CYBERCRIME PREVENTION SEMINAR

Protect Yourself and Your Business

Presented by:

Drew Sanford

and

Hi-Link Technology Group
Drew Sanford

Drew Sanford is the CO-Founder of CARVIR, LLC. a security vendor focused at enabling Managed Service Providers to bring Enterprise Class Tools into the SMB space. CARVIR’s clients MSPs from all over North America and the World.

Before founding CARVIR, Drew served as COO and Co-Owner of a Nashville, TN based MSP that served customers in the Southern part of the United States focused on the Automotive, Manufacturing, Distribution and Medical verticals.

Drew has served as CIO of numerous organizations during his career and has co-written two books.

In his personal life, Drew enjoys serving as a board member on numerous area non-profits focused on the arts and the underserved within the community.
Cyber Security Goals

- State of Security 2018
- Latest Attacks
- Who Are The Victims
- The Problem We Face
- What You Can Do
Poll

- Have you or do you personally know someone that has been infected with Ransomware?
  - Yes
  - No
Are Small & Midsized Businesses Safe?

76% businesses experienced situations where malware / exploits have bypassed AV solutions
14% small businesses rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective
Not Just Big Business

1 in 5 of all small businesses will suffer a cyber breach this year.

81% of all breaches happen to SMBs, just like yours.

97% of all breaches could have been prevented with today's technology.
AV Is No Match For The New Threat Landscape

Malware
- Ransomware, trojans, worms, backdoors
- File-less / Memory-based malware

Exploits
- Document-based exploits
- Browser-based exploits

Live Attacks
- Script-based: Powershell, Powersploit, WMI, VBS
- Credentials: credential-scraping, Mimikatz, tokens
Traditional AV Solutions Cannot Keep Pace

390K new malicious code samples per day (according to AV-Test.org)
Legacy AV Vendors Cannot Respond Fast Enough

95% of Malware types showed up for less than 30 days

4 out of 5 Malware variants lasted less than 1 week
Multiple-Tools vs. Unified Approach

Unified Approach

- Single, lightweight agent
- Single management console
- Fewer FTEs
- Reduced TCO

Pre-Execution

Advanced Static Prevention + Whitelisting / blacklisting

On Execution

Dynamic Malware Detection
Dynamic Exploit Detection

Post-Execution

Mitigation
Remediation
Forensics

Multi-Solution Approach

- Multiple agents
- Multiple management consoles
- More FTEs
- > 4x TCO of SentinelOne
Anatomy Of A Ransomware Attack

Entry: Email, Drive-By Click, or Insider Threat

Protecting The Human Is Your First Priority
1) Every Email
2) Every Website
3) Every Click
4) Every Shared Network File
5) Every Cloud Storage File
6) Every Device
7) Every Employee
8) Every Time

An Attacker Only Needs To Be Right ONCE!
From: John Smith [mailto: john.smith@abcsteelworks.com]
Sent: Wednesday, April 27, 2016
To: Susan Jones
Subject: Payment Needed Today!

Susan - Are you available to make urgent payment for me today?

John M. Smith, President and CEO
T: 555-555-1111  e: john.smith@abcsteelworks.com

From: Susan Jones [mailto: susan.jones@abcsteelworks.com]
Sent: Wednesday, April 27, 2016
To: John Smith
Subject: RE: Payment Needed Today!

Yes, I am in the office all day. Please send me the payment details.

Susan Hoyle
Controller/CFO
T: 555-555-2222  e: susan.jones@abcsteelworks.com

From: John Smith [mailto: john.smith@abcsteelworks.com]
Sent: Wednesday, April 27, 2016
To: Susan Jones
Subject: RE: Payment Needed Today!

Attached are payment instructions. Code to Admin Expenses. I am out and not reachable by cell today use email only. Let me know as soon as payment sent - must be done today or we pay big late fee.

John M. Smith, President and CEO
T: 555-555-1111  e: john.smith@abcsteelworks.com

Is salutation consistent for sender?

