

Ransoc Desktop Locking Ransomware Ransacks Local Files and Social Media Profiles | Proofpoint US

By November 14, 2016 Proofpoint Staff

Published: 2016-11-14 · Archived: 2026-04-05 22:30:23 UTC

Overview

[Ransomware](#) has exploded in the last year, becoming the malware of choice for many threat actors because of its easy monetization and ease of distribution, whether via massive email campaigns or through a variety of exploit kits. Proofpoint research suggests that the number of ransomware variants has grown tenfold since December 2015. While most such malware encrypts a victim's files and demands that a ransom be paid in Bitcoins to decrypt them, Proofpoint researchers recently discovered a new variant that scrapes Skype and social media profiles for personal information while it scans files and torrents for potentially sensitive information. Instead of encrypting files, it threatens victims with fake legal proceedings if they fail to pay the ransom.

The Discovery

In the last week of October, our colleague at FoxIT InTELL, Frank Ruiz, pointed us to a new browser locker variant. Unlike traditional encrypting ransomware like Locky, browser lockers are full-screen web apps that prevent users from accessing their operating systems or closing the browser window. In this case, the browser locker displays a fake "Penalty Notice" offering to let the victim "settle [their] case out of court," avoiding the threat of legal actions and much larger penalties for objectionable content and suspicious activity purportedly discovered on the victim's computer (Figure 1).

