

Наиболее популярные семейства ВПО

На основе аналитики атак в январе – сентябре 2021 года



ОГЛАВЛЕНИЕ

Введение.....	3
Уровни и цели злоумышленников	4
Общие тренды.....	6
Атаки на российские органы власти.....	6
Массовая атака HAFNIUM.....	7
ВПО Glupteba.....	8
Криптомайнер Lemon Duck.....	11
ВПО Formbook Stealer.....	15
Заключение	17

Введение

Как и годом ранее, в 2021-м злоумышленники продолжают активно использовать тему коронавируса для проведения массовых фишинговых рассылок. Также продолжает расти количество хостов с широко известными уязвимостями, а низкая кибергигиена, отсутствие элементарных процессов патчинга и нерегулярность работ по оценке защищенности способствуют тому, что даже злоумышленники с низкой квалификацией могут нанести организации непоправимый ущерб. В некоторых случаях успешная атака может даже повлиять на работоспособность крупных промышленных предприятий и социально значимых объектов.

Эксплуатация уязвимостей и недостатков инфраструктуры является лишь точкой входа злоумышленника в сеть жертвы. После этого этапа следует загрузка вредоносных программ, которые выполняют всю «черную работу» (от кражи данных до запуска произвольного кода). В настоящем отчете рассмотрены наиболее популярные семейства зловредов, которые активно использовали хакеры в январе – сентябре 2021 года.



Отчет сформирован на основе данных, собранных и проанализированных экспертами центра противодействия кибератакам Solar JSOC и отдела расследования киберинцидентов Solar JSOC CERT компании «Ростелеком-Солар» в январе – сентябре 2021 года.

Уровни и цели злоумышленников

Уровни нарушителей

В основе нашего исследования лежит модель уровней нарушителей, которая учитывает значительное расслоение подходов злоумышленников к атакам на инфраструктуру. Данная модель выделяет пять основных категорий нарушителей:

Категория нарушителя	Типовые цели	Возможности нарушителя	Защитные меры
Автоматизированные системы	Взлом устройств и инфраструктур с низким уровнем защиты для дальнейшей перепродажи или использования в массовых атаках	Автоматизированное сканирование	Установить и настроить UTM и WAF, задать правило о своевременной установке патчей и обновлений
Киберхулиган / Энтузиаст-одиночка	Хулиганство, нарушение целостности инфраструктуры	Официальные и open-source-инструменты для анализа защищенности	Установить и настроить антивирус, антиспам, UTM и WAF, задать правило о своевременной установке патчей и обновлений. Анализировать журналы аудита СЗИ
Киберкриминал / Организованные группировки	Приоритетная монетизация атаки: шифрование, майнинг, вывод денежных средств	Кастомизированные инструменты, доступное ВПО, доступные уязвимости, социальный инжиниринг	Добавить к базовым средствам защиты инструменты непрерывного мониторинга и реагирования и анализаторы периметрового трафика или подключить коммерческий SOC. Повышать киберграмотность сотрудников

Категория нарушителя	Типовые цели	Возможности нарушителя	Защитные меры
Кибернаемники / Продвинутые группировки	Нацеленность на заказные работы, шпионаж в интересах конкурентов, последующая крупная монетизация, хактивизм, деструктивные действия	Самостоятельно разработанные инструменты, приобретенные O-day-уязвимости	Дополнить базовые средства защиты продвинутыми решениями (Anti-APT, Sandbox, контроль технологических сегментов). Подключить продвинутый инструментарий SOC, включая EDR и NTA. Также нужна глубокая аналитика регистрируемых событий для выявления взаимосвязи между инцидентами
Кибервойска / Прогосударственные группировки	Кибершпионаж, полный захват инфраструктуры для возможности контроля и применения любых действий и подходов, хактивизм	Самостоятельно найденные O-day-уязвимости, разработанные и внедренные «закладки»	Необходим весь доступный спектр инструментов и сервисов, высокая зрелость ИТ- и ИБ-инфраструктуры, качественная экспертиза для построения процессов и выявления неочевидных аномалий на сети и хостах. Использовать маппинг по Killchain+Mitre ATT&CK для выявления цепочек взаимосвязей между инцидентами

