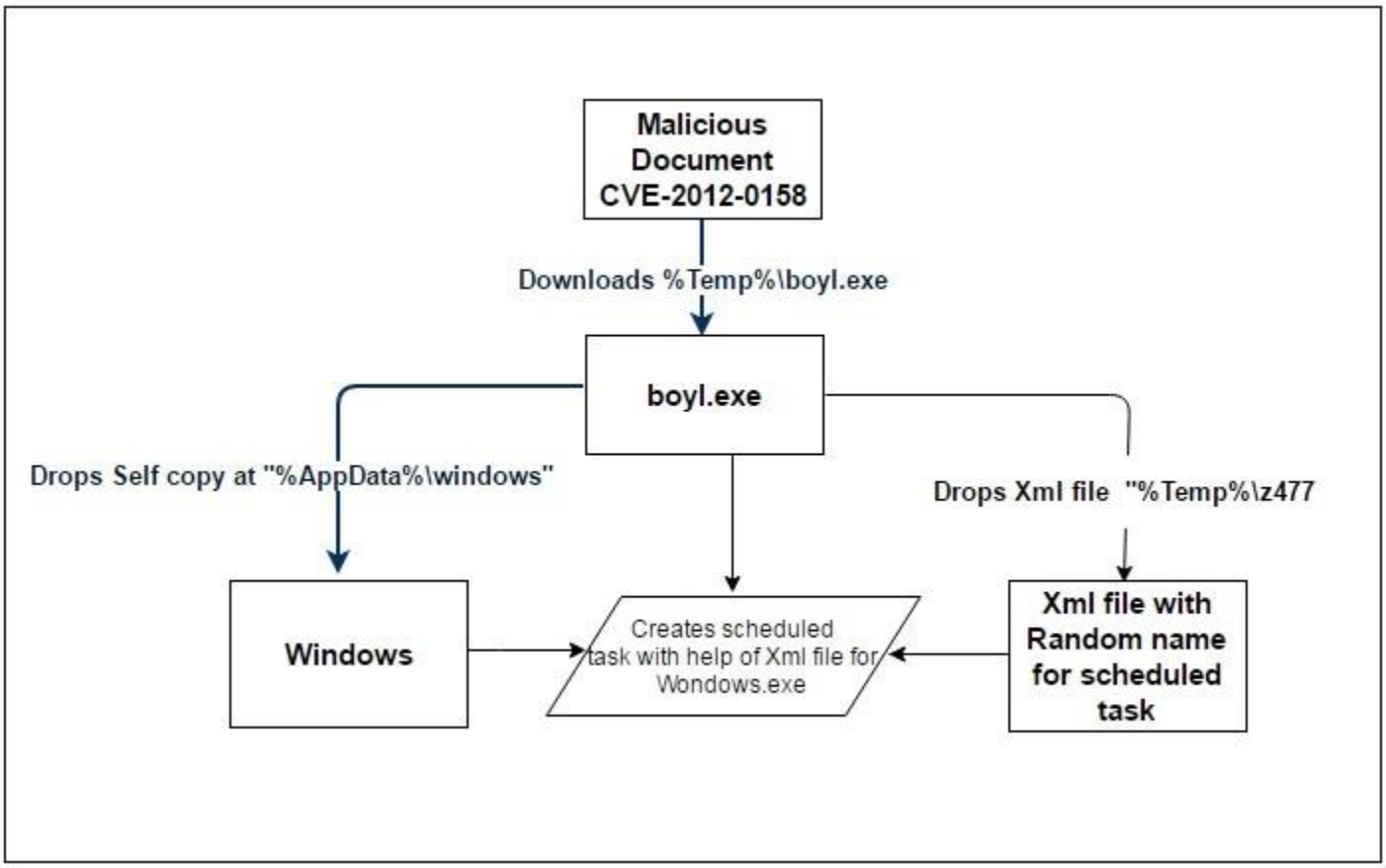
Infection Vector
The malicious document (CVE-2012-0158) received via email, downloads an executable in %Temp% folder and executes the same.



Activity of RTF file

MD5: f64d50cd17304eeb102a27869df86101
CVE: CVE-2012-0158

The RTF file is specially crafted which downloads an executable file from "http://cruisemillato.com/logs/boyl.exe" at location "%Temp%\boyl.exe" and executes the same.

