halcyon | Ransomware Research Center

Play Ransomware Destroys EDR/EPP via Disk Manager - Seizes Network Firewalls

Play ransomware gang, known for its systematic organization and efficiency with victim payouts, has remained a prominent threat since its formation in 2022. Halcyon work since April 2025 to regain access, recover critical systems, and evict Play actors from targeted environments highlighted. Several novel techniques used by the gang for maximum impact and downtime:

- **EDR and EPP Removal via Disk Management Tools:** Use of disk partition managers to remove endpoint detection and response (EPP and EDR) and antivirus solutions prior to ransomware.
- **Firewall Infrastructure Compromise:** Complete takeover of SonicWall firewalls.
- **NAS Factory Reset:** Factory reset of network attached storage.
- **Local Backup Encryption:** Purposeful encryption of local backup software.

Background

Play Ransomware, also known as PlayCrypt, emerged in June 2022 initially operating as a closed group. According to the FBI, the gang has compromised over 900 entities since its creation. The group gains initial access primarily through unpatched Fortinet SSL VPN vulnerabilities and has also exploited Microsoft Exchange (ProxyNotShell, OWASSRF) and SonicWall appliances. The ransomware uses intermittent encryption and recompiles binaries per deployment to evade signature-based detection.

Play relies on living-off-the-land techniques alongside custom tools like Grixba for network enumeration and PlusBrute for credential brute-forcing. Having compromised numerous organizations globally as of May 2025, Play has evolved from its original closed structure to incorporate RaaS elements, enabling broader operational reach.

The group has since expanded to target VMware ESXi environments with a Linux-based variant. In September 2025, Halcyon observed Play operators seizing control of SonicWall firewalls during intrusions, among other techniques observed across recent engagements.

Mitigation

Organizations should adopt layered defenses aligned to common ransomware tactics:

- **Harden Initial Access Vectors:** Reduce exposure from trusted relationships and third-party access pathways [T1199].
- **Limit Lateral Movement and Credential Abuse:** Monitor and restrict Remote Services [T1021] and misuse of Valid Accounts [T1078].
- **Detect Data Staging and Exfiltration:** Monitor for Archive Collected Data [T1560] and Exfiltration Over Command-and-Control Channel [T1041].
- **Protect Against Encryption Impact:** Ensure resilience against Data Encrypted for Impact [T1486] through tested recovery processes.
- **Deploy Dedicated Anti-Ransomware Solution:** Deploy dedicated anti-ransomware defenses to block malicious binaries pre-execution [M1038], detect runtime behaviors and data exfiltration attempts [M1040], prevent tampering and network intrusion [M1031], and protect the integrity of backups to reduce extortion leverage [M1053].

EDR/EPP Removal Using Partition Management Utility/Disk Manager

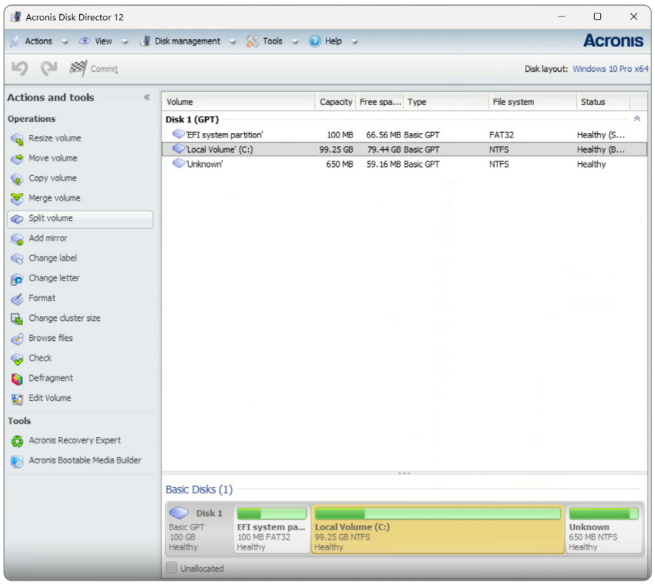
Play ransomware group uses a novel technique to bypass Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) by completely removing them from the active disk using a legitimate partition management/disk manager utility, which remove endpoint defenses without directly disabling or terminating security processes.

