RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **PART2-T08**

Magecart Attacks Require Rethinking Your Credit Card Security

Raja Patel

Vice President of Products, Web Security
Akamai Technologies

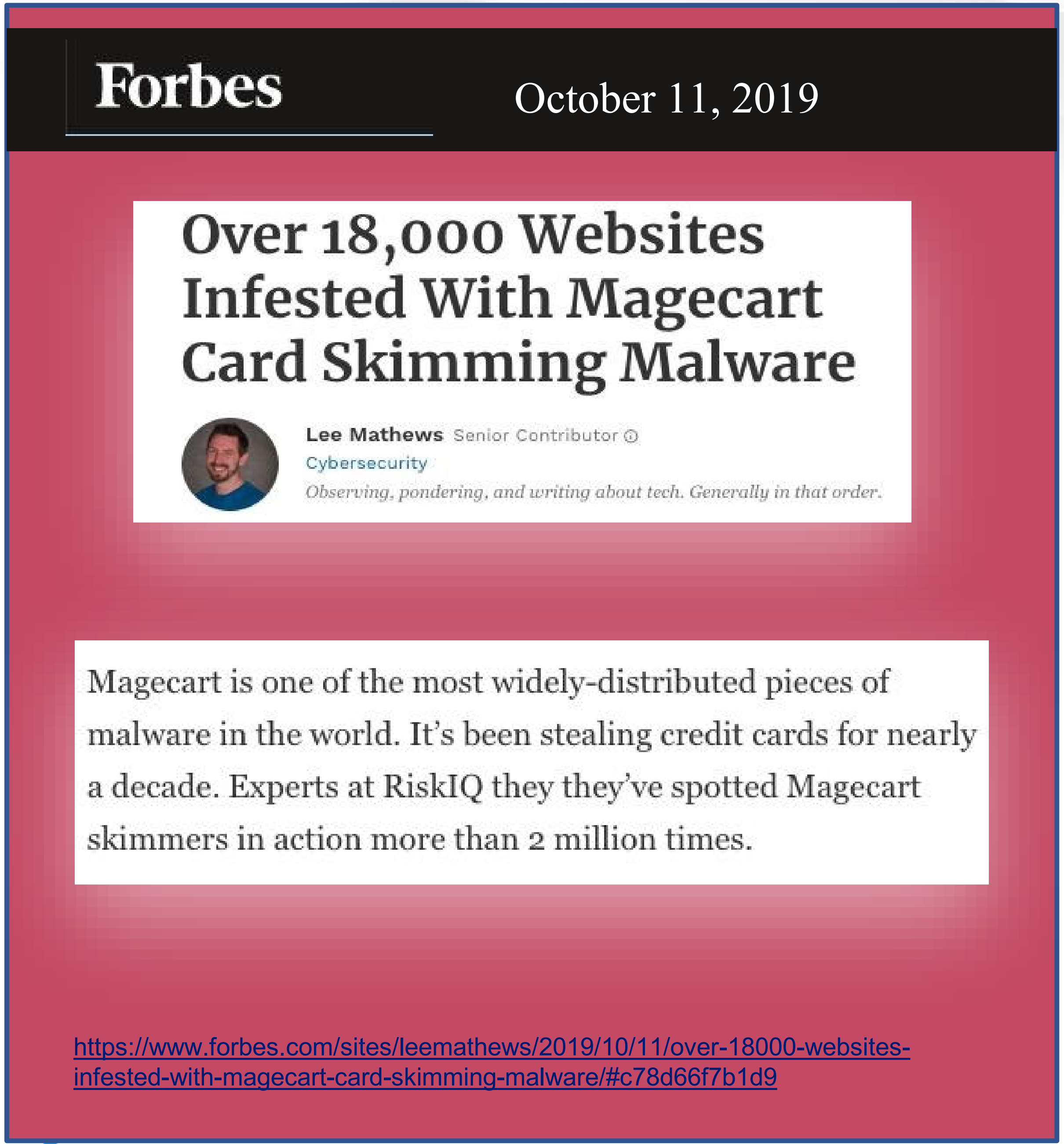
#RSAC

Magecart

- Hacker groups stealing sensitive data via third-party scripts
- Sites that use credit card processing are at constant risk
  - One infection can infect 1000s of sites in a single update
  - 20% are reinfected within a month of last attacks[1]

[1] Source: **SANGUINE SECURITY**, 2018

https://sansec.io/labs/2018/11/12/merchants-struggle-with-magecart-reinfections/



Forbes

October 11, 2019

Over 18,000 Websites Infested With Magecart Card Skimming Malware

Lee Mathews Senior Contributor
Cybersecurity
Observing, pondering, and writing about tech. Generally in that order.

