WHITE PAPER

How Cybercriminals Make Money With Your Email

An Osterman Research White Paper

Published July 2013

SPONSORED BY

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

Cybercriminals make enormous amounts of money by exploiting weak defenses in corporate and personal email defenses, deficiencies in corporate policies focused on protecting email users and user ignorance. Criminals are aided in their efforts by three key trends that are becoming increasingly prevalent:

- Criminals are able to develop highly sophisticated malware because they are well funded, often supported directly by organized criminal groups.
- Many users share large amounts of information through social media and other venues that enable criminals to obtain useful information about their potential victims that can be used to develop sophisticated spearphishing attacks.
- There are a growing number of devices and access points from which users access email, making it more difficult for organizations to defend against email-borne threats and that make it easier for criminals to exploit weak defenses on a number of levels.

KEY TAKEAWAYS

- Email-delivered malware, as well as the total volume of new malware, are increasing at a rapid pace.
- Cybercriminals use a variety of techniques, including spearphishing, shortened URLs, advanced persistent threats, traditional phishing, man-in-the-middle attacks, spam, botnets, ransomware, scareware and other techniques to defeat corporate defenses. Scareware is often delivered as a pop-up message, but sometimes is delivered via spam messages in email[i].
- The financial and auxiliary consequences of cybercrime can be enormous and can be multi-faceted: direct costs of remediating the cybercriminal activity, lost business opportunities, a damaged corporate reputation and the like.
- Cybercrime is a business – albeit a nefarious one – that is driven by fairly traditional business decision-making. The goal of any email defense solution, therefore, is to make continued attacks against an organization unprofitable so that cybercrime activity is reduced.
- To minimize the impact and effectiveness of cybercriminal activity, an organization should undertake an ongoing program of user education, as well as deploy appropriate technologies designed to address new cybercriminal techniques.

ABOUT THIS WHITE PAPER

This white paper focuses on key issues that organizations should address in the context of cybercrime delivered through email, and it offers some practical advice on what organizations should do to protect themselves. It also offers a brief overview of McAfee, the sponsor of this white paper, and its relevant solutions.

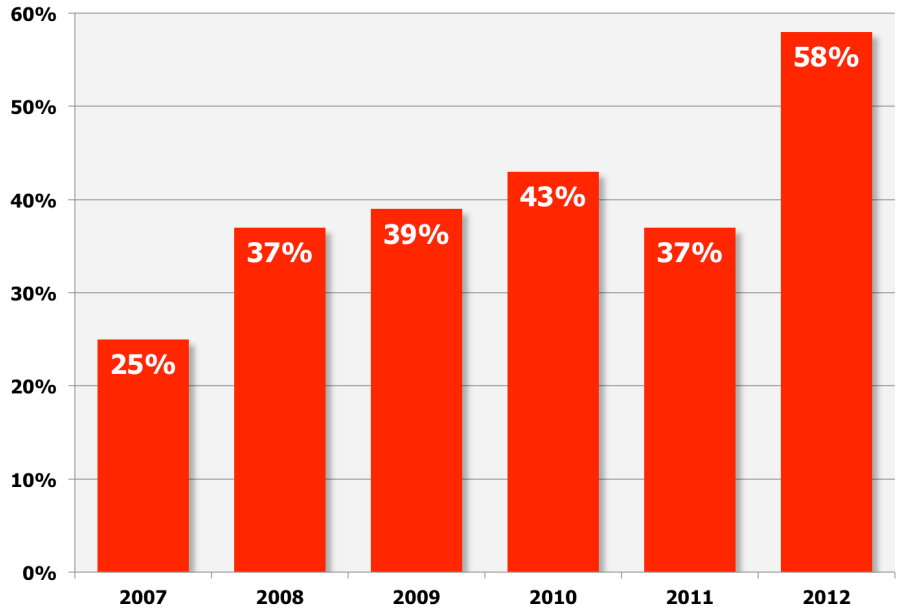
Cybercrime is a business – albeit a nefarious one – that is driven by fairly traditional business decision-making.

WHAT DO CYBERCRIMINALS DO?

