FORTRA

GUIDE *(Agari)*

Ransomware: Exploring The Leading Cyber Extortion Tool

Ransomware has rapidly risen to the top of the cyber threat landscape and continues to gain momentum at an alarming rate. Criminals have evolved ransomware attacks from merely targeting individuals to now effectively extorting businesses for larger sums of money by threatening to publicly share or destroy private company data. Such attacks do not only affect the targeted organization, but also its customers and users – and, as a result, do not only cause financial loss, but also affect the reputation of targeted organizations.

In this exploration of ransomware, Agari will cover the bases of ransomware attacks, uncover delivery techniques and examples from criminals, as well as share countermeasures you can take to prevent these attacks from reaching your organization and employees.

What is Ransomware and How Does it Spread?

Ransomware is a form of malware that typically encrypts the hard drive of the compromised computer, requesting a payment in return for giving the victim the decryption key. Some ransomware is spyware, extracting valuable or embarrassing information that is later used for purposes of extortion. Ransomware benefits from the existence of non-traceable communications (like Tor) and non-traceable payments (like Bitcoin).

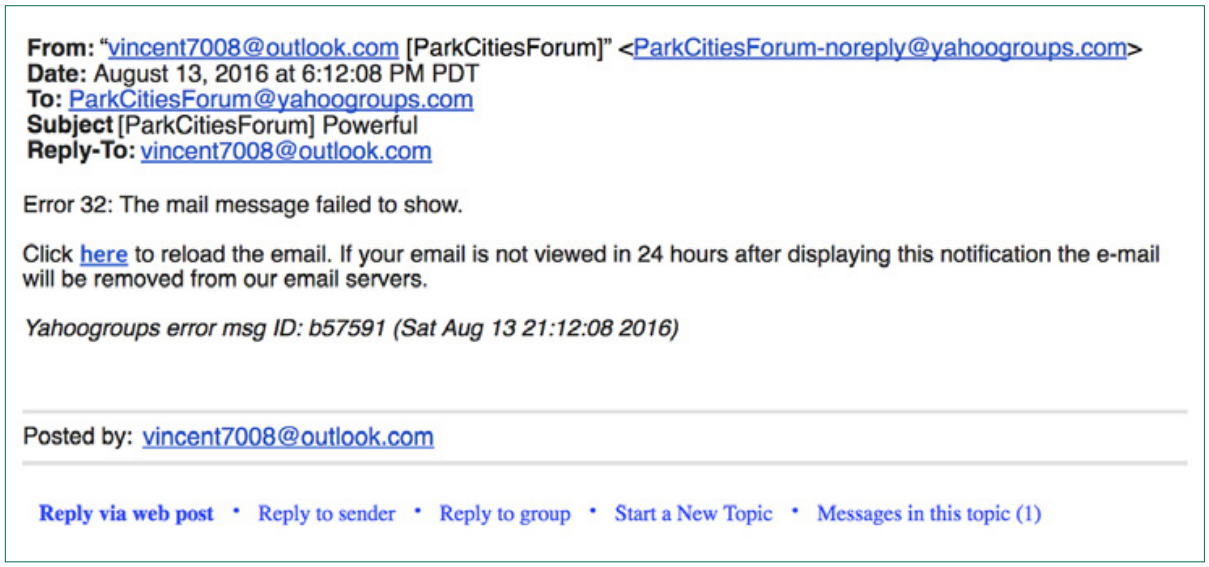
Ransomware uses obfuscation techniques such as crypters to evade antivirus tools, and their success almost always hinges on the willingness of end users to be tricked or seduced into installing them. The most common delivery technique involves email, since email is pervasive and poorly defended against abuse.

> "Ransomware does not only cause **financial loss,** but also **affects the reputation of targeted organizations.**"

While ransomware itself relates to the payload of malware, as opposed to the manner in which it propagates, it is worth noting that most ransomware attacks are delivered by Trojans. A Trojan is a type of malware that is commonly spread by email, and is installed when unsuspecting users open dangerous attachments. The emails typically come from senders the victims know, think they know, or with tantalizing names.

Sometimes, malicious emails contain links to sites where visitors are prompted to install Trojans - often masquerading as popular games or file sharing applications. Such sites also attract visitors using search engine optimization techniques, and in some cases, online advertisements.

An example Trojan-associated email spread on Yahoo groups:



From: "vincent7008@outlook.com [ParkCitiesForum]" <ParkCitiesForum-noreply@yahoogroups.com>
Date: August 13, 2016 at 6:12:08 PM PDT
To: ParkCitiesForum@yahoogroups.com
Subject [ParkCitiesForum] Powerful
Reply-To: vincent7008@outlook.com

Error 32: The mail message failed to show.

