Prevent Data Breaches with Stronger Email Security

Summary

Email remains the #1 threat vector for many organizations. To fight the onslaught of cyber threats, nothing short of a multilayered security architecture, backed by strict security policies and staff training, can protect an organization. Spam filters, antivirus and anti-malware are the foundation of a comprehensive security apparatus, but new technologies are emerging to aid organizations in their defense.

Cybercriminals are becoming increasingly adept at stealing information or disrupting network operations, but in 2013 they found another way to make trouble – denying users access to their own data and demanding ransom in return. The ransomware, called CryptoLocker, is often delivered via malicious email. An unsuspecting user opens an attachment, unleashing code that encrypts files such as Word documents, JPEGs, PDFs and PowerPoint slides.

By doing something as commonplace and reflexive as opening an email and clicking an attachment, employees are unwittingly infecting networks with one of the Internet's most invasive and difficult to eradicate malware threats.

Once networks are infected, victims are told to pay at least $300 or lose their data. In some cases, the infection is serious enough to halt business operations. An Australian firm had to send its staff home for five days and spend more than $4,000 on remediation.[1] CryptoLocker appeared in September 2013, and by the end of 2013 it had infected more than 250,000 machines.[2]

This digital hostage taking illustrates how creative hackers have become. It also proves that no matter how airtight data protection gets, cybercriminals persist in attacking the most vulnerable attack surface in IT security – people. And nowhere are your people more exposed to cyber-attacks than through all the messages streaming into their email inboxes every day.

Click First. Think Second.

Adding to security professionals' already daunting task, admins tell us users seem more likely to open an attachment or click a URL at work than at home. They assume it's safe if it clears the organization's security protection measures (unaware of emerging threats that evade traditional defenses) – or they simply care less about office machines than their own.

Email is often the entry point for all manner of malware attacks.

CryptoLocker is just one example. Email is often the entry point for all manner of malware attacks. Attacks vary from the indiscriminate and massively disruptive variety, such as CryptoLocker, to sophisticated targeted attacks and Advanced Persistent Threats (APTs), which zero-in on specific companies,

groups or individuals within an organization to steal intellectual property and sensitive data.

Fighting back requires a multilayered security strategy that addresses fundamental questions:

- How are attacks launched and where do they originate?
- Which business units are targeted and how sophisticated are the threats?
- Which attack vectors are used to deliver payloads and which applications are vulnerable to exploits?

The answers require clearly defined security policies. Organizations must also train staff on when not to open suspicious attachments and URLs. Given the dependence on email for everyday communications and cybercriminals' reliance on it as an attack vector, multilayered defenses are more important than ever.

Frequent and Costly

Cyber-attacks are getting more common and more expensive. The Ponemon Institute estimates in its "Cost of Cyber Crime Study" that cybercrimes cost U.S. organizations an average of $8.9 million a year. Organizations worldwide suffered an average of 1.8 successful attacks per week, and the overall number of successful weekly attacks was 102, up from 72 the previous year – a whopping 42% jump.[3] Ponemon's "Cost of Data Breach: Global Analysis" found that U.S. companies on average spend $5.4 million per breach, and that each breach compromises an average of 28,800 records, at a cost of $277 per record.[4]

Companies spend $5.4 million per data breach.

No industry is immune, though some offer bigger targets than others. Verizon found the finance industry tops the list, with retail scoring a distant second, followed by food services (restaurants and eateries), manufacturing and information companies. In its "2013 Data Breach Investigations Report," Verizon estimates more than 47,000 attacks occurred in 2012 in 27 countries, including the United States. 37% affected finance organizations, 24% took place in retail and restaurant settings, and 20% affected manufacturing, transportation, utilities, and information and professional services.[5]

Phishing is a preferred method of attack, especially for cyber espionage. Verizon found that attacks employing phishing and other social tactics increased fourfold in 2012 from the prior year. Phishing is effective at organizations large and small; 82% of social-tactic attacks at large companies involve phishing, compared to 71% at small companies. Email, Verizon says, is the most common vector in social attacks.

