Email-based Threat Intelligence: To Catch a Phish

Version 1.5
Released: March 21, 2013

Securosis, L.L.C. 515 E. Carefree Highway Suite #766 Phoenix, AZ 85085 **T** 602-412-3051
info@securosis.com www.securosis.com

Author's Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Securosis blog, but has been enhanced, reviewed, and professionally edited.

Special thanks to Chris Pepper for editing and content support.

Licensed by Malcovery Security

Malcovery Security is the leading provider of actionable cyber security intelligence and forensic analysis, delivered through software and services that target cyber criminals and their activities. The company's patent-pending technology provides the ability to identify the 'root sources' of cybercrime attacks (servers, perpetrators, locations, etc.), delivering rich intelligence information about cross-brand attacks and targeted attacks, as well as advanced notification of emerging e-mail-based threats. Unlike services that serve as a response to these attacks today--services that simply address the symptoms, but cannot provide the intelligence to actually stop the cybercriminal -- Malcovery Security's solutions provide the unique intelligence required to respond effectively to attacks on customers' brands, to disrupt phishing activities and successfully prosecute cybercriminals.

Malcovery Security is based on technologies developed at the University of Alabama at Birmingham (UAB) The Center for Information Assurance and Joint Forensics Research (CIA|JFR) and is based in Pittsburgh, PA. and Birmingham, AL. For more information, please visit www.Malcovery.com or connect with Malcovery on Facebook (facebook.com/malcovery), Twitter (twitter.com/malcovery) and LinkedIn (http://www.linkedin.com/company/malcovery-security)

Copyright

Table of Contents

Industrial Phishing Tactics

Threat intelligence comes in many shapes and sizes, all of which are useful for Early Warning of imminent attack. After introducing the initial Early Warning concepts we explored how network telemetry and other information about your pipes can help to identify compromised devices in Network-based Threat Intelligence. We continue discussing all sorts of threat intelligence by focusing on phishing in Email-based Threat Intelligence.

But if you are targeted by phishing attacks you probably already know what we're talking about. Attackers target your brand, they stage high-volume attacks to steal personal information from customers, and then ultimately they monetize stolen personal data – typically by looting the accounts of your customers. All of which cost your organization big money.

So this paper will dig into the seedy underbelly of the phishing trade, starting with an explanation of how large-scale phishers operate. Then we will jump into threat intelligence on phishing – basically determining what kinds of trails phishers leave – which provides data to pump into the Early Warning system. Finally we will cover how to get Quick Wins with email-based threat intelligence. If you can stop an attack, go after the attackers, and ultimately disrupt attempts to steal personal data you will, right? We wrote this paper to show you how.

> Attackers target your brand, they stage high-volume attacks to steal personal information from customers, and then ultimately they monetize stolen personal data – typically by looting the accounts of your customers. All of which cost your organization big money.

Sizing up Targets

Why do phishers target specific brands? *To harvest and monetize personal information.* Obviously targeting financial institutions is a no-brainer. So you probably see phishing attempts targeting every major bank, brokerage, and other financial institution like PayPal fly into your inbox all the time. Retailers are also low-hanging fruit – once phishers gain access to an online shopping account they can buy all sorts of stuff using customers' credit. And your organization is left holding the bag. Fun!

Lately we have been seeing phishing attempts target other major consumer brands such as shipping companies, phone companies, and airlines. Why, especially given the success of targeting the financials over and over again? What exactly is the risk of 'stealing' a frequent flyer account? Seeing how close the flyer is to the next upgrade, right? Not exactly. It's about getting presence on a device, however possible. When a user (who may work for your organization) clicks a phish, they may enter account information into the phishing site — this account credential is the attacker's first loot. Especially when attackers attempt to use stolen credentials on other sites, knowing many consumers use the same credentials on multiple sites.

But that's not the only opportunity for pwnage. Attackers also systematically install malware on the device, and that's where the real monetization happens. Once they have a foothold they mine personal data from the victim as long as they can. Attackers collect bank accounts, credit card numbers, passwords, and other sensitive information. So the non-financial brands become a means to an end to steal financial account data.

