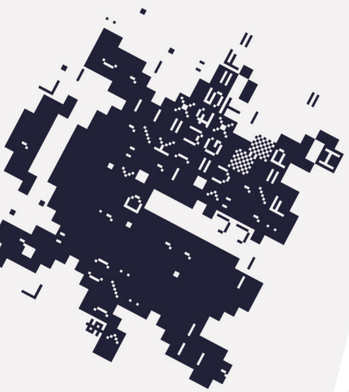
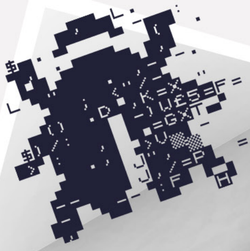
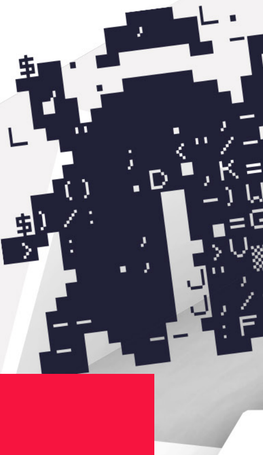
REVERSINGLABS







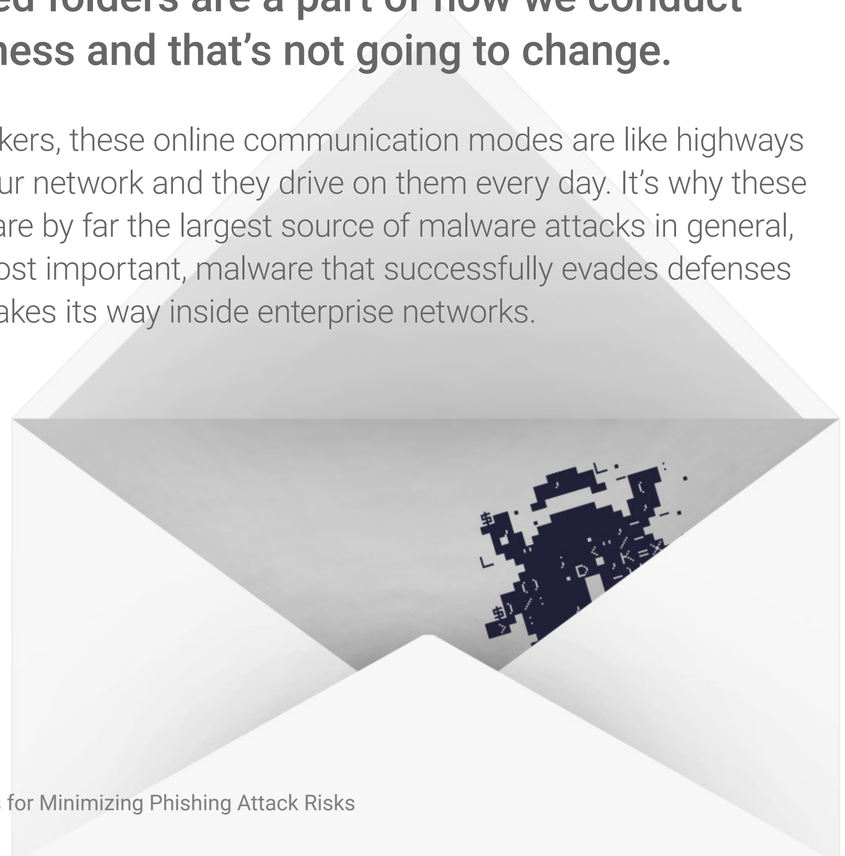
Strategies for Minimizing Phishing Attack Risks

Gaining Insights into the Destructive Objects Used in Phishing Attacks

The Phishing Attack Situation

There’s no way around it. Sending emails with attachments, downloading web files and using shared folders are a part of how we conduct business and that’s not going to change.

To hackers, these online communication modes are like highways into your network and they drive on them every day. It’s why these paths are by far the largest source of malware attacks in general, and most important, malware that successfully evades defenses and makes its way inside enterprise networks.



