www.riskiq.com

Report

Threat Landscape 2017: RiskIQ's #Infosec Predictions

Table of Contents

With cyber attacks ranging from Yahoo! to the Democratic National Committee and the rise of ransomware to the Shadow Brokers, 2016 was an exciting year for the cybersecurity community. However, we expect 2017 to provide a very different digital threat landscape than years past. The explosive growth of the internet of things (IoT), combined with new digital business models in which organizations use digital channels more than ever before to conduct transactions with customers and employees, will attract threat actors to target these new threat vectors in the upcoming year. As a security professional, here are some of the trends you need to watch out for.

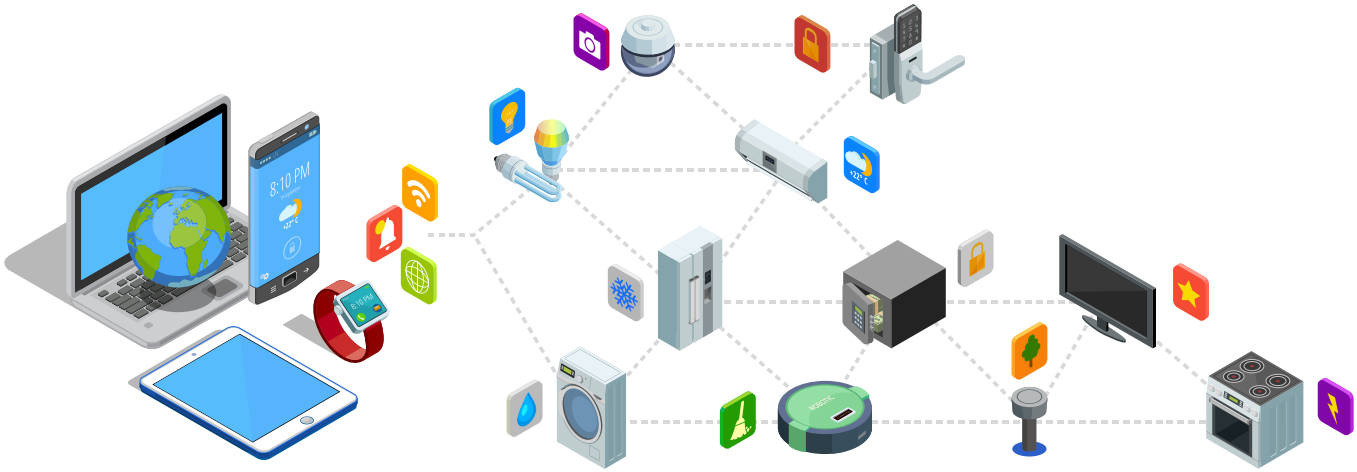
1 Phishing attacks will rapidly expand across new digital channels like social media

Our stats show it, and so does everyone else's: as zero-days and trivial host exploits get harder to pull off, threat actors are reverting to forms of attack that are unsophisticated and primitive—but have proven to be highly effective. That's why phishing is rising in popularity and traditional email and web phishing, spear phishing, and whaling (Business Email Compromise or BEC) all usually share many of the same simple root causes: domain infringement and content, branding, and keyword impersonation.

Phishers are also starting to conquer new ground. We are now seeing a hard pivot by phishers into leveraging social media, and in 2017, this trend will grow exponentially—especially with social networks adding online marketplaces (Facebook) and payment gateways. At RiskIQ, we've been seeing threat actors leverage fake mobile apps for quite some time, but in 2015, we saw a rise in phishers moving to social media in the U.S., primarily targeting banks and major brands with a significant social media sentiment following. In early 2016, we detected some of the first phishing attacks via social media targeting in other countries, such as Japan.

2 IoT will increase as a new attack vector—but not how you think

People have sounded the IoT alarm for years now, but threat actors have primarily exploited IoT in DDoS attacks, like the one we saw targeting Dyn late in 2016. This attack crippled internet traffic across over half the continental U.S. and many other parts of the world. Many will predict that IoT will be leveraged in more sophisticated attacks such as ransomware and data leaks in 2017, but for the most part, we'll continue to see the same kind of attacks we saw in 2016.



Why? While IoT is likely to continue to standardize operating systems around Android and Linux variants, which will eventually make it easier to write broad-scale attack and exploit code, for now, IoT operating systems and embedded systems are incredibly fragmented. Current IoT devices use a large combination of proprietary software and OSS (open-source) mixes, so it's hard to write a single worm or attack that influences every IoT device as broadly as previous Internet worms, which targeted ubiquitous and universally standard Windows operating systems.

3 Threat actors will discover and target organization's blinds spots

As perimeter security gets stronger and stronger, malicious actors will look for softer entry points to an organization. As a result, hackers are becoming increasingly sophisticated at collecting external data about their targets, and are using it to discover and exploit assets online that security teams are unaware of, or lack the resources to protect.

Expect adversaries such as nation-states, hacktivists, and cyber criminals to ramp up targeting these unmonitored, and often undefended, externally (internet) exposed assets such as Cloud applications, partner and vendor applications, and third-party hosting providers. This new tactic will lead to an increasing number of data breaches via digital channels, where many digital assets are unknown and unmanaged by the organizations that are responsible for them.

4 The cat and mouse attacker-defender game will evolve, and #ThreatHunters and #DFIR investigators will need more (and better) data

Threat actors are getting more sophisticated at hiding their tracks by anonymizing their infrastructure and getting better at detecting and hiding from security scanners and crawlers that detect attacks via websites and ads. Hunt teams will need to deploy increasingly modern sophisticated technology to detect them in the form of new combined internet security datasets that link together related hosts, third-party web components, and WHOIS information. This enhanced data will fingerprint and track these new threat actor tactics.