THE PROBLEM IS GETTING WORSE

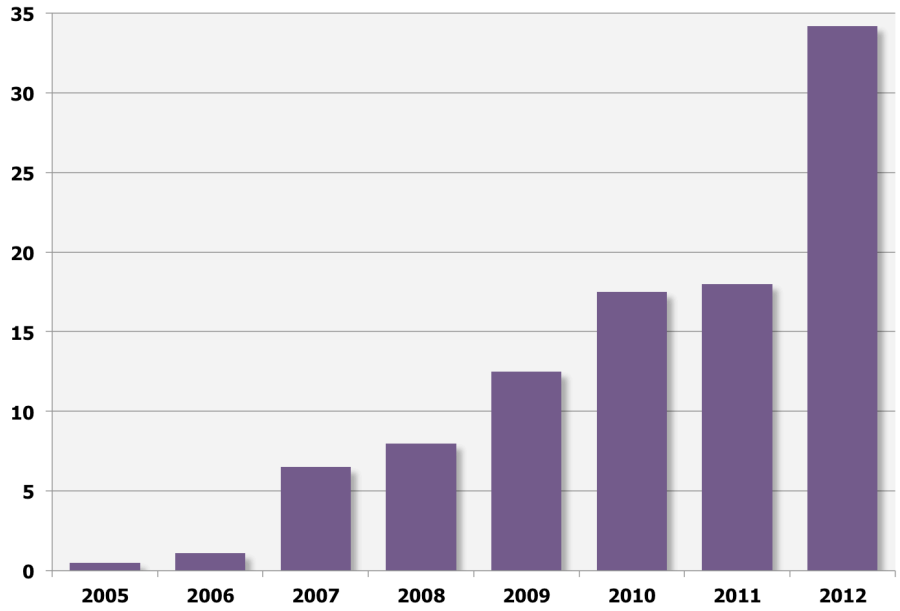
Cybercriminals use a number of methods to deliver email-based threats to their victims and they do so quite successfully, as evidenced by the following figure that demonstrates the large proportion of mid-sized and large organizations in North America that have been the victims of email and Web-based threats during the previous 12 months. Illustrating the seriousness of the malware problem itself, the next figure shows the rapid increase in new malware over the past few years.

Percentage of Organizations Infiltrated by Email-Based Malware
2007-2012



Source: Osterman Research, Inc. surveys of mid-sized and large organizations

New Malware Detected (millions of malware programs detected)
2005-2012



Source: AV Test (http://www.av-test.org/en/statistics/malware/)

It's important to note that while we saw something of a hiatus in the infection growth rate from email-based malware during 2011, as well as a flattening in the amount of new malware detected, this may have been due to the March 2011 takedown of the Rustock botnet – a key delivery path for spam and malware – that had infected more than 800,000 Windows-based computers[ii].

58% of organizations were infiltrated by email-based malware in 2012.

METHODS USED BY CYBERCRIMINALS

Among the many methods used by cybercriminals are:

- **Spearphishing**
  Spearphishing is a more focused variant of phishing in which a single individual or a small group of individuals within a firm are targeted by cybercriminals. Quite often, a company's CFO or CEO will be targeted because they are likely to have access to a company's financial accounts. A common method for gaining access to this information is through delivery of a highly targeted email that will contain an attachment or a link, clicking on which will infect the victim's PC with a Trojan that can then be used to harvest login credentials to a bank account. Smaller companies, churches, school districts and similar types of small to mid-sized organizations are among the more common targets of spearphishing attacks because they often lack sophisticated defenses that can protect against these types of attacks.

  Spearphishing has been aided to a great extent by social media, since cybercriminals can use content posted to Facebook, Twitter or other social media sites to improve the likelihood of delivering their content. For example, a CFO that posts to Facebook information about their recent online purchase of a new Lytro camera will be very likely to open a malicious email with the subject line "Problem with your Lytro camera order" and to click on any links contained therein.

