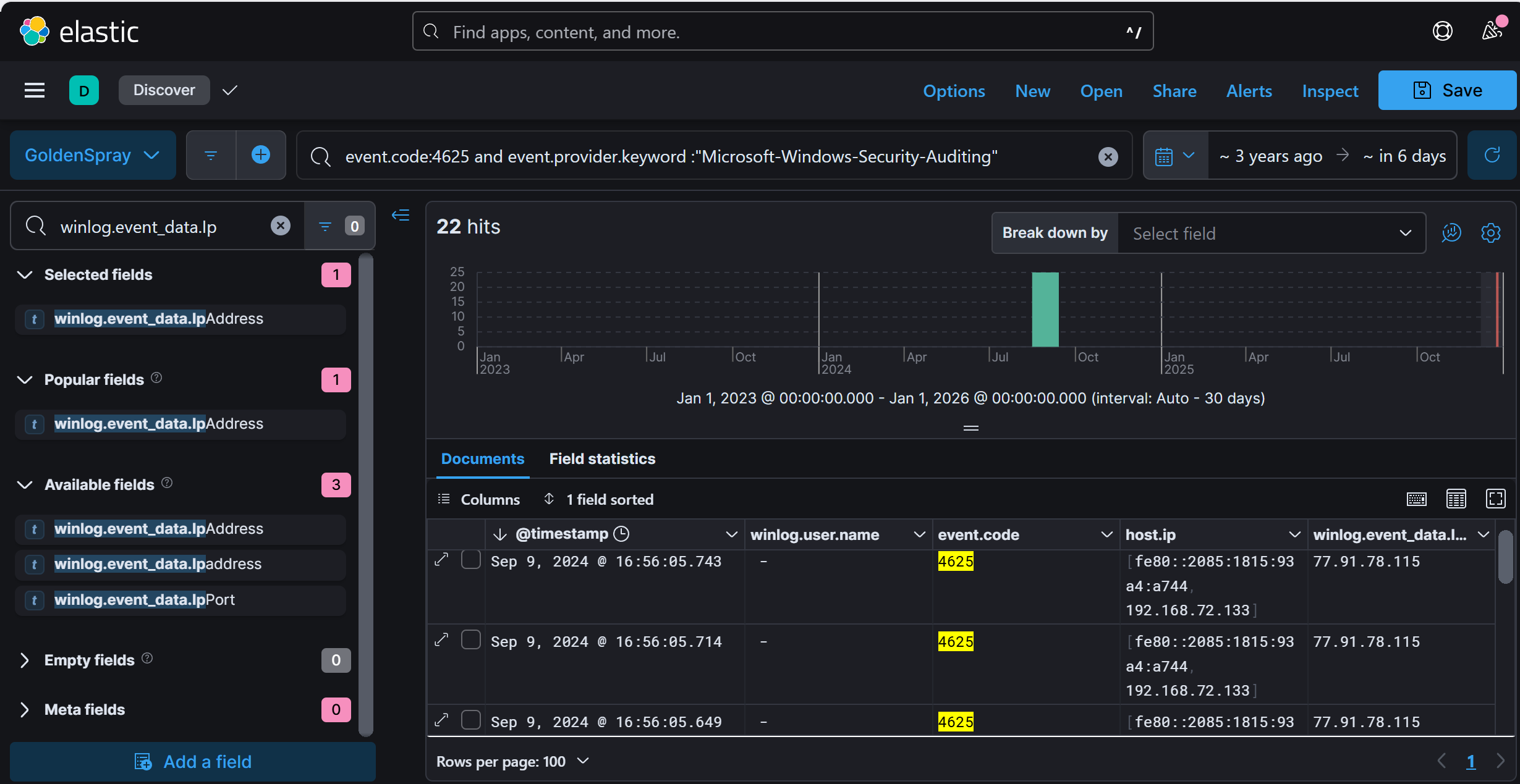
[**GoldenSpray Lab Official Walkthrough**](https://cyberdefenders.org/blueteam-ctf-challenges/goldenspray/)

Scenario

As a cybersecurity analyst at SecureTech Industries, you've been alerted to unusual login attempts and unauthorized access within the company's network. Initial indicators suggest a potential brute-force attack on user accounts. Your mission is to analyze the provided log data to trace the attack's progression, determine the scope of the breach, and the attacker's TTPs.

