Point-of-Sale (POS) Malware: Tactics and Strategies for Protecting Customer Payment Information

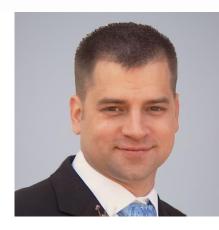
Bit9 and Carbon Black

Jeffrey J. Guy | 20 Feb 14 jjguy@bit9.com @jjguy



©2014 Bit9. All Rights Reserved

Introduction



Jeffrey J. Guy

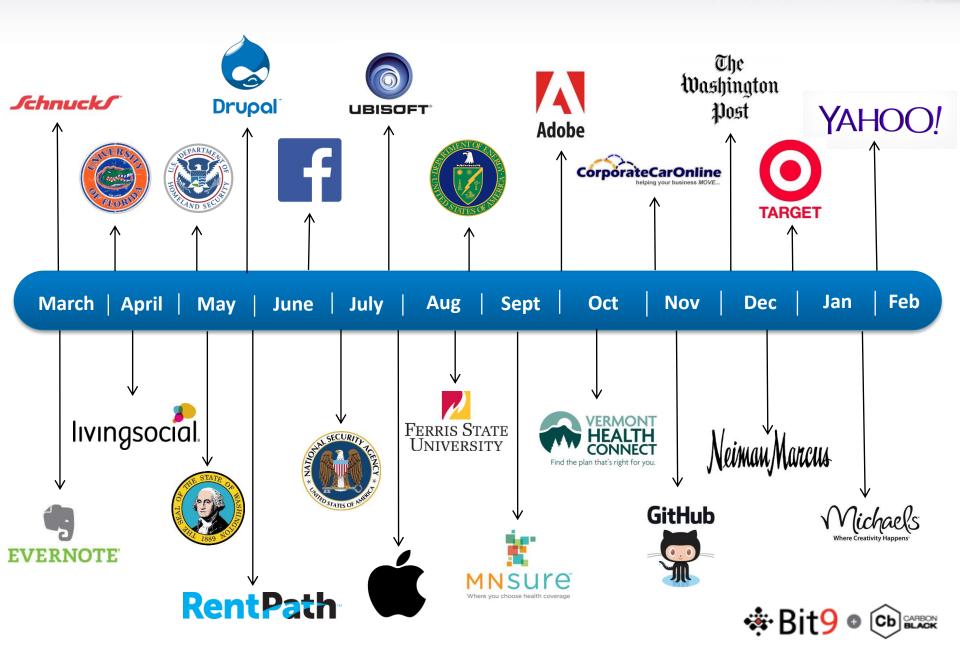
- Background
 - 6 years USAF, USAF Red Team
 - 7 years ManTech, CNO R&D services
 - 2 years at Cb, now Bit9
- Director, Product Management at Bit9
 - Formerly Director of Operations at Carbon Black

• Feb. 13, 2014

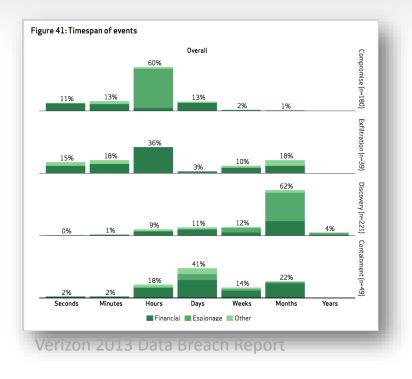
• Bit9 and Carbon Black merged to deliver single solution prevention, detection and response

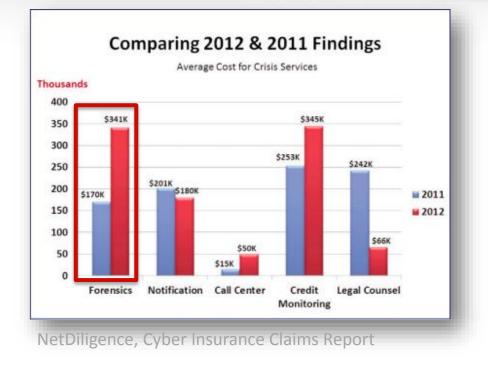


Assume You Will Get Breached (Last 12 Months)



The State of Information Security



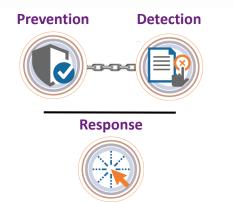


Compromise happens in seconds Data exfiltration starts minutes later It continues undetected for months Remediation takes weeks At \$341k per incident in forensics costs

THIS IS UNSUSTAINABLE



Endpoint security is evolving



Prevention Visibility Response

Traditional Security

- Prevention: Provided by endpoint antivirus. Easily bypassed.
- Detection: Provided by endpoint antivirus. Efficacy limited to the opinion of your AV vendor's signature database.
- Response: Usually by external consultants.

