Harnessing Analytics for Proactive and Preventive Security

Cisco Day with PLDT and SMART

4 October, 2015

ener Camiling
ecurity Sales Manager, GSSO

camilin@cisco.com

@gencam

s affiliates. All rights reserved.

he Perfect Storm

Digitization

+

Internet of Everything

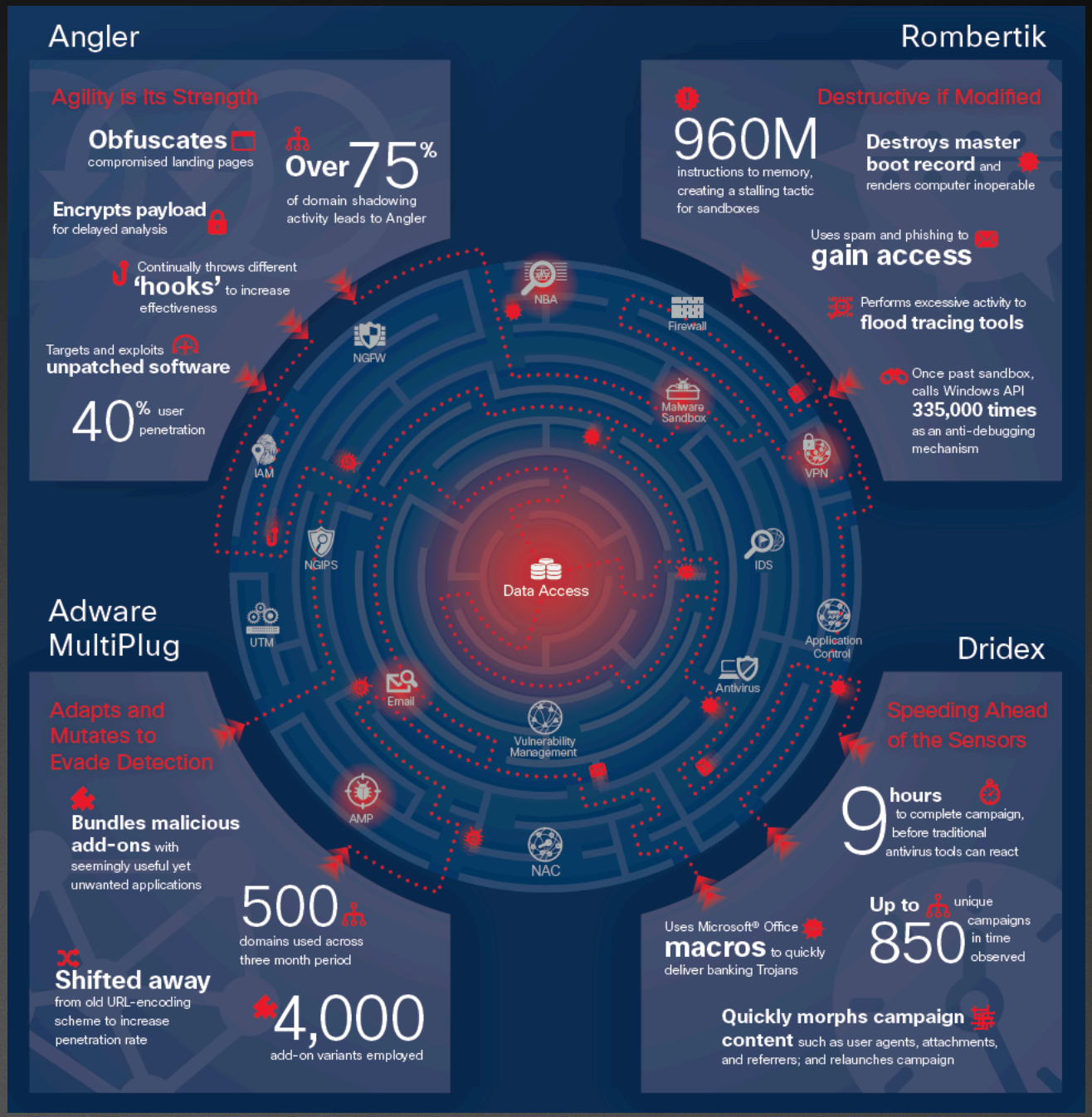
Experian Gets Hacked, Exposing SSNs, Data From 15 Million T-Mobile Customers

Credit monitoring firm suffers its second major data breach.

Credit monitoring firm Experian North America yesterday announced that one of its servers had been breached and personal information of some 15 million T-Mobile USA customers had been exposed, including names, dates of birth, addresses, Social Security numbers, and other forms of identification.

Among the victims were new applicants for T-Mobile services who were undergoing a credit check. The encryption for the SSNs and other ID information may have been compromised, according to T-Mobile.