5 Your biggest vulnerability may actually come from your partners or vendors

As mentioned, adversaries are increasingly probing organizations' partners and vendors looking for vulnerability by association. Large organizations with mature security operations teams often have strong detection capabilities and defenses, so even if an adversary manages to break in the front door, they won't stay in for long.

It's much easier for adversaries to target and compromise a smaller, weakly defended partner or vendor with whom you may be sharing your information or a private network connection to your internal systems. They will use this third party to ransack the data you share with the victim or use the victim as a backdoor into your internal systems. Examples of ripe targets including marketing data collection vendors, who not only have access to an individual customers' data but can also yield access to data for thousands of organizations.

We are also observing situations in which adversaries are focusing on partners that are acquisition targets so they can quickly compromise them when the acquisition intention is announced. This way, they can lay in wait until the acquired company's networks are plugged into the acquiring parent, creating a new backdoor in the corporate networks and data.

6 Web application complexity will increase faster than web security tools can keep up

Web applications increasingly rely on external and third-party, dynamically loaded components to power the website, ranging from marketing trackers to performance management monitors to data-display widgets. These third-party widgets, often externally loaded JavaScript, are extremely difficult for web application and source code scanners to scan and test accurately—and can be beyond the ability of a web application firewall to defend.

Employing third-party JavaScript components presents security challenges because the code runs in each user's web browser when they visit a website. Each executed third-party component represents an organization's forfeiture of security control to the third party, and many security teams we talk to are unaware how many third party components the business has deployed.

As a result, the exploitation of these oft-undefended third-party components is proving to be an environment of particular interest to adversaries, as recent compromises to tracking, analytics, and identity widgets would attest.

6a Undetected JavaScript keyloggers will steal credit card info

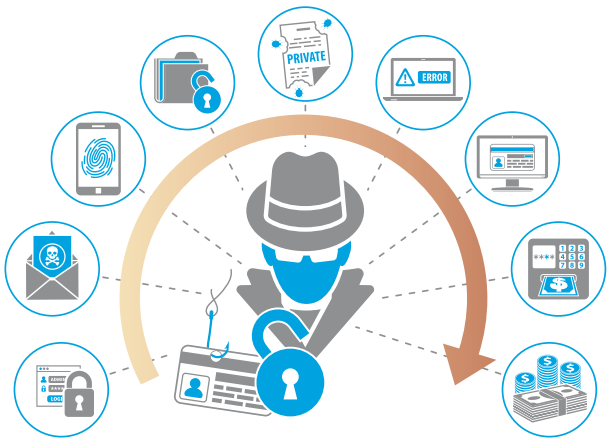
As a recent new example of increased web app complexity, i.e. number six in action, RiskIQ has detected global adversaries using new, hard-to-detect JavaScript keyloggers to steal credit card info in websites they have hacked.

Modern vulnerability scanners are unable to detect embedded attacks in progress, and threat actors know this. To avoid detection, these threat actors will launch attacks that rewrite the document object model (DOM) of a web page to mask the vulnerability. They'll then inject keyloggers, which are spyware that can record every keystroke made to log a file. That means when you're punching your credit card info into a compromised eCommerce site; it falls right into the hacker's hands.

RiskIQ's Threat Research Team recently discovered new shopping cart exploitation using these very methods

7 Modern threat actors move fast. Seconds will count more than ever

We are increasingly hearing of attack campaigns from instances of domain infringement used for phishing and malware campaigns that go live the day the account is created and only last for a few hours. The speed at which these attacks appear and vanish make them unsolvable by human analysts. That means companies need automation that can quickly and accurately detect these attacks, and push them into global blocking solutions in minutes—if not seconds—to get ahead of them.



A new year, a fresh approach to InfoSec

You can materially improve your security posture by implementing a complete digital risk management framework across your digital channels. Start with comprehensive visibility across your web, social and mobile assets and adopt an integrated platform for external threat management—one that provides the tools that help you discover your entire attack surface, and alerts your security team as threats materialize in the wild and provides proper workflow and relevant data for quick incident response.

About RiskIQ

RiskIQ is a cybersecurity company that helps organizations discover, understand and mitigate known, unknown, and malicious exposures across web, mobile, and social digital channels. The company's External Threat Management platform combines a worldwide proxy and sensor network with synthetic clients that emulate users to detect, monitor, and take actions against threats outside the Firewall. RiskIQ is used by thousands of security analysts including many from the Fortune 500 and leading financial and consumer institutions to defend their business and protect customer's and partner's trust. The company is headquartered in San Francisco, California, and backed by Summit Partners, Battery Ventures, Georgian Partners and MassMutual Ventures. Information security professionals can sign up for a fully functioning trial version of PassiveTotal for free by visiting www.riskiq.com/whats-new-passivetotal.

RISKIQ®

San Francisco

22 Battery Street, 10th Floor
San Francisco, CA 94111
USA

info@riskiq.com
1.888.415.4447

Kansas City

7730 Hedge Lane Terrace
Shawnee, KS 66227
USA

info@riskiq.com
1.888.415.4447

London

33 Cannon Street
4th Floor
City of London
EC4M 5SB
UK

info@riskiq.com
+44 (0)203 282 7149

To learn more about RiskIQ, please visit: **www.riskiq.com**