June 27, 2025

EMERGING THREATS

MOMMY ACCESS BROKER

mommy, also known as "Miyako" or "Miya," is an emerging and sophisticated cyber threat actor that has gained attention since 2024 due to their advanced cyber-espionage capabilities and active involvement in high-profile attacks. Operating within underground cybercrime markets, mommy specializes in providing illicit services, including access to compromised networks and the sale of sensitive data. Their activities indicate a focus on espionage, data exfiltration, and exploiting high-value targets, particularly government entities, telecommunications companies, and critical infrastructure providers.

THREAT SUMMARY

mommy, also known as "Miyako" or "Miya," is an emerging and sophisticated cyber threat actor that has gained attention since 2024 due to their advanced cyber-espionage capabilities and active involvement in high-profile attacks. Operating within underground cybercrime markets, mommy specializes in providing illicit services, including access to compromised networks and the sale of sensitive data. Their activities indicate a focus on espionage, data exfiltration, and exploiting high-value targets, particularly government entities, telecommunications companies, and critical infrastructure providers.

The threat group has been observed selling unauthorized access to networks and systems, enabling other threat actors to opportunistically access compromised devices for further exploitation or to deploy malicious payloads. The access broker has targeted a range of industries, including government institutions in the United States, critical infrastructure providers, and telecommunications. With a particular focus on monetizing stolen access and information, the access broker is a part of a growing trend of "access-as-a-service" models, where cybercriminals commodify network access for profit. These activities point to the increasing commercialization of cybercrime, where stolen credentials and system vulnerabilities are sold to the highest bidder, often nation-state actors. Additionally, with a focus on maintaining anonymity and privacy in their operations, it is a significant challenge for cybersecurity efforts and makes them a formidable threat to organizations worldwide.

In January 2025, a copy of the access broker's "Guide", previously offered for sale, was uploaded to VirusTotal. The guide outlines detailed methodologies for conducting intrusions, maintaining persistence, expanding initial footholds, and monetizing compromised access and data. Intel 471's TITAN reporting, cited in the "Intel 471 References" section below, provides invaluable insights into the access broker's activities, affiliations, and operational links to other groups, often surfacing intelligence well before any public leaks or reporting. This advanced visibility ensures greater preparedness and a deeper understanding of how the broker operates within the broader cybercriminal ecosystem.

TITAN References:

Info Report: Hacking Guide Analysis
https://titan.intel471.com/report/inforep/ed60c1019a8fb92d005a9a26f20218e9)

TITAN Search: mommy

https://titan.intel471.com/search/Actor:mommy/reports?data_sets=news%2Creports%2Cdataleaks%2Ccve%2Cmalware%2Ccredentials%2Cgeopol&ordering=latest&period_of_time=all)

Info Report: TITLE REDACTED

https://titan.intel471.com/report/inforep/0a111df83cfe33aca412a01f2ec22525)

Info Report: TITLE REDACTED

https://titan.intel471.com/report/inforep/afe4f9dbf27c524372c0fa03e3d346bf)

Info Report: TITLE REDACTED

https://titan.intel471.com/report/inforep/024cc5139af775d5769d8909f870f65f)

Info Report: TITLE REDACTED

https://titan.intel471.com/report/inforep/80ae1f0e542d5c9fff6895fe4fccfdaa)

Info Report: TITLE REDACTED

https://titan.intel471.com/report/inforep/411328b7752ccf9b229bf22cc7ae4e70)

Info Report: TITLE REDACTED

https://titan.intel471.com/report/inforep/8a0d657c7b2562bdc2b1fca682b5d236)

Info Report: TITLE REDACTED

https://titan.intel471.com/report/inforep/6a93c14d644af35e8ed71f2f324f9b69

SYNOPSIS

mommy (or Miyako) employs a range of advanced techniques to infiltrate and compromise target networks. Identified in a step-by-step intrusion guide found in VirusTotal, Intel 471 TITAN Report, the access broker employs a variety of sophisticated tactics, techniques, and procedures (TTPs) to gain unauthorized access to networks and systems. With the guide serving as a paid training manual for aspiring access brokers and cybercriminals looking to replicate their methods, it can give them a blueprint (walkthroughs, tools, commands, and philosophies) to perform the same attacks as the broker themselves do and provides suggestions of how to market and sell the access systems and data.

The Initial Access walkthrough within the step-by-step guide includes the leveraging of publicly available PoCs for known CVEs and scanning internet-exposed systems using tools like Shodan, FOFA, and Leakix. They exploit several vulnerabilities, including those impacting F5's Big-IP Advanced Firewall Manager, Palo Alto Network's PAN-OS, and Webmin, as well as a zero-day vulnerability in OpenBSD.