Общие тренды

Атаки на российские органы власти

В начале 2021 года эксперты «Ростелеком-Солар» завершили расследование серии кибератак на федеральные органы исполнительной власти (ФОИВ) РФ. Удалось выяснить, что злоумышленники использовали три основных вектора для проникновения в инфраструктуру жертвы:

- 1 Таргетированные фишинговые рассылки.** Злоумышленники изучили новостной фон вокруг выбранного ФОИВ и для каждой цели подготовили индивидуальные рассылки.
- 2 Эксплуатация уязвимостей веб-приложений, опубликованных в интернете.** Во многих инфраструктурах встречаются известные уязвимости веб-приложений, эксплойты для которых хакеры находят в открытом доступе или приобретают в даркнете. Наличие известных веб-уязвимостей становится следствием нерегулярной инвентаризации внешней инфраструктуры и нечастых работ по оценке защищенности. Это сильно упрощает атаку, снижает ее стоимость и делает инфраструктуру доступной даже для злоумышленников с низкой квалификацией. В противном случае киберпреступникам приходится самостоятельно искать ошибки на периметре жертвы, что требует от них глубокой экспертизы, а также временных и финансовых затрат.
- 3 Взлом инфраструктуры подрядных организаций (Trusted Relationship).** Чаще всего данный вектор атаки свидетельствует о высокой квалификации злоумышленников. Такие атаки не свойственны киберхулиганам и хакерам с низкой квалификацией, основная цель которых – прямая монетизация за счет шифрования инфраструктуры, подмены реквизитов, вывода средств с расчетных счетов и прочих манипуляций. Взлом подрядчика позволяет проникнуть в инфраструктуру основной жертвы и долго находиться внутри сети, собирая необходимую информацию об организации (особенно если подрядчик имеет привилегированную учетную запись в корпоративной сети своего заказчика).

Дальнейшее продвижение во взломанной инфраструктуре осуществлялось за счет разработанного злоумышленниками вредоносного ПО, которое собирало данные и выгружало их в облачные хранилища российских компаний «Яндекс» и Mail.ru Group. В своей сетевой активности ВПО маскировалось под легитимные утилиты Яндекс.Диск и Disk-O. Подробное техническое описание этих атак эксперты «Ростелеком-Солар» приводили [в аналитическом отчете](#), подготовленном совместно с НКЦКИ (Национальным координационным центром по компьютерным инцидентам, созданным ФСБ России).

Массовая атака HAFNIUM

В начале марта 2021 года корпорация Microsoft опубликовала информацию об атаке на американские организации китайской группировки HAFNIUM с использованием O-day-уязвимостей Microsoft Exchange. Сразу после публикации эксперты Solar JSOC стали отмечать возросшую активность злоумышленников на сети ханипотов «Ростелеком-Солар». При проведении технических расследований удалось обнаружить и исследовать тактику и инструменты атакующих.