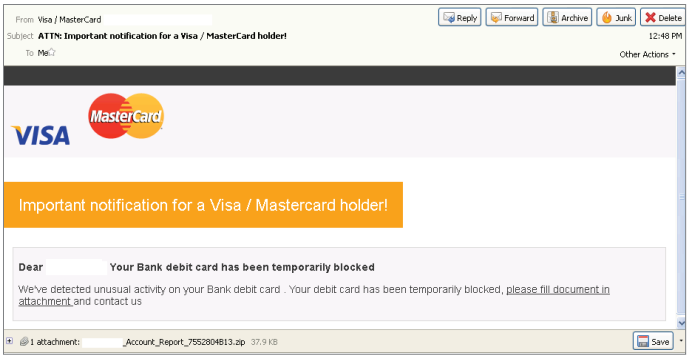
Phishing is also how a user at IT security company RSA was tricked into opening a document with malicious code. In a well-crafted APT, a group of RSA employees were sent a spreadsheet called "2011 Recruitment Plan" twice in two days. One employee took the bait, even retrieving it from the email junk folder. A zero-day exploit in the document swiped data from the company.[6]

As sophisticated as they are, APTs still require something as simple as a mouse click to get going. And even a security company can fall prey to phishing because of people's propensity for clicking items in their email.

Evolving Threats and Tactics

In the past, any computer user could be attacked simply for having an Internet connection. Hackers carried out attacks primarily for sport – to show they could. Over time, threats have evolved into far more sophisticated – and damaging – data-theft attempts that creatively employ stealth and deception to deliver payloads. Attacks are more focused, targeting users and organizations with specific types of information, such as trade secrets and payment card data. In cases such as CrytoLocker, the goal is financial gain.

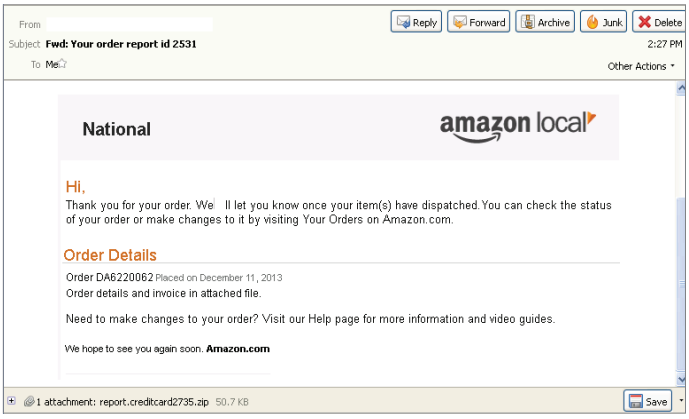
The inbox is a primary target. Threats delivered through email range from garden-variety viruses and worms to rootkits, botnets, targeted attacks and APTs. Increasingly, blended threats combine various malware types and tactics to maximize impact and accelerate the spread of infection.



Email threats often steal the logos and branding of well-known companies to trick users into feeling they are being contacted by a legitimate entity.

Consider an APT or targeted attack that delivers a payload after stealing user credentials via a phishing attack. The malware could contain a self-replicating virus or worm that attacks a server to spread the infection, but the original email seemed innocuous enough.

In the case of malicious links, the email itself contains no malicious code and nothing happens until a trusting user opens a URL programmed to spread infection. A Trojan horse could be delivered through email and hide dormant until it is commanded to steal confidential information. Rootkits delivered through URLs or files can hide malicious code from filters and detection tools.



This malicious email purporting to be from Amazon actually delivered the Androm malware, which remotely controls infected machines.

In a real-world example, a cybercriminal targeted an HR director through spear-phishing with a "malformed" email containing a suspicious embedded link. The link, entitled "LinkedIn Profile," was embedded in an attached PDF called "Resume." Because the email had legitimate contextual data, it bypassed the organization's mail server's content filtering. Malformed emails contain unusual strings of characters designed to elude interpretation by the server. This is mostly possible because of the mail server's inability to open and test the malicious PDF attachment.

The URL was actually a redirect to a Command and Control (C&C) server ready to send out malicious code. When someone clicked the URL, it opened an encrypted communications tunnel to the C&C server that bypassed detection. Once the malicious payload was discovered, the business had already been affected. Meanwhile, a vulnerable vector had been exploited to send out confidential data and establish a foothold.

Under Attack

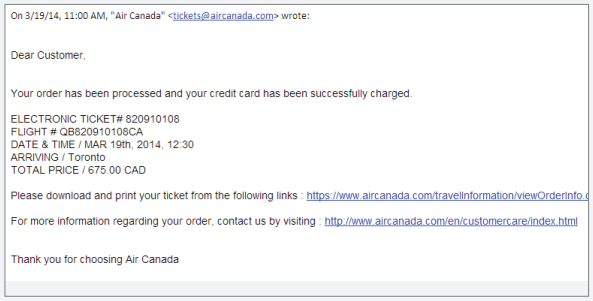
Cybercrime is relentless. Sources of threats are varied: low-rent hackers seeking financial gain, terrorist groups looking to cause disruption, foreign governments bent on stealing trade or defense secrets. Today anyone with a browser can be a hacker, thanks to the proliferation of threat types

