

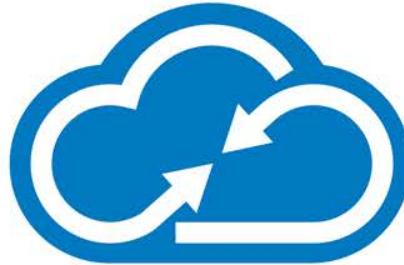
Innovative Computing Systems

PROVEN. RELIABLE. TRUSTED.

Kyle Worley, Senior Systems Engineer

# TOP CYBERSECURITY THREATS FACING LAW FIRMS

[www.innovativecomp.com](http://www.innovativecomp.com)



Innovative Computing Systems

# Full-Service Technology Partner

- Enterprise Content Management
- Managed IT Services
- Enterprise Servers & Storage
- Networking & Telephony
- Desktop Management
- Training
- Cloud Services
- Security
- Management Consulting

[www.innovativecomp.com](http://www.innovativecomp.com)

# HEADLINES



CRAVATH, SWAINE & MOORE LLP

]HackingTeam[

**WEIL  
GOTSHAL**



# PII HARVESTING

- Credit and debit card fraud down in 2015 while PII breaches are on the rise
- PII is highly sought after by criminals as it can be leveraged for financial fraud such as applying for credit, filing fraudulent tax refunds, and submitting false medical or insurance claims
- Credit and debit card numbers can be changed – SS numbers, names, addresses, etc. cannot
- PII underground value does not diminish over time



What is PII?	
PII includes: Name, email, home address, phone #	
<u>Sensitive PII includes:</u>	
<i>If Stand-Alone:</i>	<i>If Paired With Another Identifier:</i>
➤ Social Security number	➤ Citizenship or immigration status
➤ Driver's license or state ID #	➤ Medical information
➤ Passport number	➤ Ethnic or religious affiliation
➤ Alien Registration Number	➤ Sexual orientation
➤ Financial account number	➤ Account passwords
➤ Biometric identifiers	➤ Last 4 digits of SSN
	➤ Date of birth
	➤ Criminal history
	➤ Mother's maiden name

Active Filters

Clear

x Active vendor

Categories

Drugs 8390

**Fraud Related 1426**

CC & CVV 334

Accounts 494

Documents & Data 299

Dumps 65

Guides & Tutorials 1663

Services 570

Counterfeits 372

Digital Goods 1439

Drug Paraphernalia 162

Electronics 144

# Fraud Related

+ Filter

Popularity - This month Sort



CC from the US (Centurion, Signature & Platinum)

BTC 0.0176

Buy It Now

railguycc ( 98.1% ) **Level 4 ( 1226 )**



FAVORITE



[LEGENDARY] NON-AVS // •Bill=Ship• // NEW BASE

BTC 0.0000

Buy It Now

Yasuo ( 99.1% ) **Level 5 ( 2219 )**



FAVORITE



TCF Membership

BTC 0.1102

Buy It Now

Verto ( 99.9% ) **Level 5 ( 1170 )**



# PHISHING & WHALING ATTACKS

- **Phishing** – attempts to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication
- **Spearing** – occurs when cybercriminals target individual staff members in a specific company
- **Whaling** – targets the C-suite, partners, upper management, and other individuals of high worth or influence
  - Recent FBI study shows that whaling attacks have cost businesses \$2 billion over the past two years and experienced a 300% increase in 2015 over the previous year



# RANSOMWARE

- CryptoLocker emerged in 2013 and brought ransomware to the forefront, raking in \$27M in its first three months
- Many imitators have emerged since 2013 including CryptoWall, which is now king
- Binaries continuously re-encoded, numerous variants make AV largely ineffective
- Have you tested your backups lately?



## Anatomy of a Crypto-Ransomware Attack

New variants of ransomware known as **CryptoLocker**, **CryptoDefense** and **CryptoWall** are spreading via spam emails, drive-by downloads, or by malware already on your computer. Once you're infected, **crypto-ransomware** hijacks all your files, locks them up with unbreakable encryption, and demands a ransom of \$300-\$500 in bitcoins to unscramble them.

### 5 STAGES OF CRYPTO-RANSOMWARE

#### 1 INSTALLATION

After a victim's computer is infected, the crypto-ransomware installs itself, and sets keys in the Windows Registry to start automatically every time your computer boots up.



#### 2 CONTACTING HEADQUARTERS

Before crypto-ransomware can attack you, it contacts a server operated by the criminal gang that owns it.