  One spearphishing attack may have derailed Coca Cola's $2.4 billion acquisition of China Huiyuan Juice Group. Coca Cola's Pacific Group deputy president received an email from what he thought was the company's CEO, but in reality the email was from a (probably) Chinese firm known as the Comment Group. The email contained malware that allowed the perpetrator to access sensitive content for more than 30 days. Shortly thereafter, the Chinese government blocked the acquisition because of concerns over competition in the beverage industry.[iii]

- **Short URLs**
  Shortened URLs – that might appear in emails, Tweets, etc. – are commonly used to bring unsuspecting victims to malicious sites with the hope of infecting their device with malware. The attraction of a short URL for potential victims is that they fit nicely in character-limited tools like Twitter, and they can also condense very long links into a short URL when used in non-HTML emails. More importantly for cybercriminals, they mask the identity of the malicious site, hiding it from both individuals who might be suspect when reviewing the URL, as well as automated systems.

- **Advanced Persistent Threats**
  Advanced Persistent Threats (APTs) are protracted attacks against a government, company or some other entity by cybercriminals. Underscoring the seriousness of APTs is the fact that these threats are generally directed by human agents (as opposed to botnets) that are intent on penetrating corporate or other defenses, not simply random or automated threats that are looking for targets of opportunity. As a result, those responsible for APTs will change tactics as they encounter resistance to their attacks by their targets, such as the deployment of new defense mechanisms.

- **Phishing**
  A phishing attack is a campaign by a cybercriminal designed to penetrate anti-spam and/or anti-malware defenses. The goals of such an attack can include infection of users' PCs for the purpose of stealing login credentials, to gain access to corporate financial accounts, to steal intellectual property, to search through an organization's content, or simply to gain access for a purpose to be determined at a later date. Email is a useful threat vector for phishing attacks and can be quite successful for cybercriminals. For example, a common phishing

Spearphishing has been aided to a great extent by social media, since cyber-criminals can use content posted to Facebook, Twitter or other social media sites to improve the deliverability of their content.

scheme is to send an email citing UPS' inability to deliver a package and a request for a user to click on a link to print an invoice.

THE EASE OF GATHERING INFORMATION THROUGH SOCIAL MEDIA

To see how much information we could gather on a senior executive, in late February 2013 Osterman Research chose a company at random in Kent, Washington after doing a quick Google search for companies in the area.

Our researcher then visited this company's Web site, found an owner listed, and then did a search for his name on Facebook. Although Osterman Research has no relationship with this individual, a quick look at his wall revealed his former employers, where he went to high school, the fact that he is also a realtor, where he had lunch last Friday, his phone number, information about his Washington State Ferry ride on the previous Tuesday, information about an upcoming company event in early March 2013, the names of two people who gave him gifts in late January 2013, and what he had for dessert on January 13, 2013.

A cybercriminal could have used any of this information to craft a spearphishing email with a subject line that would likely have attracted his attention and made it more likely for him to click on a link to a malware site that might have infected his PC.

- **Man-in-the-Middle Attacks**
  A man-in-the-middle attack is one in which a third party intercepts messages between two parties when both parties are attempting to exchange public keys. In essence, the third party impersonates itself as both recipient and sender, so that the two legitimate recipients and senders think they are communicating with each other, when in fact each is communicating directly with the unauthorized third party. The result of a man-in-the-middle attack can be relatively innocuous, with the third party simply listening in on a conversation; or it can be more malicious and result in the loss of network credentials or sensitive information.

- **Spam**
  While in some ways spam is less of a problem today than it was before the successful takedown of various botnets at the end of 2010 and early 2011, it remains a serious and vexing problem for organizations of all sizes. Spam consumes storage and bandwidth on corporate servers, users must scan spam quarantines to ensure that valid messages have not been misidentified and placed into the quarantine, and malicious content can mistakenly be withdrawn from a spam quarantine, thereby increasing the potential for infecting one or more PCs on the corporate network.

  Spam filters can often be defeated by simple text obfuscation like the misspelling of particular words, Bayesian poisoning, the introduction of valid text into spam messages to make them look legitimate, use of various HTML techniques to trick spam filters, use of various languages, etc. Spam filters that use less sophisticated filtering techniques and Bayesian approaches to filtering can be fooled by these tactics.

