kaspersky

PseudoManuscrypt: масштабная серия атак с использованием шпионского ПО

Kaspersky ICS CERT

16.12.2021 Version 1.1

В июне 2021 года эксперты Kaspersky ICS CERT обнаружили вредоносную программу, загрузчик которой был схож с загрузчиком вредоносной программы Manuscrypt, которая входит в арсенал APT группы Lazarus. В 2020 году Lazarus использовали Manuscrypt в атаках на предприятия оборонной промышленности разных стран, подробно эти атаки мы описывали в отчёте «Lazarus атакует оборонную промышленность с помощью вредоносного ПО ThreatNeedle».

Любопытно, что для передачи украденных данных на сервер злоумышленников вредоносная программа использует реализацию протокола KCP, которая ранее была замечена только в составе вредоносного ПО, используемого группой APT41.

Обнаруженное вредоносное ПО получило название PseudoManuscrypt.

Загрузчик PseudoManuscrypt попадает в систему посредством Malware-as-a-Service (MaaS) платформы, которая распространяет вредоносные инсталляторы под видом пиратского ПО. В ряде случаев загрузчик PseudoManuscrypt распространялся через ботнет Glupteba (основной установщик которого также распространяется через MaaS-платформу под видом пиратского ПО). Это означает, что тактика распространения вредоносных программ не демонстрирует какой-либо конкретной направленности.

В период с 20 января по 10 ноября 2021 года продукты «Лаборатории Касперского» заблокировали PseudoManuscrypt на более чем 35 000 компьютеров в 195 странах мира. Такое большое количество атакованных систем не характерно ни для группы Lazarus, ни для APT-атак в целом.

Среди атакованных PseudoManuscrypt значительное число промышленных и государственных организаций, включая предприятия военно-промышленного комплекса и исследовательские лаборатории.

Согласно нашей телеметрии, не менее 7,2% всех компьютеров, атакованных вредоносным ПО PseudoManuscrypt, являются частью систем промышленной автоматизации (АСУ ТП) в организациях различных отраслей — инжиниринг, автоматизация зданий, энергетика, производство, строительство, коммунальные услуги и управление водными ресурсами.

Основной модуль PseudoManuscrypt обладает обширными и разнообразными шпионскими функциями. Кража данных VPN-соединений, регистрация нажатий клавиш, создание снимков и запись видео с экрана, запись звука с микрофона, кража данных из буфера обмена и данных журнала событий операционной системы (что также делает возможным кражу данных о RDP подключениях) и многое другое. По сути,

функциональность PseudoManuscrypt предоставляет злоумышленникам практически полный контроль над зараженной системой.

Полный текст отчёта опубликован на портале Kaspersky Threat Intelligence. Если вам нужно больше информации, напишите нам: ics-cert@kaspersky.com.

Технические подробности

Обнаружение загрузчика. Общие данные

В июне 2021 года эксперты Kaspersky ICS CERT обнаружили серию атак, мишенями которой стали организации по всему миру, в том числе государственные и промышленные предприятия.

Внимание экспертов привлекли срабатывания детектирующей логики антивирусных решений, созданной для обнаружения активности APT группы Lazarus. Однако картина происходящего была необычной для того, чтобы однозначно связать вредоносную активность с Lazarus. В частности, обнаруженной вредоносной программой было атаковано как минимум 35 тысяч систем, что значительно больше, чем при таргетированной атаке.

В ходе исследования было установлено, что вредоносное ПО загружает и расшифровывает полезную нагрузку из системного реестра, при этом место расположения полезной нагрузки в реестре уникально для каждой зараженной системы.

Обнаруженный загрузчик имеет общие черты с загрузчиком вредоносной программы Manuscrypt, которую группа Lazarus использовала в 2020 году для атак на оборонные предприятия различных стран. (Более подробная информация об атаке доступна в отчёте «Lazarus атакует оборонную промышленность с помощью вредоносного ПО ThreatNeedle».)

Обе вредоносные программы загружают и расшифровывают полезную нагрузку из реестра, при этом для получения места расположения полезной нагрузки в реестре в обоих случаях используется специальное значение в формате CLSID. Кроме того, таблицы экспорта исполняемых файлов обеих вредоносных программ практически идентичны:

Manuscrypt 2020

```
; Export directory for Loader.dll
;
                dd 0
                dd 59F2C7DCh
                dw 0
                dw 0
                dd rva aLoaderDll
                dd 1
                dd 1
                dd 1
                dd rva off_180015288
                dd rva off_18001528C
                dd rva word_180015290
;
; Export Address Table for Loader.dll
;
off_180015288   dd rva ServiceMain
;
; Export Names Table for Loader.dll
;
off_18001528C   dd rva aServicemain

;
; Export Ordinals Table for Loader.dll
;
word_180015290  dw 0
aLoaderDll      db 'Loader.dll',0
aServicemain    db 'ServiceMain',0
```

PseudoManuscrypt 2021

```
; Export directory for Loader.dll
;
                dd 0
                dd 6099042Fh
                dw 0
                dw 0
                dd rva aLoaderDll
                dd 1
                dd 1
                dd 1
                dd rva off_180002218
                dd rva off_18000221C
                dd rva word_180002220
;
; Export Address Table for Loader.dll
;
off_180002218   dd rva ServiceMain
;
; Export Names Table for Loader.dll
;
off_18000221C   dd rva aServicemain

;
; Export Ordinals Table for Loader.dll
;
word_180002220  dw 0
aLoaderDll      db 'Loader.dll',0
aServicemain    db 'ServiceMain',0
```

Сравнение таблиц экспорта двух вредоносных программ

Помимо этого, обе вредоносные программы имеют схожий формат имён исполняемых файлов:

Manuscrypt 2020	PseudoManuscrypt 2021
%APPDATA%\Temp\BTM0345.tmp	I59RFRLY9J.tmp
ETS4658.tmp$temp\ETS4657.tmp	I59RFRLY9J.tmp
$%temp\ETS5659.tmp	ZWSPAMYXHY.tmp
$temp\ets4658.tmp	L2KPEK1I5J.tmp