Эксплуатация O-day-уязвимостей позволила злоумышленникам не только обойти процесс аутентификации, но и произвести удаленный запуск произвольного кода от имени системы. В качестве полезной нагрузки они загружали на сервер два веб-шелла: один – для загрузки на сервер произвольных файлов, второй – для запуска команд через cmd.exe:

```
function t1
{
    $nocoutput = $nocoutput + "bttme2:\n\n"+([datetime]::Now.AddMilliseconds(-([environment]::TickCount)))-join $d) +%c;
    $nocoutput = $nocoutput + "Account Policy:\n\n" + ((net accounts /domain) -join $d)+%c;
    $nocoutput = $nocoutput + "ipconfig:\n\n" + ((ipconfig /all) -join $d)+%c;
    $nocoutput = $nocoutput + "nslookup:\n\n"+(nslookup -vc mail.ru 8.8.8.8)-join $d) +%c;
    $nocoutput = $nocoutput + "netstat:\n\n"+(netstat -anop tcp)-join $d) +%c;
    $nocoutput = $nocoutput + "Local users:\n\n" + ((Get-WmiObject -Class Win32_UserAccount -Filter "LocalAccount='True'"
    $nocoutput = $nocoutput + "arp:\n\n"+(arp -a)-join $d) +%c;
    $nocoutput = $nocoutput + "route:\n\n"+(route print)-join $d) +%c;
    $nocoutput = $nocoutput + "dccontrol:\n\n"+(nltest /dclist:-join $d) +%c;
    $nocoutput = $nocoutput + "trustPRIMARY:\n\n"+(nltest /DOMAIN_TRUSTS /PRIMARY /V)-join $d) +%c;
    $nocoutput = $nocoutput + "trustDIRECT_OUT:\n\n"+(nltest /DOMAIN_TRUSTS /DIRECT_OUT /V)-join $d) +%c;
    $nocoutput = $nocoutput + "trustDIRECT_IN:\n\n"+(nltest /DOMAIN_TRUSTS /DIRECT_IN /V)-join $d) +%c;
    $nocoutput = $nocoutput + "All_Trusts:\n\n"+(nltest /DOMAIN_TRUSTS /All_Trusts /V)-join $d) +%c;
    $nocoutput = $nocoutput + "LAPS:\n\n"+(gci 'c:\program files\LAPS\CSE\Admpwd.dll')-join $d) +%c;
    $nocoutput = $nocoutput + "diskinfo:\n\n"+(reg query hklm\system\currentcontrolset\enum\usbstor)-join $d) +%c;
    $nocoutput = $nocoutput + "localgroup:\n\n"+(net localgroup)-join $d) +%c;
    $nocoutput | Out-File -Append $pth;
    t4;
}
function t2
{
    $nofoutput = "`n`n msi:`n`n" + ((reg query "hklm\software\policies\microsoft\windows\installer\alwaysinstallelevated" /s
    $nofoutput = $nofoutput + "`n`n Installed Applications:`n`n" + ((registry_values "hklm:\SOFTWARE\Microsoft\Windows\Curre
    $nofoutput = $nofoutput + "`n`n Shares on the machine:`n`n" + ((registry_values "hklm:\SYSTEM\CurrentControlSet\services
    $nofoutput = $nofoutput + "`n`n enum:`n`n" + ((registry_values "hklm:\system\currentcontrolset\services\disk\enum" "all"
```

Также в инструментарий злоумышленников входила кастомная сборка утилиты Mimikatz:

```
function t6
{
    if (Test-Path c:\Windows\cluster\twindump.dll)
    {
        start c:\Windows\cluster\accace.exe -ArgumentList "ase2af6das3fzc2 agasg2aa23gfdgd" -WindowStyle hidden
    }
}
```

Чаще всего злоумышленники после загрузки шеллов осуществляли сбор интересующей их информации (данные о хосте и учетных записях, содержание почтовой переписки) и, предварительно архивируя, загружали ее в облака.

Несмотря на то что уязвимости были обнаружены еще в марте 2021 года, наши эксперты до сих пор фиксируют массовые сканирования и попытки их эксплуатации на наших ханипотах.

Подробнее о технических аспектах обнаружения злоумышленников и наличия уязвимостей мы писали [в этой статье](#).

ВПО Glupteba

В начале этого года эксперты Solar JSOC расследовали инцидент заражения одной из организаций вредоносом семейства Glupteba.

Оказалось, что ВПО незаметно находилось в инфраструктуре жертвы более двух лет и все это время успешно выполняло свои функции. При этом наличие антивируса никак не препятствовало работе малвари.

Ранее мы уже сталкивались с Glupteba, но в ходе расследования обратили внимание на наличие огромного количества новых модулей. Очевидно, что данный вредонос регулярно дорабатывается разработчиками. Ежедневно с помощью сети сенсоров и ханипотов мы фиксируем десятки отечественных организаций из разных сфер деятельности, чья инфраструктура скомпрометирована Glupteba.

