FIT 2017 | FREEBUF

How Cybercrime Bypasses common security controls in the enterprises

Richard Rushing

CISO of Motorola Mobility（a Lenovo Company）

About Me

- ✓ CISO of Motorola Mobility
  - @secrich – On Twitter
  - Have a Crazy Family all part of the fun
  - Been Doing this way to LONG
- ✓ Security Startup Veteran
  - SecureIT, Verisign, AirDefense
- ✓ Corporate Veteran (Siemens, GE, Mot
- ✓ We can only improve by adding Compl

we are so….

A

What retail wireless security?

TJX has plenty of company in the blithe-indifference pool

By Jaikumar Vijayan FOLLOW
Computerworld Nov 15, 2007 12:00 AM PT

RELATED TOPICS
Security
Mobile & Wireless
Malware & Vulnerabilities
Network Security
Endpoint Security
Wireless Networking

INSIDER

In Scott Walker's state, Democrats seek outsourcing penalties

Wisconsin Gov. Scott Walker is still a cipher on offshore outsourcing and the H-1B issue. But Wisconsin

READ NOW

TJX may be in a class all by itself in terms of the number of records compromised in a data breach. But the retailer apparently has plenty of company when it comes to wireless security issues of the sort that led to the compromise it disclosed earlier this year.

A survey of over 3,000 retail stores in several major U.S. cities by wireless security vendor AirDefense Inc. reveals that a large number of retailers are failing to take even the most rudimentary steps for protecting customer data from wireless compromises.

Among the biggest issues: weakly protected client devices, wrongly configured wireless access points inside stores, data leakage, poorly named network identifiers, and outdated access-point firmware.

According to AirDefense, about 85% of the 2,500 wireless devices that it discovered in retail stores, such as laptops and barcode scanners, were vulnerable to wireless hacks. Out of the 4,748 access points that were monitored for the survey, about 550 had poorly named SSIDs that could give away the store's identity.

"One thing we did not expect was the large number of point-of-sale devices that looked as if they had been turned on" and left in essentially the configuration in which they arrived at the store, said Richard Rushing, chief security officer at AirDefense . Many of the access IDs that were being used by retailers had names that were dead giveaways, such as 'retail wireless', 'POS WiFi' or 'store nu Rushing said. "I can guarantee that all of these stores were als configurations" on their access points, he said. "You really are doors of hackers," with such weak security practices, he said.

NECTING THE INFORMATION
URITY COMMUNITY

Video Radio Reports White Papers Ev

ENDPOINT MOBILE PERIMETER RIS

hite House

t's house exposes some interesting nce, but solid defenses inside

, chief security officer of AirDefense, on a ween the White House and the U.S. Treasury y at the laptop on Rushing's lap, a three-foot from his briefcase, pulling in transmissions ured national institutions.

hite House. We're looking for wireless (To see a photo of Rushing and his antenna,

As we sit, scanning the IDs of dozens of wireless networks in the area, the shadow of a uniformed White House security officer falls over our screen. He's the first one to notice our antenna, even though we've passed at least eight officers on our walk so far.

Damn, I'm thinking. *Now we're in for an hour of police questioning, or maybe worse. I wonder when I'll get home tonight?*

"Excuse me, gentlemen," the officer says politely. "I don't mean to interrupt, but what is that device you have there?"

Rushing, a trained penetration tester and ethical hacker, doesn't try to hide anything. "It's an antenna," he says.

The officer frowns for a moment closely. Then his face brightens. "Cool," he ithout another word, he turns and walks away.

s in front of the of his briefcase nds.

Definition of Bypass

noun

✓ a road passing around a town or its center to provide an alternative route for through traffic.

synonyms: detour, alternative route, diversion, shortcut

verb

Go past or around.