Имена исполняемых файлов

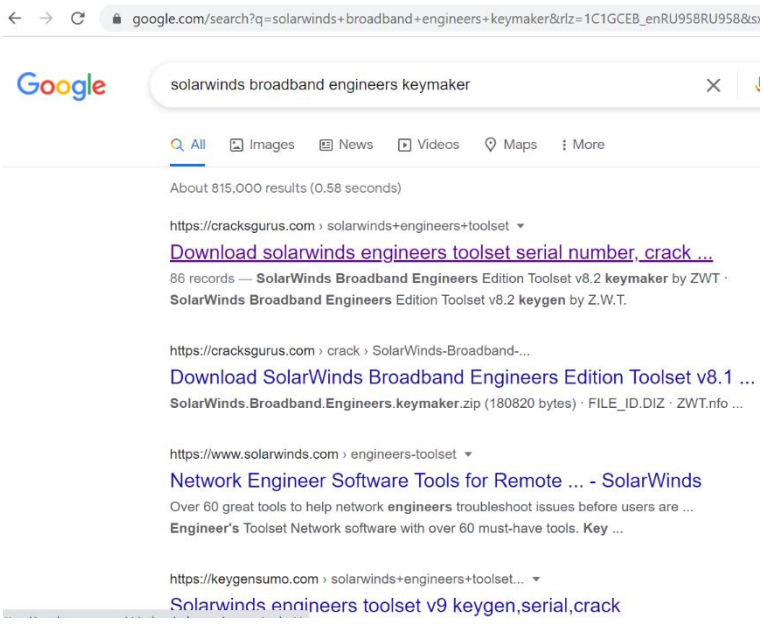
Чтобы подчеркнуть схожесть обнаруженной вредоносной программы с Manuscrypt, при том, что её нельзя однозначно связать с Lazarus, мы приняли решение назвать эту троянскую программу PseudoManuscrypt.

Заражение систем

Загрузчик PseudoManuscrypt попадает на компьютер жертвы через сложную цепочку установок множества других вредоносных файлов и создания множества процессов. Эта цепочка начинается с фейковых архивов инсталляторов взломанного ПО. Ниже даны примеры названий таких архивов, которые включают в себя упоминание ПО самого различного предназначения и профиля:

```
microsoft_office_365_july_keygen_by_keygensumo.zip
windows_10_pro_full_keygen_by_keygensumo.zip
adobe_acrobat_v8_0_keygen_by_keygensumo.zip
garmin_1_serial_keygen.zip
call_of_duty_black_ops_keygen_by_keygensumo.zip
kaspersky_antivirus_keys_july_keygen_by_keygensumo
solarwinds_broadband_engineers_keymaker.zip
modscan32_v8_a00_crack.zip
```

Стоит отметить, что среди этих архивов встречаются и фейковые инсталляторы индустриального ПО, например, приложение для создания устройств MODBUS Master и получения данных с PLC, а также генератор ключей для утилиты от SolarWinds, используемой сетевыми инженерами и системными администраторами.



Вредоносные веб-страницы с инсталляторами в результатах поисковой выдачи

Ресурсы, которые распространяют данные инсталляторы, могут появляться на верхних позициях в результатах поисковых запросов. Это говорит о том,

что злоумышленники активно занимаются их продвижением в поисковой выдаче.

Поток исполнения

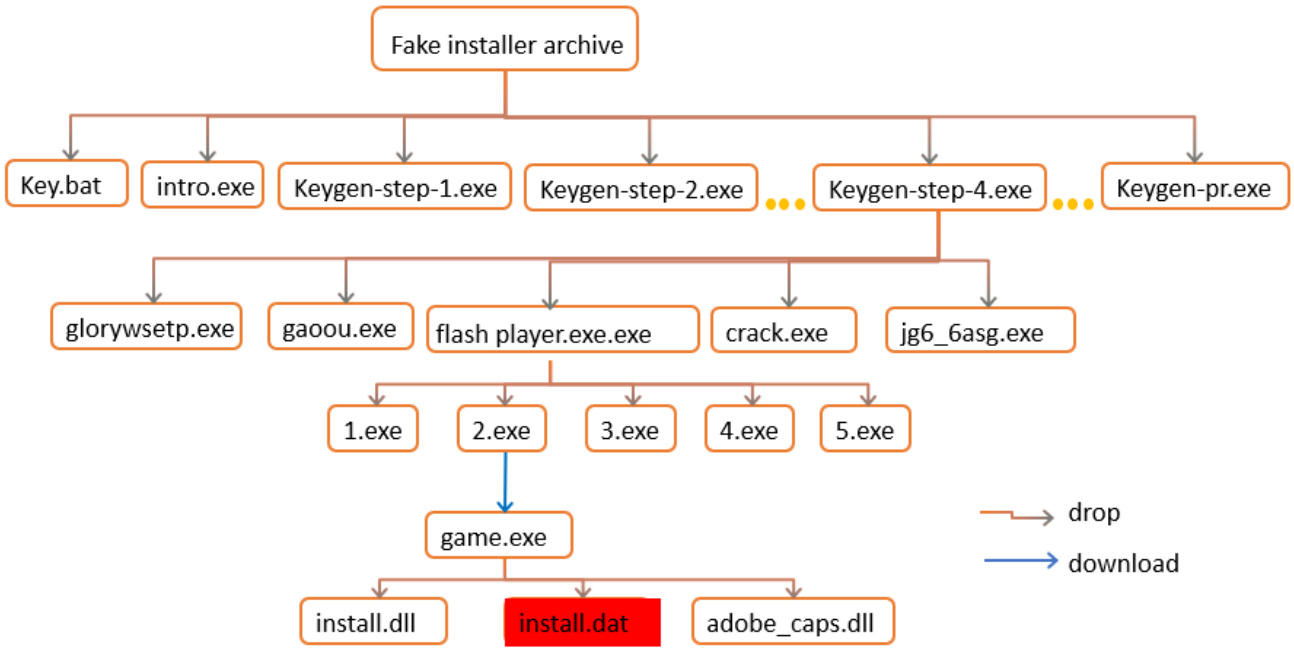
Существует множество вариантов потока исполнения цепочки различных вредоносных программ, приводящих к установке PseudoManuscrypt.

Помимо исследуемого файла, установщики вредоносного ПО скачивают и запускают множество других вредоносных программ, в частности шпионские программы, бэкдоры, майнеры криптовалют и рекламное ПО.

На каждом этапе мы обнаружили большое количество разнообразных устанавливаемых дропперов и скачиваемых модулей, дублирование функциональности модулей в части кражи информации, а также использование каждым из них собственных серверов управления. Это позволяет предположить, что инсталляторы предлагаются злоумышленниками в рамках MaaS-платформы, возможно, многим операторам различных вредоносных кампаний, одной из которых, по-видимому, является кампания распространения PseudoManuscript.

Ниже приведены примеры и фрагменты графов, которые показывают цепочку процессов, ведущих к установке PseudoManuscrypt.

Вариант 1.



