Stop the Exploit. Stop the Attack.

Justin Walker & Chris Chaves

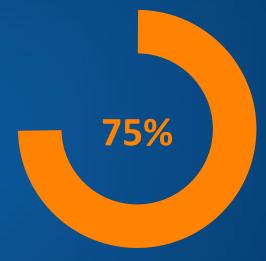
February 2018



The age of single-use disposable malware



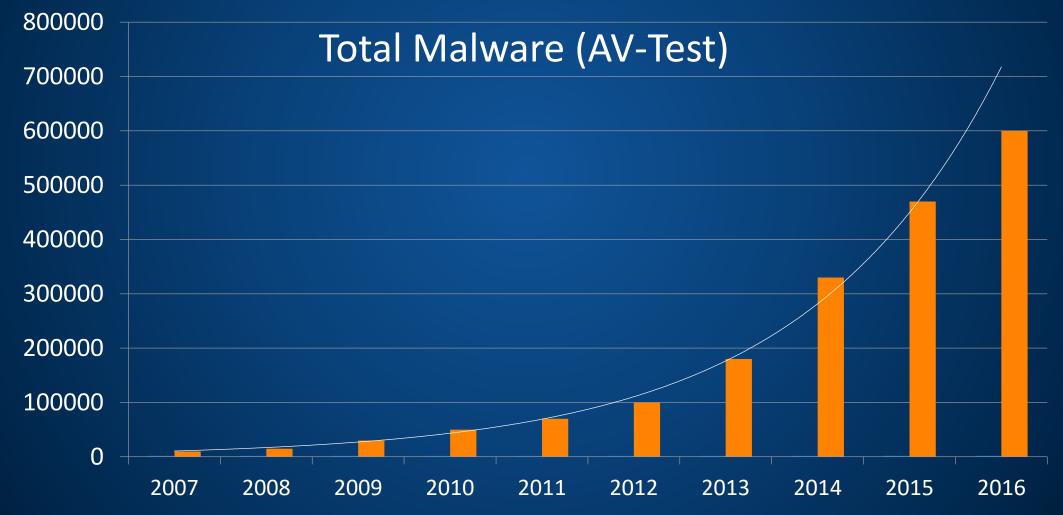
SophosLabs receives and processes 400,000 previously unseen malware samples each day.



75% of the malicious files SophosLabs detects are found only within a single organization.

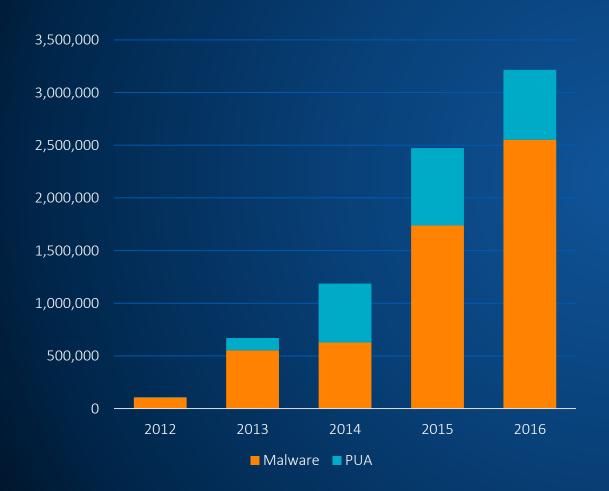
Exponential growth in new malware

27% of all malware variants in history were created in the last 12 months

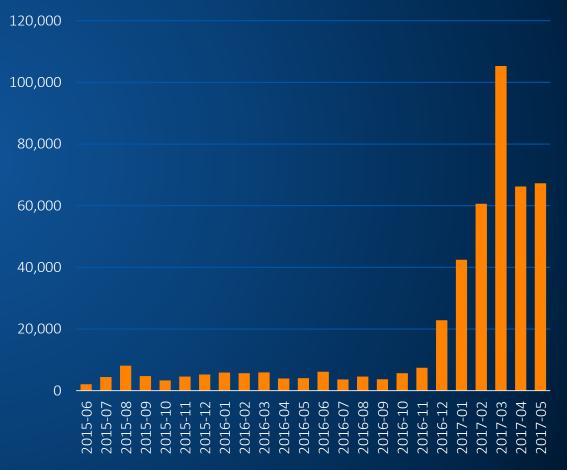


Mobile Threats Are Real...

