Threat Intelligence Report

Exploitation of Remote Administration Tools

Remote administration tools (RATs) are widely used by organizations across the globe and in every industry. However, when left unsecured or mismanaged, RATs introduce significant cybersecurity risks; risks that can be realized through direct compromises or indirectly through supply chain attacks. RATs allow users to connect to a machine or network remotely for a variety of legitimate purposes such as allowing enterprise help desk teams to provide IT support to employees. Any legitimate access channel, however, can also be fraudulently accessed and leveraged by threat actors who – once inside the network – can access sensitive data, manipulate settings, view e-mail communications, and more. Because many organizations use RATs for innocuous reasons, these tools may not fall into the scope of solutions which are designed to detect malicious activity on the network. Mitigating the cybersecurity risks posed by these tools requires organizations to assess existing protections and processes, and implement additional measures based on specific vulnerabilities or gaps discovered.

THREAT ACTIVITY

- In 2023, the FTI Cybersecurity team assisted a high-profile organization in the professional services industry after a remote support software user account was compromised through a phishing attack. This allowed client data to be exfiltrated and held for ransom.
- In January 2024, threat actors leveraged a popular RAT to access endpoints of targeted organizations. Once initial access was gained, the threat actors attempted to deploy ransomware.
- In February 2024, a global RAT used by millions of customers fell victim to a cyber attack that compromised production systems. Although this attack targeted the well-known RAT and not its users, it demonstrates the vulnerabilities posed by RATs.
- As of February 2024, a vulnerability in a prevalent RAT is being widely exploited by threat actors. The vulnerability allows threat actors to bypass authentication requests and access restricted information.

THREAT ASSESSMENT

Recent cyber attacks leveraging RATs highlight the risks posed by third-party software, particularly remote access software. Whether exploited via supply chain attack or direct compromise, threat actors have multiple options for malicious activity once unauthorized access is obtained:

- **Data exfiltration**: Threat actors can steal sensitive or proprietary data such as client or personal information, intellectual property or financial insights. Once in possession of this sensitive material, threat actors can hold it for ransom, sell it on the dark web, or use it to commit fraud.
- **Malware installation**: Beyond data theft, threat actors can leverage this compromise to spread malware to other users within the system to launch new cyber attacks, further the reach of the initial exploit, or gain access to additional users/machines.
- **Systemic compromise**: After compromising a single user account, threat actors can gain full control over systems by escalating privileges to increase their level of access and evade security controls. This includes the ability to modify configurations and identify where critical assets are stored.
- **Maintain persistence**: Using the cover of a legitimate RAT, threat actors can covertly establish a foothold within the compromised network, carrying out malicious operations without being detected and conducting surveillance to be exploited at a later date.

RECOMMENDED ACTION

Know your environment: Determine which tools are actively used and belong on systems, and remove any that are illegitimate.

Implement whitelisting: This process adds an additional layer of security by only allowing preapproved software and programs to be used, preventing malicious software and code from being downloaded.

Establish network segmentation: Restricting access to certain devices, information, or applications will reduce a threat actor's ability to move laterally within the network.

Enable geofencing: Limit and control network access to geographical areas that are predetermined based on expected traffic.

Perform updates: Regularly patching and updating software to ensure that current versions are running will prevent known vulnerabilities from being exploited.

SOURCES

Sources include open-source information from public and private industry reporting.

- Newest Ivanti SSRF zero-day now under mass exploitation
- AnyDesk Hacked: Revokes Passwords, Certificates in Response
- TeamViewer abused to breach networks in new ransomware attacks
- CISA – Guide to Securing Remote Access Software

Why FTI Cybersecurity

Multidisciplinary Expertise

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, prosecuting offices, and global private sector institutions

Globally Positioned

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

Integrated & Comprehensive

Comprehensive services include crisis communications, e-discovery, forensic investigations, and more

Seamless integration of FTI Consulting's expertise across service offerings

FTI Cybersecurity Global Offices

Americas

Atlanta
Boston
Chicago
Dallas
Houston
Irvine
Los Angeles
Mexico City
Miami
New York
Philadelphia
Roseland
San Francisco
Sao Paulo
Seattle
Toronto
Washington, DC
Wayne

EMEA

Berlin
Brussels
Cape Town
Dubai
Dublin
Dusseldorf
Frankfurt
Johannesburg
London
Madrid
Mumbai
Munich
Paris
Zurich

APAC

Brisbane
Hong Kong
Melbourne
Perth
Shanghai
Singapore
Sydney
Tokyo

CONTACT FTI CYBERSECURITY

Email: #fticybersecurity@fticonsulting.com

Phone: +1-844-CYBR-FTI (+1-844-292-7384)