Polymorphic Phishing Attacks: 5 Insights to Help Stop Them

Threat actors are evolving quickly and modern day attacks are more complex and sophisticated. Learn why intelligence and human reporting + AI are a MUST.

COFENSE.COM

Polymorphic malware applies changes rapidly — as frequently as every 15-20 seconds![1]

What exactly makes a phishing attack polymorphic? In these campaigns, attackers make slight changes to the same email—to the subject line or sender name, for instance—as they probe security systems to see what might get through.

Polymorphic attacks normally begin with a targeted campaign, designed to grab user credentials. When the first few users take the bait, the attacker uses their credentials to target other users. Again, the dynamic change in the attack prevents automated controls—normally, secure email gateways (SEGs)—from screening out the messages.

Why are polymorphic attacks more successful? A campaign that lacks uniformity doesn't look like a campaign and makes it difficult for security operators to keep rules up to date at the gateway. For many cybersecurity teams who lack bandwidth, finding the full scope of a polymorphic attack to quarantine is challenging and time consuming.

Even worse, polymorphic attacks are not only effective, they are very easy to launch thanks to automated and inexpensive kits sold on the black market.

This is why human reporting, plus AI and threat intelligence are all needed for a comprehensive phishing defense strategy.

The Stakes Are High Around the Globe

The numbers tell the tale:

$3.86 Million

The cost of a data breach in 2021 was $4.24 million, this was a 10% rise from the average cost in 2019 which was **$3.86 million** [2]

1.38 Hours

The average breakout time – initial intrusion to lateral movement – is **1.38 hours** [3]

24 Days

The global median dwell time of an attacker is **24 days**[4]

The Stakes Are High Around the Globe

Real-world polymorphism

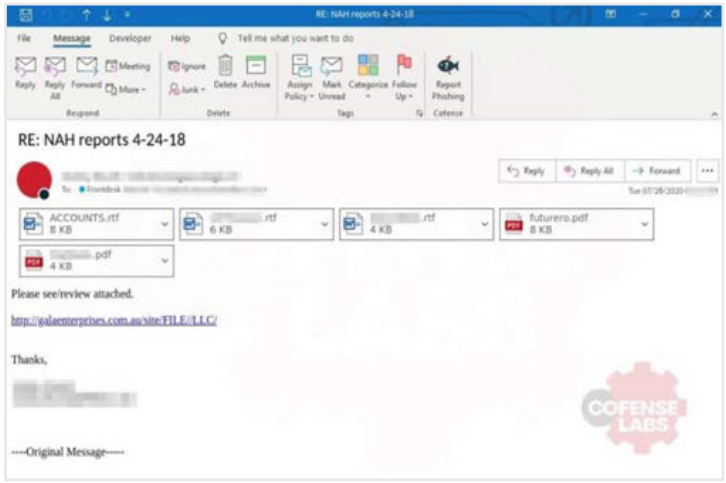
Polymorphism is easy to achieve via simple programmatic logic in phishing kits. By using templates and wordlists, actors are able to quickly generate similar, but slightly different emails en masse. The predominant advanced actors in the phishing landscape, however, have figured out an even better method for creating unique emails.

Emotet, QakBot, and others have been using stolen emails at a massive scale for some time now. Beyond having unique subjects, their typical phishing emails will have unique bodies constantly changing payload hashes, and payload URL's.

Without diligent tracking of all attributes of these botnets, identifying which emails are part of a campaign is difficult at best.