"The investigation is ongoing, but what we know right now is that the hacker acquired the records of approximately 15 million people, including new applicants requiring a credit check for service or device financing from **September 1, 2013 through September 16, 2015,**" said T-Mobile CEO John Legere in a statement to customers. "These records include information such as name, address and birthdate as well as encrypted fields with Social Security number and ID number (such as driver's license or passport number), and additional information used in T-Mobile's own credit assessment. Experian has determined that this encryption may have been compromised. We are working with Experian to take protective steps for **all** of these consumers as quickly as possible."


Angler
Agility is Its Strength
Obfuscates compromised landing pages
Over 75% of domain shadowing activity leads to Angler
Encrypts payload for delayed analysis
Continually throws different 'hooks' to increase effectiveness
Targets and exploits unpatched software
40% user penetration
Rombertik
Destructive if Modified
960M instructions to memory, creating a stalling tactic for sandboxes
Destroys master boot record and renders computer inoperable
Uses spam and phishing to gain access
Performs excessive activity to flood tracing tools
Once past sandbox, calls Windows API 335,000 times as an anti-debugging mechanism
NBA
Firewall
NGFW
Malware Sandbox
IAM
VPN
NGIPS
IDS
Data Access
UTM
Application Control
Antivirus
Email
Vulnerability Management
AMP
NAC
Adware MultiPlug
Adapts and Mutates to Evade Detection
Bundles malicious add-ons with seemingly useful yet unwanted applications
500 domains used across three month period
Shifted away from old URL-encoding scheme to increase penetration rate
4,000 add-on variants employed
Dridex
Speeding Ahead of the Sensors
9 hours to complete campaign, before traditional antivirus tools can react
Up to 850 unique campaigns in time observed
Uses Microsoft® Office macros to quickly deliver banking Trojans
Quickly morphs campaign content such as user agents, attachments, and referrers; and relaunches campaign

tegrated Threat Defense Architecture

Visibility

Control

Intelligence

Context

Faster Time to Detection, Faster Time to Remediat

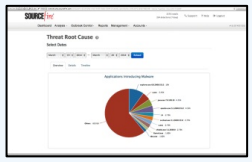
MP Provides Contextual Awareness and Visibility

