2016

STATE OF SPEAR PHISHING

GreatHorn is a cybersecurity platform that helps organizations detect and prevent the most common sources of data breaches *before* they happen.

CONTACT US
GreatHorn Inc.
www.greathorn.com
+1-800-604-2566

“GreatHorn is a critical part of our cyber defense, as they help us detect and stop the kinds of attacks that other solutions miss.”

Bob Chin, CIO, Minuteman Health

EXECUTIVE SUMMARY

Every week, every month, every year, the number, scope, and damage inflicted by data breaches increases. Despite millions of dollars invested into the cybersecurity industry, large scale breaches just keep coming.

Over 90% of all cyberattacks begin in the same way, via carefully crafted emails that are designed to trick one or more of users into providing access to their accounts.

These emails often look exactly like valid communications from a company or individual whom employees know, and it only takes one successful deception to unravel an organization's entire cybersecurity framework.

Attackers can use credentials from a single user to move inside a network, escalating privileges, gaining access to critical infrastructure, and stealing sensitive data.

GreatHorn provides a unique approach to preventing these kinds of attacks: a fully-automated analysis engine, based on a foundation of machine learning, a data set comprised of millions of analyzed emails, and a realtime, end-user-centric approach to flagging threats before they become data breaches.

Unlike gateway-based alternatives, GreatHorn can compare an organization's unique information set -- relationships between internal and external domains, frequently contacted partners, and specific authentication patterns that can reveal compromised accounts -- to extrinsic threat details drawn from this massive data lake of previously detected threats.

We believe security should be automatic, ambient, and effective, and we're building a new kind of security company to make that belief a reality.

SPEAR PHISHING ATTACKS ARE ON THE RISE.

Modern adversaries are sophisticated, smart, and patient. Yesterday's technologies can't keep up.

Spear phishing attacks are highly customized attempts to use email to exploit users' trust by appearing to be legitimate and from well-known sources.

Every day, over 135 billion corporate messages are sent through the world's email systems; of those, approximately 1% are typically spear phishing attempts, capable of stealing credentials, IP, and even financial resources in seconds.

Research shows the average user is tricked into clicking on malicious links more than 50% of the time, especially if the email points to a domain belonging to a business partner, customer, or service provider that they regularly interact with.

Stopping this kind of attack requires comprehensive analysis that can both keep pace with the volume of email received by your organization as well as direct alerting to end users at the moment that an attack comes in.

90%

of all data breaches begin via spear phishing

THE GROWING PROBLEM

Spear phishing may seem like a narrow area of focus, but most large data breaches are initiated via email exploitation.

Until now, most organizations have had no way to systematically detect and respond to these attacks.

Most data breaches begin with spear phishing.

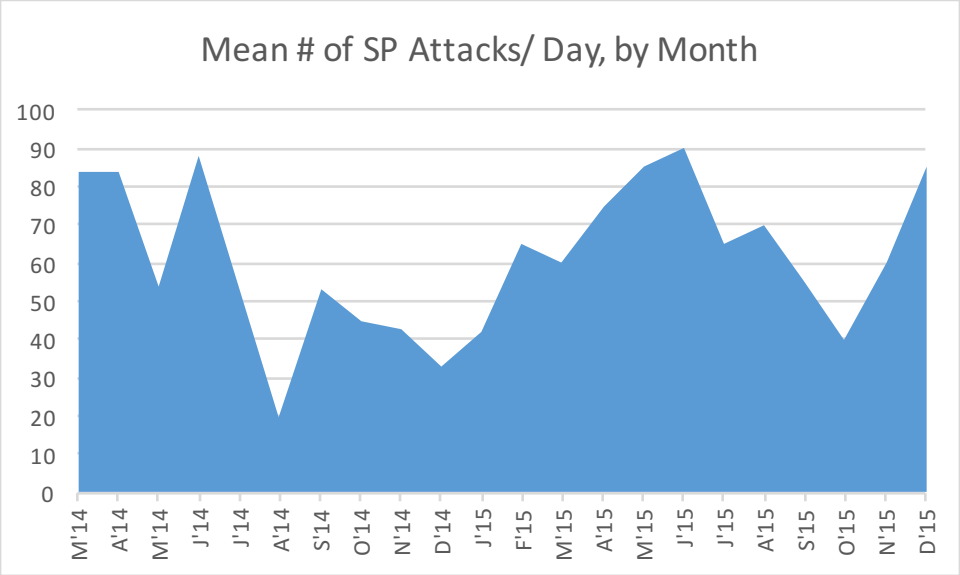
Deceiving ordinary users into clicking on a link, opening a file, or authorizing a wire transfer is one of the most successful ways to gain illicit access to an organization's resources, and it works most of the time.