Magecart is one of the most widely-distributed pieces of malware in the world. It's been stealing credit cards for nearly a decade. Experts at RiskIQ they they've spotted Magecart skimmers in action more than 2 million times.

https://www.forbes.com/sites/leemathews/2019/10/11/over-18000-websites-infested-with-magecart-card-skimming-malware/#c78d66f7b1d9

Credit Card Stealing Malware Strikes Websites of Two International Hotel Chains

Baseball Hall of Fame Website Hacked With Credit Card Stealing Malware

This is How 380,000 British Airways Passengers Got Hacked

FBI Warns of Hidden Online Shopping Threats, Including E-Skimming, 'Magecart Attacks'

https://www.newsweek.com/fbi-warns-hidden-online-shopping-threats-including-e-skimming-magecart-attacks-1467311

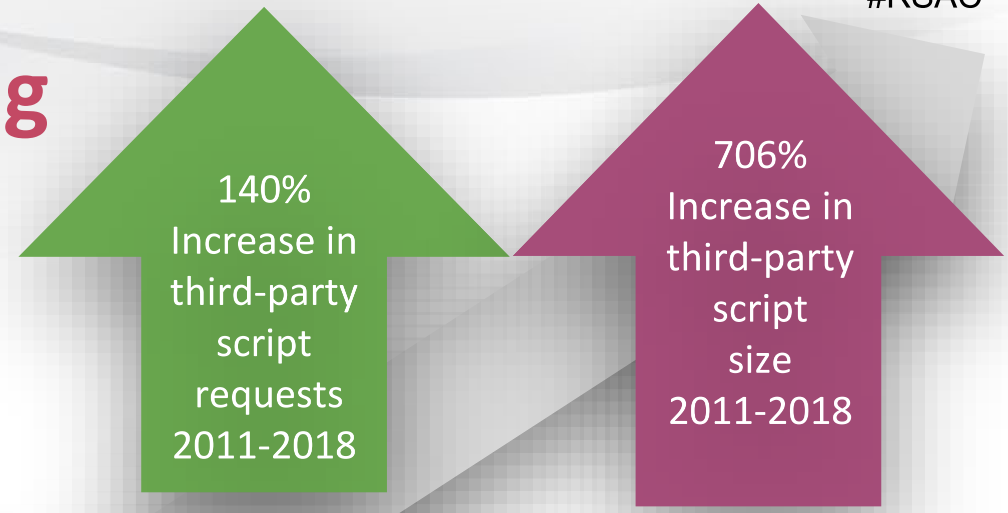
Agenda

- Why is Magecart a Big Deal?
- What is a Magecart Attack?
- Intrusion vs Detection
- A Comprehensive Security Strategy
- The Call to Action

Third-Party Script Use is Accelerating

Driven by Digital Transformation

- Enhances the Web Experience
- Easy to Add/Modify
- Promotes consistent experience
- Integrated with Third-Party Service
- Maintained by Third-Party