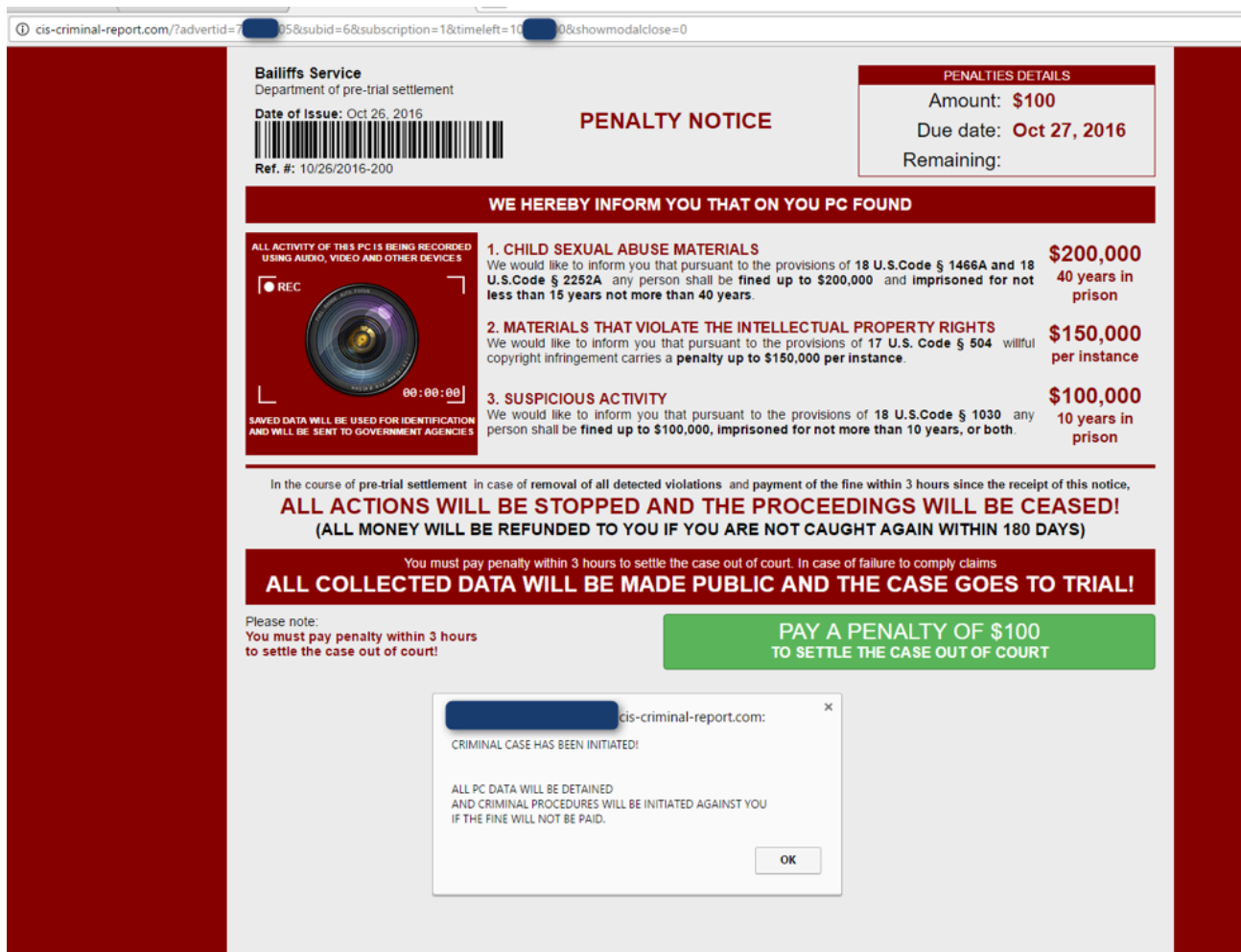


Figure 1: Browser locker “Penalty Notice”

This browser locker was spread in United States via malvertising traffic (primarily fed by the Plugrush and Traffic Shop traffic exchanges on adult websites) aimed at Internet Explorer on Windows and Safari on OS X.

This type of threat was endemic between 2012 and 2014 and was frequently seen spreading concurrently via exploit kit with “Police Locker” malware [1]. Since then, the same kind of traffic has largely focused on exploit kit distribution of crypto ransomware and other malware as well as Tech Support scams in which victims are told to contact a fake tech support service to remove malware from their PCs, usually for a fee to be paid by credit card.

However, in the first week of November, we discovered an unusual malware variant that we believe is tied to the “Penalty Notice” browlock shown in Figure 1 based on visual and thematic similarities and distribution mechanisms. Note, however, that while the browser locker functions cross-platform, the related malware, dubbed Ransoc, is a Windows binary.

Ransoc

In a sandbox environment, we observed this new malware perform an IP check and send all of its traffic through the Tor network. Further examination revealed that the malware scanned local media filenames for strings associated with child pornography.

We also noticed that it was running several routines interacting with Skype, LinkedIn, and Facebook profiles (Figure 2).

```
signed int RunStealers()
{
    signed int v0; // esi@1
    signed int v1; // edi@19
    int v3; // [esp+10h] [ebp-8h]@20

    v0 = 0;
    if ( HIWORD(dword_46AB80) < 0xAu )
    {
        ++HIWORD(dword_46AB80);
        v0 = 1;
        sub_4015F0();
        if ( !sub_406990("ip", (int)IPStealer, 0) )
        {
            HIWORD(dword_46AB80) = 255;
            sub_4015F0();
        }
    }
    if ( (unsigned __int16)dword_46AB7C < 0xAu )
    {
        LOWORD(dword_46AB7C) = dword_46AB7C + 1;
        ++v0;
        sub_4015F0();
        if ( !sub_406990("wifi_location", (int)WifiLocationStealer, 0) )
        {
            LOWORD(dword_46AB7C) = 255;
            sub_4015F0();
        }
    }
    if ( HIWORD(dword_46AB7C) < 0xAu )
    {
        ++HIWORD(dword_46AB7C);
        ++v0;
        sub_4015F0();
        if ( !sub_406990("skype", (int)SkypeStealer, 0) )
        {
            HIWORD(dword_46AB7C) = 255;
            sub_4015F0();
        }
    }
    if ( HIWORD(dword_46AB74) < 0xAu )
    {
        ++HIWORD(dword_46AB74);
        ++v0;
        sub_4015F0();
        if ( !sub_406990("linkedin", (int)LinkedInStealer, 0) )
        {
            HIWORD(dword_46AB74) = 255;
            sub_4015F0();
        }
    }
    if ( (unsigned __int16)dword_46AB74 < 0xAu )
    {
        LOWORD(dword_46AB74) = dword_46AB74 + 1;
        ++v0;
    }
}
```

```
sub_4015F0();
if ( !sub_406990("facebook", (int)FacebookStealer, 0) )
{
    LOWORD(dword_46AB74) = 255;
    sub_4015F0();
}
}
if ( (unsigned __int16)dword_46AB78 < 0xAu )
{
    LOWORD(dword_46AB78) = dword_46AB78 + 1;
    ++v0;
    sub_4015F0();
    if ( !sub_406990("torrent", (int)TorrentStealer, 0) )
    {
        LOWORD(dword_46AB78) = 255;
        sub_4015F0();
    }
}
v1 = 0;
if ( HIWORD(dword_46AB78) < 0xAu )
{
    sub_4287A0((int)&v3, lpParameter);
    ++HIWORD(dword_46AB78);
    v1 = 1;
    ++v0;
    sub_4015F0();
    if ( !sub_406990("global_files", (int)FileStealer, 0) )
    {
        HIWORD(dword_46AB78) = 255;
        sub_4015F0();
    }
}
if ( (unsigned __int16)dword_46AB84 < 0xAu )
{
    if ( !v1 )
        sub_4287A0((int)&v3, lpParameter);
    LOWORD(dword_46AB84) = dword_46AB84 + 1;
    ++v0;
    sub_4015F0();
    if ( !sub_406990("webcam", (int)WebcamStealer, 0) )
    {
        LOWORD(dword_46AB84) = 255;
        sub_4015F0();
    }
}
goto LABEL_28;
}
if ( v1 )
LABEL_28:
    sub_4287D0(&v3);
return v0;
}
```