Ключевые особенности данного ВПО:

1 множество модулей, написанных под абсолютно разные задачи (прокси, модули для брутфорса и эксплуатации различных уязвимостей, в том числе EternalBlue (CVE-2017-0144), стилеры, модули ядра для сокрытия присутствия, сканеры сети, майнеры);

2 высокая скорость распространения в инфраструктурах из-за наличия в них большого числа незакрытых уязвимостей EternalBlue;

3 сложность очистки инфраструктуры от ВПО из-за множества систем самозащиты и возможностей перезапуска. К ним относятся драйверы, скрывающие процессы ВПО и его файлы, задачи в планировщике, ключи автозапуска, потоки, контролирующие работу модулей, отдельные модули, контролирующие работу основного модуля, которые при необходимости могут скачать ВПО заново. Вредонос также располагается на файловой системе в нескольких местах одновременно;

4 ВПО написано на языке Go. Основной модуль довольно объемный.

Признаки заражения Glupteba:

1 множество файлов в директории %TEMP%\csrss, на которые постоянно срабатывает антивирусное ПО. В этой директории располагаются дополнительные модули, перечисленные выше;

2 для некоторых модулей Glupteba свойственна повышенная сетевая активность по различным портам, характерная для сетевого оборудования (Telnet, SSH, порты MikroTik).

Стоит также отметить, что ВПО распространяется не через почтовые рассылки, а через эксплойт-киты или через замену ссылок на различных файлообменниках на те, что ведут к Glupteba. Пример ссылок, связанных с одним из CDN-серверов:

URL

```
http://regpodcasts.com/ru53332/lumion%2010-rtmd-adpha1_afwaaedkcafbufwasap88xlsa.exe
http://regpodcasts.com/ru53332/pro+evolution+soccer+2019-rtmd-ak7y8v42ggaa6rocaelefwasa08d2w0a.exe
https://regpodcasts.com/
https://regpodcasts.com/ru53332/(KEYWORD)-RTMD-AHS_m18bUwQASzkCAEVHGQAFAN-kgFwA.exe
https://regpodcasts.com/ru53332/-RTMD-amhb716nyaabzqcae5mgqasamxqcdoa.exe
http://regpodcasts.com/ru53332/sparkol%20Videoscribe%20crack%203-rtmd-aifz8l63mwaapzmaelefwasafbfqsa.exe
http://regpodcasts.com/ru53332/bartender+crack+11-rtmd-ahx08v6ypaaa6rocafrsfwasagisbaca.exe
https://regpodcasts.com/ru53332/-RTMD-AAEbMF-2mwAAvhwCAERFFwASACR2gMsA.exe?1605184828
http://regpodcasts.com/ru53332/advanced%20systemcare%2013-rtmd-ae5ua18spwaaedkcaefufwaoagjrsxya.exe
http://regpodcasts.com/ru53332/aquasoft+slideshow+premium+11-rtmd-aib9bl8uiwqaszkcaevufwamajjkausa.exe
http://regpodcasts.com/ru53332/cmediacm108driversand-rtmd-acnlp1_oogaafzscavtfwaoag2a2ca.exe
http://regpodcasts.com/ru53332/mirzapur2018s01e09hindi720pweb-dl(2)-rtmd-agwyk1-ybwqaezkcaexfwasafydrdaa.exe
http://regpodcasts.com/ru53332/gta-v-psspp-iso-zip-file-rtmd-akm8v19nygqaszkcafbifwasaaawjgbia.exe
http://regpodcasts.com/ru53332/lumion+pro+10-rtmd-aocitv_oxqqavhwcaezsfwasanarbyma.exe
http://regpodcasts.com/ru53332/retouch4me-rtmd-acomsl88dwaetkcafvfwafakcribka.exe
https://regpodcasts.com/ru53332/Retouch4me-RTMD-ACOMsl88dwaetkCAFJFwAFACRlibkA.exe
http://regpodcasts.com/ru53332/how+to+install+downloaded+garmin+maps+on+sd+card-rtmd-ab5dtf90aqqavhwcaedsfwagabjeguqa.exe
http://regpodcasts.com/ru53332/mega-rtmd-akoxsf9pywqafzscaedcfwasahu3wkya.exe
http://regpodcasts.com/ru53332/never+kiss+your+best+friend+(2020)+www-rtmd-ai3frl-ybwqaezkcafbgqasaarcd6ya.exe
http://regpodcasts.com/ru53332/passmark+keyboardtest+3-rtmd-ahhprv_bmgaa6rocafrofwagah9qlpca.exe
```