Real domain has ‘w’

Fake domain: replaced ‘w’ with ‘vv’ (two v’s)

Other examples of domain name alterations:

• l vs. i or 1
• q vs. g
• 0 vs. O
• rn vs. m
• Extra/missing letters abcsteellworks.com
  abcsteelwork.com

Can you spot any other warning signs?
Poll

Should you pay the ransom if you get infected?

- Yes
- No
$2,100,000 Per Week In Ransom Payments

In February, officials at Hollywood (Calif.) Presbyterian Medical Center paid a relatively small sum, $17,000 in Bitcoin, for the release of their patient data and their multi-million dollar HIT system after a ransomware attack. But one well-known security industry firm, Symantec, Mountain View, Calif., estimated in 2012 that ransomware practitioners knocked down more than $30,000 per day in ransom payments world-wide.

Today, “it's probably more like $300,000 a day,” said Michael Bruemmer, vice president of Experian’s data breach resolution unit, and it's made largely on volume. “The average payment is about 2 Bitcoins, or $670. It's really small amounts.”
Victims Don’t Talk

The reason the public is not hearing more about them is because the victims don’t talk.

“It's like an iceberg, where you only see 30% above the water,” Bruemmer said since many in healthcare industry remain quiet about getting hit.

What’s Your Reputation Worth?

http://www.modernhealthcare.com/article/20161202/NEWS/161209980
Connecticut Courts Hit with Ransomware Attack

According to court officials, 114 of the 535 servers were affected, but the threat has since been contained.

By David Owens, The Hartford Courant / March 9, 2018

(TNS) — A ransomware attack has knocked the Connecticut court system’s computers off line.

The ransomware infection began Friday morning, said Melissa Farley, a Judicial Branch spokeswoman.
State employees worked throughout the weekend to contain a virus that had spread to more than 100 computers, a Department of Administrative Services spokesman said Monday.

Jeffrey Beckham said most computers were protected, but the virus infected about 160 in a dozen agencies. The impact to state business is not expected to be significant, he said.

The bug was detected late Friday afternoon, Beckham said, and staff noticed that it matched the profile of a ransomware virus. The DAS technical security team began to work with the agencies for which the alert was triggered.

Agency IT workers went to work and commissioners were alerted to the virus. DAS worked with agency employees to get it under control so it wouldn’t spread further.

They made “significant progress,” he said, and contained the virus Sunday night. Most computers were protected by antivirus software and other precautions.

“The total number of infected machines that were not handled by antivirus protections was approximately 160 across 12 agencies,” Beckham said.

There are no reports of files being encrypted or of data loss, Beckham said.
“Cybersecurity is a current trend that all industries are dealing with. The challenge is to provide convenient, flexible technology tools to employees and consumers without compromising the security of our systems.”

—Robert Lanni, CIO & SVP, Conbee Inc.

914INC: If your IT budget were limitless, what would be on your wish list and why?

Coppola: I'd put more into securing systems. You don't want to be the next Yahoo, the next company that gets hit. You don't want to be on the front page of the papers [because of something like that].

Cacchiani: With all the money in the world, I would spend more on the planning side, to be sure we can build what we need to execute.

Jacknis: One issue with budgets is the push and pull between maintaining what you have and investing in new technology. As a CIO, I was aggressive in throwing old things out, but a lot of CIOs don't have the power to do that. Many of them would like to do new things because 70 percent of their budget is just maintaining old things.

Lanni: I would invest in IT R&D to expand the use of artificial intelligence, robotics, and home automation — the Internet of Things. All of these technologies will have an increased impact on how we work, play, shop, socialize, and live. Plus, I think they are cool.

914INC: What are the most common mistakes made by business owners or managers, regarding IT needs?

Jacknis: Fear. From fear, you don't ask tough questions because you are afraid of looking
The Cyber Environment

People

Cyber Identity

Information Layer

Physical Infrastructure

Geographic Layer

© 2016 In-Q-Tei, Inc.
Everything Connected

One individual...

...with multiple, complex relationships to other levels of the environment...