Halcyon observed Play download “Acronis Disk Director” from:

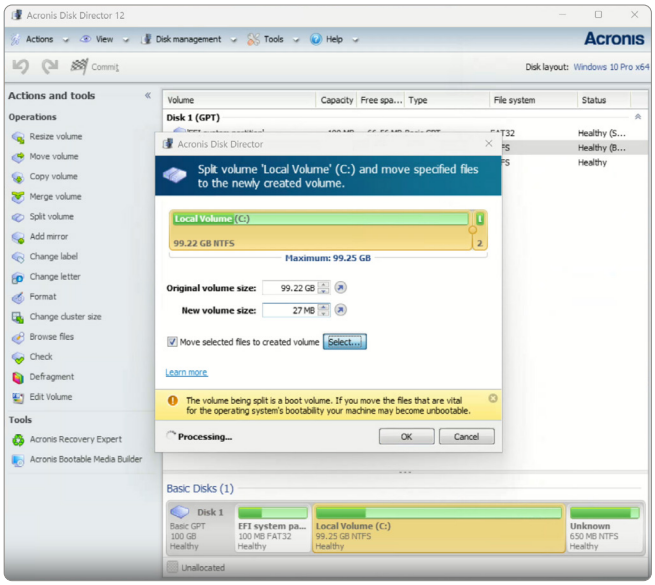
- https://dl.acronis.com/u/AcronisDiskDirector12.5_trial_en-EU[dot]exe

Play executed the installer, launched DiskDirector.exe, and Acronis Disk Director was used to schedule an Acronis task to split a partition. Play operators then moved the EDR and EPP from ProgramData and ProgramFiles folders to the newly created partition, deleted the partition split with EDR and EPP, and cleaned up metadata upon reboot.

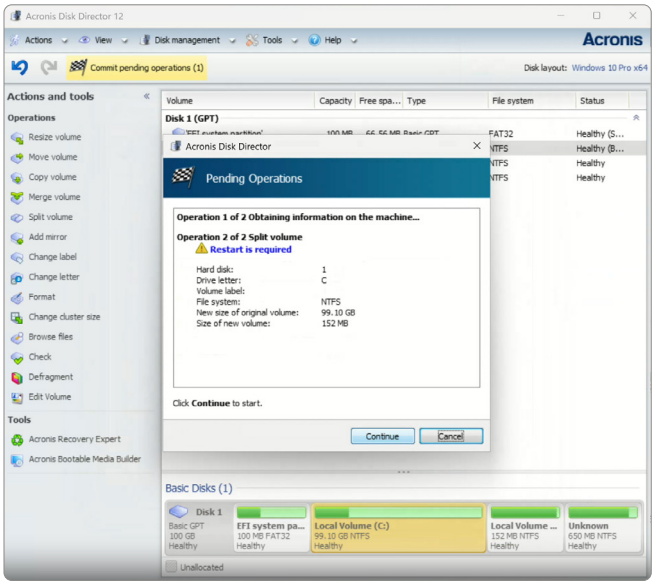
The Task file was generated by Acronis and stored within C:\ProgramData\Acronis\DiskDirector. This resulted in the EDR and EPP no longer being present, allowing Play ransomware to execute without any prevention mechanisms. The attached screenshots show how this process would be conducted manually to remove EDR and EPP. The task from Play is completely automated and hidden:



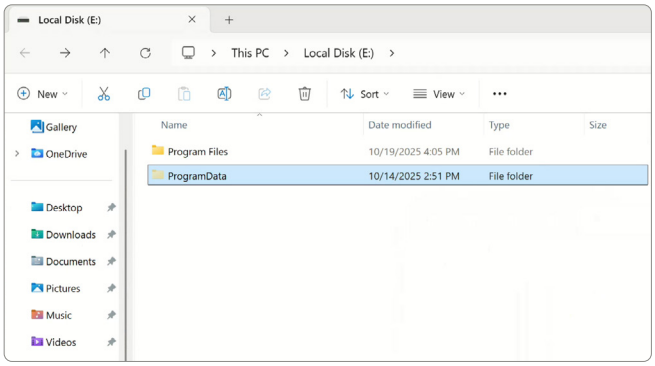
Step 1. Split Volume Selection in Acronis Disk Director 12



Step 2. Splitting Disk Volumes, then with Select for selecting the EDR and AV folders



Step 3. Splitting Volume Operation Underway, requiring a Restart



Step 4. Newly created partition with the EDR and EPP solutions (now non-functional)

Upon reboot, the EDR and EPP are still present but are not functional as those are no longer in the functional directories. The files are on the new partition in the respective Program Files and ProgramData folders as shown below. Play's Acronis task then deletes the partition.