"bypass the farm and continue to the road"

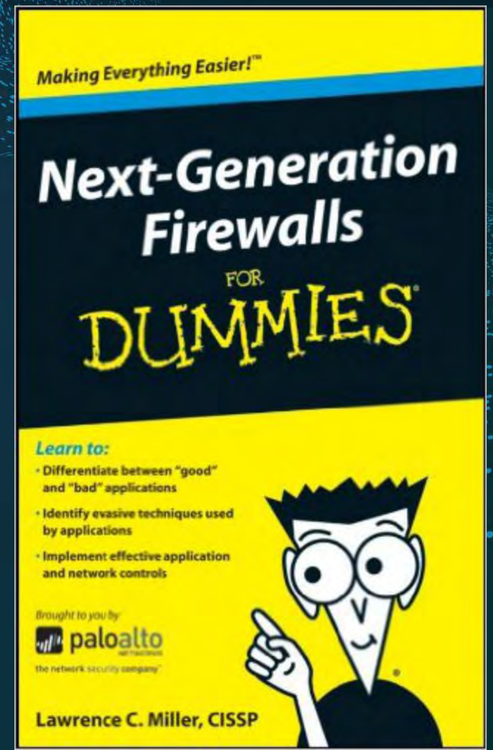
synonyms: go around, go past, make a detour around;

Items covered

- ✓ Network Controls
  - Firewalls
  - Web Application Firewalls
  - Sandboxes
  - Traffic
- ✓ Endpoint Controls
  - Antivirus
  - Exploit Mitigation
  - Advance Detection

Network controls--Firewalls

- ✓ Even Scanner like NMAP can tell information
  - Handshakes, Options, Resets, etc.
- ✓ Next Generation Firewall
  - – Needs to allow more traffic to determine if to block
  - -UDP rules them all
- ✓ IPV6 configuration never matches IPv4
  - -CRC, Fragments, So many ways
- ✓ Your Firewall Hides NOTHING!



Network controls-- Firewalls

- ✓ Application specific rules require more packets
  - Packets will pass thru the firewall
  - Can be as much as 35 packets before being blocked
- ✓ So understand what application types
  - Allows for the best results
  - Many Exploits are Blocked by Signature
  - Customized the specific exploit
- ✓ Encryption is your friend

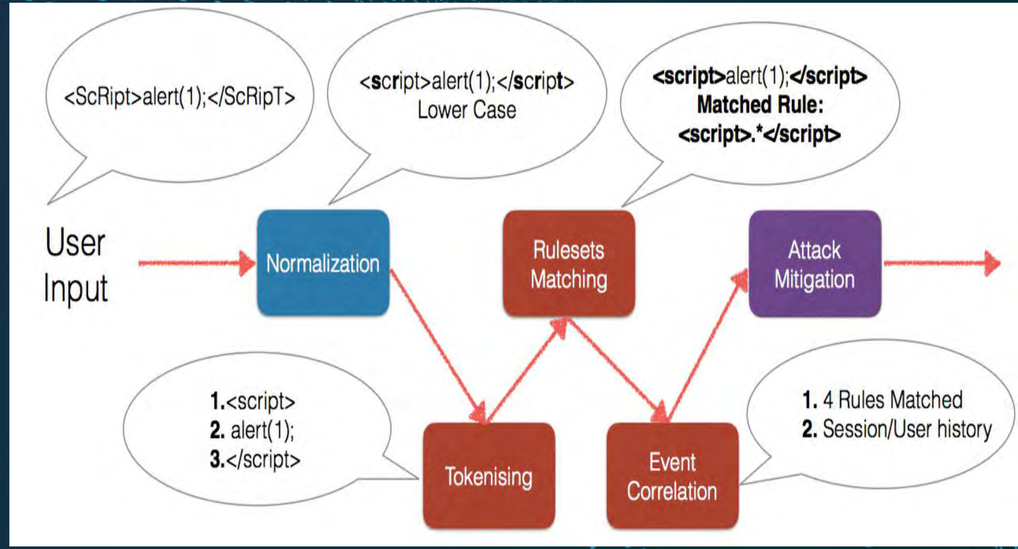
Web Application Firewall （ WAF)

✓ Over 250 protocol-level evasion techniques have been released

- Automating WAF Fingerprinting with Burp, Nmap and wafw00f

✓ HTTP Parameter Pollution – HPP

- Encoding Techniques for Bypassing
- HTTP Parameter Fragmentation – HPF
- Remote File Inclusion for WAF Bypassing