В названиях файлов явно прослеживаются имена платных программ, взломанные версии которых часто ищут пользователи.

Приводим также примерный алгоритм очистки зараженной машины (в прямой последовательности действий):

- остановить службы WinmonProcessMonitor, WinmonFS, Winmon;
- остановить процессы C:\Windows\RSS\csrss.exe, C:\Windows\windefender.exe, а также любые процессы, запущенные из C:\users\<username>\appdata\local\temp\csrss;
- удалить всю папку C:\Windows\RSS;
- удалить всю папку C:\users\<username>\appdata\local\temp\csrss;
- удалить файлы C:\WINDOWS\System32\drivers\Winmon.sys, C:\WINDOWS\System32\drivers\WinmonFS.sys, C:\WINDOWS\System32\drivers\WinmonProcessMonitor.sys, C:\Windows\windefender.exe;
- удалить задачи CSRSS и ScheduledUpdate;
- удалить ключ автозапуска (HKCU(HKLM)\SOFTWARE\Microsoft\Windows\CurrentVersion\Run) с запуском чего-либо из C:\Windows\RSS (имя ключа генерируется случайным образом);
- удалить службы WinmonProcessMonitor, WinmonFS, Winmon.

По нашим оценкам, более 3% отечественных организаций скомпрометированы Glupteba.

Кроме этого, Glupteba, скорее всего, является основой для формирования ботнета Mëris, состоящего из сетевых устройств компании MikroTik. Именно с его помощью в сентябре 2021 года была организована серия мощнейших DDoS-атак (в том числе атака на компанию «Яндекс» с впечатляющим значением в 21,8 млн RPS).

Благодаря сети ханипотов специалисты «Ростелеком-Солар» смогли получить и проанализировать команды, которые используются для управления зараженными устройствами. Выявленные в них ошибки позволили обнаружить 45 000 сетевых устройств, идентифицировать их географическое местоположение и изолировать от ботнета.

Для взлома устройств MikroTik, которые мы наблюдаем на сети ханипотов, хакеры использовали брутфорс паролей по SSH и эксплуатацию уязвимости CVE-2018-14847, позволяющей получить учетную запись администратора. После удачного входа на устройство прописывается команда на добавление определенной задачи в планировщик задач RouterOS.

Анализ доменных имен, с которых взломанные устройства скачивали скрипты, указал на ВПО семейства Glupteba, которое имеет в своем арсенале модуль для заражения MikroTik. ВПО тоже работает через брутфорс паролей по SSH и эксплуатации уязвимости CVE-2018-14847 и создает ровно такие же задачи. Подробнее о расследовании написано [в нашей статье](#) на Хабре.

Криптомайнер Lemon Duck

Несмотря на то что в последнее время наиболее популярным типом ВПО являются шифровальщики-вымогатели, майнеры также часто используются злоумышленниками с разным уровнем квалификации. В первую очередь это связано с тем, что криптовалютный рынок вырос в последние полгода в несколько раз, что увеличило ценность майнинга.

Кроме этого, практически единственным признаком наличия майнера является нагрузка центрального процессора, но логика его работы позволяет запускать его в то время, когда пользователь не работает за компьютером, например ночью или в выходные. Благодаря этому присутствие ВПО остается незамеченным.

Владельцы майнинговых ботнетов концентрируются исключительно на слабозащищенных уязвимых целях. Это могут быть как персональные компьютеры граждан, так и корпоративные, на которых не проводится регулярный патчинг.

