AdVran
SECURITY AT YOUR FINGERTIPS

Incident Response Report
INC-2026-03-10-7A2F
Generated: March 10, 2026 — 7:36 PM PST
Prepared for: [redacted]
Prepared by: **Michael M.**
Approved by: **Adrian Monges**

CYBER INCIDENT RESPONSE

Critical Security Incident Detected

Rogue Remote Monitoring & Management (RMM) tool installation on endpoint "WORKSTATION-01"

SEVERITY	SIGNALS PROCESSED	HOST STATUS	REMEDIATIONS
CRIT	**12**	**ISOLATED**	**7**
Immediate response required	Behavioral detections	Network quarantined	All completed successfully

<4m
RESPONSE TIME

7:32:09 PM
FIRST SIGNAL

7:32:37 PM
LAST SIGNAL

7:36:34 PM
ISOLATED + REMEDIATED

⚠ CRITICAL — HOST COMPROMISED

Immediate Action Required

The AdVran SOC team identified a critical compromise on endpoint **"WORKSTATION-01"** at Client Company. A user executed a malicious file disguised as a W-9 tax form, which installed two unauthorized Remote Monitoring & Management (RMM) tools: **Datto Centrastage** and **ScreenConnect (ConnectWise Control)**. These tools give the threat actor persistent, unauthorized remote access to the machine. The host has been **immediately isolated from the network** to prevent lateral movement. Both the endpoint and the associated user account should be considered compromised until fully remediated.

Incident Scope

AFFECTED HOST WORKSTATION-01	AFFECTED USER User01
SECURITY PRODUCTS Windows Defender	DETECTION TIME Mar 10, 2026 7:32 PM

AdVran SAMPLE

© 2026 AdVran

AdVran
SECURITY AT YOUR FINGERTIPS

Incident Response Report
INC-2026-03-10-7A2F
Generated: March 10, 2026 — 7:36 PM PST
Prepared for: [redacted]
Prepared by: **Michael M.**
Approved by: **Adrian Monges**

INVESTIGATIVE SUMMARY

Threat Analysis

Retroactive hunting uncovered rogue RMM deployment via social engineering

The AdVran SOC team's Retroactive Hunting & Response capability identified suspicious activity through newly developed detection methodologies. A user attempted to install a **Rogue Remote Monitoring and Management (RMM)** tool on the affected endpoint. Both the endpoint and associated user account should be considered compromised until fully remediated.

Network Isolation Active
The AdVran SOC agent has isolated this host from the network to prevent the incident from spreading.

ATTACK TIMELINE

Mar 10, 2026 7:32:09 PM	**User Downloads Malicious File** User "User01" downloads **w9_form (5).exe** via Chrome. Filename masquerades as a W-9 tax form.
Mar 10, 2026 7:32:14 PM	**Malicious Executable Launched** Chrome spawns **w9_form (5).exe** which installs Datto Centrastage RMM, then chains a second RMM.
Mar 10, 2026 7:32:19 PM	**ScreenConnect RMM Installed** Datto Centrastage chains a ScreenConnect (ConnectWise Control) installation for redundant persistence.
Mar 10, 2026 7:32:37 PM	**AdVran SOC Detects & Isolates** Rogue RMM detected via behavioral signals. Host **immediately isolated** and incident response begins.

THREAT DESCRIPTIONS

Malicious Remote Management Tool

A legitimate remote management tool misused by a threat actor to gain unauthorized access to the endpoint. Attackers use these to hide their presence and maintain persistent access.

Rogue ScreenConnect

The AdVran SOC team has been tracking threat actors who convince users via email to run malicious ScreenConnect installers that give remote access to the host.

AdVran SAMPLE

© 2026 AdVran

WHAT THIS MEANS

Understanding This Incident

What happened, why it matters, and what we're doing about it

What happened?

Someone on the "WORKSTATION-01" computer opened a file they thought was a W-9 tax form. It wasn't. It was a fake file that secretly installed two programs letting the hacker control the computer remotely.

What is an RMM tool and why is it dangerous?

