kaspersky

Threat Intelligence & The hateful eight:

Common TTPs of the Modern Ransomware Groups

Nikita Nazarov
Head of Threat Exploration

Vladislav Burtsev
Threat Intelligence Analyst

Dmitry Galov
Senior Security Researcher

Масштаб современных кибератак

1

Средний ущерб от успешной кибератаки

SMB: 105k$
Enterprise: ~1M$

2

Отношение лидеров бизнеса

68% лидеров бизнеса считают, что риски, связанные с кибербезопасностью, растут

3

Мотивация атак

71% атак были финансово мотивированными

4

Оценка активности шифровальщиков

На 181% выросла доля детектируемых ежедневно программ-вымогателей

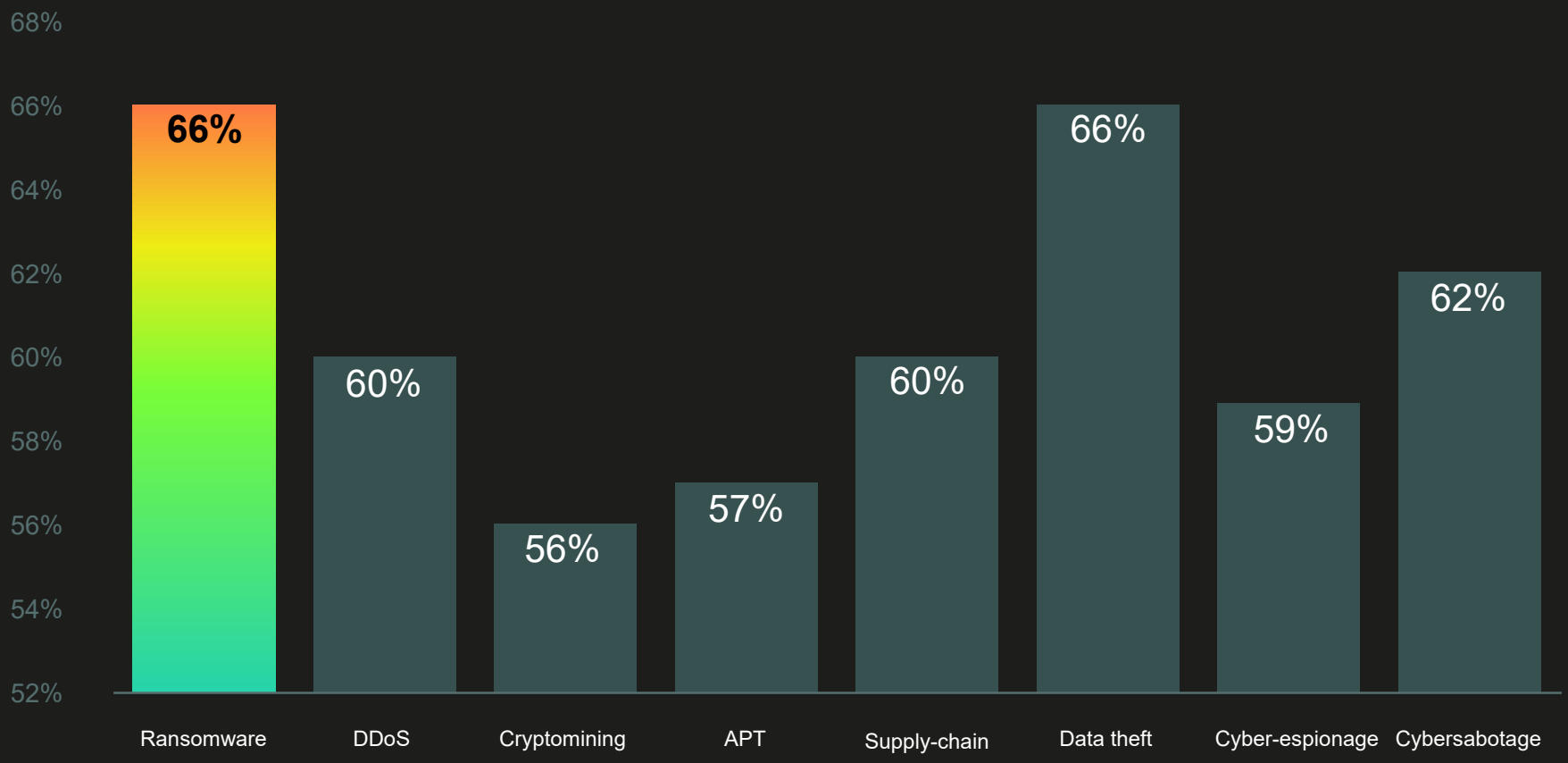
5

Последствия

Ежедневно эксперты “Лаборатории Касперского” находили в среднем 9500 зашифрованных такими зловредами файлов

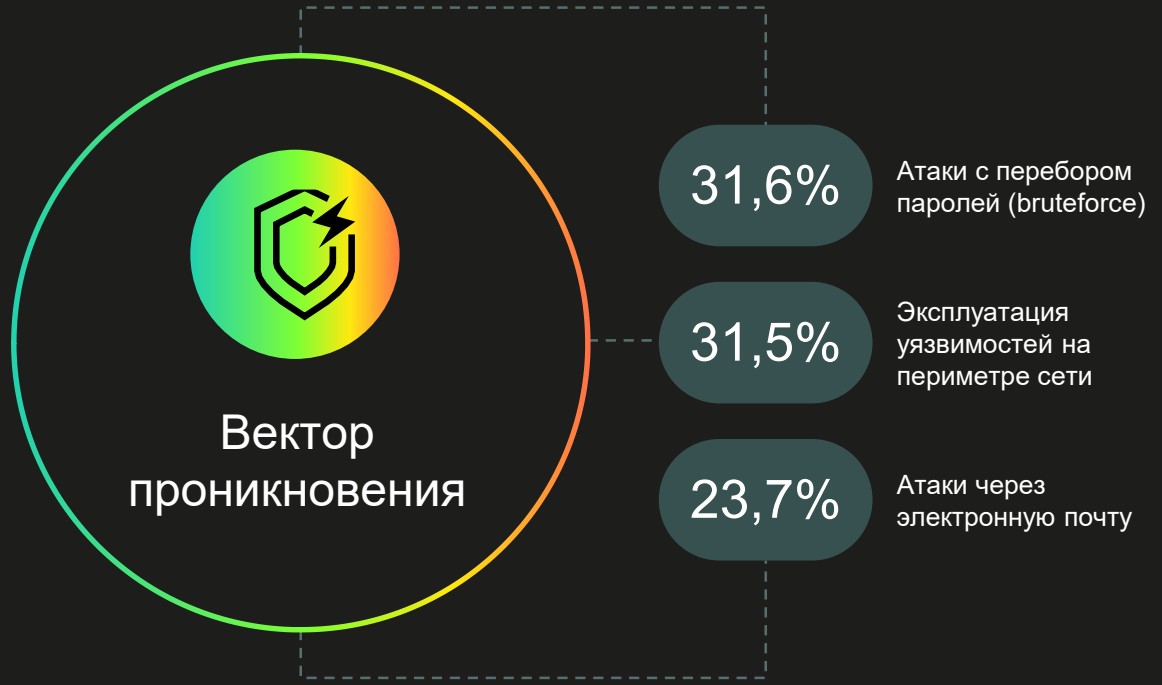
Источники данных: Kaspersky, Accenture, Verizon

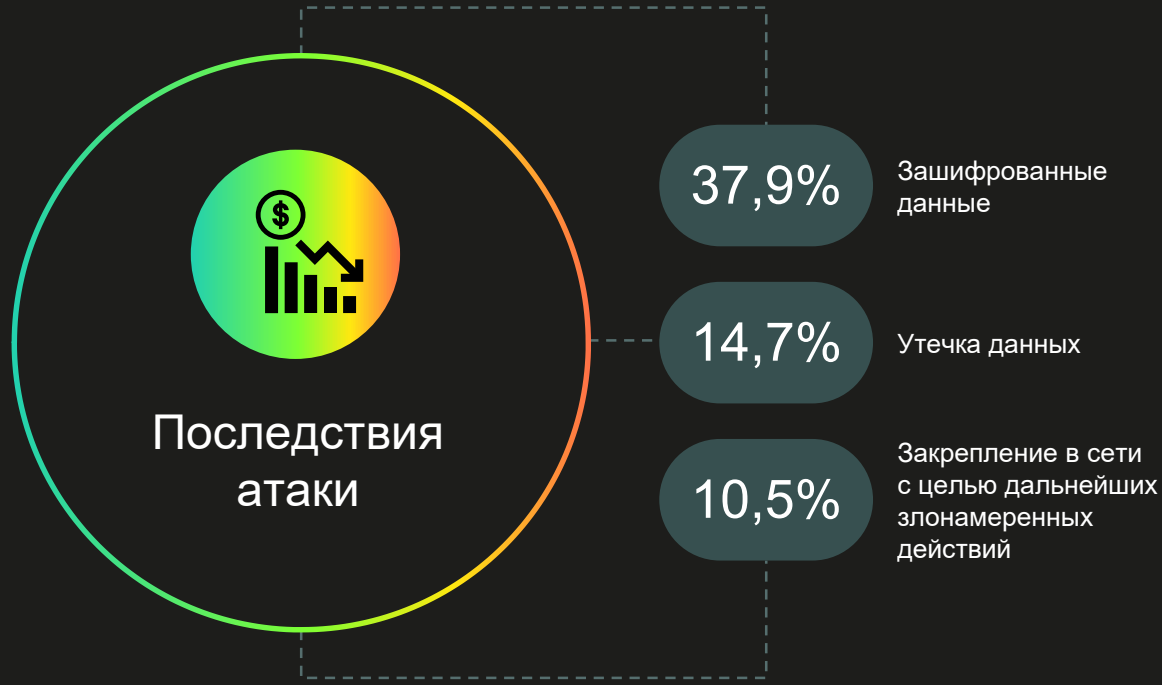
Опрос: Вероятность различных типов угроз