So basically every large consumer brand has been and will continue to be a serious phishing target. These companies have millions of customers, which means millions of devices for attackers to mine and monetize. Obviously the highest value phishing attacks target financials, where the victim can be monetized immediately. But the endgame is installing malware, which is why we increasingly see secondary brands emerge as phishing targets.

It is outside of the scope of this research, but we would be negligent if we didn't at least mention that it's a very bad idea to save financial information in the website of any retailer or other services company. Sure, one-click buying is convenient, as is not entering that pesky credit card number with every purchase. But it also leaves you at the mercy of the website's security – not a good place to be. If you do need to save personal information on these sites, at least use very strong unique passwords with a password manager, as Rich has described numerous times in places like MacWorld.

> Why do many phishing campaigns target only a few popular brands? Is this just Pareto at work? The real reason is the phishing kit, which offer a packaged phishing campaign for a very modest price.

The Phish

Phishing is the front end of a multi-faceted attack, so let's take a look at the first set of steps in Cloppert's Kill Chain to show how it applies to phishing. First let's look at reconnaissance, which starts with picking the brand to target, typically a financial or payment company. APWG statistics (PDF) show that upwards of 65% of phishing targets are financial and payment organizations. Duh. But let's be clear about why many phishing campaigns target only a few popular brands. Is this just Pareto at work? The real reason is the advent of the phishing kit. Just like malware kits, phishing kits offer a packaged phishing campaign for a very modest price. This takes care of the weaponization step in the kill chain – these kits include everything you need to go phishing, with the exception of domains to host the phishing site. Images, emails, designs, and even a few malware variants are included, which is driving down the average IQ of phishers.

You might think phishing kits need to be constantly updated to keep pace with the constant web site changes undertaken by major consumer brands. Not so much – most consumer victims wouldn't be able to tell a vintage 2009 Wells Fargo site from the latest and greatest. The images and code used on the phishing site tell a story about the attacker and can provide significant intelligence to disrupt the attack, so we will delve into that later in the paper.

The other key link in the phishing kill chain is delivery. The primary delivery mechanism for phishing is email, which requires attackers to evade spam filters. Without going into the details, we know the attackers are rather sophisticated in how they test both delivery of email and the domain names they drive victims to. Similarly to the way attackers use VirusTotal and other AV test harnesses, phishing professionals focus quite a bit of effort on testing against common anti-spam engines, because increasing their successful delivery rate has a dramatic impact on profitability. At the end of the day phishing, like all email attacks, remains a numbers game.

But email isn't the only delivery vehicle for phishing attacks. Increasingly we see social networks used to deliver links to phishing sites. This gets even trickier in constrained environments like Twitter with built-in link shorteners, because opaque shortened links can easily lead to phishing sites.

> Increasingly we see social networks used to deliver links to phishing sites. This gets even trickier due to built-in link shorteners, because opaque shortened links can easily lead to phishing sites.

Monetizing the Phish

Once the phishing email is delivered and the victim clicks the link, the fun begins. The first information capture point is authentication to the phishing website which impersonates the target site. This sets the stage for the initial monetization, using captured credentials to loot the victim's account if it's a financial or payment site. Backend processes launder the stolen money. But the attack cycle doesn't end there. Attackers want to maintain a presence on compromised machines and to steal every credential they can. They have a few tactics for that:

- **MITM:** Many phishing sites are really just proxies, running a man-in-the-middle (MITM) attack. They capture authentication credentials and pass them through to the real site to maintain their camouflage. The victim sees the web site they expect, but all their traffic is routed through the attacker's network. Attackers can sniff all network traffic for authentication credentials and other interesting data to steal. Even better, the malware downloaded once the victim hits the phishing site will permanently redirect traffic back to the attacker so they can see everything the victim does.

