Приложение 1. Индикаторы компрометации

Директории, создаваемые вредоносной программой

%APPDATA%\Roaming\NTLocalAppData
%APPDATA%\Roaming\LocalDataNT
%APPDATA%\Roaming\NTLocalData

Вредоносные почтовые вложения

Имя файла	MD5
Отраслевая программа закупок ПАО РОСАТОМ.exe	34A1E9FCC84ADC4AB2EC364845F64220
Отраслевая программа закупок ПАО РОСАТОМ (код 917815).rar	59e172ec7d73a5c41d4dbb218ca1af66
OPLATA REESTR skrin dogovor.doc.com	DDCD67B7B83E73426B4D35881789E7DC
doc.pdf.oplat 27.12.2017.rar	
1с пп.pdf	
(№ 444.pdf.com	2374C93EFBE32199B177EB12F96B6166
новый текстовый.txt.com	C531C45B08B692D84CF0699EF92F0134
oplata022018rm.rar	
oplata 1c_2 scan.pdf.com	e5562389a49680c25e67b750b2c368eb
reestr oplat 1c от 01.12.2017.rar	
1C tshetim.rar	3a636038a3d893e441f25696bcbf2c73
1C kopiya №5.pdf.scr	f9b14393b995a655e72731c8b6ce78fd
WinRAR pp.rar	6e10bc85be5d330e9aed5b5c87ccee38
kopiya WinRAR.docx.scr	f8ec2d059d937723becd92eae050a097
act sverki 09.10.2017 crbarin.pdf.com	21ae834bdd5b89bacacca4d51cf82148
ooooplata №489 012018 pdf.com	21089b34d8f9cb7910f521e30aa55908

Иное вредоносное ПО, используемое злоумышленниками или обнаруженное на серверах управления вредоносным ПО

Семейство вредоносной программы	MD5
AzoRult	3463d4a1dea003b9904674f21904f04b
BabylonRAT	075ff2fb2e33a319e56a8955fade154e
BabylonRAT	aa6797ec4d23a39f91ddd222a31ddd1e
Betabot	ba9747658aa8263b446bc29b99c0071f
AzoRult	61aecb3e037e01bc0ad1062e6ff557e6

AzoRult	4fd16e0e8bf3ae4ff155e461b2eccb79
Betabot	db0954a2f9c95737d1e54a1f9cf01404
Delphi Keylogger	ccb184bbb7d257f02e2f69790d33f3b6
BabylonRAT	5f19025a2ac2afeb331d4a0971507131
Betabot	579a5233fe9580e83fb20c2addb1a303
Hallaj PRO Rat	567157989551a5c6926c375eb0652804
AzoRult	5a610962baf6081eb809a9e460599871

Модули вредоносной программы, устанавливаемые в систему

Путь к файлу в зараженной системе	MD5
%APPDATA%\Roaming\NTLocalAppData\winspool.drv	3EE5C1AB93EFE2C4023275B64652D015
	160E19D53A441715B6BF08C4D48B0DAC
	964E8B7A72B5A8013355899A6AC086C7
	5A6EFA2921D3174BB9808FA3A3400D13
	E70F6D97CFA140D34F1D47860F2F7E13
%APPDATA%\Roaming\LocalDataNT\winspool.drv	3ee5c1ab93efe2c4023275b64652d015
	5A6EFA2921D3174BB9808FA3A3400D13
	5b85ad4de2c70479b2b98378410b4b3c
%ALLUSERSPROFILE%\rfusclient.exe	4f980bf18db0bcf44b088ca64b015513
%ALLUSERSPROFILE%\rutserv.exe	442d8a7375e2c60b9975c7fb2fb7370e
%APPDATA%\Roaming\LocalDataNT\msimg32.dll	70c16fce0a489c77345ccfe5aee22e8a
%APPDATA%\Roaming\NTLocalAppData\msimg32.dll	8c4e9016b9b4db809dd312f971a275b1
	16b4ebfdf74db8f730f2fb4d03e86d27
%APPDATA%\Roaming\NTLocalData\rmmzx.exe	7e680f2c66fcb42facd8630cce2abe2c

Легитимные объекты, используемые вредоносным ПО

Путь к файлу в зараженной системе	MD5
%APPDATA%\Roaming\LocalDataNT\seldon1.7-netinstall.exe	f3cb88f1b5e6717b1c45c67f66009afd
%APPDATA%\Roaming\LocalDataNT\vp8encoder.dll	3e6c2703e1c8b6b2b3512aff48099462
%APPDATA%\Roaming\NTLocalAppData\vp8encoder.dll	
%APPDATA%\Roaming\NTLocalAppData\IMG.JPG	42752438b8903a00d17b93ec354643b8

%APPDATA%\Roaming\NTLocalData\IMG.JPG	
%APPDATA%\Roaming\NTLocalAppData\pp.pdf	6c92bfdb0463fd86e0b710444b827b7c

