ПРАКТИКА МЕЖДУНАРОДНЫХ РЕАГИРОВАНИЙ НА ИНЦИДЕНТЫ ИБ
ВЗГЛЯД КРИМИНАЛИСТА НА SOC


ARE YOU READY?

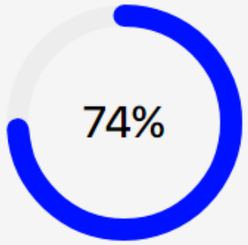
СТАТИСТИКА ГОТОВНОСТИ К РЕАГИРОВАНИЮ НА ИНЦИДЕНТЫ ИБ

State sponsored malware	40%
Watering hole	64%
Attack from 3rd party infrastructure	63%
Supply chain attacks	63%
Client-bank Attack	65%
Attack on payment processing systems	52%
Attack on ATMs	62%
Ransomware (encryption)	55%
Unauthorized access to servers	61%
Unauthorized access to DB	62%
Unauthorized access to web app or bypassing WAF	54%

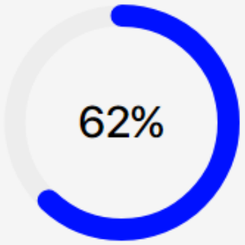
Unauthorized access to networking hardware	47%
Inside (data leak)	59%
Inside (sabotage)	59%
Inside (Unauthorized access)	63%
Inside (Unauthorized cryptocurrency mining)	63%
Classical malware (Trojans)	68%
Spear phishing attack (link)	70%
Spear phishing attack (attachment)	58%
Cryptocurrency mining via malware	66%
Intrusion attack	57%
DDOS	49%

На основе проверок на готовность более 100 компаний из различных отраслей

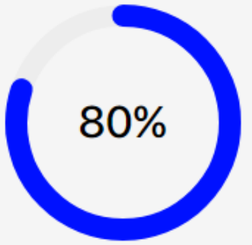
РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ В БАНКОВСКОЙ СФЕРЕ



Атакованных банков не было готово к реагированию на инцидент



Атакованных банков оказались не способны централизованно управлять своей сетью



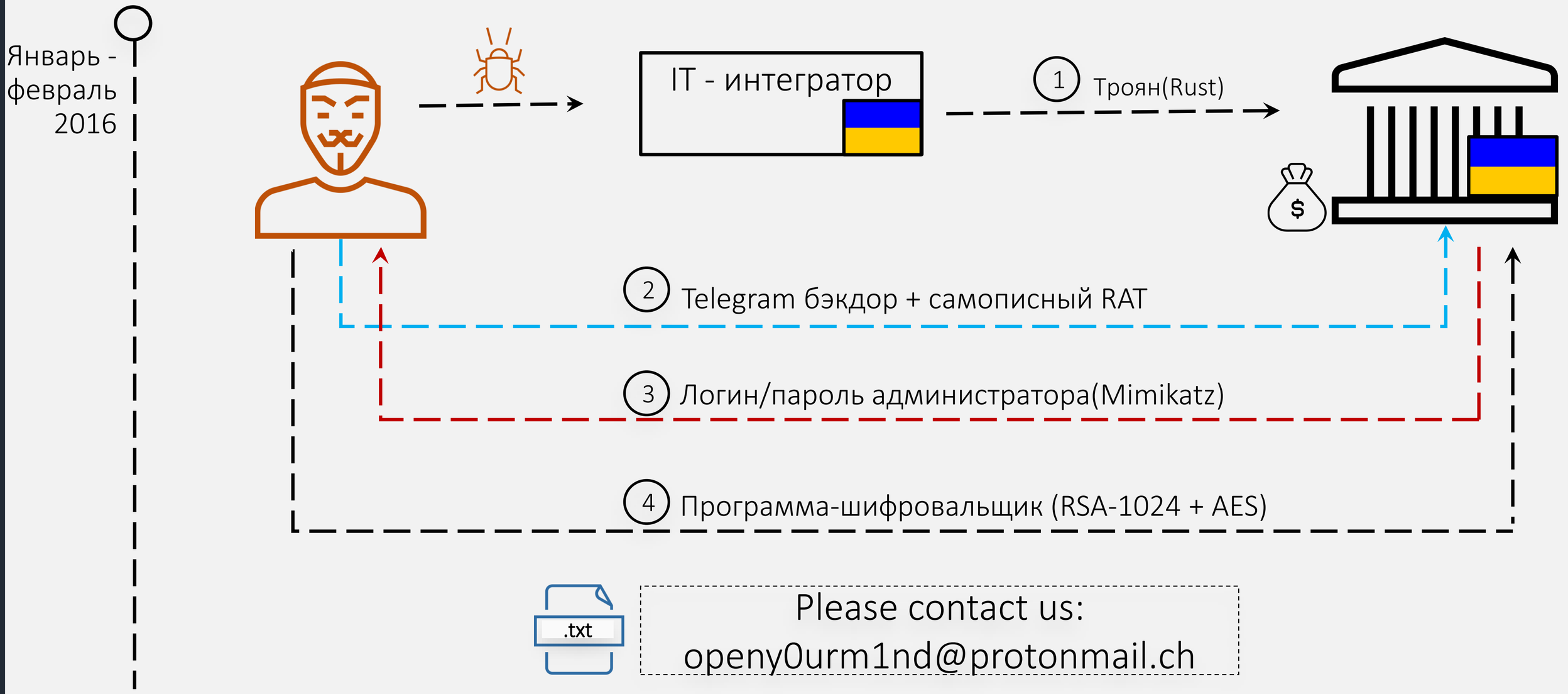
Атакованных банков не имели достаточно глубины журналирования

