FireEye
SECURITY REIMAGINED

REPORT

FIREEYE LABS

AN INSIDE LOOK
Into the World of Nigerian Scammers

JULY 2015

AUTHORS:

ERYE HERNANDEZ
DANIEL REGALADO
AND NART VILLENEUVE

SECURITY
REIMAGINED

CONTENTS

Executive Summary

419 scams, a modern twist on the classic advance-fee con game, first surfaced in the 1980s and remain active today. They typically start with a message from someone claiming to have come across a large sum of money. The catch: getting this money requires an upfront payment to cover, say, legal fees or outstanding taxes. If you come up with the money, the scammer promises, you'll get a cut of the total.

According to the U.S. Bureau of International Narcotics and Law Enforcement Affairs (INL), this scam results in losses of hundreds of millions of dollars annually worldwide.[1]

While 419 scams do not require the scammer to know anything about their victims, another type of scam involving payment diversion, where the scammer diverts funds in a business transaction to a bank account they control, requires some knowledge about the transaction and the parties involved. FireEye Labs discovered an active operation of a group of cybercriminals involved in multiple executions of the payment diversion scam. The group is composed of loosely organized individuals who use basic, but effective, tools to defraud their victims of thousands of dollars.

The cybercriminals behind this operation are located in Nigeria and are using malware as a component of their fraud scams. The group adopted the Microsoft Word Intruder (MWI) exploit kit[2] as one of its primary methods. It uses MWI to infect victims with HawkEye—a commercial keylogger that has become well known due to its high rate of infection success across multiple industries[3]—and another keylogger called KeyBase.

While using keyloggers to steal victims' credentials has been discussed in detail before, we have never seen the entire context of their operations until now. Key findings of our case study include the following:

	Scammers lack technical skills and rely heavily on third-party malicious tool developers to create and maintain their tools.
	Scammers assemble a "tool set" for conducting their fraud operations. They pay third-party malicious tool developers for a range of tools, including builders, crypters, and infostealers. For a basic tool set, a scammer might pay between $200–$3,600. By paying this small amount of overhead upfront, the scammers can overcome their relative lack of skill and assemble a tool kit. It's basic but effective. Victims are conned out of thousands—maybe even millions—of dollars. We estimate the group has targeted 2,328 victims in 54 countries. This group prefers to target small to medium businesses in Asia because they are non-native English speakers and are usually not as technically savvy as big businesses.
	Scammers use accomplices or hired hands to open bank accounts for them in foreign countries.
	The scammer group in this case study is based in Nigeria. It focuses on payment diversion fraud, a type of scam that targets legitimate business transactions.

This paper examines the world of the Nigerian scammers, detailing their end-to-end operations as they select their victims, acquire malware, execute the scam, and collect money.

[1] http://www.state.gov/documents/organization/2189.pdf
[2] https://www.fireeye.com/blog/threat-research/2015/04/a_new_word_document.html
[3] http://www.insightpartners.com/2015/06/hawkeye-keylogger-campaigns-affect-multiple-industries/

Overview of the Nigerian Group

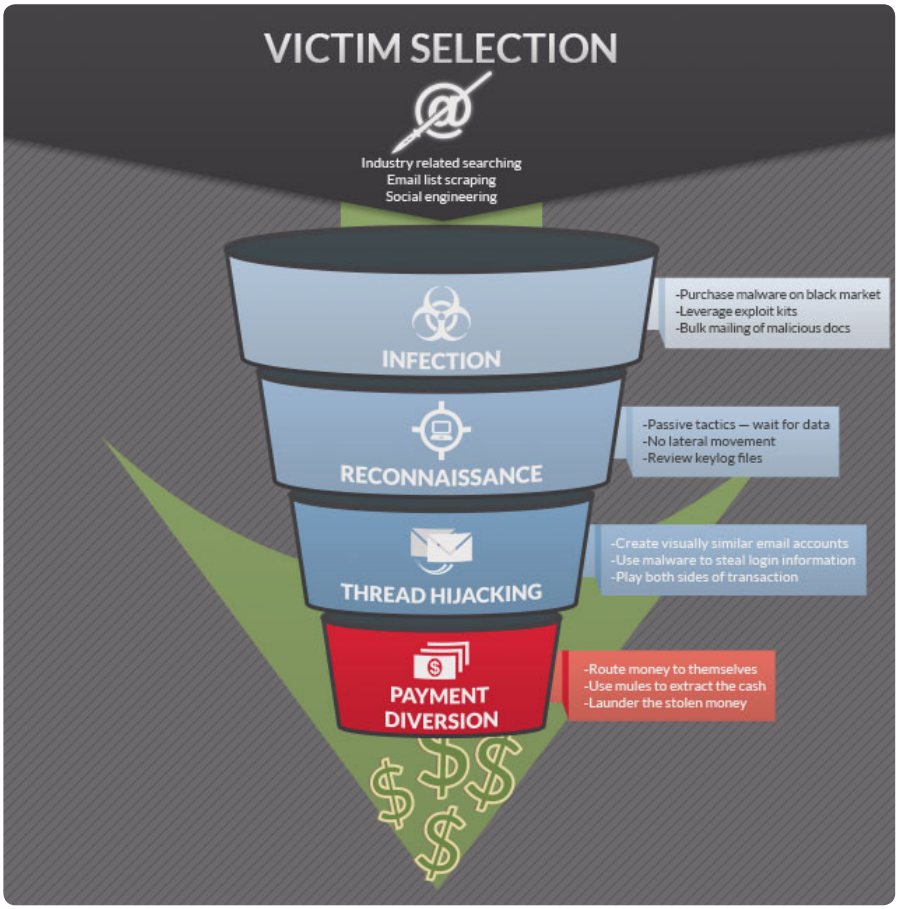
The scammer group in this case study is based in Nigeria and is composed of at least four people who share the same command-and-control (CnC) server. They are loosely organized and despite sharing the same CnC, each person has his or her own strategies to deliver exploits or acquire new targets. A few of these strategies are outlined in detail in the following sections.

