# Incident Response

## Sample Client

**Caught at 7:32 PM. Contained in 3 minutes 57 seconds.**

A real attack on an AdVran-managed business, documented exactly the way the client received it. Company, computer and user names have been changed. Incident INC-SAMPLE-0310 · 10 March 2026.

| 3m 57s | 12 | 7 of 7 | After hours |
|---|---|---|---|
| From SOC detection to isolated and fully remediated | Behavioral signals correlated by the SOC | Remote remediations completed successfully | Detected at 7:32 PM, when no one was in the office |

Severity: Critical · Status: Resolved and closed

# A fake W-9 opened a back door.
# We closed it in under 4 minutes.

An employee downloaded a file disguised as a W-9 tax form. It quietly installed **two remote-control tools** that would have handed an attacker the computer. At 7:32 PM, after the office had closed, the AdVran SOC caught it, **cut the computer off from the network** and removed both tools before the attacker could do any damage.

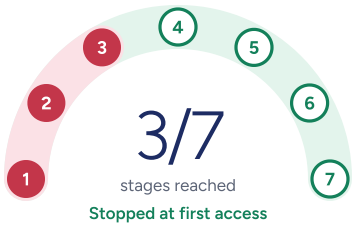
| 28s | 12 | 3m 57s | 7/7 |
|---|---|---|---|
| **Attack chain** | **Signals correlated** | **Detection to remediated** | **Remote fixes** |
| Download to second back door | Behavior, not signatures | 7:32:37 to 7:36:34 PM | Completed successfully |



| 7:32:09 PM | 7:32:37 PM | 7:36:34 PM |
|---|---|---|
| First malicious signal | SOC detects · host isolated | Remediated · threat gone |

## How far the attacker got

✓ Stopped at first access




| | | |
|---|---|---|
| 1 | Paid ad | REACHED |
| 2 | Download | REACHED |
| 3 | Execution | REACHED |
| 4 | Persistence | STOPPED |
| 5 | Remote control | STOPPED |
| 6 | Spread | CUT OFF |
| 7 | Ransomware | CUT OFF |

## Incident scope

INC-SAMPLE-0310

| | |
|---|---|
| Severity | Critical |
| Affected host | **WORKSTATION01** |
| Affected user | user01 |
| Threat | Rogue remote access (RMM) |
| Detected | 10 Mar 2026 · 7:32 PM |
| Detected by | AdVran 24/7 SOC |
| Host status | ✓ Back in service |
| Resolution | ✓ Closed |

## Signal activity · 7:32:09 to 7:32:37 PM

One bar per second



| :09 | :19 | :27 | :37 |
|---|---|---|---|
| First signal | Second tool installs | First correlation | Isolated |

Process · 6 Autorun · 3 Correlated · 2 System · 1

## Already done for the client

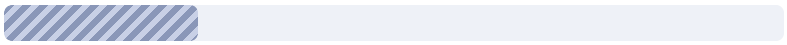
- ✓ Computer isolated from the network
- ✓ Local password reset on the device
- ✓ Both remote-access tools removed
- ✓ Older crypto miner found and removed
- ✓ Services and registry keys deleted
- ✓ Backup workstation set up

# Most breaches go unseen for months. This one lasted minutes.

The industry measures breaches in days. AdVran measures them in seconds, because a person is watching every signal around the clock, not reading an alert the next morning.

## Time an attacker has inside the network

Drawn to the same scale

| | | |
|---|---|---|
| **Industry average**<br>Identify and contain a breach |  | 258 days |
| **Industry average**<br>Just to identify a breach |  | 194 days |
| **Industry average**<br>To contain, once identified |  | 64 days |
| **This incident · AdVran**<br>Detection to fully remediated | Too small to see at this scale | 3m 57s |

Industry figures: IBM Cost of a Data Breach Report 2024, global averages.

**$4.88M**
**Average cost of a data breach**
IBM Cost of a Data Breach Report 2024

**$0**
**Ransom paid in this incident**
The attacker never reached the encryption stage

**7:32 PM**
**When it was caught**
After hours, with the office empty

### WITHOUT A 24/7 SOC

- The alert waits in an inbox until someone checks it, often the next business day.
- The attacker has all night with two working back doors.
- Remote tools look like normal IT software, so antivirus stays quiet.
- The usual next step is spreading to other computers, then ransomware.