- **Key logging:** The attacker may also install a key logger on the victim's device to capture all their keystrokes. Keystroke data is handy for harvesting account credentials as the victim goes about their business. This is handled by the malware installed on the victim's device during the initial drive-by click.

Besides monetizing the victim's account credentials, many phishers get 'commissions' from bot networks for installing malware kits and adding devices to botnets.

- **Screen grabbing:** Finally, the malware may also take screen captures at certain times, such as when hitting Submit on banking or payment sites. Again, this allows them to capture account information, balances, etc. to help determine where efforts are best spent. They don't want to go through the hassle to access an empty bank account.

Besides monetizing the victim's account credentials, many phishers get 'commissions' from bot networks for installing malware kits and adding devices to botnets. We have recently seen phishing attacks install multiple malware packages on a victim device to double or triple the value of a compromised device. That's free enterprise at work, folks. But it's not really free — not to your organization anyway — so let's delve into costs to the business.

Cost of Phishing to Your Organization

Phishing is predominately a consumer attack, so many companies don't feel a compelling need to deal with it, especially given the kinds of direct attacks most organizations deal with. But there are clear costs of phishing to an enterprise, so let's break them down.

- **Financial loss:** The most obvious are direct losses due to account compromise. These are most obviously and easily quantified by financials and payment brands (which is why they are targeted by a majority of phishing attacks) but other consumer brands are not immune. For example, retailers may ship fraudulently purchased goods and be unable to collect payment or recover the goods.

- **Clean-up costs:** There are costs involved in taking down phishing sites or cleaning customer devices compromised by clicking messages they thought came from you. There is likely no legal requirement to help these customers clean their devices, but alienating customers is not good for customer satisfaction — especially in highly competitive industries such as banking, retail, and telecommunications.

- **Brand damage:** Damage to an organization's brand is very difficult to quantify. When a customer has a problem they often blame the phishing impersonated brand, whether they deserve it or not. Obviously the bigger the brand footprint, the more frequently targeted, the more compromised customers, and so the greater the brand damage from phishing. The data is generally inconclusive but there are clear costs resulting from brand tarnish, particularly in highly competitive industries.

Phishing remains a huge problem, with which the broader technology ecosystem continues to struggle. The bar for successfully waging a phishing attack continues to descend with more sophisticated phishing kits, and increasingly advanced malware allows attackers to monetize victims over and over again. The question is: how can you gather information to more effectively defend yourself against phishing?

Analyzing the Phish Food Chain

Phishing attacks are designed to get victims to click something, then to steal the victim's account credentials and download malware onto their device. Of course phishing, like every other attack, leaves a trail. Following it can help you prioritize remediation activities, identify adversaries, and ultimately take action to protect your environment and customers. But first you must be able to analyze the email to identify the patterns to look for. And that requires a lot of email – a whole lot.

Sampling All the Phish in the Sea

Email-based threat intelligence entails analyzing scads of spam email using Big Data Analytics. You didn't think we'd be able to resist that buzzword, did you? Of course not! But whether you call it big data or just "a lot of data", the first step in implementing an email-based threat intelligence program is to aggregate as much email as you can. Which raises a reasonable question: where can you get that kind of email? If you are a private enterprise it can be hard. There are various spam archives available on the Internet (Google is your friend), but not many fresh ones.

> First you must be able to analyze the email to identify the patterns to look for. And that requires a lot of email – a whole lot.

Alternatively you could establish partnerships with email service providers, who tend to have millions of blocked emails from internal spam filters lying around. Another source would be other consumer brands – perhaps some of them would be willing to swap. You give them a copy of your spam mailbox in exchange for theirs. Besides email addresses there isn't likely to be sensitive data in obvious spam, so this shouldn't trip the general security aversion to sharing data.

But you will likely need an intelligence feed from a third-party analysis provider. As discussed in both the Early Warning System and Network-based Threat Intelligence (NBTI) research, we see a market emerging for intelligence providers specializing in aggregating and analyzing these data sources to provide better security intelligence as a stand-alone offering. These companies provide intelligence that can be used by enterprises to shorten the window between attack and detection.