Figure 2: Code examining Skype and social media profiles

The code also examined folders from Torrent software (Figure 3).

```

4695CF      db      0
4695D0  off_4695D0  dd offset aUtorrent ; DATA XREF: TorrentStealer:loc_4074407r
4695D8      ; "uTorrent"
4695D4  off_4695D4  dd offset aUtorrent ; DATA XREF: TorrentStealer+2D7r
4695D4      ; "uTorrent"
4695D8 ; int dword 4695D8[]
4695D8  dword 4695D8  dd 1Ah ; DATA XREF: TorrentStealer+337r
4695D8  dd offset sub_407330 ; DATA XREF: TorrentStealer+677r
4695E0  dd offset aUuze | ; "Uuze"
4695E4  dd offset aAzureusActive ; "Azureus\\active"
4695E8  dd 1Ah
4695EC  dd offset sub_4073A0
4695F0  dd offset aUuzeLeap ; "Uuze Leap"
4695F4  dd offset aUuzeLeap_resume ; "Uuze Leap\\.resume"
4695F8  dd 1Ah
4695FC  dd offset sub_407330
469600  dd offset aQBittorrent ; "qBittorrent"
469604  dd offset aQBittorrentBT_ ; "qBittorrent\\BT_backup"
469608  dd 1Ch
46960C  dd offset sub_407330
469610  dd offset aDeluge ; "Deluge"
469614  dd offset aDelugeState ; "deluge\\state"
469618  dd 1Ah
46961C  dd offset sub_407330

```

Figure 3: Code examining Torrent folder contents

To determine the nature of the malware's interaction with these services, we ran it manually in our sandbox. We logged into fake social network accounts then closed the browser and launched the Skype desktop application. As suspected, after running the malware, we saw it connecting to the fake Facebook and LinkedIn profiles we created (Figure 4).

R...	Protocol	Requ...	IP	Host	URL	Body	Content-Type
200	HTTP	GET	54.243.91.166	api.ipify.org	/	12	text/plain
200	HTTP	GET	54.169.185.206	ipinfo.io	/geo	123	applicati
301	HTTP	GET	108.174.10.10	linkedin.com	/profile/view	0	
200	HTTP	CON...	108.174.10.10	Tunnel to	www.linkedin.com:443	750	
302	HTTPS	GET	108.174.10.10	www.linkedin.com	/profile/view	0	
200	HTTP	CON...	108.174.10.10	Tunnel to	www.linkedin.com:443	750	
200	HTTPS	GET	108.174.10.10	www.linkedin.com	/profile/view?id=A...	366 307	text/ht
301	HTTP	GET	31.13.64.35	facebook.com	/me/about	0	text/html
200	HTTP	CON...	31.13.64.35	Tunnel to	facebook.com:443	916	
301	HTTPS	GET	31.13.64.35	facebook.com	/me/about	0	text/plain
200	HTTP	CON...	31.13.93.36	Tunnel to	www.facebook.com:443	916	
301	HTTPS	GET	31.13.93.36	www.facebook.com	/me/about	0	text/html
200	HTTP	CON...	31.13.93.36	Tunnel to	www.facebook.com:443	916	
200	HTTPS	GET	31.13.93.36	www.facebook.com	/profile.php?id=...&sk=about	457 205	text/html
200	HTTP	CON...	31.13.93.7	Tunnel to	scontent.xx.fbcdn.net:443	918	
200	HTTP	CON...	23.40.243.104	Tunnel to	media.lcdn.com:443	736	
200	HTTPS	GET	31.13.93.7	scontent.xx.fbcdn.net	/v/t1.0-1/c0.0.160.160/p160x160/...	952	image/jp
200	HTTPS	GET	23.40.243.104	media.lcdn.com	/mpr/mpr/shrinkp_400_400/...	28 206	image/jp