### WITH ADVRAN · WHAT ACTUALLY HAPPENED

- 12 signals correlated and confirmed as an attack at 7:32 PM.
- The computer was isolated, so it could not be used to reach other machines.
- Seven remote remediations removed both back doors.
- An engineer followed up on site and the client got this report.

## Antivirus did not stop this. People and process did.

The attacker used **legitimate remote-access software**, the kind antivirus is built to allow. What caught it was behavior: a browser launching a renamed installer, then two remote tools registering as services within 28 seconds. That is the difference between owning security tools and having a team that watches them.

24/7 SOC · Behavioral detection · Network isolation · Remote remediation

# What happened, and what it means.

Every AdVran incident report starts with the version a business owner can read in two minutes. The technical detail follows on the next pages.

### What happened?

Someone on WORKSTATION01 opened a file they thought was a W-9 tax form. It was a fake that secretly installed two programs letting an attacker control the computer remotely.

### What could the attacker do with it?

See the screen, open files, steal passwords, reach company data, or use this computer to get to others on the network. Access like this often ends in ransomware.

### What did AdVran do?

The moment the threat was confirmed, we cut the computer off from the network. We then stopped the programs, deleted the malicious files and removed everything that would let them restart.

### What is an RMM tool, and why is it dangerous?

RMM means remote monitoring and management. IT companies use these real tools to manage computers. Attackers use the same tools because antivirus usually does not flag them. It is like a burglar using a real locksmith's kit.

### Why two remote-access programs?

A backup plan. The attacker installed Datto CentraStage and ScreenConnect so that if one was removed, the other would still let them in.

### Is it safe now?

Yes. Our engineers inspected the computer on site, cleaned the remaining traces, reset the password and returned it to service. It stays under 24/7 SOC monitoring.

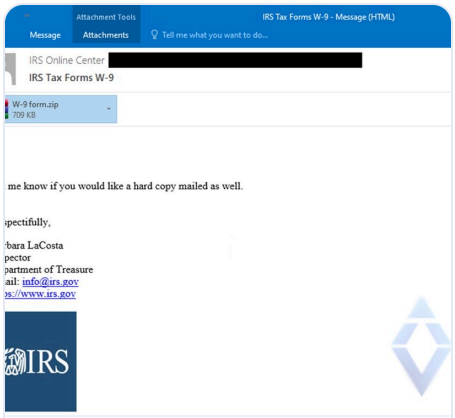
## Known campaign · fake W-9 tax forms

Likely link

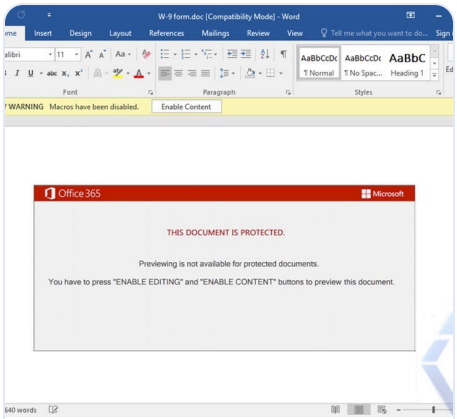
The tactics match an active campaign that uses fake IRS W-9 forms to deliver malware, tied to the **Emotet** operation. It spreads through emails and downloads dressed up as tax paperwork. Once inside, it steals contacts and drops more payloads, including ransomware.

It started with malicious Word macros and moved to OneNote files with hidden scripts after Microsoft blocked macros by default. This incident used a disguised **.exe** download instead.

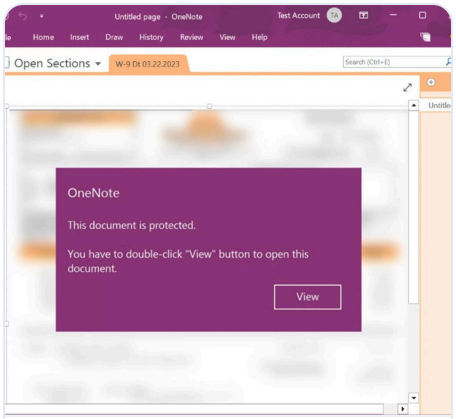
| | |
|---|---|
| File named "w9_form" | Match |
| Delivered by browser download | Match |
| Chains RMM installs for persistence | Match |
| Several copies downloaded | Match |
| Legitimate tools to evade antivirus | Match |




**Fake IRS email**
"IRS Tax Forms W-9" with a zipped attachment




**Word lure**
Asks the reader to "Enable Content" to run macros




**OneNote lure**
A fake "View" button runs a hidden script

Public examples of the W-9 campaign published by security researchers. Not from the client's systems.