Android malware keeps growing



Android ransomware

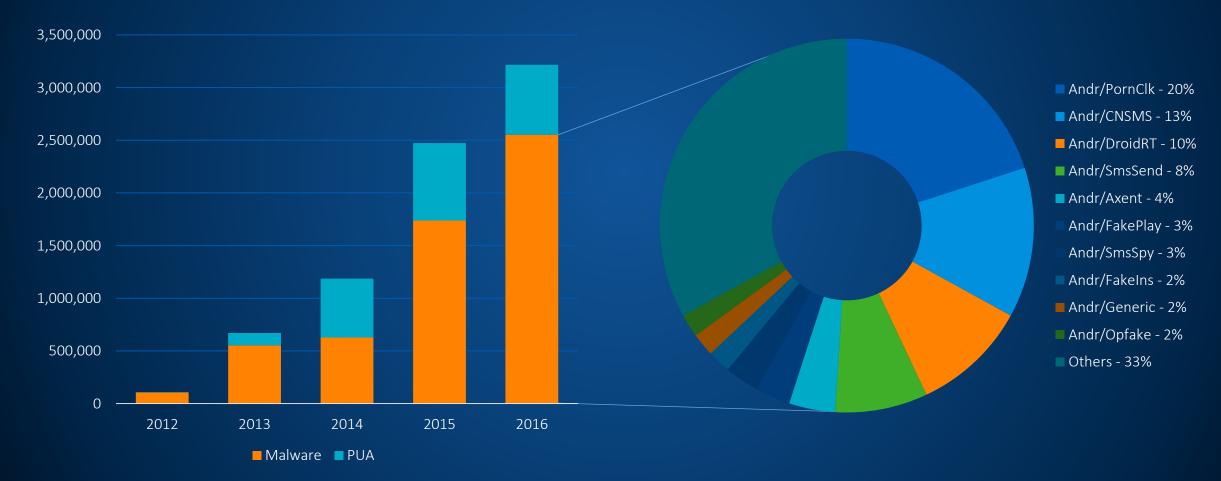


Source: SophosLabs, 2017

Mobile Threats Are Real...