RMM stands for "Remote Monitoring and Management." These are real tools that IT companies use to manage computers from a distance. Hackers use the exact same tools because antivirus programs usually don't flag them. It's like someone using a real locksmith's toolkit to break into your house. The tools are legal, but the intent is criminal.

What could the hacker do with this access?

The hacker could see everything on the screen, open files, steal passwords, access company data, or use this computer to reach other computers on your network. This type of access often leads to **ransomware**, where criminals lock all your files and demand payment.

Why were there two remote access programs?

The hacker installed two programs (Datto Centrastage and ScreenConnect) as a backup plan. If one gets removed, the other still gives them access.

What did we do about it?

The moment our system detected the threat, we **cut the computer off from your network** so the hacker couldn't reach other machines. We then remotely killed the programs, deleted the malicious files, and cleaned up everything that would have let them restart. All actions completed successfully.

Is it safe now?

The remote access tools have been removed and the computer is isolated. We still need to physically inspect the device and the "User01" user account credentials should be changed. Full next steps are outlined later in this report.

AdVran SAMPLE

© 2026 AdVran

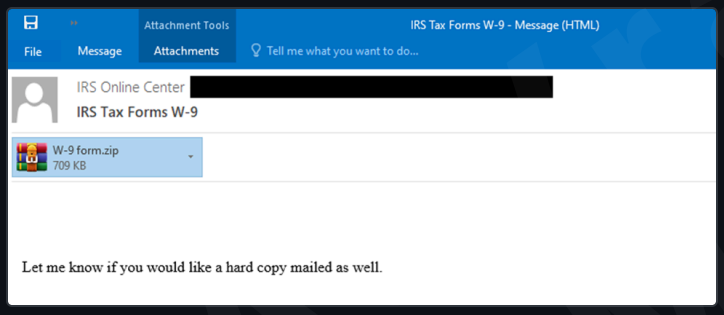
KNOWN THREAT CAMPAIGN

Possible Link: Emotet W-9 Tax Form Campaign

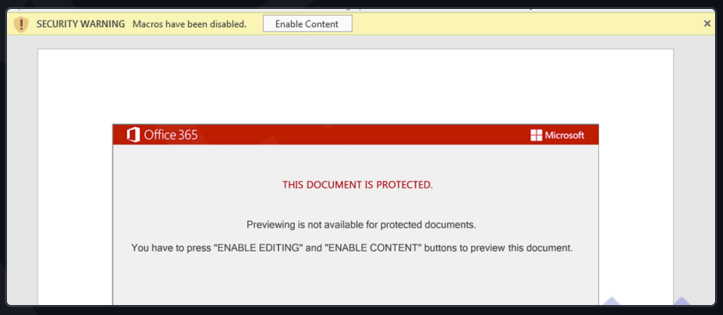
This incident closely resembles an active phishing campaign abusing fake IRS W-9 forms to deliver malware

Emotet Malware — Fake W-9 Tax Forms

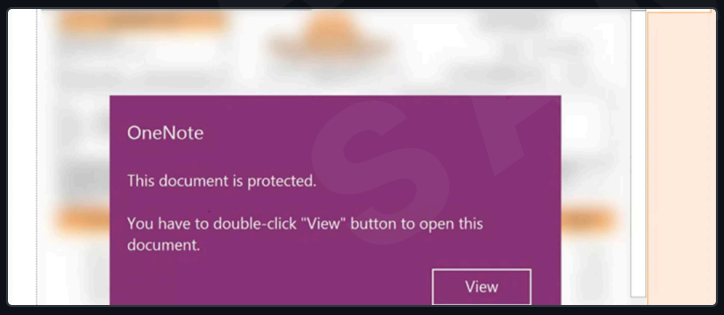
The tactics in this incident are consistent with **Emotet**, a malware operation targeting American taxpayers with fake W-9 tax forms. Emotet spreads through phishing emails disguised as IRS communications. Once installed, it steals email contacts and deploys additional payloads including ransomware. It originally relied on malicious macros in Word documents but has shifted to **OneNote files** with embedded scripts after Microsoft began blocking macros by default.