Конфигурационные файлы вредоносного ПО

Путь к файлу в зараженной системе	MD5
%APPDATA%\Roaming\LocalDataNT\InternetId.rcfg	8c5b459d59cde2f045a84947715cd767
	46d0d84f2623a116f39cc9487ac42325
	ffc1424e9bf7481a5b70a58e246fed45
	e2465454004a30e4384ffc6addacebca
%APPDATA%\Roaming\NTLocalAppData\InternetId.rcfg	52f03af53b73c606fb448f897fd61abe
	d94c39cbf88e3b470e39c28cd0c64865
	ee56723bf5fc7ad520c601af692e9537
	a027cb63ce9e3842e2fda29951ac0626
	4ff18a14437332737a7adfaf3fdc8894
	fa7bf66cf0d1ffd8773848cc0e9d97da
%APPDATA%\Roaming\LocalDataNT\notification.rcfg	1397ba437d24a03931720287007a2ce5
	482ad30376b02fc43bd84521dd823f20
%APPDATA%\Roaming\NTLocalAppData\notification.rcfg	9d98fc53cc578cdedd0125b567ba97bf
	7b2b766029ac0ddc25a3f7f6635d5dfa
	0cbd2ed26d8e9e984f2f2211db04673c
	f750453b6eb5cc1a2e83be95980ba9bf
%APPDATA%\Roaming\LocalDataNT\Options.rcfg	7f2f5143ac6fe02518853946b9c6d417
	1ba3c285bb65d9e24e49aab0c42cdba8
	4b346396d67bf113f4b497aa817f66d0
	3111797aa87101fd67573c7669ca4e92
%APPDATA%\Roaming\NTLocalAppData\Options.rcfg	ec2c5f7cff8cfb8d3731e06bdb99d687
	6c71e65f0cc9870472d47cd9b71d8902
	f866f79657b696e901e9f046de62e31e
	3a878d7072511bda3de6adba00c7aeaa
	06813c2f312769e3662afc5c682db1a0

	3bd21d949771d628081b48160cddd213
%APPDATA%\Roaming\LocalDataNT\Password.rcfg	60154c16e8d06c1519188d396c713837
%APPDATA%\Roaming\NTLocalAppData\Password.rcfg	60154c16e8d06c1519188d396c713837
	bd01624c021a36ff960bf92cace9e5bc
	c6b7d274f25667c4c4035b4a08493d0e
%APPDATA%\Roaming\LocalDataNT\tvr.cfg	bdf3f1c6c90ccc8c10a22b48bfbe3fa5
%APPDATA%\Roaming\NTLocalAppData\tvr.cfg	4c93b851992e03c51292d0b956450de1
	3dad56414442ca61ef6810fdf48d5528
%APPDATA%\Roaming\NTLocalData\tvr.cfg	3dad56414442ca61ef6810fdf48d5528

Ключи реестра вредоносной программы

Путь к ключу реестра	**Значение ключа реестра**
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\WinPrint	"%APPDATA%\Roaming\LocalDataNT\WinPrint.exe" r "WinPrintSvc.exe"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\NTAdminSystem	"%SystemDir%\rundll32.exe" "%AppData%\Roaming\NTLocalAppData\winspool.drv",RAI r "NTAdmin.exe"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\NTAdminSystem	%AppData%\Roaming\NTLocalAppData\NTAdmin.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\sys	%ProgramData%\rutserv.exe "
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\SkypeC0SvcService.exe	C:\Windows\system32\regsvr32.exe /s scrrun.dll "C:\Users\user\AppData\Roaming\NTLocalData\msimg32.dll " htvrh666 "C:\Users\user\AppData\Roaming\NTLocalData\SkypeC0SvcService.exe" r
HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\CalendarRecordSetting	Настройки параметров программы
HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\InternetId	
HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\notification	
HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\Options	
HKEY_CURRENT_USER\Software\TektonIT\Remote Manipulator System\Server\Parameters\Password	

Характерные особенности сетевой активности легитимного ПО, используемого вредоносной программой

1. Host: server.remoteutilities.com
2. Host: rmansys.ru
3. Host: rms-server.tektonit.ru
4. User-Agent: Mozilla/4.0 (compatible; RMS)
5. User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate)
6. Подключения к серверам *.teamviewer.com
7. Комбинация следующих полей HTTP заголовка: HTTP/1.0 и Content-Type: image/jpeg.

Серверы, используемые злоумышленниками

Перечисленные веб-ресурсы не имеют отношения к реально существующим организациям; некоторые из доменных имен выбраны злоумышленниками для маскировки под легитимные ресурсы известных компаний.

rosatomgov.ru (IP: 81.177.141.15)
micorsoft.info (IP: 208.91.198.93)
buhuchetooo.ru (IP: 185.51.247.125)
barinovbb.had.su (IP: 185.51.247.169)
barinoh9.beget.tech (IP: 87.236.19.244)
papaninili.temp.swtest.ru (IP: 77.222.57.247)
mts2015stm.myjino.ru (IP: 81.177.135.151)
document-buh.com (IP: 191.101.245.101)

Адреса электронной почты, на которые вредоносное ПО производит отправку сообщений

barinovbb2018@yandex.ru
drozd04m@gmail.com
barinovbb@yandex.ru
barinovbb101@yandex.ru

Приложение 2. Yara-правила для детектирования данной угрозы

```
import "pe"

rule RMS_winspooldrv_dllhijack {
meta:
   description = "winspool.drv malicious file used in RMS RAT"
   hash = "5a6efa2921d3174bb9808fa3a3400d13"
   hash = "bb188e1e92e2be8a1ff009fe22f58f7f"
   version = "1.1"
strings:
        $a1= "Password.rcfg" fullword
        $a2 = "Password.rcfg" wide fullword
        $b1= "winspool.drv" fullword
        $b2= "killrms" wide fullword
```

```
condition:
      uint16(0) == 0x5A4D
           and any of ($a*)
           and all of ($b*)
           and filesize < 100000
}
rule TeamViewer_msimg32_dllhijack {
meta:
   description = "msimg32.dll malicious file used in TeamViewer"
   hash = "16b4ebfdf74db8f730f2fb4d03e86d27"
   hash = "8c4e9016b9b4db809dd312f971a275b1"
   version = "1.1"

strings:
           $a1="msimg32.dll" fullword

condition:
      uint16(0) == 0x5A4D
           and any of ($a*)
           and pe.exports("SvcMain")
           and pe.number_of_exports >6
           and filesize > 50000
           and filesize < 200000
}
```