Training alone doesn't work.

While security awareness training (SAT) is a strong component of a "defense-in-depth" security posture, on its own it amounts to hoping that employees do the right thing. Enforcing security policy and preventing the potentially catastrophic consequences of a breach should be automated and algorithmic.

Comprehensive detection is key.

Building out a properly defined strategy for stopping these kinds of attacks has to happen across your entire user base. GreatHorn's approach to detection is based on the premise that user workflows should never be interrupted, and that early detection and end-user alerting can prevent these kinds of breaches before they happen.



"GREATHORN WAS AN OBVIOUS FIT FOR US, AS HAVING REALTIME BREACH DETECTION AND PREVENTION BUILT INTO THE TOOLS WE USE DAILY MAKES IT EASY TO DEMONSTRATE OUR COMMITMENT TO PROTECTING OUR CUSTOMERS' DATA."

-Alok Tayi, CEO, Tetrascience

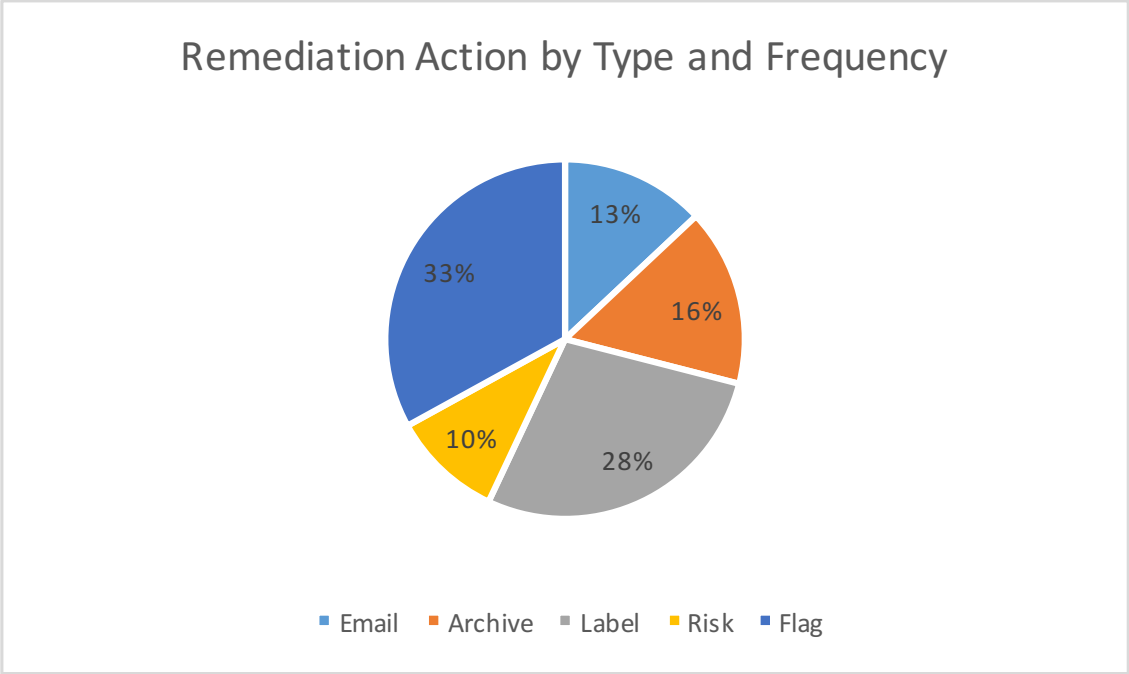
SPEAR PHISHING BY THE NUMBERS

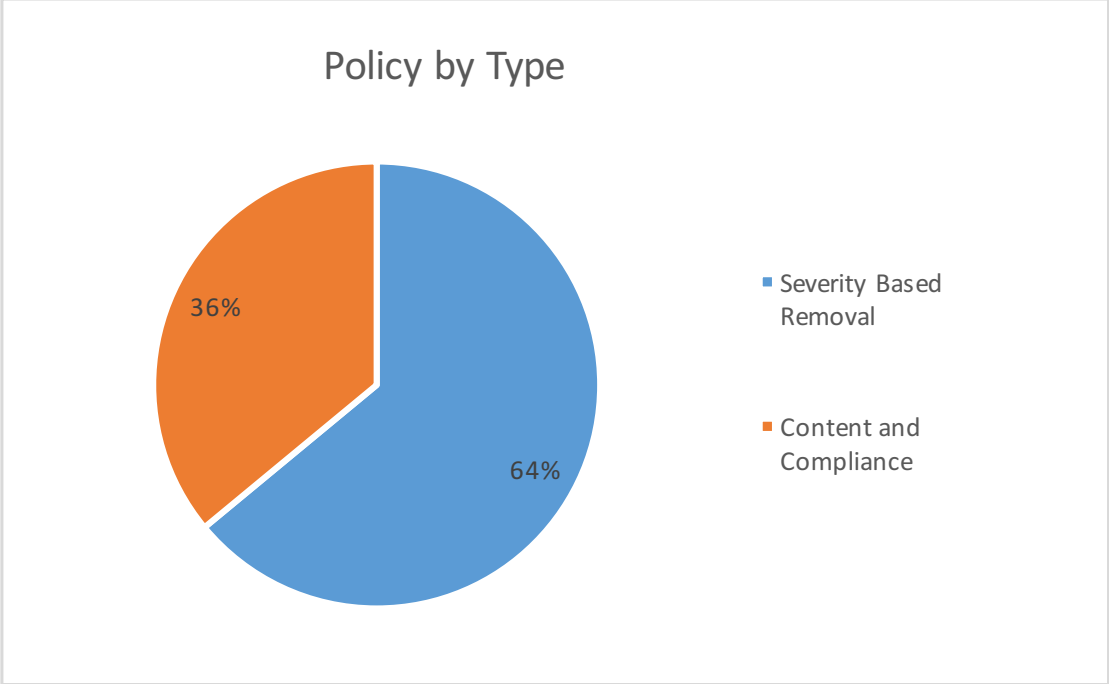
Drawing from over 3 terabytes of enterprise mailbox data, the GreatHorn Data Cloud reveals that attackers are relying increasingly on advanced attacks and payload-free messages to deceive users.

6,938	mailboxes analyzed for this report
20,335,178	emails in the sample set
352,467	suspicious messages detected
33,175	spoofing attacks identified and removed
9,363	homograph-based attacks interdicted

DEPLOYMENT METRICS

Effectively protecting against spear phishing at scale requires automation, not manual intervention. GreatHorn allows for a range of advanced remediation actions via its unique Policy Engine and native platform integrations.



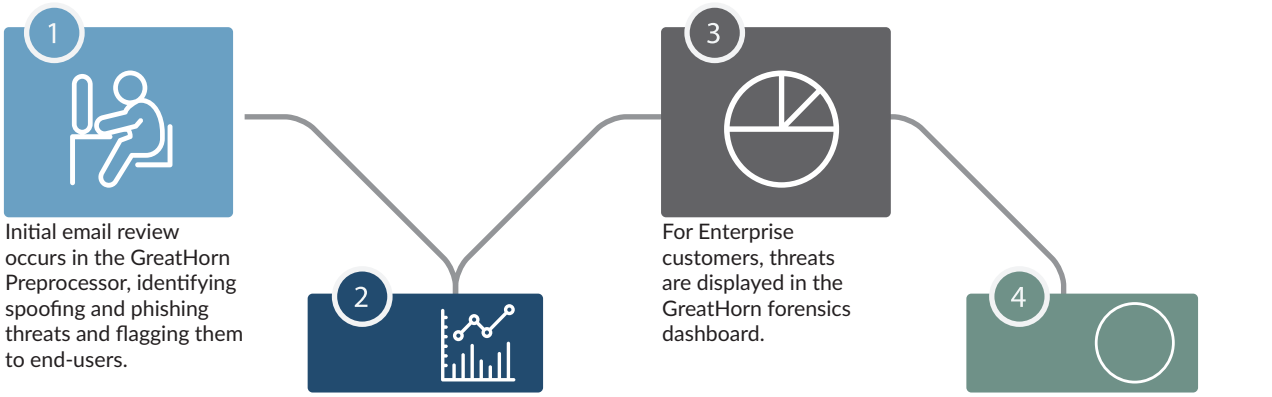


GREATHORN OVERVIEW

GreatHorn is designed to provide effective, end-to-end security without impeding user productivity.