Phishing email impersonating IRS with W-9 form.zip (709 KB)



Word document prompting "Enable Content" to run macros



OneNote variant — fake "View" button runs VBScript

Indicators Matching This Incident

- ✓ File named "w9_form" — matches Emotet naming
- ✓ Delivered via web browser download
- ✓ Chains RMM installation for persistence
- ✓ Multiple file variants downloaded
- ✓ Uses legitimate tools to evade detection

What does this mean for the client?

The user on "WORKSTATION-01" likely received a phishing email appearing to be from the IRS or a business contact requesting a W-9 form. The attachment was a disguised installer. This is a **social engineering attack** that exploits trust and urgency around tax season. Even careful employees can fall for these because the emails look legitimate.

© 2026 AdVran

SIGNAL INTELLIGENCE

Lead Signal Details

Detection signal and process chain analysis for the compromised endpoint

> **Signal: Web Browser Process Spawning Renamed RMM**
>
> Fires when a browser spawns a child process matching known RMM signatures but renamed to evade detection. **w9_form (5).exe** was identified as a renamed RMM installer.

Signal Name	`Web Browser Process Spawning Renamed RMM`
Detected At	`Mar 10, 2026 7:32:09 PM PST`
Start Time	`Mar 10, 2026 7:32:09 PM PST`
Command	`"C:\Users\User01\Downloads\w9_form (5).exe"`
Executable	`C:\Users\User01\Downloads\w9_form (5).exe`
Process ID	`87635967-1c5d-11f1-a828-90ccdfe0cc24`
Parent Process	`C:\Program Files\Google\Chrome\Application\chrome.exe`
User	`User01`

PROCESS CHAIN VISUALIZATION

```
1. chrome.exe (Google Chrome — legitimate browser)
   └─ w9_form (5).exe (Malicious — renamed RMM installer)
      ├─ Datto Centrastage RMM (First-stage persistence)
      └─ ScreenConnect Client (Second-stage persistence)
         ├─ Service: ScreenConnect Client (8f371a4a6994693c)
         └─ Service: ScreenConnect Client (dca3be798b3393e7)
```

> **Why This Matters**
>
> Two separate RMM tools ensure persistence. If one is removed, the other maintains access. Both are legitimate software used by IT teams, making them hard to detect with traditional antivirus.

© 2026 AdVran

SIGNALS INVESTIGATED

Behavioral Detection Signals

12 signals processed by the AdVran SOC team in chronological order of detection

Multiple Download Attempts Detected

The signals reveal that user "User01" downloaded and executed **three separate copies** of the malicious file: **w9_form.exe**, **w9_form (3).exe**, and **w9_form (5).exe**, all via Google Chrome. This pattern suggests repeated attempts, likely from a phishing email or malicious website the user visited multiple times.

TIME (PST)	SIGNAL	DETAILS

7:32:09 PM	Web Browser Process Spawning Renamed RMM
	PROCESS
		User: User01
		`C:\Users\User01\Downloads\w9_form (5).exe`
		`Parent: chrome.exe`

7:32:12 PM	Suspicious Rogue RMM Installation PROCESS	**User:** User01 `C:\Users\User01\Downloads\w9_form.exe`
7:32:14 PM	Suspicious Rogue RMM Installation PROCESS	**User:** User01 `C:\Users\User01\Downloads\w9_form (5).exe`

7:32:17 PM	Web Browser Process Spawning Renamed RMM
	PROCESS
		User: User01
		`C:\Users\User01\Downloads\w9_form (3).exe`
		`Parent: chrome.exe`

7:32:19 PM	Suspicious Centrastage (Datto) Deploy MSI SYSTEM	**User:** SYSTEM `msiexec.exe /i "C:\WINDOWS\TEMP\ScreenConnect.ClientSetup.msi" /qn /norestart`

7:32:22 PM	Web Browser Process Spawning Renamed RMM
	PROCESS
		User: User01
		`C:\Users\User01\Downloads\w9_form.exe`
		`Parent: chrome.exe`

Continued on next page. Signals 7 through 12 including correlated detections and persistence mechanisms.