Q1: What is the attacker's IP address?

* Investigate failed login attempts in the logs. Look for a pattern of multiple failed attempts within a short period.
* Use Event ID 4625 (Failed Logon) in Windows Security logs. Filter logs in Elastic using event.code: 4625.
* Query Elastic with event.code: 4625 AND event.provider.keyword: Microsoft-Windows-Security-Auditing. Identify the source IP associated with multiple failed logins.

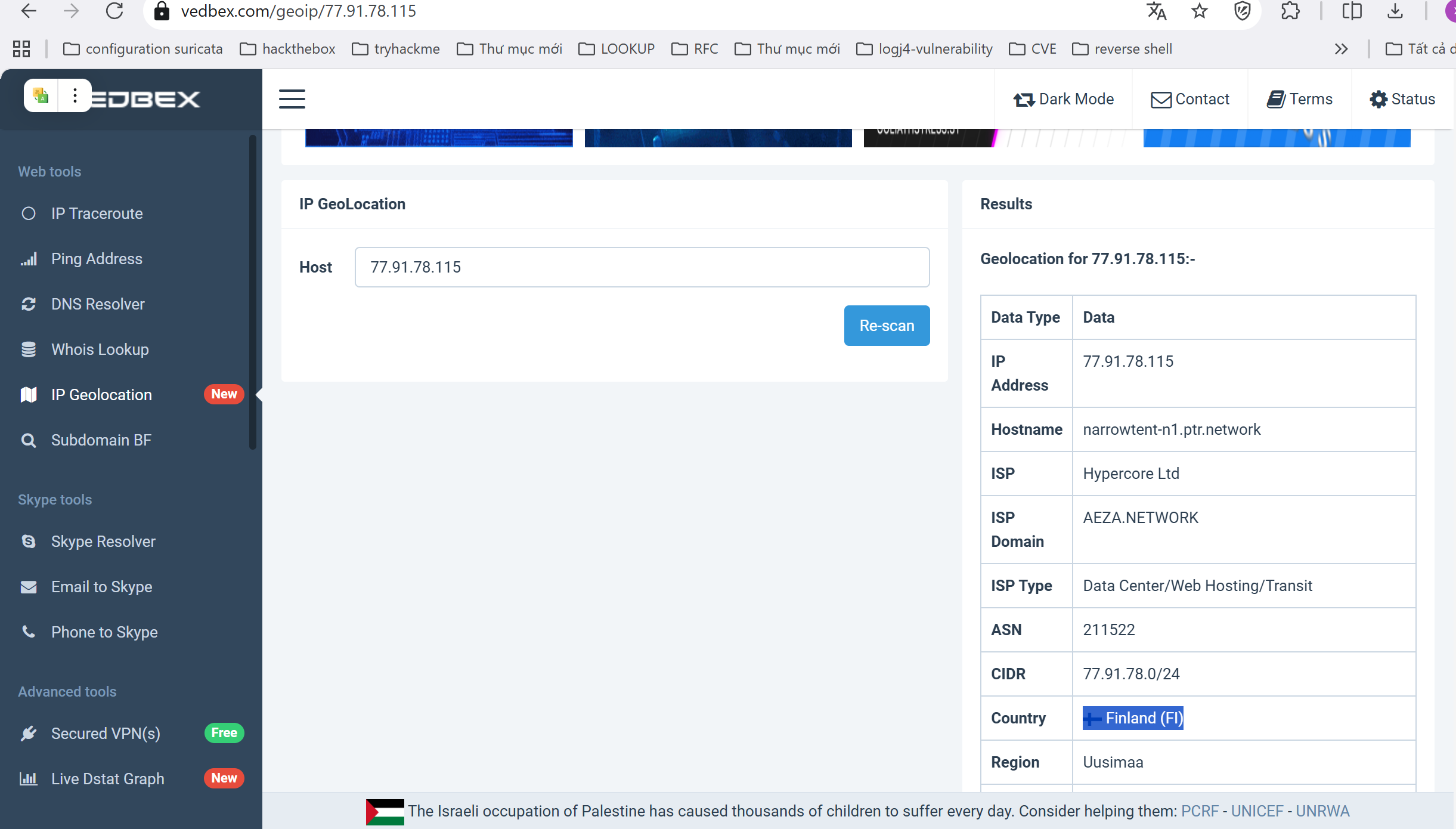


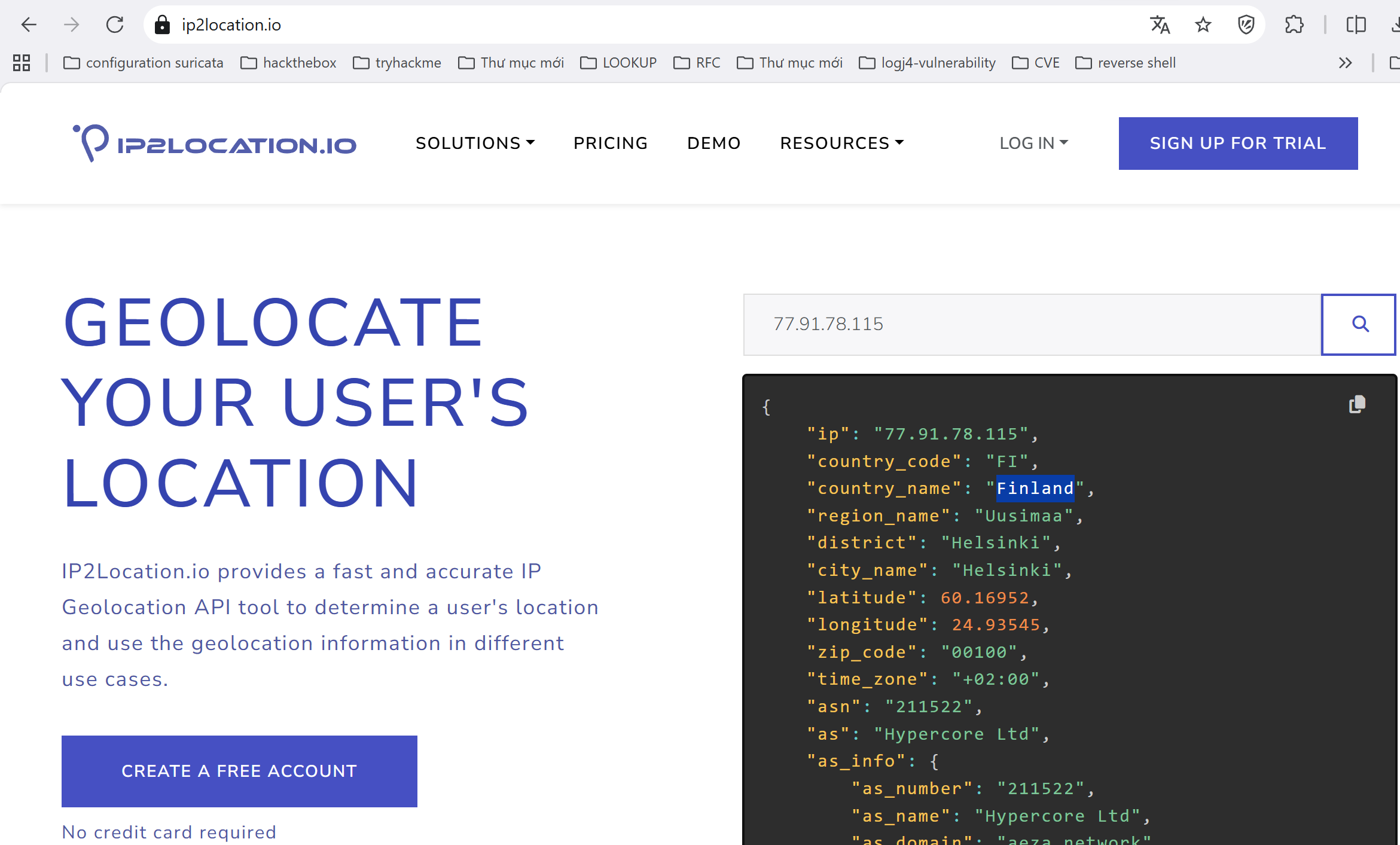
Anwser: 77.91.78.115

Top of Form

Q2: What country is the attack originating from?Top of Form

* Now that you have the attacker’s IP, you need to determine where it's coming from.
* Use an IP geolocation service to map the IP address to a country.
* Enter the attacker's IP into a service like IP2Location.io or MaxMind GeoIP to find the country.