BUILT WITH SECURITY IN MIND

GreatHorn's core approach to securing user email is designed around a four-stage analysis pipeline, ensuring that your organization's private information is never at risk:



ROBUST DETECTION

Realtime, effective security for today's most advanced persistent threats.

DIFFERENT BY DESIGN

The nature of spear phishing and communication based attacks has evolved over the course of the last 24 months.

From homograph attacks to sophisticated spoofing attempts, it has become nearly impossible for end-users to identify threats and attacks on their own. GreatHorn's patent-pending approach to threat identification is automating the burden of finding threats. Powered by a massive data set and ever-more-accurate machine learning systems that are capable of finding and preventing these increasingly pervasive and subtle attack types, no other solution today can boast the breadth or depth of detection that GreatHorn has.

We believe that security should be automated and ambient, and GreatHorn deploys in minutes, natively leveraging platform APIs to manage detection, rather than expensive and slow gateway-based detection systems.

DETECT

GreatHorn's core algorithms look at a wide range of threat factors, including DNS records, email headers, relationship statistics, email content, and even the presence of file types known to be transmission vectors for spear phishing attacks.

CLASSIFY

With millions of messages analyzed, GreatHorn can quickly and accurately separate noise from signal, flagging suspicious emails and threats based on an unmatched set of data points, ensuring that even the most sophisticated adversary cannot successfully deceive a user or gain access to data that should be protected.

RESPOND

Designed around realtime data classification and user awareness, GreatHorn provides immediate and effective remediation at the end-user level, supplemented by a world-class "single pane of glass" forensic dashboard that allows information security teams to set policy for how to automatically handle potential threats.

From content and compliance policies to behavioral analytics, this combination of response options ensures that your team can focus on what matters, without being distracted by noise and false positives.

ABOUT GREATHORN

GreatHorn is a cybersecurity startup based in Boston, Massachusetts, founded by a team of industry experts.

WHO WE ARE

Founded in 2015, GreatHorn is designed to be a new kind of security company, focused on the most insidious kinds of cyber-attacks: those that target end users directly, and rely on deceptive messaging and technical manipulation of communication systems to gain access to information, data, and credentials.

WHAT WE DO

Natively integrated into modern cloud communication systems, including Google Apps and Office 365, GreatHorn helps its customers detect and defend against data breaches by interrupting spear phishing, credential theft, and other trust-based attacks faster and more accurately than any other solution on the market.

Designed with security in mind, GreatHorn requires no rerouting of email or change in deliverability, instead using core APIs provided by the cloud platform providers themselves to detect, flag, and respond to threats in realtime.

With millions of messages processed each week, GreatHorn's threat intelligence and discovery is uniquely positioned to find even the most subtle attempts at intrusion, and customers can rest easy knowing that they benefit from this massive (and ever-growing) set of threat indicators.

OUR VISION IS TO USE TECHNOLOGY, DATA, AND INSIGHT TO STOP DATA BREACHES BEFORE THEY HAPPEN

Are you truly protected from modern attacks?

Most organizations simply are not ready to protect against the most common causes of data breaches: exploits that target their end users where they work, in email and via their cloud communication platforms.

GreatHorn can deploy in minutes, and effectively help detect and stop these sophisticated modern attacks before they result in breaches. Unlike training or simulation-based approaches, GreatHorn works automatically and in realtime, and can scale from 10-person startups to 10,000+ person enterprises.

Don't wait until you've been compromised -- contact us for a free assessment today.

GreatHorn Inc
116 Beech St, Belmont MA 02478
Phone: (800) 604-2566
info@greathorn.com
www.greathorn.com

GreatHorn