The level of expertise among the group varies. Some prefer the more traditional route of spamming to acquire victims. Others focus on specific targets and use social engineering tactics to infect victims.

Some group members are more technical than others, but the group shares tools and techniques. For example, some provide fellow scammers with malicious documents and binaries created from tools they acquire from third-party malicious tool developers. And the more seasoned scammers provide less experienced scammers with email accounts of victims, helping them find good business transactions to hijack.

The Nigerian group uses the MWI exploit kit to create malicious documents that infect victims with keyloggers such as HawkEye and KeyBase. They also primarily focus on payment diversion fraud, which is a scam that targets business transactions.

Figure 1: The steps taken to target victims and extract payment



Members of the group share tools and techniques **but each uses different strategies.**

Victim Selection and Infection

The scammers often coordinate their spamming (or "bombing," as they call it) activity and share tools with other scammers. In Figure 2, the scammer references a shared exploit and a service he refers to as "vip," which in this context is a VPN service provider called VIP72. VIP72 provides a VPN and SOCKS proxy that masks the scammer's IP address when using stolen credentials to log into victims' email accounts.

This scammer also mentions "Alibaba," a well-known e-commerce portal used in this case to find potential victims. The scammer filters victims based on geography—countries where the scammer already has bank accounts or can easily transfer money into those accounts.

Figure 3 shows a sample email sent by the scammer feigning interest in a manufacturer's products sold through Alibaba. In this example, the scammer attaches an exploit document, which purports to be a product inquiry related to the vendor's products. This delivery mechanism is clever. The supplier, which expects inquiries from prospective customers as a regular part of doing business, would likely not hesitate to open the document.

Figure 2: Sharing exploits and VPN access

[[REDACTED] - 11/23/2014 4:00:35 PM]

yes boss
baba the exploit we talked about boss
i want to bomb

[[REDACTED] - 11/23/2014 4:21:17 PM]

thank you so much boss
i go use your vip later but now now to bomb from alibaba but not now i will
inform you then sha

Figure 3: Email sent by scammer with exploit document attached

[Alibaba Manufacturer Directory - Suppliers, Manufacturers, Exporters & Importers - Google Chrome - 11/12/2014 5:10:18 PM] [REDACTED]
Subject: URGENT ORDER

Dear All,

Please provide me with your best prices for this sample in the attachement

Regards
[REDACTED]

Scammers often target those who don't speak English as a first language.

We have also seen scammers search Google for email listings of trade show participants and suppliers or distributors of various goods. The scammers extract email addresses from these pages using email scraping tools. Of particular interest to them are email addresses from free email service providers as shown in Figure 4. There are a few possible reasons for them to target free email accounts:

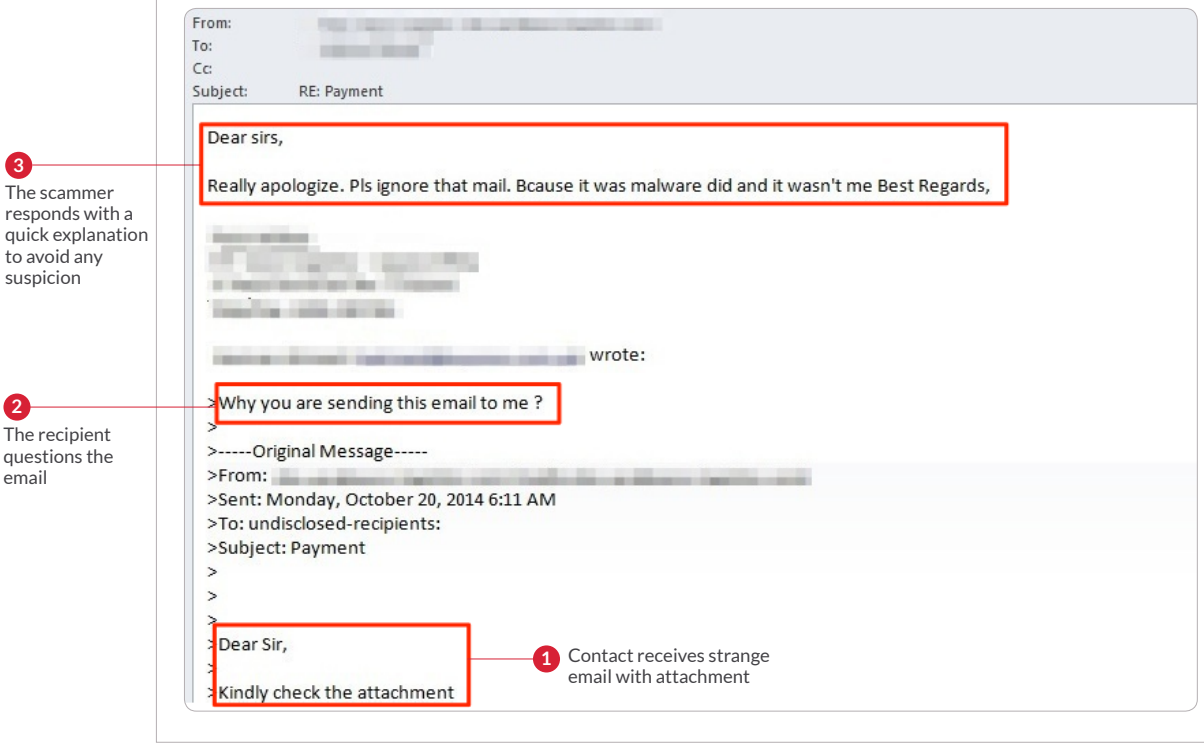
- Fewer obstacles to spoof the email addresses. The scammers would not have to register a domain and set up an email server.
- A free email account might indicate that the user is not technically savvy or is a small business.