AdVran SAMPLE

© 2026 AdVran

SIGNALS INVESTIGATED (CONTINUED)

Correlated Detections & Persistence

Advanced correlation signals and persistence mechanism detections

TIME (PST)	SIGNAL	DETAILS
7:32:24 PM	Suspicious Rogue RMM Installation PROCESS	**User:** User01 C:\Users\User01\Downloads\w9_form (3).exe
7:32:27 PM	Suspicious Datto RMM with Screenconnect RMM Activity CORRELATED	Correlates: Web Browser Process Spawning Renamed RMM, Suspicious Rogue RMM Installation, Suspicious Centrastage (Datto) Deploy MSI
7:32:29 PM	Windows Trial ScreenConnect Service AUTORUN	**User:** SYSTEM ScreenConnect Client (dca3be798b3393e7)\ScreenConnect.ClientService.exe C2: instance-d3yc7o-relay.screenconnect.com:443
7:32:32 PM	ScreenconnectUrlNotHosted AUTORUN	ScreenConnect Client (8f371a4a6994693c) Persistence: Service (Own Process) C2: brooksideonline17.com:8041
7:32:35 PM	Correlated ScreenConnect Install from Downloads CORRELATED	Correlates: Web Browser Process Spawning Renamed RMM, Suspicious Rogue RMM Installation, ScreenconnectUrlNotHosted
7:32:37 PM	Windows Trial ScreenConnect Service AUTORUN	ScreenConnect Client (dca3be798b3393e7) Persistence: Service (Own Process) C2: instance-d3yc7o-relay.screenconnect.com

COMMAND & CONTROL INFRASTRUCTURE IDENTIFIED

C2 Server 1

brooksideonline17.com:8041

ScreenConnect Client (8f371a4a6994693c)
Non-standard port, likely attacker-controlled domain

C2 Server 2

instance-d3yc7o-relay.screenconnect.com:443

ScreenConnect Client (dca3be798b3393e7)
Uses legitimate ScreenConnect relay infrastructure

Key Findings from Signal Analysis

3 malicious file variants downloaded: w9_form.exe, w9_form (3).exe, and w9_form (5).exe. This indicates the user attempted to run this file multiple times, or the source delivered multiple payloads.

2 distinct C2 servers were established. One via an attacker-controlled domain (brooksideonline17.com) on a non-standard port, and another via legitimate ScreenConnect relay infrastructure to blend with normal traffic.

28-second attack chain from first signal (7:32:09 PM) to last (7:32:37 PM). The entire compromise happened in under 30 seconds.

SAMPLE

© 2026 AdVran

AUTOMATED REMEDIATIONS

SOC-Assisted Remediation Actions

Remote actions executed and approved by the AdVran SOC team to neutralize the threat

All Remediations Completed Successfully

All 7 actions below were **executed remotely and completed successfully**. Each approved by **Adrian Monges Rodriguez**.

KILL PROCESS

Kill ScreenConnect Client Service ✓ DONE

`C:\Program Files (x86)\ScreenConnect Client (dca3be798b3393e7)\ScreenConnect.ClientService.exe`

`PID: 24064`

Approved by: Adrian Monges Rodriguez

DELETE SERVICES

Delete Service — ScreenConnect Client (8f371a4a6994693c) ✓ DONE

Approved by: Adrian Monges Rodriguez

Delete Service — ScreenConnect Client (dca3be798b3393e7) ✓ DONE

Approved by: Adrian Monges Rodriguez

DELETE REGISTRY KEYS

Delete Registry Key ✓ DONE

`HKLM\SYSTEM\CurrentControlSet\Services\ScreenConnect Client (8f371a4a6994693c)`

Approved by: Adrian Monges Rodriguez

Delete Registry Key ✓ DONE

`HKLM\SYSTEM\CurrentControlSet\Services\ScreenConnect Client (dca3be798b3393e7)`

Approved by: Adrian Monges Rodriguez

DELETE MALICIOUS FILES

Delete File — ScreenConnect Client Service (Instance 1) ✓ DONE

`C:\Program Files (x86)\ScreenConnect Client (8f371a4a6994693c)\ScreenConnect.ClientService.exe`