Let's dig into the kinds of intelligence we look for in phishing emails, going back to the metaphor we introduced in the NBTI paper: the Who, What, Where, and When of phishing.

A select few highly effective phishers (hundreds, not thousands) are behind many of the attacks we see in the wild. So the ability to identify the authors of attacks can yield all sorts of information, enabling you to profile and analyze your adversaries.

Who?

'Who' is behind phishing is probably the most important intelligence you can develop. A select few highly effective phishers (hundreds, not thousands) are behind many of the attacks we see in the wild. So the ability to identify the authors of attacks can yield all sorts of information, enabling you to profile and analyze your adversaries. Why is adversary analysis important?

- **Motive:** Is the phish part of a targeted attack (spear phishing)? Is it part of a widespread attack on a financial institution to harvest account information? Is it designed to steal intellectual property? Knowing your adversary allows you to determine his or her motives, and thus to more effectively judge the true threat of the attack to your organization.
- **Tactics:** Does this phisher use malware extensively? Do they just harvest account information? Is key logging their main technique? Understanding and profiling the adversary can indicate which controls to implement to ensure protection. Keep in mind that the ultimate target of the phishing attack is usually customers rather than employees. This helps you decide whether helping customers protect themselves is a worthwhile expense.
- **Capabilities:** Finally, isolating your adversary and tracking them over time (as discussed below) provides clues to their capabilities. Do they rely purely on commercial phishing kits? Are they able to package 0-day attacks? Is it something in the middle? The more you know about your attackers the better you can respond.

The ultimate objective of adversary analysis is to more effectively prioritize remediation activities. Knowing who you are dealing with and what they are capable of is key, and can help you determine the urgency of response.

What?

So how can you find a specific attacker within a corpus of tens of millions of spam and phishing messages? It all comes back to profiles. The links embedded in the phishing messages indicate the locations of phishing sites, and you will see patterns in the domains and IP addresses used in attacks. Working backwards you can analyze the phishing site to determine the attack(s) in use, the tactics and capabilities used, and if you get lucky perhaps the attacker's identity. This next level of analysis involves looking at 'what' the attack does.

A key development that made phishing far more accessible to unsophisticated attackers was the emergence of phishing attack kits. These kits provide everything an attacker needs to launch a phishing campaign – including images, email copy, and specific tactics for capturing account credentials. Of course phishing messages still need to evade an organization's spam filters, but that tends to be reasonably straightforward given that phishing messages should look *exactly* like legitimate messages. That takes most of the sophisticated content analysis done by anti-spam filters out of play.

But these kits leave a trail in HTML, images, malware packages, installers, etc. downloaded and used to install the kit on a compromised device. If you get an actual phishing kit you can analyze it just like any other malware (as discussed *ad nauseum* in Malware Analysis Quant) for clues to the malware used and what is ultimately done with stolen account credentials – all of which can help identify the attacker.

Even better, profiling attack kits enables you to look for similar attack profiles to identify the attacker more quickly next time. Given a sufficient corpus of spam and phishing messages, you can mine the data for patterns of IP addresses and domains to help identify the adversary and assist in selection of appropriate remediations.

Where?

As described above, phishing messages look like legitimate email, which gets them past much of the content analysis used by anti-spam filters. But you can (and need to) analyze email headers to figure out where the messages come from, the path they take to your gateway, and clues in links to phishing sites. That brings us to the 'where' the victim is directed once they take the bait and click a phishing link.

> But you can (and need to) analyze email headers to figure out where the messages come from, the path they take to your gateway, and clues in links to phishing sites.

The 'location' of a web site is an IP address and normally a domain name; both are important when analyzing phishing messages. Phishers leverage compromised sites as phishing and malware distribution locations, so it is common to see multiple phishing sites on the same (usually shared hosting) server with a single IP address. The value and urgency of taking down and analyzing sites which host multiple phishing sites are particularly high.