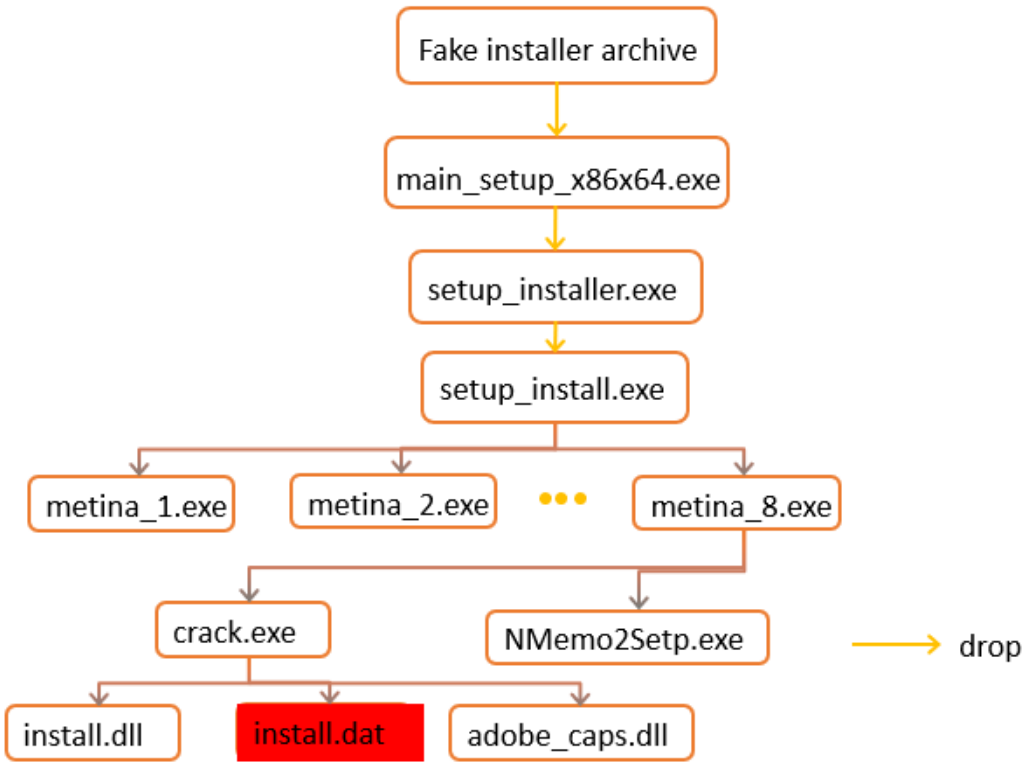
Поток исполнения, вариант 1

В первом варианте:

- из фейкового инсталлятора распаковывается файл key.bat;
- key.bat запускает Keygen-step-4.exe (e41826b342686c7f879474c49c7eed98);
- Keygen-step-4.exe устанавливает и запускает flash player.exe (2aab0ec738374db4e872812a84a0bc11);
- flash player.exe устанавливает и запускает 2.exe (8b9f6b0c98c0afdd75c2322f1ca4d0e8).

Файл 2.exe скачивает по ссылке hxxps://google[.]diragame[.]com/userf/3002/gogonami.exe основной модуль PseudoManuscrypt — game.exe (0001759655eacb4e57bdf5e49c6e7585).

Вариант 2.



Поток исполнения, вариант 2

Во втором варианте:

- из фейкового инсталлятора извлекается файл main_setup_x86x64.exe (1fecb6eb98e8ee72bb5f006dd79c6f2f);
- main_setup_x86x64.exe устанавливает и запускает setup_installer.exe (5de2818ced29a1fedb9b24c1044ebd45);

- setup_installer.exe устанавливает в систему и запускает setup_install.exe (58efaf6fa04a8d7201ab19170785ce85);
- setup_install.exe устанавливает и запускает файл metina_8.exe (839e9e4d6289eba53e40916283f73ca6).

Файл metina_8.exe извлекает и запускает PseudoManuscrypt — crack.exe (89c8e5a1e24f05ede53b1cab721c53d8).

В этом варианте задействована инфраструктура и установщики вредоносного ПО Glupteba (такие как setup_installer.exe). Ботнет Glupteba известен исследователям с 2011 года и представляет собой многомодульную платформу, загружающую в разное время рекламное ПО, шпионское ПО, криптомайнеры, шифровальщики, спам модули и другое ПО, традиционно связанное с киберкриминалом. Платформа Glupteba весьма сложна и использует для распространения внутри атакованной сети множество разных модулей, эксплуатирующих различные уязвимости, в том числе для роутеров, а также руткиты. Поэтому на компьютерах пользователей, инфицированных PseudoManuscrypt с использованием ботнета Glupteba, обнаруживаются еще и руткиты, и модули с эксплойтами EnternalBlue, и прочие модули Glupteba.

В еще одном варианте, описанном BitDefender, инсталлятор PseudoManuscrypt (8acd95006ac6d1eabf37683d7ce31052) скачивался по ссылке hxxps://jom[.]diregame[.]live/userf/2201/google-game.exe — согласно нашей телеметрии, по крайней мере 17 мая 2021. Стоит отметить, что по данной ссылке в разное время загружались различные семейства вредоносного ПО.

Поиск других компонентов вредоносной программы

В ходе поиска других компонентов и версий исследуемой вредоносной программы нам удалось найти более 100 различных версий загрузчика PseudoManuscrypt.

Согласно данным нашей телеметрии, массовое распространение исследуемого варианта загрузчика началось 10 мая 2021 года. Первые же его варианты были обнаружены 27 марта 2021 года — задолго до начала атаки.

Основная часть файлов, обнаруженных в марте, — «тестовые сборки». Разработчик поочерёдно удалял части кода вредоносной программы, пытаясь таким образом понять, какую именно часть кода вредоносной программы ему следует модифицировать, чтобы обойти детектирование антивирусных решений.

В это же время разработчик добавил во вредоносную программу динамический импорт функции VirtualAlloc. Эта функция используется для выделения памяти, необходимой для хранения полезной нагрузки вредоносного ПО, которая загружается из системного реестра.

Любопытным является тот факт, что некоторые тестовые сборки загрузчика содержали комментарии, записанные в поля метаданных исполняемого файла. Данные комментарии написаны на китайском языке, что позволяет предположить, что разработчик вредоносной программы говорит и пишет по-китайски:

property	value
md5	6D5C642BF966CB1D503DA10A0884F5D6
sha1	E35BAA13A24F984C2DAD1626B70BB3A6049EF072
sha256	9E26F0C43BC4E2D767D431A13F121E59594BA5F2919283819AF069A1B3D8B16E
file-type	dynamic-link library
date	empty
language	English-US
code-page	Unicode UTF-16, little endian
CompanyName	TODO: <公司名>
FileDescription	TODO: <文件说明>
FileVersion	1.0.0.1
InternalName	dll.dll
LegalCopyright	Copyright (C) 2021
OriginalFilename	**dll.dll**
ProductName	TODO: <产品名>
ProductVersion	1.0.0.1

Метаданные исполняемого файла вредоносной программы

Основной компонент вредоносного ПО

Наконец, нам удалось обнаружить основной модуль PseudoManuscrypt, который имеет функциональность установки вредоносного ПО в систему, а также содержит полезную нагрузку, которая позволяет понять намерения злоумышленника.