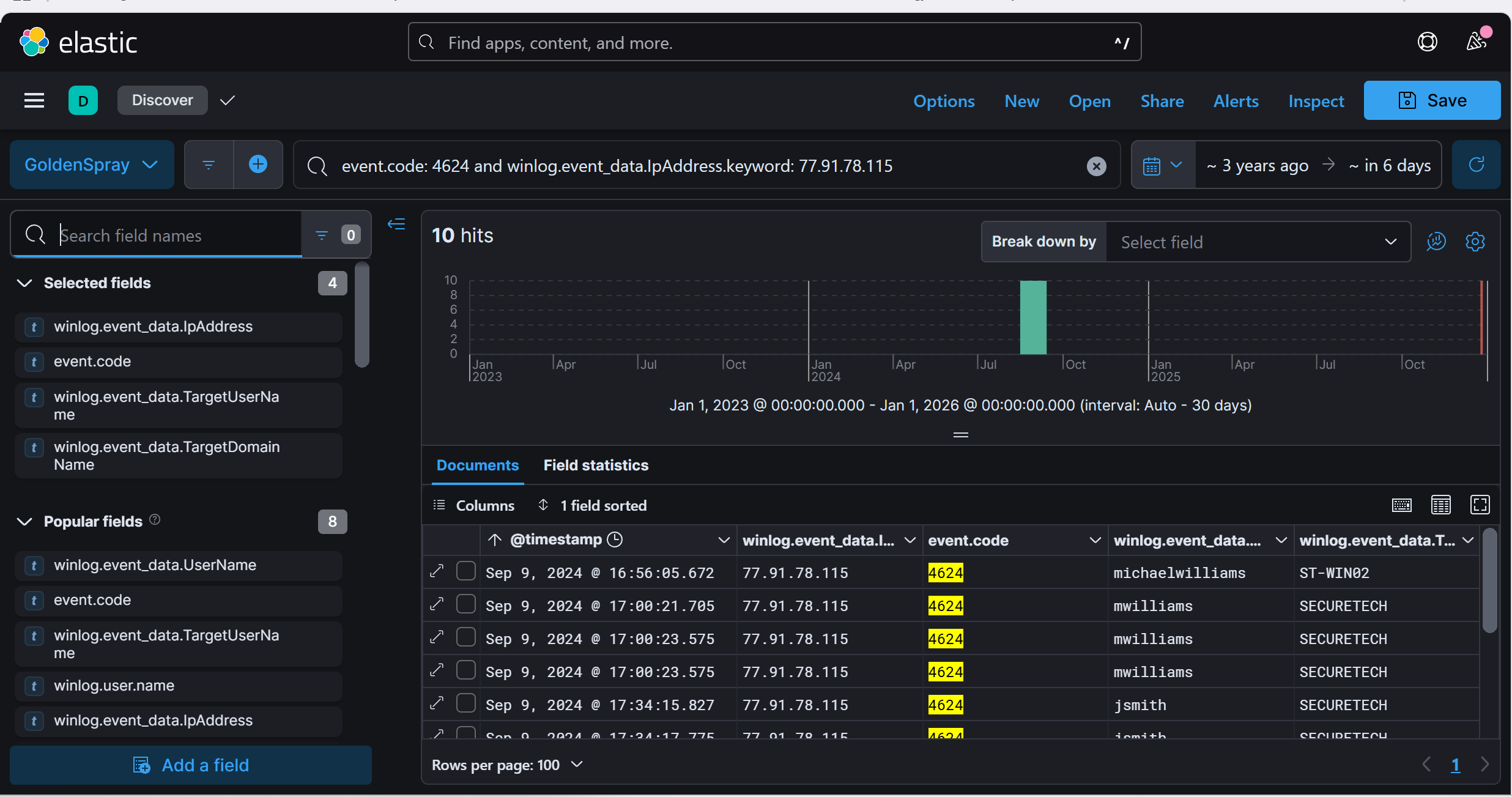


Answer: Finland

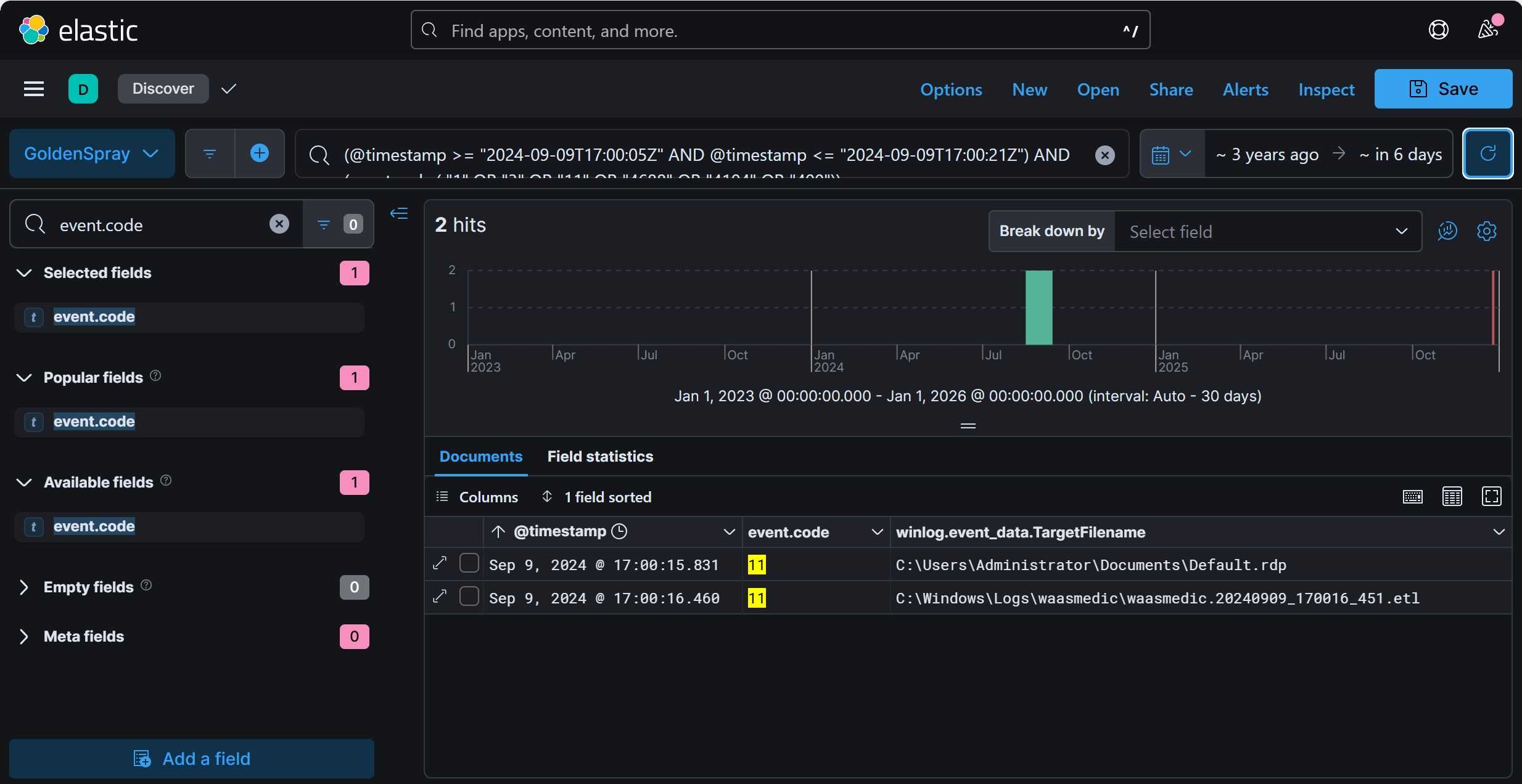
Q3: What's the compromised account username used for initial access?