`SHA256: 7976bc6647fead449fdd424f7ccb5150b5d896b4db23782493a11580a2515244`

Approved by: Adrian Monges Rodriguez

Delete File — ScreenConnect Client Service (Instance 2) ✓ DONE

`C:\Program Files (x86)\ScreenConnect Client (dca3be798b3393e7)\ScreenConnect.ClientService.exe`

`SHA256: c0f495e2a491f6bb90f062cefbe2668d82edd8acb1569b8be4a0d3324628d62d`

Approved by: Adrian Monges Rodriguez

AdVran SAMPLE

© 2026 AdVran

MANUAL REMEDIATIONS

Required Follow-Up Actions

Actions recommended by the AdVran SOC team to be conducted by your IT team

CRIT

Security Awareness Training for Affected User

Enroll the user "User01" in an immediate security awareness training session to reinforce safe practices in the corporate environment. This user was socially engineered into executing a malicious file disguised as a W-9 form. Targeted training should cover recognizing suspicious downloads and verifying file legitimacy before execution.

CRIT

Audit Affected Directories for Additional Artifacts

Manually inspect the following directories on the "WORKSTATION-01" endpoint for additional suspicious files and remove anything found:

```
C:\Users\User01\Downloads\
C:\Program Files (x86)\ScreenConnect Client*\
C:\ProgramData\ (check for Datto/CentraStage artifacts)
C:\Users\User01\AppData\Local\Temp\
```

CRIT

Reset User Credentials

The "User01" account should be considered compromised. Reset the local Windows password directly on the device, and change passwords for any other accounts that may share the same credentials. Review all recent sign-in activity for anomalies.

URG

Verify No Lateral Movement Occurred

Review network logs and authentication events for any signs that the attacker moved laterally from "WORKSTATION-01" to other endpoints or servers on the network before isolation was enacted. Check for RDP sessions, SMB connections, or credential usage from this machine.

URG

Check for Datto Centrastage Remnants

While the automated remediations target ScreenConnect, the initial payload also installed Datto Centrastage RMM. Verify that this tool has been fully removed including services, scheduled tasks, registry entries, and any agent files in `C:\ProgramData\CentraStage\` or similar paths.

AdVran SAMPLE

© 2026 AdVran

ON-SITE INVESTIGATION

Physical Device Inspection Findings

Results from the on-site inspection of the "WORKSTATION-01" endpoint by the AdVran team

HOW THE ATTACK HAPPENED

During the on-site investigation, we were able to reconstruct the full chain of events by reviewing browser history, downloaded files, and system logs on the "WORKSTATION-01" endpoint.

~1:00 PM	**User Searches for W-9 Form** The user used Google to search for a W-9 tax form. The search results displayed a **malicious Google Ad** at the top of the page, above the legitimate results. The ad appeared to be a real W-9 download site.
~2:00 PM	**Malicious Download via Google Ad** The user clicked the sponsored ad link and downloaded a file named **w9_form.exe**. The threat actors paid for Google Ads placement to make their malicious link appear as the top search result, a well-known tactic used in malvertising campaigns.
~2:00 PM	**Executable Runs and Displays Real W-9** When the .exe was launched, it actually **displayed a legitimate-looking W-9 form** to avoid suspicion. While the user filled out the form, the executable silently installed ScreenConnect (a legitimate RMM tool) in the background, giving the threat actor remote access.
7:32 PM	**AdVran SOC Detects and Responds** Our SOC team detected the rogue RMM activity, immediately isolated the device from the network, and executed all 7 automated remediations within minutes.

Why This Attack Worked

This was a sophisticated attack. The threat actors used **paid Google Ads** to position their malicious link above legitimate search results. The downloaded file displayed a real W-9 form so the user had no reason to suspect anything was wrong. The malware installed a legitimate IT tool (ScreenConnect) rather than traditional malware, making it harder for antivirus to flag. Everything about this attack was designed to look normal.