Источник: Kaspersky Survey, 2022

Общая информация по шифровальщикам





Индустрии

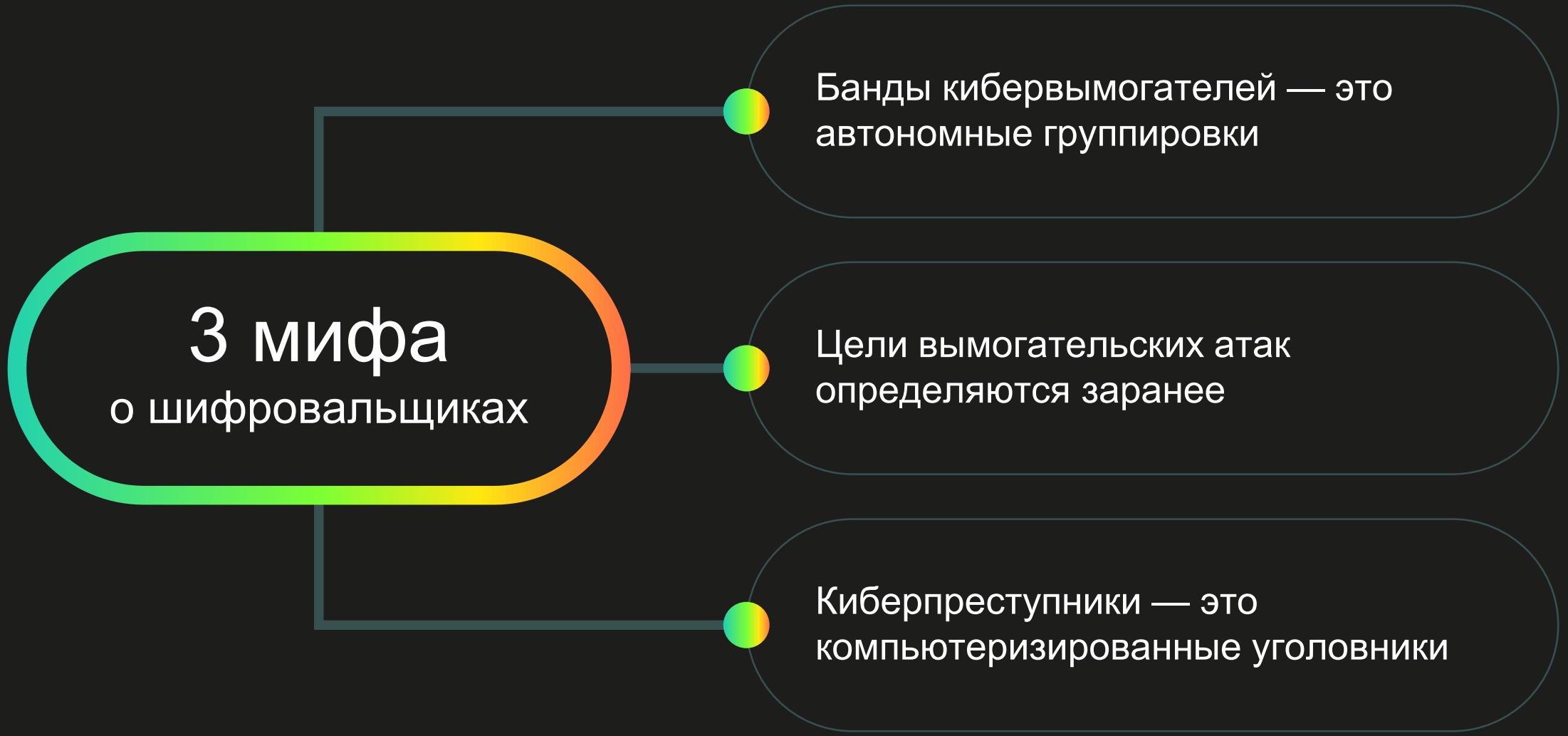
22%	19%	13%	13%
Промышленные предприятия	Государственный сектор	Финансовые организации	Телекоммуникации

Регионы

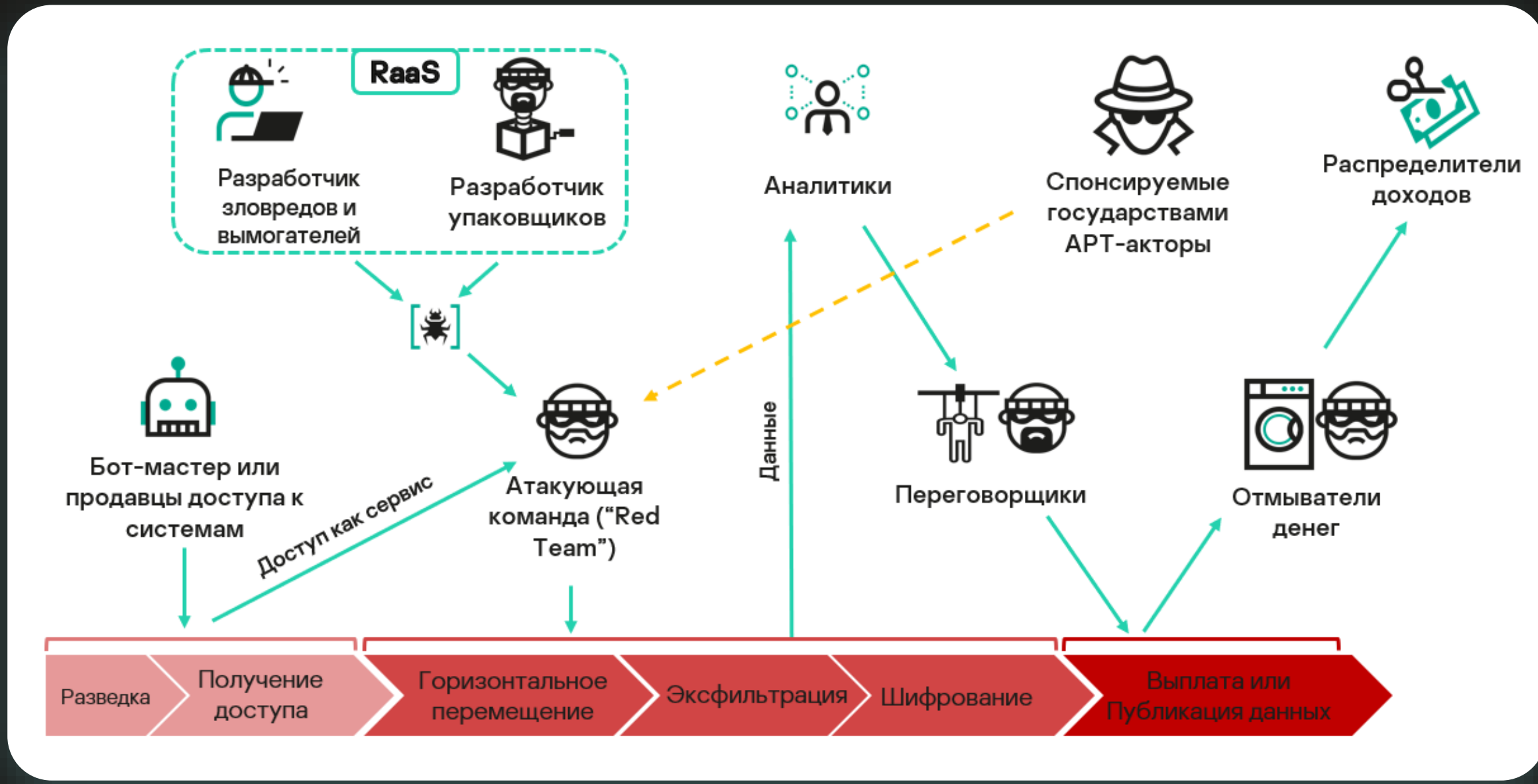
27,8%	26,8%	24,7%	16,5%
СНГ	Ближний Восток и Африка	Европа	Америки