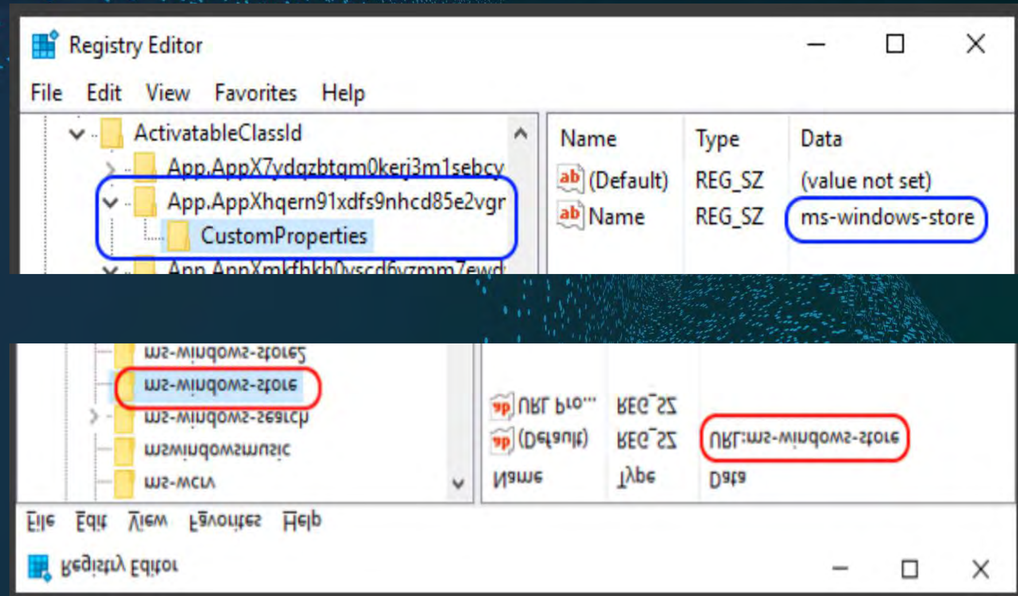


File Impersonation

- ✓ What determines the format of the file
  - Most of the time the extension is just used
  - Can use an Exploit
  - Can you embedded other code
- ✓ JPG images great place
  - If viewed with Browser
  - JPG Modified to be JavaScript, Or other format.
- ✓ Many other formats to use, Browser is the weak link

Browsers – Loading Files

- ✓ New Protocols all the time
  - New unrestricted applications
  - ms-windowstore://collection/?CollectionId=
- ✓ URL Interesting
  - Enumerate all loadable protocols
  - Which apps accept arguments so we can try to inject code
  - (binary or pure JavaScript, depending on how the app was coded and how it treats the arguments Files



