



KZ-CERT

Служба реагирования на компьютерные
инциденты Республики Казахстан



Анализ и исследование инцидентов информационной безопасности

**Жанат Жакупов
Улыкбек Шамбулов
KZ-CERT «ГТС» КНБ РК**



KZ-CERT

Служба реагирования на компьютерные инциденты Республики Казахстан



Статистика



Отработано:

В 2017г. - 25 958 инцидентов ИБ, из них ГО – 748 инцидентов ИБ;

В I квартале 2018г. - 5 479 инцидентов ИБ, из них ГО – 202 инцидентов ИБ.



Проверено:

В 2017г. – 130 **тысяч** доменных имен выявлено 456 инцидентов ИБ, из них ГО – 12 инцидентов ИБ;

В I квартале 2018 г. – 133 **тысяч** доменных имен выявлено 136, из них ГО – 3 инцидентов ИБ.



Отработано:

В 2017 г. - 131 фишинг-инцидента ИБ, из них ГО 1;

В I квартале 2018 г. - 114 фишинг-инцидента ИБ



Отработано:

В 2017 г. - 660 инцидентов ИБ website defacement, из них ГО - 86 инцидентов ИБ;

В I квартале 2018 г. – 695 инцидентов website defacement, из них ГО - 4 инцидента ИБ.



KZ-CERT

Служба реагирования на компьютерные
инциденты Республики Казахстан



Краткий обзор:

Инструментарии по информационной
безопасности необходимый для CERTs/SOCs

“Arsenal”



KZ-CERT

Служба реагирования на компьютерные
инциденты Республики Казахстан



Категория инструментов

- Для обнаружения (Detection Tools)
 - Фиды (Information Feeds)
- Для анализа (Analysis Tools)
- Платформы для автоматизация процессов реагирования (Threat intelligence platform)



KZ-CERT

Служба реагирования на компьютерные инциденты Республики Казахстан



Detection Tools



glastopf

Passive DNS (STS)
Fast-flux

Система
мониторинга (STS)



ALIEN VAULT

Web Crawler(STS)
~130,000 доменов .kz

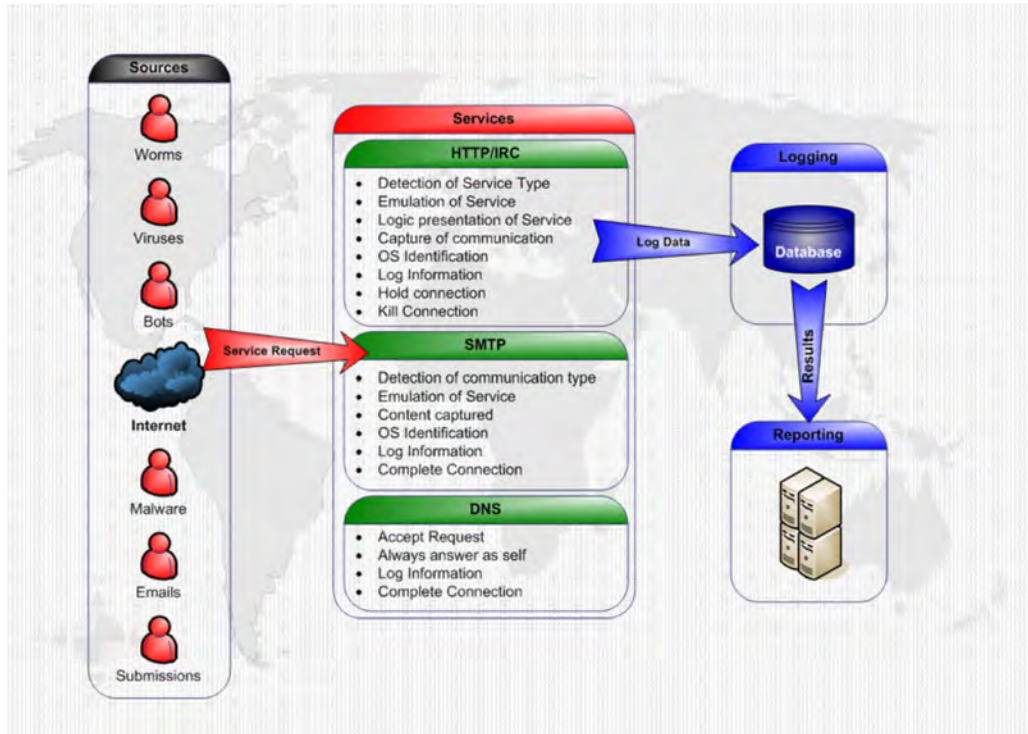


KZ-CERT

Служба реагирования на компьютерные инциденты Республики Казахстан



Detection Tools (Sinkhole)