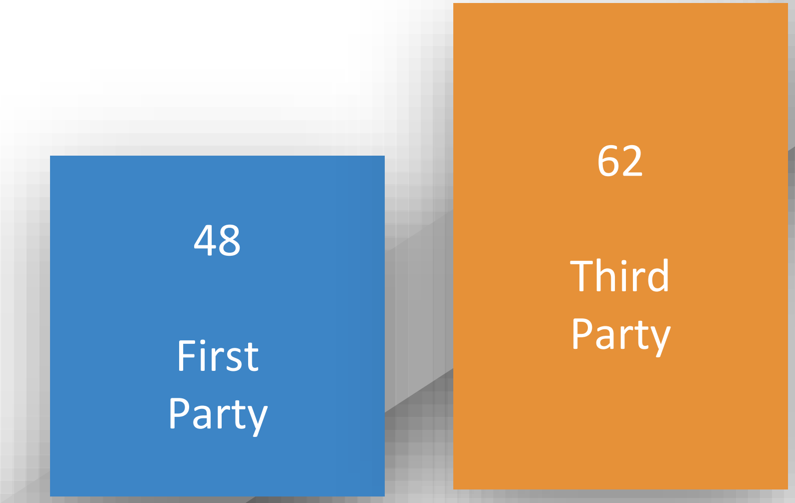


140% Increase in third-party script requests 2011-2018

706% Increase in third-party script size 2011-2018

Script Requests and Sizes, 2018

Source: JavaScript growth and third parties, SpeedCurve, 2018



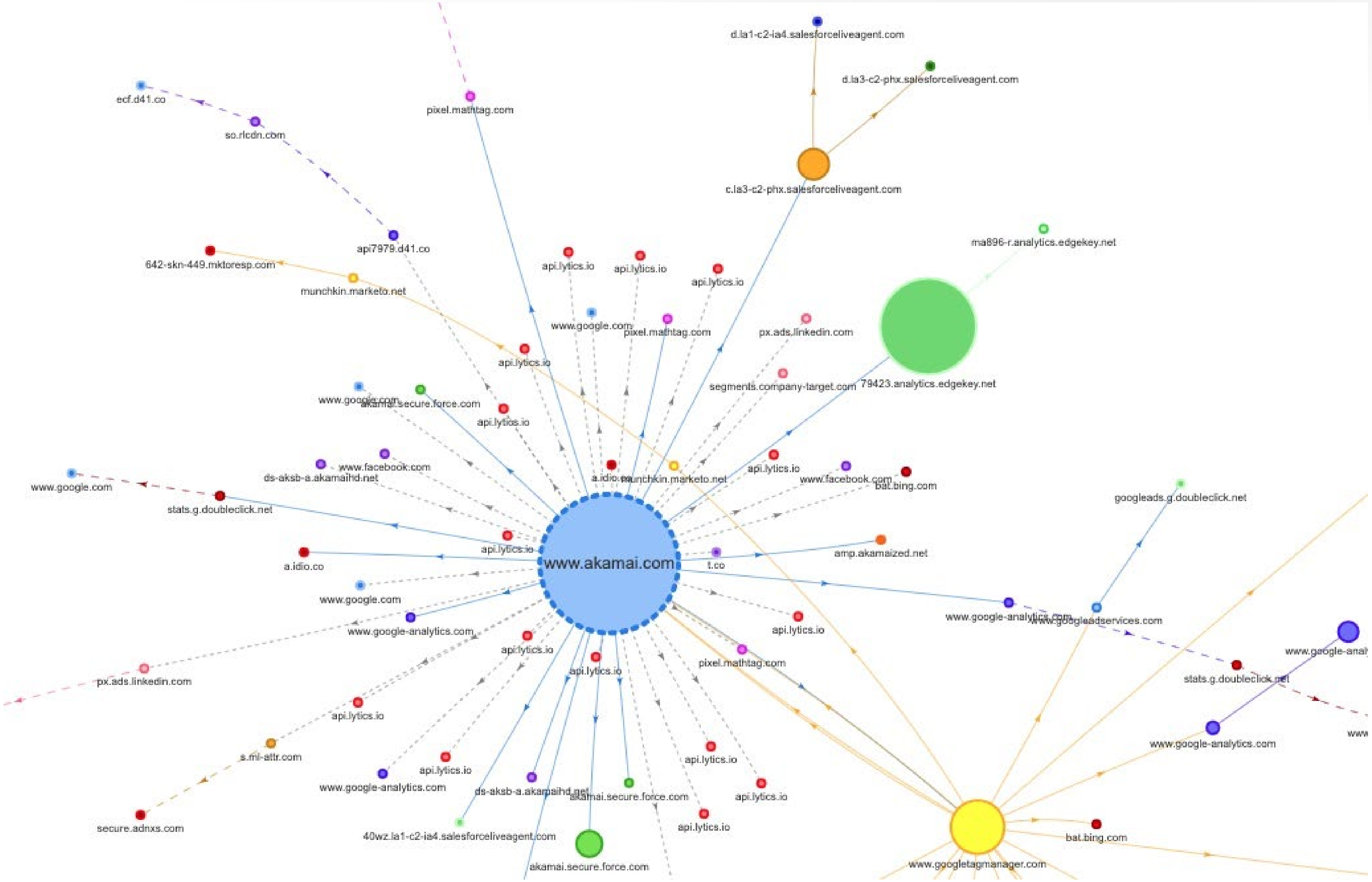
48 First Party

62 Third Party

Average Resources Per Page, 2017

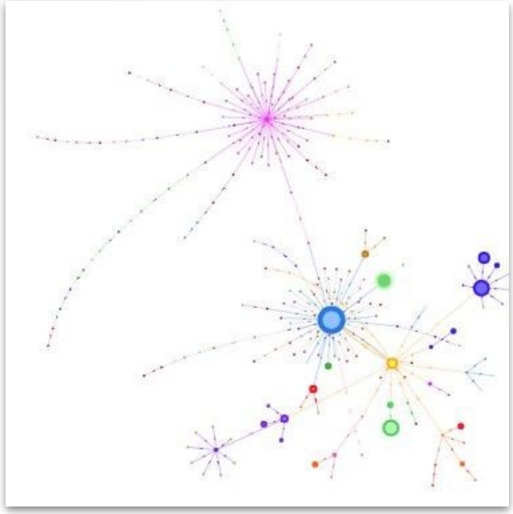
Source: Security and Frontend Performance, Challenge of Today: Rise of Third Parties, Akamai Technologies and O’Reilly Media, 2017

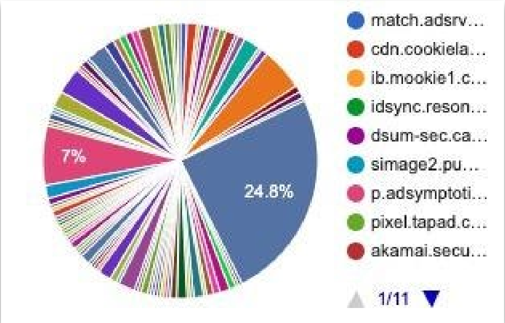
Analyzing Third-Party Application Activity



Source: https://requestmap.herokuapp.com/render/200107_S4_75af286693538a095b33ac5e4740b0b8/