10 YEAR CHALLENGE

2009

2019

АТАКА ЧЕРЕЗ ПОСТАВЩИКА УСЛУГ



COBALT

С ноября 2016

Фишинг

Инфраструктура финансовой организации

Пользовательский сегмент:
- Кадровая служба
- Бухгалтерия
- Секретариат

Elevated Permissions

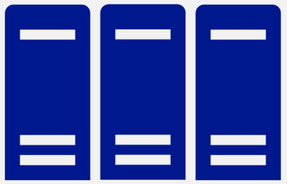
Сетевая инфраструктура:
- Административный сегмент
- Операционный сегмент

Банкоматы, процессинг, SWIFT

Scan Deep

Find Hidden Way

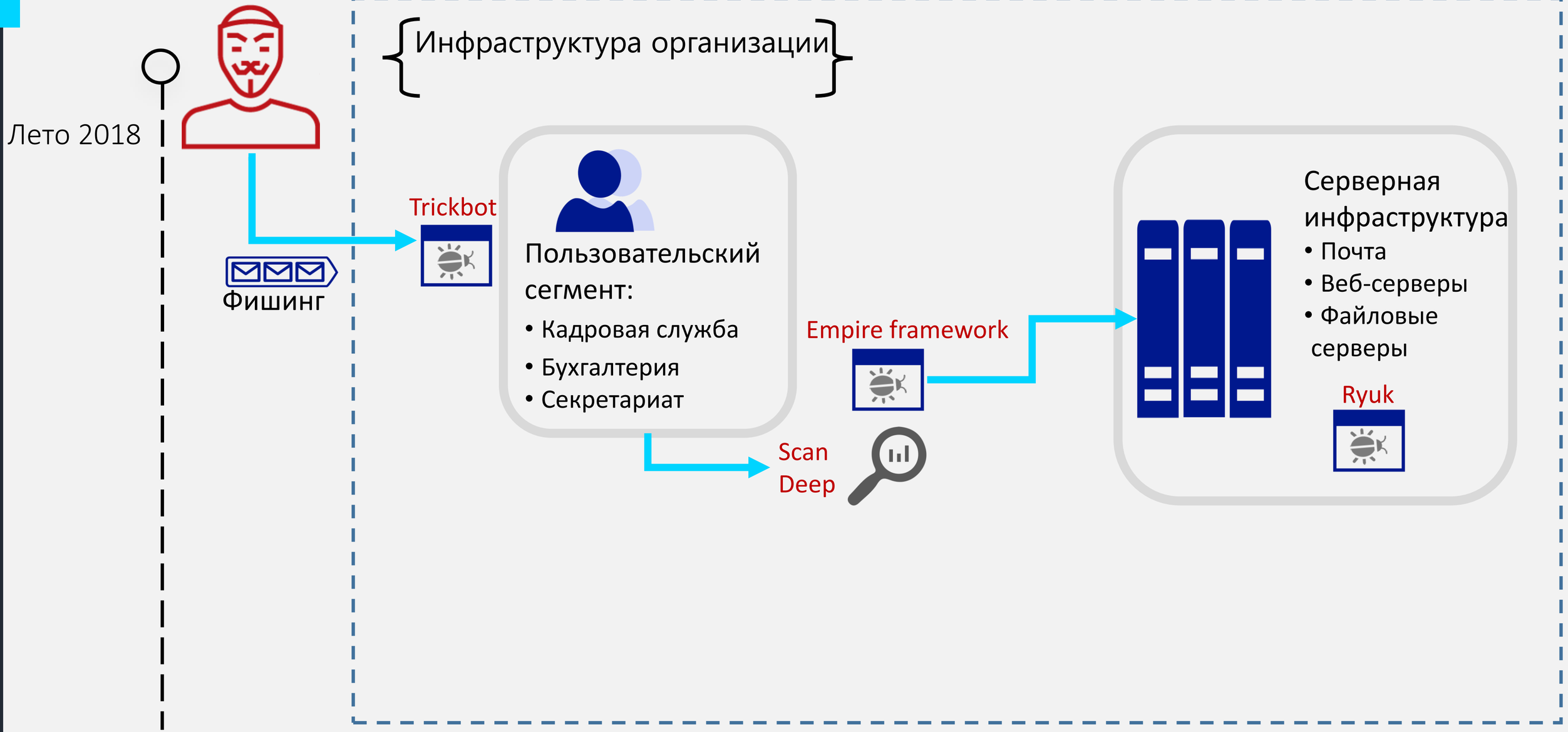
Malware



Серверная инфраструктура:
- Почта
- Веб-серверы
- Файловые серверы

Изолированный сегмент сети

RYUK И TRICKBOT



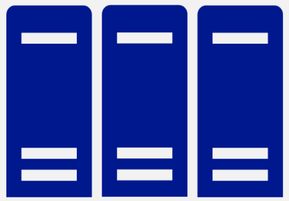
WANNAMINE HELLFIRE

Начало 2019

Retail

Monero Mining

WMI-class



Серверная инфраструктура:
- Почта
- Веб-серверы
- Файловые серверы
- Сервера управления складом

