RISKIQ®

THINK OUTSIDE THE FIREWALL™

2016 Malvertising Report

Malvertising was once again on the rise in 2016, increasing 132% over 2015 according to RiskIQ detection data. This sharp increase, the reporting of which has now become an annual tradition for threat researchers, comes as little surprise — the rise of programmatic advertising has introduced sophisticated profiling capabilities, which threat actors leverage with malvertising to target precise groups of users via an array of techniques. Because of its highly targeted nature, malvertising offers a big return on investment for its practitioners.

The stakes are high in the fight against malvertising

According to a report compiled by eMarketer, the worldwide paid media market, which accelerates every year, recently hit more than half a trillion dollars, with spending expected to reach $674 billion by 2020. However, malvertising curtails this growth. Because more and more users are now wary of the dangers presented by malvertising, they can use ad blockers, which eat away at digital advertising revenue. In 2016, 69.8 million Americans were expected to use an ad blocker, an increase 34.4% over last year. In 2017, that figure is projected to grow by another 24%, or 86.6 million people.

Malvertising as a digital threat is particularly effective as it's difficult to detect and take down malicious ads because they are delivered through ad networks such as Google and Facebook and not resident on web pages. Threat actors use malvertising to propagate malware, ransomware, and scams (disingenuous advertising), as well as redirect victims to phishing pages and pages hosting exploit kits.

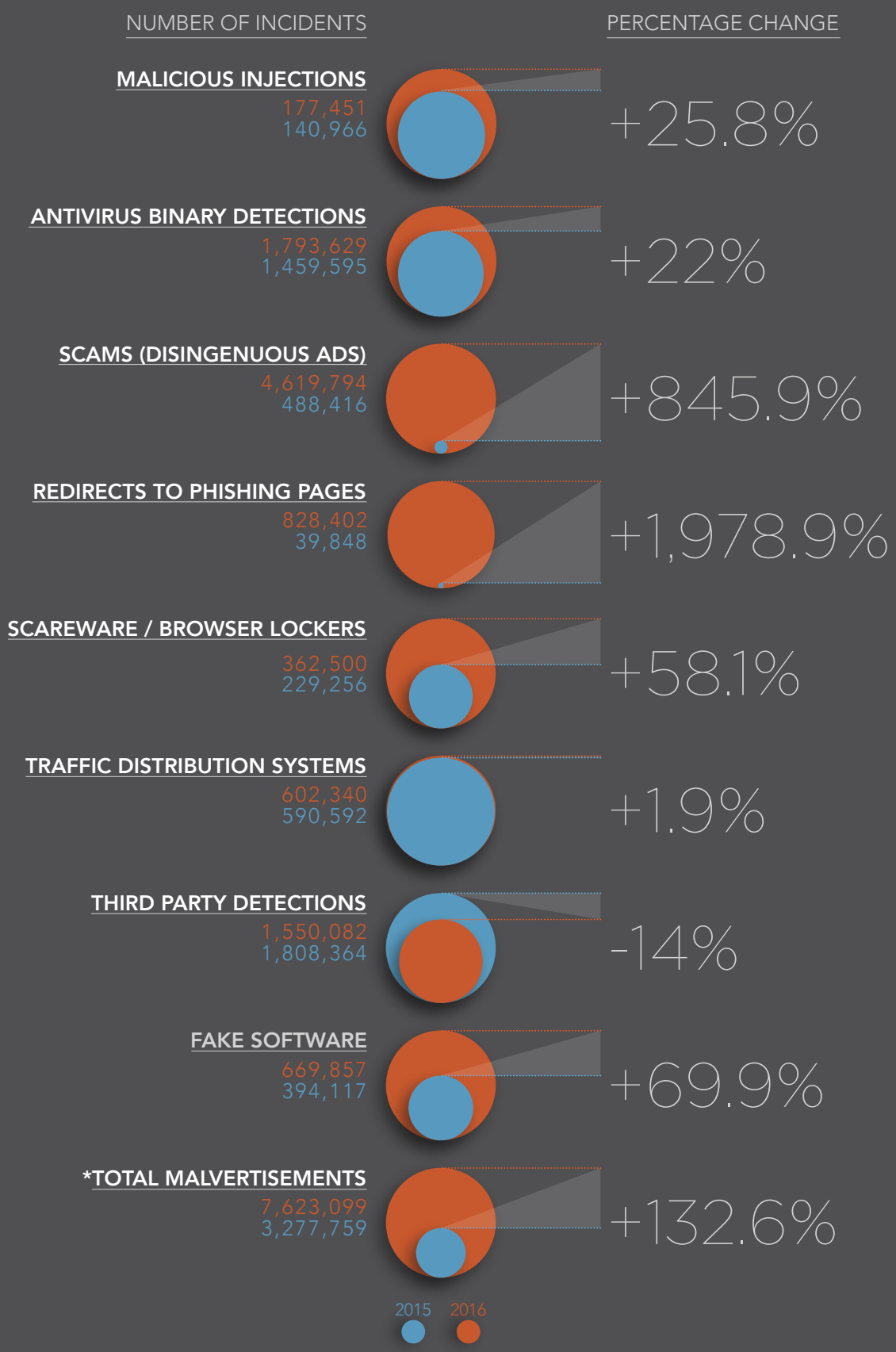
RiskIQ, which mitigates this risk for digital advertisers and publishers through our curated blacklist of malicious ads, intelligently scans from over 2 billion pages and nearly 20 million mobile apps per day. This proprietary blacklist lets ad ops, brand managers, and security staff vet new demand sources and prevent malware within their ad infrastructure. Our advanced crawling infrastructure, which allows us to capture the entire ad, ad redirect chain, and creative sources, indicates which part of the ad-serving process was compromised and helps us identify the entity responsible.

Visit https://www.riskiq.com/blog/uncategorized/malvertising-on-the-rise-again/ to learn more about how RiskIQ is working with brand, security, and AdTech professionals to mitigate digital threats and improve business.

Methodology

For each incident of malvertising detected by RiskIQ, our threat research team pulled RiskIQ blacklist incidents associated with our clients to make sure that every incident they found linked to an ad sequence and could be categorized. For the total number of malvertising incidents, they pulled landing page submissions (a single ad markup submission) that resulted in any number of blacklist incidents. This way, no matter how many individual incidents an ad associated with, it was counted as one instance of malvertising.

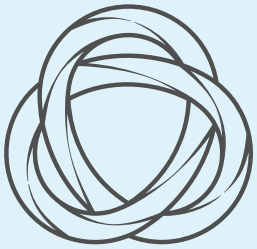
HERE'S WHAT WE DETECTED IN 2016, AND HOW IT COMPARES TO WHAT WE FOUND IN 2015:



*Some of the total malvertising incidents fall under multiple categories

About RiskIQ

RiskIQ is the leader in digital threat management, providing the most comprehensive discovery, intelligence, and mitigation of threats associated with an organization's digital presence. With more than 80 percent of attacks originating outside the firewall, RiskIQ allows enterprises to gain unified insight and control over web, social, and mobile exposures. Trusted by thousands of security analysts, RiskIQ's platform combines advanced internet data reconnaissance and analytics to expedite investigations, understand attack surfaces, assess risk, and take action to protect business, brand, and customers. Based in San Francisco, the company is backed by Summit Partners, Battery Ventures, Georgian Partners, and MassMutual Ventures. Visit RiskIQ.com or follow us on Twitter.



RISKIQ®

THINK OUTSIDE THE FIREWALL™