Complete www.akamai.com

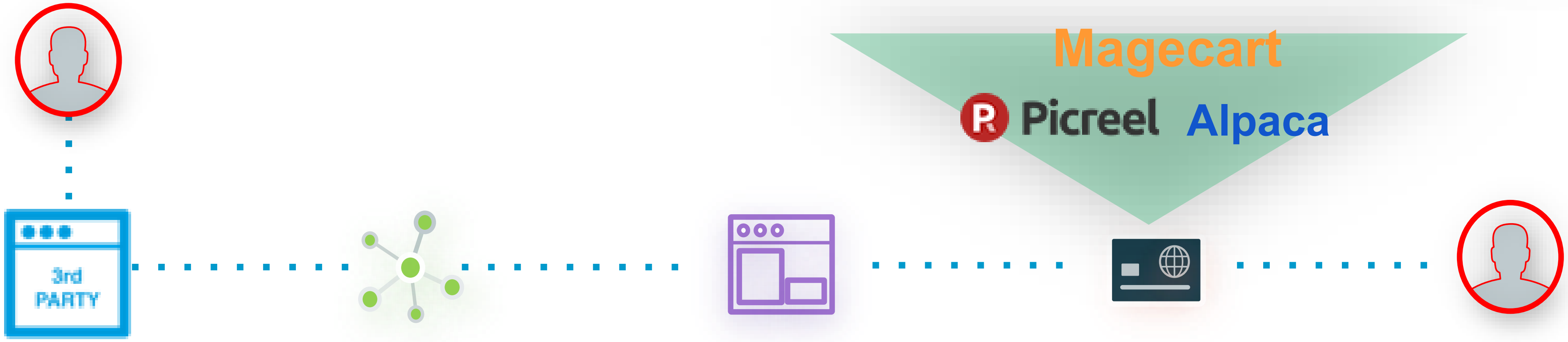




68% Third-Party Scripts

Third-Party Scripts Can Introduce Vulnerabilities

Complex supply chains that can be compromised by attackers



Malicious code added to 3rd Party updates

Delivered via supply chain

PII Skimmed

Malicious code executes

Sent back to hackers

4,800

Websites compromised monthly

↑ **78%**

- Outside of control and visibility
- Scripts added by other teams
- Come from trusted sources
- Re-infection is common

Source: Symantec 2019 Internet Security Threat ReportEvery month an average of 4,800 websites are compromised

Script Compromises and Examples

Data skimming

Major North American Retailer (4Q19)
Credit card info stolen from payment page

Accidental exfil

Major Online Search Service (4Q19)
Unsecure access to 250M customer records

Risky services

International Retailer (4Q19)
Unsecure access to 1.3TB of customer data

(CVEs) Known vulnerabilities

Travel Services (4Q19)
Exposed over 380,000 customer's personal and payment info

Third-Party Script Protection Approaches

Content Security Policy Whitelisting

- Supports rigorous CSP
- Prevention-focused
- Requires continuous manual analysis and testing

Synthetic Site Scanning

- Simple websites
- Useful for policy updates
- Requires continuous manual analysis and testing

Access Control/ Sandboxing

- Simple websites, low PII
- Combines with CSP
- Requires continuous manual analysis and testing

In-App Detection

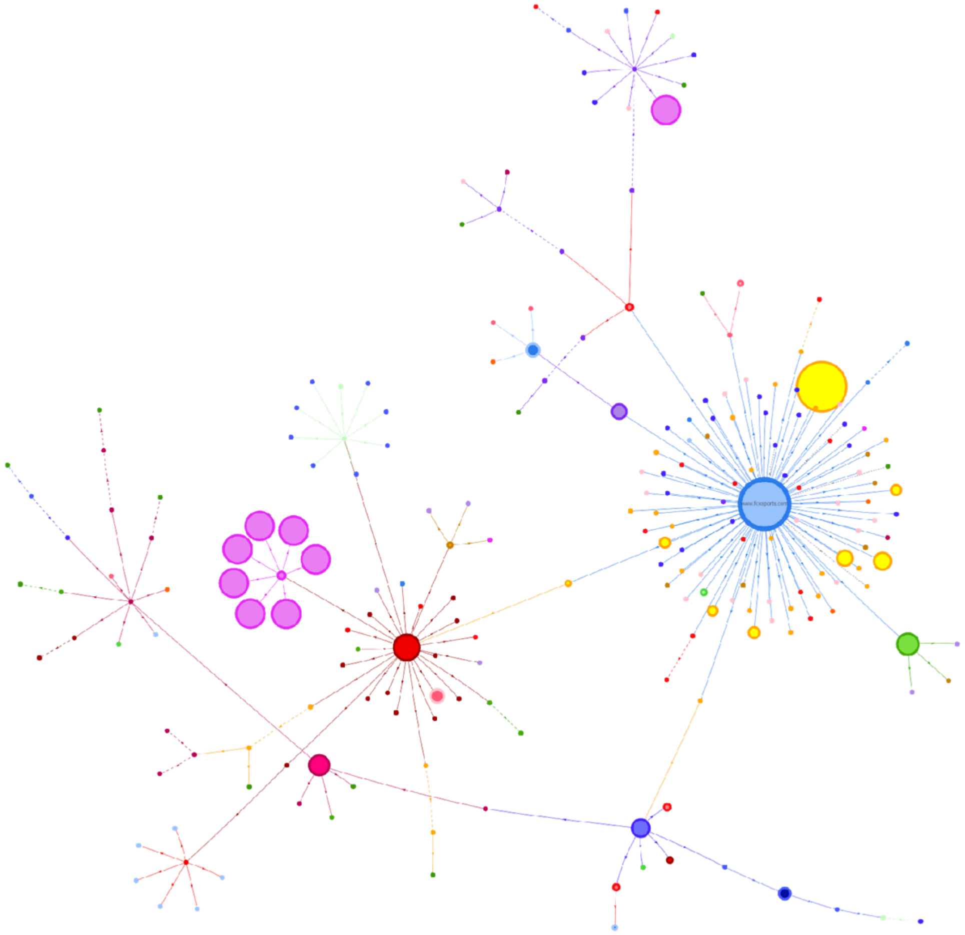
- Monitors app script behaviors
- Detection-focused
- Quick mitigation, low business impact

