

Next-Generation Endpoint Protection

Enduser Protection



Tom Bulhaupt
Sr. Security Engineer

SOPHOS

Ran offli

f |
A K
atta
data



Credit: [Hollyw](#)

Network million c

CSO | Feb 14, 2016 3:43 PM PT

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 disco... Next: The Spy, sorry, The Fridge Who Loved Me →

by John E Dunn



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.

Capital kickers

LIKE THIS

EMC, hospital to pay \$90,000 over stolen laptop with medical

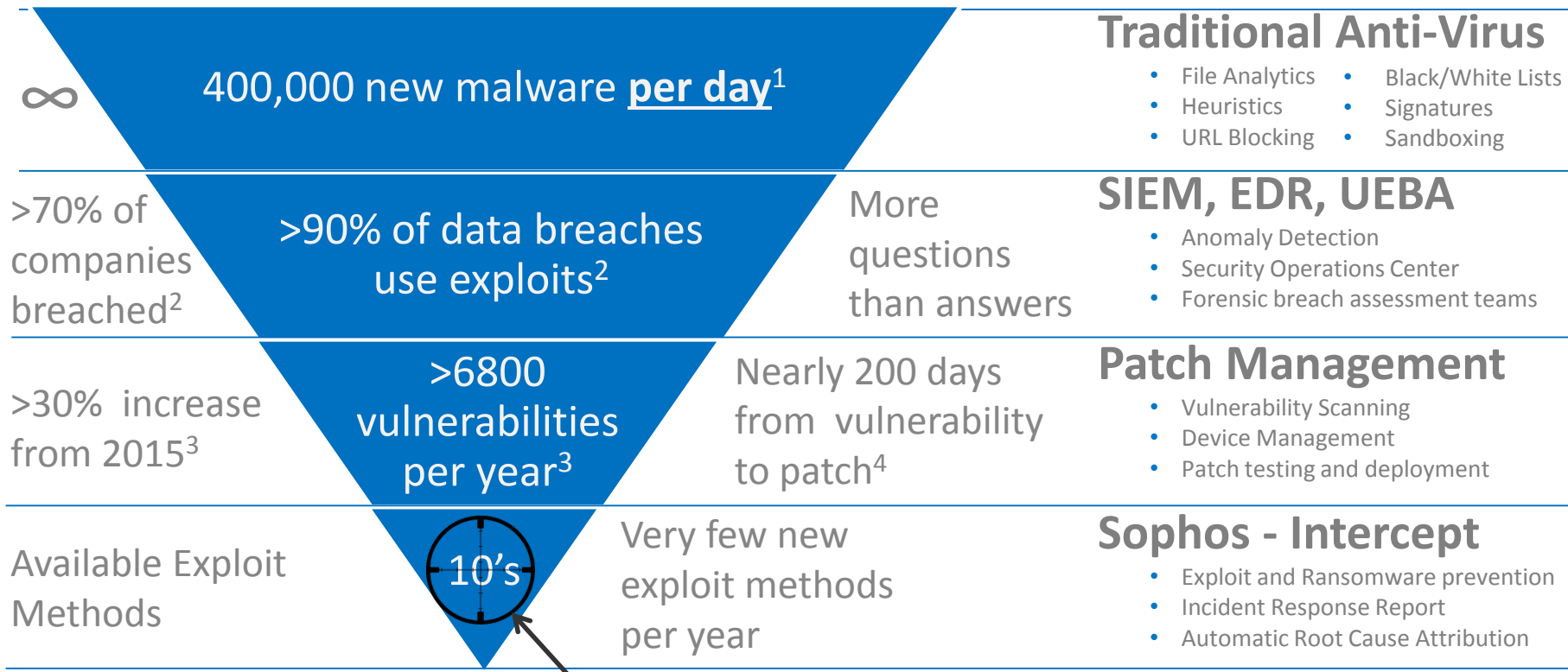
Review: Stop insider attacks with these 6 powerful tools

al Turns Away Patients "Virus" Disrupts Network

How to Turn on Windows 10's 'Device' feature?