Activity of boyl.exe:
To evade detection by antivirus software, this binary is obfuscated with Confuser 6.0.

The following activities are observed:

1. The executable copies itself to "%AppData%\windows"
2. Drops Xml file named "z477" at "%Temp%\z477" which contains properties of scheduled task to be created.
3. Drops main component as "%Temp%\Pony.exePony.exe" and executes it and then deletes it.

Persistence

To remain persistent in the infected system, it creates a scheduled task with the help of "%Temp%\z477" xml file using "C:\WINDOWS\system32\schtasks.exe" /Create /TN "Update\windows" /XML %Temp%\z477".

The XML file contains following code:

```
    <Principals>
        <Principal id="Author">
            <UserId>SYSTEM1\Base6</UserId>
            <LogonType>InteractiveToken</LogonType>
            <RunLevel>LeastPrivilege</RunLevel>
        </Principal>
    </Principals>

    <Settings>
        <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>
        <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
        <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
        <AllowHardTerminate>false</AllowHardTerminate>
        <StartWhenAvailable>true</StartWhenAvailable>
        <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
        <IdleSettings>
            <StopOnIdleEnd>true</StopOnIdleEnd>
            <RestartOnIdle>false</RestartOnIdle>
        </IdleSettings>
        <AllowStartOnDemand>true</AllowStartOnDemand>
        <Enabled>true</Enabled>
        <Hidden>false</Hidden>
        <RunOnlyIfIdle>false</RunOnlyIfIdle>
        <WakeToRun>false</WakeToRun>
        <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
        <Priority>7</Priority>
    </Settings>

    <Actions Context="Author">
        <Exec>      <Command>%Appdata%\windows</Command> </Exec>
    </Actions>
</Task>
```

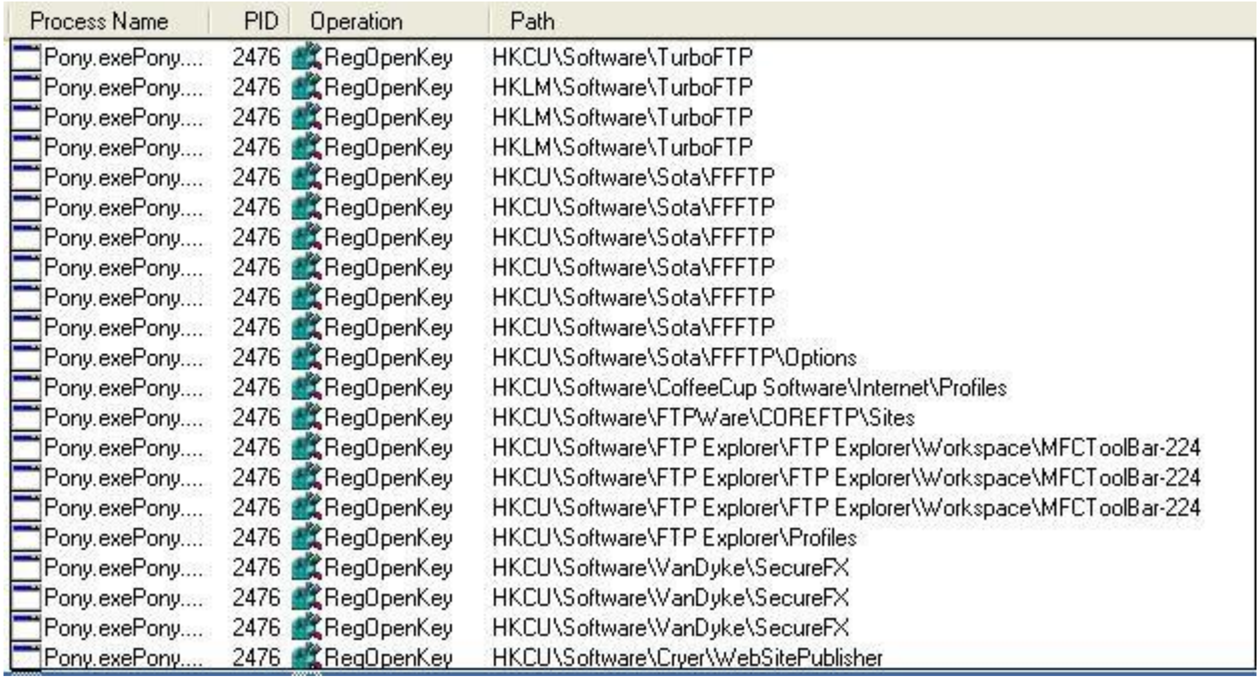
Activity of "Pony.exePony.exe"