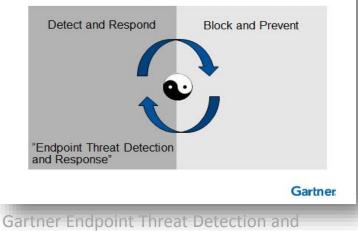
Emerging Model

Prevention, detection and response as a single, integrated and continuous process.



Protection = Prevention, Detection and Response

Complete Protection = Blocking+Detection



Response Tools and Practices, Sept. 2013

		vork Core	
Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			
	Figure 1: Framew	vork Core Structure	1

for Critical Infrastructure, Feb 2014

"Security...will shift to rapid detection and response capabilities linked to protection systems to block further spread of the attack."

"Functions organize basic cybersecurity activities at their highest level. These Functions are: Identify, Protect, Detect, Respond, and Recover."



Prevention

Traditional Prevention



- Small local signature database of known-bad, wide-spread, wellknown threats
- Single global database, centrally managed
- Efficacy limited to the opinion of your vendor's global database, at the moment of compromise

Emerging Prevention



- Local database of known-good applications
- Tailored policies to your environment, not the world's
- Lessons from network perimeter history: default-deny



Detection

Traditional **Detection**



- Small local signature database of threat data
- Single global database, centrally managed
- Efficacy limited to the opinion of your vendor's global database, at the moment of compromise
- Only action is block, thus requires high confidence

Emerging **Detection**



- Large global database of threat data
 - IOCs, VirusTotal, iSIGHT, US Cert, Bit9 Software Reputation Service and ATIs
- Efficacy is the consensus opinion of the industry's collective intelligence
- Can block or flag for review, increasing overall utility
- True detection in depth



Response

Traditional Response



- Ad hoc, as-needed activity by expensive, external consultants
- Relies heavily on disk and memory artifacts for historical record
- Guidelines on IR prep (e.g., NIST 800-61, etc.) limit preparations to administrative measures

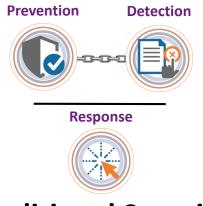
Emerging Response



- Even your entry-level staff can do IR in seconds
- Complete historical record of when/where/what/how
- Better, faster and cheaper than traditional IR



What Does This Mean for Your Security?



Traditional Security Bottom Line

- Prevention: dependent on AV signature of your one chosen vendor at the moment of compromise
- Detection: dependent on AV signature of your one chosen vendor
- Response: expensive and time-consuming forensics, limited to present and future



Emerging Security Bottom Line

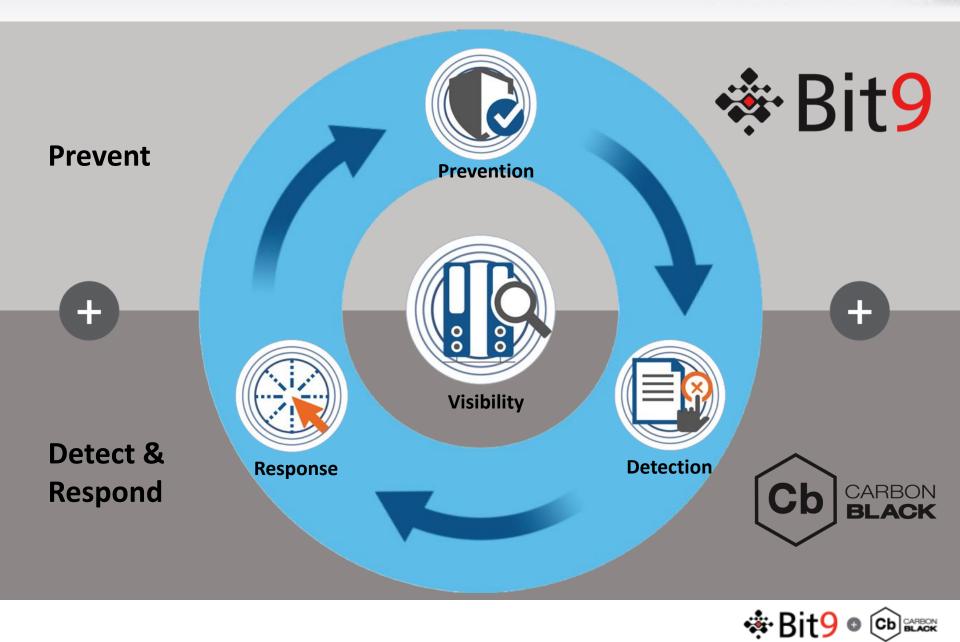
- Prevention: likely never runs, default-deny
- Detection: consensus opinion of the industry's collective intelligence
- Response: complete breadth and depth in seconds, including complete history



BlackPOS in Carbon Black – DEMO!