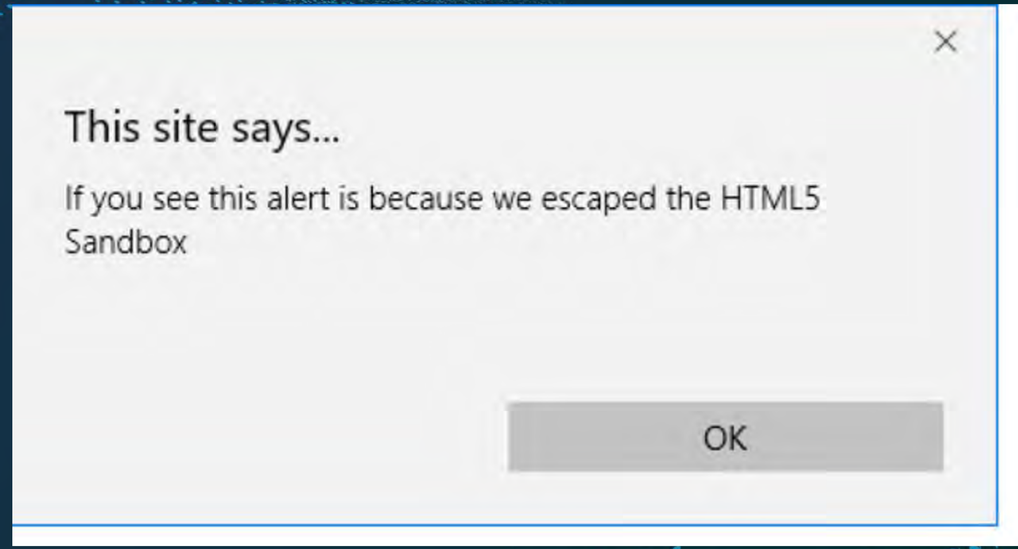
Sandbox

✓ HTML5 Sandbox

- Impose restrictions to a webpage using the sandbox iframe attribute or the sandbox http header.

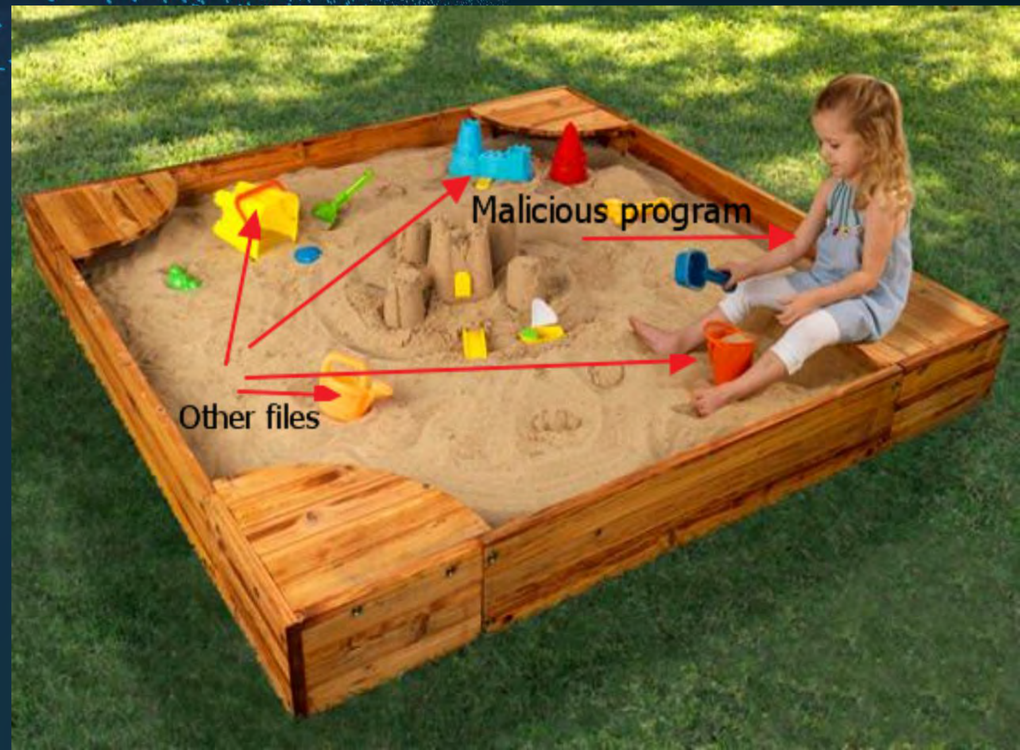
- <iframe src=”sandboxed.html” sandbox></iframe>

✓ If you can escape,is it a sandbox?



Sandbox

- ✓ Waiting
- ✓ Waiting More……
- ✓ New ways to see if your in a Sandbox
  - # CPU's
  - Count CPU Cycles
  - Embed Another document, Powerpoint inside and Excel file
- ✓ Just be good at the time of scanning



Endpoint Proxy/VPN

✓ IPV6 is rarely used but always configured

- IPv6 usually bypass most attempts to pick up Configuration issues

- If the system receives an IPv6 Router Advertisement it will immediately configure IPv6