Lemon Duck – это наиболее популярный ботнет, с которым наши эксперты регулярно сталкивались в отчетном периоде. Это модульный ботнет, основная деятельность которого заключается в майнинге криптовалюты с помощью XMRig-майнеров как на процессорах, так и на графических картах.

Особенностью Lemon Duck является огромное количество техник распространения:

- Рассылка почты. При попадании на хост с клиентом Outlook выполняет рассылку писем с заранее определенными темой, текстом и вредоносным вложением с расширениями .js, .zip или .rtf (в недавних атаках вложение называлось readme).
- Брутфорс. Перебираются пароли SMB-хранилищ, баз данных MS SQL, RDP (через freerdp), SSH (через plink.exe).
- Эксплуатация уязвимостей:
 - RDP BlueKeep (CVE-2019-0708);
 - SMBGghost (CVE-2020-0796);
 - LNK exploit (CVE-2017-8464);
 - EternalBlue (CVE-2017-0144);
 - Apache Hadoop YARN (без номера, 8088/tcp);
 - Web Logic (CVE-2020-14882, порт 7001/tcp);
 - ElasticSearch 1.4.0/1.4.2 RCE (CVE-2015-1427, порт 9200/tcp);
 - Apache Solr (CVE-2019-0193, порт 8983/tcp).
- Распространение через съемные и сетевые диски.
- Pass-the-hash для SMB-хранилищ.
- Возможность распространения на Linux-системы:
 - NoSQL базы данных Redis (порты 6379/tcp и 16379/tcp);
 - эксплойт для Apache Hadoop YARN (порт 8088/tcp YARN ResourceManager WebUI);
 - брутфорс ssh;
 - ElasticSearch 1.4.0/1.4.2 RCE (CVE-2015-1427, порт 9200/tcp);
 - Apache Solr (CVE-2019-0193, порт 8983/tcp).

В последних версиях криптомайнер стал намного опаснее, так как у него появился функционал для удаленного управления системой. Это приводит к установке бэкдора (RAT), хищению данных (в том числе учетных), а также загрузке ВПО Ramnit, которое, в частности, используется для кражи чувствительной информации (паролей из браузеров, ftp-клиентов и т. д.).

При реагировании на атаки Lemon Duck полезно знать индикаторы его активности. ВПО продолжает активно развиваться, и какая-то часть из представленных индикаторов может стать неактуальной, но мы постарались выбрать из них те, что встречаются наиболее часто:

1 Форматы имен:

- M6.bin.ori
- M6G.bin
- M6.bin.exe
- M[0-9][A-Z].bin
- mimi.dat (mimikatz)

2 Порт-индикатор заражения: 65529/tcp

Сетевой модуль Lemon Duck перед заражением очередного хоста проверяет, прослушивается ли данный порт. Если прослушивается, то хост считается зараженным и пропускается

3 Характерные имена задач планировщика заданий Windows и время их использования

Ddrivers - Декабрь 2018

MicrosoftwindowsBluetooths - Декабрь 2018

Rtsa - Сентябрь 2019, но также используется при эксплуатации EternalBlue и в 2021

bluetool - Ноябрь 2019

Rtsa1 - Февраль 2020

Rtsa2 - Февраль 2020

bluetea - Апрель 2020

blackball - 2021

blackbell - Одновременно имя задачи и фильтра WMI

[O-9a-zA-Z]{6,11} - 2021

[O-9a-zA-Z]{6,11}\[O-9a-zA-Z]{6,11} - 2021

MicroSoft\Windows\[O-9a-zA-Z]{6,11}\[O- - 2021

9a-zA-Z]{6,11} - 2021



BPO Formbook Stealer

Последнее время мы стали замечать в инфраструктуре заказчиков заражение стилером Formbook.