Phishing, a hacker favorite, isn’t a type of malware. Rather, it’s an attack delivery method. A recent study revealed the extent and severity of the problem:

92%
of malware comes through email, and it's the largest hole for organizational data loss

68%
of malware originates from Microsoft Office

30%
of all phishing emails are opened by users and

12%
click on the infected attachment or link.

A Bad Situation That's Getting Worse

Resourceful attackers, inadequate defenses

Sophisticated attackers have plenty of advanced tactics to choose from. One of these is polymorphic malware, which changes frequently to beat anti-virus tools and compromise organizations' file sharing sites. These ever-changing threats are extremely difficult to defend against using existing controls.

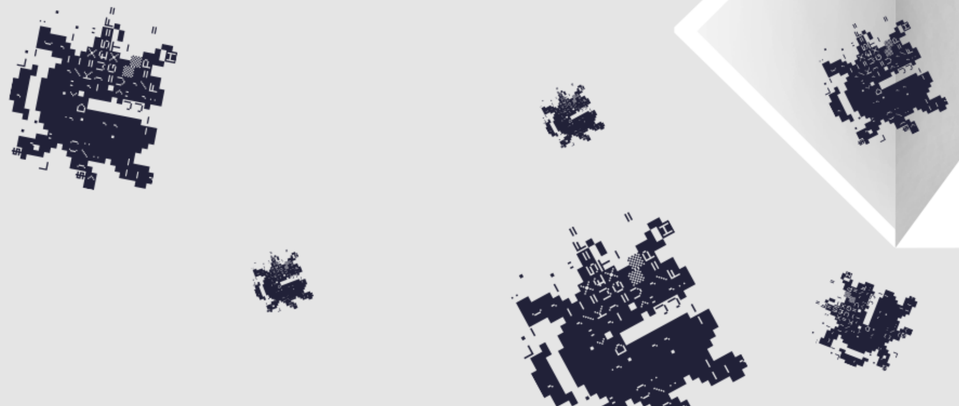
Lots of alerts, threat data and entry points

Most organizations suffer from a lack of integration across existing security infrastructure, too many alerts coming from endpoints, and overwhelming amounts of data coming from threat intelligence feeds. Combined, these factors make it very difficult to defend against phishing attacks at all points of entry.

Doing that in real-time? For most security teams today, their response would be "Yeah, right." Advantage: HACKERS.

The Bottom Line

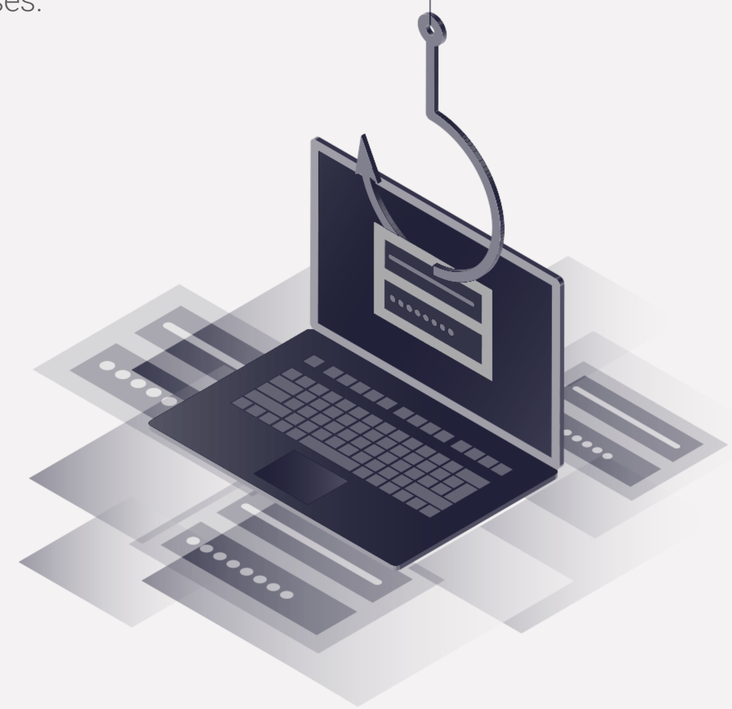
To counter the growing phishing problem, enterprises need **better, faster and more comprehensive** ways to detect and neutralize these attacks.