...that also change over time.
The SentinelOne Endpoint Protection Platform

**Nation-grade APTs**
- File-less / Memory-only malware
- Exploits & script-based attacks

**Common threats**
- Blocked files & applications

**PREVENTION**
- Dynamic Whitelisting / Blacklisting
- Cloud Intelligence

**DETECTION**
- Advanced Static Analysis
- Dynamic Behavior Detection

**RESPONSE**
- 360-degree Attack View
- Forensics

**PRE-EVENTION**
- Dynamic Behavior Detection

**ON-EVENTION**
- Static Protection

**POST-EVENTION**
- Mitigation
- Remediation
- Rollback
- Auto-immunize

**Common threats**
- APTs
- File-based malware

**Dynamic Protection**
- Dynamic Behavior Detection
- Dynamic Whitelisting / Blacklisting
- Cloud Intelligence

**360-degree Attack View**
- Prevention
- Detection
- Response

**HI-LINK TECHNOLOGY GROUP**
Advanced Static Prevention

- Major breakthrough in signature-less detection, based on machine learning

- **Deep File Inspection (DFI) engine** prevents advanced malware—on access

- Supported on all endpoint platforms: **Windows / MacOS / Linux**

- Engine supports all mitigation actions

31,000 Unique file characteristics defined and referenced

Known *and* unknown file-based malware
<table>
<thead>
<tr>
<th>Source</th>
<th>Action</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>WINWORD.EXE (shipment.doc)</td>
<td>gathered WMI information</td>
<td>WINWORD.EXE (shipment.doc)</td>
</tr>
<tr>
<td>OUTLOOK.EXE</td>
<td>created process</td>
<td>WINWORD.EXE (shipment.doc)</td>
</tr>
<tr>
<td>WINWORD.EXE (interactive session)</td>
<td>installed a low level key logger</td>
<td>WINWORD.EXE (interactive session)</td>
</tr>
<tr>
<td>WINWORD.EXE (interactive session)</td>
<td>checked whether process is being debugged</td>
<td>WINWORD.EXE (interactive session)</td>
</tr>
<tr>
<td>WINWORD.EXE (interactive session)</td>
<td>checked whether process is being debugged</td>
<td>WINWORD.EXE (interactive session)</td>
</tr>
<tr>
<td>WINWORD.EXE (interactive session)</td>
<td>created process</td>
<td>cmd.exe (CLI interpreter)</td>
</tr>
<tr>
<td>WINWORD.EXE (interactive session)</td>
<td>created process</td>
<td>conhost.exe</td>
</tr>
<tr>
<td>WINWORD.EXE (interactive session)</td>
<td>created process</td>
<td>waitfor.exe</td>
</tr>
<tr>
<td>WINWORD.EXE (interactive session)</td>
<td>created process</td>
<td>FXC_ProxyProcess.exe</td>
</tr>
<tr>
<td>WINWORD.EXE (interactive session)</td>
<td>created process</td>
<td>WINWORD.EXE (interactive session)</td>
</tr>
<tr>
<td>WINWORD.EXE (interactive session)</td>
<td>created process</td>
<td>WINWORD.EXE (interactive session)</td>
</tr>
<tr>
<td>WINWORD.EXE (interactive session)</td>
<td>created process</td>
<td>WINWORD.EXE (interactive session)</td>
</tr>
<tr>
<td>WINWORD.EXE (interactive session)</td>
<td>created process</td>
<td>WINWORD.EXE (interactive session)</td>
</tr>
<tr>
<td>WINWORD.EXE (interactive session)</td>
<td>created process</td>
<td>WINWORD.EXE (interactive session)</td>
</tr>
</tbody>
</table>
Suspicious Behavior → Quarantine

SOC Analysis

- Quarantine
- Remediation
- Detection
- SOC
Visionary Leader on the 2017 Gartner MQ

“...SentinelOne has had stellar growth in the enterprise EPP market, and expects it to continue for the next couple of years as it maintains a reputation as a leading NGAV vendor.”