Q Contains text		Search			D Reset search terms Action
+ Add Criteria					
Process Name (50+) 🚯	Group (1) 🚯	Hostname (2) 🚯 🕘	Parent Process (50+) ()	Process Path (50+) 🚯	Process MD5 (50+) ()
Q	Q	Q	Q	Q	Q
svchost.exe (92.7%)	default group (100.0%)	xpsp3 (97.2%)	wscript.exe (93.0%)	c:\windows\microsoft.net	5e7f3968069d32b26af0d
mscorsvw.exe (1.5%)		j-8205a0c27a0c4 (2.8%)	mscorsvw.exe (1.5%)	c:\windows\microsoft.net	d87acaed61e417bba546
ngen.exe (0.9%)			msiexec.exe (1.3%)	c:\windows\system32\w	8219c45e4723fea835e5c
Process Analy f6f8df8d6c2197c7a		9c59c8d8ad6ce13d470eb8f	ftp.exe		ays about 3 days ago E Export events to CSV 35e7a11adec96fbd29c59c8d8a
-	3c8b35e7a11adec96fbd2	cmd.exe	fto.exe	f6f8df8d6c2197c7a3c8b	E Export events to CSV
-	3c8b35e7a11adec96fbd29	cmd.exe cmd.ex	ftp.exe	f6f8df8d6c2197c7a3c8b md.txt Company: Unknown	E Export events to CSV
-	3c8b35e7a11adec96fbd2	cmd.exe cmd.exe cmd.exe cmd.exe cmd.exe cmd.exe cmd.exe chwindows\sy cho-s:c:\docur	ttp.exe ystem32\cmd.exe /c ments and settings\administrator\desktop\cr hsystem32\cmd.exe /c	f6f8df8d6c2197c7a3c8b md.txt Company: Unknown Product: Unknown	E Export events to CSV
f6f8df8d6c2197c7a	3c8b35e7a11adec96fbd29	cmd.exe cmd.ax cmd.ax emd.ax emd.ax cmd.ax cmd.ax cmd.ax chwindowshy rp-s:c:\docur c:\windowshy rp-s:c:\docur c:\windowshy rp-s:c:\docur	ftp.exe ystem32%cmd.exe /c ments and settings\administrator\desktop\cr	f6f8df8d6c2197c7a3c8b md.txt Company: Unknown Product: Unknown Description: Unknown	E Export events to CSV
f6f8df8d6c2197c7a	3c8b35e7a11adec96fbd29	cmd.exe cmd.exe cmd.exe emd.exe emd.exe cmd.exe cmd.exe cmd.exe cmd.exe cmd.exe cmd.exe cmd.exe cmd.exe chwindowshsj rp-s:c:\docur chwindowshsj rp-s:c:\docur chwindowshsj rp-s:c:\docur chwindowshsj rp-s:c:\docur chwindowshsj rp-s:c:\docur chwindowshsj rp-s:c:\docur	ftp.exe ystem32'cmd.exe /c ments and settings'administrator'desktop'cr system32'cmd.exe /c septeula \\10.116.240.31	nd.txt Company: Unknown Product: Unknown Description: Unknown	E Export events to CSV
f6f8df8d6c2197c7a	3c8b35e7a11adec96fbd29	cmd.exe cmd.exe cmd.exe cmd.exe cmd.exe crmd.exe	ftp.exe ystem32'cmd.exe /c ments and settings'administrator'desktop'cr system32'cmd.exe /c septeula \\10.116.240.31	nd.txt Company: Unknown Product: Unknown Description: Unknown Signed: Unsigned	E Export events to CSV
f6f8df8d6c2197c7a	Currently selected	cmd.exe cmd.ex	ftp.exe ystem32'cmd.exe /c ments and settings'administrator'desktop'cr system32'cmd.exe /c septeula \\10.116.240.31	nd.txt Company: Unknown Product: Unknown Description: Unknown Signed: Unsigned Publisher: Unknown	E Export events to CSV
f6f8df8d6c2197c7a	3c8b35e7a11adec96fbd29	cmd.exe cmd.ex	ftp.exe ystem32'cmd.exe /c ments and settings'administrator'desktop'cr system32'cmd.exe /c septeula \\10.116.240.31	nd.btt Company: Unknown Product: Unknown Description: Unknown Signed: Unsigned Publisher: Unknown ふ Alliance Feeds 3 hit(VirusTotal	S) in 2 report(s)

Security Lifecycle



Come Say "Hi" at RSA!

