Kaspersky ICS CERT

kaspersky

Стеганография в атаках на промышленные предприятия

Вячеслав Копейцев

17.06.2020 Версия 1.1

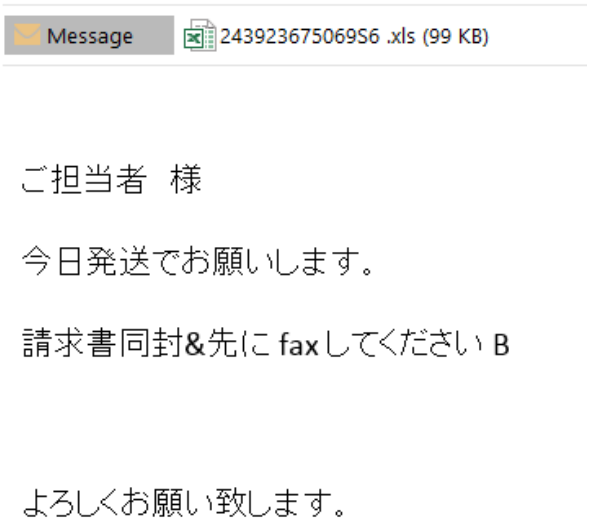
Эксперты Kaspersky ICS CERT выявили серию атак на организации, расположенные в различных странах. На начало мая 2020 года известны случаи атак на системы в Японии, Италии, Германии и Великобритании. До 50% целей атакующих приходится на организации, относящиеся к различным отраслям промышленности. Среди жертв атак оказались в том числе поставщики оборудования и программного обеспечения для промышленных предприятий. Злоумышленники используют вредоносные документы Microsoft Office, PowerShell скрипты, а также различные техники затруднения детектирования и анализа вредоносного ПО.

В качестве начального вектора атаки используются фишинговые письма с текстом на целевом для каждой конкретной жертвы языке. Вредоносная программа, используемая в этой атаке, выполняет деструктивную активность только в том случае, если операционная система имеет локализацию, соответствующую языку, использованному в фишинговом письме. Например, в случае атаки на компанию из Японии текст фишингового письма и документ Microsoft Office, содержащий вредоносный макрос, написаны на японском, а для успешной расшифровки модуля вредоносной программы операционная система должна иметь японскую локализацию.

В результате на. компьютеры жертв устанавливается банковские троянцы семейства Bebloh (Shiotob, URLZone) и Ursnif (Gozi, ISFB).

Технические подробности

Злоумышленники присылают жертве фишинговое письмо с просьбой срочно открыть прикреплённый документ.



Скриншот фишингового письма с вредоносным вложением

Документ Excel, прикреплённый к письму, содержит вредоносный скрипт-макрос (вердикт Trojan.MSExcel.Agent.be). После открытия документа пользователь видит сообщение с просьбой включить исполнение содержимого документа. В случае если пользователь согласится это сделать, вредоносный макрос будет выполнен.

Основная задача макроса заключается в расшифровке и запуске PowerShell скрипта. Запуск скрипта производится со следующими параметрами:

-ExecutionPolicy ByPass,
-WindowStyle Hidden,
-NoProfile,

т.е. выполнить скрипт, несмотря на установленную политику, в скрытом режиме без загрузки пользовательской конфигурации.

```
Function GeneralCatalog()
GeneralCatalog = "pzq /p pzq /p CBjREFuryy -rC  OLCnfF -j 1 -abAvAgR -ABCEbsVY    "". ( $cFubZR[
End Function


Function lAstReport()
lAstReport = "ynpr(',','/')).ercynpr(';','+') ),[VB.pBzceRFfVBa.pbZCErfFVBAzBQr]::QRpbzcerff ) |
End Function
```

Фрагмент обфусцированного макроса, запускающего PowerShell скрипт

Запускаемый PowerShell скрипт (вердикт HEUR:Trojan.PowerShell.Generic) случайно выбирает один из записанных в нём URL адресов, которые указывают на публичные веб-хостинги изображений imgur.com и imgbox.com, загружает изображение, расположенное по ссылке, и начинает процедуру извлечения данных.

Изображение, загружаемое вредоносной программой

Данные сокрыты в изображении при помощи методов стеганографии и извлекаются вредоносной программой из пикселей, номера которых заданы алгоритмом. Использование стеганографии позволяет злоумышленникам обойти некоторые средства защиты, в частности, сканеры сетевого трафика.