ThreatSecure Catches Air Canada Ticket Malware En Route

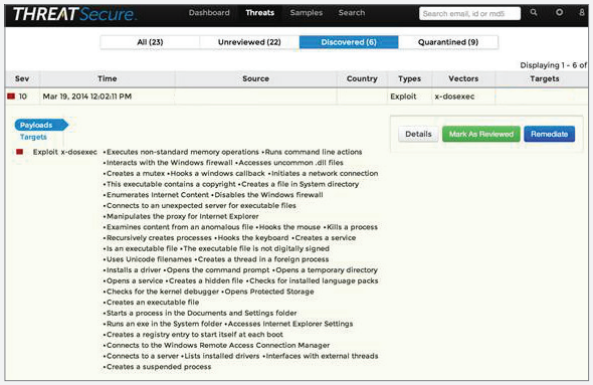
When discovered, none of the 51 antivirus vendors on VirusTotal detected the sample.

At RSA Conference 2014, ThreatTrack Security launched the ThreatSecure email appliance, a new approach to catching email-based malware attacks that evade traditional signature-based defenses.

The email (pictured below) was directed to an employee inbox purporting to be from Air Canada and directing the recipient to download and print their ticket. (Note: Air Canada was not hacked, nor were they part of this malware. The malicious URL distributing a previously unidentified malware is simply being masked to look like it's coming from Air Canada.)



The link **hxxps://www.aircanada.com/travelInformation/viewOrderInfo.do?action=download&fid=QB820910108CA** pointed to another address **hxxp://alienstub.com/pdf_ticket_820910108.zip**, which hosted the malware, a zipped malicious file. Once the zip file was decompressed, the user saw a file called **pdf_ticket_820910108.pif**



ThreatTrack SECURITY

and the availability of downloadable kits to deliver malicious payloads.

IT association ISACA notes that with PCs and servers connected to the Internet around the clock, hacking opportunities abound. Exploits target operating systems, web-aware user applications such as Adobe Reader, Microsoft Office, browsers and the Java programming language. And, of course, "attackers also seek to take advantage of computer users (e.g., spear-phishing or other social engineering) by deploying commonly available web-enabled, user-friendly hacking tool kits," the association said in a report titled "Responding to Targeted Cyberattacks."[7]

ISACA recommends that IT security professionals maintain this stance: "The network is compromised, or soon will be. How do we protect the most important data in a compromised environment? How do we make it difficult for attackers to be successful? How do we detect that an attack is underway? How do we respond to today's sophisticated attacks?"

Fighting Back

To fight the onslaught of cyber threats, nothing short of a multilayered security architecture, backed by strict security policies and staff training, can protect an organization. Spam filters, antivirus and anti-malware are the foundation of a comprehensive security apparatus, but new technologies are emerging to aid organizations in their defense.

Scanning emails for malicious content at the endpoint is a good start, but once emails with attachments get through "front-door" filters, attached files should be scanned again before opening. Files and URLs that rouse suspicion must be isolated and analyzed. In addition, organizations need to regularly update and patch applications to help eliminate vulnerabilities that cybercriminals can exploit.

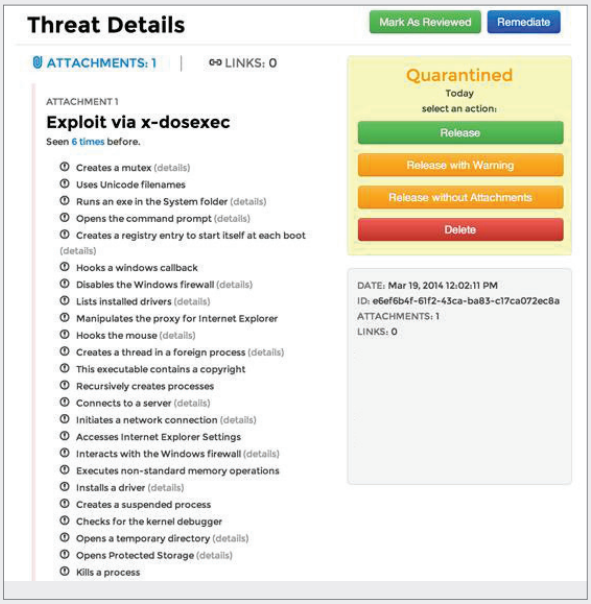
Once email security is addressed at the endpoint and at the Exchange server, IT professionals need to consider the growing tide of advanced threats that evade traditional signature-based detections. A new breed of advanced malware defenses are emerging that address this new threat vector by deploying a mix of traditional detection methodology backed by real-time dynamic malware analysis and cloud-based threat intelligence. This new layer of email security is playing a critical role in organizations' ability to defend their #1 vulnerability from the world's most sophisticated malware threats.

