FIVE PHISHING PREDICTIONS.

2018

COFENSE.COM

BUCKLE UP, FOLKS. WE'RE IN FOR A ROUGH RIDE.

Predictions are like bellybuttons. Everybody has one. But phishing predictions from Cofense™ are worth thinking about.

The Cofense Intelligence™ and Cofense Research teams spend every day analyzing the latest data on phishing attacks and related threats. Customers use our insights to report and respond to real attacks that endanger their operations, bottom lines and reputations. Millions of their users get security awareness training through Cofense phishing simulations that mirror active threats.

If you want burger predictions, ask your favorite fast-food chain. For phishing predictions, you're in the right place. As you'll see, our experts forecast plenty to keep you busy...

DID YOU KNOW?

Sources: Symantec, 2017; Barkly, 2017.

PREDICTION 1. MORE MALWARE WILL TARGET OSX.

The good news from Cupertino: Apple's operating system is making real headway in the enterprise, and not just for mobile. For example, General Electric, one of America's largest corporations, announced last year it will actively promote Mac as a preferred option to all of its 330,000 employees. Businesses are following the lead of consumers (employees) who dearly love their Macs and iPhones.

The bad news from Cupertino: this will inevitably lead to an influx of OSX-based malware. In a sign of things to come, 2017 saw the appearance of OSX/Dok, a new malware attack that can monitor traffic to and from an infected Mac, making it capable of capturing credentials to sites you'd rather keep private. And earlier in 2018, the OSX Ma/Mi malware, similar to the DNSChanger malware circa 2012, reared its head to steal the personal information of victims.

It's an old story. The price of success, it seems, is a bullseye on your backside.

DID YOU KNOW?

90%

Over 90% of enterprises use Mac, with nearly half offering a choice of Mac and PC. Reasons for Mac adoption: ease of deployment, security, device configuration, support, software/app development and integration.

Source: 9to5 Mac, 2017.

PREDICTION 2. ATTACKERS WILL SEND MORE VICTIMS TO "SECURE" HTTPS SITES.

Services like Let's Encrypt have made it easier to host secure content, especially for small businesses and website owners. As of December 2017, Let's Encrypt had issued 62.3 million certificates, 22.1 million of which are active and online.

While this benefits many businesses and anybody else who wants to operate a secure website, it also makes it easier for phishing attackers to obtain TLS certificates, allowing them to create sites that appear legitimate. Throughout 2018, phishers will almost certainly capitalize on the ability to create secure-looking websites that are intended to harvest credentials, and other private information unwitting victims may supply, or to deliver malware without raising suspicion.

Not only will this make real-time inspection of traffic harder for network defense technologies, it will also make it more difficult for victims to identify malicious sites. A padlock in the address bar no longer signals the user is in safe territory. Wave goodbye to that signpost and hello (again) to the need for holistic phishing defense, through both network monitoring and user behavioural conditioning.

DID YOU KNOW?

HTTPS AS A DEFAULT

As of November 2017, 28% of the Alexa Top 1 Million websites used HTTPS as a default. Not only that, over 40% of the Internet's most popular websites have a secure implementation of HTTPS.

Source: statoperator.com, 2017.

PREDICTION 3. SOCIAL ENGINEERING ATTACKS WILL GET EVEN MORE SOPHISTICATED.

Due to the rise in successful BEC and W-2 fraud attacks over the past few years, we expect to see a corresponding increase in phishing attacks that rely heavily on social engineering and multi-staged conversational approaches to abscond with money and valuable data.

After all, as technological solutions to phishing attacks improve, why wouldn't the bad guys find better ways to skirt the machines altogether? It's hard, if not impossible, for traditional email security defenses to catch social engineering and sophisticated linguistics in emails without malicious links or attachments.

The Cofense Phishing Defense Center has been tracking this trend closely. We have seen that building rapport through social engineering is useful to attackers in creating credential theft or malware delivery phish. Attackers are luring users to engage in conversation and develop trust prior to compromising their device or harvesting the target's login credentials for account access. Once compromised, the attacker exploits that advantage for financial gain.

Because malicious actors are targeting your users and not just your technology, you need to train them to recognize and report phishing, including emails without links or attachments signaling "Malware inside!"

DID YOU KNOW?

98%

43% of breaches result from social engineering attacks. What's more, phishing emails accounted for 98% of all social-engineering related incidents and breaches.

Source: Verizon Data Breaches Investigations Report, 2017.

PREDICTION 4. PHISHING FOR CLOUD ACCESS WILL BECOME DE RIGEUR.

These days, almost everyone is using the cloud to store and provide critical data. This trend will keep growing...and so will attacks to gain access to these accounts. As businesses and individuals increasingly move to the cloud, malicious actors are following.

Whether it's document sharing services or a single sign-on suite, the keys to the enterprise kingdom can be stolen by attackers who obtain account login credentials—or through the delivery of malicious plugins and cloud applications that connect to your legitimate cloud accounts, similar to last year's Google Docs worm.