Top of Form

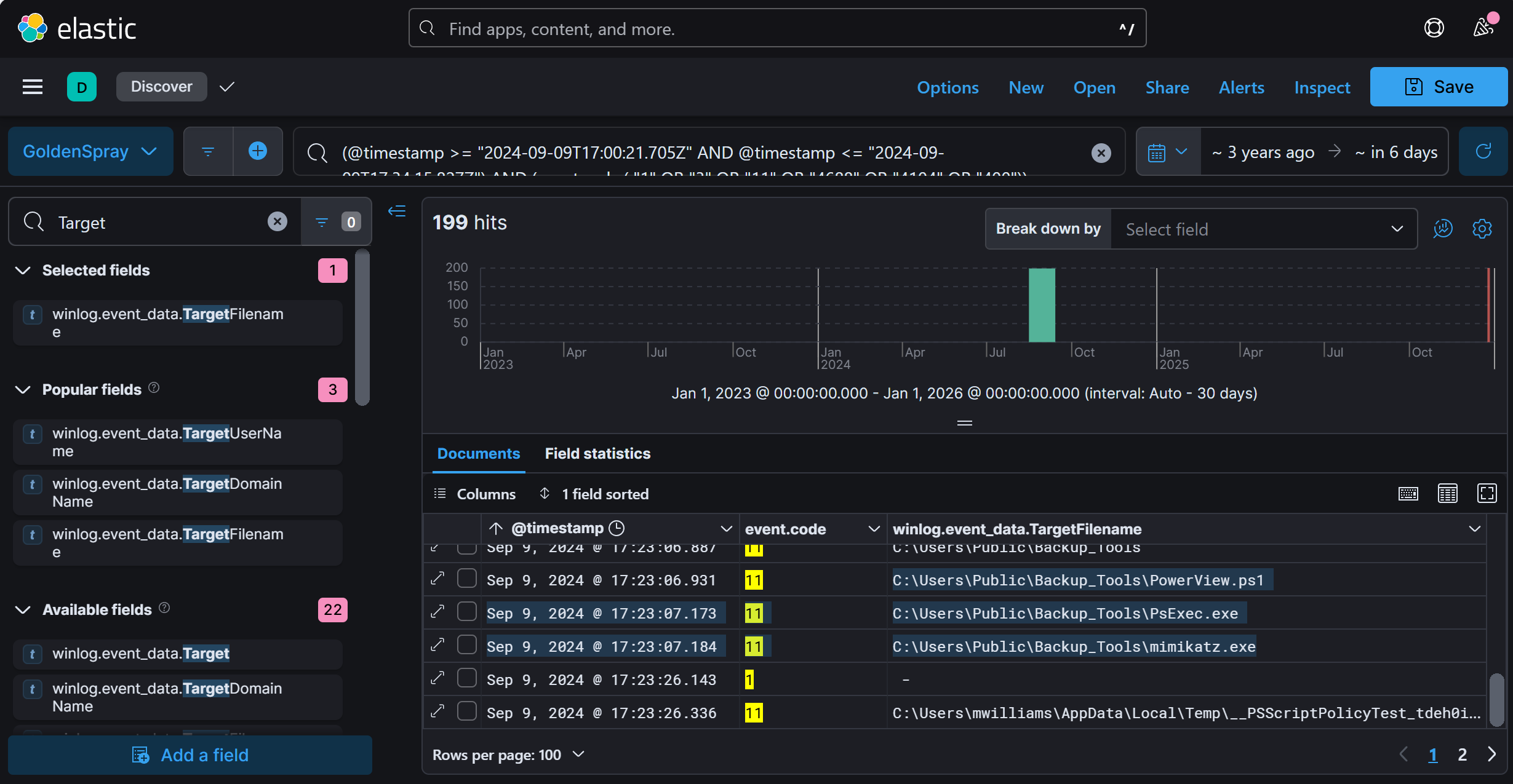
* Once an attacker gains access, there should be a successful login event associated with their IP.
* Look at Event ID 4624 (Successful Logon) in Windows Security logs. Filter logs in Elastic using event.code: 4624.
* Query Elastic using event.code: "4624" AND winlog.event\_data.IpAddress: <attacker's IP>. Find the username linked to a successful login.