NOTE: There are many other utilities besides Acronis Disk Director 12 that have similar functionality. A sample list is provided below for reference:

PARTITION & DISK MANAGEMENT TOOLS RANSOMWARE REPORT

#	TOOL NAME	TYPE	NOTABLE USE
1	AOMEI Partition Assistant Server Edition	COMMERCIAL	Windows server partition management
2	EaseUS Partition Master Server Edition	COMMERCIAL	Resize, merge & clone partitions
3	MiniTool Partition Wizard Server Edition	COMMERCIAL	Disk conversion & recovery
4	Paragon Hard Disk Manager for Business	COMMERCIAL	Backup, wipe & partition control
5	DiskGenius	COMMERCIAL	Partition editing & data recovery
6	Macrium Reflect Server	COMMERCIAL	Imaging & disk cloning
7	Active@ Partition Manager	COMMERCIAL	Low-level partition operations
8	Active@ Disk Editor	COMMERCIAL	Raw sector & hex editing
9	DMDE (DM Disk Editor & Data Recovery)	COMMERCIAL	Disk editor & recovery tool
10	WinHex	COMMERCIAL	Hex editor & forensics
11	GParted Live	BOOTABLE OPEN SOURCE	NTFS & Windows partition support
12	Parted Magic	BOOTABLE	Live disk partitioning & wiping
13	Clonezilla SE (Server Edition)	BOOTABLE OPEN SOURCE	Network-based disk cloning
14	NIUBI Partition Editor Server	COMMERCIAL	Non-destructive partition resizing
15	Hasleo Disk Clone and Partition Manager	COMMERCIAL	Disk cloning & partition ops
16	O&O PartitionManager	COMMERCIAL	Windows-native partition control
17	TeraByte BootIt Bare Metal	BOOTABLE COMMERCIAL	Boot management & imaging
18	Symantec Ghost Solution Suite	COMMERCIAL	Enterprise imaging & deployment
19	R-Drive Image Technician	COMMERCIAL	Drive imaging & disaster recovery

Firewall Takeover

Halcyon observed Play attempting to take over a firewall, including SonicWall, restricting access to the victim environment, limiting it to only Play's network traffic. This required coordination with the Internet Service Provider (ISP) to terminate the connection between two geographic locations as well as terminate the Internet feed to each location.

Unlike Akira's exploitation of CVE-2024-40766 with focus on SSL VPN, Play targeted the IPsec VPN access, especially in cases where RADIUS was not setup with multi-factor authentication. Play reset the passwords to the firewalls, making the firewalls unrecoverable. A backup configuration submitted to SonicWall support in early 2025 was the last known good configuration and was used to restore the firewalls to a known clean state.

NAS Factory Reset

Play performed factory resets of network attached storage devices. These devices held the victims' most sensitive information for the organizations and were entirely exfiltrated prior to the factory reset. Play, also proceeded to reset a physical, network-attached storage with a domain-joined account where the virtual machines were hosted. The recovery for each storage device requires restoring from cloud backups or rebuilding from scratch.

Encryption of Local Backup Software

Play purposefully encrypted the local backup solution (Veeam) that held the victim's virtual machines and other critical data. In the case of Play, it was a virtual machine on a domain-joined ESXi host which would be used to orchestrate the restoration of virtual machines. The recovery for each was different. Each ESXi host had to be rebuilt due to the encryption.

Following the ESXi rebuilds, there was extensive coordination needed with the cloud provider to build a local instance (taking days) that could then receive the backed-up files in the cloud. Afterward, all backups were restored after several weeks of work. Across the firewall recovery, NAS restoration, and ESXi rebuilds, Halcyon collaborated extensively with victims to regain access, recover critical systems, and evict the actors.

The Halcyon Ransomware Research Center unites experts, drives smart policies, and delivers actionable intelligence to detect, disrupt, and defeat ransomware. Explore the Center's latest reports, analysis, and resources here.