To expand their victim pool further, scammers sometimes send infected documents to their victim's contacts. Figure 5 shows a contact receiving a strange email with an attachment (1). In this case, the recipient questions the email (2) and the scammer responds with a quick explanation to try to avoid any suspicion (3). The new victim does not seem to realize that they have already been infected (hence this screenshot being captured by the malware).

Figure 4: Scammer searching for email addresses of potential victims

```
[shanghai expo sales rep email list or @yahoo.com or @hotmail.com or @gmail.com -
Google Search - Mo - 3/19/2015 12:36:38 PM]
```

Figure 5: New victim asking about weird email



Occasionally, a victim gets infected twice, as shown in the following screenshots of an infected victim's desktop. These screenshots would not have been possible if the victim was not already infected by the keylogger. In Figure 6, we see the victim receiving an email containing a malicious attachment. This attachment triggers the victim's antivirus as shown in Figure 7. This file attachment turns out to be a KeyBase keylogger binary, which is obfuscated to avoid detection by AV products using the Cryptex obfuscator. The initial infection was able to bypass the victim's local antivirus protection as the screenshots were generated by it.

The scammers' operations focus on infecting victims who do not speak English as their first language. This makes the scammer more credible to the victims as it is not that easy for the victims to detect grammatical errors, as the victims themselves often make similar mistakes in their emails. Figure 8 shows that nearly half of the victims are from India and there is a very clear targeting of Asian countries.

Nearly half of the victims are from India. **Asian countries are also highly targeted.**

Figure 6: Email with malicious file sent to existing victim

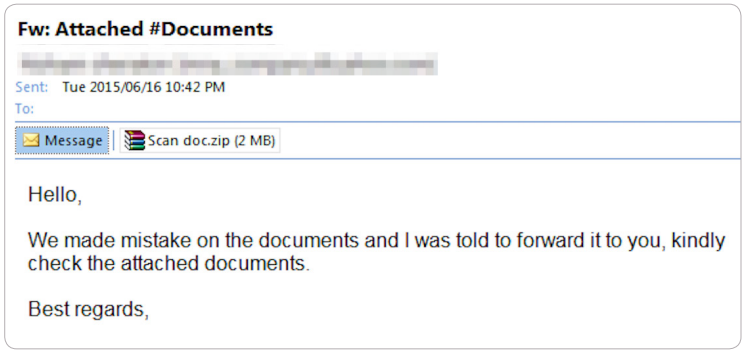


Figure 7: Opening the zip file shows the victim's antivirus firing

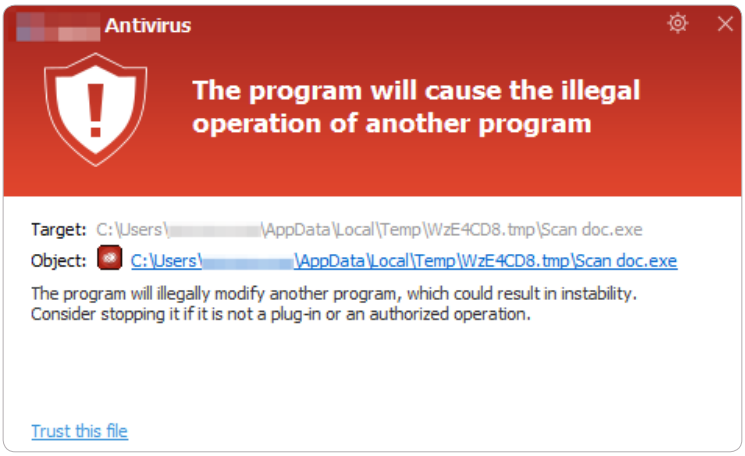
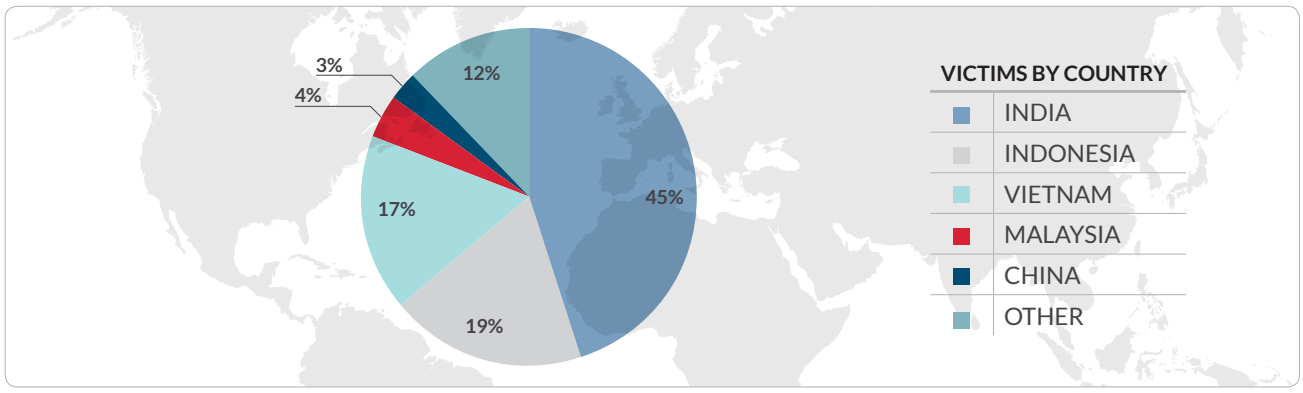


Figure 8: Victim breakdown by country



Tools of the Trade

In general, scammers typically lack the technical skills required to break in to their victim's accounts, so they acquire tools from others.