# A browser launched a renamed remote-access installer.

Retroactive threat hunting flagged the first signal: Chrome starting a program that matched a known RMM signature under a different name. From there the SOC followed the whole process chain.

## Lead signal

Critical

| | |
|---|---|
| Signal | **Web browser spawning renamed RMM** |
| Detected | 10 Mar 2026 · 7:32:09 PM PST |
| Executable | `C:\Users\user01\Downloads\w9_form (5).exe` |
| Parent process | `chrome.exe` |
| User | user01 |

## Process chain

WORKSTATION01

**What ran, and what it started**

```
chrome.exe            legitimate browser
└ w9_form (5).exe   renamed RMM installer
   ├ Datto CentraStage RMM   first foothold
   └ ScreenConnect client    second foothold
      ├ service 8f371a4a6994693c
      └ service dca3be798b3393e7
```

## Attack timeline · 10 March 2026

28 seconds end to end

**7:32:09 PM — Malicious file downloaded**
user01 downloads `w9_form (5).exe` in Chrome. The name imitates a W-9 tax form.

**7:32:14 PM — Installer launched**
The file installs Datto CentraStage RMM, then chains a second remote tool.

**7:32:19 PM — ScreenConnect installed**
A ScreenConnect client is added as a backup way in.

**7:32:37 PM — AdVran SOC detects and isolates**
Behavioral signals confirm a rogue RMM. The host is cut off from the network and response begins.

## Mapped to MITRE ATT&CK

The industry framework for attacker behavior

| TACTIC | TECHNIQUE | ID | WHAT WE SAW |
|---|---|---|---|
| RESOURCE DEV. | **Malvertising** | T1583.008 | Paid Google ad above the real results |
| INITIAL ACCESS | **Drive-by compromise** | T1189 | Download from the sponsored link |
| EXECUTION | **User execution: malicious file** | T1204.002 | `w9_form.exe` run three times |
| DEFENSE EVASION | **Masquerading** | T1036 | Installer renamed to look like a tax form |
| PERSISTENCE | **Windows service** | T1543.003 | Two ScreenConnect client services |
| COMMAND & CONTROL | **Remote access software** | T1219 | Datto CentraStage and ScreenConnect |
| COMMAND & CONTROL | **Non-standard port** | T1571 | `brooksideonline17.com:8041` |

# Signals investigated, in order of detection.

Twelve behavioral signals were processed for WORKSTATION01 between 7:32:09 and 7:32:37 PM PST. Three copies of the same file were downloaded and run, which points to repeated attempts from one source.

All 12 | Process 6 | Autorun 3 | Correlated 2 | System 1

7:32:09 to 7:32:37 PM PST

| TIME | SIGNAL | TYPE | DETAIL | WEIGHT |
|---|---|---|---|---|
| 7:32:09 | Browser spawning renamed RMM | PROCESS | w9_form (5).exe · parent chrome.exe | |
| 7:32:12 | Suspicious rogue RMM install | PROCESS | w9_form.exe | |
| 7:32:14 | Suspicious rogue RMM install | PROCESS | w9_form (5).exe | |
| 7:32:17 | Browser spawning renamed RMM | PROCESS | w9_form (3).exe · parent chrome.exe | |
| 7:32:19 | Datto CentraStage deploy MSI | SYSTEM | msiexec /i ScreenConnect.ClientSetup.msi /qn | |
| 7:32:22 | Browser spawning renamed RMM | PROCESS | w9_form.exe · parent chrome.exe | |
| 7:32:24 | Suspicious rogue RMM install | PROCESS | w9_form (3).exe | |
| 7:32:27 | Datto RMM with ScreenConnect activity | CORRELATED | Links signals 1, 2 and 5 | |
| 7:32:29 | Trial ScreenConnect service | AUTORUN | service dca3be798b3393e7 · SYSTEM | |
| 7:32:32 | ScreenConnect URL not hosted | AUTORUN | service 8f371a4a6994693c · own process | |
| 7:32:35 | ScreenConnect install from Downloads | CORRELATED | Links signals 1, 2 and 10 | |
| 7:32:37 | Trial ScreenConnect service · host isolated | AUTORUN | service dca3be798b3393e7 · persistence | |

