Agenda

- Introduction
- Threat landscape
- Security Strategy
- Threat intelligence
- Ensuring success

SCTE.
CABLE-TEC EXPO.
ATLANTA, GA > OCTOBER 11-14

Phishing

Web links in emails, SMS, or other places designed to encourage clicks that take people to malicious web sites where their valuable personal information can be harvested.

Malware

Malicious software developed to damage or disrupt devices or their data (by encrypting it with a secret key) or to gain unauthorized access to a network.
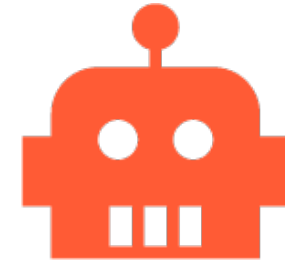
Malicious Bots*

Software that's secretly installed on computers and remotely controlled. Networks of malicious bots are used to find and upload valuable information, launch DoS attacks, provide access to machines and much more.

* There are legitimate bots too that perform many repetitive tasks on the internet

Typical Threat Distribution

Phishing
14.0%

Botnets
21.0%

Spam
13.0%

Malware
52.0%
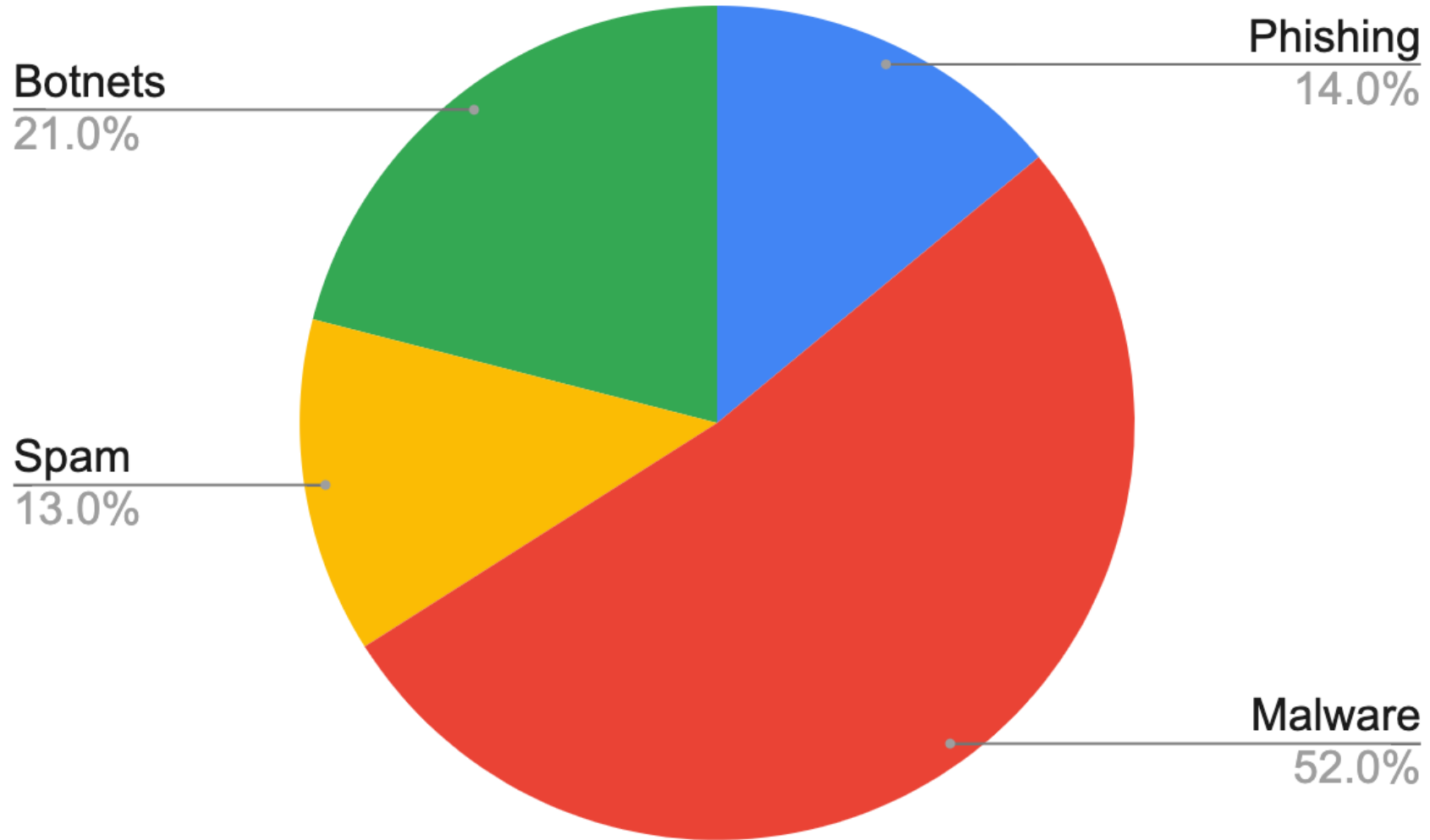
Create typos that evade a quick glance