- Jason Meurer, Cofense Senior Research Engineer

Cofense Research Spotlight



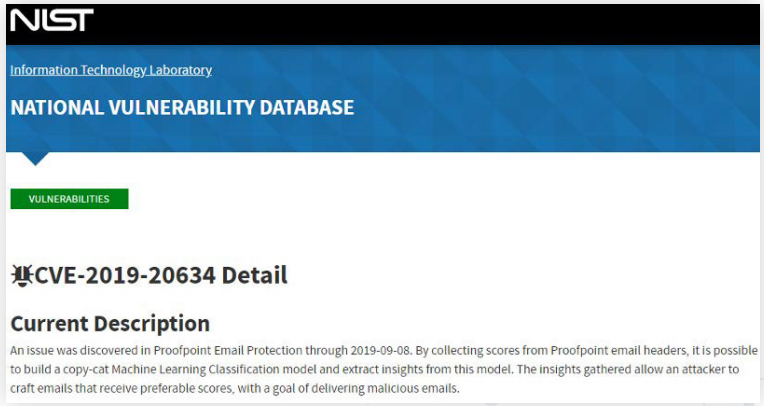
An Emotet reply chain email - this email has been heavily redacted, and the stolen message content is not visible. This email, however, contained medical billing information, along with a number of benign attachments, including bills and documents included in the initial email.

This particular email was distributed to a small set of Brazilian users, but a large number of variable COVID-related emails were seen during the same day.

Top 5 Insights to Help You Level Up Your Phishing Defense Against Polymorphic Attacks

1 Not All Phishing Threats Are Blocked by Technology

Perimeter controls will stop most phishing emails. After all, security tech is designed to stop threats in volume. But what happens when attackers use technology to fool your technology? Here's an example. The US National Institute of Technology (NIST) laboratory issued a notice on the threat below.


NIST

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

CVE-2019-20634 Detail

Current Description

An issue was discovered in Proofpoint Email Protection through 2019-09-08. By collecting scores from Proofpoint email headers, it is possible to build a copy-cat Machine Learning Classification model and extract insights from this model. The insights gathered allow an attacker to craft emails that receive preferable scores, with a goal of delivering malicious emails.

Researchers developed a Proof of Concept attack called ProofPudding to show how a machine learning algorithm could be used to find weaknesses in Proofpoint's SEG. Proofpoint added email headers that contained sensitive information on their algorithms. By selectively sending variations of emails to the gateway, the researcher(s) were able to determine which alterations and/or specific keywords would be blocked or allowed through the gateway.

In other words, while the SEG stopped most of the thousands of phishing emails it saw, it lacked the insight to know an attacker had made adjustments. It did the job it was programmed to do, again and again and again, but wasn't instructed to look for other troubling indicators.

2 Human Intuition is a Key Ingredient

Unlike machines, humans—both well-trained users and professional security teams—come equipped with intuition. They know or can be trained to trust their gut when looking at emails. Human intuition is crucial in the cyber-kill chain, especially when polymorphic phishing attacks hit.

A kill chain will typically have several links, spanning attacker reconnaissance to acting on objectives. Defenders want to stay left of email delivery, the point at which a breach becomes a possibility. When malicious emails get past that point, as some inevitably do, security teams need visibility so they can respond, ***fast***.

Phishing & The Cyber-Kill Chain

Why are humans critical to staying left of breach? **Consider this:**

100%

of threats seen by the Cofense Phishing Defense Center™ are identified and reported by users

0%

are stopped by perimeter controls

Ordinary employees, trained to say something when they see something, alert our phishing experts to investigate possible threats. Going back to the NIST example in the previous section, this is exactly where timely insights help you stay left of breach, in particular when facing attacks that morph in the blink of an eye.

3 The Best Awareness Training Mimics Relevant Threats

In a world of infinite threats, which ones should you train users to detect?

Rule of thumb: threats your industry or organization faces. These days, that's likely to include polymorphic phishing.

Focus on Your C.A.R.T.

Current | Active | Real | Threats

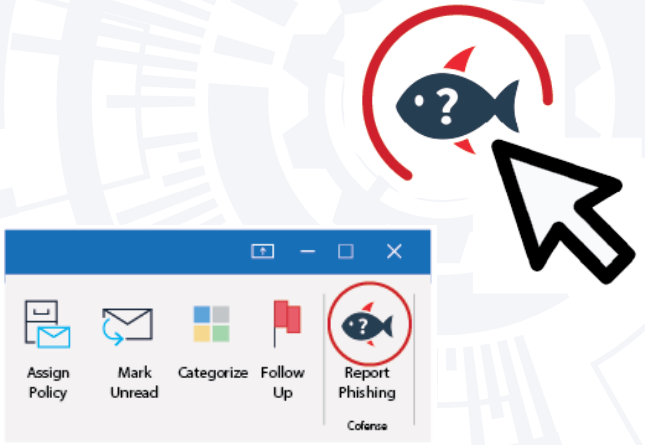
Ideally, awareness training concentrates on threats that elude your SEG. Some companies also simulate threats they think they're likely to see, based on available intelligence.