Извлечённые из изображения данные последовательно закодированы алгоритмом Base64, зашифрованы алгоритмом AES и снова закодированы Base64. Примечательно, что в качестве ключа расшифровки используется текст исключения (exception), и для этого код скрипта намеренно содержит ошибку. При этом текст исключения будет зависеть от локализации операционной системы – по всей видимости, вредоносный скрипт в каждой конкретной атаке готовится злоумышленниками для жертв из определённой страны.

Расшифрованные и раскодированные данные представляют собой ещё один PowerShell-скрипт, который запускается на выполнение.

```
(0..286)|.('%')
{
        foreach(${x} in(0..635))
        {
                ${p}=${G}.("GetPixel").Invoke(${x},${_});
                ${O}[${_}*636+${x}]=([math]::("Floor").Invoke((${p}."B"-band15)*16)-bor(${p}."g" -band 15))
        }
};

${EE}=[System.Text.Encoding]::"UTf8"."gETsTRING"(${O}[0..182171]);
${eRROr}.("Clear").Invoke();
${ErRorActIOnPReFeReNCE} ="SilentlyContinue";
&("null")|.("Out-Null");[string]${ness}=${eRRoR}[0]."EXCeption";
${VUS}=[Regex]::("Matches").Invoke(${NeSS},'(?<=: ).*?(?='')') -join'';
```

Фрагмент кода распаковки данных

Второй PowerShell скрипт тоже декодирует часть своего содержимого при помощи Base64, после чего распаковывает полученный буфер с данными при помощи алгоритма Deflate. В результате вредоносная программа получает ещё один PowerShell скрипт – в данном случае обфусцированный экземпляр вредоносной программы семейства Bebloh (Shiotob, URLZone). В других случаях злоумышленники использовали троянцев семейства Ursnif (Gozi, ISFB).

```
${A&LSQUO;TTR&LSQUO;IBUtEs} = 'AutoLayout, AnsiClass, Class, Public, SequentialLayout, Sealed, BeforeFieldInit'
${tY&LSQUO;p&LSQUO;ebU&LSQUO;ILDEr} = ${modU&LSQUO;lEbui&LSQUO;lDer}.`D&LSQUO;Efi&LSQUO;NEtyPE`('IMAGE_NT_HEADERS32', ${AT&LSQUO;T&L
${t&LSQUO;ypebu&LSQUO;ilder}.`dEFIN&LSQUO;eFi&LSQUO;elD`('Signature', [UInt32], 'Public') | &(`{0}{2}{1}` -f'Ou','ull','t-N')
${T&LSQUO;YpeB&LSQUO;UildEr}.`dEfin&LSQUO;E&LSQUO;FIeLD`('FileHeader', ${imag&LSQUO;e_FiL&LSQUO;e_hEad&LSQUO;Er}, 'Public') | &(`{0}
${tyPEB&LSQUO;Ui&LSQUO;ld&LSQUO;ER}.`De&LSQUO;Fi&LSQUO;N&LSQUO;eFIElD`('OptionalHeader', ${imaGe_OPTi&LSQUO;ON&LSQUO;AL&LSQUO;_&LSQU
${Im&LSQUO;AGe&LSQUO;_nt&LSQUO;_hEadEr&LSQUO;s32} = ${t&LSQUO;YPebu&LSQUO;iL&LSQUO;DEr}.`cR&LSQUO;EATeT&LSQUO;YpE`()
${W&LSQUO;I&LSQUO;N32Types} | &(`{1}{0}{2}` -f'-Me','Add','mber') -MemberType (`{3}{0}{1}{2}`-f 'r','opert','y','NoteP') -Name (`{4}
${a&LSQUO;TtrIBu&LSQUO;TeS} = 'AutoLayout, AnsiClass, Class, Public, SequentialLayout, Sealed, BeforeFieldInit'
${TyP&LSQUO;EBU&LSQUO;I&LSQUO;ldeR} = ${m&LSQUO;oDULEbuIl&LSQUO;der}.`dEF&LSQUO;in&LSQUO;eTyPe`('IMAGE_DOS_HEADER', ${aTtrib&LSQUO;U
${tYPe&LSQUO;B&LSQUO;UilD&LSQUO;eR}.`D&LSQUO;EFinE&LSQUO;FieLd`('e_magic', [UInt16], 'Public') | &(`{0}{2}{1}` -f 'Ou','l','t-Nul')
${T&LSQUO;ypEbui&LSQUO;LDER}.`D&LSQUO;E&LSQUO;Fin&LSQUO;eFIeLd`('e_cblp', [UInt16], 'Public') | &(`{1}{0}`-f 'll','Out-Nu')
${TyPEb&LSQUO;UI&LSQUO;LD&LSQUO;Er}.`defIneFi&LSQUO;e&LSQUO;ld`('e_cp', [UInt16], 'Public') | &(`{0}{1}`-f 'Out-Nul','l')
${TY&LSQUO;pEb&LSQUO;UILD&LSQUO;eR}.`DE&LSQUO;F&LSQUO;InEFIElD`('e_crlc', [UInt16], 'Public') | &(`{1}{2}{0}` -f 'll','O','ut-Nu')
${TYPEB&LSQUO;Uil&LSQUO;D&LSQUO;ER}.`d&LSQUO;eF&LSQUO;inE&LSQUO;FiEld`('e_cparhdr', [UInt16], 'Public') | &(`{2}{1}{0}` -f 'll','t-N
${TyPE&LSQUO;B&LSQUO;UI&LSQUO;lDer}.`d&LSQUO;E&LSQUO;FINEFiElD`('e_minalloc', [UInt16], 'Public') | &(`{0}{1}` -f 'Out','-Null')
```