It is critical to also address user behavior. Organizations must train employees to spot and avoid suspicious email. As the National Cyber Security Alliance states on its website, "Training employees is a critical element of security. They need to understand the value of protecting customer and colleague information and their role in keeping it safe."[8]

Analysis by ThreatSecure quickly revealed the sample as an exploit categorized with a high severity (see in-product analysis screen above), exhibiting malicious behavior like disabling the Windows firewall, changing proxy settings in Internet Explorer, opening the command prompt, creating executable files and connecting to Windows Remote Access Connection Manager.

At the time of receiving the ThreatSecure analysis, none of the 51 antivirus vendors on VirusTotal detected the sample.

In addition to the risk assessment above, ThreatSecure provided the following Threat Details for the security administrator to take corrective action and address the threat.



Learn more at
www.ThreatTrackSecurity.com/ThreatSecure

Defense in Depth

Layer Your Email Defense with ThreatTrack Security

ThreatTrack Security advocates a layered security strategy in the battle against malware that enables users to defend their organizations from email-borne threats at the endpoint, on the Exchange server and on the network.

VIPRE® BusinessPremium™

VIPRE Business Premium endpoint protection defends against malicious email, keeping users' inboxes safe from viruses with direct support for Microsoft Outlook and any program that uses POP3 or SMTP.

VIPRE® Exchange™

VIPRE Email Security for Exchange provides an efficient and effective layered security approach for email inspection, cleansing and management at the Microsoft Exchange Server.

THREATSecure™

For advanced threats evading traditional layers of defense, the ThreatSecure email appliance offers real-time detection and closed-loop endpoint remediation of Zero-days, targeted attacks and other sophisticated malware distributed via email.

Employees must learn to not click URLs and documents from unknown sources, as well as anything suspicious that appears to come from a known or trusted source. Users should be trained to alert IT security professionals whenever they receive a suspicious email so IT can isolate and analyze it. IT can then determine if there is a threat, its origin and motivation, and what type of data it seeks. Information culled through analysis can then be shared with employees to reinforce the importance of avoiding suspicious emails.

Conclusion

Fighting email threats may feel like an uphill climb, but organizations cannot relent in shoring up their defenses and training staff to prevent security incidents. As CryptoLocker demonstrates, cybercriminals are getting more creative and audacious. Ponemon breaks down the causes of security breaches into three categories – malicious attacks (37%), negligence (35%) and system glitches (29%). The breakdown underscores the importance of multilayered security and an educated staff to protect against the barrage of cybercrime attempts that organizations face everyday.

About ThreatTrack Security Inc.

ThreatTrack Security specializes in helping organizations identify and stop Advanced Persistent Threats (APTs), targeted attacks and other sophisticated malware designed to evade the traditional cyber-defenses deployed by enterprises and government agencies around the world. The company develops advanced cybersecurity solutions that **Expose**, **Analyze** and **Eliminate** the latest malicious threats, including its ThreatSecure advanced threat detection and remediation platform, ThreatAnalyzer malware behavioral analysis sandbox, ThreatIQ real-time threat intelligence service, and VIPRE business antivirus endpoint protection.

1. Uncracking Cryptolocker, December 2013 - http://www.crn.com.au/Feature/364753,uncracking-cryptolocker.aspx

2. Cryptolocker ransom Trojan infected 250,000 PCs, Dell SecureWorks estimates At least 0.4 percent of victims paid up, December 2013 - http://news.techworld.com/security/3494576/cryptolocker-ransom-trojan-infected-250000-pcs-dell-secureworks-estimates/

3. 2012 US Cost of Cyber Crime Study, October, 2012 - http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

4. 2013 Cost of a Data Breach Report, May, 2013 - https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

5. 2013 Data Breach Investigations Report, April, 2013 - http://www.verizonenterprise.com/DBIR/2013/

6. Anatomy of an Attack, April, 2011 - https://blogs.rsa.com/anatomy-of-an-attack/

7. Responding to Targeted Cyberattacks - http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Responding-to-Targeted-Cyberattacks.aspx

8. Train Your Employees - http://www.staysafeonline.org/business-safe-online/train-your-employees

To learn more about ThreatTrack Security
call +1-855-885-5566 or visit www.ThreatTrackSecurity.com.

ThreatTrack SECURITY