The Phishing Scam

All phishing is based on deception.

Cybercriminals use phishing as a way to trick people into sharing their credentials (log-ins and passwords). When a victim falls for it, hackers steal their credentials and use them to access valuable or sensitive data of all kinds. Cybercriminals then either sell the credentials or data on the black market or use it for other criminal purposes.



There are two basic types of phishing attacks:

Social engineering — In these attacks, hackers create fake versions of websites, and send email messages encouraging users to click on a link or download a file. Once the user falls for it, the hackers have their way in. It's a numbers game, so hackers continually broaden their nets to cover more people, thereby increasing their chances for success.

Spear phishing — These attacks target a specific individual or job role due to their access to information or data. Attackers research their targets online and elsewhere, and then use that intel to craft a legitimate-looking email to con the user into clicking a link or downloading a file. Once that happens, the attacker is in control.

How Phishing Attacks Work

Following are the three basic phases of phishing attacks, along with a few of the most popular methods used by attackers. Understanding these phases and methods is a key early step in managing the problem. Here is how they do it.

SEND PHISHING EMAIL

Attacker sends malicious **email** to an unsuspecting person. The email looks legitimate but contains malware hidden in an **attachment** or **link**. When the user clicks on it, it takes them to a malicious site.

EXPLOIT USERS: 3 METHODS

METHOD 1

Email **attachment** with embedded malware

- User downloads attachment
- File executes, malware checks machine for vulnerabilities

METHOD 2

Malicious **link to spoofed login**

- User clicks link in email
- Link opens spoofed web login page
- User enters credentials, hits submit

METHOD 3

Malicious **link launches exploit kit**

- User clicks link in email
- Link opens malicious site
- Site launches an exploit kit, checks user's machine for vulnerabilities

STEAL DATA

Attacker gains unauthorized access to all assets that the user/victim has rights to until detected. Most malware remains undetected on networks due to the difficulty of detecting advanced phishing tactics.

Credentials are sent to the attacker who can now access personal or work data as if they were the actual authorized user.

269 BILLION

emails are sent every day.

150 MILLION

of those are phishing emails **from attackers**.

↑ 36%

Email fraud attacks rose to 36% of targeted organizations

↑ 80% ↑ 4%

Up 80% vs. the year-ago quarter and 4% vs. the previous quarter

↓ 68%

The number of spoofed identities plunged 68% vs. the previous quarter

Most companies were targeted

at least once

Fireeye, Email Threat Report, https://www.fireeye.com/offers/rpt-email-threat-report.html

Three-Step Guide to Mitigating Phishing Risks

Cybercriminals' advanced tactics combined with the limitations of traditional security tools means that phishing attacks are often successful.

To counter this growing threat and thwart these attacks, organizations clearly need a better approach. Following is a three-pronged strategy that companies can implement to lower phishing risks and reduce or eliminate high-impact attacks in their environments.

Create Layered network security controls

using resources such as endpoint detection and response (EDR) with SIEM and SOAR event orchestration for prioritized alerting.

Make end-user training a priority

Introduce employees and users to phishing techniques by running attack simulations to increase their awareness of this type of attack. Enable them to avoid falling for the deception while encouraging users to report phishing threats.

Focus on high-risk targets

Use role and domain-based scoring to determine which individuals are at the highest risk, and take additional security measures with them.

Layered Network Security Controls

The first step is for an organization to implement a combination of the following security resources.

Email Security Gateways

Blocking known malicious files and senders and preventing assets from leaving the network (data loss).

Anti-Virus Systems

Checking signatures of incoming executables against databases of known malware and watching for suspicious activities caused by unknown viruses.

EDR

Model hashes of files for attacks using AI and alerting when suspicious behavior is found.