Инсталляция

Основной модуль вредоносной программы записывает свой код в специальный ключ реестра, находящийся в ветке HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID. Имя ключа (значение CLSID) будет уникальным для каждой системы, поскольку формируется на основе ключа реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid,

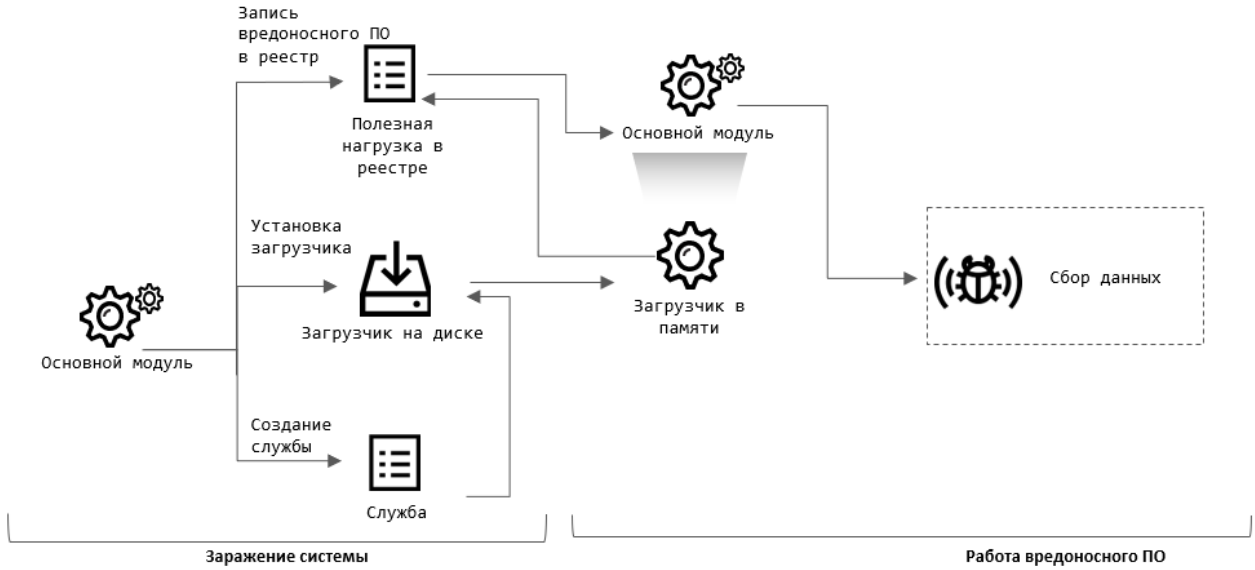
который содержит уникальный идентификатор системы. Код вредоносной программы хранится в реестре в зашифрованном виде.

Далее вредоносная программа извлекает в папку %TEMP% или в папку %WinDir% (в зависимости от модификации вредоносного ПО) компонент-загрузчик, который является DLL-библиотекой и имеет случайное имя файла в формате [0-Z]{10}.tmp, например, I59RFRLY9J.tmp.

Для обеспечения автоматического запуска полезной нагрузки после загрузки системы, троянская программа создаёт сервис, в качестве исполняемого файла которого устанавливается компонент-загрузчик. В первых найденных образцах вредоносного ПО сервис, создаваемый вредоносной программой, имел имя AppService.

Наконец, вредоносная программа добавляет себя в исключения антивирусного решения Windows Defender, модифицируя ключ реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths.

После этого, как и при последующих перезапусках системы, запускается загрузчик вредоносного ПО. Загрузчик использует значение ключа MachineGuid для определения места нахождения полезной нагрузки в системном реестре, загружает, расшифровывает и запускает основной компонент вредоносного ПО.



Установка и запуск вредоносного ПО

Деструктивная активность, версия 1

Первый обнаруженный вариант основного модуля PseudoManuscrypt имеет несколько модулей, общей целью которых является кража конфиденциальной информации с компьютера жертвы.

1. Keylogger. Позволяет вредоносной программе перехватывать коды клавиш, нажатых пользователем на клавиатуре. Помимо кодов клавиш, вредоносная программа также фиксирует имя окна приложения, в которое были введены данные, а также дату и время ввода информации. Данный компонент заимствован злоумышленниками из другой вредоносной программы — Fabookie (Trojan.Win32.Fabookie), которая имеет несколько модулей для кражи аутентификационных данных к различным сервисам и веб-сайтам.

   Из Fabookie авторы PseudoManuscrypt взяли только keylogger и проигнорировали модули, позволяющие осуществить монетизацию атаки кратчайшим способом, — например, модуль для кражи банковской информации с веб-страниц — что может косвенно говорить о целях атаки.

2. Кража данных из буфера обмена. Позволяет злоумышленникам перехватывать информацию, копируемую пользователем, который работает на зараженной системе.

3. Кража данных о VPN подключениях. Вредоносная программа получает содержимое служебных файлов Windows, в которых хранятся данные о VPN подключениях, настроенных на зараженной системе:

   %UserProfile%\Application Data\Microsoft\Network\Connections\pbk\rasphone.pbk

   %ProgramData%\Microsoft\Network\Connections\pbk\rasphone.pbk

   Из указанных файлов троянская программа пытается извлечь следующие данные:

   - Адрес сервера для подключения
   - Логин и пароль, если они сохранены

   Стоит обратить внимание на тот факт, что различные компоненты вредоносной программы работают одновременно, предоставляя из различных источников информацию, которая может быть использована злоумышленниками в совокупности.

   Например, адрес сервера VPN, сохранённый в параметрах подключения, может быть получен вредоносной программой из файла

rasphone.pbk. При этом логин и пароль для подключения может быть перехвачен модулем keylogger. Если пользователь будет копировать параметры подключения через буфера обмена, данные будут перехвачены соответствующим модулем вредоносной программы.

4. Помимо кражи данных о VPN подключениях PseudoManuscrypt имеет функциональность для чтения журналов событий Windows: Application, System и Security. Достоверно нельзя утверждать, для чего именно злоумышленники используют содержимое лог-файлов операционной системы, однако теоретически в совокупности с другими данными, собираемыми вредоносной программой такая информация может быть использована для кражи аутентификационных данных RDP подключений. Это звучит обоснованно, учитывая функциональность вредоносной программы для кражи данных о VPN подключениях.
5. Запись звука с микрофонов, подключенных к зараженной системе. Данная функция активируется по команде с сервера управления вредоносным ПО.

