GIGAOM

VENDOR PROFILE

Zimperium

Key Criteria for Evaluating Phishing Prevention & Detection Platforms

SIMON GIBSON

TOPICS: PHISHING SECURITY AND RISK

GIGAOM

Zimperium

Key Criteria for Evaluating Phishing Prevention & Detection Platforms

TABLE OF CONTENTS

1. Summary

We covered Zimperium in our December 2018 Landscape Report, and they continue to stand out in their approach and philosophy. Zimperium was early to realize that growth in mobile provided attackers opportunities to exploit it not only because of sheer numbers but because of complexity that arises out of mobile. In the majority of companies, BYOD is encouraged, and even where corporate devices are issued and MDM is deployed, users can conduct personal communications using mobile. These are not limited to email.

As is the case across the cybersecurity spectrum, attackers target the weakest link. With phishing, attackers target users, and with the explosion of mobile, attackers increasingly are turning to attacks that leverage mobile devices. They include messaging apps like Signal, WhatsApp, and SMS. Attackers understand this and, phishing has extended beyond protecting corporate email inboxes.

Mobile devices contain a tremendous wealth of information about their owners and how their owners interact with the connected world. As mobile devices became more pivotal for conducting business, their interactions with connected devices such as desktops and trusted access control mechanisms increases. A mobile device can be infected with malware designed to be delivered and exploited in trusted environments or other systems such as connected cars.

The approach that Zimperium undertook is designed to protect the mobile endpoint from being the point of entry, and their focus on that is what sets them apart. Zimperium deploys to mobile endpoints as an App in Google Play or App Store or with an MDM or their SDK.

Their product is designed to understand the behavior of three main components. The device, the apps installed, the networks it connects to, and the behavior they observe. These all culminate around the Zimperium phishing prevention app. They have a large install footprint of 70mm devices and, in some cases, can retrieve anonymized attack signature data. This information, in combination with their threat research team, trains their engine so it can detect unusual behavior indicative of a compromise.

The approach is driven by threat intelligence behavioral heuristic analysis. This approach is intended to ensure that users' information is kept private. They do not analyze, nor are they able to view content included in web pages, emails, attachments, or secure messages. Instead, they can observe what resource is being requested and by what and analyze DNS requests and SSL certificates. All of the mobile devices' network behavior is observed, and they can determine if the device is actually compromised.

2. About the Vendor Profile

HOW TO READ THIS REPORT

The Vendor profile is part of a series of documents aimed at giving the reader the tools to better understand technology, evaluate it, and explore the market to find the best solutions for his organization.

In this context, and to get a complete view of the state of the solutions available in the market, the reader should consider the following documents:

Key Criteria to Evaluate Phishing Prevention & Detection Platforms is an introduction to the technology, defines the necessary evaluation metrics, the key criteria to evaluate new solutions, and the impact of the latter on the former. It is dedicated to those end-users that are approaching a new technology for the first time, or want an update on the latest evolution.

Vendor Profiles for Key Criteria are easy-to-read deep dive documents that cover a single vendor regarding the solutions described in the other reports. They provide more details on the solution, how the vendor approached the key criteria, and the impact that its solution has on the evaluation metrics. This document helps end-users to get a quick but complete evaluation of single vendors.

3. Key Criteria Analysis

Analytics: At Zimperium's core, their Z9 engine analytics capabilities are fundamental to how Zimperium approaches the detection and prevention of attacks. They look at how the device and the applications on it behave. This includes things like clicks, what the applications on the device attempt to do, static analysis of application binary code to detect malware, and what networks the device tries to connect to. Their model is trained in the cloud to detect phishing kits and other TTPs that would be indicative of an attack.

This cloud-based training produces heuristics that are then sent to their mobile application, which, after receiving updates, is autonomous.

Approaching the problem this way enables Zimperium to observe the behavior and create a profile of the device and apply their model to identify compromised devices despite the sandboxed nature of mobile applications.

Deployment: Zimperium could easily be categorized as an EPP, and they deploy off of AppStore or GooglePlay or be MDM deployed. They also offer an SDK and pricing model for organizations that want to embed z9 engines in their mobile applications. This is a big plus for enterprises like banks that have large numbers of mobile applications and other security companies that white-label Zimperium.

In the phishing prevention ecosystem, their approach enables them to deploy on BYOD or managed systems. It gives them an edge with regard to broad coverage that includes not only enterprise email, but all email on the device as well as messaging while maintaining user privacy.

Reporting: With every phishing protection vendor, we looked at their ability to report as an opportunity to make their customers' lives easier. With Zimperium running on the endpoint, they report when they detect a compromised endpoint. They can gather information for forensic analysis that includes application package bundle information, signing certificate information, what networks were available, DNS information as well as process information.