Command and control server 1

**brooksideonline17.com:8041**

ScreenConnect client 8f371a4a6994693c · non-standard port, attacker-controlled domain

Command and control server 2

**instance-d3yc7o-relay.screenconnect.com:443**

ScreenConnect client dca3be798b3393e7 · real ScreenConnect relay, used to blend in

**SOC ANALYST NOTE**

No single signal here would alarm a busy IT team. A browser download, a software install and a new service each look routine on their own. Correlated within 28 seconds on the same machine, they describe an attacker setting up two independent ways back in.

# Remote remediation and follow-up actions.

The following actions were executed remotely by the AdVran SOC while WORKSTATION01 was isolated from the network. All seven completed successfully. Follow-up actions for the client are listed below with their status after the on-site visit.

| 7/7 | 0 | 4/5 | 7:36 PM |
|---|---|---|---|
| **Remote actions** Completed successfully | **Failed actions** No errors reported | **Follow-ups closed** During the on-site visit | **Threat removed** Same evening as the attack |

| # | ACTION | TARGET | APPROVED BY | STATUS |
|---|---|---|---|---|
| 01 | **Kill process** | `ScreenConnect.ClientService.exe · PID 24064` | A. Monges Rodriguez | ✓ Done |
| 02 | **Delete service** | `ScreenConnect Client (8f371a4a6994693c)` | A. Monges Rodriguez | ✓ Done |
| 03 | **Delete service** | `ScreenConnect Client (dca3be798b3393e7)` | A. Monges Rodriguez | ✓ Done |
| 04 | **Delete registry key** | `HKLM\…\Services\ScreenConnect Client (8f371a…)` | A. Monges Rodriguez | ✓ Done |
| 05 | **Delete registry key** | `HKLM\…\Services\ScreenConnect Client (dca3be…)` | A. Monges Rodriguez | ✓ Done |
| 06 | **Delete file** | `ClientService.exe · SHA256 7976bc66…a2515244` | A. Monges Rodriguez | ✓ Done |
| 07 | **Delete file** | `ClientService.exe · SHA256 c0f495e2…4628d62d` | A. Monges Rodriguez | ✓ Done |

**SHA256 of the deleted ScreenConnect binaries · for the client's records**

```
Instance 8f371a4a6994693c   7976bc6647fead449fdd424f7ccb5150b5d896b4db23782493a11580a2515244
Instance dca3be798b3393e7   c0f495e2a491f6bb90f062cefbe2668d82edd8acb1569b8be4a0d3324628d62d
```

## Follow-up actions the SOC set for the client

Status after the on-site visit

| PRIORITY | ACTION | WHY | STATUS |
|---|---|---|---|
| Critical | **Coach the affected user** | Socially engineered into running a fake W-9 | ✓ Done on site |
| Critical | **Audit folders for leftover files** | Downloads, Temp, ProgramData, ScreenConnect | ✓ Cleaned |
| Critical | **Reset user credentials** | Treat the account as compromised | ✓ Reset on device |
| Urgent | **Remove Datto CentraStage remnants** | The first tool, not covered by remote actions | ✓ Cleaned |
| Urgent | **Check for lateral movement** | RDP, SMB or reused credentials before isolation | ⓘ Recommended |

# On site: how the attack really started.

An AdVran engineer inspected WORKSTATION01 in person and rebuilt the full chain from browser history, downloaded files and system logs. It did not start with an email. It started with a search.

## What the inspection found

10 March 2026

**~1:00 PM — The employee searches Google for a W-9 form**
A malicious ad sits at the top of the results, above the real ones, posing as a W-9 download site.

**~2:00 PM — The sponsored link downloads w9_form.exe**
Attackers paid for the ad placement. This is called malvertising.

**~2:00 PM — The program shows a real W-9**
While the employee fills in the form, ScreenConnect installs silently in the background.