To obtain exploits, crypters, infostealers and remote access tools (RATS), they access forums to inquire and search for malicious software as shown in Figure 9. We have observed several instances of the scammers interacting with tool providers. As these interactions show, the scammers are heavily reliant on third-party malicious tool developers to create and maintain their tools. They rely on these third-party tool providers to furnish them with documentation or tutorials on the tools, to create stealthy exploits, and to troubleshoot issues.

When purchasing malicious software, the scammers typically test their tools and occasionally seek help from the providers when they run into issues, as shown in Figure 10.

Figure 9: Forum post by one of the scammers seeking an Office exploit

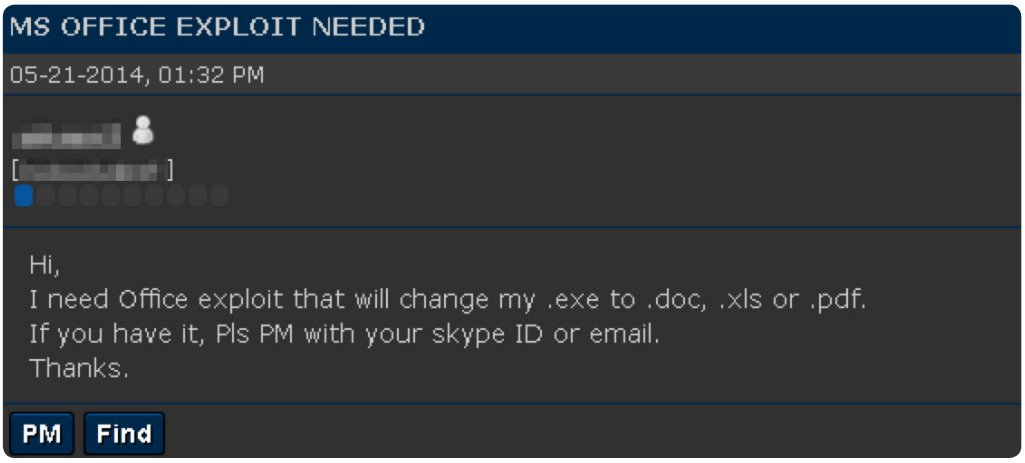


Figure 10: Scammer reporting a bug with the provider's malware

chrome : Freelancer.com | Online Jobs | Freelance Employment | Outsourcing Services | Programmers | Web Design | Freelancers - Google Chrome]

Hello bro,

You did a nice job with the project but i think made a mistake. The IP that it is suppose to send is the Internet IP. not the computer IP on the computer internal.

Please kindly check this. Thank you This is what it brought for my computer

[Screenshot of wrong IP address]

And that is not an internet connection IP

Figure 11: Scammer asking the provider to FUD an exploit

[[REDACTED] - 5/3/2015 7:01:51 PM]

hi
can you FUD the exploit for me?
its 3/35
so much is it?
no, its expensive for old customer

Figure 12: A site that a scammer uses to check detection rates

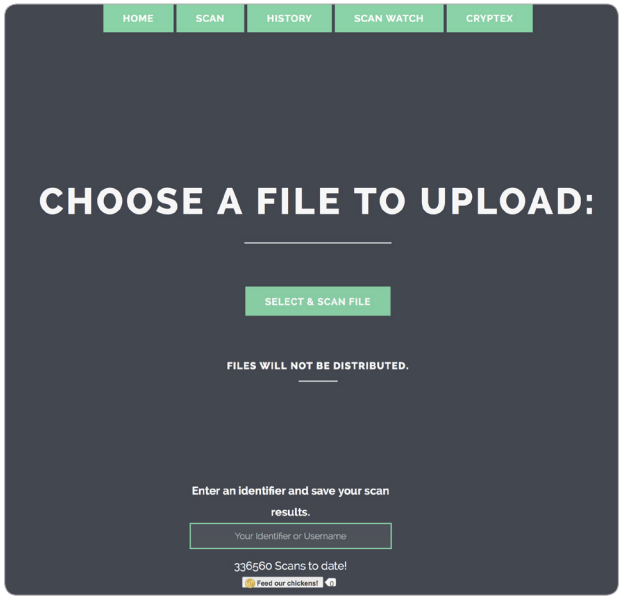
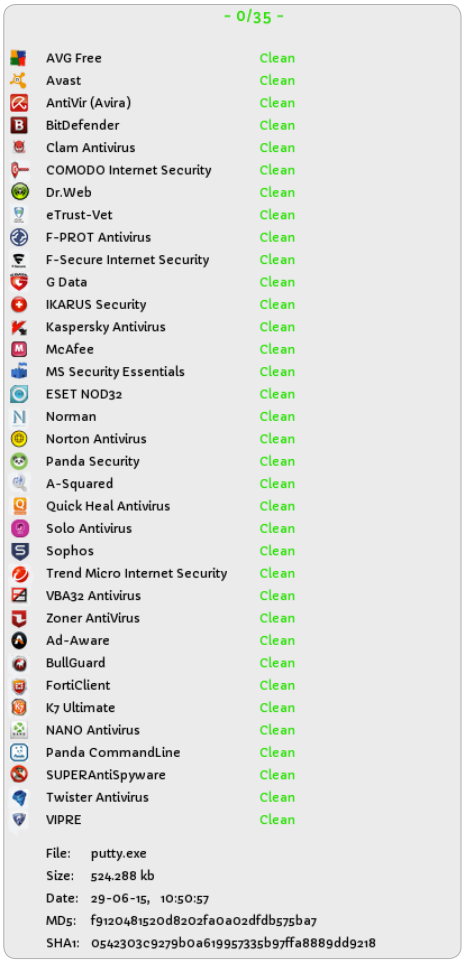