Formbook имеет следующий функционал:

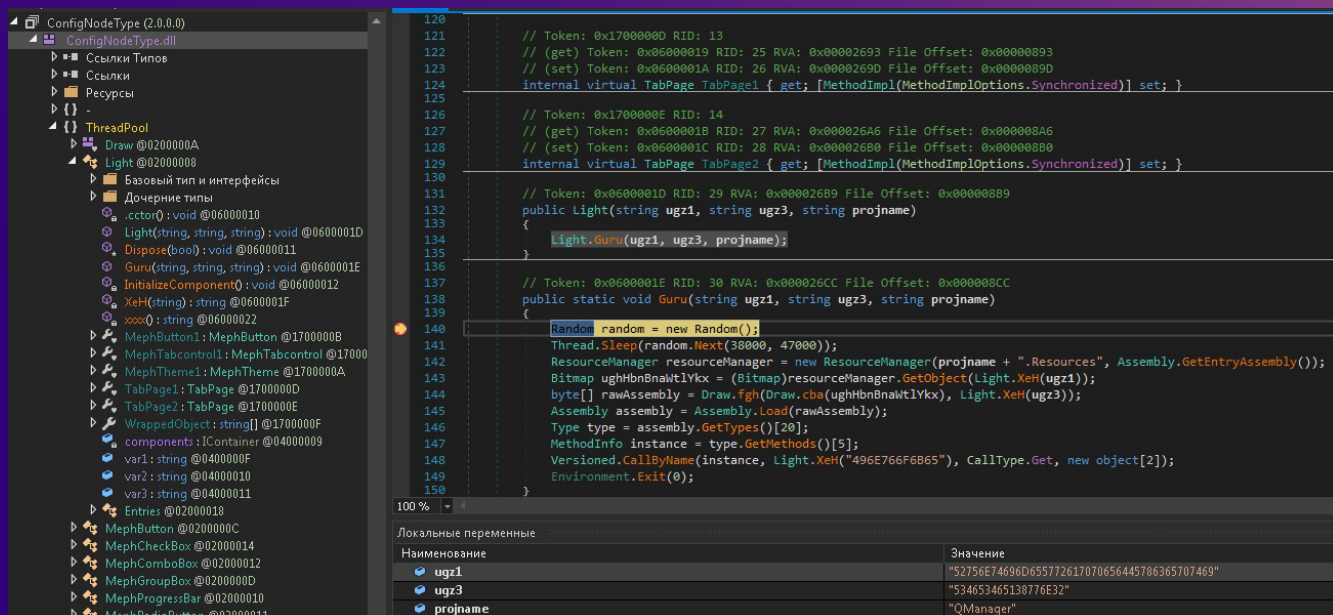
- сбор паролей браузеров, хранилища Windows, Outlook;
- инжектирование в браузеры для сбора чувствительной информации;
- сбор нажатий клавиш и данных из буфера обмена;
- удаленное управление системой;
- загрузка файлов.

Чаще всего Formbook попадает на систему жертвы с помощью фишинговых писем в виде запакованного в архив исполняемого файла.