Источник: Incident Response Analyst Report, Kaspersky

Популярные мифы о шифровальщиках



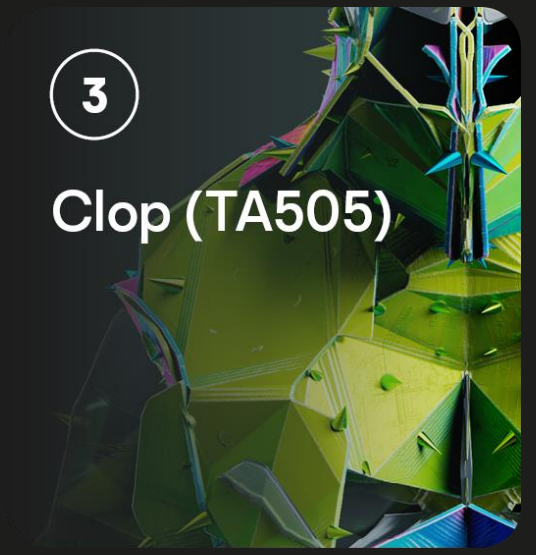
Экосистема вымогательского «бизнеса»

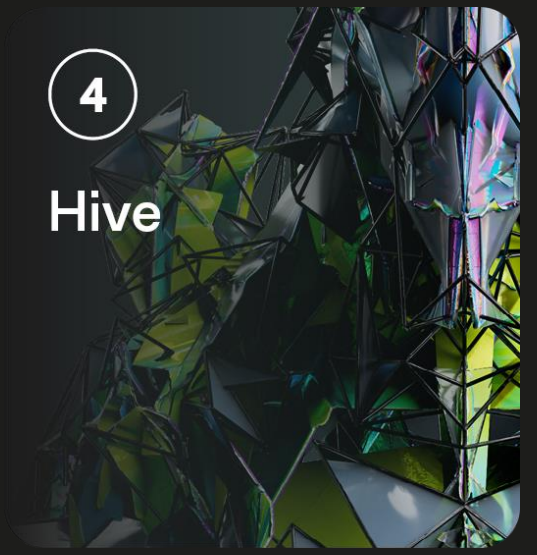


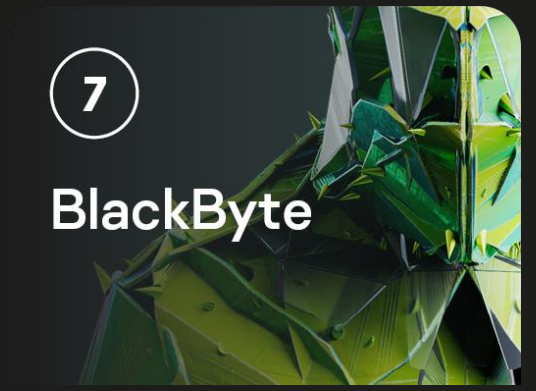
На основе нашей статистики мы составили график появления новых группировок Ransomware

2017	Фев	PClock	WannaCry	Erebus	PetrWrap	Crypat	Hermes	AecHu
	Март	Matrix	Pycl	BTCWare				
	Апр	Poster	Ranion	Tiny	Everbe			
	Май	Manna	Ferber	Jaff	Rao	Savant		
	Июнь	Fairy	MacRansom	Erebus	NotPetya			
	Авг	Nubi						
	Окт	Magni	Pyrgen	BadRabbit				
	Нояб	Phobos	Ordin					
	Дек	Clop						
2018	Янв	GandCrab						
	Апр	WhiteRose	BlackHeart					
	Авг	Ryuk						
	Сент	LimeRat						
	Окт	WannaCash	Scrobo	Dcrtr				
	Нояб	Stop/DJVU						
2019	Янв	Anatova	MegaCortex					
	Фев	Vega						
	Март	JNEC	RobbinHood					
	Май	JSWorm	Wesker	Maze				
	Июнь	VoidCrypt						
	Июль	DoppelPaymer						
	Сент	NetWalker						
	Окт	Medusa	Snatch					
	Нояб	Thanos	NextCry	WastedLocker				
	Дек	Lockbit	PwndLocker	DMR				
2020	Янв	Makop	Bitpylock					
	Фев	RagnarLocker	Conti	Cuba	Sorena			
	Март	TeslaRvng	Blackin					
	Апр	WannaRen	Ransomexx	Sfile				
	Май	Snake						
	Июнь	Avaddon	GottaCrypt					
	Июль	EvilQuest	Fonix					
	Авг	Darkside	XmrLocker					
	Сент	MountLocker						
	Окт	Egregor						
	Нояб	HelloKitty	CoronaLock					
	Дек	Suncrypt	DeathRansom	Cring	Babuk	Hades		
2021	Янв	Lorenz	Pysa					
	Март	Quoter						
	Апр	Jesus	Qlocker					
	Май	DiscoRan	Everest					
	Июнь	Hive	Zikma					
	Июль	AvosLocker	Scrypt	BlackMatter				
	Авг	Loki	LockFile					
	Сент	Chaos	Blackbyte	Colossus				
	Окт	Diavol	Prans					
	Нояб	Polaris	Rook	Surtr	Sabbath			
	Дек	BlackCat						
2022	Янв	NightSky						
	Фев	Stormous	Krus	Hermetic				
	Март	Freeud	Pandora					

Восемь наиболее активных групп Ransomware



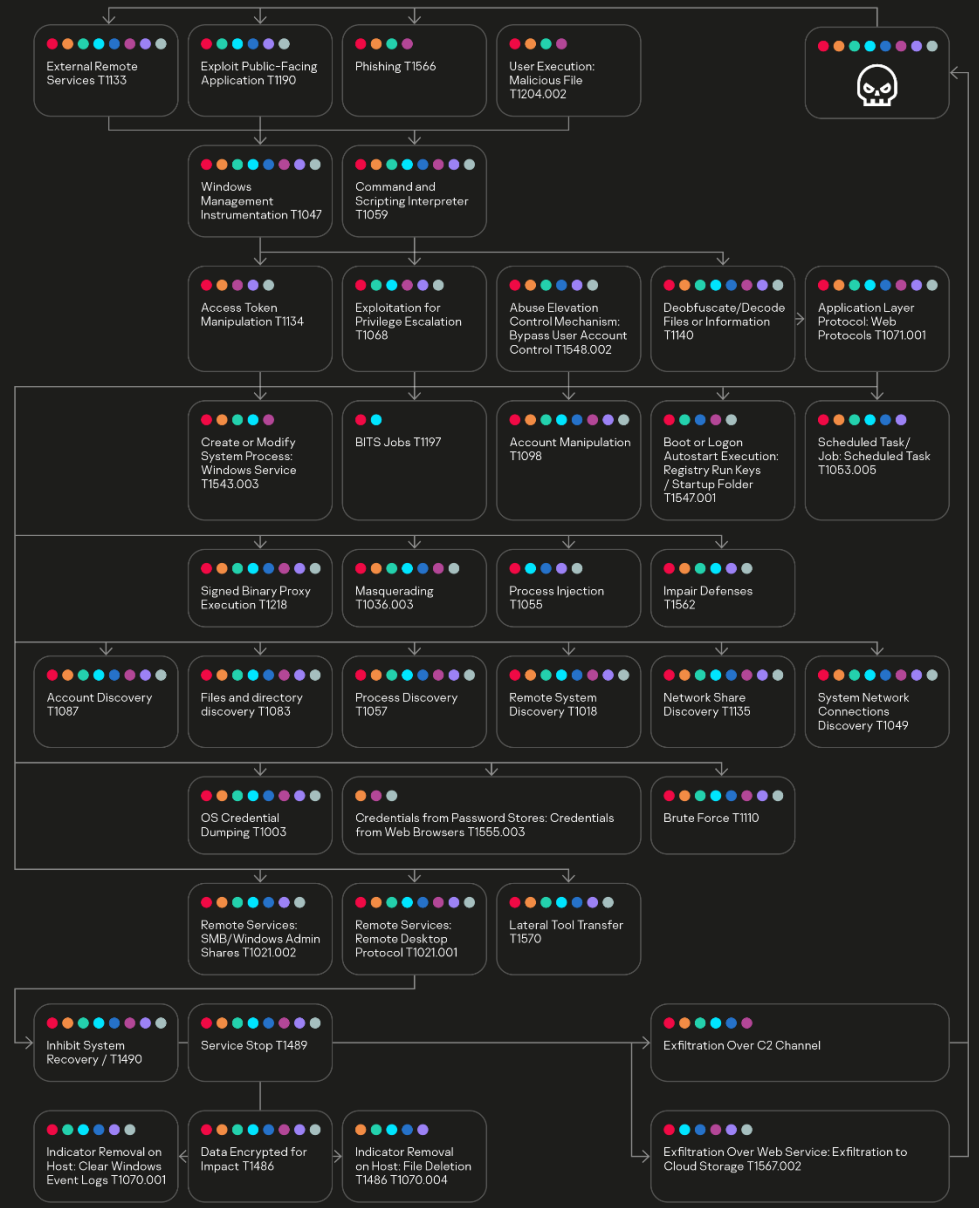




Cyber Kill Chain

- Conti/Ryuk
- Pysa
- Lockbit 2.0
- RagnarLocker
- Clop (TA505)
- Hive
- BlackByte
- BlackCat

