ivanti

The Role of Machine Learning in Complete Mobile Phishing Protection

How Ivanti Mobile Threat Defense provides on-device, zero-day detection of mobile phishing attacks

Table of Contents

Introduction

Phishing has been a threat for at least a quarter of a century, but the rise of mobile has made phishing even more effective and complicated to combat.

With mobile usage now surpassing desktop usage, particularly among enterprise users, cybercriminals see mobile as a prime target for phishing attacks. And mobile devices make phishing attacks even more likely to succeed, bringing completely new threat vectors and unique technical issues that must be addressed.

When it comes to detecting mobile phishing attacks, Ivanti Mobile Threat Defense (MTD) knows protection must occur where the attack is actually happening: on-device. And that protection must utilize machine learning in order to combat even zero-day threats.

Phishing attacks are on the rise

The number of phishing attacks is rapidly increasing. Verizon's 2021 Verizon Data Breach Investigations Report (DBIR) found that phishing was the top tactic used in data breaches for the third straight year. This trend shows no signs of stopping as DBIR data reveals the percentage of breaches where phishing was present rose 25% from 2019 to 2020 (11% to 36%). The increase has many causes, including a low barrier to entry for attackers.

Cybercriminals can set up phishing attacks in minutes and make the attacks incredibly difficult to detect at scale. While no cyberattack offers guaranteed success, many cybercriminals have found that phishing is as close to a sure thing as they can get.

Mobile phishing requires a new approach

Enterprise IT and security teams use a variety of anti-phishing countermeasures to protect traditional endpoints, most of which are focused on corporate email (e.g. email and web gateways, next-gen firewalls). Even with all of these protections in place, there's still plenty of room for improvement.[II]

And mobile makes things ever more challenging from a security perspective. Mobile devices make phishing attacks even more likely to succeed, bringing completely new threat vectors and unique technical/user issues that must be addressed.

Phishing attack contenders:

Credential phishing uses mass spam email campaigns.

Spear phishing is more targeted and includes exploits that use attachments like payment notices, invoices or W-2 tax forms.

Smishing uses SMS text messages.

Whale phishing targets an organization's C-level.

Vishing is voice or phone spoofing.

Automated phishing attacks use man-in-the-middle (MITM) exploits to defeat two-factor authentication.

Top 10 reasons mobile makes phishing attacks easier

01 Users are in charge.

Users typically administer their own devices, lacking the automated patching and processes that corporate desktops and laptops have.

02 Small screens.

Small screen size makes it more difficult to access and view key information.

03 OSs and apps = great hiding places.

OSs and apps limit the availability of information needed to properly assess the authenticity of emails, web pages, etc.

04 Users trust too much.

Users feel a personal connection to their mobile devices, fostering unfounded trust in the device and the content on it.

05 No side-by-side view.

Viewing web pages and other data side by side is difficult or impossible.

06 Look before you tap.

User interface limits the amount of available information while prompting users to make fast decisions.

07 Gotta toggle.

Moving between web pages or between apps requires cumbersome toggling.

08 Texts = urgent.

Users view SMS as more urgent and so can be less inclined to verify requests sent via SMS.

09 Don't ask, just tell.

GUI design encourages actions such as accept, reply, send, like, etc., facilitating user responses to requests.

10 Texting while distracted

Users use mobile devices while walking, talking, driving, etc., and can receive and respond to requests while distracted, without having to view the originating app, making it more likely they will accept the request.

Mobile has unique technical/user issues

Mobile devices are considered personal, regardless of whether the organization or the user owns them. Even though mobile anti-phishing solutions protect the enterprise, their success will be strongly connected to user perception across a myriad of technical factors, including:

- Battery consumption.
  If users perceive the solution is draining their battery, they may uninstall protection.
- Memory resources.
  If users perceive the solution is consuming memory (e.g. with a large database of known bad URLs), they may uninstall protection.
- Data usage/cost.
  If users perceive the solution is using too much of their data plan (e.g. with cloud-based lookups for every suspicious URL), they may uninstall protection.
- User privacy.
  If users perceive the solution is sending personal information (including where they are browsing) off of the device (e.g. with cloud-based lookups), they may uninstall protection.

