, a system service that enables logging on and off. Winlogon.exe then does the following (see "Logon Phase" for further details):

- Starts the Services subsystem (Services.exe), also known as the Service Control Manager (SCM).
- Starts the Local Security Authority (LSA) process (Lsass.exe).
- Parses the Ctrl+Alt+Del key combination at the Begin Logon prompt.

Process for detecting interactive login events

1. Install Carbon Black Enterprise Response on all POS systems
2. Create a new sensor group called "POS"
3. Move all POS systems sensors into the "POS" group so we can limit the scope of our searches.
4. Create alert in Carbon Black Enterprise Response console

1. Alert on user login:
    1. Group: "POS"
    2. Process_name:Winlogon.exe
        1. NOTE: This can also be done with registry values if you want.
        2. NOTE: if you really want to get specific you can specify " parent_name:smss.exe" to make sure it is a login event running winlogon.exe
        3. The above two conditions translate to this query if you're interested
            1. cb.urlver=1&cb.q.process_name=Winlogon.exe&cb.q.group=(group%3A%22POS%22)&sort=&rows=10&start=0
    3. Run query and make sure you are getting results.
        1. They should be few and far between since interactive logins on a POS devices don't happen often unless your POS software requires it. You may have to log into one just to make this query fire results if you have a quiet network. To add a watchlist:



Add Watchlist

Name: POS System Interactive Login

Search Query: cb.urlver=1&cb.q.process_name=Winlogon.exe&cb.q.hostname=rnolet

☑ Email Me

☑ Create Alert

☑ Log to Syslog

4. Make query a watchlist and set it to alert you upon any logon events for devices in the POS sensor group
5. Go do something else with confidence that now you know you'll be alerted of any unauthorized successful access attempts on your POS appliances like what would happen during the initial manual data exfiltration attempts.

GO TO THE WINCHESTER, HAVE A PINT
AND WAIT FOR THIS ALL TO BLOW OVER

Breaking News: Carbon Black releases new tool to stop Java-based attacks. In other news, Redmond’s technical support staff report a rise in ban-hammer based coffee shop attacks. Find out why at 11

“Until next time, remember my motto. Flag it, Tag it, and Bag it.”

10 Shares 3 1 6

Tags: Carbon Black malware pos ransomware

More Posts