Dynamic analysis systems (sandboxes)

Identify malware in attachments by executing suspicious files in controlled environments.

SIEM and SOAR tools

Correlate and automate threat alerts by providing context and orchestrating expedited responses.

Threat intelligence feeds

Deliver the latest threat data seen in the wild and information about threats targeting companies or types of organizations.

Employee/end-user training

Forewarned is forearmed. That's why organizations implement programs designed to familiarize their employees or users with the phishing methods and techniques used by hackers.

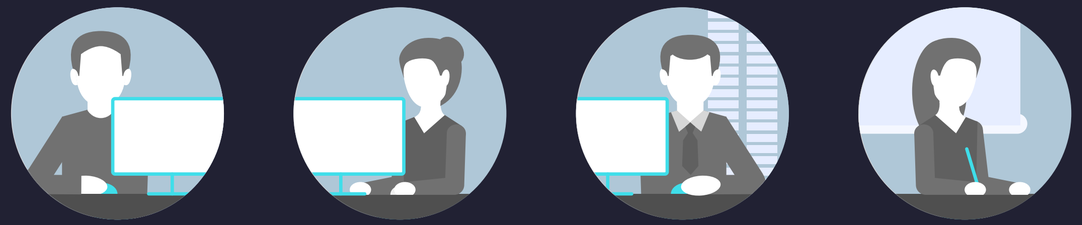
The goal is to train users on how to spot these attacks so they don't fall for them. When the deception fails, so do the attacks.

With education, users are more likely to think before they click. And if users do get tricked and an attack gets through, they can be more effective as part of their company's last line of defense.

In addition, users who spot attacks can submit them to an "abuse box" monitored by the SOC. Engaging end users to report attacks in progress can increase capture rates and significantly decrease response times.

Highly Targeted Employees

As a group, lower-level employees receive 67% of highly targeted attacks. But C-level executives, directors, department heads may be targeted disproportionately more often.



CONTRIBUTOR	MANAGEMENT	UPPER MANAGEMENT	EXECUTIVE
40%	27%	27%	6%

By department, workers in operations and production functions are the most exposed, representing 23% of highly targeted attacks, roughly the same as the previous quarter.

↑ 4x

Email-based corporate credential phishing attacks rose 4 times vs. the previous quarter.

Individual contributors and lower-level management accounted for 67% of highly targeted malware and phishing attacks.

67%

Attacks against executives and upper-level managers rose 4 points to about a third of all attacks.

↑ 4 points

High-risk Targets

Attackers target specific individuals, roles and domains based on their access to sought-after data and information. Surprisingly, their targets aren't always members of senior management. Low- and mid-level managers are among the most frequently targeted.

Organizations can provide enhanced protection for their frequently targeted staff members by tracking threat and attack trends. Over time, attack index scores can be built based on the profiles of those most likely to be attacked.

High-scoring individuals can be tapped for more intensive training and other ratcheted-up security measures.

Proofpoint, Protecting People, https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-protecting-people-autumn-2018.pdf