Tools such as Bloodhound, Burp Suite, Nmap, OWASP Amass, and Sliver are also utilized for reconnaissance, information gathering, and lateral movement, while DNS tunneling and living-off-the-land binaries (LOLBins) facilitate evasion. The guide emphasizes rapid exploitation, automation, and scalability, demonstrating how to test, validate, and deploy exploits with minimal setup. This methodology enables both the broker and their follower(s) to systematically compromise high-value targets with little technical friction, forming the backbone of their access operations.

These tools and services indicate that mommy operates with a high degree of sophistication, offering customizable cyberattack capabilities to other threat actors and even a blueprint for aspiring attackers on how to operate as an access broker. Their activities underscore the increasing commercialization of cybercrime, where access to critical systems and data is commodified and sold to the highest bidder.

HUNT PACKAGE COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('C4F4DE9B-C04A-4067-A018-13C789521C19'),touched:!t)

RELATED HUNT PACKAGES

CURL/WGET Download and Execute - Potential Payload Download Followed by Execution

https://hunter.cyborgsecurity.io/details/use-case/b585a013-e56d-4c3f-ac29-f2a610ac0ce8

Desktopimgdownldr LOLBin - Download File

https://hunter.cyborgsecurity.io/details/use-case/89673666-d647-465d-981b-0c8ff896c32d

Common Suspicious Powershell Execution Argument Techniques - Bypass and Unrestricted Policies

https://hunter.cyborgsecurity.io/details/use-case/9762067d-ac45-450e-b1f0-bea9d2e219d7

CronJobs Pointed at Hidden Directories - Linux

https://hunter.cyborgsecurity.io/details/use-case/c9b77333-a233-4e86-8cba-9675686375df

hh.exe LOLBin - Download File

https://hunter.cyborgsecurity.io/details/use-case/520eeaf4-02b9-4f23-8060-d56dec4bfece

Powershell History Modification or Deletion

https://hunter.cyborgsecurity.io/details/use-case/ccdd03de-8fbf-436b-99ba-00dfee83d42f

Living Off The Land Technique - Esentutl.exe

https://hunter.cyborgsecurity.io/details/use-case/dd2fd4e0-dab9-47cd-b1ba-8aa3b63a7af9

Usage of chmod to Enable Execution - Potential Payload Staging

https://hunter.cyborgsecurity.io/details/use-case/dfbdc565-a37c-472b-a4c7-6c0e5325b255

sshd Process Executing Commands as root User - Potential Abuse or RCE

https://hunter.cyborgsecurity.io/details/use-case/626d36f2-6615-4c98-956c-2b060d1878df

Methods for Downloading Files with PowerShell

https://hunter.cyborgsecurity.io/details/use-case/c7b320fb-ac67-45b0-92c4-b0f1e10b4e46

Wevtutil Cleared Log

https://hunter.cyborgsecurity.io/details/use-case/7ceada06-54e2-4b44-9dca-b4e8d4ba401d

Powershell Download and Execute Dropper Behavior - Separate Command Calls

https://hunter.cyborgsecurity.io/details/use-case/a669df93-4b21-45d9-bbb6-e9c987587cef

Microsoft SQL executing LOLBins

https://hunter.cyborgsecurity.io/details/use-case/9b9c2062-16e7-4706-b0b2-3f78083597fe

Linux Command History Removal

https://hunter.cyborgsecurity.io/details/use-case/9d6c5d91-306b-4447-a36e-5f83d958f677

MITRE CONTEXT

- **Actors:**
  - mommy Access Broker
- **Threat Names:**
  - Sliver
- **Mitre Technique IDs:**
  - T1021.004
  - T1105
  - T1564.004
  - T1222.002
  - T1070.001
  - T1218
  - T1053.003
  - T1070
  - T1133
  - T1005
  - T1190
  - T1070.003
  - T1059.001
  - T1195.001
  - T1218.001
  - T1059
  - T1003.003
- **Mitre Technique Names:**
  - NTDS
  - Ingress Tool Transfer
  - External Remote Services
  - Compromise Software Dependencies and Development Tools
  - NTFS File Attributes
  - PowerShell
  - Indicator Removal
  - Linux and Mac File and Directory Permissions Modification
  - Compiled HTML File
  - Command and Scripting Interpreter
  - SSH

    - Cron
    - Clear Command History
    - System Binary Proxy Execution
    - Exploit Public-Facing Application
    - Data from Local System
    - Clear Windows Event Logs
- **Mitre Tactic Names:**
    - Collection
    - Credential Access
    - Defense Evasion
    - Command and Control
    - Execution
    - Persistence
    - Initial Access
- **Exploits Vulns:**
    - CVE-2024-3400
    - CVE-2024-1709
    - CVE-2024-3094
    - CVE-2024-1708
    - CVE-2021-4436
    - CVE-2025-0282

REFERENCES

1. https://titan.intel471.com/report/inforep/ed60c1019a8fb92d005a9a26f20218e9
2. https://www.virustotal.com/gui/file/1fe8c33c1a836bc30f699ced372e6ff4aff397d19a8a5284aff1ecf2711d0d47