Figure 4: Ransoc capturing photos from social media account profiles

The malware, which we call Ransoc because of its connections to social media, then displayed a Penalty Notice that was visually and functionally similar to the browser locker shown in Figure 1. The new Penalty Notice is shown in Figure 5. It appears that this penalty notice only appears if the malware finds potential evidence of child pornography or media files downloaded via Torrents and customizes the penalty notice based on what it finds. If we manually changed file names to match specific strings, we were able to trigger the penalty notice.

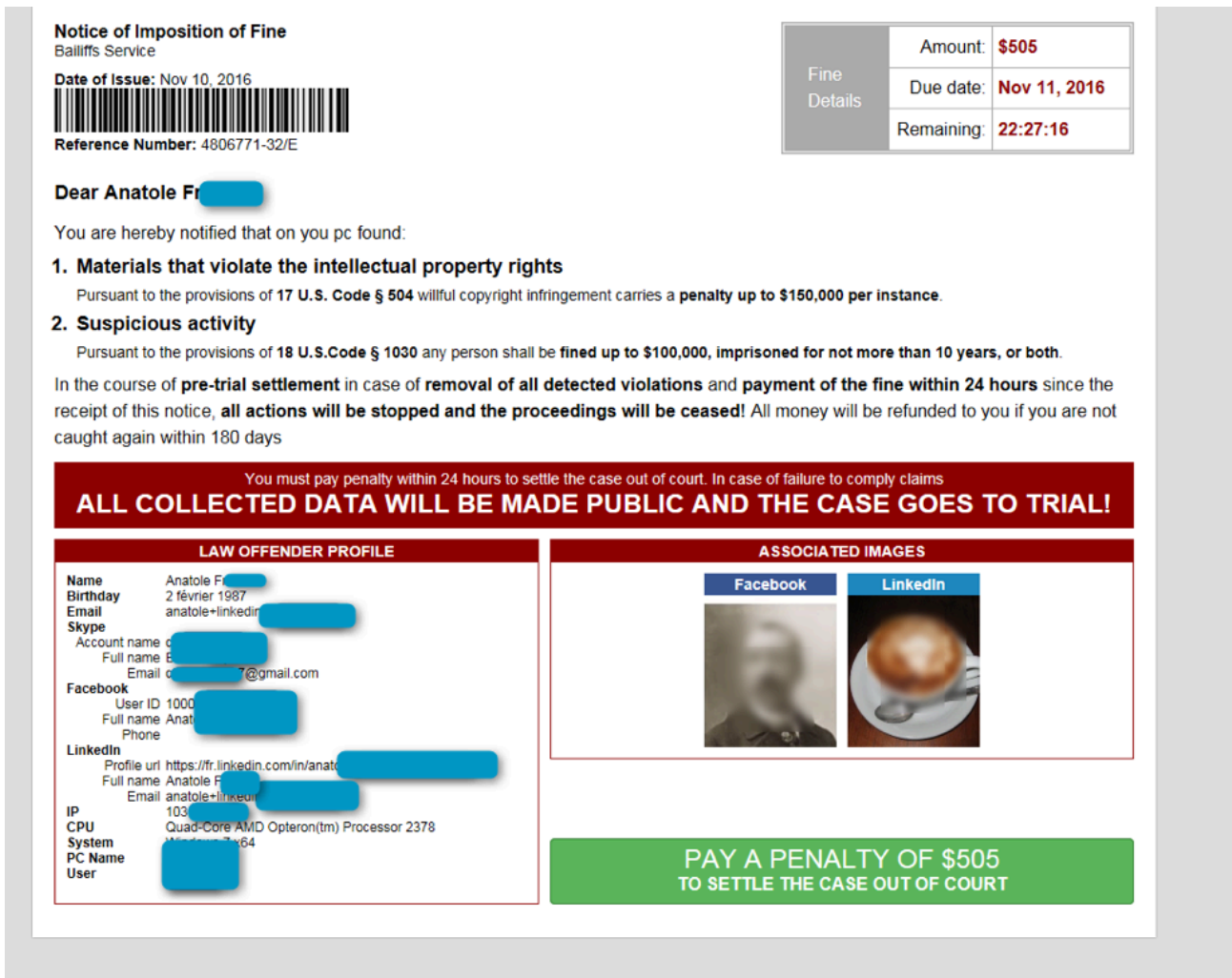


Figure 5: New penalty notice with social media profile information and a threat stating that “All Collected Data will be made public and the case goes to trial!”