As the attack surface expands, threat actors are quick to capitalize. We expect adversaries to increasingly target your business enterprise and individual cloud accounts. Beware, access to your personal cloud accounts at work could compromise your business networks!

DID YOU KNOW?

20%

Over 20% of phishing attacks target cloud storage companies. That's nearly as many launched against financial institutions, the #1 target.

Source: PhishLabs, 2017.

PREDICTION 5. PHISHING WILL DRIVE GROWTH IN CRYPTOCURRENCY MINING BOTS.

In the past few months, the number of cryptocurrency mining applications distributed by phishing emails has exploded. Increasingly, malicious actors are distributing cryptominers not as an afterthought or secondary payload, but rather as the primary deliverable.

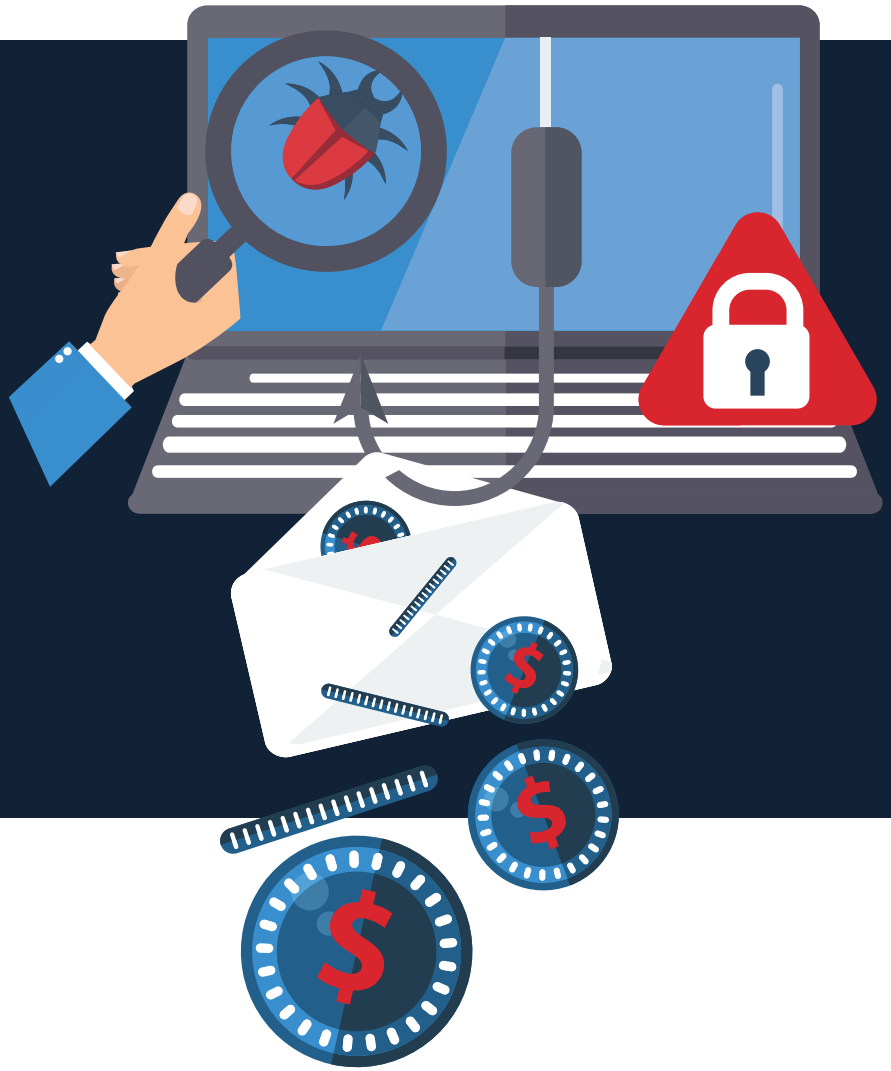
Though this sort of software isn't new, its profitability was hampered by low cryptocurrency values and lack of uptake among larger retailers and distributors. Higher values and the proliferation of cryptocurrencies have solved that problem, albeit wild fluctuations will likely cause some actors to prioritize potentially less lucrative, but more stable, currencies.

Expect to see aggressive distribution of cryptocurrency miners and more sophisticated mining software. Phishing remains the most effective way to distribute both malware and repurposed, legitimate software.

DID YOU KNOW?

96 COUNTRIES

96 countries do not restrict the use of Bitcoin. It's one reason why Bitcoin has an almost 60% share of the cryptocurrency market.



Source: Bitcoin.com, 2017.

COFENSE

"MAY YOU LIVE IN **INTERESTING TIMES**."

This ancient curse is current reality for anyone battling phishing (pretty much everyone). What's interesting: how the evolution of a scourge follows the success of so many things, like Apple's inroads in the enterprise, the way Let's Encrypt has helped small businesses and the game-changing popularity of the cloud.

What's an organization to do? Glad you asked.

To learn more about building a collective defense against today's top threats, visit our website:

www.cofense.com.

Good luck—and be careful out there!