Security Mindsets to Adopt Today

Sentinel IPS

Ted Gruenloh
Director of Operations
Sentinel IPS

@tedgruenloh
@sentinelips

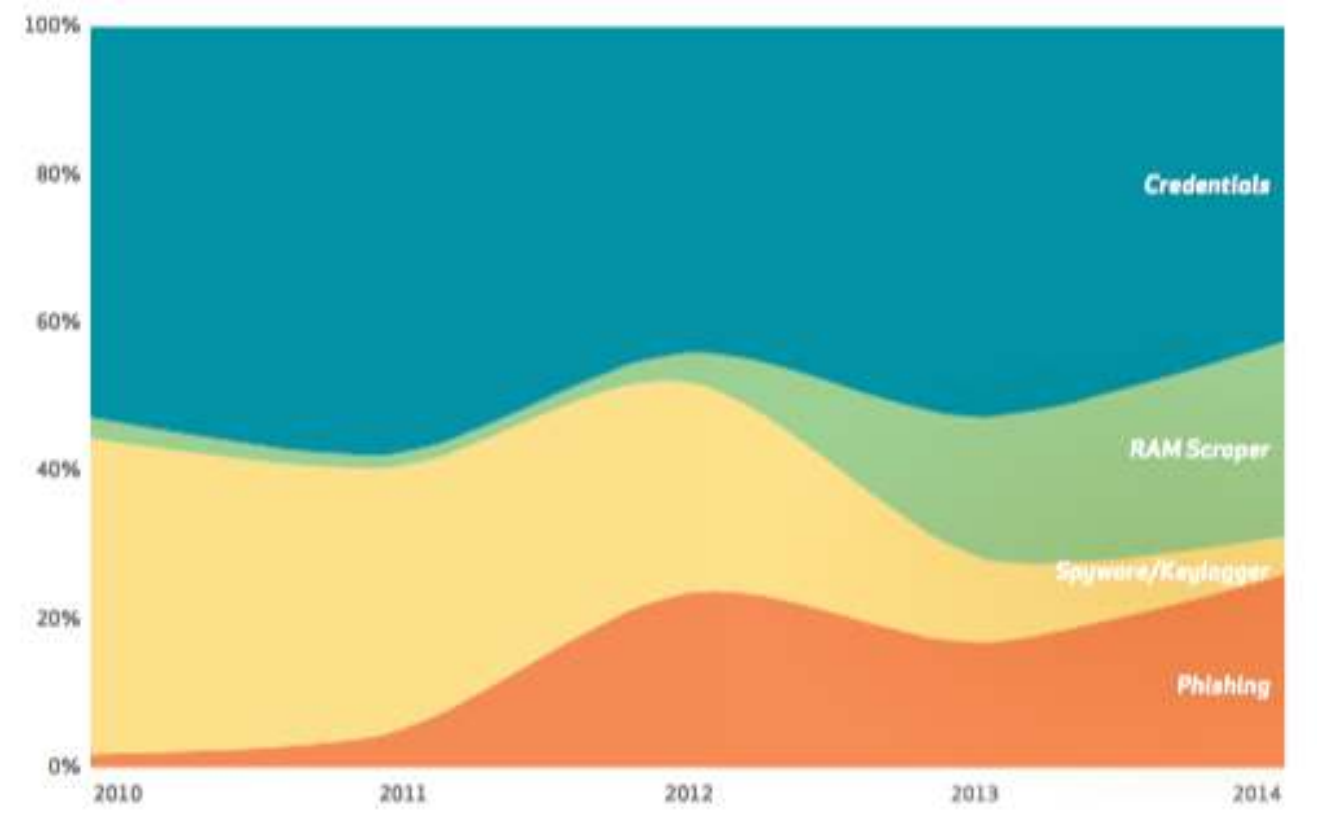
NETWORK SECURITY

isn't about devices or hardware.