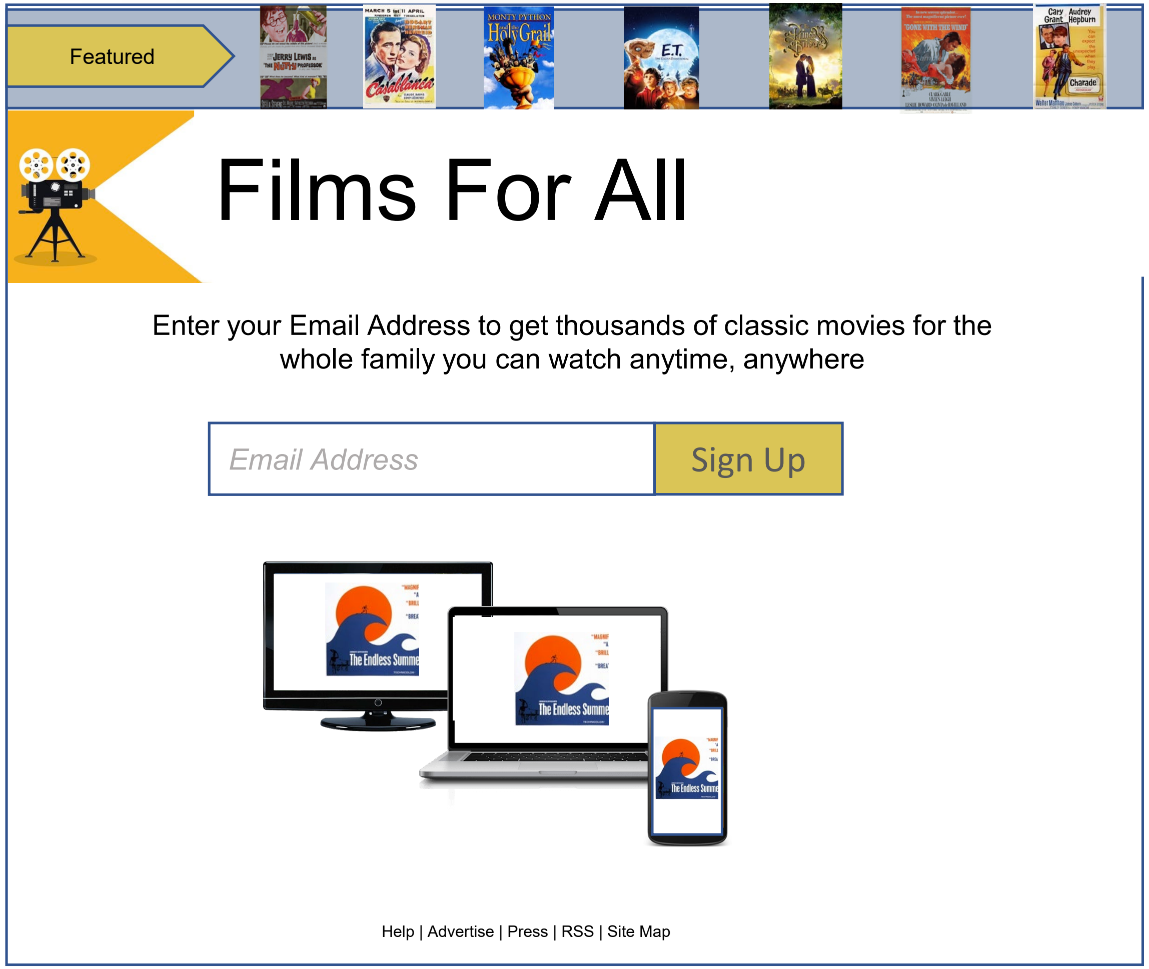
Attributes of an Effective Magecart Protection Service