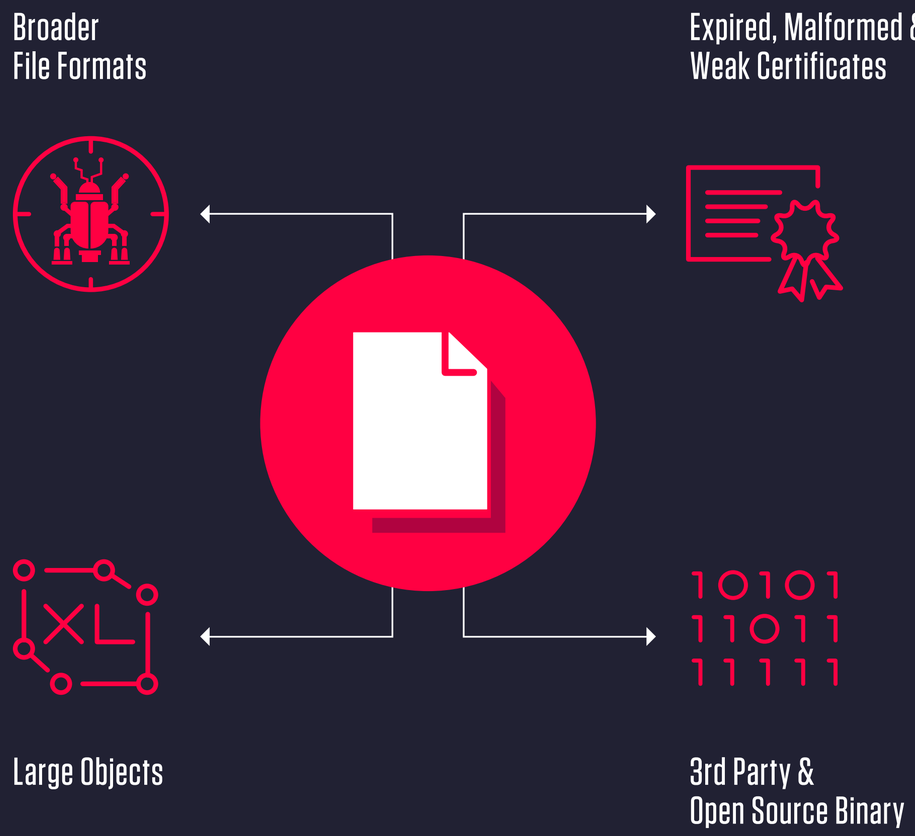
Yet Many Attacks Are Still Succeeding

Despite embracing strategies such as those described above, implementing a range of security resources, making significant security investments and taking layered approaches, enterprises are still failing to prevent many phishing attacks.

In fact, one respected source puts the number of successful phishing attacks at around 30% of the total attempted.

The reason is that SOCs don't have the tools and data required to instantly identify malware and quickly move through SIEM alerts.

Instead, they're still using tedious, manual processes. That's nowhere near fast enough to identify, prioritize, respond to and contain these attacks.



A Closer Look at How Attacks Get Through

The complexity of file and object formats, and varied file sizes and types make it difficult for SOC teams to quickly detect the presence of malware. Also, security issues with trusted third-party software, open source code and malformed certificates are difficult to detect, which means there are still plenty of ways for attackers to circumvent existing security controls.

No security solution is perfect. Every type has its flaws and weaknesses. When it comes to phishing attacks, however, traditional security solutions have one major problem. None of them have the ability to look inside incoming files (with speed at scale) to detect the presence of malware, and to understand its form and structure.

Simply put, if you can't see it, you can't stop it.

