Next-Generation Endpoint Protection

Enduser Protection

Tom Bulthaupt
Sr. Security Engineer

SOPHOS

NEWS

US college pays $28,000 to get files back after ransomware attack

10 JAN 2017 7

Data loss, Malware

Previous: News in brief: cookie monster slain; FBI disclo...

Next: The Spy, sorry, The Fridge Who Loved Me

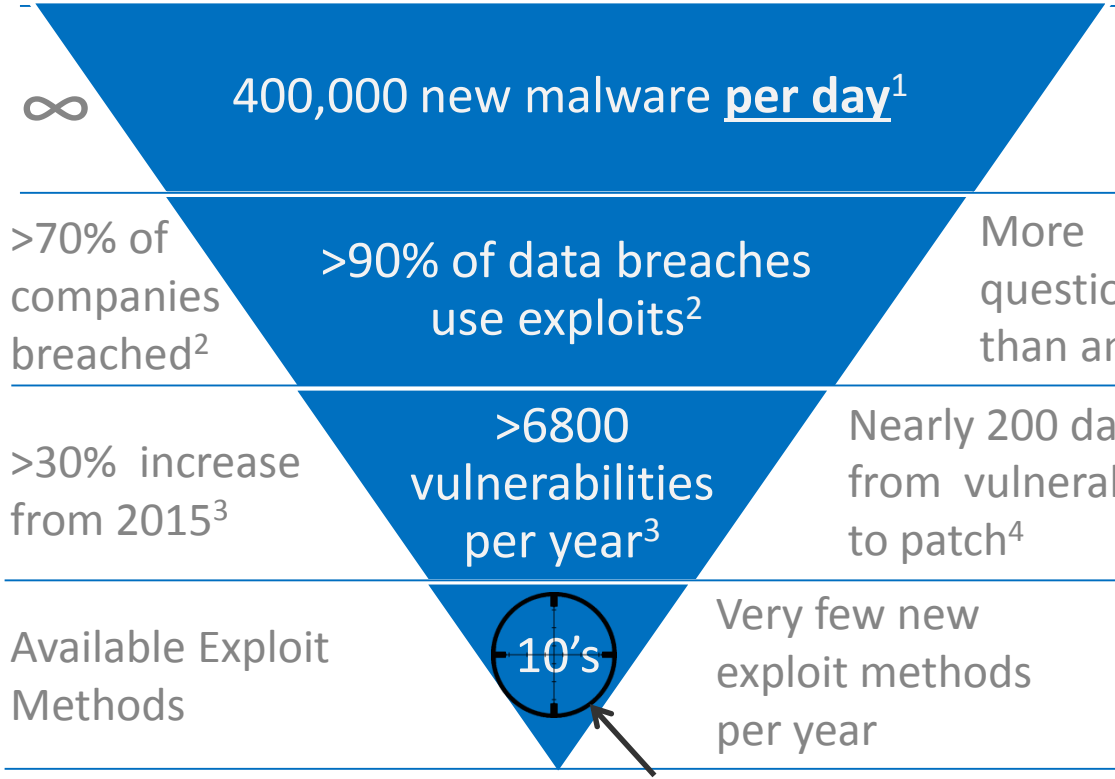
by John E Dunn

f 0

Los Angeles Valley College (LAVC) has paid a public record of $28,000 (£22,500) in Bitcoins to extortionists after ransomware encrypted hundreds of thousands of files held on its servers.

CSO | Feb 14, 2016 3:43 PM PT

Data Breaches - The root of the problem



More questions than answers

Nearly 200 days from vulnerability to patch[4]

Very few new exploit methods per year

Traditional Anti-Virus

- File Analytics
- Heuristics
- URL Blocking
- Black/White Lists
- Signatures
- Sandboxing

SIEM, EDR, UEBA

- Anomaly Detection
- Security Operations Center
- Forensic breach assessment teams

Patch Management

- Vulnerability Scanning
- Device Management
- Patch testing and deployment

Sophos - Intercept

- Exploit and Ransomware prevention
- Incident Response Report
- Automatic Root Cause Attribution

1 – Virus Total 2 – NSS Labs
3 – Gartner 4 – White Hat Security

Anti-Exploit – Targets the root of the problem

IT Ops

Anti-Hacking

Traditional anti-malware

- Understand the malware
- Identify its components
- Block its delivery
- Detect its presence on the device through file, process, signal and attribute monitoring
- Lockdown the device to trusted applications only

This method looks for malware

Next Generation

- Understand objectives and methods used
- Detect the attack on the device and processes
- Stop the malicious activity
- Track the action to a root cause
- Provide answers to critical questions

This method looks for hacking

Sophos Intercept X

Core Capabilities

- Signatureless detection
  - CryptoGuard – Detect and recover from Ransomware
  - Comprehensive Exploit Prevention
  - Malicious Traffic Detection
  - Synchronized Security
- Incident Response Report
  - Automatic Identification of root cause
  - IOC artifact list
  - Visualization of the attack events
- Forensic Malware Removal
  - Sophos Clean a 2nd opinion scanner

Packaging

- Intercept X runs alongside competitive AV

SOPHOS

The 'Kill Chain'

Exposure | Delivery | Exploit | Execute | Command Control | Action on Objective

Breach Response

Investigate | Remediate | Adjust Security

Prevent

- **Exposure** – Web Protection, Device Control
- **Delivery** – Download Reputation
- **Exploit** – Runtime Memory Analytics
- **Execution** – File Analytics / Heuristics

- **Exploit** – Exploit Prevention
- **Execution** – CryptoGuard

Detect

- **Command & Control**
  - Malicious Traffic
- **Action on Objective**
  - Data Loss Prevention
  - Auto-Start registry

- **Action** – Event Recorder

Respond

- **Investigate**
  - Alerting and Reports
- **Remediate**
  - Malware Removal
  - Malware Quarantine

- **Investigate** – Incident Report
- **Remediate** – Forensics Cleanup
- **Adjust Sec** – Recommended Actions

SOPHOS

Thank You

Questions ???