New mobile phishing vectors bypass existing solutions

Corporate email is the primary attack vector for phishing on traditional endpoints. Since two-thirds of emails are read on mobile devices and most corporate mobile users do not use always-on VPNs for all traffic, this vector is very dangerous on mobile devices. Mobile also brings a number of new attack vectors existing solutions are powerless to prevent, including:

- Personal email.
  Corporate email gateways detecting phishing attacks are not relevant when users access their personal emails on mobile devices.
- SMS and messaging apps (e.g. WhatsApp).
  While email accounts may have protections, SMS and messaging apps do not.
- Malicious apps (e.g. BankBot).
  Traditional anti-phishing techniques are not equipped to detect malicious apps that mimic legitimate apps to phish credentials.

Key to mobile anti-phishing: on-device, machine learning-based detection

While gateways and firewalls can protect traditional endpoints against email-based phishing attacks, mobile devices have all the new vectors/issues discussed and are outside of the corporate network the majority of the time. Additionally, while lists of known bad URLs can help in an email stream (by pulling emails that have not yet been seen, for example), they do not provide protection against zero-day phishing sites that a mobile device can be accessing in real-time via SMS, etc.

When it comes to detecting mobile phishing attacks, Ivanti knows protection must occur where the attack is actually happening: on-device. And that protection must utilize machine learning in order to combat even zero-day threats.

MTD's proven machine learning approach is perfectly suited for enterprise mobile security in the Everywhere Workplace. Our machine learning engine analyzes system data to identify malicious behavior, and then creates sophisticated math models to enable on-device detection. MTD is not looking for a specific or partial match to a known attack (e.g. a URL in the phishing case); it is identifying attacks, even those never seen before, by telltale actions indicating a threat is occurring or imminent.

MTD provides on-device, machine learning-based detection of device, network, phishing and malicious app attacks.

While creating a highly effective machine learning-based detection engine like that used by MTD is complex and requires years of data collection and training, the concept may be best understood via simple analogies from other parts of life.

For example, based on years of training and a few key questions asked of a patient, a heart surgeon can look at an electrocardiogram readout and immediately diagnose the situation. She does not need to know in advance that the patient has a certain condition; she ascertains it by knowing which data is relevant (and which data should be ignored) in making an accurate diagnosis. Machine learning operates the same way, albeit in an automated fashion.

For targeted attacks, hackers...

1. Use unknown or morphing attacks designed to avoid simple deterministic detection.
2. Focus on compromising the device, which is the primary way to remain persistent and own/weaponize the device going forward.
3. Utilize man-in-the-middle (MITM) attacks or phishing techniques to deliver the exploits required to compromise the device. For the most part, they will not drop an app in the App Store or Google Play and hope someone from the targeted organization will download it.

As a result, enterprise mobile security solutions must...