  Spam that contains attachments used to be quite common as means of delivering malware. While not as common today, spam with malicious attachments still finds its way into many organizations. PDF files, images, calendar invitations, spreadsheets and zip files are all used as payloads to carry malicious content.

While not as common today, spam with malicious attachments still finds its way into many organ-izations.

- **Botnets**
  Cybercriminals often use botnets that consist of tens of thousands of 'zombie' devices – personal and workplace devices that are infected with a virus, worm or Trojan that permit them to be controlled by a remote entity. Spammers can rent botnets for distribution of their content, typically at relatively modest rates. By using botnets, cybercriminals can send a small number of messages from each of thousands of computers, effectively hiding each sending source from detection by ISPs or network administrators using traditional detection tools. Botnets are a serious problem not only because they are responsible for a large proportion of spam sent today, but also because they are used for a range of purposes beyond simple spam delivery: perpetrating distributed denial-of-service attacks, click fraud and credit card fraud. Botnets are successful because they can be difficult to detect and to take down.

- **Ransomware**
  Ransomware is a type of cybercriminal attack, most often introduced to a PC by an email-delivered or other worm, in which a user's PC is locked or its files encrypted until a "ransom" is paid to a cybercriminal. For example, one variant of ransomware, Reveton, is a drive-by virus that displays a message informing victims that they have downloaded child pornography or pirated material, demanding payment of a fine to restore access to their PC. During two days in May 2012, victims paid a total of more than $88,000 to cybercriminals to restore access to their PC.

- **Scareware**
  Scareware is a less invasive form of ransomware in that it warns users that their PC is infected with malware, often reporting the discovery of thousands of different instances of malware. It then offers to disinfect the computer by offering anti-virus software for a nominal fee. While the fee is typically on the order of $40 – albeit for software that does nothing – the real damage often results from providing cybercriminals with a valid credit card number and CVV code. Scareware is often delivered as a pop-up message, but sometimes is delivered via spam messages in email[iv].

- **State-sponsored malware**
  One example of state-sponsored malware is Stuxnet. This malware was designed to target a particular type of Siemens controller used in Iran's uranium enrichment plant at Natanz, Iran and was set to expire in June 2012 (although the malware propagated globally before its expiration date). While the malware was not designed to attack companies or consumers, it was a good example of how malware can be designed to go after a specific type of target and remain undetected by its victim.

Ransomware is a type of cyber-criminal attack, most often introduced to a PC by an email-delivered or other worm, in which a user's PC is locked or its files encrypted until a "ransom" is paid to a cyber-criminal.

BENEFITS REALIZED BY CYBERCRIMINALS

First and foremost, it is essential to understand that cybercrime is a business – an illegitimate one to be sure – but one that is guided by fundamental business principles focused on the benefits to be gained from a particular activity, return-on-investment considerations, investments in research and development, and the like.

The benefits to cybercriminals from their activities are substantial. For example, cybercriminals that use phishing, spearphishing or other techniques can steal enormous amounts of money in a short period of time, as discussed below. Cybercriminals can also gain access to confidential information, intellectual property, Protected Health Information, or other information that might prove valuable at present or at a future date.

THE CONSEQUENCES TO BUSINESS AND GOVERNMENT

The flip side of the benefit to cybercriminals is the pain experienced by their victims. Aside from the direct financial losses that can result, an organization that falls victim to email-based or other types of cybercrime can suffer a loss of reputation as news of the problem is reported in the press or among their customer base. Some customers may cancel orders or switch to a different supplier if they determine they can no longer trust the victims of cybercrime to safeguard their own data and, by extension, the data provided to them by their customers or business partners. The negative publicity alone can actually be worse than the loss of funds.

DATA BREACHES

Among the more serious and expensive consequences of email-based or other cybercrime is the breach of customer data. Because 46 of the 50 US states, one Canadian province and many countries around the world have data breach notification laws in place, organizations that are victims of cybercrime and a resulting data breach are liable for notifying the affected parties about the breach. Aside from the direct cost of notifying customers about the breach is the potentially much higher cost of losing customers who are upset about the loss of their data, paying for credit reporting services for customers as a means of ameliorating their concerns, and the negative publicity that can result.