Figure 13: Detection rate report based on the uploaded file



The scammers are also concerned about their malware being "Fully UnDetectable" (FUD), as shown in Figure 11. Additional layers of protection, like encryption, are used to prevent exploits from being detected. Because scammers lack the skills to make "FUD" exploits themselves, they often rely on underground service providers to develop or modify these tools for them.

Aside from encoding or encrypting their exploits, they also run them through underground antivirus scanners to verify detection rates and ensure that their tools will bypass AV detections on their victims' computers. Figure 12 shows an antivirus scanner that one of the scammers uses to verify detection rates. Once a file has been uploaded, it is submitted to multiple AV software products and the results are presented in a report as shown in Figure 13.

This group uses the MWI builder, a tool that creates malicious documents that exploit vulnerabilities in Microsoft Word. It is mainly used to download and install malware onto the victim's computer. For more details on this tool, please refer to a blog we recently published about MWI[4].

[4] https://www.fireeye.com/blog/threat-research/2015/04/a_new_word_document.html

They also use MWISTAT shown in Figure 14, which is a package that allows the group to track their various MWI infection campaigns, success rates, and the location of their victims. The average price for the builder ranges from $2000-$3500. These tools allow the group to gain privileged access on the victim's computer to download and install malware and to track their operations from a simple, easy-to-use management console.

In one example, if the MWI exploit is successful, the HawkEye Keylogger is downloaded and installed on the victim's computer. The HawkEye Keylogger is a commercial keylogger available from HawkEye Products. It includes a GUI builder interface to allow the user to configure various options, including installation options; propagation methods; what data to capture; and the method for delivering the stolen data. It can be customized to meet the needs of the attacker. It not only logs keystrokes but it can recover browser passwords and also take screenshots of the victim's desktop. Figure 15 shows some of the settings that can be configured from the builder. The average price for this keylogger ranges from $20-$50.

Scammers are concerned about **their malware being Fully UnDetectable, or FUD.**

Figure 14: MWISTAT panel showing information on infected victims

[+] MWISTAT 2.0

MICROSOFT WORD INTRUDER

FILES | LOGS | STATS | TOOLS

NAVIGATION: **FILES > 00000000 [all files] > LOGS**

DATE_TIME	FILE_ID [FILE_NAME]	IP_ADDRESS	IP_INFO	ACTION	USER-AGENT	GET_DATA
December 19 2014 12:18:40	0	192.168.2.16	US	SUSP	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)	id=
December 19 2014 12:19:13	0	192.168.2.16	US	SUSP NOID	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)	id=00000000
December 19 2014 12:19:39	73514245 [test.exe]	192.168.2.16	US	OPEN	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)	id=73514245
December 19 2014 12:19:55	73514245 [test.exe]	192.168.2.16	US	LOAD	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)	id=73514245&act=1
December 19 2014 12:21:01	73514244	192.168.2.16	US	SUSP NOID	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)	id=73514244

CLEAN STATS

The KeyBase keylogger is another commercial keylogger also used in this operation. Similar to the HawkEye Keylogger, it logs keystrokes, recover browser passwords, and takes screenshots of victims' desktops. It is also fully customizable. Figure 16 shows the configuration window for the KeyBase builder. The price for this keylogger is $45.

The scammers use a variety of tools for distributing these exploits and keyloggers, such as email extractors, email notifiers, bulk mailing providers, and VPN/proxy providers. The email extractors help scammers scrape email addresses of potential targets from various sites which are fed to bulk mailing applications. They use proxy providers as a precaution when logging into their victims' accounts to hide their IP addresses. They also use email notifiers to monitor incoming emails.

Figure 15: HawkEye Keylogger builder

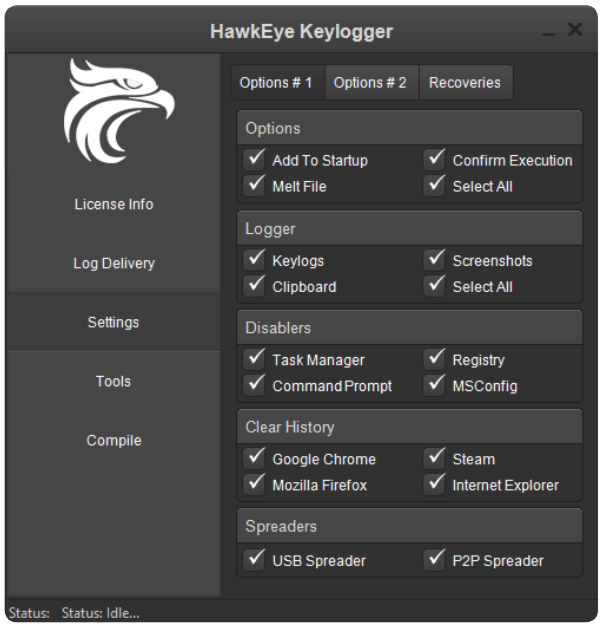
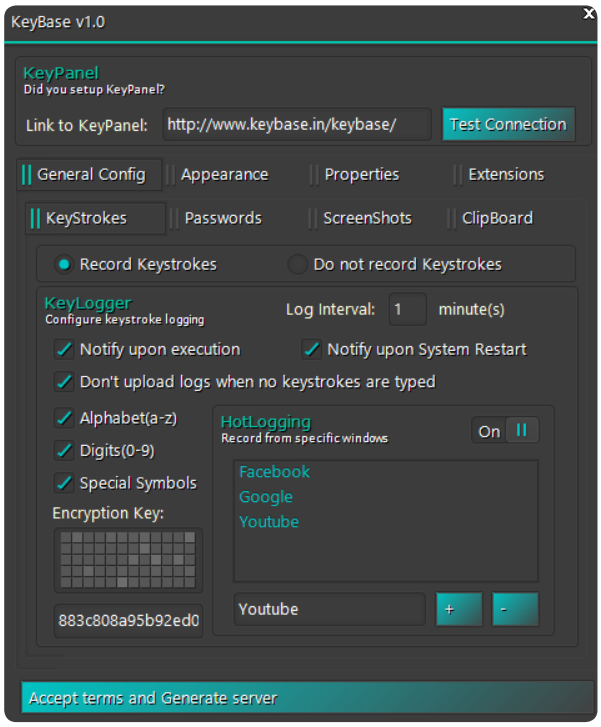


