REPORT

FireEye

TOP WORDS USED IN SPEAR PHISHING ATTACKS:

Successfully Compromise Enterprise Networks and Steal Data

SECURITY REIMAGINED

CONTENTS

Executive Summary 3

Introduction 3

File Names 4

Top 5 File Extensions 6

Conclusion 6

About FireEye 7

Executive Summary

Aided by their targets' porous defenses and unwitting end users, today's cybercriminals are able to deliver advanced malware that exploits systems and enables a range of malicious activities. Much of this advanced malware is being delivered via emails with malicious file attachments. This report provides a look at the nature of the files cybercriminals are distributing, specifically those that are effectively bypassing traditional security defenses such as firewalls, next-generation firewalls, intrusion prevention systems (IPS), anti-virus (AV), and secure gateways. This report describes the common words used in file names and file types that characterize this advanced malware, providing key insights for users and security teams looking to guard against advanced threats.

Introduction

In spite of all the security defenses designed to protect email communications, this channel continues to represent fertile ground for cybercriminals—and a critical area of vulnerability for most organizations. Email communications represent one of the most frequently used avenues of attack. The risks posed by these attacks are significant. Not only is email the avenue for spam and mass-distributed malware, it is also the way many advanced persistent threat (APT) attacks are initiated. GhostNet, Night Dragon, Operation Aurora, the RSA breach, and many of the other APTs that have been publicly documented have been initiated at least in part through targeted spear phishing emails.

The reality is that cybercriminals continue to use this mode of attack because it works. In the most recent Advanced Threat Report for 1H 2012, FireEye reported a 56% increase in the amount of malicious emails between Q1 2012 and Q2 2012. It is important to realize this increase isn't in the total number of malicious emails distributed; it is an increase in the number of emails that are getting past organizations' existing traditional security defenses.

FireEye is in a unique position to illuminate this advanced targeted attack activity. Hundreds of customers around the world have deployed the FireEye Malware Protection System™ (MPS). The FireEye solutions are deployed behind firewalls, next-generation firewalls, IPS, AV, and other security gateways, and represent the last line of defense for organizations. These solutions feature appliances that automatically gather threat intelligence that can be aggregated, analyzed, and shared. Through these solutions FireEye is able to report on the nature of advanced threats.

This report focuses on the characteristics of the advanced malware being distributed via email attachments and that is circumventing traditional defenses. Through the data presented, this report provides vital insights into the attributes of advanced malware and the tactics of cybercriminals, so security teams and users can better understand the nature of today's threats. It is important to underscore that the findings below detail the advanced threats that effectively bypass existing mechanisms. Put another way there's a very good chance these types of malware will be coming to your inbox soon —if they're not there already.

Filenames

When cybercriminals distribute malicious files, they do so intending to dupe an unsuspecting recipient into downloading or installing these files locally. To do so they use a range of tactics. The words used within these file names provide some clear insights into the tactics that cybercriminals use and that are proving to be effective. The chart below provides a look at the most common words that appear in the malicious files that FireEye solutions have detected. To be clear, these are the words used by attackers that helped enable them to evade all traditional IT security defenses.

2H 2011

Rank	Word	Percent of Attachments
1	label	15.17
2	invoice	13.81
3	post	11.27
4	document	10.92
5	postal	9.80
6	calculations	8.98
7	copy	8.93
8	fedex	6.94
9	statement	6.12
10	finanacial	6.12
11	dhl	5.20
12	usps	4.63
13	8	4.32
14	notification	4.27
15	n	4.22
16	irs	3.60
17	ups	3.46
18	no	2.84
19	delivery	2.61
20	ticket	2.60

1H 2012

Rank	Word	Percent of Attachments
1	dhl	23.42
2	notification	23.37
3	delivery	12.35
4	express	11.71
5	2012	11.30
6	label	11.16
7	shipment	9.88
8	ups	9.47
9	international	8.94
10	parcel	8.16
11	post	6.95
12	confirmation	5.81
13	alert	5.80
14	usps	5.80
15	report	5.79
16	jan2010	5.52
17	april	4.71
18	idnotification	3.60
19	ticket	3.58
20	shipping	2.92

***Note:** The charts above list the percentages of terms included in malicious attachments detected by the FireEye MPS appliances. Note: given that a single malicious attachment can include multiple terms the percentages will not equal 100%.

2H 2011

Topic	Percent Total
Postal	19.20
Banking/Tax	5.98
Urgency	1.72
Airline	1.81
Billing	4.98

1H 2012

Topic	Percent Total
Postal	26.33
Banking/Tax	3.83
Urgency	10.68
Airline	2.45
Billing	0.68

***Note:** The charts above summarize the top 5 most common categories of terms used in malicious email attachments.

One way cybercriminals fool users is by sending files purporting to be notifications about express shipments. Given the ubiquity of these services, and their inherent importance and urgency, users are being compelled to open malicious files labeled with shipping-related terms. This ploy is one of the most common. Shipping and postage-related terms made up over 26% of words featured in malicious file names, and comprised 7 of the 10 most common words identified in the first half of 2012. File names such as DHL document.zip, Fedex_Invoice.zip, and Label_Parcel_IS741-1345US.zip represent samples of the types of file names criminals are using.