Чтобы выделить общие паттерны различных схем атак и TTPs, используемые различными группами вымогателей, мы создали диаграмму Cyber Kill Chain



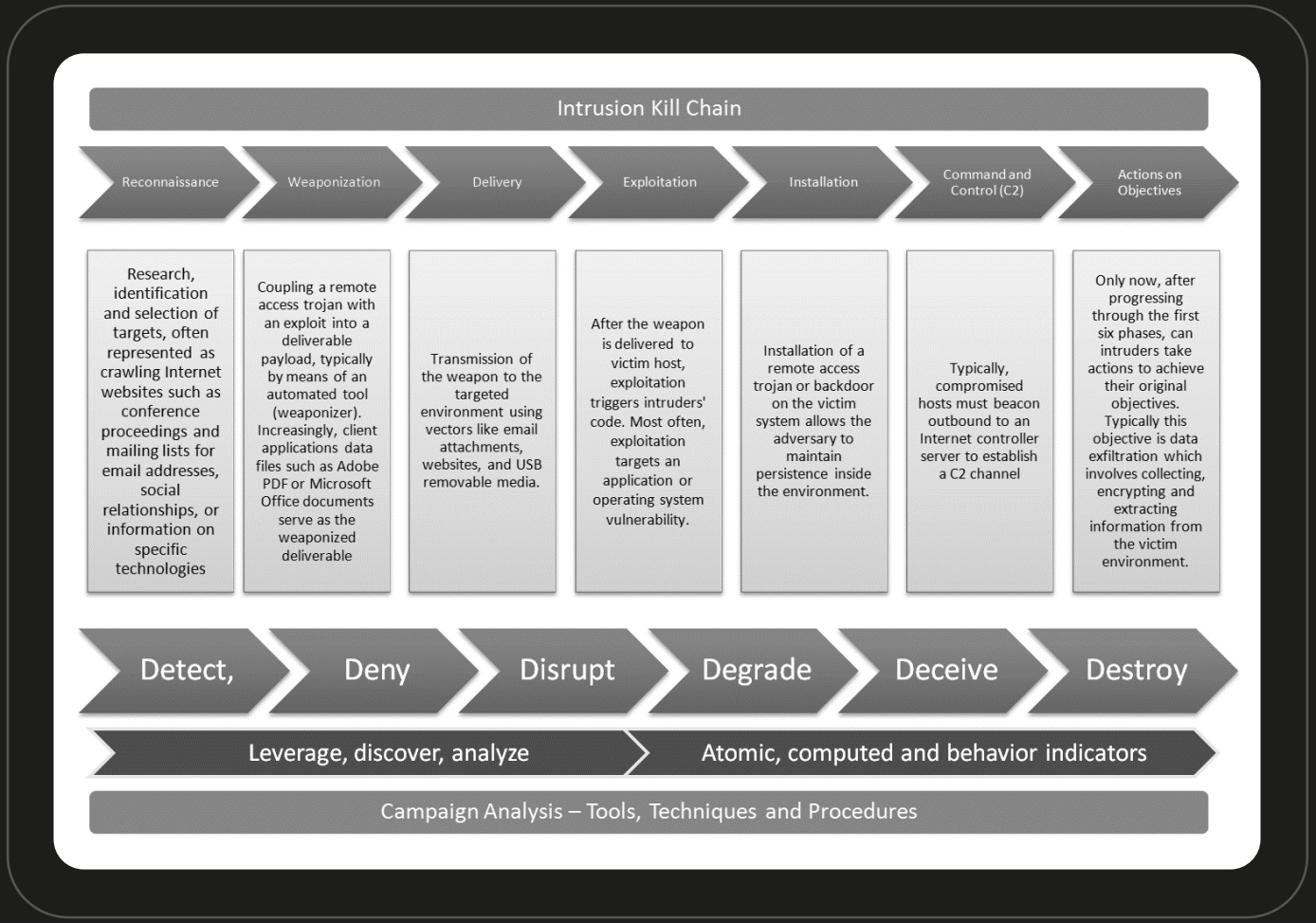
Cyber Kill Chain

1996 F2T2EA

2011 Cyber Kill Chain

2012 Intelligence — Driven Defense

2013 ATT&CK Matrix



F2T2EA

1996 F2T2EA

2011 Cyber Kill Chain

2012 Intelligence — Driven Defense

2013 ATT&CK Matrix

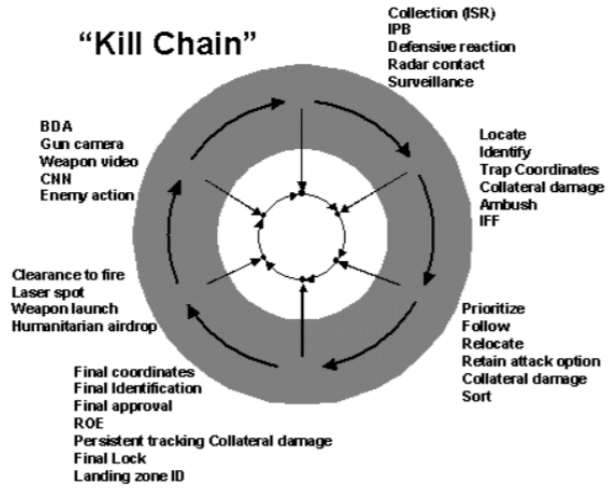


Figure 1-1. F2T2EA

The Find, Fix, Track Target, Engage, Assess (F2T2EA) methodology seen in Figure 1-1 mechanizes the operational level "kill chain" during the execution process. Theater and national assets/resources detect objectives of potential significance (find). These systems identify and determine the location of a target (fix). From this location, tracking systems acquire and monitor the object (track). Dynamic decision-making then directs resources (target), and applies capabilities (engage) in a timely and decisive manner. To assure the desired effect, an assessment (assess) occurs during or after engagement to determine whether the target should be reattacked. These sequential steps describe a critical path that must occur for each dynamic event.

TABLE I. KEY INDICATORS OF KILL CHAINS

Phase	Indicators
Find	detection range(km), transmit power(kW), endurance(h), working frequency(MHz), pulse width(μs)，pulse repetition rate(kHz), antenna length(m), radome thickness(m), azimuth beam width(°), elevation beam width(°)，antenna side lobe（dB）
Fix	transmit power(kW), received frequency(MHz), dynamic range(dB), sensitivity(dBv), output power(kW), MTBF(h), peak power(w), recognition range (km)
Track	target tracking capacity, angular accuracy(°), velocity measurement range（kn），clutter improvement factor(dB), operating range(km), endurance(h), MTBF(h)
Target	navigation capability, target processing capacity, azimuth(°), data transfer rate(kbps), working frequency(MHz), operating range(km)
Engage	tactical range(km), service ceiling(m), maximum suspension weight(kg), maximum level flight speed(km/h), hitting probability(%),maximum attack range(km), maximum missile speed(km/h)
Assess	endurance(h), transmit frequency(MHz), received frequency(MHz), dynamic range(dB), sensitivity(dBv) , operating range(km) , MTBF(h)