**7:32 PM — AdVran SOC detects and responds**
Rogue RMM activity detected, device isolated, all 7 remote remediations run within minutes.

### Browser history

A Google search for a W-9, then a click on the sponsored result at the top of the page.

### Downloads folder

Three copies of the same file: `w9_form.exe`, `(3)` and `(5)`.

### System logs

ScreenConnect installed in the background while the fake form was on screen.

**WHAT THE EMPLOYEE DOWNLOADED**

**`w9_form.exe`**

A program, from a sponsored search ad. Shows a form, installs remote access.

**WHAT A REAL W-9 LOOKS LIKE**

**`fw9.pdf`**

A document, downloaded from irs.gov. Opens in a PDF reader and cannot install anything.

## Why it worked

The attackers bought ad space so their link outranked the real IRS site. The file showed a genuine-looking form, so nothing seemed wrong. And it installed a **legitimate IT tool** instead of classic malware, which antivirus is less likely to flag. Everything was built to look normal.

## What we told the employee

A real W-9 is always a **.pdf**, never an **.exe**. An .exe is a program, not a document. Check the web address, watch for the “Sponsored” label on search results, and when in doubt download tax forms directly from **irs.gov**.

## On-site cleanup

✓ System clear

| | | | |
|---|---|---|---|
| Reconnected after remote cleanup was verified | ✓ Done | Local Windows password reset on the device | ✓ Done |
| Full system scan | ✓ Done | **Older crypto coin miner** found and removed | ✓ Bonus find |
| Remaining ScreenConnect and Datto traces removed | ✓ Done | Backup workstation set up for the employee | ✓ Done |

**We found a second threat nobody knew about.** The full scan turned up a crypto miner installed long before this incident, quietly using the computer’s power. It was removed in the same visit. A backup workstation with the employee’s accounting and email apps now keeps the business running if the main PC is ever down.

# Incident closed and host back in service.

All remote and on-site remediation is complete. The computer is back in service and remains under AdVran SOC monitoring. No further action is required from the client.

| 3m 57s | 12 | 7/7 | 6/6 |
|---|---|---|---|
| **Response time** Detection to remediated | **Signals processed** All tied to one incident | **Remote remediations** Completed successfully | **On-site actions** Including a bonus find |

## Detection and response summary

Around 1:00 PM on 10 March 2026, an employee searched Google for a W-9 form and clicked a malicious ad at the top of the results. Around 2:00 PM the download showed a real W-9 while silently installing remote-access tools.

At 7:32 PM the AdVran SOC detected the rogue RMM activity and isolated the host. Seven remote remediations ran and all completed by 7:36 PM.

On site, we confirmed the attack chain, cleaned the remaining traces, removed an older crypto miner, reset the local password and coached the employee. The device is back in service.

## Incident details

| | |
|---|---|
| Organization | Sample Client |
| Incident ID | INC-SAMPLE-0310 |
| Affected host | WORKSTATION01 |
| Severity | Critical |
| Host status | ✓ Back online |
| Resolution | ✓ Resolved |

| PREPARED BY | REVIEWED BY | GENERATED | CLASSIFICATION |
|---|---|---|---|
| **AdVran SOC** Incident response team | **Adrian Monges Rodriguez** Founder, AdVran | **10 March 2026** 7:36 PM PST · updated after on-site visit | **Confidential** Client leadership and IT only |

## The full incident, start to finish

| ~1:00 PM | ~2:00 PM | 7:32 PM | 7:36 PM | On site | Closed |
|---|---|---|---|---|---|
| Google search for a W-9 | Fake W-9 from a paid ad | SOC detects rogue RMM | Isolated and remediated | Cleaned, miner removed | Back in service, monitored |

## What stops the next one

### Application control

Unapproved remote tools are blocked before they ever run, even when renamed.

### DNS and web filtering

Known malvertising and fake download sites are blocked at the network.

### Security awareness training

Short, regular lessons on fake forms, ads and .exe files dressed as documents.

### 24/7 SOC monitoring

Already in place. It is what caught this attack at 7:32 PM, after hours.

**One open item.** A review of network and sign-in logs for lateral movement from WORKSTATION01 before isolation is recommended. AdVran can complete it on request and add the result to this report.