Android malware keeps growing

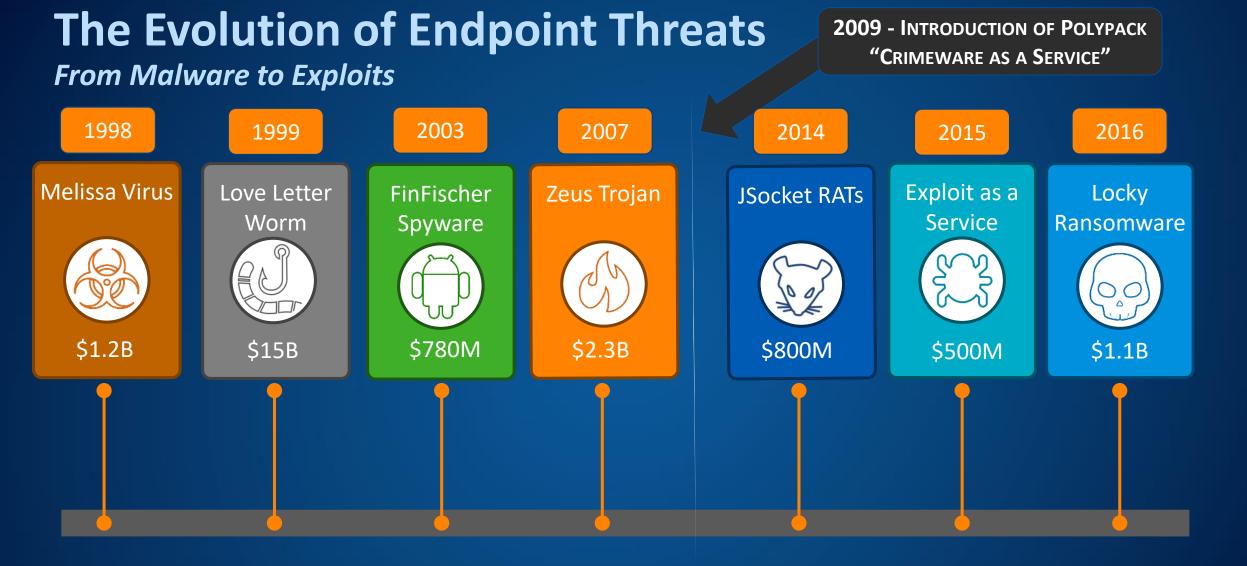
Top ten Android malware 2016



Business Ramifications of a Cyber Attack

- Attacks are from within the perimeter, focused on Software Exploits
- Ransomware alone reached over \$1.2B in damages last year
- Lack of Threat Intelligence after a Breach (What? Where? When? & HOW?)





TRADITIONAL MALWARE

ADVANCED THREATS

From cottage industry for full industrialization

Black hole ^β	9	STATISTICS	тн	READS	FILES	SECURITY PRE	FERENCES	5			<u>Loqout</u> ⇒[]	
Adv:						cq#1: JID#2: htries. 24/7. Loads from 8%.						
Start date:		End date	ə:		Apply	Autoupdate interval: 10 s	ec	[FULLY INTEGRATED SAAS
STATISTIC						EXPLOITS			LOADS	96 T		CONSOLE INCLUDING NETWORK
TOTAL INFO					11.25%	🔆 Java OBE >			569	36.69 🔵	_	
23948 HITED	13247	HOSTS -	1490 LOA	DS 🔵	LOADS	PDF LIBTIFF >			326	21.02		AND ENDPOINT TECHNIQUES
	102 11 1	10515				🔆 Java SMB >			227	14.64 🛑		FROM INFECTING A WEBSITE, ALL
-						🔆 FLASH >			162	10.44 🔵		
TODAY INFO 23948 HITED	19047.	Hosts 🔵	1400.00		11.25%	🔆 PDF ALL >			112	7.22 🔵		THE WAY TO DELIVERING AN
23940 HITED	132478	HOSTS	1490104	ibs 🔷	LOADS	🔆 JAVA SKYLINE >			103	6.64 🔵		ENDPOINT PAYLOAD AND SELLING
-						🔆 HCP >			52	3.35 🔵		
05 1	HITS	HOSTS	LOADS	96								THE RESULTS
Windows 7	10506	5609	293	5.22		BROWSERS 1	HITS	HOSTS	LOADS	96		
Windows Vista	1015	636	79	12.42		Firefox >	5912	3855	465	12.08 🔵		
Windows XP	12427	7366	1136	15.44		💋 MSIE >	6570	3728	569	15.28 🔵		
Mildons Ar	12427	7300	1150	15.44		O Opera >	11466	6165	484	7.85 🔵		
THREADS	HITS T	HOSTS	LOADS	96		COUNTRIES	HITS	HOSTS 1	LOADS	96	_ =	
>	11967	6850	745	10.88 🔵		Russian Federation	23937	13239	1490	11.25 🔵		
>	6784	3926	453	11.54 🔵		Germany	3	2	0	0.00		ZERO DAY EXPLOITS
• •	5182	3064	314	10.25 🔵		🔡 United Kingdom	2	2	0	0.00		
default >	11	8	0	0.00		Ukraine	2	1	0	0.00		AUTOMATICALLY INCLUDED
>	4	3	0	0.00 (Netherlands	2	1	0	0.00		
						United States	1	1	0	0.00		
						Greece	1	1	0	0.00		
CROSS P	LATFOR	rm & A	AGILE D	EVELOP	PED	[Add w	idget			

We insist on being vulnerable

"Patch Tuesday"

In the Perfect World

- Patch Fast, Patch Often
- Defect-Free Software



"Exploit Wednesday"