Between 2H 2011 and 1H 2012, several trends were identified. For example, the percentage of file names referencing words related to shipping grew from 19.20% to 26.33%. In addition, the number of files referencing words associated with urgency grew from 1.72% to 10.68%.

Following are some other common categories:

- **Urgency.** Words related to urgency such as confirmation, alert, and notification represent the second most common category of words found. These words can be used on their own, but were often seen used in tandem with other categories such as shipping, as in UPS-Delivery-Confirmation- Alert_April-2012_215759.zip, or taxes such as IRS-Penalty-Income-Tax-Warning-Notification-28306SUD4811L9JS.zip.

- **Finance.** References to financial institutions and associated transactions and communications are also prevalent. Following are a few representative files names: VisaCard-N486102989.zip, PayPal.com_2012_Account_Update_Form.html, and Lloyds TSB - Login Form.html.

- **Taxes.** References to taxes and the IRS also were seen in significant numbers, featuring files names like Tax_Refund.zip, irspdf.zip, and tax_return_form.pif.

- **Travel.** Many file names purporting to be about travel bookings, typically flight reservations, represented another common category with such file names as Ticket_American_Airlines_ID3457-144.zip, Delta_Air_Lines_Ticket_ID271-3714.zip, and A_Airline_Ticket_ID279-44-357US.zip commonly discovered.

- **Billing.** Rerms that reference invoices, purchase orders, and the like represent another significant category of terms.

Following are a few examples of the files detected: Purchase Order 74457.zip, Invoice_ID757731.zip, and Invoice_Copy.zip..

Top 5 File Extensions

When it comes to the extensions of malicious files, cybercriminals continue to adapt their approaches to the shifting landscape of security defenses and mechanisms. One clear trend is the move away from .EXE files. Historically, .EXE represented the bulk of malicious attachment types. Today however, only a small fraction of .EXE files make it through security defenses. Further, .EXE files also typically raise notification from the user's computer operating system, prompting users to acknowledge and agree to the installation of an .EXE file, which further reduces their likelihood of effectively compromising targeted system.

Now, .ZIP files represent the vast majority, 76.91%, of advanced malicious files. The complexity of these attachments, which can contain many distinct files and file types, coupled with a lack of user awareness of the danger of these file extensions, has made them a highly effective means for distributing malware and effectively exploiting systems.

PDFs also pose a significant threat. These file types are ubiquitous and familiar to just about every computer user. Further, many users are unaware of the fact that malware can be distributed through PDF files, and malware embedded in these file types is proving to be difficult for conventional defenses to detect. For all these reasons, PDFs provide cybercriminals with a very effective means of attack.

Conclusion

By referencing important and usually time-sensitive information—express shipment notifications, tax return forms, financial account status, airline ticket confirmations, and so on—cybercriminals are fostering a sense of urgency in their targets, hoping to get them to rush into downloading the malware that exploits their system. Given the limited efficacy of .EXE files, criminals today are leveraging .ZIP files, PDFs, and other file types to bypass existing traditional security defenses. To guard against these threats, users need to be educated on the dangers of advanced malware and the forms it can take today. In addition, security teams need advanced technologies that can detect and stop the advanced threats that are currently bypassing their conventional defenses. To guard against these threats, users need to be educated on spear phishing emails, especially how they are socially engineered to look authentic and the dangers they pose. In order to detect and block these advanced targeted attacks, companies are turning to next-generation threat protection that guards against attacks that bypass traditional IT security defenses.

2H 2011

Extensions	Percent
zip	85.79
exe	5.91
pif	2.67
scr	2.06
bat	1.79

1H 2012

Topic	Percent Total
zip	76.91
pdf	11.79
exe	3.98
doc	2.67
pif	1.09

***Note:** The charts above detail the relative percentages of file extensions used in the malicious files detected by the FireEye MPS appliances.

About FireEye

FireEye is the leader in stopping advanced cyber attacks that use advanced malware, zero-day exploits, and APT tactics. The FireEye solutions supplement traditional and next-generation firewalls, IPS, anti-virus, and gateways, which cannot stop advanced threats, leaving security holes in networks. FireEye offers the industry's only solution that detects and blocks attacks across both Web and email threat vectors as well as latent malware resident on file shares. It addresses all stages of an attack lifecycle with a signature-less engine utilizing stateful attack analysis to detect zero-day threats. Based in Milpitas, California, FireEye is backed by premier financial partners including Sequoia Capital, Norwest Venture Partners, and Juniper Networks.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**