- In-App detection of suspicious behavior
- Easy-to-setup and administer
- Automated, Always on
- Filters out noise & targets problems
- Threat intelligence to stop known threats
- Feedback loop to access control policies

Third-Party Script Website Example

Films For All*– Subscription Signup





Featured

Films For All

Enter your Email Address to get thousands of classic movies for the whole family you can watch anytime, anywhere

Email Address | Sign Up

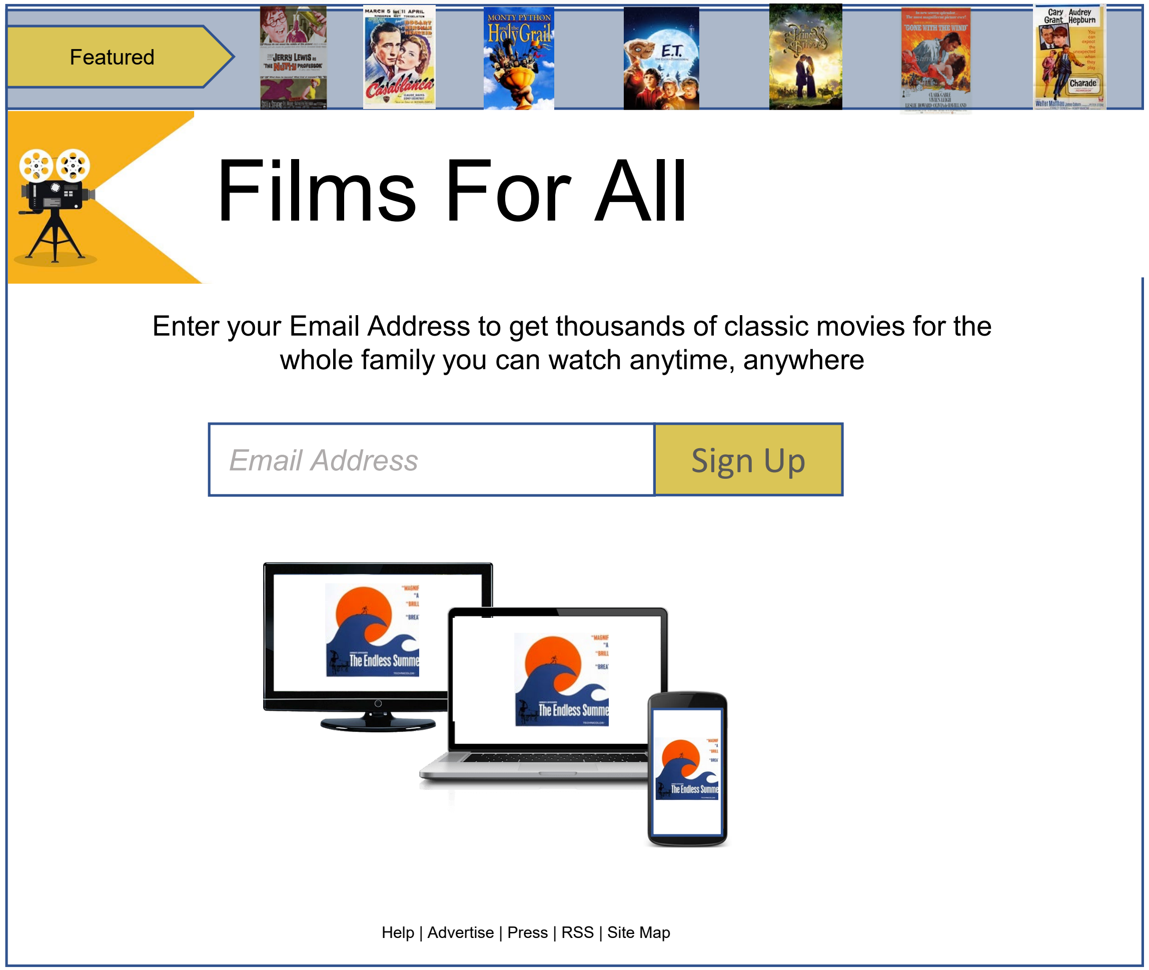
Help | Advertise | Press | RSS | Site Map

Films For All – Subscription Signup

Common site construction relies upon a constellation of service providers for analytics and site functionality.

- Might be dozens of hostnames
- An average of scripts 110 scripts
- Could be multiple tag managers
- A/B testing tool

This is an attack surface hackers could use to monitor or interact with Films For All users, or exfiltrate data they enter into the site.