Фрагмент кода обфусцированного скрипта

Семейство Bebloh/Shiotob известно с 2009 года. Троянцы этого семейства крадут пароли от FTP-клиентов и электронной почты, а также «прослушивают» интернет-трафик браузеров, чтобы украсть данные для авторизации на различных сайтах. Семейство Ursnif обладает более расширенной функциональностью, его новейшие версии включают в себя обновленные модули для кражи данных, в том числе кошельков для криптовалюты.

Общая схема проведения атаки

Заключение

Предыдущие варианты этой атаки исследователи наблюдали, по меньшей мере, с 2018 года. Новая волна атак обратила на себя внимание ввиду высокого процента промышленных предприятий и компаний – разработчиков и поставщиков продуктов для промышленных организаций в числе потенциальных жертв, а также благодаря нескольким нестандартным техническим решениям, применённым злоумышленниками.

Во-первых, модуль вредоносной программы закодирован внутри изображения при помощи методов стеганографии, а само изображение размещено на легитимных веб-ресурсах. Всё это делает практически невозможным обнаружение загрузки такого вредоносного ПО при помощи средств мониторинга и контроля сетевого трафика: с точки зрения технических решений такая активность не отличается от обычного обращения к легитимному хостингу изображений.

Вторая интересная особенность найденного вредоносного ПО – использование текста исключения (exception) в качестве ключа для шифрования полезной нагрузки вредоносной программы. Такая техника может помочь вредоносной программе избежать детектирования в системах автоматического анализа класса Sandbox, а также усложнит задачу выявления функциональности программы для аналитика, в том случае, если специалисту не известно, какой языковой пакет использовался на компьютере жертвы.

Во всех выявленных случаях вредоносное ПО было заблокировано антивирусными решениями «Лаборатории Касперского».

Если вы столкнулись с подобной атакой, вы можете сообщить нам об этом, воспользовавшись специальной формой на нашем веб-сайте.

Рекомендации

- Проводить обучение сотрудников предприятий навыкам безопасной работы с почтой и, в частности, выявлению фишинговых писем;
- Ограничить выполнение макросов в документах Microsoft Office;
- Ограничить выполнение PowerShell скриптов (при возможности);
- Особое внимание обращать на события запуска процессов PowerShell, инициированные приложениями Microsoft Office;
- Ограничить получение программами привилегий SeDebugPrivilege (при возможности);
- Установить на все системы антивирусное ПО с возможностью централизованного управления политикой безопасности, поддерживать в актуальном состоянии антивирусные базы и программные модули защитных решений;
- Использовать учетные записи пользователей с правами доменного администратора только при необходимости. После использования таких учетных записей перезапускать систему, на которой была выполнена аутентификация;
- Внедрить парольную политику с требованиями к уровню сложности и регулярной смене пароля;
- В случае подозрений на заражение систем выполнить проверку антивирусным ПО и принудительную смену паролей для всех аккаунтов, которые использовались для входа на скомпрометированных системах.

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