- ✓ Don't you love sensationalist statements like that?
- ✓ Permission to speak freely, sir?
- ✓ Every network is different.
- ✓ Security should be about MINDSETS.

1 FIX THE PEOPLE.

Threat Actions



Source: Verizon 2015 Data Breach Investigations Report

1 FIX THE PEOPLE.

- ✓ ~60% of threat actions take advantage of PEOPLE.
- ✓ So many examples, so little time. (Sally Beauty, Target, etc.)
- ✓ Better credentials should be easy. The no-brainers:


What makes a great password?


How are your application logins?


Do people take their logins seriously?

- ✓ Strongly consider **consistent** training and testing.

http://www.securingthehuman.org/enduser/

2 NEW-SCHOOL LAYERED SECURITY.

- ✓ Now it's all about VISIBILITY.
- ✓ And, it's a combination of people, policies, and devices
- ✓ And, it includes protection, detection, and disruption
- ✓ Parallels to another old-school term: The Cyber Kill Chain

2 NEW-SCHOOL LAYERED SECURITY.

Simplified Kill Chain paralleling protection, detection, disruption, and VISIBILITY.

Recon	People, IPS/IDS, Firewall, Scanning, vulnerability, and penetration testing, active threat intelligence
Weaponization & Delivery	Policy (e.g., USB flash drives), People (e.g., phishing), IPS/IDS, mail and SPAM filters, web proxies, patching procedures
Exploitation & Installation	Anti-virus, host-based solutions, sandbox solutions (e.g., FireEye), HIPS
Command & Control	IPS/IDS, SIEM with threat intelligence, Network Monitoring tools, NetFlow anomalies
Actions & Objectives	NetFlow anomalies, Network Monitoring tools, DLP, system hardening and network segmenting to disrupt movement

3 KNOWING WHAT'S NORMAL &

4 BEING ABLE TO ACT WHEN IT'S NOT.

- ✓ Tools for knowing what's normal … You know better than I do
- ✓ Living in the real world: What's most important to you?
- ✓ Plan in place for fixing what's important to you, quickly?
- ✓ These two are all about RELEVANT DATA.

5 THREAT INTELLIGENCE: THE NEW BLACK

- ✓ What is “Threat Intelligence”, again?
- ✓ “Actionable” vs. “Active” Threat Intelligence

FREE

EMERGING THREATS
http://rules.emergingthreats.net

SentinelIPS
CI Army list at http://cinsscore.com

ALIEN VAULT
Open Threat Exchange

http://shadowserver.org

INTERNET STORM CENTER
http://dshield.org
(SANS Internet Storm Center)

NOT-SO-FREE

THREATSTREAM

THREATCONNECT

iSIGHTPARTNERS

6 HANG WITH THE COOL KIDS.

- ✓ Membership in industry info-sharing groups, like the ISACs
- ✓ Are you on Twitter yet? Here are some good follows:

@briankrebs
@DarkReading
@SCMagazine
@SentinelIPS
@AlienVault
@ThreatPost
@CISecurity
@SearchSecurity
@KimKardashian

7 YOU'VE BEEN BREACHED.

- ✓ OK, maybe not. But how do you know?
- ✓ Rethink traditional layers, from the inside out
- ✓ Play 'what-if?' and prioritize
- ✓ Influences all the other MINDSETS.

1. FIX THE PEOPLE.
2. NEW-SCHOOL LAYERED SECURITY.
3. KNOW WHAT'S NORMAL.
4. BE ABLE TO ACT WHEN IT'S NOT.
5. THREAT INTELLIGENCE.
6. HANG WITH THE COOL KIDS.
7. ASSUME YOU'VE BEEN BREACHED.

THANKS!
QUESTIONS?

Ted Gruenloh
Director of Operations
(972) 991-5005
tedg@sentinelips.com

Download the eBook at
http://www.sentinelips.com

@tedgruenloh &
@sentinelips

Ted Gruenloh