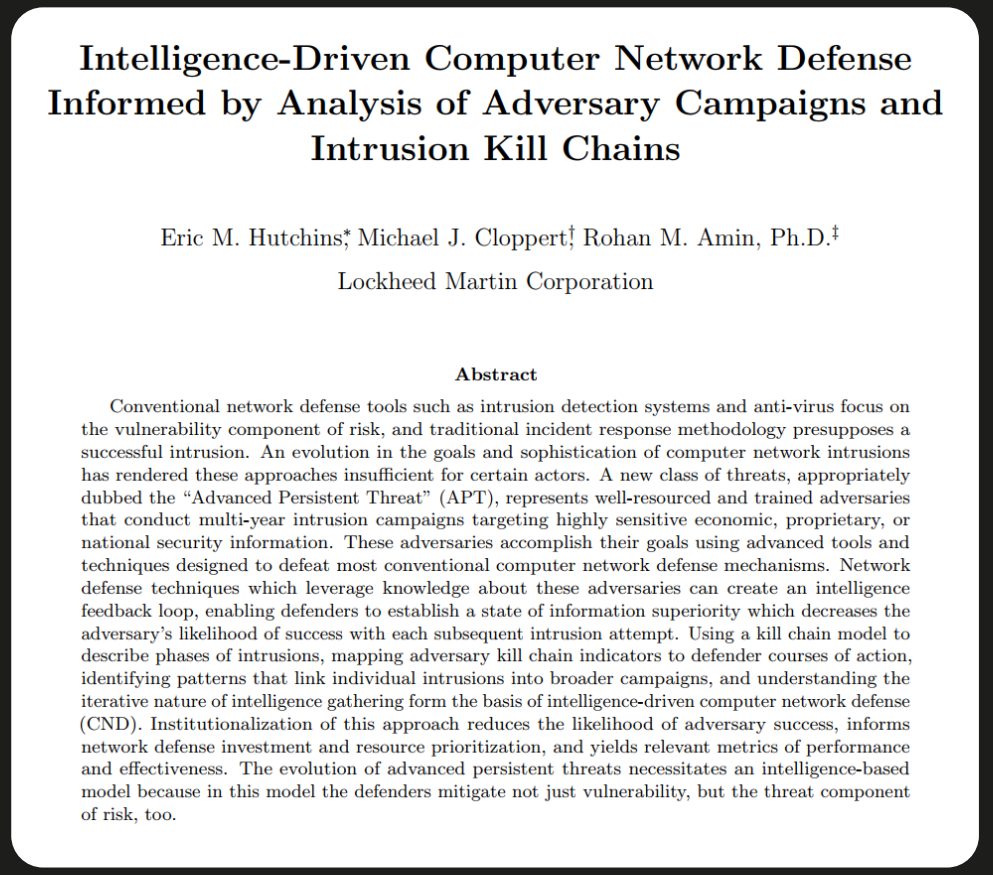
Intelligence-Driven Defense

1996 F2T2EA

2011 Cyber Kill Chain

2012 Intelligence — Driven Defense

2013 ATT&CK Matrix



Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

Eric M. Hutchins*, Michael J. Cloppert†, Rohan M. Amin, Ph.D.‡

Lockheed Martin Corporation

Abstract

Conventional network defense tools such as intrusion detection systems and anti-virus focus on the vulnerability component of risk, and traditional incident response methodology presupposes a successful intrusion. An evolution in the goals and sophistication of computer network intrusions has rendered these approaches insufficient for certain actors. A new class of threats, appropriately dubbed the "Advanced Persistent Threat" (APT), represents well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information. These adversaries accomplish their goals using advanced tools and techniques designed to defeat most conventional computer network defense mechanisms. Network defense techniques which leverage knowledge about these adversaries can create an intelligence feedback loop, enabling defenders to establish a state of information superiority which decreases the adversary's likelihood of success with each subsequent intrusion attempt. Using a kill chain model to describe phases of intrusions, mapping adversary kill chain indicators to defender courses of action, identifying patterns that link individual intrusions into broader campaigns, and understanding the iterative nature of intelligence gathering form the basis of intelligence-driven computer network defense (CND). Institutionalization of this approach reduces the likelihood of adversary success, informs network defense investment and resource prioritization, and yields relevant metrics of performance and effectiveness. The evolution of advanced persistent threats necessitates an intelligence-based model because in this model the defenders mitigate not just vulnerability, but the threat component of risk, too.

Intelligence-Driven Defense — Courses of Action

1996 F2T2EA

2011 Cyber Kill Chain

2012 Intelligence — Driven Defense

2013 ATT&CK Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	“chroot” jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