User Education Provided

We spoke with the affected user directly and explained the incident. Key guidance provided: **legitimate W-9 tax forms are always .pdf files, never .exe files.** Any file with an .exe extension is a program, not a document. We advised the user to always verify the URL and look for the "Ad" label on Google search results before clicking. If unsure, go directly to **irs.gov** to download official tax forms.

AdVran SAMPLE

Incident Response Report
INC-2026-03-10-7A2F
Generated: March 10, 2026 — 7:36 PM PST
Prepared for: [redacted]
Prepared by: **Michael M.**
Approved by: **Adrian Monges**

ON-SITE REMEDIATION

Device Cleanup & System Scan

Actions performed on-site to fully clean the device and return it to service

REMEDIATION STEPS PERFORMED

Device Reconnected to Network ✓ DONE

Host "WORKSTATION-01" removed from network isolation and reconnected after initial remote cleanup was verified.

Full System Scan Executed ✓ DONE

Complete system scan performed to identify any additional threats or remnants from the incident.

Incident Remnants Cleaned ✓ DONE

Remaining artifacts from the ScreenConnect/Datto installation identified during the scan were removed.

Local Windows Password Reset ✓ DONE

On-device password for the "User01" account changed directly on the machine.

ADDITIONAL FINDING: CRYPTO COIN MINER

Pre-Existing Threat Discovered

During the full system scan, we discovered an **old Crypto Coin Miner** already present on the device. This is unrelated to the current incident and was likely installed at an earlier date. Coin miners run in the background and use the computer's processing power to mine cryptocurrency for the attacker, slowing down the system and increasing power consumption. This threat was also removed during the cleanup.

Crypto Coin Miner Removed ✓ DONE

Pre-existing coin miner identified and removed from the system. Unrelated to the W-9 incident.

ADDITIONAL ON-SITE WORK

Secondary Workstation Configured ✓ DONE

Set up a second on-site computer for the affected user as a backup workstation with access to QuickBooks and Outlook, ensuring business continuity if the primary PC is ever compromised again.

System Status: Clear

The "WORKSTATION-01" endpoint has been fully cleaned, scanned, and returned to the network. All threats from the W-9 incident as well as the pre-existing coin miner have been removed. A secondary workstation has been configured as a backup. Both devices are online and protected by the AdVran SOC monitoring platform.

SAMPLE

© 2026 AdVran

INCIDENT STATUS OVERVIEW

What Happened & What We Did

Full summary of the incident from detection through on-site remediation

<4m	12	7/7	6/6
RESPONSE TIME	SIGNALS PROCESSED	REMOTE REMEDIATIONS	ON-SITE ACTIONS

Detection & Response Summary

Around 1:00 PM PST on March 10, 2026, the user on "WORKSTATION-01" searched Google for a W-9 tax form. Threat actors had placed a malicious **Google Ad** at the top of the results. The user clicked the ad and downloaded a file called w9_form.exe around 2:00 PM. The file displayed a real W-9 form while silently installing ScreenConnect, a remote access tool, in the background.

At **7:32 PM PST**, the AdVran SOC team detected the rogue RMM activity and **isolated the host within minutes**. We executed 7 automated remediation actions remotely, all approved by Adrian Monges Rodriguez and completed successfully.

During the **on-site inspection**, we confirmed the attack chain, cleaned up incident remnants, discovered and removed a pre-existing **crypto coin miner**, reset the local password, and spoke with the affected user about recognizing .exe files vs. .pdf documents. The device has been returned to the network and is fully operational.

Incident Details

ORGANIZATION
[redacted]

INCIDENT ID
INC-2026-03-10-7A2F

AFFECTED HOST
WORKSTATION-01

SEVERITY
CRITICAL

AFFECTED USER
User01 (WORKSTATION-01)

HOST STATUS
✓ BACK ONLINE

DETECTION TIME
Mar 10, 2026 7:32 PM PST

RESOLUTION
Resolved

Incident Closed

All remote and on-site remediations are complete. The device has been fully scanned, cleaned, and returned to the network. The system is protected and being actively monitored by the AdVran SOC platform. No further action is required at this time.

SAMPLE

© 2026 AdVran