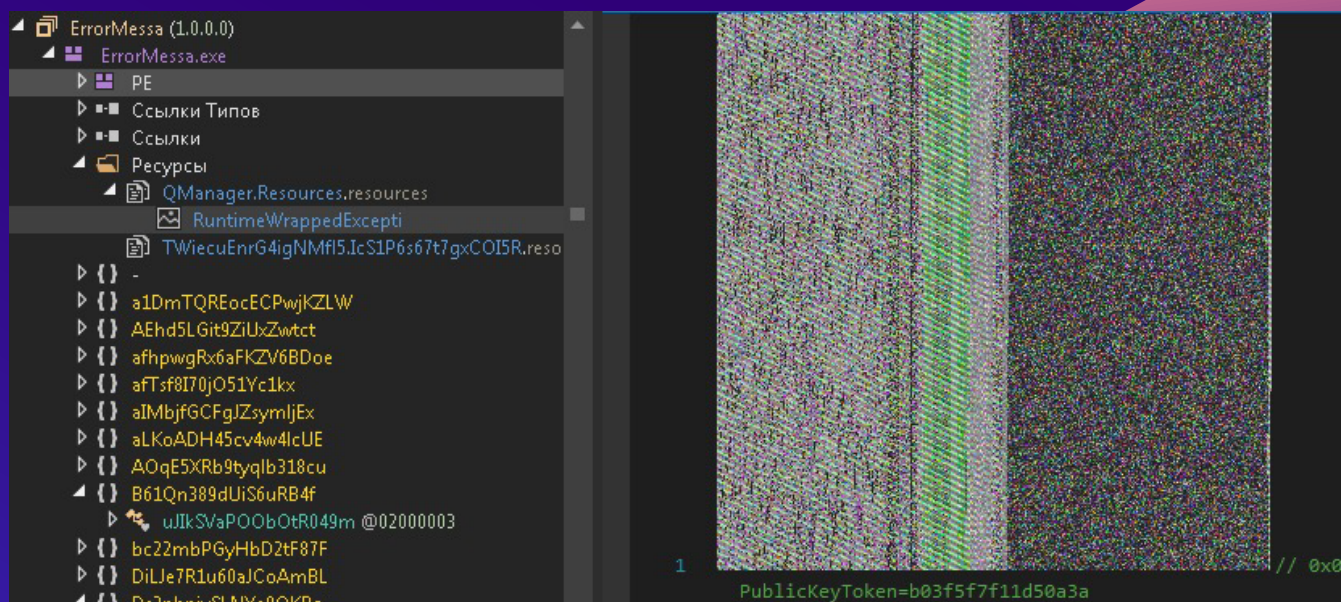
В последнее время Formbook рассылается в очередной .net-оболочке. Код оболочки обфусцирован, основная сборка называется ErrorMessage. Первым делом происходит расшифрование и запуск еще одной .net-сборки ConfigNodeType. Зашифрованная сборка ConfigNodeType выглядит так:

[illegible]

Точка входа ConfigNodeType выглядит так:



ConfigNodeType находит среди ресурсов ErrorMessage пиксельное изображение RuntimeWrappedExcepti, извлекает и расшифровывает еще одну сборку SinkProvider:



SinkProvider расшифровывает очередную промежуточную сборку, которая содержит ресурс htCFq (зашифрованный Formbook), после чего расшифровывает конечную полезную нагрузку. После этого Formbook запускается с помощью process hollowing в легитимный процесс RegSvcs.exe.

Точка входа Formbook:

```
.text:0041EB00 ; ===== S U B R O U T I N E =====
.text:0041EB00
.text:0041EB00 ; Attributes: library function bp-based frame
.text:0041EB00
.text:0041EB00 public start
.text:0041EB00 start proc near
.text:0041EB00 push ebp
.text:0041EB01 mov ebp, esp
.text:0041EB03 sub esp, 64h
.text:0041EB06 call sub_41B370
.text:0041EB08 mov esp, ebp
.text:0041EB0D pop ebp
.text:0041EB0E retn
.text:0041EB0E start endp
.text:0041EB0E
```

Заключение

В заключение отметим, что часть обнаруженных в отчетный период вредоносных программ была известна и раньше, но в своих новых итерациях демонстрирует очевидную эволюцию. Это касается не только способов обхода средств защиты, но и способности перестраивать функционал, подключая дополнительные модули.

Наряду с повышением сложности логики работы ВПО можно отметить рост популярности вредоносных программ, которые распространяются по схеме Software-as-a-Service. Очевидно, что модель SaaS приведет к снижению требований к технической подготовке злоумышленников, так как все сложности в реализации и настройке ВПО на себя будут брать разработчики. Крупные организации, которые могут обеспечить себе дорогую и продвинутую киберзащиту, останутся непреступны для злоумышленников с низкой квалификацией. Но в то же время число успешных атак на небольшие компании, которые пока защищены недостаточно хорошо, будет расти, ведь в арсенале непрофессиональных хакеров появится более эффективное ВПО.



rt.ru

rt-solar.ru

solar@rt-solar.ru

+7 (499) 755-07-70