BLOG SERIES CALL OUT

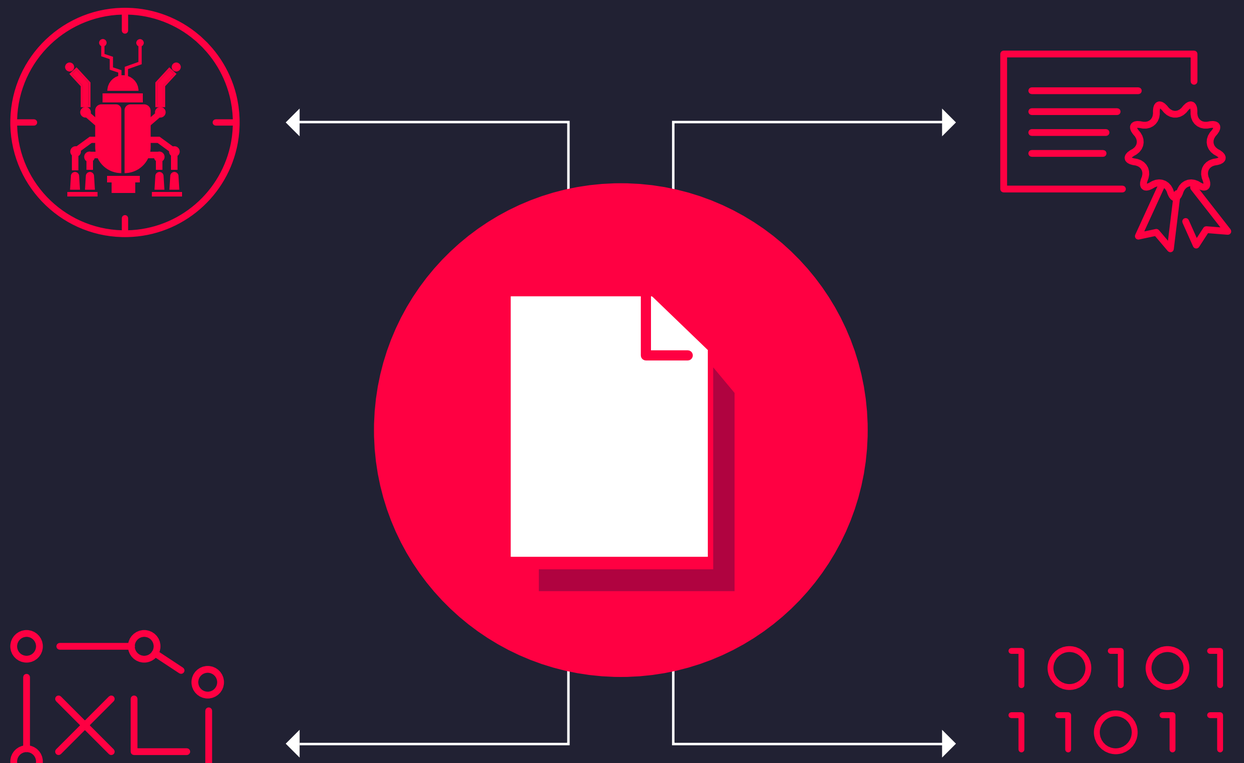
Check out our five-part blog series on advanced research into modern phishing attacks

Broader File Formats

malware in emerging formats including encrypted PDF's

Expired, Malformed & Weak Certificates

or loose usage of private keys



Large Objects

size and complexity break other analysis tools

3rd Party & Open Source Binary

including infected third party or open source

Bottom line:
No traditional security solution can look into files to see the form and structure of malware to understand the DNA of the file and display it. So, malware is still getting through.

Advanced Defense:
Real-time Insights into Destructive Objects

You've implemented some form of the three-pronged phishing defense strategy outlined above. But relentless attacks are still coming in via email — and sometimes they succeed. You've had it with phishing attacks and you want to shut them down completely.

How can you do that?

There is a fourth prong to this strategy now available that can help reduce the 30% of attacks that are being missed. It's called 'static analysis', and it gives you the ability to gain visibility of and insights into destructive objects in real time.

STATIC ANALYSIS works by instantly exposing destructive objects and their malware indicators in files without having to execute them. This technology provides information with unprecedented detail to SOC analysts. It gives them real-time visibility into malware – a capability they have never had before.

With static analysis, they can instantly see items such as: threat levels, last time seen globally, other related hash names and malware families, and pre-classifications of 'Malicious' or 'Known Good' along with severity and confidence levels. Results are filtered, grouped and instantly displayed, which allows SOC analysts to quickly determine whether to escalate or ignore a particular threat or alert for the fastest possible threat triage. And it can be implemented to cover all points of entry.

SOLUTION BRIEF CALL OUT

Learn more about high-risk Phishing attacks in our solution brief

More on Static Analysis Solutions

Static analysis solutions are designed to easily integrate into existing systems (e.g. Exchange Online Protection, ATP, ProofPoint, IronPort, Symantec Email Gateway, FireEye EX/AX). They add dimensions of depth to those controls with destructive object visibility that is not available through the use of those tools alone. SOC analysts can rapidly escalate suspicious or malicious email incidents to existing triage tools, SOAR platforms and DFIR/SOC teams.

With static analysis solutions, organizations can extend and optimize their existing security capabilities for increased effectiveness and ROI. Following are brief descriptions of how static analysis solutions achieve this.