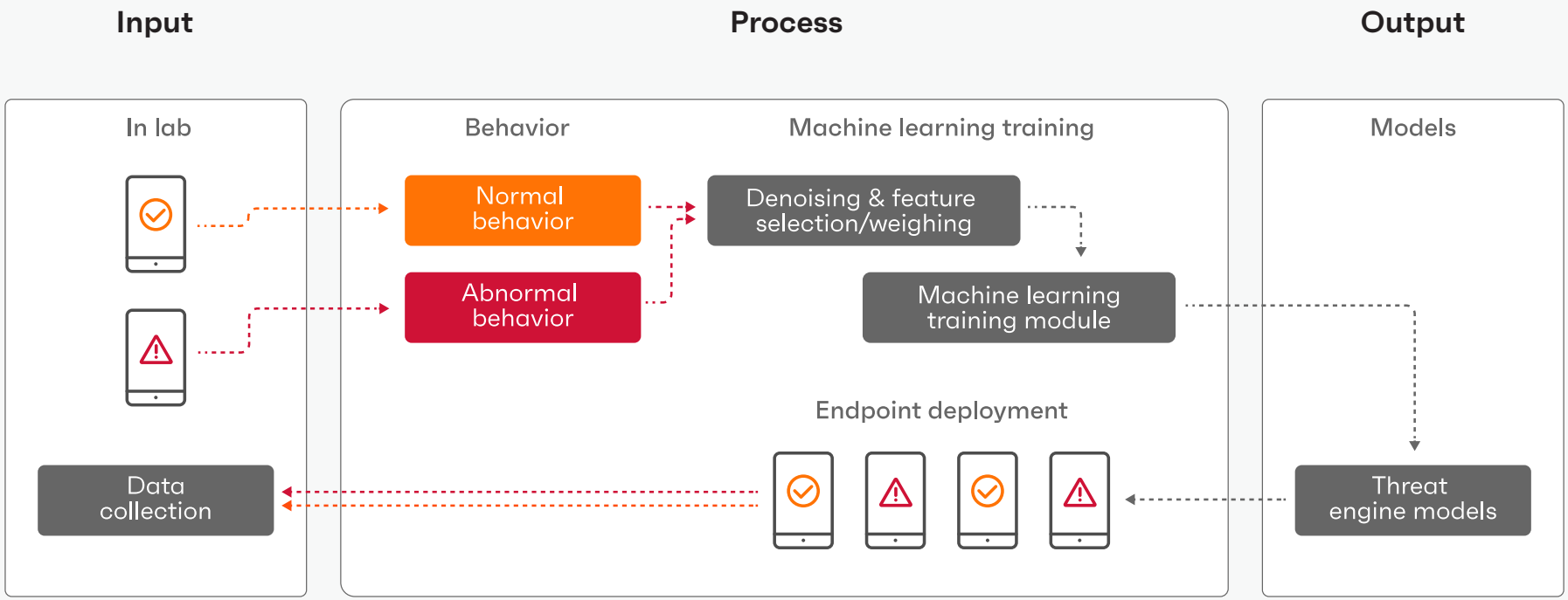
1. Augment any deterministic approaches with machine learning-based detection to stop unknown/morphing attacks used for targeted efforts.
2. Simultaneously cover all attack vectors across the device. A single point of failure is enough to fully compromise a device.
3. Detect threats on-device, and not require cloud-based lookups. If an attacker uses an MITM or rogue access point, he controls the network and will not connect the device to any cloud-based detection solution.
4. Use the right environment for the right problem, e.g.:
   a. **Training.** Given the billions of data points needing analysis, machine learning training should occur offline in the cloud.
   b. **Detection.** To prevent MITM circumvention and other risks associated with cloud-based approaches, actual detection must occur on-device.

Ivanti strongly believes in a few fundamental truths about enterprise mobile security

With these tenets in mind, the next sections articulate MTD's implementation and approach to cloud-based machine learning training and on-device detection of phishing sites. We believe this combination is the only way to provide effective enterprise mobile security.

Training: cloud-based machine learning

In order to create highly accurate predictors of mobile threats, a machine learning engine like that used by MTD must analyze (and repeatedly reanalyze) billions of data points. To process such a massive amount of data, Ivanti leverages dozens of high-performance computing clusters that live in the cloud to build its machine learning models. The models are then evaluated on-device to provide immediate detection, even of previously unknown threats – and even when disconnected.



Detection: on-device and machine learning-based

In keeping with the philosophy of "right environment for the right problem," the heavy lifting of machine learning occurs in the cloud. And, once the models are delivered to devices, all actual detection occurs on-device, in real time.

Here are some of the benefits of on-device, machine learning-based detection:

- **Detects even unknown threats.**
  Unlike deterministic solutions, machine learning detects even previously unknown or zero-day threats.
- **Machine speed detection.**
  Since mobile attacks occur at machine speed, protection must be able to respond in kind. Only real-time, on-device detection can match machine speed. Cloud lookups cannot match that speed since they inherently have delays associated with traversing networks back and forth.
- **Highest privacy protection.**
  By doing all detection on-device, data that may be considered sensitive does not need to be exfiltrated to the cloud.
- **Disconnected protection.**
  On-device detection provides immediate protection against network attacks like MITMs that can render cloud-based detection useless. Only on-device detection can continue providing protection even when disconnected from the network.