The ransom message displays accurate personal data captured from Skype and social media profiles, including profile photos. It threatens to expose the collected "evidence" to the public, with legitimate social profile information being used as a social engineering lure to convince victims that sensitive information may actually be at risk of exposure. Unlike most ransomware variants, the target here is the victim's reputation rather than their files. Ransoc also includes code that may allow it to access a victim's webcam, although we did not verify this functionality.

The ransom message is actually a full-screen window that functions much like the browser locker application shown in Figure 1. However, Ransoc checks every 100ms for regedit, msconfig, and taskmgr, killing the processes before victims have a chance to remove or disable the malware. Ransoc only uses a registry autorun key to persist, though, so rebooting in Safe Mode should allow users to remove the malware. The sample we examined had an HKCU\Software\Microsoft\Windows\CurrentVersion\Run\JavaErrorHandler registry key with a value of a shortcut pathname ending in 'JavaErrorHandler.lnk', although future versions may use a different key.

The payment system (Figure 6) is also unusual.

Notice of Imposition of Fine
Bailliffs Service

Date of Issue: Nov 09, 2016



Reference Number: 4806771-32/E

Fine Details	Amount: \$505.00
	Due date: Nov 11, 2016

Please enter your billing details

Phone:

Email:

ZIP/Postal code:



Country:

State/Province:

City:

Address:

Please enter your credit card details

CardNumber  

VALID THRU 01 / 17

Card Holder

Firstname Lastname

The last three digits

Name of the bank which issued the card

SUBMIT & CONFIRM

Figure 6: Ransoc payment page

Credit card payment is almost unheard of in ransomware schemes. While it removes the hassle and confusion for many victims associated with Bitcoin processing, it also potentially allows law enforcement to trace activity back to the cybercriminal more easily.

This fairly bold approach to ransom payments suggests the threat actors are quite confident that people paying the ransom have enough to hide that they will probably not seek support from law enforcement. In fact, while Ransoc may seem to be motivated by vigilantism against genuine criminals, the motives are likely less-than-altruistic, as the attackers target users who will be unlikely to resist or inform the authorities and thus increase the likelihood of payment. This theory is further bolstered by the fact that most victims encounter this malware via malvertising on adult websites and the penalty notice only appears when Ransoc encounters potential evidence of illegally downloaded media (via BitTorrent) and certain types of pornography. To encourage payment, the ransom note also claims that money will be sent back if the victim is not caught again in the 180 days.

Conclusion

Although exploit kit activity has dropped off precipitously over the past year, malvertising activity remains strong, with threat actors exploring new ways to infect victims and extort money through this vector. By incorporating data from social media accounts and Skype profiles Ransoc creates a coercive, socially engineered ransom note to convince its targets that they are in danger of prosecution for their browsing habits and the contents of their hard drives. With bold approaches to collecting payments, the threat actors appear confident in their targeting, introducing new levels of sophistication to ransomware distribution and monetization.

Indicators of Compromise (IOCs)

Date	Domain	IP	Comment
2016-10-27	cis-criminal-report[.]com	5.45.86.171	Browlock for IE Windows
2016-10-27	criminal-report[.]jin	5.45.86.171	Browlock for Safari OSX
2016-11-03	violation-report[.]jin	5.45.86.171	Browlock for IE and Safari
2016-11-02	latexfetishsex[.]com	78.47.134.204	Intermediate Redirector/TDS
2016-11-03	italy-girls[.]mobi	5.9.86.131	Intermediate Redirector/TDS
2016-11-10	N/A	5.45.86.148	IP found in the Ransoc
sha256			Comment
fee53dc4e165b2aa45c3e7bd100b49c367aa8b7f81757617114ff50a584a1566			Ransoc PenaltyNotice

References

[1] <http://malware.dontneedcoffee.com/2014/05/police-locker-available-for-your.htm>