Seamlessly Integrate at Scale Across the Enterprise

- Enrich EDR, SIEM and SOAR systems, and other network security resources to contain malware in real time.
- Integrate destructive file and object insights across existing security infrastructure elements to become a force multiplier for enterprises.

Speed File Analysis with Actionable Intel

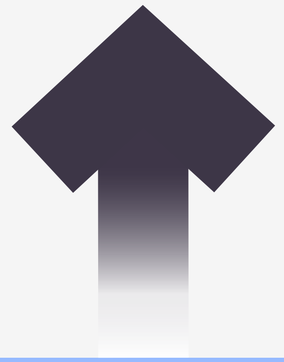
- Instant results without executing malware.
- Speed the detection of hidden high-risk files and objects through automated static analysis, and instantly prioritize the highest-risk files with actionable details.

Detect Threats with a Global Repository

- Exposes malware in any file type, size or format.
- Static analysis object processing results can be compared against global known malware and goodware databases for accuracy and confidence with results.

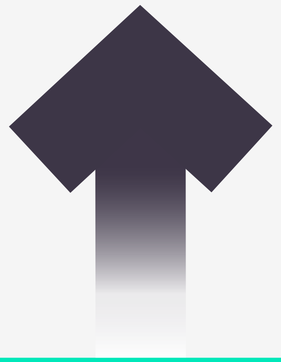
How Static Analysis Can Help Strengthen Each Level of the Three-Tiered Approach

In addition to adding a fourth layer of phishing attack protection in and of itself, static analysis can improve the other three layers. Here's how.



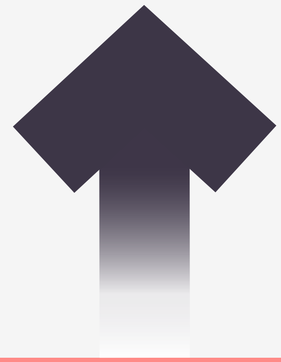
Layered Security

Ensure that file and object insights are applied to all existing security controls, and make malware intelligence and context instantly viewable in SOC analysts' dashboards.



User training

Reduce reliance on employee/user training by detecting phishing attacks before they make it to the users. No clicks or downloads means no successful attacks.



High-risk targets

Static analysis solutions can help this group by generating scores tied to the threats they face. The scores can trigger additional machine learning-based behavioral analysis security measures including heightened surveillance of anomalous activity.

ReversingLabs:
Your Partner in Preventing High-Impact Phishing Attacks

ReversingLabs provides advanced malware analysis and insights into destructive phishing attacks. Through its Titanium automated static analysis and file reputation platform, ReversingLabs delivers the fastest and most accurate insights in the industry, finding the hidden objects that are armed to destroy enterprise business value.

This hybrid cloud platform has tightly coupled connectors that seamlessly integrate with existing security investments such as EDR, email, SIEM, threat intelligence platforms and sandboxes. This integration greatly reduces incident response times for SOC analysts, while providing high priority and detailed threat information to threat hunters so they can take quick action through advanced search and YARA rule tooling.