Underscoring the seriousness of data breaches is the sheer magnitude of the problem. For example, the Privacy Rights Clearinghouse maintains a database of data breaches dating back to 2005. Since they have been keeping records, there have been 3,680 data breaches made public as of mid-April 2013 resulting in the breach of 607.5 million records. Among the data breaches published are the following two examples that illustrate just how serious the problem has become.

- Reported in March 2013, Uniontown Hospital (Uniontown, PA) was the victim of one or more hackers who accessed patient information, including encrypted passwords, contact names, email addresses and usernames.

- Between May and November 2012, a computer used by an employee of St. Mark's Medical Center (La Grange, TX) was infected by malware, resulting in potential exposure of sensitive content, including patient billing information that was stored on the device.

Among the more serious and expensive consequences of email-based or other cybercrime is the breach of customer data.

DRAINING OF FINANCIAL ACCOUNTS

A variety of organizations have been targeted with keystroke loggers like Zeus that allow criminals to transfer funds out of corporate financial accounts. There have been a number of cases of this type of theft – many targeted to small and mid-sized organizations as noted earlier – resulting in major financial losses, as in the examples below:

- Hillary Machinery: $800,000[v] (its bank was able to recover only $600,000)
- The Catholic Diocese of Des Moines: $600,000[vi]
- Patco: $588,000[vii]
- Western Beaver County School District: $700,000[viii]
- Experi-Metal, Inc. : $560,000[ix]
- Village View Escrow: $465,000[x]
- An unidentified construction company in California: $447,000[xi]
- Choice Escrow: $440,000[xii]
- The Government of Bullitt County, Kentucky: $415,000[xiii]
- The Town of Poughkeepsie, New York: $378,000[xiv]
- An unidentified solid waste management company in New York: $150,000[xv]
- An unidentified law firm in South Carolina: $78,421[xvi]
- Slack Auto Parts: $75,000[xvii]

BEST PRACTICES TO ADDRESS THE PROBLEM

To protect against email-borne threats, organizations should undertake a two-pronged course of action:

- **Train users**
  Most will agree that despite the enormous amounts spent on email security solutions, users are still the weak link in the security chain. The primary reason for this is that increasingly they are the targets, often supplying cybercriminals with the information they need by posting detailed personal information on social networks and other sites. Moreover, criminals can often harvest many corporate email addresses and use them to launch a phishing or spearphishing attack against a company's employees. Smaller organizations are typically most vulnerable to attack because they often lack the budget or expertise to thwart sophisticated attacks.

  While users cannot prevent all attacks, they should be considered the first line of defense in any email-based defense system. Consequently, users should be trained to take a common-sense approach to managing email. Although the following recommendations seem obvious, many users are guilty of violating these basic provisions, often because they are rushed in their work or simply are not sufficiently cautious when dealing with email:

  - Do not click on links in email from unknown sources.
  - Do not re-use passwords and change them frequently.
  - Do not connect to unsecured Wi-Fi hotspots, such as might be found in a coffee shop, at an airport, etc.
  - Double-check the URL of links that seem legitimate before clicking on them. Although the URL displayed may not match the URL behind the link, many email clients will display the actual URL upon mouseover.
  - If an email is trapped in spam quarantine, assume that the spam-filtering system accurately trapped the email – do not assume it is a false positive unless being absolutely certain that it is.
  - Do not send sensitive content via email without encrypting either the content or the message.
  - Be careful to ensure that sensitive content is not openly posted on social media sites, particularly those that are used for corporate purposes.

  While initial training is important, ongoing training that is designed to remind employees of new cyberthreats, new spam and malware techniques, etc. is essential as a means of maintaining a robust defense posture. This might include sending simulated phishing emails to employees to determine the effectiveness of employee training, just how careful employees pay attention to their training, etc. The goal is to provide a feedback loop that consists of testing, training, testing and remediation. Employees who fall prey to simulated phishing attempts or other cyberthreats can receive additional training or other remediation education designed to help them become more careful when inspecting their email.