Click here to reload the email. If your email is not viewed in 24 hours after displaying this notification the e-mail will be removed from our email servers.

Yahoogroups error msg ID: b57591 (Sat Aug 13 21:12:08 2016)

Posted by: vincent7008@outlook.com

Reply via web post • Reply to sender • Reply to group • Start a New Topic • Messages in this topic (1)

The above message was sent with various subject lines intended to attract attention, such as "Powerful" and "Interesting?" from corrupted computers of users on the group.

Masquerading as a Known Entity

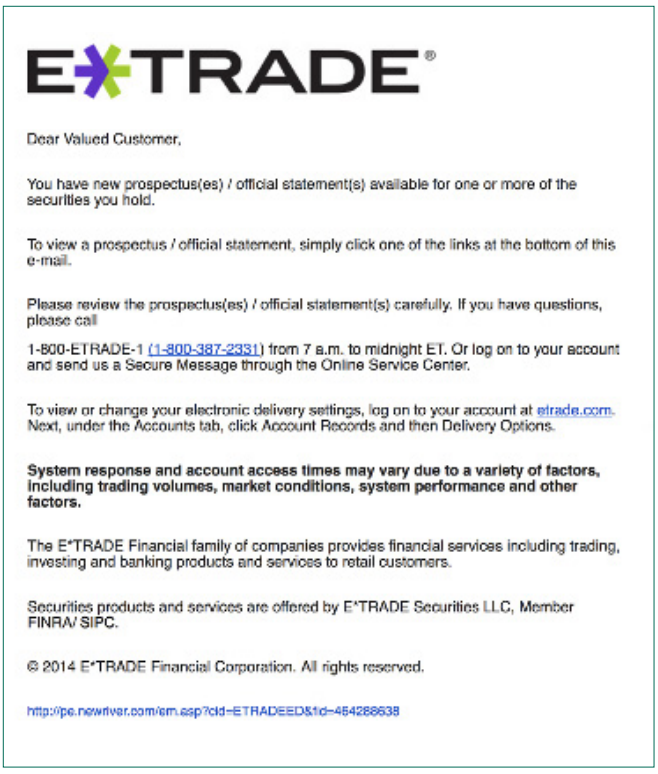
Some Trojan campaigns specifically aim to spoof legitimate emails sent from legitimate companies. These campaigns typically relate to common services, such as banking, healthcare, parcel delivery or government facilities - areas that most email recipients are likely to be able to relate to.

A common storyline used by distributors of Trojans is that the recipient has received a parcel from a popular delivery company, such as FedEx. An attachment or a hyperlink supposedly provides more information about the delivery - although, in reality, clicking on either will lead to a Trojan being installed.

So how can email recipients know whether an email is genuine or fake?

"It is worth noting that **most ransomware attacks are delivered by Trojans through email.**"

Consider the example in this email:



E*TRADE

Dear Valued Customer,

You have new prospectus(es) / official statement(s) available for one or more of the securities you hold.

To view a prospectus / official statement, simply click one of the links at the bottom of this e-mail.

Please review the prospectus(es) / official statement(s) carefully. If you have questions, please call

1-800-ETRADE-1 (1-800-387-2331) from 7 a.m. to midnight ET. Or log on to your account and send us a Secure Message through the Online Service Center.

To view or change your electronic delivery settings, log on to your account at etrade.com. Next, under the Accounts tab, click Account Records and then Delivery Options.

System response and account access times may vary due to a variety of factors, including trading volumes, market conditions, system performance and other factors.

The E*TRADE Financial family of companies provides financial services including trading, investing and banking products and services to retail customers.

Securities products and services are offered by E*TRADE Securities LLC, Member FINRA/ SIPC.

© 2014 E*TRADE Financial Corporation. All rights reserved.

http://pe.newriver.com/em.asp?cid=ETRADEED&id=464288638

Thumbs Up or Down?

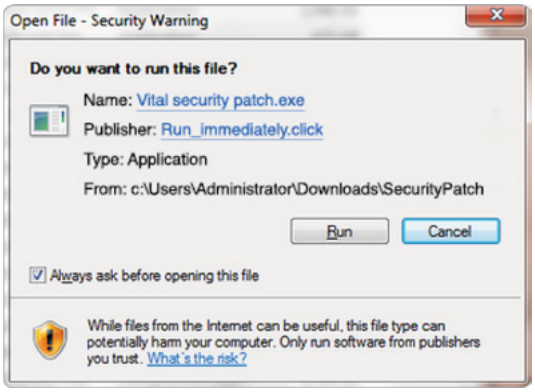
Is the example email above legitimate or not? That may be very difficult for a typical user to determine. The sender is "prospectus_mbox@investordelivery.com"; the greeting is suspiciously anonymous with "Dear Valued Customer"; and the URLs are related to "newriver.com" instead of E*TRADE. If we were to rely purely on the well-meaning advice given by organizations like the FBI, we would surely conclude that this is a bad email - but in reality, this email is actually legitimate.