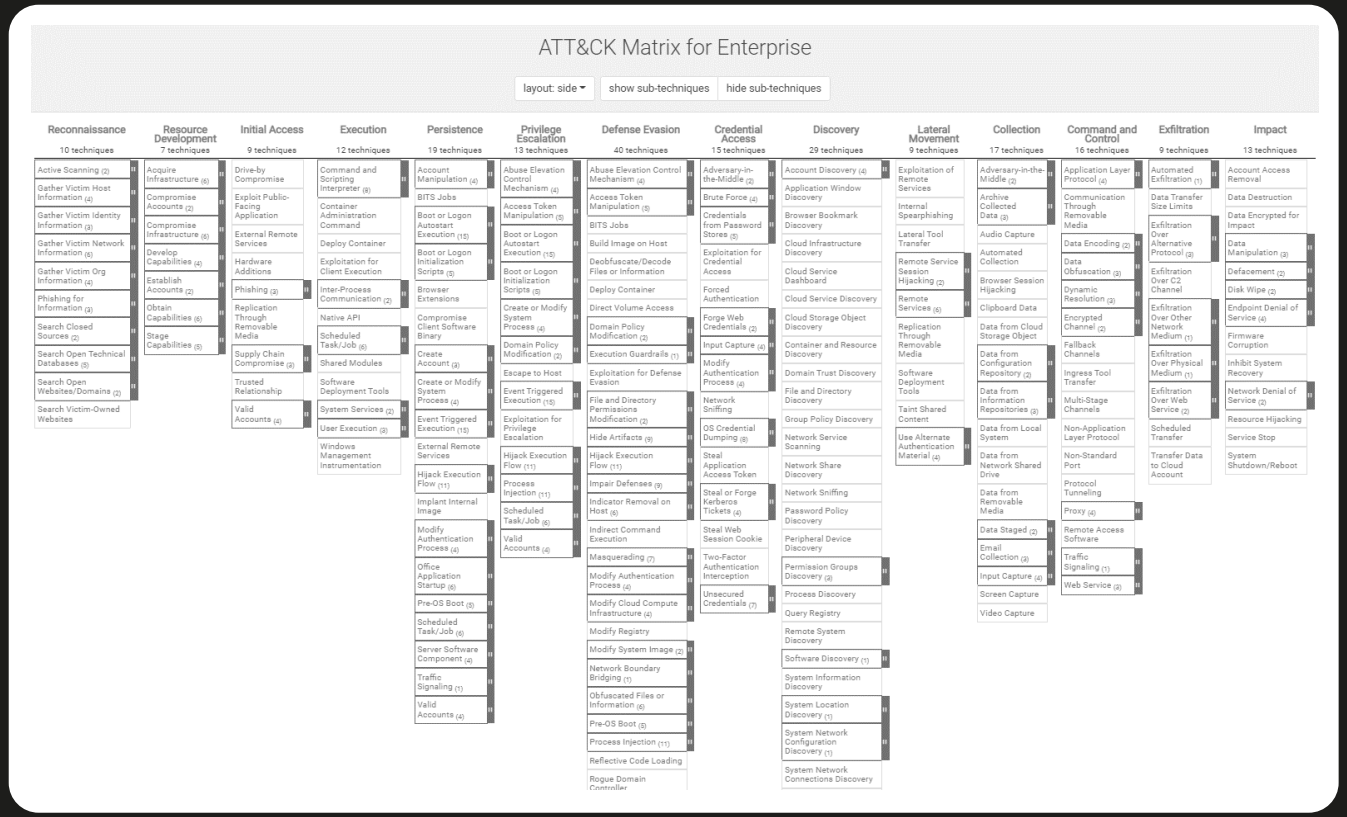
MITRE ATT&CK

1996 F2T2EA

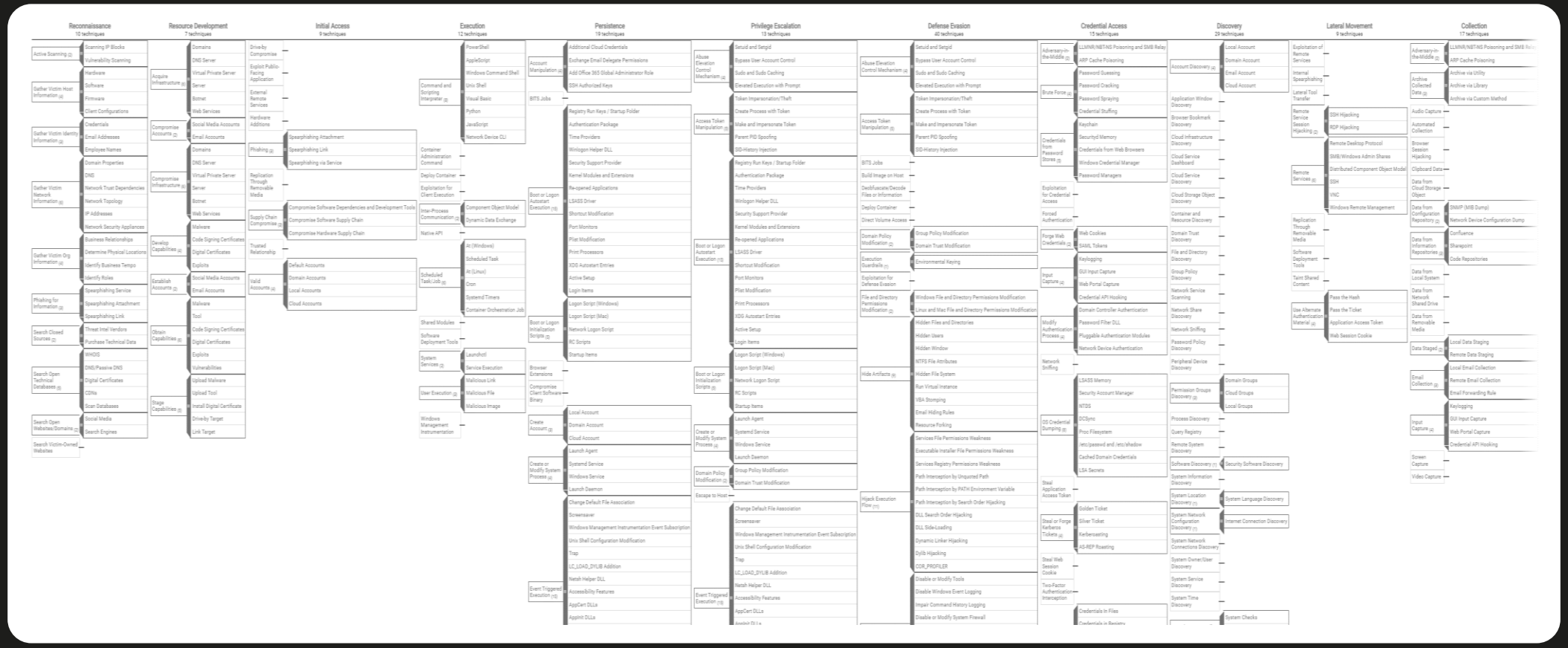
2011 Cyber Kill Chain

2012 Intelligence – Driven Defense

2013 ATT&CK Matrix



MITRE ATT&CK


Reconnaissance
10 techniques
Active Scanning (2)
Scanning IP Blocks
Vulnerability Scanning
Gather Victim Host Information (4)
Hardware
Software
Firmware
Client Configurations
Gather Victim Identity Information (3)
Credentials
Email Addresses
Employee Names
Gather Victim Network Information (6)
Domain Properties
DNS
Network Trust Dependencies
Network Topology
IP Addresses
Network Security Appliances
Gather Victim Org Information (4)
Business Relationships
Determine Physical Locations
Identify Business Tempo
Identify Roles
Phishing for Information (3)
Spearphishing Service
Spearphishing Attachment
Spearphishing Link
Search Closed Sources (2)
Threat Intel Vendors
Purchase Technical Data
Search Open Technical Databases (5)
WHOIS
DNS/Passive DNS
Digital Certificates
CDNs
Scan Databases
Search Open Websites/Domains (2)
Social Media
Search Engines
Search Victim-Owned Websites
Resource Development
7 techniques
Acquire Infrastructure (8)
Domains
DNS Server
Virtual Private Server
Server
Botnet
Web Services
Compromise Accounts (2)
Social Media Accounts
Email Accounts
Compromise Infrastructure (6)
Domains
DNS Server
Virtual Private Server
Server
Botnet
Web Services
Develop Capabilities (4)
Malware
Code Signing Certificates
Digital Certificates
Exploits
Establish Accounts (2)
Social Media Accounts
Email Accounts
Obtain Capabilities (6)
Malware
Tool
Code Signing Certificates
Digital Certificates
Exploits
Vulnerabilities
Stage Capabilities (5)
Upload Malware
Upload Tool
Install Digital Certificate
Drive-by Target
Link Target
Initial Access
9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (3)
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Replication Through Removable Media
Supply Chain Compromise (3)
Compromise Software Dependencies and Development Tools
Compromise Software Supply Chain
Compromise Hardware Supply Chain
Trusted Relationship
Valid Accounts (4)
Default Accounts
Domain Accounts
Local Accounts
Cloud Accounts
Execution
12 techniques
Command and Scripting Interpreter (8)
PowerShell
AppleScript
Windows Command Shell
Unix Shell
Visual Basic
Python
JavaScript
Network Device CLI
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (3)
Component Object Model
Dynamic Data Exchange
Native API
Scheduled Task/Job (6)
At (Windows)
Scheduled Task
At (Linux)
Cron
Systemd Timers
Container Orchestration Job
Shared Modules
Software Deployment Tools
System Services (2)
Launchctl
Service Execution
User Execution (3)
Malicious Link
Malicious File
Malicious Image
Windows Management Instrumentation
Persistence
19 techniques
Account Manipulation (5)
Additional Cloud Credentials
Exchange Email Delegate Permissions
Add Office 365 Global Administrator Role
SSH Authorized Keys
BITS Jobs
Boot or Logon Autostart Execution (15)
Registry Run Keys / Startup Folder
Authentication Package
Time Providers
Winlogon Helper DLL
Security Support Provider
Kernel Modules and Extensions
Re-opened Applications
LSASS Driver
Shortcut Modification
Port Monitors
Print Processors
XDG Autostart Entries
Active Setup
Login Items
Logon Script (Windows)
Logon Script (Mac)
Network Logon Script
RC Scripts
Startup Items
Boot or Logon Initialization Scripts (5)
Browser Extensions
Compromise Client Software Binary
Create Account (3)
Local Account
Domain Account
Cloud Account
Create or Modify System Process (4)
Launch Agent
Systemd Service
Windows Service
Launch Daemon
Event Triggered Execution (15)
Change Default File Association
Screensaver
Windows Management Instrumentation Event Subscription
Unix Shell Configuration Modification
Trap
LC_LOAD_DYLIB Addition
Netsh Helper DLL
Accessibility Features
AppCert DLLs
AppInit DLLs
Privilege Escalation
13 techniques
Abuse Elevation Control Mechanism (4)
Setuid and Setgid
Bypass User Account Control
Sudo and Sudo Caching
Elevated Execution with Prompt
Access Token Manipulation (5)
Token Impersonation/Theft
Create Process with Token
Make and Impersonate Token
Parent PID Spoofing
SID-History Injection
Boot or Logon Autostart Execution (15)
Registry Run Keys / Startup Folder
Authentication Package
Time Providers
Winlogon Helper DLL
Security Support Provider
Kernel Modules and Extensions
Re-opened Applications
LSASS Driver
Shortcut Modification
Port Monitors
Print Processors
XDG Autostart Entries
Active Setup
Login Items
Logon Script (Windows)
Logon Script (Mac)
Network Logon Script
RC Scripts
Startup Items
Boot or Logon Initialization Scripts (5)
Launch Agent
Systemd Service
Windows Service
Launch Daemon
Create or Modify System Process (4)
Domain Policy Modification (2)
Group Policy Modification
Domain Trust Modification
Escape to Host
Event Triggered Execution (15)
Change Default File Association
Screensaver
Windows Management Instrumentation Event Subscription
Unix Shell Configuration Modification
Trap
LC_LOAD_DYLIB Addition
Netsh Helper DLL
Accessibility Features
AppCert DLLs
Defense Evasion
40 techniques
Abuse Elevation Control Mechanism (4)
Setuid and Setgid
Bypass User Account Control
Sudo and Sudo Caching
Elevated Execution with Prompt
Access Token Manipulation (5)
Token Impersonation/Theft
Create Process with Token
Make and Impersonate Token
Parent PID Spoofing
SID-History Injection
BITS Jobs
Build Image on Host
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (2)
Group Policy Modification
Domain Trust Modification
Execution Guardrails (1)
Environmental Keying
Exploitation for Defense Evasion
File and Directory Permissions Modification (2)
Windows File and Directory Permissions Modification
Linux and Mac File and Directory Permissions Modification
Hide Artifacts (6)
Hidden Files and Directories
Hidden Users
Hidden Window
NTFS File Attributes
Hidden File System
Run Virtual Instance
VBA Stomping
Email Hiding Rules
Resource Forking
Hijack Execution Flow (11)
Services File Permissions Weakness
Executable Installer File Permissions Weakness
Services Registry Permissions Weakness
Path Interception by Unquoted Path
Path Interception by PATH Environment Variable
Path Interception by Search Order Hijacking
DLL Search Order Hijacking
DLL Side-Loading
Dynamic Linker Hijacking
Dylib Hijacking
COR_PROFILER
Disable or Modify Tools
Disable Windows Event Logging
Impair Command History Logging
Disable or Modify System Firewall
Credential Access
15 techniques
Adversary-in-the-Middle (3)
LLMNR/NBT-NS Poisoning and SMB Relay
ARP Cache Poisoning
Brute Force (4)
Password Guessing
Password Cracking
Password Spraying
Credential Stuffing
Credentials from Password Stores (3)
Keychain
Securityd Memory
Credentials from Web Browsers
Windows Credential Manager
Password Managers
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (2)
Web Cookies
SAML Tokens
Input Capture (4)
Keylogging
GUI Input Capture
Web Portal Capture
Credential API Hooking
Modify Authentication Process (4)
Domain Controller Authentication
Password Filter DLL
Pluggable Authentication Modules
Network Device Authentication
Network Sniffing
OS Credential Dumping (8)
LSASS Memory
Security Account Manager
NTDS
DCSync
Proc Filesystem
/etc/passwd and /etc/shadow
Cached Domain Credentials
LSA Secrets
Steal Application Access Token
Steal or Forge Kerberos Tickets (4)
Golden Ticket
Silver Ticket
Kerberoasting
AS-REP Roasting
Steal Web Session Cookie
Two-Factor Authentication Interception
Credentials In Files
Discovery
29 techniques
Account Discovery (4)
Local Account
Domain Account
Email Account
Cloud Account
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (3)
Domain Groups
Cloud Groups
Local Groups
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (1)
Security Software Discovery
System Information Discovery
System Location Discovery (1)
System Language Discovery
System Network Configuration Discovery (1)
Internet Connection Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
System Checks
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
SSH Hijacking
RDP Hijacking
Remote Services (6)
Remote Desktop Protocol
SMB/Windows Admin Shares
Distributed Component Object Model
SSH
VNC
Windows Remote Management
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (4)
Pass the Hash
Pass the Ticket
Application Access Token
Web Session Cookie
Collection
17 techniques
Adversary-in-the-Middle (2)
LLMNR/NBT-NS Poisoning and SMB Relay
ARP Cache Poisoning
Archive Collected Data (3)
Archive via Utility
Archive via Library
Archive via Custom Method
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage Object
Data from Configuration Repository (2)
SNMP (MIB Dump)
Network Device Configuration Dump
Data from Information Repositories (3)
Confluence
Sharepoint
Code Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (2)
Local Data Staging
Remote Data Staging
Email Collection (3)
Local Email Collection
Remote Email Collection
Email Forwarding Rule
Input Capture (4)
Keylogging
GUI Input Capture
Web Portal Capture
Credential API Hooking
Screen Capture
Video Capture