wesrternsurnion.com/online   login.moffice356.com
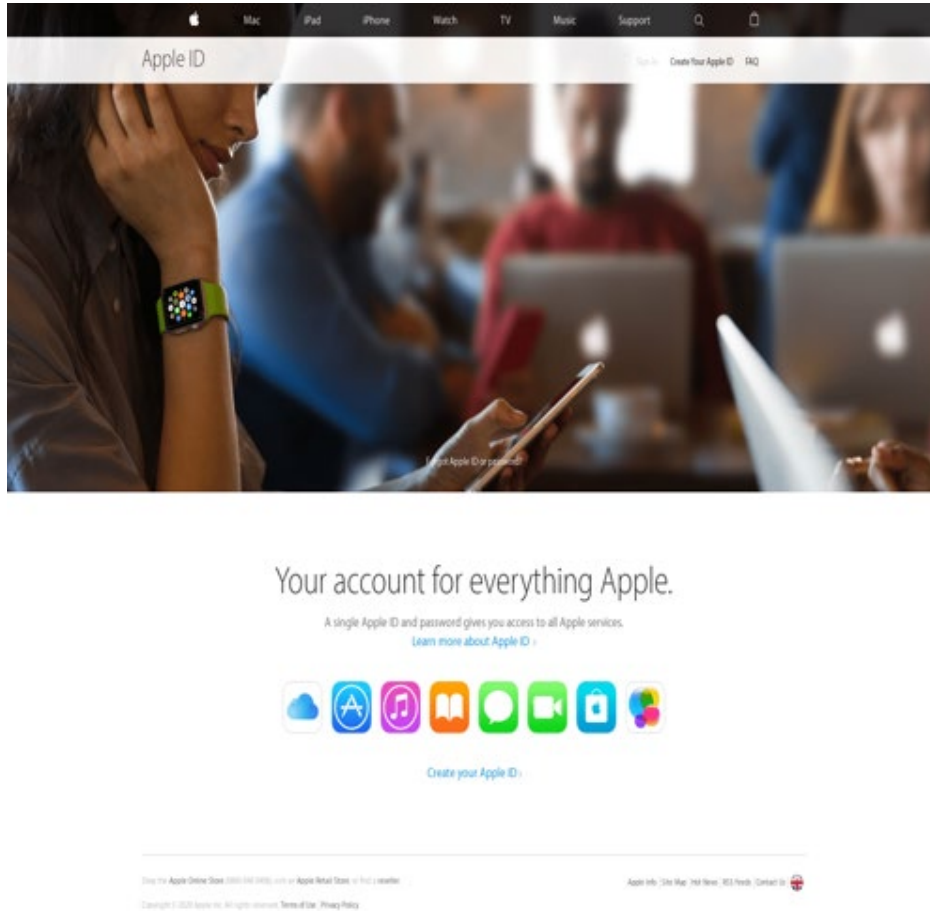
Cuse a different top level domain