Деструктивная активность, версия 2

В июле 2021 года был обнаружен второй вариант вредоносной программы, в котором злоумышленники расширили шпионскую функциональность. Были добавлены следующие модули:

1. Запись видео с экрана компьютера. Работает в сочетании с другими модулями для перехвата информации, такими как keylogger и модуль для кражи данных из буфера обмена. Запись видео с экрана позволяет злоумышленникам видеть, в какие поля и какие окна пользователь вводил информацию, а также следить за передвижением курсора по экрану и видеть, куда пользователь совершает клики мышью.

   Из интересных особенностей данного модуля можно выделить поддержку прозрачных окон (технология aero peek) и сжатие видео при помощи кодека GNU GPL XviD 1.3.0.
2. Кража аутентификационных данных из мессенджеров QQ и WeChat, популярных в странах Азии.
3. Сбор подробных сведений об установленной системе (версия Windows, номер сборки, Service Pack, информация об установленных обновлениях и издании), а также о роли системы, например, выполняет ли система функцию контроллера домена.

4. Сбор сведений о сетевых подключениях. Вредоносная программа собирает имена сетевых адаптеров, а также информацию о типе подключения (проводное соединение, Wi-Fi, оптоволоконная линия и т.д.).

5. Противодействие антивирусным решениям. Вредоносная программа пытается получить привилегии SeDebugPrivilege и завершить следующие процессы, относящиеся к защитным решениям:

sepWscSvc.exe
HipsTray.exe
UnThreat.exe
DF5Serve.exe
DefenderDaemon.exe
PowerRemind.exe
SafeDogSitelIS.exe
SafeDogTray.exe
SPlDer.exe
f-secure.exe
avgwdsvc.exe
BaiduSdSvc.exe
ServUDaemon.exe
1433.exe
vsserv.exe
remupd.exe
PSafeSysTray.exe
AlilM.exe
mssecess.exe
MsMpEng.exe
QUICK HEAL
QUHLPSVC.EXE
V3Svc.exe
patray.exe
AYAgent.aye
Miner.exe
TMBMSRV.exe
knsdtray.exe
K7TSecurity.exe
QQPCTray.exe
ksafe.exe
rtvscan.exe
ashDisp.exe
avcenter.exe
kxetray.exe
egui.exe
Mcshield.exe
RavMonD.exe
KvMonXP.exe
360sd.exe
360tray.exe
DR.WEB
cfp.exe
DUB.exe
avp.exe

Также вредоносная программа удаляет ключи реестра, относящиеся к сервисам защитных решений, в имена которых входят следующие подстроки:

Symantec
UnThreat
Defender
PowerShadow
QuickHeal
F-Secure
BitDefender
Windows Defender
1433
NOD32

6. Сбор сведений о процессах, которые принимают сетевые подключения по TCP и UDP портам.
7. Одна из функций PseudoManuscrypt удаляет файл с именем «TestDown», лежащий в папке вместе с вредоносной программой, очищает из кэша браузера URL адрес htt[p]://sw.bos.baidu.com/sw-search-sp/software/df60f52e0e897/qqpcmgr_12.7.18996.207_1328_0.exe, снова загружает файл по указанному URL на место файла «TestDown» и присваивает вновь созданному файлу атрибуты скрытый и системный.
8. Очистка журналов событий Windows: Application, Security и System.
9. Запись данных, переданных с сервера управления вредоносным ПО, в системный файл %System32%\drivers\etc\hosts, позволяет злоумышленникам перенаправлять пользователя на вредоносные веб-ресурсы или блокировать доступ к выбранным сайтам.
10. Передача текстовых сообщений между сервером управления и вредоносной программой. Вредоносная программа может открыть окно со своего рода чатом.

    Сервис новой версии PseudoManuscrypt устанавливается в систему под именем "iexplore" и имеет отображаемое имя "System Remote Data Simulation Layeerr". Также новая версия вредоносной программы получила функции обновления своего исполняемого файла и удаления из системы по команде с сервера управления вредоносным ПО.

    Интересно, что один из образцов вредоносного ПО использует IP адрес 192.168.1.2 в качестве прокси-сервера, что может говорить о том, что в некоторых случаях злоумышленники готовят образец вредоносного ПО с учетом особенностей сетевой архитектуры атакуемой организации.

    Также в новой версии PseudoManuscrypt злоумышленники добавили функцию записи кодов клавиш, нажатых пользователем на клавиатуре, в локальный лог-файл: %System32%\9cda11af69ab0a2b6a9167f7131e7b93.key.

    Наконец, при обращении к серверу управления вредоносным ПО новая версия троянской программы передаёт следующие HTTP заголовки:

```
HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/x-shockwave-flash, application/vnd.ms-excel,
application/vnd.ms-powerpoint, application/msword, */*
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
User-Agent:Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Connection: Close
Cache-Control: no-cache
```

Как можно заметить, вредоносная программа ожидает получить ответ на китайском языке.

Передача данных злоумышленникам

Данные, собранные вредоносной программой, передаются на сервер управления вредоносным ПО. В ходе исследования было обнаружено четыре таких сервера: email.yg9.me, google.vrthcobj.com, toa.mygametoa[.]com и tob.mygametob[.]com.

Для подключения к серверу используется протокол KCP. Этот протокол, согласно заявлению разработчиков, работает на 10%-20% быстрее, чем общепринятый сетевой протокол TCP. В ходе создания вредоносной программы злоумышленники воспользовались определённой реализацией протокола KCP.