In the Real World

- Slow to Patch
- Zero-Day Exploits Continue



Threats evolve and security must adapt or die



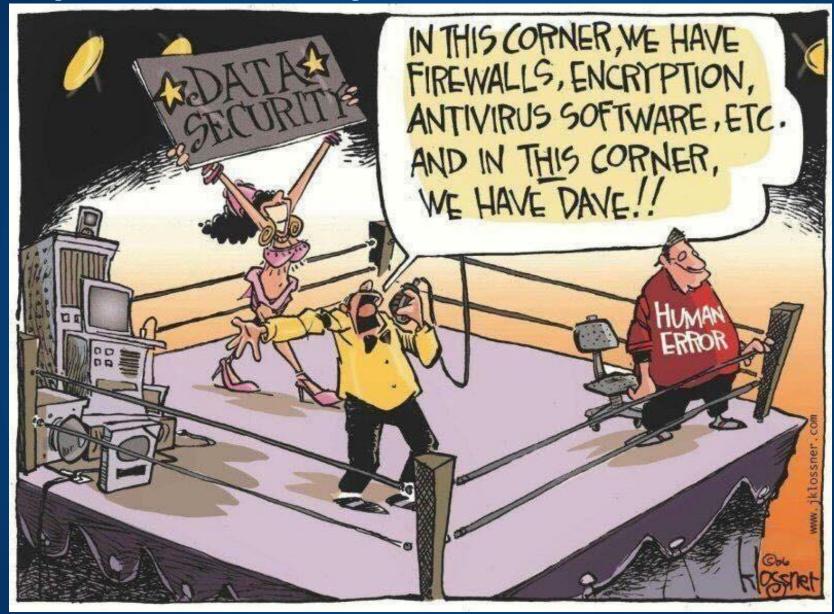




ADVANCED MALWARE

ACTIVE ADVERSARY LIMITED VISIBILITY

You're only as secure as your users



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 Runs alongside competitive AV
- Ultimate is the most complete Sophos EP

CryptoGuard

SOPHOS

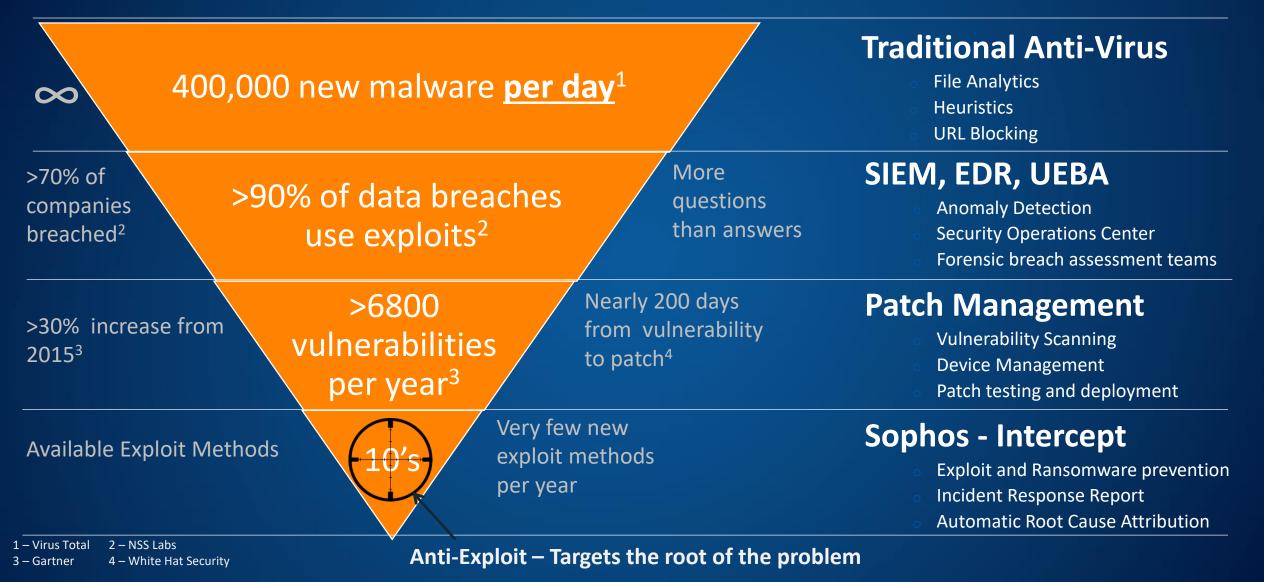
- Simple and Comprehensive
- Universally prevents spontaneous encryption of data
- Notifies end user on rapid
 encryption events
- Rollback to pre-encrypted state