# What stopped this attack comes with every AdVran plan.

Nothing in this report was a special project. Detection, isolation, remediation, the on-site visit and this report are what every AdVran managed security client gets as standard.

7:32:09 PM

### Endpoint detection

Behavioral detection on every device flagged a renamed installer that antivirus alone would miss.

**EDR on every device**

7:32:37 PM

### 24/7 SOC

Analysts correlated 12 signals after business hours and confirmed the attack.

**Managed detection and response**

At detection

### Network isolation

The computer was cut off so the attacker could not reach any other machine.

**Automated containment**

7:36:34 PM

### Remote remediation

Seven remote actions removed both tools while the computer was isolated.

**SOC-assisted remediation**

On-site visit

### Engineers on site

We rebuilt the attack, cleaned the traces, found an older miner and coached the employee.

**On-site support**

After closure

### Clear reporting

This report, delivered once the incident was closed, plus a monthly report on everything else.

**Incident and monthly reports**

## Included in AdVran managed security

✓ One team · one contract

- EDR on every device
- Managed detection and response
- 24/7 SOC monitoring and response
- Patch management · OS and apps
- Vulnerability management
- Remote monitoring and inventory
- Email security
- Dark web monitoring
- Monthly security audit
- Security posture management
- Incident reports like this one
- On-site engineers

## Would your current provider have caught this at 7:32 PM?

Most small businesses find out about an intrusion when the ransom note appears. Our free security assessment shows where your business stands today: exposed services, unpatched software, email spoofing and who is watching after hours.

Free assessment · Real findings · Easy-to-read report · No obligation

## How the free assessment works

1. **A short call** — Tell us how your business runs and what worries you.
2. **We scan** — Computers, network, email and website, without disrupting work.
3. **You get a report** — Every finding ranked, with what to fix first.

# One team. Zero gaps.

Managed IT and cybersecurity under one contract, with a 24/7 SOC included. Our engineers manage and monitor your company the way an in-house hire would: proactively, personally, accountably.

| 24/7 | 10+ | 38 | 5,000+ | 5.0 ★ |
|---|---|---|---|---|
| SOC monitoring | Years in business | Compliance frameworks | Endpoints managed | Google-rated |

## How AdVran runs your security

**Assess**
Scan, inventory and score every device.

**Prioritize**
Rank fixes by business impact.

**Remediate**
Engineers apply and verify fixes.

**Monitor**
24/7 SOC with EDR and MDR.

**Report**
Monthly proof-of-work reporting.



### Adrian Monges Rodriguez · Founder

A senior engineer and cybersecurity expert who managed complex network infrastructure at **Boeing** on projects with **NASA** and other defense and aerospace organizations. The same rigor now protects Southern California companies.

BOEING NASA KIOXIA

## Certified engineers

ITIL 4 Foundation · CISA · OSCP+ · CEH Master · CISM · CompTIA CySA+ · CompTIA SecurityX · Cisco CCNA · CompTIA Network+ · AWS Cloud Practitioner · PMP · Microsoft Fundamentals

Monthly executive security reports signed off by the engineers who did the work: threats blocked, patches applied, issues resolved. You never have to wonder what your IT provider did.

## Google reviews

Public reviews, 5 out of 5

★★★★★

"AdVran has become an invaluable extension of our foundation. They have removed all the IT hurdles we faced before and help guide us forward towards our mission."

**James and Teresa Keller Foundation** · Non-profit · Google review

★★★★★

"We switched over to AdVran's services after having issues with a previous MSP. Adrian and his team have been incredibly fast in supporting our business operations. If you are looking for an honest and reliable IT partner, I wouldn't look anywhere else."

**Gutierrez Manufacturing** · Manufacturing · Google review

★★★★★

"The best thing about AdVran is their proactive approach, they anticipate our needs before they become issues. They are incredibly easy to work with and provide quick responses that keep our operations running smoothly."

**Pro Compact Estates LLC** · Real estate · Google review

## Let's walk through this together.

Start with a free security assessment. An engineer reviews your environment and shows you what your first report would contain. No obligation.

Book a free assessment

**(714) 694-4573**
contact@advran.com
advran.com
AdVran Inc. · 155 N Riverview Dr #111
Anaheim, CA 92808