Data Breaches - The root of the problem



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

CryptoGuard

- Simple and Comprehensive
- Universally prevents spontaneous encryption of data
- Notifies end user on rapid encryption events
- Rollback to pre-encrypted state

CRYPTOGUARD

Exploit Protection

Attack Intercepted

Exploit Test Tool (32-bit) 1.4' has been terminated to prevent execution of malicious code. Please check your computer for malware and software updates.

Threat Details Incident Response

Threat summary

What: Backdoor:Win32/Cryptowall (RaaS), Trojan: Win32/Exploit-Test-Tool (RaaS)

Why: Encrypted common business files and asks for money for file recovery

Where: On WINDOWS (Host belongs to John.Bush)

When: Infected on Oct 29, 2023 9:08 PM
Detected on Oct 29, 2023 9:08 PM

How: Encrypted critical system files

Activity record

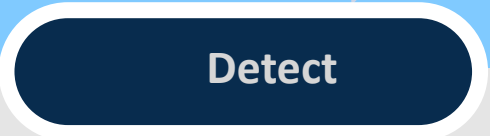
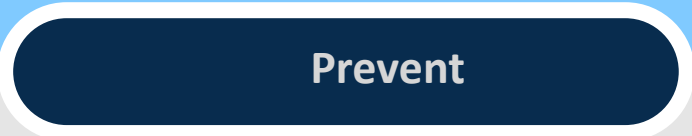
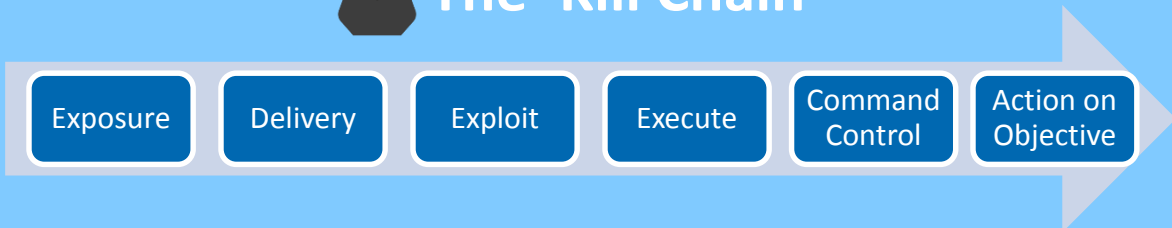
Scan results Sophos Clean

Malicious software was detected. Close all applications and click Next to remove the malware. Certain programs may terminate unexpectedly.

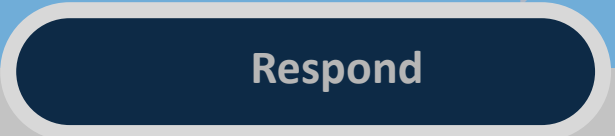
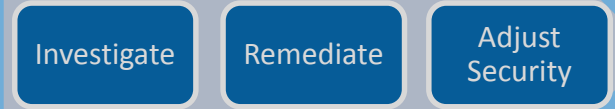
File Name	Signature	Category
Explorer.EXE	[VFP] [6320] Run	Trojan
Win32.Loader.O	[VFP] [6320] Run	Trojan.Win32.Patched.1
cekj\pgehmohobmdikfnopibpmgnm\		iPumper
C:\Documents and Settings\John\Local Settings\Application Data\Google\Chrome\User Data\Default\		NationZoo
browser.startup.homepage		NationZoo
C:\Documents and Settings\John\Application Data\Mozilla\Firefox\Profiles\zuyzy6r.default\prefs.js		NationZoo
Launch Internet Explorer Browser.lnk		NationZoo



The 'Kill Chain'



Breach Response



Exposure – Web Protection, Device Control

Delivery – Download Reputation

Exploit – Runtime Memory Analytics

Execution – File Analytics / Heuristics

Exploit – Exploit Prevention

Execution – CryptoGuard

Command & Control

- Malicious Traffic

Action on Objective

- Data Loss Prevention
- Auto-Start registry

Action – Event Recorder

Investigate

- Alerting and Reports

Remediate

- Malware Removal
- Malware Quarantine

Investigate – Incident Report

Remediate – Forensics Cleanup

Adjust Sec – Recommended Actions

Thank You

Questions ???