shadowSERVER



KZ-CERT

Служба реагирования на компьютерные инциденты Республики Казахстан



Information Feeds



shadowSERVER



TEAM CYMRU™



SPAMHAUS



CERT.PL >_



zone-h

unrestricted information



OpenPhish





KZ-CERT

Служба реагирования на компьютерные инциденты Республики Казахстан



Information Feeds



CIRCL

Computer Incident Response Center Luxembourg





KZ-CERT

Служба реагирования на компьютерные инциденты Республики Казахстан

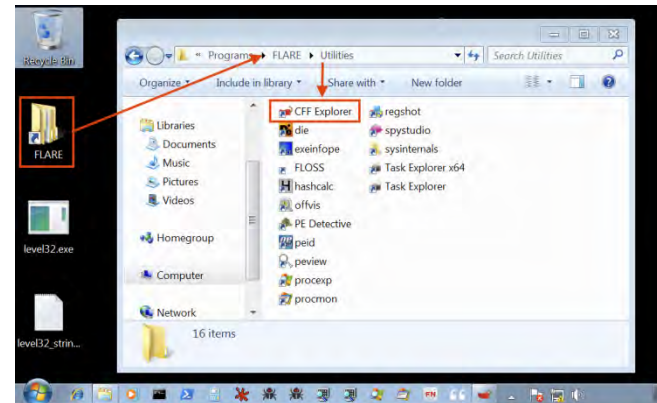


Analysis Tools (Desktops)

Kali-Linux (Debian)



Flare VM (Windows)





KZ-CERT

Служба реагирования на компьютерные инциденты Республики Казахстан



Analysis Tools (Reverse)

IDA Pro
(Windows)

```
{0x400efc}
{fcn} sym_phase_2 71
; CALL XREF from 0x00400e56 (sym_phase_2)
0x00400efc 55          push rbp
0x00400efd 53          push ebx
0x00400efe 4883ec28   sub rbp, 0x28
0x00400ef2 4889e6     mov rsi, rsp
0x00400ef5 e852050000 call sym.read_six_numbers ;[a]
0x00400ef9 833c2401   cmp dword [rsp], 1 ; {0x1:4}=0x2464c45
0x00400ef9 7420       je 0x400f30 ;[b]
```

```
0x400f10
0x00400f10 e825050000 call sym.explode_bomb ;[f]
0x00400f15 eb19       jmp 0x400f30 ;[b]
```

```
0x400f30
; JMP XREF from 0x00400f15 (sym_phase_2)
; JMP XREF from 0x00400ef9 (sym_phase_2)
0x00400f30 488d5c2404 lea rbx, [rsp + 4] ; 0x4
0x00400f35 488d6c2418 lea rbp, [rsp + 0x18] ; 0x18
0x00400f3a ebdb       jmp 0x400f17 ;[c]
```

Radare 2
(Linux)

Hopperapp
(Mac OS)



KZ-CERT

Служба реагирования на компьютерные инциденты Республики Казахстан



Одно окно для всех инструментов

The screenshot shows the Cortex web interface. At the top, there is a navigation bar with the Cortex logo, a '+ New Analysis' button, an 'Analyzers' button, and a 'Jobs' button. Below the navigation bar, the main content area is titled 'Analyzers'. On the left side, there is a sidebar with 'Data types' listed: url, file, hash, ip, domain, fqdn, email, certificate_hash, filename, mail, mail_subject, and other. Each data type has a green box with a number indicating the count of analyzers. The main area contains a search bar 'Search for analyzer description' and a list of analyzers. Each analyzer entry includes its name, version, author, license, and a 'Run' button. The analyzers shown are: JoeSandbox_Url_Analysis (Version: 1.0, Author: CERT-BDF, License: AGPL-V3), JoeSandbox_File_Analysis_Inet (Version: 1.0, Author: CERT-BDF, License: AGPL-V3), JoeSandbox_File_Analysis_Noinet (Version: 1.0, Author: CERT-BDF, License: AGPL-V3), and Virusshare (Version: 1.0, Author: Nils Kühnert, CERT-Bund, License: AGPL-V3).