This is a UPX packed file. It is the main pony stealer that steals passwords and sends the information to "http://cruisemillato.com/images/boylogs/gate.php"

The following list contains usernames and passwords that the malware has collected for admin:

```
123456 password phpbb qwerty 12345 jesus 12345678 1234 abc123 letmein test love 123 passwo
dragon trustno1 111111 iloveyou 1234567 shadow 123456789 christ sunshine master computer p
football angel jesus1 123123 whatever freedom killer asdf soccer superman michael cheese i
fuckyou blessed baseball starwars 000000 purple jordan faith summer ashley buster heaven p
hunter lovely andrew thomas angels charlie daniel 1111 jennifer single hannah qazwsx happy
654321 amanda nothing ginger mother snoopy jessica welcome pokemon iloveyou1 11111 mustang
jasmine orange testing apple michelle peace secret 1 grace william iloveyou2 nicole 666666
fuckyou1 asshole hahaha poop blessing blahblah myspace1 matthew canada silver robert forev
rainbow guitar peanut batman cookie bailey soccer1 mickey biteme hello1 eminem dakota sama
taylor forum john316 richard blink182 peaches cool flower scooter banana james asdfasdf vi
123321 startrek george winner maggie trinity online 123abc chicken junior chris passw0rd a
merlin google friends hope shalom nintendo looking harley smokey 7777 joseph lucky digital
bandit enter anthony corvette hockey power benjamin iloveyou! 1q2w3e viper genesis knight
foobar adidas rotimi slayer wisdom praise zxcvbnm samuel mike dallas green testtest maveri
mylove church friend god destiny none microsoft 222222 bubbles 11111111 cocacola jordan23
loving nathan emmanuel scooby fuckoff sammy maxwell jason john 1q2w3e4r baby red123 blabla
chelsea 55555 angel1 hardcore dexter saved 112233 hallo jasper danielle kitten cassie stel
windows mustdie gates billgates
```

The malware makes access to the registry keys to check whether the following applications are installed or not.



Process Name	PID	Operation	Path
Pony.exePony....	2476	RegOpenKey	HKCU\Software\TurboFTP
Pony.exePony....	2476	RegOpenKey	HKLM\Software\TurboFTP
Pony.exePony....	2476	RegOpenKey	HKLM\Software\TurboFTP
Pony.exePony....	2476	RegOpenKey	HKLM\Software\TurboFTP
Pony.exePony....	2476	RegOpenKey	HKCU\Software\Sota\FFFTP
Pony.exePony....	2476	RegOpenKey	HKCU\Software\Sota\FFFTP
Pony.exePony....	2476	RegOpenKey	HKCU\Software\Sota\FFFTP
Pony.exePony....	2476	RegOpenKey	HKCU\Software\Sota\FFFTP
Pony.exePony....	2476	RegOpenKey	HKCU\Software\Sota\FFFTP
Pony.exePony....	2476	RegOpenKey	HKCU\Software\Sota\FFFTP
Pony.exePony....	2476	RegOpenKey	HKCU\Software\Sota\FFFTP\Options
Pony.exePony....	2476	RegOpenKey	HKCU\Software\CoffeeCup Software\Internet\Profiles
Pony.exePony....	2476	RegOpenKey	HKCU\Software\FTPWare\COREFTP\Sites
Pony.exePony....	2476	RegOpenKey	HKCU\Software\FTP Explorer\FTP Explorer\Workspace\MFCToolBar-224
Pony.exePony....	2476	RegOpenKey	HKCU\Software\FTP Explorer\FTP Explorer\Workspace\MFCToolBar-224
Pony.exePony....	2476	RegOpenKey	HKCU\Software\FTP Explorer\FTP Explorer\Workspace\MFCToolBar-224
Pony.exePony....	2476	RegOpenKey	HKCU\Software\FTP Explorer\Profiles
Pony.exePony....	2476	RegOpenKey	HKCU\Software\VanDyke\SecureFX
Pony.exePony....	2476	RegOpenKey	HKCU\Software\VanDyke\SecureFX
Pony.exePony....	2476	RegOpenKey	HKCU\Software\VanDyke\SecureFX
Pony.exePony....	2476	RegOpenKey	HKCU\Software\Cryer\WebSitePublisher