Likewise, domain name structure can yield useful information on domain generation algorithms and other mechanisms attackers use to obfuscate phishing domains to make them look legitimate. Again, this kind of intelligence enables you to identify useful patterns as you watch for and block new sites using similar domain names. We will discuss how to leverage this information next under Quick Wins.

We should also mention the pros and cons of reputation in the battle to identify phishing email. Of course with sufficient data, phishing IP addresses and domains can be assigned negative reputation and be blocked by anti-spam and web filters. But many phishing sites appear on recently compromised servers, using clean domain names and IP addresses with good reputations. Over time reputation is invaluable for disrupting attacks, but its value is minimal during the first wave.

Historical context is not something a tool can provide in an automated fashion. You need HUMINT (human intelligence) for that.

When?

You can examine the history of pretty much any aspect of a phishing message you're evaluating – including the phishing kit, IP addresses, domains, and specific attackers. History can show you how tactics have changed and inform guesses about what will happen next. As we discussed in the Early Warning research, this historical context is not something a tool can provide in an automated fashion. You need HUMINT (human intelligence) for that. But understanding your adversaries can help you more effectively plan defenses and responses.

Keep in mind that the velocity of phishing attacks continues to increase while the life span of individual attacks declines. With better and more sophisticated phishing kits we see more attacks launched at common brands; and given the attackers' need to stay one step ahead, sites are mined and abandoned more quickly. With a phishing site up for a matter of hours rather than days, sometimes historical information is all you will have because the attacker moves on before you have enough information for a full analysis.

Quick Wins with EBTI

We are big on Quick Wins at Securosis. Mostly because we know how hard it is to justify new technology (or processes or people), and that if you can't show value quickly on a new project, every subsequent request gets harder and harder to push through. Until you have a breach, that is. Then your successor gets *carte blanche* for a honeymoon period to do the stuff you were trying to do all along.

Disrupting a phishing attack is an application of simple economics. If it costs more for attackers to phish your brand, their margins will decline and eventually they will switch to more profitable attacks on alternative targets. So for Quick Wins focus on making phishing campaigns more expensive. That means messing with their sites, helping customers protect themselves effectively, and ultimately shortening the window attackers have to monetize your customers.

> Disrupting a phishing attack is an application of simple economics. If it costs more for attackers to phish your brand, their margins will decline and eventually they will switch to more profitable attacks on alternative targets.

Your quiver is filled with the key intelligence sources we discussed above, so what comes next? How can you use information like phisher email addresses, IPs, and domains to disrupt and/or stop attacks on your brand?

Taking the Phish out of the Pool

The first and most common remediation remains the phishing site takedown. A phishing attack is stopped in its tracks if the evil site is not available to harvest account credentials and/or deliver malware. But this is not an immediate fix – it takes time to prepare the documentation that ISPs, domain registrars, domain owners, browser vendors, telecom providers, and other organizations need to take sites offline. Many phishing sites are hosted on legitimate (albeit compromised) web sites, so takedowns inflict collateral damage on legitimate sites as well. We are not in the excuses business so we don't feel too bad when a compromised site is taken down until fixed, but keep in mind that the cost isn't only to the phisher.

One of the keys to dealing with advanced malware is determining when it makes more sense to observe the attacker to gain intelligence about tactics, objectives, etc., than to remediate the device immediately. Phishing sites demand a similar decision. If you have identified the phisher as a frequent attacker, does it make more sense to observe traffic from that specific attacker? Or to monitor attack kits and analyze malware downloaded to compromised devices? The answer varies, but this kind of analysis requires sophisticated incident response and malware analysis capabilities.

> If you have identified the phisher as a frequent attacker, does it make more sense to observe and analyze traffic? This kind of analysis requires sophisticated incident response and malware analysis capabilities.

A few other tactics can be helpful in disrupting phishing attacks, including directly notifying browser vendors of malicious sites because all major browsers now include real-time checks for phishing and other malware sites, and warn users attempting to visit compromised sites. Similarly, communicating with the major security vendors and submitting IP addresses and domains to their security and threat research teams can give these sites and IPs negative reputations, blocking them within web and email security gateways.