Common TTPs

Initial Access	External Remote Services T1133	Exploit Public Facing Application T1190	Phishing T1566					
Execution	User Execution: Malicious File T1204.002	Command and Scripting Interpreter T1059	Windows Management Instrumentation T1047					
Persistence	Scheduled Task T1053.005	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.001	Account Manipulation T1098	Create or Modify System Process: Windows Service T1543.003	BITS Jobs T1197			
Privilege Escalation	Abuse Elevation Control Mechanism: Bypass User Account Control T1548.002	Exploitation for Privilege Escalation T1068	Access Token Manipulation T1134					
Defense Evasion	Signed Binary Proxy Execution T1218	Process Injection T1055	Impair Defenses: Disable or Modify System Firewall T1562.004	Impair Defenses: Disable or Modify Tools T1562.001	Masquerading T1036	Indicator Removal on Host: File Deletion T1070.004	Indicator Removal on Host: Clear Windows Event Logs T1070.001	Deobfuscate / Decode Files or Information T1140
Credential Access	OS Credential Dumping: LSASS Memory T1003.001	Credentials from Password Stores: Credentials from Web Browsers T1555.003	Brute Force T1110					
Discovery	System Network Connections Discovery T1049	Remote System Discovery T1018	Network Share DiscoveryT1135	Account Discovery T1087	File and Directory Discovery T1083	Process Discovery T1057		
Lateral Movement	Remote Services: Remote Desktop Protocol T1021.001	Lateral Tool Transfer T1570	Remote Services: SMB/ Windows Admin Shares T1021.002					
Command and Control	Application Layer Protocol: Web Protocols T1071.001							
Exfiltration	Exfiltration Over C2 Channel T1041	Exfiltration Over Web Service: Exfiltration to Cloud Storage T1567.002						
Impact	Inhibit System Recovery T1490	Service Stop T1489						

Для кого этот отчет

- SOC Analysts
- Threat Hunting Teams
- Digital Forensics Specialists
- Cyber Threat Intelligence Analysts
- Cyber security specialists who are involved in the incident response

Technical Details

Каждая из техник, показанная на предыдущей диаграмме, сопоставлена с группами и сопровождается таблицей, показывающей, кто из обсуждаемых группировок использовал данную технику

MITRE ATT&CK TTP	Количество
User Execution: Malicious File T1204.002	4 / 8

Акторы, применявшие эту технику

Conti
Clop (TA505)
Ragnar Locker
Pysa
Hive

Нет подтвержденных случаев

LockBit
BlackByte
BlackCat

Подробное описание TTPs

Как уже было сказано в предыдущей главе, самый распространенный способ доставки вредоносной полезной нагрузки в рамках фишинговых кампаний заключается в отправке электронных писем с прикрепленными вредоносными документами Microsoft Office. Злоумышленники могут поместить вредоносные документы в защищенные паролем архивы, которые и прикрепляются к фишинговым письмам.

Пример исполнения

Image_path: "$windir\$system32\regsvr32.exe",
Command_line: "regsvr32 $user\$appdata\Vote1.ocx",
Parent_image_path: "$programfiles\Microsoft Office\Office14\Excel.EXE"

Правила SIGMA

SIGMA

Приложение I. Started windows shell from Trusted process
Приложение I. Drop Execution File From by Trusted Process

Mitigations

Мы собрали лучшие практики из NIST, NCSC, CISA, SANS в организованную структуру, которую можно применять в организациях

There are additional measures that can be taken to make your organization more secure: Countering data loss and Preparing for an incident

We highlight the following stages of a ransomware incident, that can be mitigated or hampered for adversaries by defenders:

Intrusion

At the intrusion stage, an adversary tries to break into a protected perimeter.

Examples: spear phishing emails, bruteforce internet-facing services (RDP)

The Defenders' Main Goal: Prevent the malware from reaching the devices

Exploitation

At the exploitation stage, an adversary tries to run code in order to escalate privileges, access and exfiltrate sensitive information, or harvest credentials.

The Defenders' Main Goal: Prevent malware from launching on endpoint devices

Lateral Movement

At the lateral movement stage, an adversary tries to spread across the network.

The Defenders' Main Goal: Prevent malware from reaching other devices

Victims

Для этого анализа мы использовали статистические источники по обнаружениям, а также источники объявлений в даркнете о жертвах, размещенных операторами Ransomware

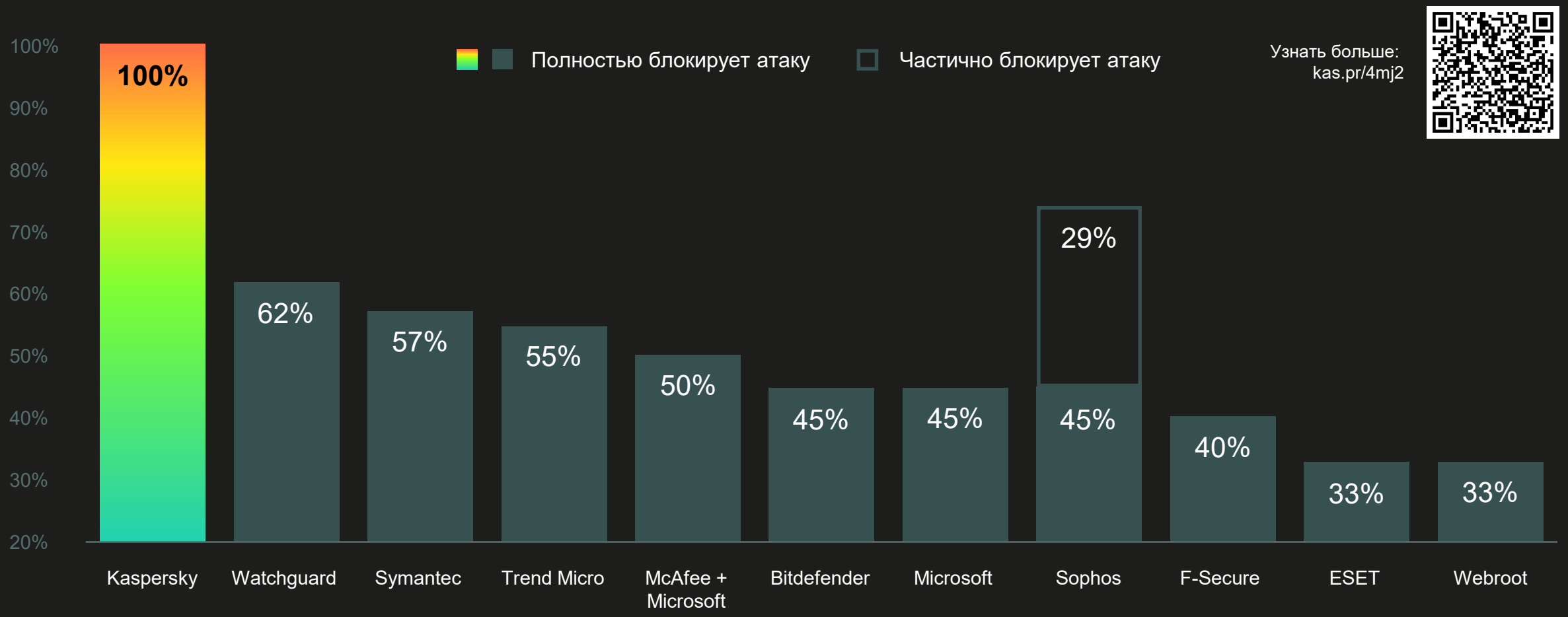
Семейство шифровальщиков	Рейтинг по отраслям	Всего пострадавших организаций
Conti/Ryuk	Производство	45
	Строительство	19
	Разработка ПО	16
	Юриспруденция	6
	Страхование	6
Pysa	Образование	18
	Производство	3
Cl0p (TA505)	Разработка ПО	9
	Юриспруденция	8
	Производство	5
	Образование	4
	Консалтинг	3
Hive	Малый бизнес	14
	Здравоохранение	7
	Юриспруденция	5
	Недвижимость	4
	Транспорт	4
Ragnar Locker	Производство	3
	Разработка ПО	3
	Юриспруденция	2
	Фармацевтика	2
	Авиастроение	2
Lockbit	Малый бизнес	12
	Юриспруденция	2
BlackCat	Малый бизнес	6
	Производство	3
	Консалтинг	2
BlackByte	Малый бизнес	5
	Строительство	2
	Консалтинг	2