- **Implement the appropriate technologies**
  The next and more important step is to implement the appropriate technologies that will thwart cybercriminal activity. This should include a layered defense system designed to:

  - Filter spam with a high degree of accuracy and a minimum of false positives.

The next and more important step is to implement the appropriate technologies that will thwart cybercriminal activity.

- Detect incoming malware, denial-of-service attacks, zero-day threats, phishing and spearphishing attempts, blended threats, bounceback attacks and other threats.
- Detect threats that are presented in short URLs.
- Evaluate solutions that offer not just protection at the time the message is scanned, but at the time the message is clicked – in other words, protect the user from the click. Criminals often get past defenses with unknown or good reputation URLs and switch the URL intent once it has gone through the initial defenses.
- Integrate with other systems, including DLP, encryption and other capabilities in order to provide an integrated solution that can be managed from a single pane of glass.

Moreover, the solution should be deployable via a variety of delivery modes, including on-premise servers, virtualized servers and in the cloud.

About McAfee

McAfee Email Protection delivers integrated inbound protection, outbound data protection, and flexibility of deployment models in an integrated, easy-to-use solution. Fueled by McAfee's Global Threat Intelligence, Email Protection defends organizations against inbound threats such as malware, shortened URLs, phishing, graymail and spam.

McAfee ClickProtect, a core feature of McAfee Email Protection, keeps users from falling victim to embedded malicious links within emails. ClickProtect checks for changes in URL intent occurring between the time the message is scanned (scan-time), regardless of how harmless it may have appeared, and when the URL is clicked by a user (click-time). At click-time, a safe-preview may be displayed to the end user to apply their own discretion. Should the URL proceed to be loaded, a full proactive emulation of the URL content is conducted to provide industry-leading zero hour malware detection rates, leveraging the same technology in McAfee Web Protection. Administrators have flexibility to configure scan-time and click-time policies, create custom warning notifications, and enable URL emulation to protect users from the click. Forensic reporting of every URL-related event provides administrators unprecedented control and decision support.

Robust outbound capabilities include encryption and content policy enforcement to keep outgoing data in emails safe from innocent mistakes and bad actors. Additional capabilities include 114+ pre-built compliance templates, deep content scanning of 300+ file types, and data loss prevention technologies. Customers have the flexibility to deploy on-site (virtual appliances, hardware appliances, blade servers), in-the-cloud (SaaS), or as an integrated hybrid combination of the two.

For more information, please visit www.mcafee.com/emailsecurity.

---

[i] http://www.net-security.org/malware_news.php?id=1772
[ii] http://krebsonsecurity.com/2011/03/rustock-botnet-flatlined-spam-volumes-plummet/
[iii] http://www.bbc.co.uk/news/business-21371608
[iv] http://www.net-security.org/malware_news.php?id=1772
[v] http://rixstep.com/1/1/20100126,00.shtml
[vi] http://krebsonsecurity.com/tag/catholic-diocese-of-des-moines/
[vii] http://www.networkworld.com/news/2009/092409-construction-firm-sues-after-588000.html
[viii] http://www.post-gazette.com/pg/09195/983738-57.stm
[ix] http://www.computerworld.com/s/article/9156558/Michigan_firm_sues_bank_over_theft_of_560_000_
[x] http://krebsonsecurity.com/2010/06/e-banking-bandits-stole-465000-from-calif-escrow-firm/
[xi] http://www.technologyreview.com/computing/23488/?a=f
[xii] http://www.bankinfosecurity.com/articles.php?art_id=3159&opg=1
[xiii] http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html
[xiv] http://www.computerworld.com/s/article/9153598/Poughkeepsie_N.Y._slams_bank_for_378_000_online_theft
[xv] http://www.suite101.com/content/protect-yourself-against-banking-crimeware-a156086
[xvi] http://www.abajournal.com/news/article/doj_says_massive_decade-old_botnet_helped_web_thieves_steal_millions/
[xvii] http://voices.washingtonpost.com/securityfix/2009/07/the_pitfalls_of_business_banki.html