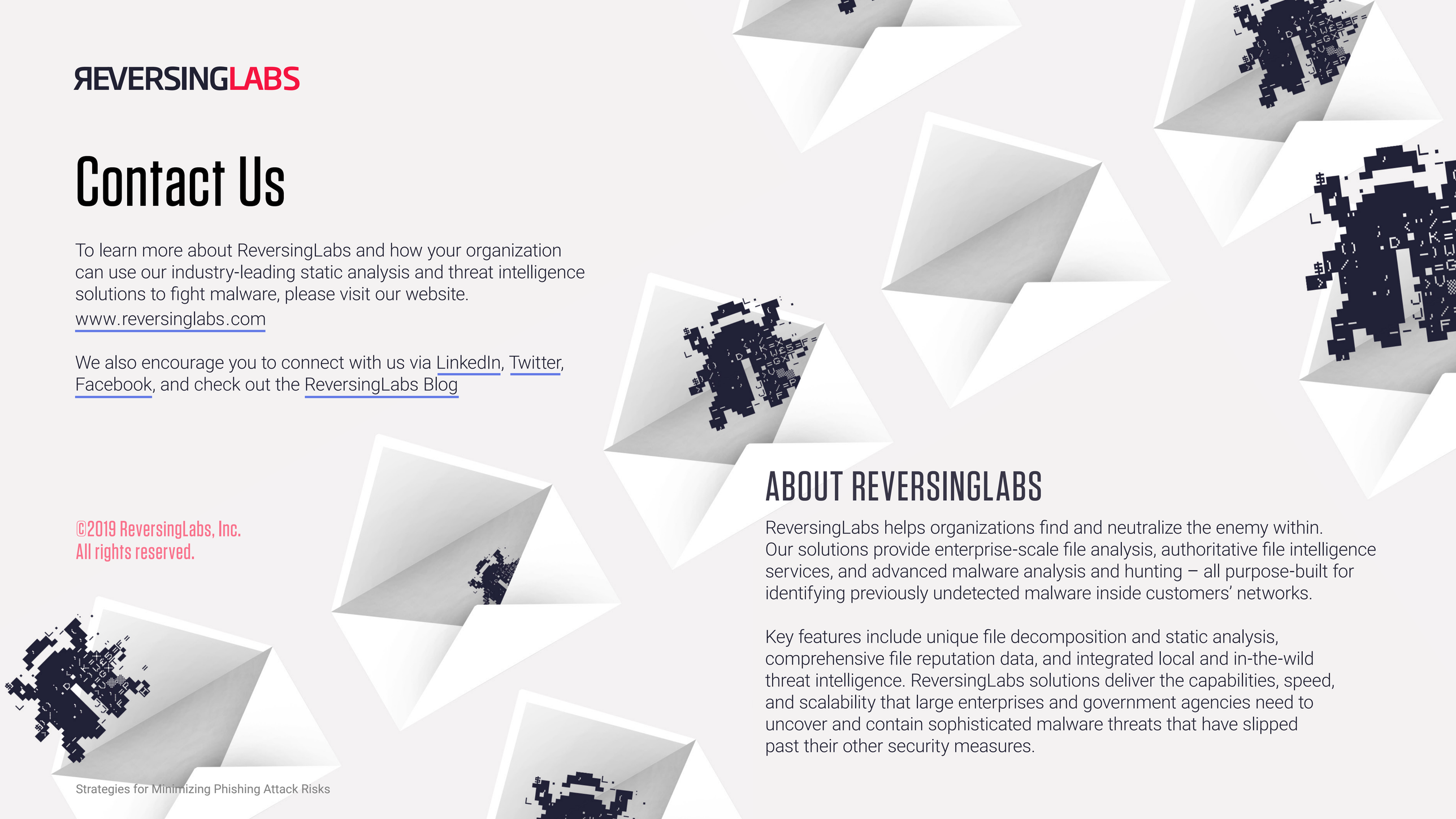
The result is that enterprises are able to more quickly find and neutralize previously undetected phishing attacks to eliminate or greatly reduce the damage they cause. Flexible and extensible by design, ReversingLabs solutions can bridge today's enterprise SOC, IT, and software development teams.

REVERSINGLABS

Contact Us

To learn more about ReversingLabs and how your organization can use our industry-leading static analysis and threat intelligence solutions to fight malware, please visit our website.
www.reversinglabs.com

We also encourage you to connect with us via LinkedIn, Twitter, Facebook, and check out the ReversingLabs Blog



ABOUT REVERSINGLABS

ReversingLabs helps organizations find and neutralize the enemy within. Our solutions provide enterprise-scale file analysis, authoritative file intelligence services, and advanced malware analysis and hunting – all purpose-built for identifying previously undetected malware inside customers' networks.

Key features include unique file decomposition and static analysis, comprehensive file reputation data, and integrated local and in-the-wild threat intelligence. ReversingLabs solutions deliver the capabilities, speed, and scalability that large enterprises and government agencies need to uncover and contain sophisticated malware threats that have slipped past their other security measures.