- Кассы и склады
- POS терминалы

Пользовательский сегмент:
- Кадровая служба
- Бухгалтерия
- Секретариат

Built-IN

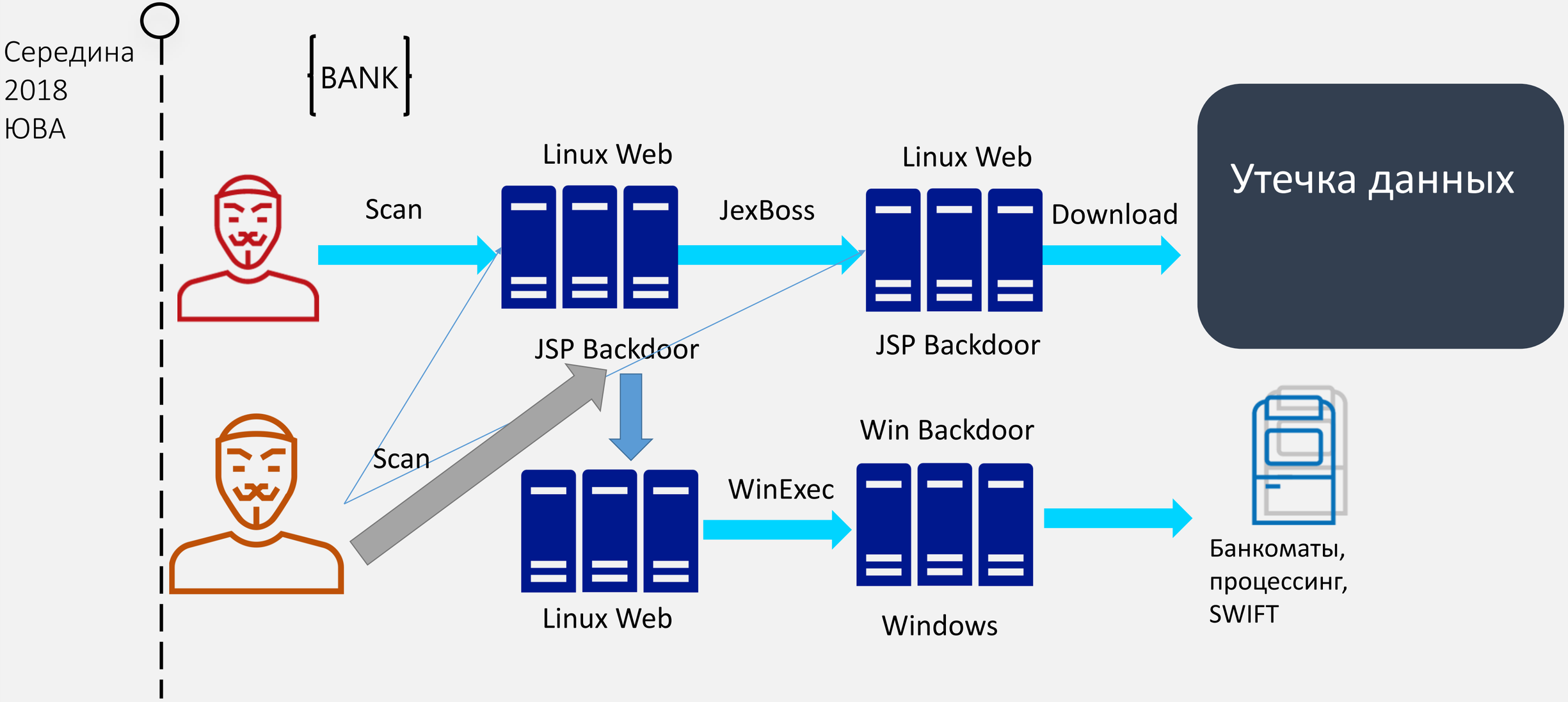
Mimikatz

Eternal Blue

Downloader

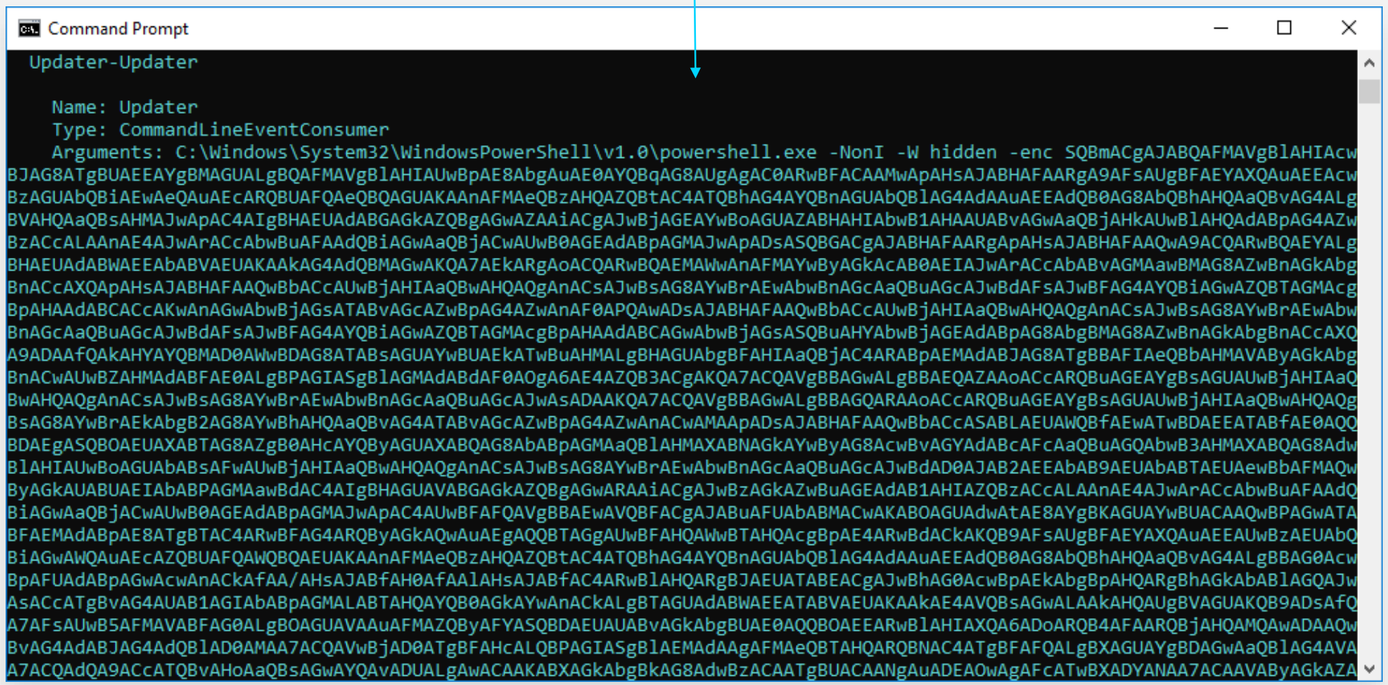
CPU LOAD 98%

2 в 1


Середина
2018
ЮВА
BANK
Linux Web
Scan
JexBoss
Linux Web
Download
Утечка данных
JSP Backdoor
JSP Backdoor
Scan
Win Backdoor
WinExec
Linux Web
Windows
Банкоматы,
процессинг,
SWIFT

СЛЕДЫ ЗАКРЕПЛЕНИЯ В СИСТЕМЕ: WMI EVENT SUBSCRIPTION

C:\WINDOWS\system32\wbem\Repository\OBJECTS.DATA



ЖИЗНЕННЫЙ ЦИКЛ АТАКИ НА ОКОНЕЧНОМ ХОСТЕ

MITRE ATT&CK ENTERPRISE MATRIX

GROUP-IB

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	33 items	58 items	28 items	63 items	19 items	20 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-hop Proxy
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Launchctl	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	Shared Webroot	Screen Capture		Multiband Communication
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Keychain	Remote System Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	LSASS Driver	Create Account	Launch Daemon	Disabling Security Tools	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking
	Mshta	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Network Sniffing	System Information Discovery	Third-party Software			Remote Access Tools
	PowerShell	Dylib Hijacking	Path Interception	DLL Side-Loading	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares			Remote File Copy
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management			Standard Application Layer Protocol
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery				Standard Cryptographic Protocol
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication Interception	System Service Discovery				Standard Non-Application Layer Protocol
	Scheduled Task	Hooking	Scheduled Task	File Permissions Modification		System Time Discovery				Uncommonly Used Port
	Scripting	Hypervisor	Service Registry Permissions Weakness	File System Logical Offsets						Web Service
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	Gatekeeper Bypass						
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	Hidden Files and Directories						
	Signed Script Proxy Execution	Launch Agent	Startup Items	Hidden Users						
	Source	Launch Daemon	Sudo	Hidden Window						
	Space after Filename	Launchctl		HISTCONTROL						
	Third-party Software			Image File Execution Options Injection						
	Trap									

legend

SOC


SOC
TI
Threat Intelligence
TH
Threat Hunting
IR
Incident Response

О КОМПАНИИ GROUP-IB

Group-IB — одна из ведущих международных компаний по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий

1000+

успешных расследований по всему миру, 160 особо сложных уголовных дел

$300 млн

возвращено клиентам Group-IB благодаря нашей работе

Официальный партнёр EUROPOL и INTERPOL

Рекомендована Организацией по безопасности и сотрудничеству в Европе (ОБСЕ)

Постоянный член Всемирного экономического форума

Threat Intelligence от Group-IB – в числе лучших мировых систем по оценке Forrester и Gartner

Одна из 7 самых влиятельных компаний в области кибербезопасности по версии Business Insider

Лидер российского рынка по исследованию киберугроз

О нас говорят: theguardian Bloomberg Forbes REUTERS Esquire

ПЕРВЫЙ КАНАЛ РОССИЙСКАЯ ГАЗЕТА ИЗВЕСТИЯ ВЕДОМОСТИ РОССИЯ 1 Коммерсантъ