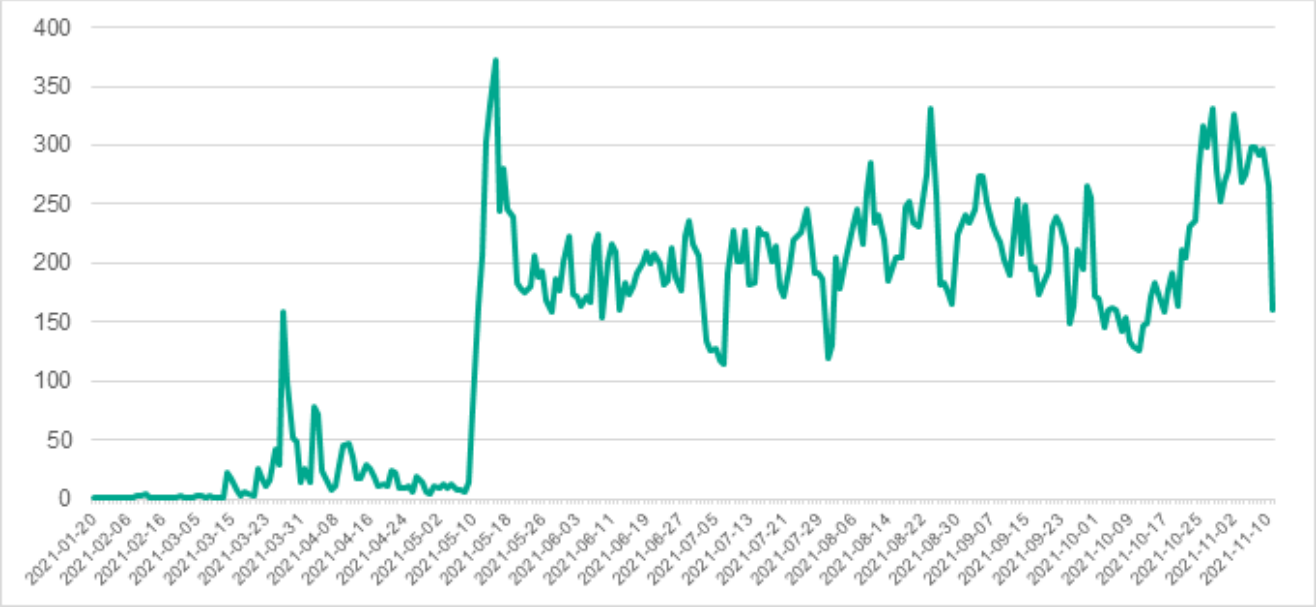
Интересен тот факт, что, согласно отчёту компании FireEye, именно эта библиотека KCP, использованная в PseudoManuscrypt, ранее применялась китайской группой APT41 в атаках на промышленные предприятия различных индустрий, в том числе связанные с инжинирингом и оборонной промышленностью. Согласно результатам анализа доступных коллекций вредоносного ПО, эта библиотека использовалась только во вредоносных программах APT41, исследованных ранее, а также в данной атаке.

Некоторые найденные образцы вредоносной программы также используют выделенный сервер d.diragame.com для отправки информации о заражении системы. Мы считаем, что данный механизм используется для сбора статистики о работе MaaS-платформы.

Жертвы

В период с 20 января 2021 по 10 ноября 2021 года PseudoManuscrypt был заблокирован продуктами Kaspersky на более чем 35 тысячах компьютеров в 195 странах мира.

На графике ниже представлено изменение количества компьютеров, на которых был заблокирован PseudoManuscrypt, по дням. Два очевидных всплеска на графике — 27 марта и 15 мая — указывают на даты выхода/начала распространения новых версий PseudoManuscrypt.

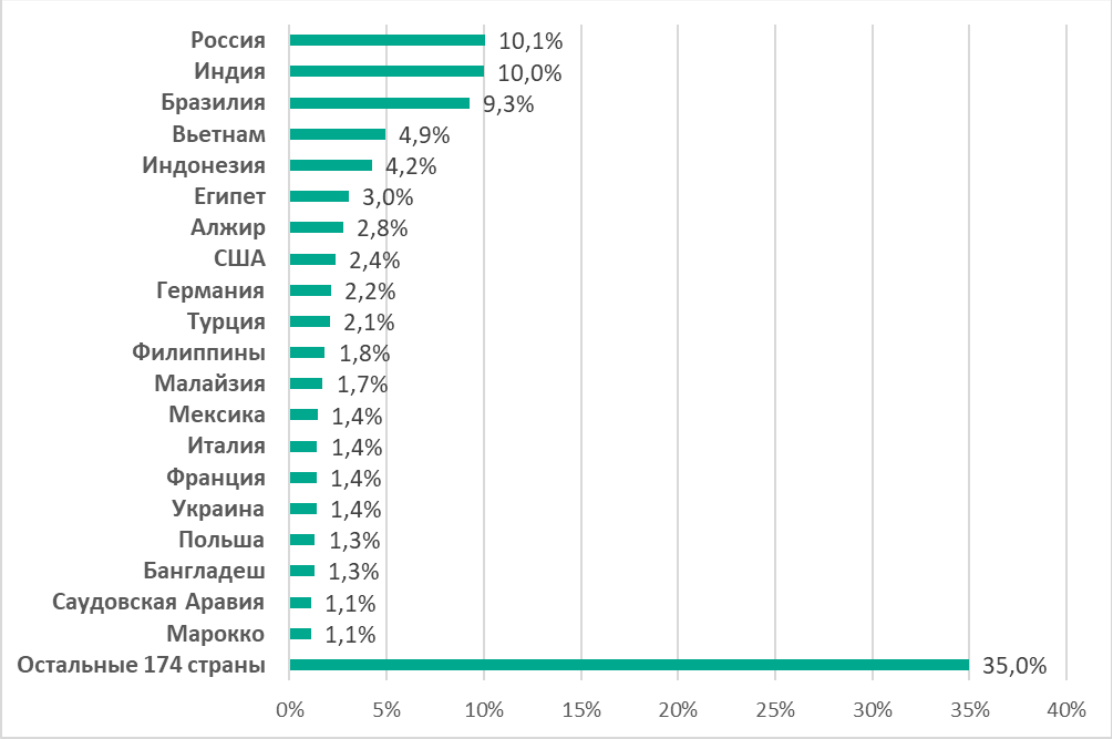


Количество систем, на которых был обнаружен PseudoManuscrypt, по дням

По меньшей мере 7,2% всех компьютеров, на которых был заблокирован PseudoManuscrypt, относятся к АСУ ТП.

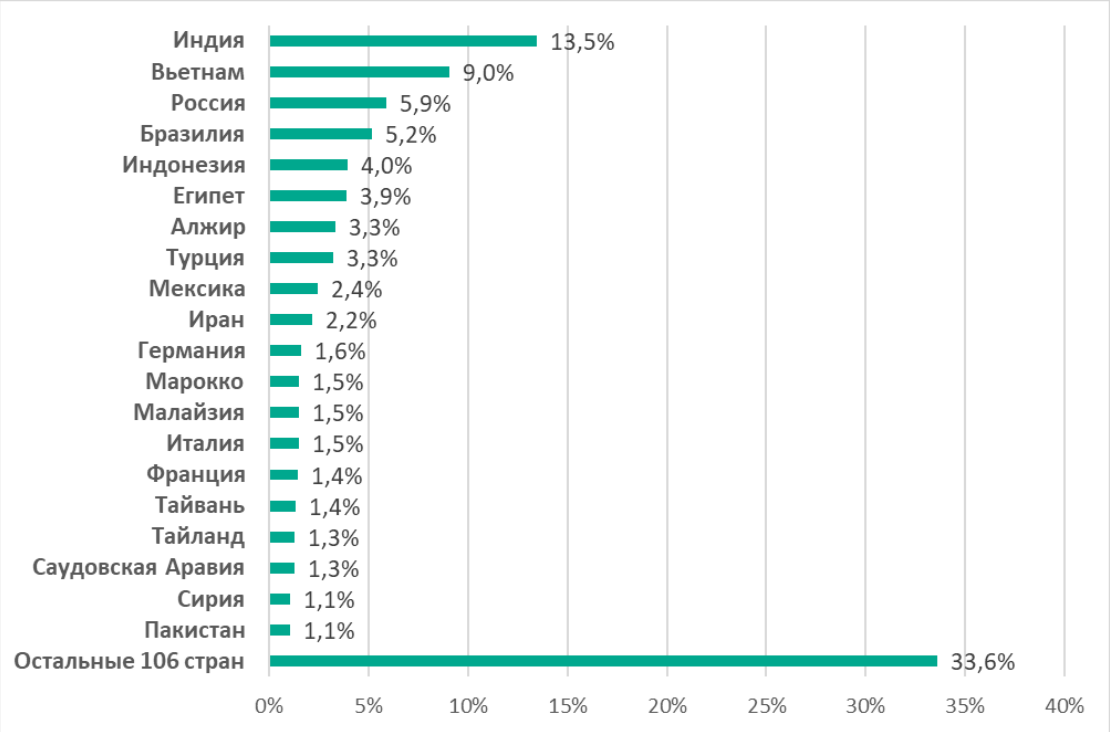
Доля промышленных систем в общем множестве компьютеров, атакованных PseudoManuscrypt