Figure 16: KeyBase Keylogger builder

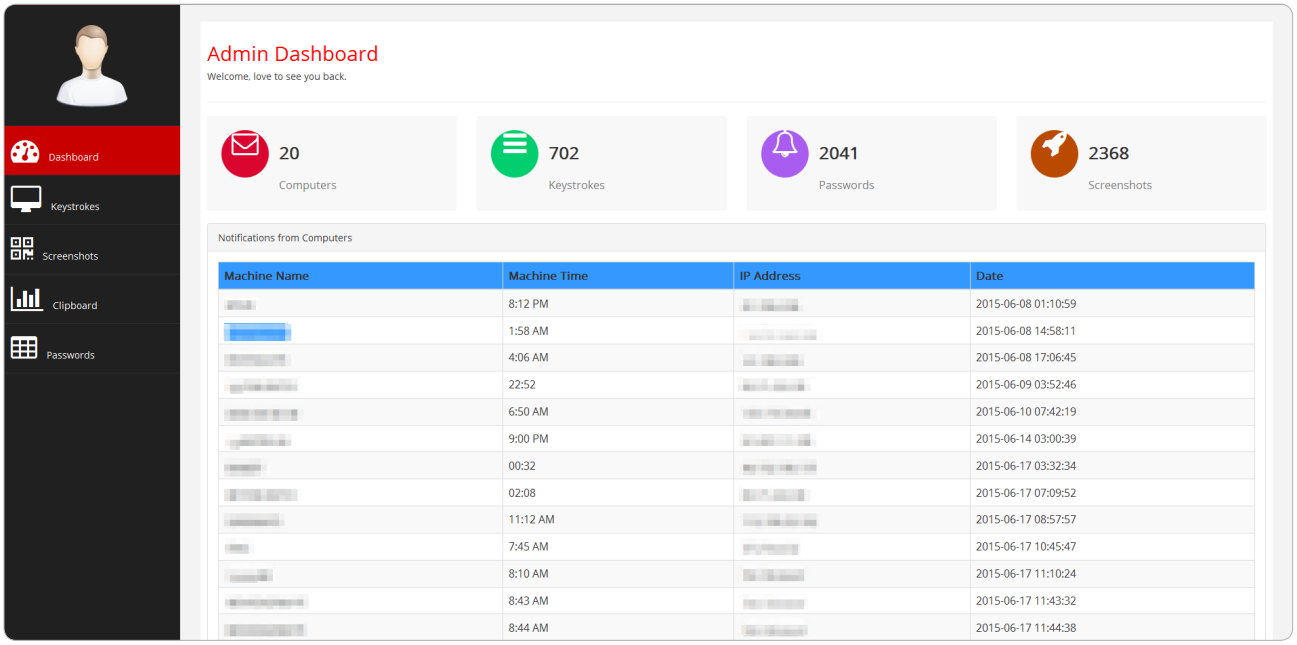


Reconnaissance

The scammers infect their victims' computers and then wait patiently for the victims' keylog files to be uploaded to the CnC server. To help them monitor their victims' logs, they utilize web interface panels like the one shown in Figure 17. More seasoned scammers typically have more than one repository. For example, one scammer had access to a server with over 2.5GB of HawkEye text logs and screenshots, while another server hosted KeyBase logs and screenshots.

These scammers consult these logs on a daily basis to determine which accounts are of interest. They primarily seek out email accounts from companies that deal with purchase transactions. Since the scammer's primary goal is to divert payments from ongoing transactions into their bank accounts, these victims are the most valuable to them. Once the scammers identify an interesting victim, they log into the victim's accounts using the stolen credentials and study the different transactions in which the victims are involved.

Figure 17: KeyBase web panel



Thread Hijacking

When reviewing the victim's emails, the scammers look for threads about legitimate transactions that they might be able to "hijack." They look for emails that contain payment details, refunds, new purchase orders, and recurring purchase orders. Once the scammer has identified a favorable email thread discussing a transaction, they hijack the thread. By playing man-in-the-middle between the buyer and the seller, the scammers relay legitimate information between the parties to avoid suspicion while injecting their own twist to accomplish their goals.

Scammers play "man-in-the-middle," relaying information between buyers and sellers to obtain details from each.