It is therefore no surprise that people are frustrated by internet security. Given how users are "trained" by authoritative bodies and service providers to accept emails such as these, it is also not surprising how successful malware distributors are. Clearly, relying on the end user for security is largely pointless.

> "The **inability to secure email** is the **number one cybersecurity threat** facing businesses, governments, and individuals today."

Tricks to Track Down

Alongside email attacks, some Trojans masquerade as security patches, and some use deceptive names to increase installation rates. For example, consider this hypothetical case in which a user performs an action that leads to being asked whether she wishes to install a piece of software. The software is deceptively named "Vital security patch.exe". In addition, the malware author chooses a deceptive publisher name — 'Run_ immediately.click' — in the hopes that the recipient mistakes this for an instruction.



A Common Series of Events

It is clearly helpful to recognize that most ransomware attacks are indeed just email-delivered Trojans that follow a typical flow of events. To summarize, the chain usually looks like this:

- **A user receives an email** commonly appearing to be from somebody they know, or a company they have a relationship with. It might be that the sender has just set a deceptive display name; it might be that he spoofed a trusted sender; or it might be that he sent the email from an account that has been taken over by an attacker. Other emails simply focus on making the email content sufficiently convincing or intriguing.

- **The email contains** a hyperlink or an attachment. If the user clicks on the link/attachment, this will initiate an installation of malware. The user may have to agree to the installation.

- **The malware will run.** Ransomware will typically encrypt the hard drive of the victim computer, then issue a ransom note.

- **After the attacker** has received the requested money (commonly using Bitcoin, since that does not make tracking feasible), the decryption key is released.

Unforeseen Consequences

Contrary to popular belief, the losses due to ransomware attacks are not limited to the ransom paid. The theft of data can have a significant impact on victims, whether individuals, organizations or governments - ranging from personal anxiety and PR disasters to unwanted exposure to competitors and hostile nation states. Loss of data can eat away at the fabric of trust, and the fear of potentially becoming victimized can limit productivity by forcing the use of onerous protective procedures.

It is increasingly becoming clear to organizations that the greater risk relates to having your data destroyed or private company information shared, as opposed to having to pay a $17,000 ransom. Moreover, even if a victim pays the ransom, there is no guarantee the stolen data will not get published or used against them.

Ransomware Attacks on the Rise

One of the most high-profile examples of ransomware was when the Hollywood Presbyterian Medical Center in Los Angeles declared a state of emergency due to a "Locky" ransomware attack. During this two week standoff, all hospital and medical records were offline, leaving the hospital defenseless while the hackers held the hospital's data records hostage until the ransom was paid.

Synopsis of the Attack

- **The Hollywood hospital** lost access to its computer systems for approximately two weeks after hackers infected hospital computers with a piece of ransomware known as Locky. All computer files were encrypted, making them inaccessible to hospital staff during this time.

- **The hospital decided** to pay the ransom – which cost them 40 Bitcoin, the equivalent of about $17,000.

- **However, the real loss** that the hospital faced was not the $17,000 ransom, but rather the millions of dollars worth of bad press, damaged reputation, and loss of business.

- **The funds paid** may also have given the criminals the resources and momentum required to build better tools to extort other organizations in the future.

> "It is increasingly become clear to organizations that the **greater risk** relates to having your **data destroyed** or **private company information shared** than having to pay a $17,000 ransom"

How to Protect Against Ransomware Attacks

In order to properly safeguard against ransomware, it is important to implement proactive, trust-based email security controls to protect recipients from socially-engineered, non-trustworthy emails.

The Agari Secure Email Cloud™ protects employees, partners, and customers from receiving untrusted emails that are the delivery mechanism for advanced email attacks such as ransomware. The Agari solution creates a unique model of trusted email by analyzing organization's inbound email and outbound email senders, and then correlating it with analysis of billions of email messages a day from the world's largest email providers including Google, Microsoft, and Yahoo. That trust model is then used to categorize and block all untrusted email from reaching your employees' or customers' inboxes.

The inability to secure email is the number one cybersecurity threat facing businesses, governments and individuals today. Protect your organization from ransomware attacks by using Agari to secure your email.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.