If you have been able to identify the email address a phisher uses to harvest account credentials, you can work with their service provider (typically a major consumer email provider such as Google, Yahoo!, or Microsoft) to restrict access to the account. Or work with law enforcement to track the attacker's identity as they access it to collect their spoils. All these tactics make it harder for phishers to lure victims to their phishing sites, steal information, and then harvest it.

Speaking of law enforcement, much of the information you need to facilitate phishing site takedowns — such as IP addresses, domains, email addresses, and phishing kit specifics — is directly useful for law enforcement's ultimate efforts to prosecute the phishers. Prosecution is rarely job #1, especially because many attackers reside in places where prosecution is problematic, but if you need to gather the data anyway you might as well let law enforcement run with it.

Other Tactics for Disrupting Phishing

Taking down the phishing site isn't your only means of disrupting attacks. You may also be able to use active controls already in place in your environment to minimize the damage caused by the attack. Let's start with the network: your intelligence efforts yield a number of data points, such as IP addresses and domains associated with an attack. Depending on the attack, you may be able to work with your network operations

> Depending on the attack, you may be able to work with your network operations team to block devices connecting to your site from these phishing IPs or domains.

team to block devices connecting to your site from these phishing IPs or domains. You could use referrer information to determine how the customer got to your site. At a minimum, you should be able to tag these devices and monitor their transactions for suspicious activity. When dealing with fraud against millions of customers, being able to focus your efforts on accounts more likely to be compromised really helps.

Another tactic is to adaptively require stronger authentication for accounts exhibiting suspicious activity. Financially motivated phishers collect account numbers and passwords, rarely worrying about security questions or additional authentication factors. So if you see a login attempt from a suspicious IP address or domain you can further challenge the user attempting to login by requiring additional authentication details. Attackers generally go after the easiest targets, so this is a great way to make attacks against you more expensive and is likely to drive phishers elsewhere.

Finally, you can work harder to stop the original phishing emails from reaching your customer's inboxes in the first place. Leverage new standards like DMARC, which enables service providers and other large-scale senders to collaborate and leverage DKIM and/or SPF message authentication technologies to provide more accurate sender authentication. Combined with traditional anti-spam analysis techniques, these technologies can minimize false positives and ensure phishing messages are tossed before customers get an opportunity to hurt themselves.

Addressing the Weakest Link

> But it may also make sense to try reducing the likelihood of compromise at the point of attack: your customer.

Ultimately, much of what you can do to disrupt phishing is reactive. But it may also make sense to try reducing the likelihood of compromise at the point of attack: *your customer*. You can start with security education, working to help customers identify phishing domains and recognize the security mechanisms consumer brands apply to email they send customers. We are painfully familiar with the frustration of security awareness training but this is another case of economics. If training your customers can demonstrably reduce fraud and/or brand damage, these programs are worth considering.

Likewise many organizations, especially in the financial sector, take an even more active approach by offering endpoint protection technology to customers for free. Preventing customers from being compromised in the first place breaks the attack cycle. Of course you need to make sure the technology is effective at blocking the typical advanced malware seen today, but some organizations have done the math and determined that providing effective endpoint protection is a much better deal than constantly cleaning up the messes of customers who clicked phishing links and logged into fake sites.

Finally, if you have isolated a particular web site being used in several phishing attacks against your customers, it may make sense to approach the company or webmaster directly to help fix their site.

This is a thankless job, but your alternative is to take down the site, then wait for it to come back up and be compromised again. If you have had to take action against a site more than once the problem is unlikely to get better on its own, so you should consider intervening.