If your security teams, or other companies, have remediated a credential phish that uses a fake invoice, that's a good candidate for the next training exercise. And if that email shifted its shape, modifying subjects, senders, or any other element, training will help to stop the next polymorphic attack.

TIP: Cofense strongly suggests you avoid randomized phishing training, where each employee receives a different phishing scenario. The intent of randomization is to prevent users from tipping each other off: *"Hey, I just got this training scenario. Don't click!"* But isn't that what you want to happen when real threats arrive—people sounding the alarm about something risky?

4 User Detection is Great, but Reporting is Even Better

Cofense has proven the value of educating users to report suspicious emails. The idea is simple: with frequent practice, any user can learn to spot a phish and report it for investigation.



"Building a culture where users can report phishing attempts gives you vital information about what types of phishing attacks are being used."

UK National Cyber Security Centre

Email reporting is the critical link between awareness and response. In reality, it's the first step in response, the first action a human takes. Reporting is truly a learned behavior, a kind of conditioning, which builds muscle-memory so users won't think twice before raising a hand.

Over 2X More Resilient

Customers that use our Cofense Reporter™ button have a phishing reporting rate over 2x higher than their click rate.

Relevance + Reporting = Stronger Phishing Defense

Training for active threats and emphasizing reporting is the formula for improved user phishing detection.

5 While Humans are Key to Detection, Automation Speeds Response

When phishing emails reach the inbox, the clock is ticking. On average, it only takes 82 seconds for users to start clicking on a phishing campaign.[5] You can imagine the implications when the campaign is polymorphic. To stop the attack, you need automation to speed your threat response.

Email Analysis

When security teams try to respond manually to email reports, they usually fall behind. There are simply too many emails, most of them harmless. Automation can cut through noise and identify real threats, plus prioritize them so analysts can budget their limited time.

Search and Quarantine

In the best-case scenario, thanks to well-trained users and advanced automation, your SOC has identified a phishing email in a handful of inboxes. But who else received the phish? Again, you'll rely on automation to search all inboxes ASAP and quarantine the threat before lasting damage is done.

At a Glance:

1. Technology controls won't stop every phishing attack. Polymorphic attacks are designed to fool controls and quickly metastasize
2. Humans have what machines lack—the intuition to detect phish that evade technology
3. Awareness training should focus on the most relevant threats, such as polymorphic campaigns that hit your email gateway
4. If your people don't report phishing, your security teams can't see the threats that make it to the inbox
5. Once humans have detected a threat, purpose-built automation will speed response and remediation to protect your bottom line

Learn More

1. See real threats that are evading email gateways
2. Why SEGs are failing more than succeeding

Contact Us

Let us show you how to defend against phishing attacks.

Visit cofense.com or schedule a demonstration with Cofense today!

Request a Demo

Sources

1. Polymorphic Malware and Metamorphic Malware: What You Need to Know
2. IBM and the Ponemon Institute
3. Crowdstrike Global Threat Report 2021
4. Infosecurity-Magazine.com Global Attacker Dwell Time Drops.
5. CyberDB - Anti-Phishing Simulation and awareness market overview

About Cofense

Cofense® is the leading provider of phishing detection and response solutions. Designed for enterprise organizations, the Cofense Phishing Detection and Response (PDR) platform leverages a global network of nearly 30 million people actively reporting suspected phish, combined with advanced automation to stop phishing attacks faster and stay ahead of breaches. When deploying the full suite of Cofense solutions, organizations can educate employees on how to identify and report phish, detect phish in their environment and respond quickly to remediate threats. Cofense understands how to improve security, aid incident response and reduce the risk of compromise. For additional information, visit www.cofense.com or connect with us on Twitter and LinkedIn.