Another key feature is Zimperium's integration with big enterprise tools like McAfee EPO, VMWare Workspace One Intelligence and Microsoft Defender ATP.

Broadness of the Solution: Zimperium is not a traditional phishing protection platform, and because of their focus, there are many things they do not do; however, that is perfectly fine. Because of their concept, they're able to cover more ground than traditional phishing prevention platforms on mobile devices. Their ability to deploy in a sandboxed environment and by using heuristics about network traffic, they cover all the vectors that might cause a mobile device to become infected and used as a launch-point for larger attacks.

4. Evaluation Metrics Analysis

Architecture: Zimperium architecture is built around detecting compromised devices by observing behavior using their training, classifiers, and analysis. They deploy to devices via AppStore and Play as well as MDMs or their SDK. Their application takes updates from the Zimperium cloud, which is used to create their detection heuristics. These classifiers are sent to their device, and they are the only product that runs completely on the device.

Their application can run in several modes. They offer users the ability to send links before they click, or it can run on the network stack and run automatically. In either case, when traffic is encrypted between the application and the service, Zimperium is unable to read the contents. To some of the vendors, we looked at this would be a handicap, but to Zimperium, they took the challenge of having to look holistically across the device, the applications, the networks, and the user behavior and developed heuristics that detect compromise and protect privacy.

Feature Sets: Zimperium can run on endpoint autonomously and collect forensic information after an attack, report it to security teams directly or via VMWare Workspace One, McAfee EPO, or Microsoft ATP. They can support multiple MDMs in a single tenant. They capture attacks in multiple stages and report the vector used in the compromise. This gives enterprises a big advantage in protecting other devices. They detect device compromises, adware, trojaned applications, and record what networks were used.

Interoperability: The zIPS solution is available in the AppStore and Google Play. It runs on Android and IOS. Their SDK allows it to be embedded in other apps, and using the app callback context enables any application to call the z9 engine and quarry activity for like clicks and get a response from their engine.

Deployment Options: Zimperium deploys via Google Play or AppStore and can be managed via an MDM. It deploys to the device and runs either as a tunnel on devices local network stack that sends all outbound traffic through the Z9 engine or deploys on the device, and users can send it links from email or messaging and the Z9 engine will reputational with a reputational score.

The city of New York uses Zimperium as part of the NYC secure program because of the effectiveness and Zimperium's commitment to maintaining users' privacy.

Pricing Models: Their pricing is straightforward and is per user and comes with all the reporting and hooks for SOAR and into enterprise management consoles. They offer an SDK and have flexible pricing for enterprises that want to deploy within their mobile apps or white-lable their engine. They are also the only MTD provider that currently is "FedRamp authorized to operate" (ATO) (utilizing AWS Govcloud).

Crowdsourcing / Internet Reputation: Much of the work Zimperium does is around using their footprint of 70mm installs to crowdsource indicators of phishing kits and anonymized endpoint

telemetry. They put much of their R&D into understanding what sort of behaviors and changes indicate not only phishing attacks but compromised devices, network attacks and malicious apps. One of their key tenants is the ability to train their engine on what a compromise looks like.

5. Bottom Line

BOYD is challenging for a lot of reasons, not the least of which is convenience. Unfortunately, convenience and security are almost always at odds. Yet, with an install base of around 2.8 billion smartphones and our ever-increasing reliance on them, there is no doubt they are the next beachhead.

Mobile devices not only store our private information, but they also connect to enterprises, and we rely on them for almost every aspect of business workflow. From sales to systems administration, from treasury functions to traveling, we trust them to authenticate us. They are trusted to connect with our enterprise systems by way of Bluetooth and IP and used to transfer files.

Attackers understand this, and while mobile operating systems are more closed than traditional open systems, it does not follow that they are more secure. Simple security economics says that the cost of the attack should be greater than the value of the target. For now, the cost of attacking mobile devices is quite high but not out of reach if the target is worth it.

If we have learned anything about security over the last ten years, it is that when we couple reliance and complacency and they reach critical mass, meaning we cannot get along without the thing. We trust the thing will always be used the way it was intended; we are instore for surprises.

You can try Zimperium out.

Zimperium's focus in this space is well-founded, and their approach, which protects privacy and provides a broad spectrum of coverage, should be in every SOCs toolbox and on their radar.

6. About Simon Gibson

Simon Gibson is a CISO and subject matter expert on security. He has been responsible for driving security capability into products, enterprises and supporting complex engagements.

Simon led the Information Security Group at Bloomberg and served as their CISO. He has managed attack teams, incident response teams and been responsible for the defensive security posture in the financial, government, manufacturing and PCI industries.

Simon is a renowned speaker and panel moderator. He has counseled fortune 100's on building their programs and worked with US Government public private information sharing initiative

7. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

8. Copyright