The scammer executes the hijacking process using a homograph (spoofing) attack[5] in which they buy domains and create email accounts that look very similar to both the buyer's and the seller's. They then copy the ongoing thread using the newly created email accounts and continue the respective conversations. They forward product inquiries received from the buyers to the sellers. Typically, they also forward quotes or invoices from the sellers to the buyers. Some scammers also infect the documents being relayed to gain access to the other party's account.

The email thread shown here demonstrates an actual scenario where the scammer plays both sides of the transaction. We have changed the email addresses and altered some information in the email to protect the victims. Figure 18 shows the original transaction thread wherein valid email addresses are being used. Take note that the email addresses contain the word "glass" with a lowercase "G."

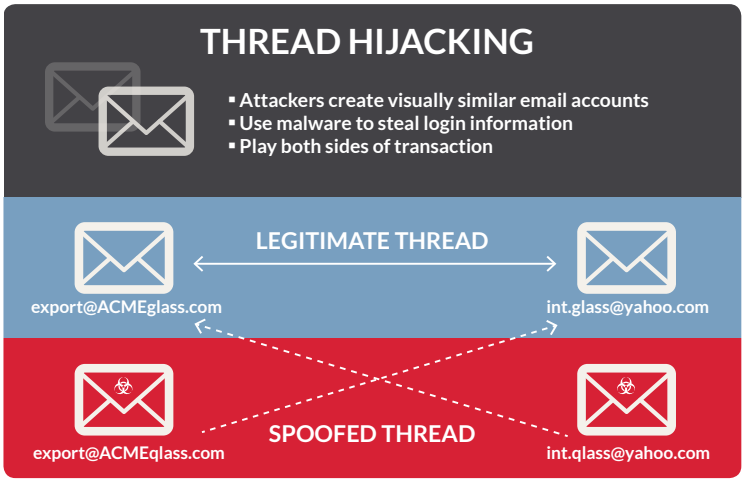
Figure 18: Original transaction thread with valid email addresses using 'glass'

From: John [mailto:export@ACMEglass.com]
Sent: Tuesday, April 28, 2015 3:54 PM
To: 'International glass' <int.glass@yahoo.com>
Subject: RE: URGENT ATTN NEEDED

Dear Sir,

Please find attached Proforma Invoices for order of 50+ FCL orders, we need the advance payment for this order complete, after we will split your order as your request.

Figure 19: Spammers hijack a legitimate email thread and relay info to gain access



[5] https://en.wikipedia.org/wiki/IDN_homograph_attack

In Figure 20, we see the scammer using a spoofed email address where they spelled "glass" with a lowercase "Q". They pretend to be the buyer sending an email to the supplier asking for changes to the invoice.

They also send an email to the supplier from a spoofed email address of the buyer, as shown in Figure 21. Notice they again spelled "glass" with a lowercase "Q."

Since the thread was legitimately established before the scammer hijacked it and the scammer copies the names and signatures of the original emails, both parties seldom realize that they are dealing with the scammer. The only difference is the spoofed email address, which would be hard to spot if the victim is not paying close attention.

Figure 20: Scammer pretending to be the buyer talking to the seller using spoofed email address ('qlass' vs 'glass')

From: International glass [mailto:int.qlass@yahoo.com]
Sent: Wednesday, April 29, 2015 11:57 AM
To: John <export@ACMEglass.com>
Subject: RE: URGENT ATTN NEEDED

DEAR John,

PLS. UNDERSTAND SIR, WE WANT TO ESTABLISH LONG TERM SMOOTH BUSINESS WITH YOU.

AS DISCUSSED IN OUR MEETING, WE ORDER 50+ FCL BUT I HAD CLEARLY TOLD THAT WE WILL TAKE 4 PI SEPARATELY AND SHIPMENTS WILL BE MADE ONE AFTER OTHER ..

SO PLS. ISSUE 4 PI AS REQUESTED WE WILL SEND ADVANCE T.T OF 30% FOR 1ST PI WITHIN A DAY.

IN FACT WE WANT TO DO MORE BUSINESS WITH YOUR SUPPORT AND COOPERATION. AND WE WILL NEVER LET YOU DOWN FOR ANY REASON.

WE AWAIT YOUR 4 PI AS REQUESTED.

Figure 21: Scammer pretending to be the seller talking to the buyer using spoofed email address ('qlass' vs 'glass')

From: John [mailto:export@ACMEqlass.com]
Sent: Tuesday, April 29, 2015 6:43 AM
To: 'International glass' <int.glass@->
Subject: RE: URGENT ATTN NEEDED

Dear Sir,

Pls remit the advance payment to our Euro Account. Adhere to this Proforma Invoice as attached.

Currency of transfer transaction = EURO

Payment Diversion

At this point, the scammer has insight to both sides of the trade conversation. They wait for an opportune moment to divert any payments made by the buyer to the scammer's bank account. We speculate that associates or hired individuals act as money mules and open these bank accounts in foreign countries on behalf of the scammers, as shown in Figure 22.

To divert funds from the transaction, the scammers provide the buyer with "updated" bank details for a bank account the scammer controls. The emails they send to change bank details vary from scammer to scammer but they all convey a similar message. For examples, see Figures 23 and 24.

Figure 22: Scammer leaving words of wisdom to fellow scammer about banks in India

[[REDACTED] - 3/27/2015 7:12:23 AM]

have this in mind that nigerians dont open acct in india

its indian people that opens acct

and then give to them

so, any india acct they must collect from an indian person or an indian banker

i have explained this thing before

Figure 23: Sample email using the payment diversion tactic

[????6.0? - Mozilla Firefox - 3/19/2015 8:32:28 AM]

Kindy Note that all the invoices that carries our Old Bank Details remains valid, Only Bank Acct details will be changed to a new Bank details from noow because our Bank just informed us that Our Bank details was suspended due to remmitance of bad check and money order from one of our customers.