✓ This may include a global address, a default route, and a new DNS server

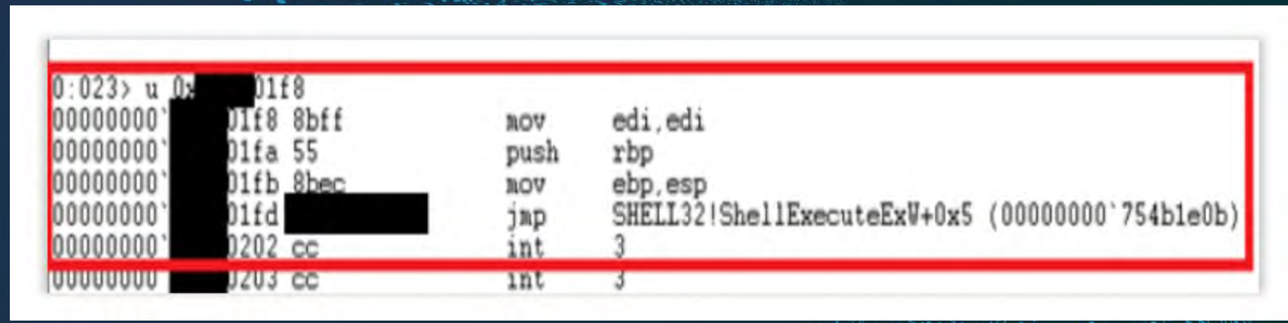
Source	Destination	Src Port	Dst Port	Protocol	Info
172.21.1.103	172.21.1.1			ESP	ESP (SPI=0xcd180228)
172.21.1.1	172.21.1.103			ESP	ESP (SPI=0x4d82aee7)
2001:470:c4e8:10:2c29:6796:	ord08s06-in-x0e.1e100.net	1670	80	TCP	netview-aix-10 > http [SYN] Seq=0
2001:470:c4e8:10:2c29:6796:	ord08s06-in-x0e.1e100.net	1669	80	TCP	netview-aix-9 > http [SYN] Seq=0 W
ord08s06-in-x0e.1e100.net	2001:470:c4e8:10:2c29:6796:	80	1670	TCP	http > netview-aix-10 [SYN, ACK] S
2001:470:c4e8:10:2c29:6796:	ord08s06-in-x0e.1e100.net	1670	80	TCP	netview-aix-10 > http [ACK] Seq=1
2001:470:c4e8:10:2c29:6796:	ord08s06-in-x0e.1e100.net	1670	80	HTTP	GET /complete/search?q=www.goog&cl
ord08s06-in-x0e.1e100.net	2001:470:c4e8:10:2c29:6796:	80	1669	TCP	http > netview-aix-9 [SYN, ACK] Se
2001:470:c4e8:10:2c29:6796:	ord08s06-in-x0e.1e100.net	1669	80	TCP	netview-aix-9 > http [ACK] Seq=1 A
ord08s06-in-x0e.1e100.net	2001:470:c4e8:10:2c29:6796:	80	1670	TCP	http > netview-aix-10 [ACK] Seq=1
ord08s06-in-x0e.1e100.net	2001:470:c4e8:10:2c29:6796:	80	1670	HTTP/XML	HTTP/1.1 200 OK

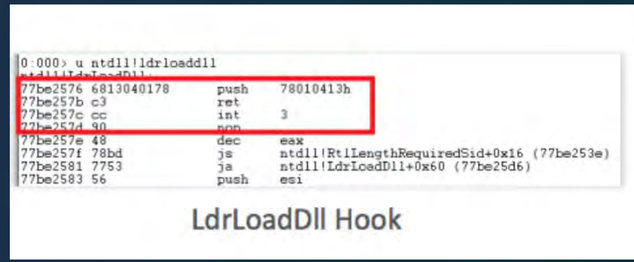
Bypassing Endpoints

- ✓ How do they do it
  - Hooking
  - Malware – Man-in-the-Middle/Browser
  - Anti-Exploit – EMET, Traps,etc..
  - APM – Application Performance Monitoring
  - Application Virtualization –Microsoft App-V
  - 3rd Party Personal Firewalls – Zone-Alarm
  - Managed by a Kernel to User Injected DLL