Making the Commitment

A Quick Win is key to disrupting imminent phishing attacks and showing value from your email-based threat intelligence program. But truly stopping phishing attacks against your environment involves making an ongoing commitment to tracking phishing sites, identifies the attackers, IP addresses, domains, and attack kits, as well as prioritizing the attacks based on the risk to your environment — or buying a service that provides similar information. While a live phishing site captures your customer's credentials the clock starts ticking until you can get the site taken down and the risk mitigated. Understanding your adversaries and their tactics, and gathering applicable data, enables you to pinpoint phishing attacks and determine the most effective remediation approach faster. And every minute counts during a phishing attack.

> Making an ongoing commitment to tracking phishing sites, identifying attackers, as well as prioritizing the attacks based on the risk to your environment — or buying a service that tracks similar information — is the only real way to react faster to phishing attacks.

If you have any questions on this topic, or want to discuss your situation specifically, feel free to send us a note at info@securosis.com or ask via the Securosis Nexus (http://nexus.securosis.com/).

About the Analyst

Mike Rothman, Analyst/President

Mike's bold perspectives and irreverent style are invaluable as companies determine effective strategies to grapple with the dynamic security threatscape. Mike specializes in the sexy aspects of security — such as protecting networks and endpoints, security management, and compliance. Mike is one of the most sought-after speakers and commentators in the security business, and brings a deep background in information security. After 20 years in and around security, he's one of the guys who "knows where the bodies are buried" in the space.

Starting his career as a programmer and networking consultant, Mike joined META Group in 1993 and spearheaded META's initial foray into information security research. Mike left META in 1998 to found SHYM Technology, a pioneer in the PKI software market, and then held executive roles at CipherTrust and TruSecure. After getting fed up with vendor life, Mike started Security Incite in 2006 to provide a voice of reason in an over-hyped yet underwhelming security industry. After taking a short detour as Senior VP, Strategy at eIQnetworks to chase shiny objects in security and compliance management, Mike joined Securosis with a rejuvenated cynicism about the state of security and what it takes to survive as a security professional.

Mike published The Pragmatic CSO <http://www.pragmaticcso.com/> in 2007 to introduce technically oriented security professionals to the nuances of what is required to be a senior security professional. He also possesses a very expensive engineering degree in Operations Research and Industrial Engineering from Cornell University. His folks are overjoyed that he uses literally zero percent of his education on a daily basis. He can be reached at mrothman (at) securosis (dot) com.

About Securosis

Securosis, LLC is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services. Our services include:

- **The Securosis Nexus**: The Securosis Nexus is an online environment to help you get your job done better and faster. It provides pragmatic research on security topics that tells you exactly what you need to know, backed with industry-leading expert advice to answer your questions. The Nexus was designed to be fast and easy to use, and to get you the information you need as quickly as possible. Access it at <https://nexus.securosis.com/>.

- **Primary research publishing**: We currently release the vast majority of our research for free through our blog, and archive it in our Research Library. Most of these research documents can be sponsored for distribution on an annual basis. All published materials and presentations meet our strict objectivity requirements and conform to our Totally Transparent Research policy.

- **Research products and strategic advisory services for end users**: Securosis will be introducing a line of research products and inquiry-based subscription services designed to assist end user organizations in accelerating project and program success. Additional advisory projects are also available, including product selection assistance, technology and architecture strategy, education, security management evaluations, and risk assessment.

- **Retainer services for vendors**: Although we will accept briefings from anyone, some vendors opt for a tighter, ongoing relationship. We offer a number of flexible retainer packages. Services available as part of a retainer package include market and product analysis and strategy, technology guidance, product evaluation, and merger and acquisition assessment. Even with paid clients, we maintain our strict objectivity and confidentiality requirements. More information on our retainer services (PDF) is available.

- **External speaking and editorial**: Securosis analysts frequently speak at industry events, give online presentations, and write and/or speak for a variety of publications and media.

- **Other expert services**: Securosis analysts are available for other services as well, including Strategic Advisory Days, Strategy Consulting engagements, and Investor Services. These tend to be customized to meet a client's particular requirements.

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.

Additionally, Securosis partners with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis. For more information about Securosis, visit our website: <http://securosis.com/>.