Data type	Count	Analyzer Name	Version	Author	License	Action
url	12	JoeSandbox_Url_Analysis	1.0	CERT-BDF	AGPL-V3	Run
		Joe Sandbox URL analysis				
		Applies to: url				
file	9	JoeSandbox_File_Analysis_Inet	1.0	CERT-BDF	AGPL-V3	Run
		Joe Sandbox file analysis with Internet access				
		Applies to: file				
hash	7	JoeSandbox_File_Analysis_Noinet	1.0	CERT-BDF	AGPL-V3	Run
		Joe Sandbox file analysis without Internet access				
		Applies to: file				
ip	21	Virusshare	1.0	Nils Kühnert, CERT-Bund	AGPL-V3	Run

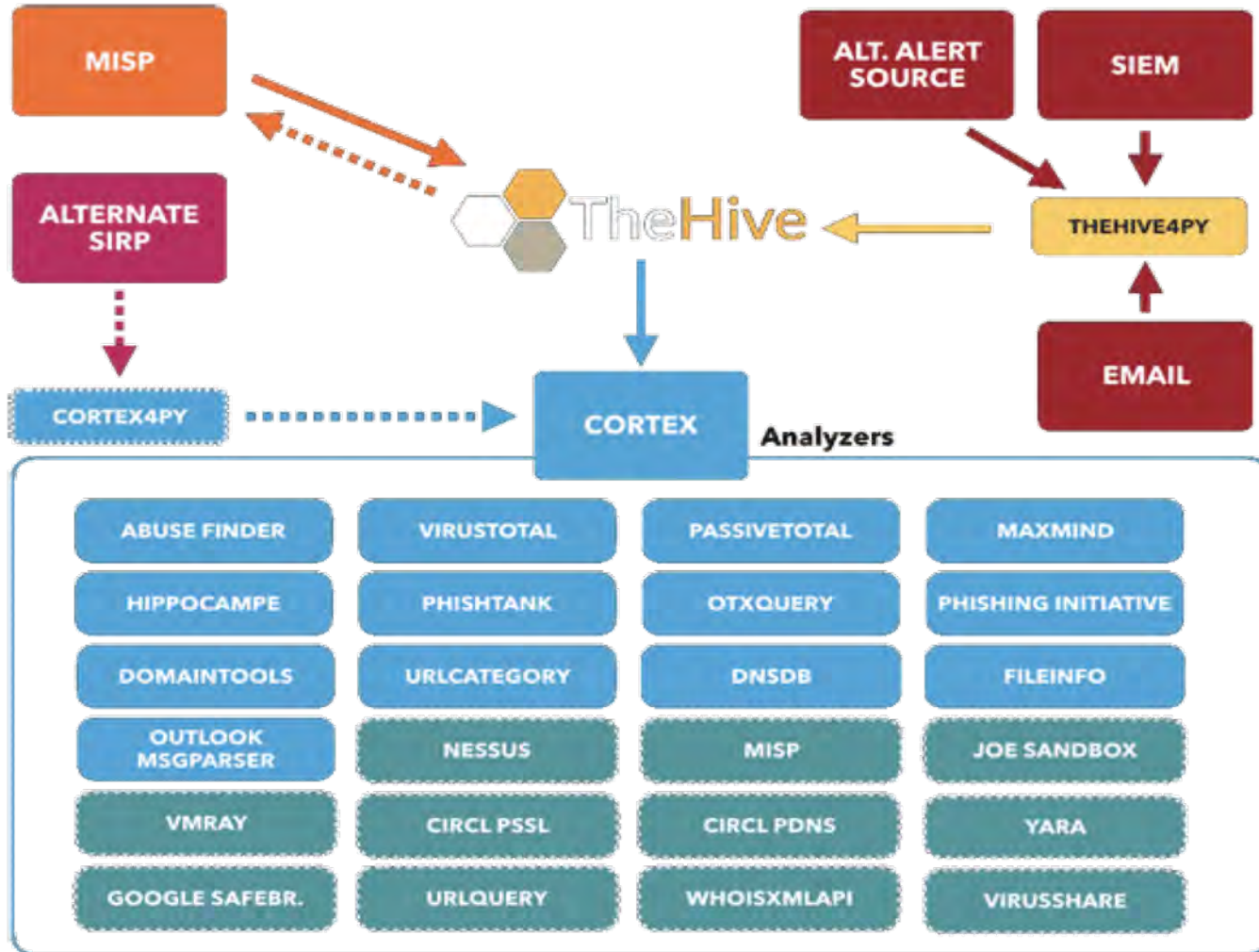


KZ-CERT

Служба реагирования на компьютерные инциденты Республики Казахстан



Журнал отработки инцидентов + Инструменты





KZ-CERT

Служба реагирования на компьютерные инциденты Республики Казахстан



Журнал отработки инцидентов + Инструменты

TheHive + New Case - My tasks 0 Waiting tasks 0 Alerts 0 Dashboards

Case, user, URL, hash, IP, domain ... Admin - admin

List of cases (24 of 24)

Quick Filters - Sort by + Stats Filters 100 per page

Statistics

Cases by Status		Case by Resolution		Top 5 tags	
Open	16	TruePositive	7	incident	7
Resolved	8	FalsePositive	1	CERT	5
				BOTNET	5
				Ботнеты	5
				Взлом	4

Title	Severity	Tasks	Observables	Assignee	Date
#28 - KZ_CERT_vulnerability_Drupal CVE-2018-7600 Drupal	M	No Tasks	0	BB	04/10/18 11:43
#27 - Сканирование портов 4786 4786 cisco CVE-2018-0171 CVE-2018-0156 (Closed at Wed, Apr 11th, 2018 8:47 +06:00 as False Positive)	M	4 Tasks	2	A	04/10/18 10:52
#26 - KZ_CERT_vulnerability vulnerability выявление уязвимости	M	5 Tasks	0	BB	04/09/18 17:14