Hooking Issues

- ✓ Unsafe Injection
- ✓ Predictable RWX Code Stubs
- ✓ Predictable RX Code Stubs
- ✓ ASLR bypass – OS functions
- ✓ Hook Bypass – Call Hook
- ✓ RWX Hook code Stubs
- ✓ RWX Hooked Modules



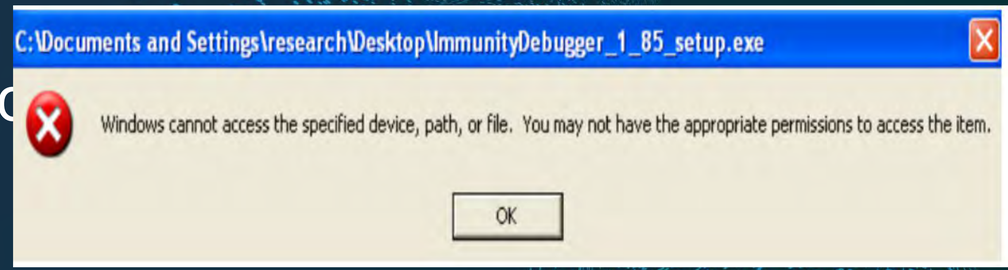


LdrLoadDll Hook

RWX Permissions

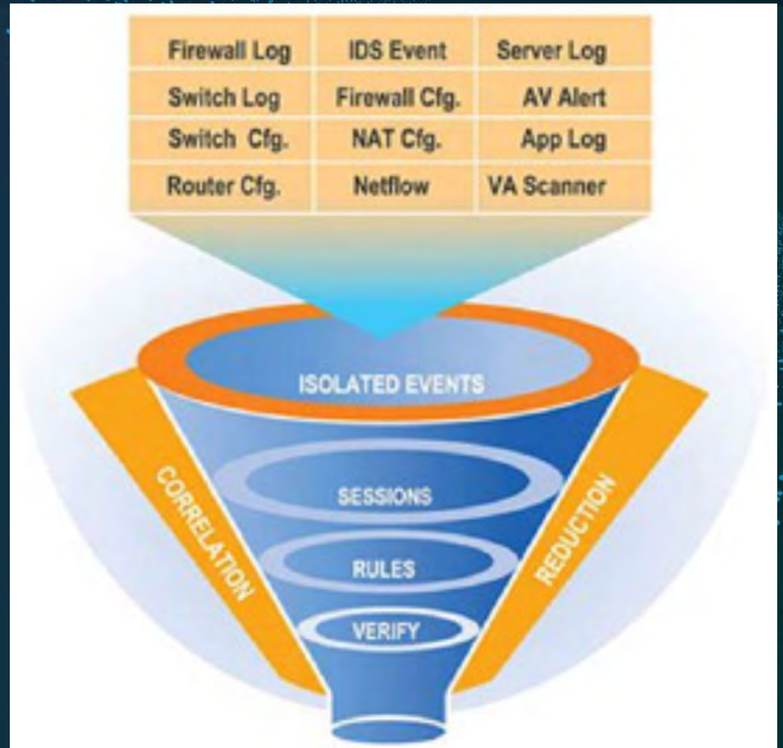
Application Whitelisting

- ✓ Applications can only be executed that are allowed
  - Bit9, AppLocker, Coretrace
- ✓ Find Applications that are Approved and can be used to execute code
  - Office, POWERSHELL,
  - DllInjection, PE-File Injection, Invoke Shellcode，Keylogging, Basic Code Execution – Scripts, Stating or Ending Applications
  - Full Code Execution - Injection/Execution



Security Logging Tools

- ✓ SIEMs
  - Recording all the data
  - Determine Issues and Problems
- ✓ Bypass
  - Critical issues in Logging – Source, Destination
  - Critical Levels control by Clients
  - Time always WIN – Set to 2 years in the future
  - NTP intercept, Change, or TimeZone



Take Away

- ✓ Plenty of ways around ALL Security Technology
  - Nothing works 100% percent
  - Endpoints are the Easy Part
- ✓ Solutions
  - Defense in Depth
  - Detection in Depth
  - Variance is the key to success
- ✓ Different Solutions vs. Single Solution

Thank You!