Как показано на диаграмме ниже, практически треть (29,4%) всех атакованных систем, не относящихся к АСУ ТП, находится в России (10,1%), Индии (10%) и Бразилии (9,3%).



Распределение по странам систем, атакованных PseudoManuscrypt и не относящихся к АСУ ТП

Распределения по странам атакованных PseudoManuscrypt АСУ ТП и не АСУ ТП компьютеров схожи. Однако у некоторых стран, находящихся преимущественно в Азии и на Ближнем Востоке, показатель в распределении атакованных АСУ ТП систем значительно выше (в 1,5-2 раза), чем в распределении атакованных компьютеров, не относящихся к АСУ ТП.

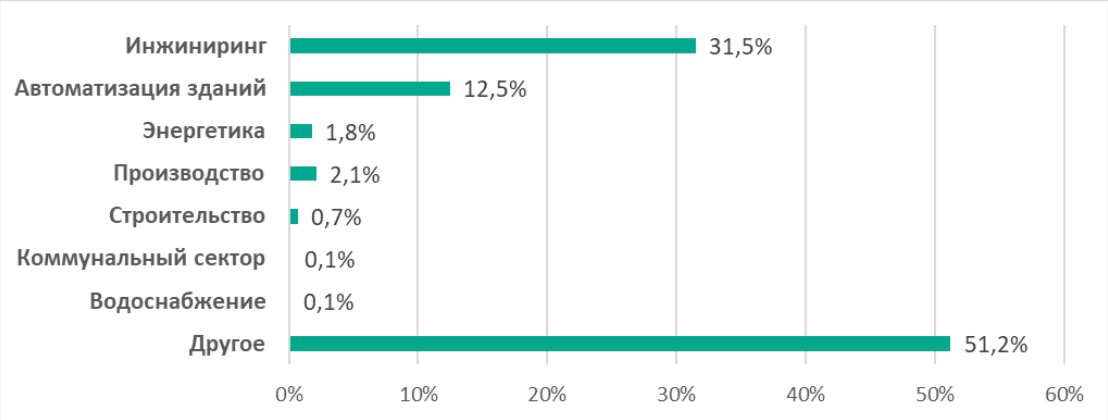


Распределение по странам систем, атакованных PseudoManuscrypt и относящихся к АСУ ТП

Значительная часть промышленных систем (31,5%), на которых был заблокирован PseudoManuscrypt, используются для инжиниринга и интеграции как продуктов, так и систем ICS, в частности, в оборонной промышленности и энергетике. Сюда входят компьютеры, используемые для 3D-моделирования и физического моделирования, а также компьютеры, на которых установлено программное обеспечение для создания «цифровых двойников».

Также среди промышленных систем, на которых был заблокирован PseudoManuscrypt, 12,5% компьютеров используются для управления системами автоматизации зданий (в т.ч. видеонаблюдение, СКУД, системы оповещения и т.д.), 1,8% — в энергетике, 2,1% — на различных производствах, 0,7% — в области строительства (проектирование конструкций), 0,1% — компьютеры коммунального сектора, 0,1% компьютеров используются в системах водоснабжения.

Порядка 51,2% промышленных систем, на которых был заблокирован PseudoManuscrypt, относятся к системам общего назначения, т.е. могут быть использованы в любой отрасли промышленности.



Распределение систем, атакованных PseudoManuscrypt, по индустриям

В ходе исследования было установлено, что жертвами атаки стали, в том числе, и правительственные организации, имеющие отношение к военно-промышленному комплексу (например, исследовательские лаборатории).

Интерес также вызывает тот факт, что, судя по информации из публичных источников, некоторые атакованные организации имеют деловые и производственные отношения с организациями, ставшими жертвой атаки, описанной нами в отчёте «Lazarus атакует оборонную промышленность с помощью вредоносного ПО ThreatNeedle».

Информация о злоумышленниках

Косвенные улики, обнаруженные в ходе расследования, позволяют сделать предположения о происхождении и уровне группы, стоящей за этой атакой:

1. Некоторые образцы вредоносной программы содержат комментарии на китайском языке в метаданных исполняемых файлов;
2. Данные отправляются на сервер злоумышленников с помощью библиотеки, которая ранее использовалась только во вредоносном ПО китайской группы APT41.
3. При подключении к командному серверу вредоносная программа указывает китайский язык в качестве предпочтительного.
4. Вредоносный файл содержит код для подключения к Baidu, популярному в Китае облачному хранилищу файлов.

5. Время суток, когда разработчик загружал новые версии загрузчика PseudoManuscrypt, приходится на интервал с 11:00 до 19:00 по часовому поясу GMT+8, в котором находятся несколько стран Восточной Азии и Азиатско-Тихоокеанского региона.