#25 - Инциденты ИБ: Ботнеты Shadowserver && Team Cumry Ботнеты incident CERT BOTNET	L	No Tasks	0	HT	04/02/18 17:24

Open in new window Hide

✓ Closed by admin 10 minutes

Сканирование портов 4786

status: Resolved
resolutionStatus: FalsePositive
metrics: []
summary: Оповестили, Cisco не обнаружено. Возможно порт 4786 используется для других сервисов
impactStatus: NotApplicable

#27 - Сканирование портов 4786

✓ Completed by Валерий Велес 18 hours

уведомление по вновь выявленным IP - адреса

status: Completed

#26 - KZ_CERT_vulnerability уведомление по вновь выявленным IP - адреса

+ Added by Валерий Велес 18 hours

Валерий Велес

уведомления направлены 'info@voip.kz'; 'abuse@voip.kz'; 'abuse@intelsoft.com'; 'anton@dalanet.kz'; 'bmg-ur@mail.ru'; 'breu sovok@gmail.com'; 'gena@kisc.kz'; 'admin@ic.kz'; 'info@astana.network.kz'; 'abuse@astana.network.kz'; 'anton@dalanet.kz'; 'breus ...

#26 - KZ_CERT_vulnerability уведомление по вновь выявленным IP - адреса

+ Added by Валерий Велес 18 hours

Валерий Велес

новые IP - адреса 85.159.24.49 188.0.146.2 11 88.151.178.62 217.196.19.242 37.208.46.2 42 176.119.227.53 176.119.229.57 91.206.88.243 109.238.163.161 85.159.24.33 89.218.65.



KZ-CERT

Служба реагирования на компьютерные инциденты Республики Казахстан



Обмена данными об угрозах и инцидентах





KZ-CERT

Служба реагирования на компьютерные
инциденты Республики Казахстан

Спасибо за внимание!



incident @ kz-cert.kz

Call-center: 1400

www.kz-cert.kz