Kindly stop all payments you have already transferred to our old bank details, I will give to you our new Bank details to transfer money.

Please confirm this, Very Important.

Awaiting your reply.

Figure 24: Sample email using the payment diversion tactic

[Write: Re: Fwd: [REDACTED] - Payment USD. 221,404.90 and USD. 219,990 // [REDACTED] // h - 3/17/2015 2:04:10 AM]

kindly stop all T/T payments to our accounts.

Our account is undergoing review due to high taxes we have incured doing business.

We have been adviced to discontinue use until the audit is over.

I will send you our raw material account tomorrow in an authorization on how to pay us for invoice

Please send all messages to me and **[REDACTED]** directly so that we can handle with our bank to enable us release your documents on time.

Scammers pressure their victims to change banking information and send their payment.

The scammers even follow up with the victim to encourage them to use the new bank information and to make sure that the payment has been completed, as shown in Figure 25.

Occasionally, the victim is reluctant to change the banking information as instructed, so the scammer must adapt and pressure the victim into sending the money. The scammer can use the information gleaned from the captured conversations and transactions to aide in convincing their victim. In Figure 26, the scammer pressures what we assume is a clerk to complete the wire transfer.

Figure 25: Follow-up email from scammer

[SquirrelMail - Google Chrome - 11/21/2014 6:08:53 AM]

Kindly advice me if you paid through our raw material account as instructed because i am not seeing the swift code in the attachment

Please reply urgently

[SquirrelMail - Google Chrome - 11/21/2014 8:35:10 AM]

Its okay because we informed you late. Please all other payments should be made through our raw material account so that we won't lose money. Please advice when other payment can be made.

[SquirrelMail - Google Chrome - 11/21/2014 8:44:42 AM]

[REDACTED]

I want to confirm to you that the Account on the attachment is our raw material account with the name **[REDACTED].**

We are using this account for now due to high taxes there by making use to lose money.

Please send the USD 900.000 and the E300.000

Please go ahead and make the payments

Figure 26: Scammer putting pressure on the victim

[Outlook.com – [REDACTED]@hotmail.com - Mozilla Firefox - 3/17/2015 10:33:31 AM]

I can see that you are not ready to transfer money. I already told you that i am on a business trip and cannot get messages and limited time for calls.

Why all this questions?

Just to transfer money to a customer and you are raising too many questions which i cant understand.

Please answer me yes or no if you can transfer money so that i can inform our indian customer as he is disturbing me to know if money is transferred or not.

Once the payment has been completed, the scammers contact their accomplice – a 'money mule' – to alert them of the new transaction. In Figure 27, the scammer contacts an accomplice who has either a familial or romantic relationship with the scammer.

The scammer continues to contact their accomplice after they get a confirmation of the wire transfer, as shown in Figure 28. In these emails, the scammer reveals that they transferred money to their accomplice's personal and business accounts. He also suggests that his accomplice should open an additional business account for future transactions.

With this single transaction, the scammer is slated to collect over $1 million. We believe that they launder their money through a few strategies such as buying gold and luxury items, or mixing the money they have obtained through these scams with money collected legitimately.

Figure 27: Scammer contacting their Indonesian accomplice

[Outlook.com – [REDACTED] - Google Chrome - 11/21/2014 9:24:14 AM]

Honey please advice your bank that you will be receiving USD 900,000 in your Indonesia Rupiah and Eur 300,000 in your dollar account. They will convert it to Rupia from Dollar and Euro to Dollar

Please fine what to tell them honey

So that they won't disturb the money okay

I love you

[REDACTED]

Figure 28: Scammer continuing to follow up with accomplice after transaction is completed

[Outlook.com - [REDACTED] - Google Chrome - 11/24/2014 12:21:53 PM]

Honey check the attachment

The money is over 1millon dollars

Please try to open a company account so that after the project they will pay all my money to you before i get to Indonesia

i love you

[Outlook.com - [REDACTED] - Google Chrome - 11/24/2014 3:28:58 PM]

Honey check the attachment, my client has already sent you money yesterday you will recieve it today

did you take a look at the attachment?

They sent Eur 302.641.00 to your dollar account and Usd 895,219.21 in your company account honey

The total money is a million dollars

Please check the attachment in my last message

Please let me know once you receive the money

I love you

[Outlook.com - [REDACTED] - Google Chrome - 11/24/2014 3:50:49 PM]

look at the attachment

please remember to tell them its for business incase they ask

[Outlook.com - [REDACTED] - Google Chrome - 11/25/2014 1:06:59 PM]

Honey

Please go to the bank and confirm if you have recieved the money

I love you

Conclusion

Payment scams have evolved since the mid-80s with the help of new technology. Today, scammers use malware to steal credentials and rely on stolen credentials to impersonate and manipulate their victims. While 419 scams are easy to spot, payment diversion fraud is trickier to detect because the scammers hijack email threads about legitimate business transactions.

To avoid being a victim of these scams, we recommend the following:

- Use two-factor authentication for any sensitive accounts, including email accounts. If cybercriminals somehow obtain your password, they still would need access to your one-time tokens.
- Never open an attachment from an unknown source.
- Pay close attention during business transactions and be skeptical of sudden changes such as updated bank account information.
- Contact the other party directly (such as via phone) to validate transaction details.
- Pay attention to email addresses and not just names displayed on the email, as scammers can establish email accounts that look very similar to legitimate ones.

Acknowledgment

We would like to thank Michael Shoukry for all his help.

To learn more about FireEye, visit:
www.fireeye.com/reports.html

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