verifyppal.xyz

Shift the familiar name to the left

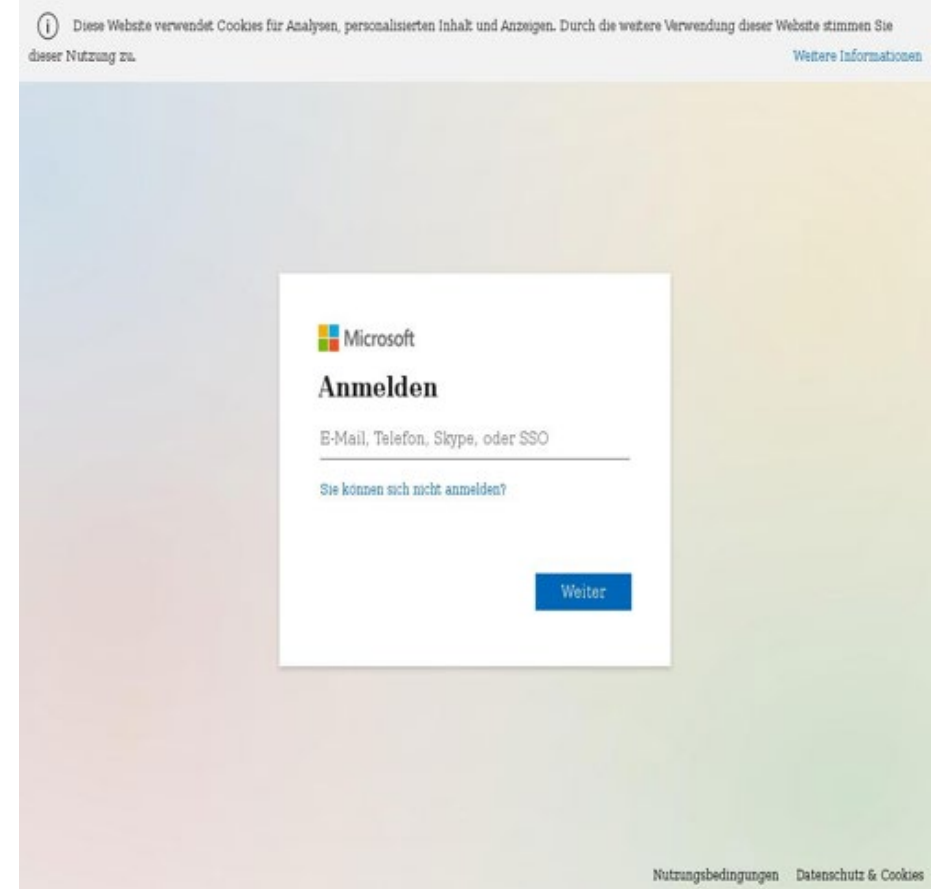signin.secure.welllsfargo.com.services.regaswel.shop

Use "lookalike" characters from non-latin character sets

7eleven.com., adidas.com., singaporeair.com.

Phishing Example Landing Pages

Microsoft

login.moffice356.com

Apple

apple.com.brlb.ru

Social engineering advances

"Covid-19 work from home policy"

"People are looking at your profile"

"Unusual sign-in activity"

28TH USENIX SECURITY SYMPOSIUM

Cognitive Triaging of Phishing Attacks

Amber van der Heijden, Luca Allodi

https://wwwusenixorg/system/files/sec19-van_der_heijdenpdf

MIT Technology Review

How phishing attacks trick our brains
Why you're more of a sucker than you think

Patrick Howell   August 8, 2019

https://wwwtechnologyreviewcom/2019/08/08/238739/how-phishing-attacks-trick-our-brains/

Samples

nytimes.cm
imagesgogle.com
ups.cm
wellsfargo.cm
wwwltrivago.com
winipedia.com

Landing pages serve malicious content based on the detected browser User-Agent and source IP address:

adware browser addons, MacOS fake system update and Windows fake AV purchase

Simple to procure and operate.