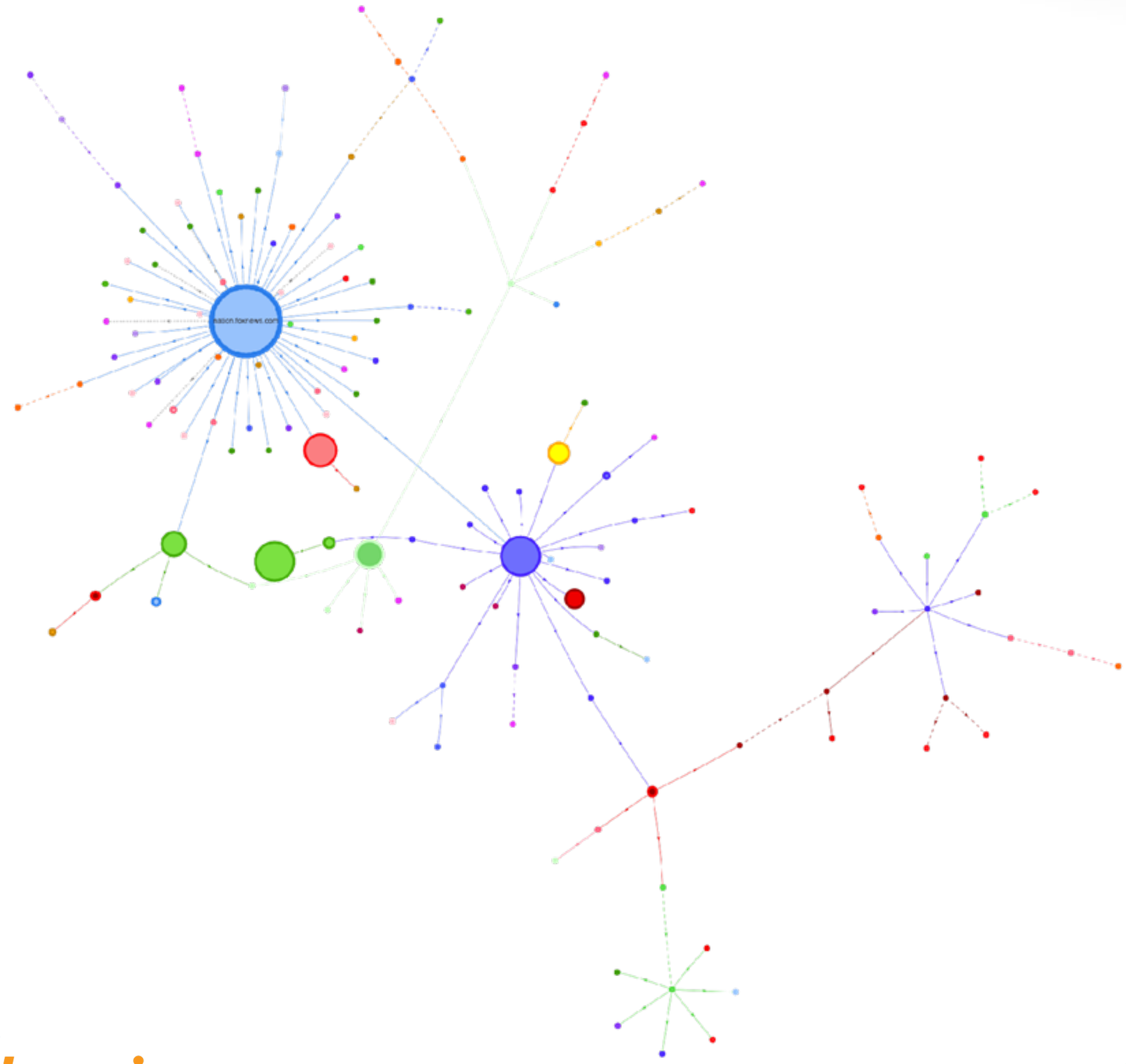


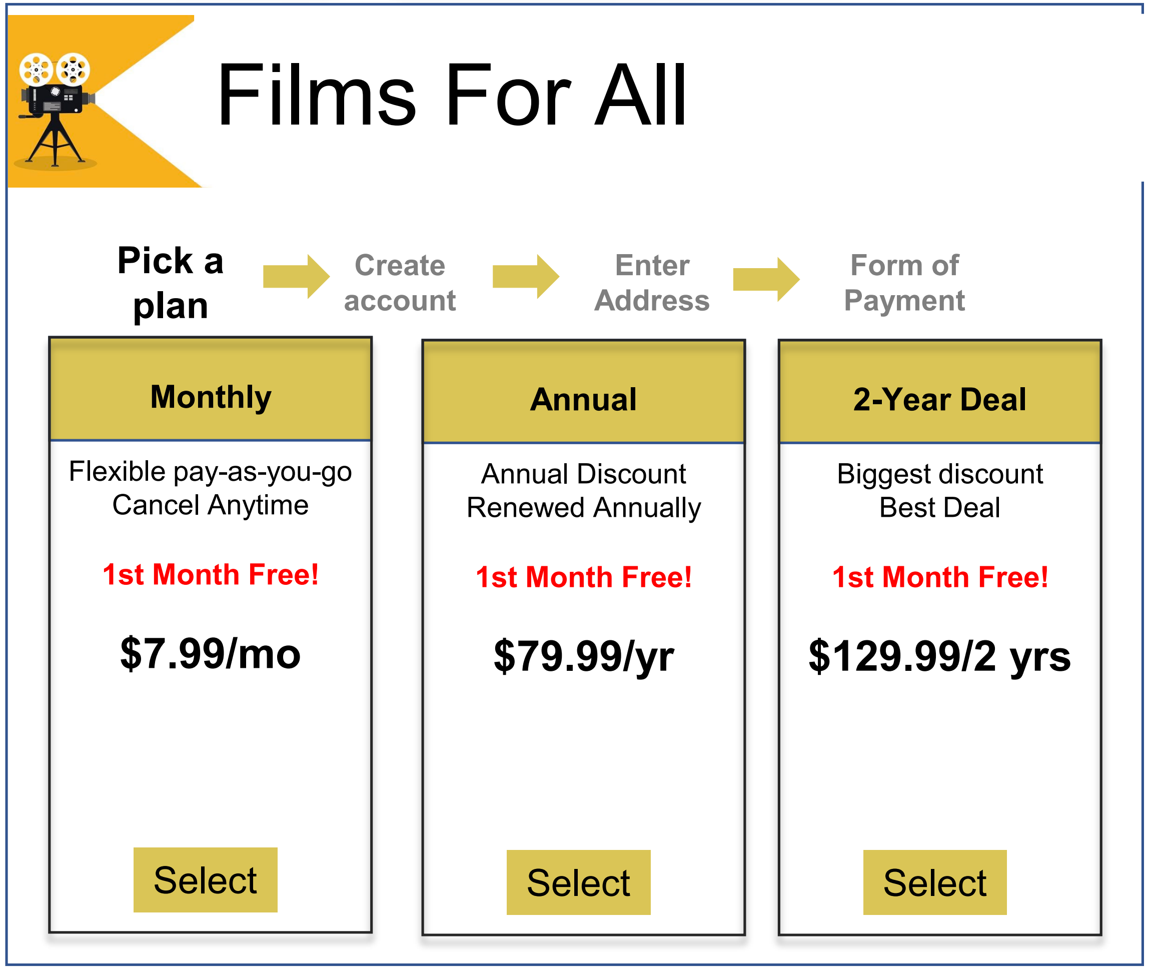
Films For All

Enter your Email Address to get thousands of classic movies for the whole family you can watch anytime, anywhere

Help | Advertise | Press | RSS | Site Map

Films For All – Account Creation





Films For All

Pick a plan → Create account → Enter Address → Form of Payment

Monthly

Flexible pay-as-you-go
Cancel Anytime

1st Month Free!

$7.99/mo

Select

Annual

Annual Discount
Renewed Annually

1st Month Free!

$79.99/yr

Select

2-Year Deal

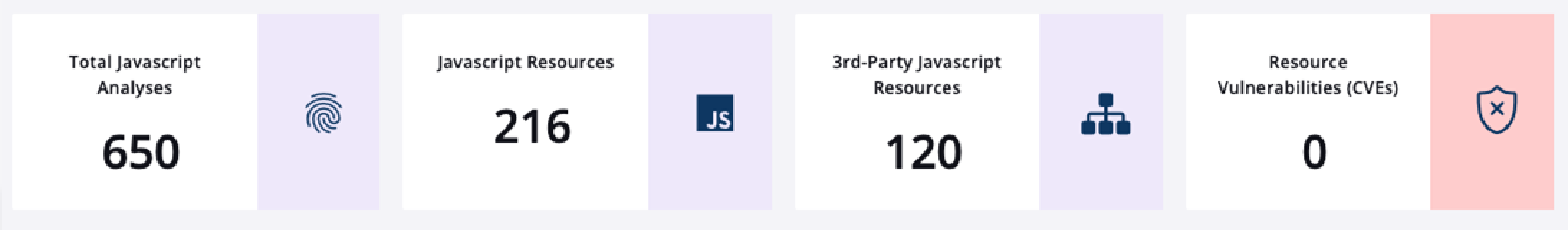
Biggest discount
Best Deal

1st Month Free!

$129.99/2 yrs

Select

Analyzing the Current Script Composition



Total Javascript Analyses

650

Javascript Resources

216

3rd-Party Javascript Resources

120

Resource Vulnerabilities (CVEs)

0

Sign-In and Sign-Up scripts

3rd-Party attack surfaces

Comparison to known threats

What to Remember

- Third-Party Scripts are essential to the modern websites
- Skimming threats are increasingly frequent & impactful
- Monitoring *Trusted* third-parties is the new requirement
- In-app script behavior detection is critical
- In-app script protection works with access control solutions

Next Steps

- Analyze your third-party script situation
- Think about which script security approach is right for you
- Test your ideas

Threats can come
from anywhere,
so we protect
you everywhere.
Akamai
Intelligent Security Starts at the Edge

RSA®Conference2020