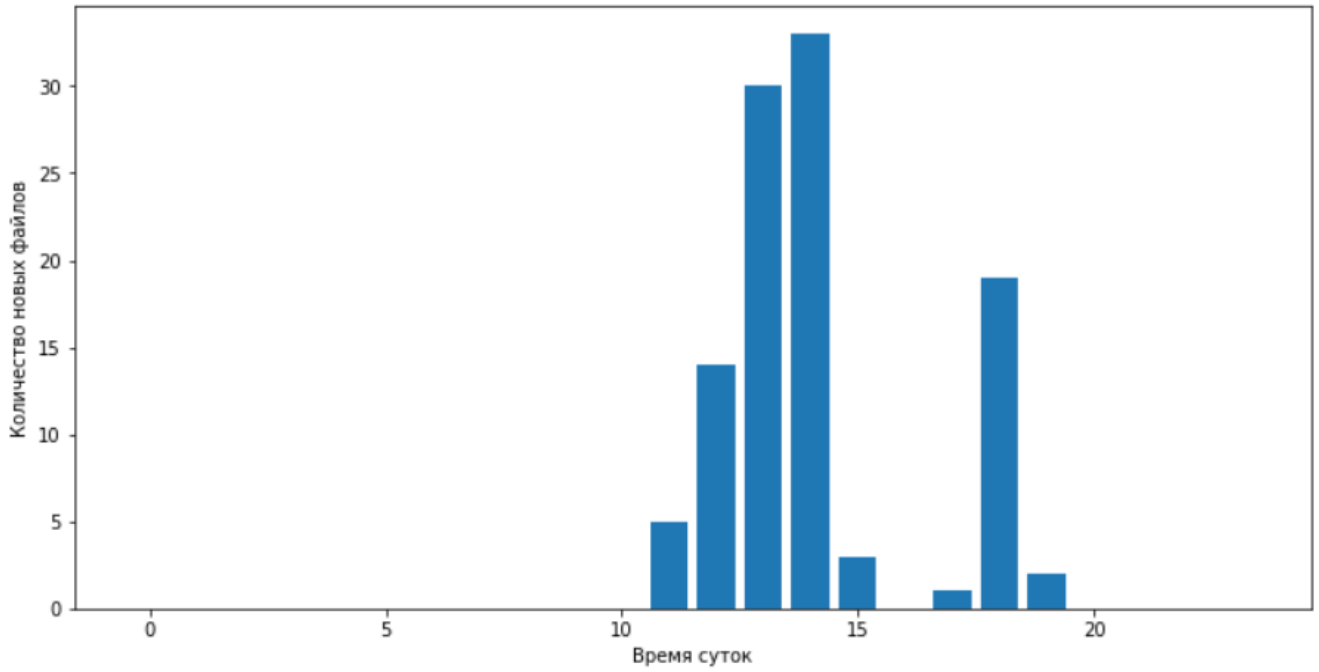


График активности злоумышленника по тестированию вредоносной программы

Заключение

Несмотря на значительную часть собранного и проанализированного материала, многие из наших находок кажутся нам необъяснёнными и не укладывающимися в известные схемы.

Так, мы не можем однозначно ответить на вопрос, преследуют ли атакующие исключительно коммерческие цели или выполняют работу в интересах правительства. Тем не менее, то обстоятельство, что среди атакованных систем встречаются компьютеры государственных организаций и объектов критической инфраструктуры в разных странах, заставляет нас говорить о высоком уровне угрозы.

Число атакованных систем велико, и явный фокус на промышленные организации и системы АСУ ТП не виден. Однако тот факт, что большое количество компьютеров (много сотен только по данным нашей телеметрии, но на деле, наверняка, гораздо больше), имеющих отношение к АСУ ТП, по всему миру оказались атакованными в ходе этой кампании, делает её,

несомненно, угрозой, заслуживающей самого пристального внимания специалистов, отвечающих за безопасность систем АСУ ТП.

Большое количество атакованных компьютеров, относящихся к инжинирингу, включая системы 3d-моделирования, разработки и использования цифровых двойников, поднимает вопрос о промышленном шпионаже как об одной из возможных целей кампании.

Мы пока не ставим точку в расследовании и будем информировать о новых находках по мере их появления.

Если по прочтении данного отчёта у вас появились какие-то вопросы или замечания, или если вы располагаете какими-то дополнительными сведениями по теме, имеющей отношение к данной вредоносной кампании, просим вас связаться с нами по адресу: ics-cert@kaspersky.com.

Рекомендации

1. Устанавливать на все серверы и рабочие станции антивирусное ПО с поддержкой централизованного управления политикой безопасности, следить, чтобы защитные решения имели последние версии антивирусных баз и программных модулей.
2. Убедиться, что все компоненты антивирусного ПО на всех системах включены, а также настроена политика запроса пароля администратора при попытке отключения защиты.
3. Убедиться, что политиками Active Directory установлены ограничения для входа пользователей в системы. Пользователям должен быть разрешён вход только на те системы, доступ к которым обусловлен рабочей необходимостью.
4. Ограничить сетевые подключения, в частности VPN подключения, между объектами технологической сети, запретить подключения по всем портам, работа которых не требуется для выполнения технологического процесса.
5. Использовать смарт-карты (токены) или одноразовые коды в качестве второго фактора аутентификации для создания VPN подключения. В тех случаях, где это применимо, использовать технологию Access Control List (ACL) для ограничения списка IP адресов, с которых может будь инициировано VPN подключение.
6. Проводить обучение сотрудников предприятия безопасной работе с сетью Интернет, электронной почтой и другими каналами связи, в

частности, разъяснять последствия загрузки и запуска файлов из непроверенных источников.

7. Использовать учетные записи с правами локальных администраторов и администраторов домена только в случае производственной необходимости.
8. Ограничить возможность программ получать привилегии SeDebugPrivilege (там, где это возможно).
9. Внедрить парольную политику с требованиями к сложности паролей и их регулярной смене.
10. Адаптировать сервисы класса Managed Detection and Response для получения оперативного доступа к высококлассным знаниям и наработкам профессиональных экспертов по кибербезопасности.
11. Использовать специальную защиту для технологического процесса. Kaspersky Industrial CyberSecurity защищает промышленные конечные узлы и позволяет сетевому мониторингу технологической сети выявлять и пресекать вредоносную активность.

Индикаторы компрометации (IOC)

Контрольные суммы (MD5)

В данной секции мы предоставляем только MD5 файлов, которые, как мы считаем, использовались в атаке, исключая тестовые образцы вредоносного ПО

1fecb6eb98e8ee72bb5f006dd79c6f2f

4da2c2abcf1df9749b64b34160bd3ebf

5dc7fbf2141f7dfe5215c94895bf959c

70e9416833b2f933b765042f8e1ea0bc

8074f73f7742309b033676cd03eb0928

8ae40c8418b2c36b58d2a43153544ddd

Пути к файлам

%WinDir%\System32\[0-Z]{10}.tmp e.g. I59RFRLY9J.tmp

%TEMP%\[0-Z]{10}.tmp e.g. I59RFRLY9J.tmp

%WinDir%\System32\9cda11af69ab0a2b6a9167f7131e7b93.key

Вердикты защитных решений

Trojan.Win64.Manuscrypt.do

URL-адреса

hxxp://email.yg9[.]me

hxxp://google.vrthcobj[.]com

hxxp://d.diragame[.]com

hxxp://toa.mygametoa[.]com

hxxp://tob.mygametob[.]com

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com