Complement other security services

Ensure transparency
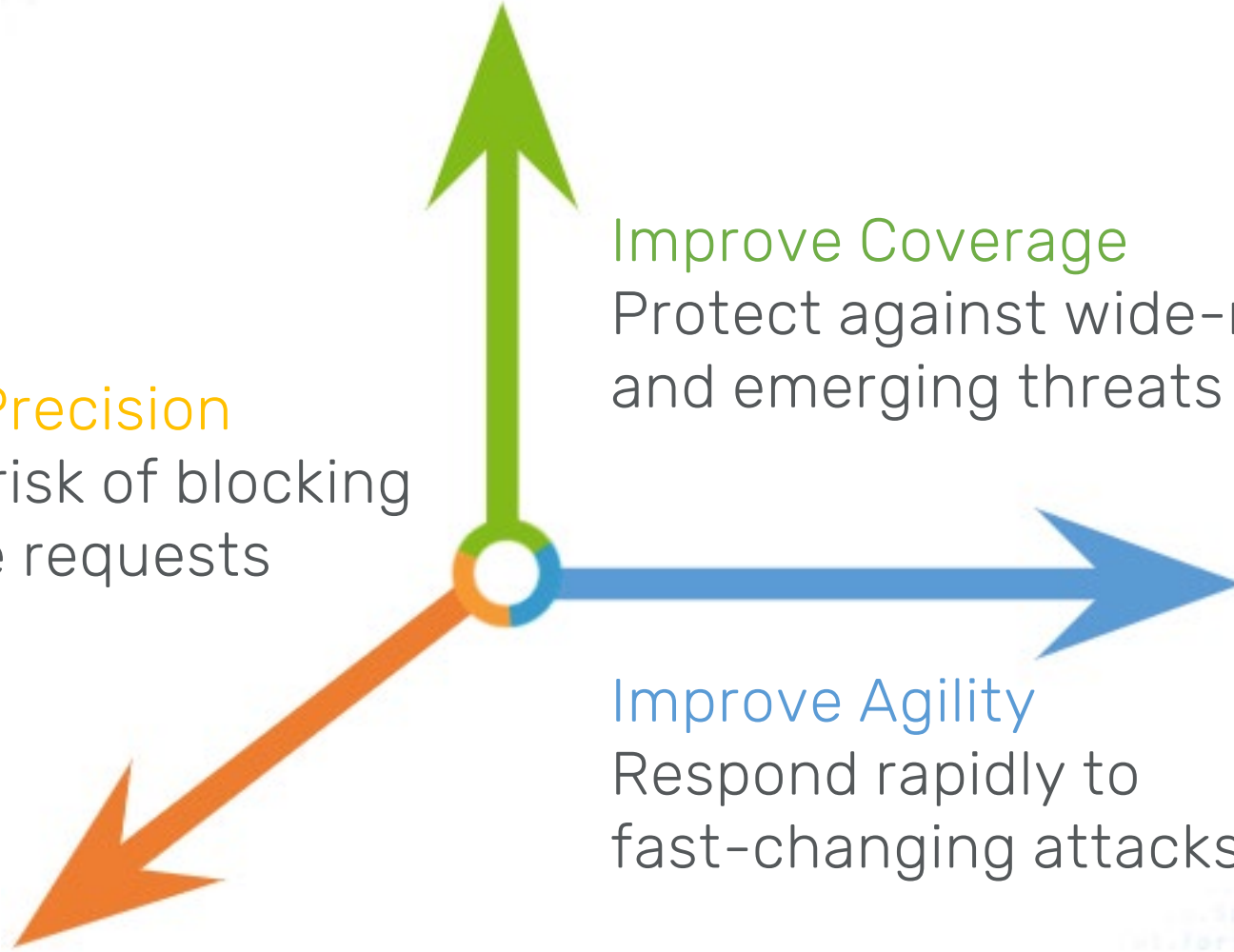
Give subscribers control