Separating hype from reality

Today, most mobile security vendors make machine learning claims. To determine the reality of the approach from any vendor (including MTD), ask these questions:

1. Does the machine learning capability work without requiring a patient zero or sacrificial lamb?
2. How extensive is the machine learning math model and how many years has it been tested in the real world?
3. How often does your solution need updating, including new URLs (for phishing detection), to detect the latest threats?
4. Does the machine learning capability work both in connected and disconnected environments?
5. Can your protection work in milliseconds, with little impact to CPU and battery usage?

Privacy-centric URL evaluation mechanisms

In order for mobile phishing detection to occur, the solution must be fed URLs that may be suspicious. There are two primary mechanisms in use.

1. **Manual submission.** Most solutions provide users with an ability to manually submit a URL for testing, but that requires users to be aware and trained, not only on phishing but on how to long-press and submit into the phishing solution.
2. **Automated evaluation.** To monitor all traffic for malicious URLs, solutions often use VPNs to automatically enable URL assessment.

For each mechanism, MTD's on-device detection provides key benefits over how cloud-based solutions utilize them (if they have them at all):

- **Manual submission**. Since MTD does all detection on-device, user privacy is protected. Data that may be considered sensitive (including websites being browsed), does not need to be exfiltrated to the cloud.
- **Automated evaluation**. In addition to the privacy advantages cited in the manual submission point above, MTD's on-device VPN uses significantly less battery than off-device ones required by cloud-based solutions because it is not establishing and encrypting outbound sessions to the cloud.

Complete mobile phishing protection

In the Everywhere Workplace, where corporate data flows freely across devices and servers in the cloud, Ivanti empowers your employees to work securely anywhere – even as mobile phishing attacks continue to increase. Ivanti's multi-vector mobile phishing protection for iOS and Android devices detects and remediates today's complex mobile phishing attacks.

Multi-tier security strategy:

- **Eliminate passwords.**
  Reduce the risk of data breaches that result from stolen credentials.
- **On-device detection and remediation for mobile threats.**
  Machine learning-based protection against device-, network-, application-level and phishing attacks (DNAP). No Wi-Fi or cellular connectivity required.
- **Multi-vector anti-phishing.**
  On-device machine learning and phishing URL lookup can be expanded to include cloud-based lookup for improved effectiveness.
- **The foundation for the industry's first end-to-end, zero trust security platform.**
  Create and enforce compliance policies to secure your Everywhere Workplace.

Attack vectors:

Achieve 100% user adoption for anti-phishing

MTD enables seamless deployment for anti-phishing, as well as protection and remediation for attacks at the device, network and application levels. No user interaction is required to activate, so admins can ensure 100% adoption. Tiered compliance actions can be leveraged to help drive and keep adoption in order to improve your organization's overall security posture.

Deploy multi-vector phishing protection and remediation

MTD anti-phishing detects and remediates phishing attacks across all mobile threat vectors, including text and SMS messages, instant messages, social media and other modes of communication, beyond just corporate email. Multi-vector phishing protection leverages on-device machine learning and database lookup. Extend to include cloud-based phishing URL database lookup for even greater effectiveness. In addition, phishing analytics can be used to provide fast and easy insight to better understand your organization's anti-phishing coverage.

Control the balance between security and user privacy

MTD anti-phishing puts your organization in complete control of maintaining balance between security and user privacy to best meet your needs and comfort level. Leverage MTD's highly effective on-device phishing detection, or easily expand detection into the cloud if you choose to do so. The choice is yours!

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 96 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information,visit ivanti.com

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

I. Verizon: 2021 Data Breach Investigations Report. - https://enterprise.verizon.com/resources/reports/dbir/
II. NewsWise: Tech companies not doing enough to protect users from phishing scams. - https://www.newswise.com/articles/tech-companies-not-doing-enough-to-protect-users-from-phishing-scams/sc-rsbn