Sigma Rules

Также мы создали SIGMA правила которые вы можете использовать в своих SIEM системах чтобы обнаруживать активность противника в собственной инфраструктуре

Техники	SIGMA
Exploit Public-Facing Application T1190	Windows Shell Start by Web Applications
User Execution T1204	Started windows shell from Trusted process Drop Execution File From by Trusted Process
Command and Scripting Interpreter T1059	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Execution of Downloaded Powershell Code Encoded/decoded PowerShell Code Execution Executing PS1 from Public Directory Powershell Suspicious Arguments Executing JavaScript from Public Directories
Windows Management Instrumentation T1047	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Suspicious Command wmic.exe Suspicious Child Process Wmiprvse.exe
Scheduled Task/Job: Scheduled Task T1053.005	Scheduled Task Start from Public Directory Windows Shell Started Schtasks
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.001	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Modification Main Registry Run Keys Adding Path of Open Folder in Run Keys via Registry Adding Suspicious File in Autorun Keys via Registry Suspicious File Creation in Startup Folder
Account Manipulation T1098	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Account Creation via Powershell Account Creation via net.exe Adding Account in Domain or Local Admin Group via net.exe Adding Account in Domain or Local Admin Group via PowerShell
Create or Modify System Process: Windows Service T1543.003	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Service Installation From Non-System Directory Service Image Path Modification via sc.exe
BITS Jobs T1197	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: File Download via Bitsadmin Suspicious Jobs via Bitsadmin
Abuse Elevation Control Mechanism: Bypass User Account Control T1548.002	UAC Bypass via COM Object Disabling UAC via Registry
Exploitation for Privilege Escalation T1068	Доступно в полной версии отчета на портале Kaspersky Threat Intelligence: Created Windows Shell from Critical Windows Process

Лучшая защита от шифровальщиков



Иногда есть возможность помочь пользователю, зараженному Ransomware, вернуть доступ к зашифрованным данным без уплаты выкупа.

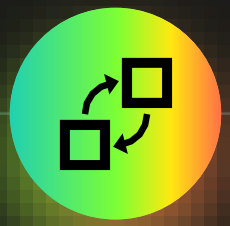
Мы создали коллекцию ключей и утилит, которые могут помочь пользователям восстановить доступ к своим системам, атакованным Ransomware группировками.

Подробнее

Ключевые элементы защиты

Квалифицированный персонал

Эффективность современных комплексных защитных решений напрямую коррелирует с уровнем экспертизы ИБ- и SOC-команд, работающих с ними. Организациям следует инвестировать в обучение сотрудников или воспользоваться услугами сторонних MDR-сервисов от надежного поставщика

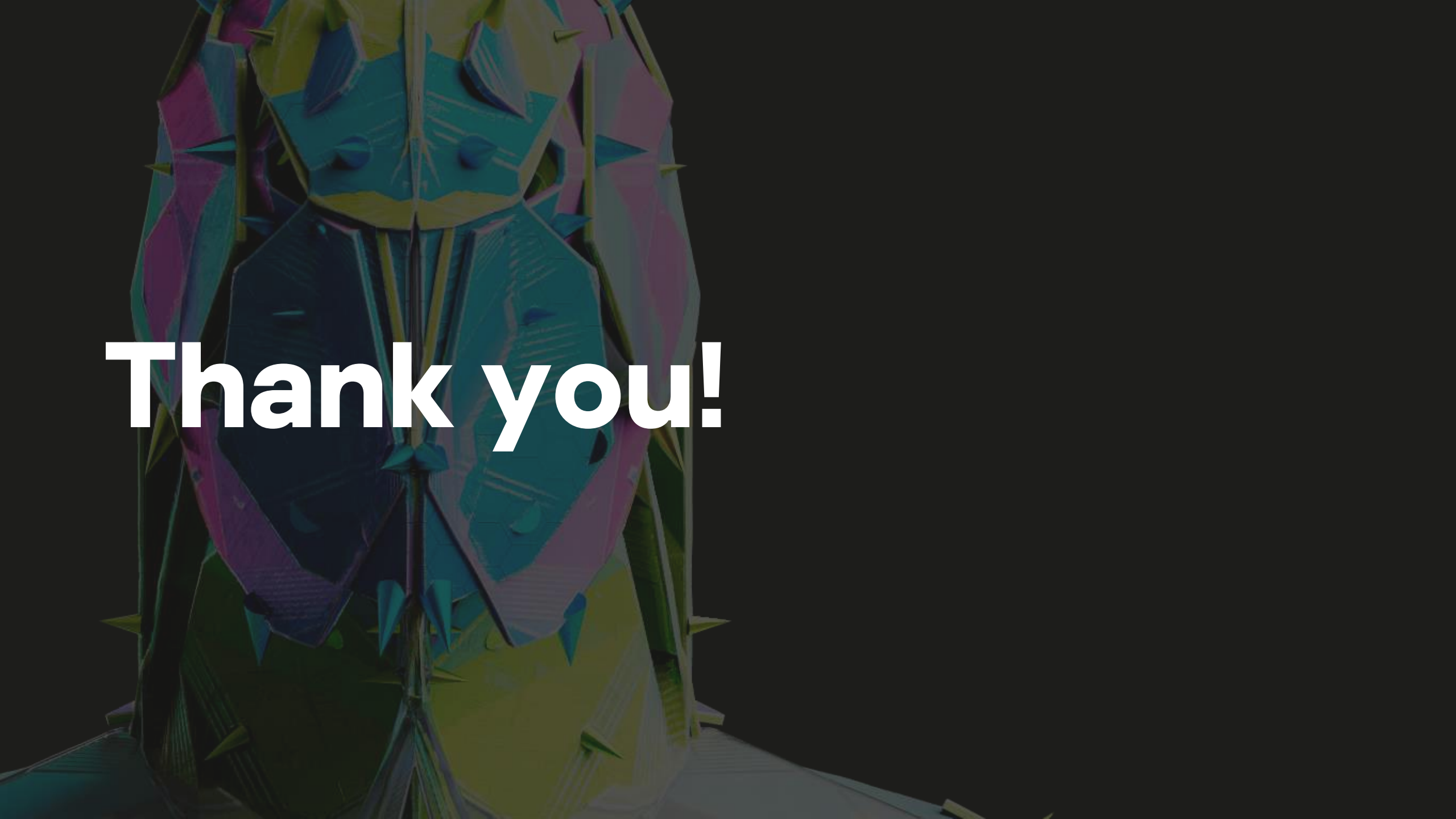


Надежные защитные решения

Экспертам ИБ/SOC требуются решения, которые надежно обеспечат мониторинг всего, что происходит в сети организации с точки зрения кибербезопасности, и с максимальной степенью автоматизации помогут своевременно обнаружить и заблокировать угрозы. Решения, на которые можно положиться и в нашей новой реальности

Аналитические данные Threat Intelligence

Без актуальной и релевантной информация о том, какие злоумышленники представляют угрозу для организации, как они действуют и какими инструментами пользуются, невозможно обеспечить защиту от современных киберугроз. Использование данных Threat Intelligence должно стать неотъемлемой частью стратегии защиты


Thank you!