| expo.scte.org

10

Improve Coverage
Protect against wide-ranging and emerging threats
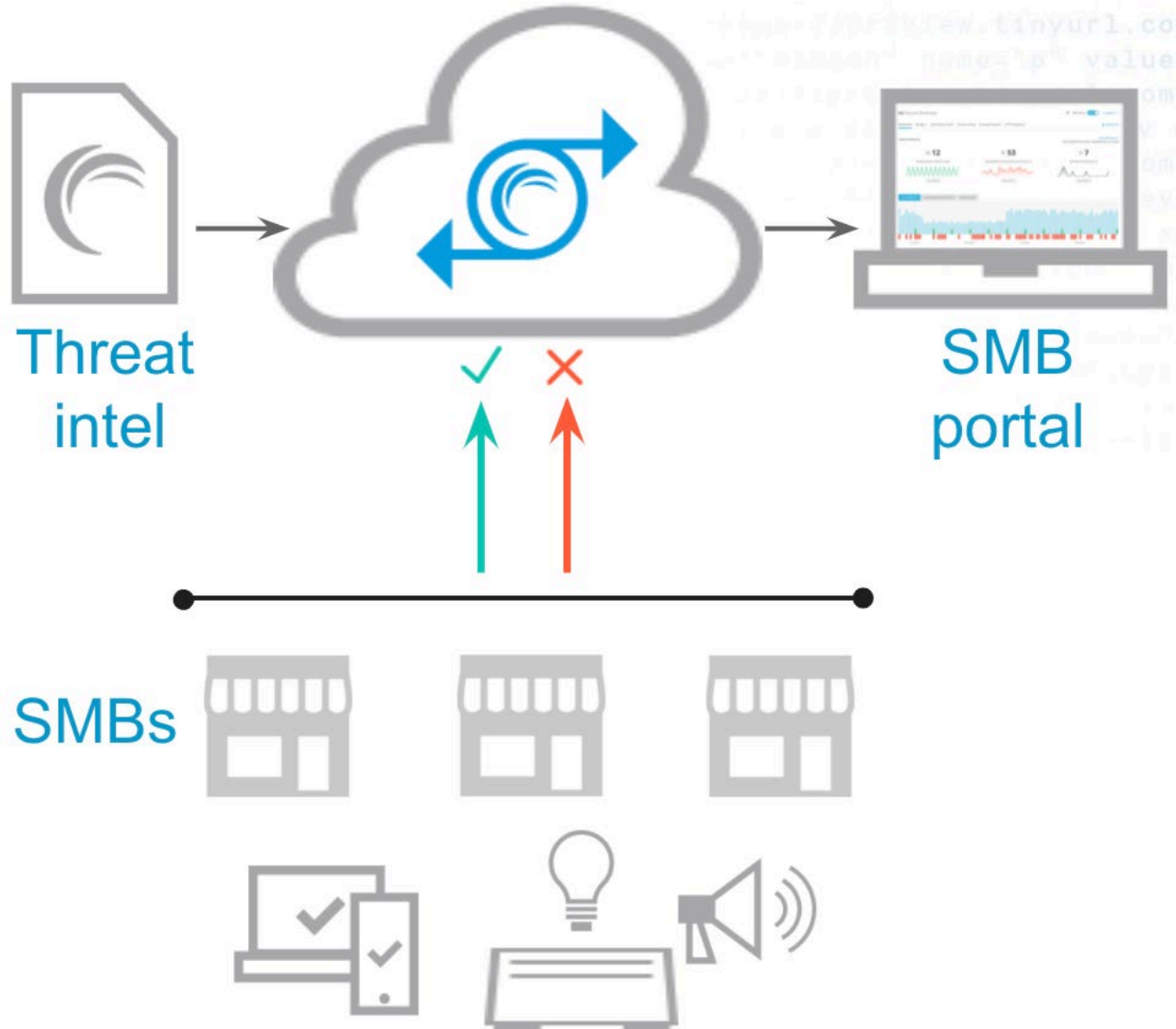
Improve Precision
Minimize risk of blocking legitimate requests

Improve Agility
Respond rapidly to fast-changing attacks

Intelligent Processing

Live streamed DNS & http data

Anomaly Detection
Monitor traffic patterns to detect DNS-DDoS, botnets, and other threats

Domain Ranking
Measure relative "importance" of both web and "infrastructure" domains

Correlation & Clustering
Use unsupervised machine learning to identify families of malicious domains

Domain Reputation
Calculate links between domains and ~90 network, client, and other "features"

Malicious activity detected & validated in seconds - minutes

Automated threat intelligence updates

Over 500,000 new malicious domains published each day

Ensuring Business Success

Sales Enablement	Customer Marketing
Sales tools summarizing key value points Solutions tools describing broader solution (access and other parts of bundles) Integration with internal sales systems Competitive overviews Security and solution videos Call scripts/talking points Internal Communications •Sales •Sales leadership •Customer support Sales Roadshows	Brand and Product Awareness Campaigns Website Broadcast media •TV •Print •Radio PR Social media Content syndication Customer Acquisition Direct Mail Email Digital media Webinars

Thank You!

Bruce Van Nice

Senior Product Marketing Manager
Akamai
hvannice@akamai.com