Exploit Protection

		1 Attack Intercepted	
		Taploit Test Tool (32-bit) 1.4" has been terminated to prevent execution of malicious code. Please check your computer for malware and software updates.	
		mittigettim ADM #00 ADDisation C:lowertineskingibugelertitast.#ea Becorptic Fastici Mitti 123413 -tast. Becorptic Pastici Mitti 0	
	Details	Help = Marbus Junes = ABC Dary - Permany Admin	
	incident R		
Threat su	ammary	Activity record	
What:	Randammanna, Cryptoscall v234, Intenst. 3 Interiment file in investment.	👤 Glan Smith	
Why:	Encrypta common business files and usits for manay for the orvetter	What's happening?	1
Where:	On WSKD345 that belongs to John Booth	Gam Smith Ont 30, 2015 5.00um	1
When:	Infractual en: Oct 29 (2015 2:08 PM Detected en: Oct 29 (2015 2:10 PM Removar ettach vector aux used	Users Smith? Unit 30, 2013 KUNARY This looks bad Elea south have been encrypted before detection. I'm going to write loads brike to show you have it	
How:	Browner affach vector was used	Glam Smith Oct 29, 3015 4 30gm	
Use Monthal	If your buildness files been imported by checking the list on Associates to see a recording of the thread as it happened. Up to with your investigation and imported provide the second pro- tein the the second second as the second second and activation of the the holes modulate as High as It's considerance and activation the infection and detection. Check and adjust as resolution.	Scan results Sophos Clean Malicious software was detected. Close all applications and click Next to remo certain programs may terminate unexpectedly.	ove the malicio
		Explorer.EXE WFP 1620 Run B Win32.Loader.O K Trojan.Win32.Patched.kl	🖇 Trojan
		cekcjpgehmohobmdikfnopibipmgnml\ C: \Documents and Settings\John\Local Settings\Application Data\Google\Chrome\User	IPumper
		browser.startup.homepage C:\Documents and Settings\John\Application Data\Mozilla\Firefox\Profiles\7zuyzy6r.di	NationZoc efault/prefs.js
		Launch Internet Explorer Browser.ink	NationZoo

Data Breaches - The root of the problem



Exploit Mitigation Techniques by Vendor

NOP sled and Polymorphic NOP sled only; no Flash Vector heap spray detection

Comprehensive Exploit Mitigation

- 20+ mitigation techniques
- Successful attacks often leverage 2-4 techniques in series
- Only 1-2 major new techniques are developed per year
- 100% signatureless

Exploit Mitigation Tecniques	Sophos Intercept X	ESET Smart Security	Kaspersky Endpoint Security	McAfee Endpoint Security	Symantec Endpoint Protection	Trend Office Scan	Webroot	Cylance PROTECT	Microsoft EMET	Malwarebytes Anti-Exploit	Palo Alto Networks Traps	Crowdstrike Falcon
Enforce Data Execution Prevention (DEP)												
Prevents abuse of buffer overflows				-						•		•
Mandatory Address Space Layout Randomization (ASLR) Prevents predictable code locations	•								•1		•	•1
Bottom Up ASLR Improved code location randomization	•								•	•		
Null Page (Null Dereference Protection) Stops exploits that jump via page 0	•								•			
Heap Spray Allocation Pre-allocated common memory areas to block attacks					•				•	•		•
Dynamic Heap Spray Stops attacks that spray suspicious sequences on the heap	•				_1						• 2	
Stack Pivot Stops abuse of the stack pointer	•											
Stack Exec (MemProt) Stops attacker' code on the stack	•											
Stack-based ROP Mitigations (Caller) Stops standard Return-Oriented Programming attacks	•											
Branch-based ROP Mitigations (Hardware Augmented) Stops advanced Return-Oriented Programming attacks	•											
Structured Exception Handler Overwrite Protection Stops abuse of the exception handler					•				•			
[1] Based on ASLR functionality offered by Windows, available only in Windows Vista and newer versions of Windows												

Exploit Mitigation Techniques by Vendor (cont.)