Visionary Quadrant Leader
Gartner 2017 Magic Quadrant Endpoint Protection Platforms

Gartner, Magic Quadrant for Endpoint Protection Platforms, 30 January 2017
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.
Your data and applications are moving to the cloud:

62% of organizations will run 100% of their IT in the cloud by 2020.
Your employees are mobile and connected everywhere:

61% of workers report working outside the office at least part of the time
Data breaches are at an all-time high:

43% of companies had a data breach in the past year.
Attacks are broader, deeper and more sophisticated than ever before.
DNS Security is Crucial

01 76% subject to a DNS attack

02 Networks exploited by:
   - Botnet Command and Control (C&C)
   - Advanced Persistent Threat (APTs)
   - Drive-by-downloads
   - Phishing

03 Ports 80 & 443 are generally open
Primary DNS Risks

01 APTs

02 Botnet Malware

03 DNS Changer Trojans

04 Ransomware

05 Web users
Webroot SecureAnywhere® DNS Protection

01. Stops DNS attacks by protecting the DNS connection

02. Filters high-risk sites with zero latency

03. Enforces acceptable web access

04. Gives visibility of web access / usage

05. Helps maintain staff productivity

06. Lowers risk, infections, and remediation costs

Reduces the number of malware threats that infect the network by up to 90%
What is SIEM?

- What devices in your network have logs?
- Is there valuable security related data in the logs?
- Do you monitor them?
  - Real-time
  - Hourly
  - Daily
  - Weekly
  - Monthly
  - Yearly
What is SIEM?

- Even a small network can generate millions of log records daily generating dozens or hundreds of “alerts”
- Each of these logs has a unique format
- Maybe you have implemented a syslog server and tried to monitor for specific lines of activity
- Now how do you leverage it?

This is where SIEM begins and basic log management ends!
What is SIEM?

• Security and Event Management (SIEM)
  • Coined by Gartner in 2005
  • An approach that combines:
    • SIM (Security Information Management)
      • Collecting, monitoring and analyzing security related data from logs
    • SEM (Security Event Management)
      • Alerting on specific triggers in log data
  • Pronounced “sim” with a silent e
Centralized Log Management

Centralized log collection and storage is used to fulfill an operational need.

SIEM

The technology began to extract intelligence from logs to meet a compliance or security need.

SIEM ++

SIEM vendors add adjacent technologies like VAS, IDS, flow analysis and deception (honeynet), for greater security and compliance.

SIEM-As-A-Service

With greater intelligence comes the need for more monitoring and analysis, but a skills shortage creates a market for managed or co-managed options that help provide a better SIEM ROI.

SIEM-As-A-Utility (future)

In the future, security will be built into the foundation of the network devices.
The Questions We Must Answer

• The 4 W’s
  • Who
    • Who is being attacked?
  • What
    • What is it trying to do?
  • Where
    • Where is the attack coming from?
  • When
    • When did it happen?
Detect and Respond

WHAT WE DO

120,295,524
LOGS ANALYZED

1,519
ALERTS

505
DASHBOARD NOTIFICATIONS

WHAT YOU GET

3
ACTIONABLE EVENTS
Anatomy of an Attack

- Corporate Users
- Branch Office
- UTM
- PROBE
- Attack
- Theft
- Make Config Changes
- Gain Access
- Create Account
- Install Backdoor
- Mail Server
- Corporate Users
- Headquarters
- Web Server
- Firewall
- Switch
- Router
- AV/Spam Spyware
No Hardware Required

Over 2,100 Log Types / Sources

Threat Response Capabilities

Ideal for compliant-centric customers

Powered by EventTracker

Actionable Security Intelligence

Real-Time Response

Endpoint Sensor

Threat Intelligence

SIEM

24/7 SOC

Continuum SOC Managed
COMPLIANCE

- PCI DSS
- JAFAN
- HIPAA
- NERC / CIP
- 23 NYCRR 500
- DoDI 8500
- SOX 404
- ARS v2.0
- FISMA/NIST 800-53
- ISO 27001
- GPG-13
- ISO 27002
- SANS CAG
- SAS-70-SOC
- GLBA
- NCUA
- EU GDPR
- GCSx
- NISPM
- DFARS
- FFIEC/CFPB
- NIST 800-171
- ICD503/DCID 6/3
What Should You Do Today?

- Vulnerability assessment
- Review how your IT team handles SPAM, technical policies and computer updates
- Employee training
- Replace your old anti-virus software
- Turn on all the security features of your firewall
- Encrypt anything that goes mobile
- Backup, backup and backup again
- Have a cyber incident response plan!