#### 2

#### 3 HANDSHAKE AND KEYS

The ransomware client and server identify each other through a carefully arranged "handshake," and the server generates two cryptographic keys. One key is kept on your computer, the second key is stored securely on the criminals' server.



#### 4 ENCRYPTION

With the cryptographic keys established, the ransomware on your computer starts encrypting every file it finds with any of dozens of common file extensions, from Microsoft Office documents to .JPG images and more.

#### 4

#### 5 EXTORTION

The ransomware displays a screen giving you a time limit to pay up before the criminals destroy the key to decrypt your files. The typical price, \$300 to \$500, must be paid in untraceable bitcoins or other electronic payments.



# SENTINELONE

- How does traditional AV work and why is it not effective?
- AV-TEST registers over 75,000 new malicious programs every day
- Enterprises adopting a “good enough” strategy when it comes to AV
- SentinelOne is the first and only AV-TEST certified enterprise antivirus replacement
- Includes dynamic rollback feature to combat ransomware

*Antivirus "is dead," says Brian Dye, Symantec's senior vice president for information security. "We don't think of antivirus as a moneymaker in any way."*

- Wall Street Journal

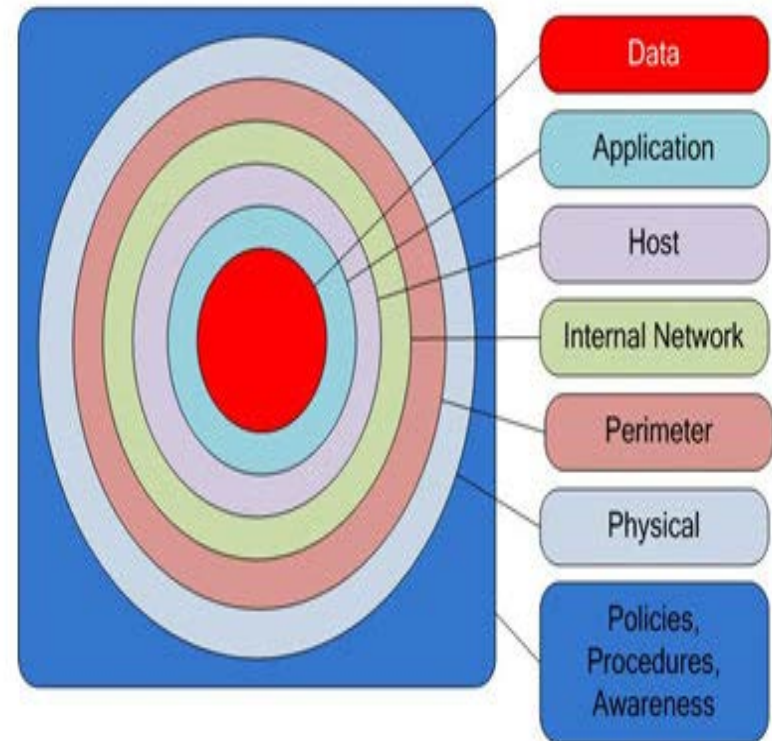


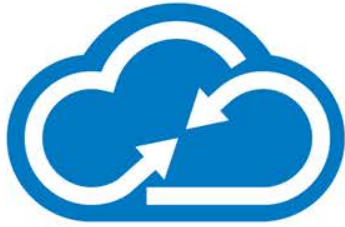


# DEFENSE-IN-DEPTH

- **Policies, Procedures, and Awareness** – Password Policies, Data Classification, Usage Policies, Security Training
- **Physical** – Guards, Cameras, Locks, Securely Wipe Data
- **Perimeter** – Firewalls, ACL Configured Routers, Email Gateway
- **Internal Network** – Network Segments, Network Intrusion Detection System
- **Host** – OS Hardening, Patch Management, Two-Factor Authentication, Anti-Virus, Host-Based Firewall
- **Application** – Application Hardening, Authentication, Software Restriction GPO
- **Data** – Access Control Lists, Encryption, Auditing, Backup and Restore Procedures

Defense in Depth Layers





Innovative Computing Systems

PROVEN. RELIABLE. TRUSTED.

## QUESTIONS? MORE INFORMATION?

Kyle Worley, Senior Systems Engineer  
[kworley@innovativecomp.com](mailto:kworley@innovativecomp.com)

Need more information? Want a longer demo?  
[sales@innovativecomp.com](mailto:sales@innovativecomp.com)

[www.innovativecomp.com](http://www.innovativecomp.com)