Comprehensive Exploit Mitigation

- Detection of exploit techniques requires no prior knowledge of the vulnerability being exploited
- Exploit behavior is a clear indicator of malicious intent

Exploit Mitigation Tecniques	Sophos Intercept X	ESET Smart Security	Kaspersky Endpoint Security	McAfee Endpoint Security	Symantec Endpoint Protection	Trend Office Scan	Webroot	Cylance PROTECT	Microsoft EMET	Malwarebytes Anti-Exploit	Palo Alto Networks Traps	Crowdstrike Falcon
Import Address Table Access Filtering (IAF) Stops attackers that lookup API addresses in the IAT									EAF ³			
Load Library Prevents loading of libraries from UNC paths									•	•		
Reflective DLL Injection Prevents loading of a library from memory into a host process												
Shellcode Stops code execution in the presence of exploit shellcode												
VBScript God Mode Prevents abuse of VBScript in IE to execute malicious code												
WoW64 Stops attacks that address 64-bit function from WoW64 process												
Syscall Stops attackers that attempt to bypass security hooks												
Hollow Process Stops attacks that use legitimate processes to hide hostile code												
DLL Hijacking Gives priority to system libraries for downloaded applications												
Application Lockdown Stops logic-flaw attacks that bypass mitigations										•	•	
Java Lockdown Prevents attacks that abuse Java to launch Windows executables												
Squiblydoo AppLocker Bypass Prevents regsvr32 from running remote scripts and code												
[3] EAF - Export Address Filtering												

Anatomy of a Ransomware Attack

Exploit Kit Spam wit Infection Command & Control Establishe



Ransomware deleted, Ransom Instructions delivered

Pre Web prote Download Device cor

CryptoGuard – Behavior Monitor

- Simple and Comprehensive
- Universally Prevents Spontaneous Encryption of Data
- Restores Files to Known State
- Simple Activation in Sophos Central

Reference of the second second

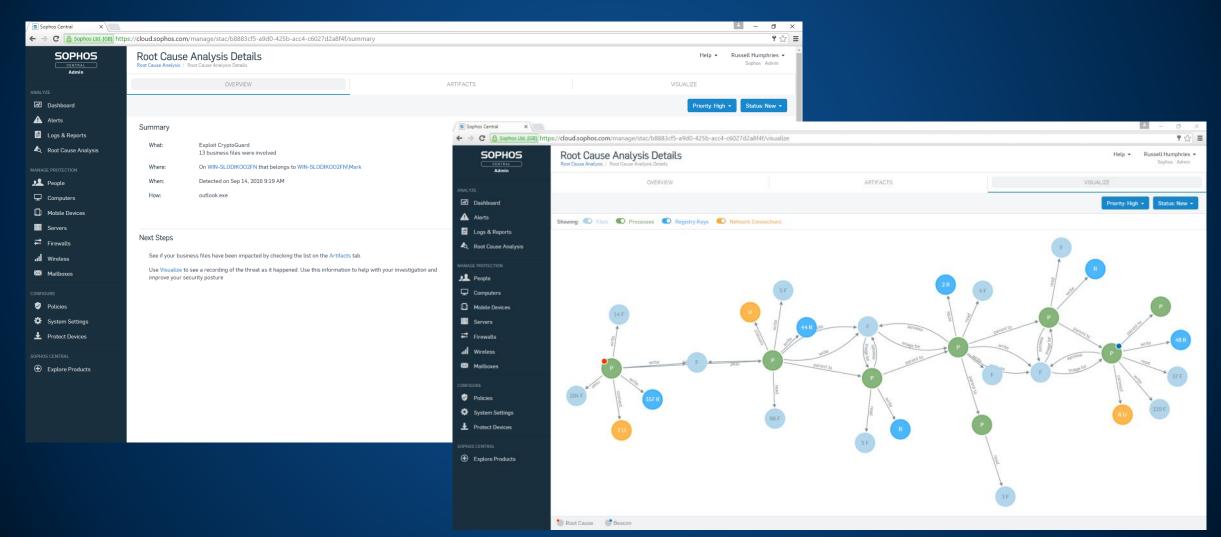
K

File analytics Heuristic evaluation On-device emulation Signature checking

Pr

Root Cause Analysis

Understanding the Who, What, When, Where, Why and How



SOPHOS Security made simple.