at Allows You to Take Control of an Attack Before It Causes Damage

Who

Focus on these users first

What



These applications are affected

here

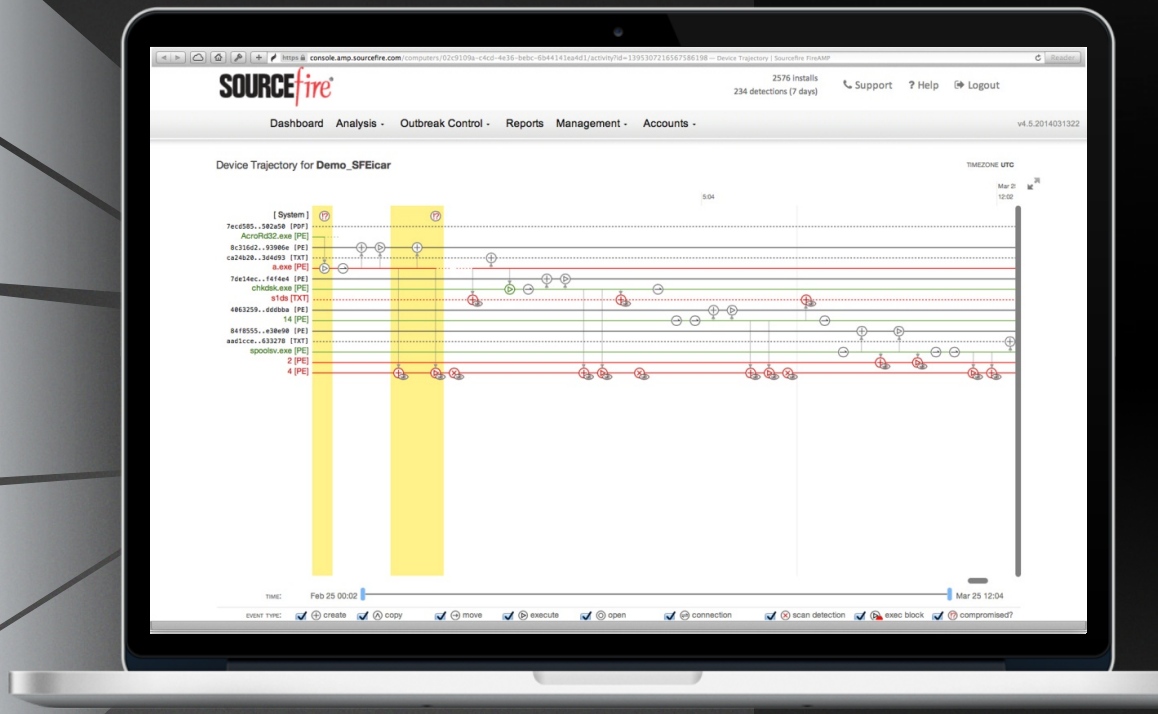
The breach affected these areas

hen

This is the scope of exposure over time

ow

Here is the origin and progression of the threat



lvanced Malware Protection Everywhere

Coming Q1CY16
Meraki MX

Dedicated FirePOWER
Appliance

Web & Email
Security Appliances

FirePOWER
Services on ISR

FirePOWER
Services on ASA

Best-in-Class
Detection

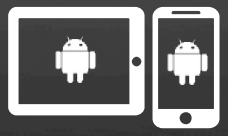
Leader in Security Effectiveness

Broadest
Deployment Options

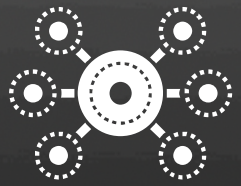
ac
S X

PC

AnyConnect



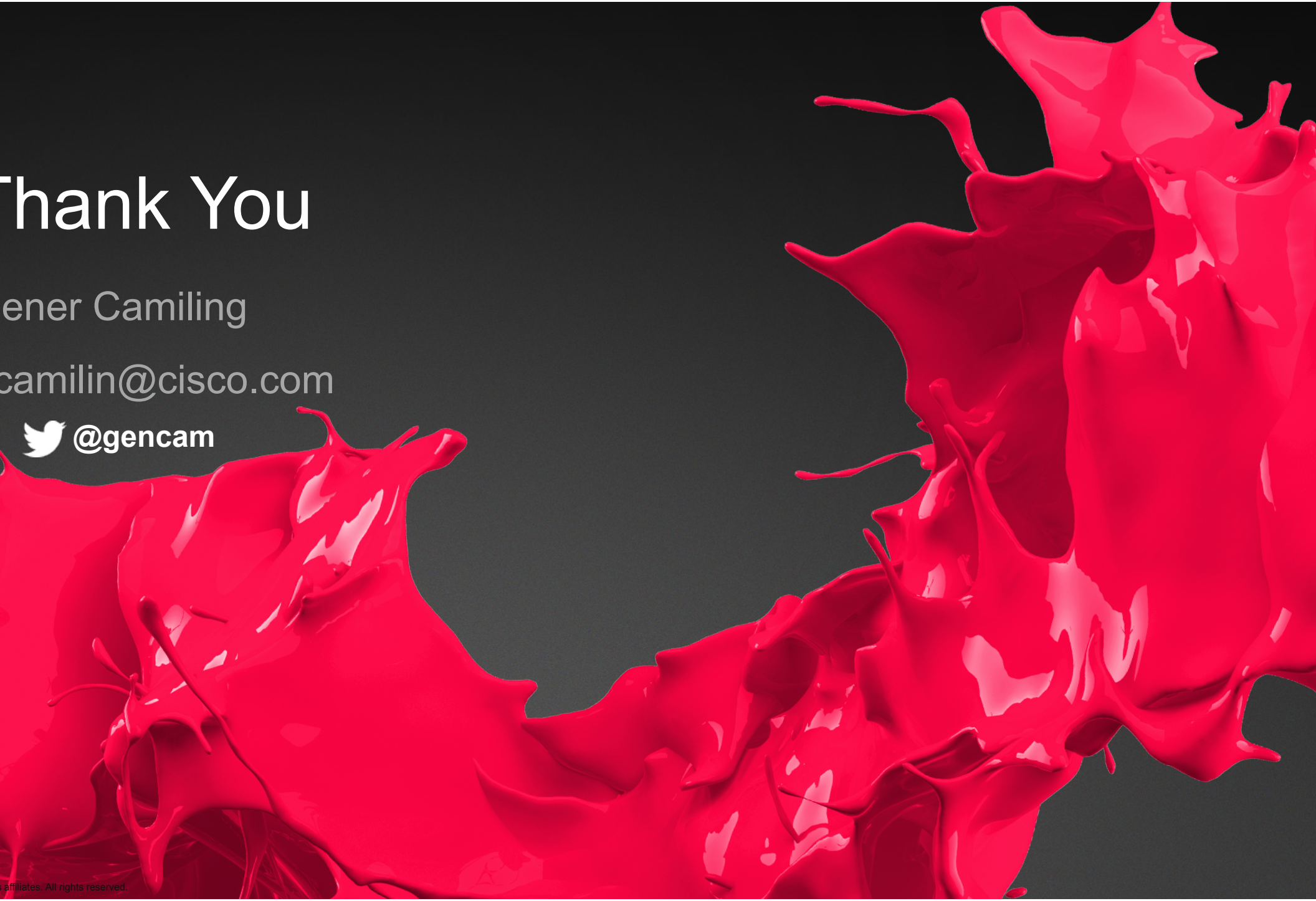
Mobile



Virtual

Cloud Based Web Security
& Hosted Email

Private C



affiliates. All rights reserved.