List of applications targeted by Pony to steal passwords:

FAR Manager	FTPGetter	Pocomail	Fling	Easy FTP	MegaCoin
Total Commander	ALFTP	IncrediMail	SoftX	Xftp	Quarkcoin

WS_FTP	Internet Explorer	The Bat!	Directory Opus	FTP Now	Worldcoin
CuteFTP	Dreamweaver	Outlook	FreeFTP	Robo-FTP	Infinitecoin
FlashFXP	DeluxeFTP	Thunderbird	LeapFTP	LinasFTP	Ixcoin
FileZilla	Google Chrome	FastTrackFTP	WinSCP	Cyberduck	Anoncoin
FTP Commander	Chromium	Bitcoin	32bit FTP	Putty	BBQcoin
BulletProof FTP	ChromePlus	Electrum	NetDrive	Notepad++	Digitalcoin
TurboFTP	Nichrome	FTP Disk	FTP Control	FTPShell	Goldcoin
FFFTP	Comodo Dragon	Litecoin	Opera	FTPInfo	Yacoin
CoffeeCup	RockMelt	Namecoin	WiseFTP	NexusFile	Zetacoin
CoreFTP	K-Meleon	Terracoin	FTP Voyager	FastStone	Fastcoin
FTP Explorer	Epic	Armory	Firefox	CoolNovo	I0coin
Frigate3 FTP	Staff-FTP	PPCoin	FireFTP	WinZip	Ya.Browser
SecureFX	AceFTP	Primecoin	Odin Secure FTP	Luckycoin	Craftcoin
UltraFXP	Global Downloader	Feathercoin	WinFTP	NovaFTP	Junkcoin
FTPRush	FreshFTP	NovaCoin	FTP Surfer	Becky!	Tagcoin
WebSitePublisher	BlazeFTP	Freicoin	SeaMonkey	LeechFTP	Bytecoin
BitKinex	NETFile	Devcoin	Flock	MyFTP	Florincoin
ExpanDrive	GoFTP	Frankocoin	Mozilla	sherrod FTP	Phoenixcoin

Communication Server

The malware collects usernames and passwords for most of the used FTP clients and Bitcoin wallets and sends the collected data to http://cruisemillato.com/images/boylogs/gate.php

Other communication servers found include:

http://www.pohniq.org.in/Sellyfeb16-march16/gate.php

http://www.pohniq.org.in/Sellyfeb16-march16/admin.php

http://www.pohniq.org.in/Sellyfeb16-march16/config.php

Following is some information collected from cruisemillato.com:

Root Directories found
The malware has 4 sub-directories that are found on Command and Control server which hosts binary files as well as Control Panel's code as php files.

Binary files found

The 'logs' directory contains around 20 executable files, as shown in the following list. The name of each binary file starts with the campaign's name.

Campaigns Found

There are four different campaign folder found in the 'images' directory. Their names are:

1. Boy
2. Bro
3. Croo
4. Kpa

Each campaign has its control panel as shown below:

How malware author creates a new campaign

Malware authors use automation tools to create control panel for new campaigns as shown in the below images.

Start of campaign

The dates of the following Personal Information Exchange (.pfx) files found on server signifies that the campaign started on or before 15 March 2016.

MD5's found in the campaigns

- 596A4EB6A31667C676C2FDD188A46F11
- CA6A7754F7CA87F6B87EF2D32156B5EF
- CA30750EF23FB3D22346492C94E23F30
- C64DF076F6A2B821CD90BB143C893D5A
- 9D3AB434994DFA7605AB923DFBB8077D
- 9481E5D1DE4DA66481462334B6F3A254
- F047D2CA7B35B1CDDBFD2DB9AA07EBC5
- 3E48A094C809D4CFC383774E1DF5E101
- 4FA21203A3E80F228486DA65E1FBB0C1
- D351CDBF34EB3412BB50EEB5D3BC70A9
- FB1E3070450CE345F3D29D6115E840DA
- 048827350CCA03E0D53E8A0443641D60
- 2C64585035F03C12BB845C2ECD5AD952

Quick Heal detection statistics for period - 17 March 2016 to 17 April 2016

Detection Name	Detection Count
TrojanPWS.Pony.DL4	2031