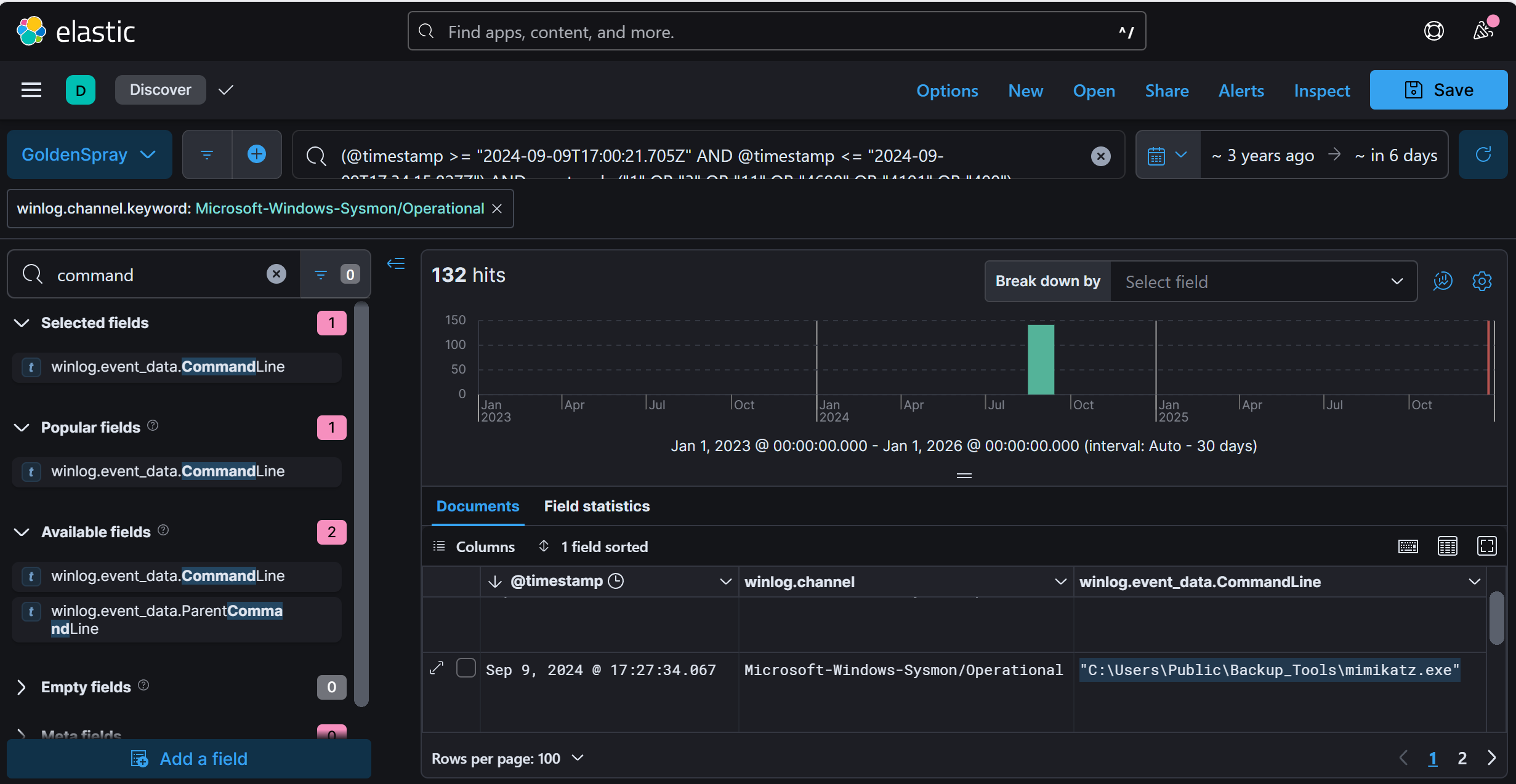


Query : (@timestamp >= "2024-09-09T16:56:05Z" AND @timestamp <= "2024-09-09T17:00:21Z") AND (event.code:( "1" OR "3" OR "11" OR "4688" OR "4104" OR "400"))



Query: (@timestamp >= "2024-09-09T17:00:21.705Z" AND @timestamp <= "2024-09-09T17:34:15.827Z") AND (event.code:( "1" OR "3" OR "11" OR "4688" OR "4104" OR "400"))

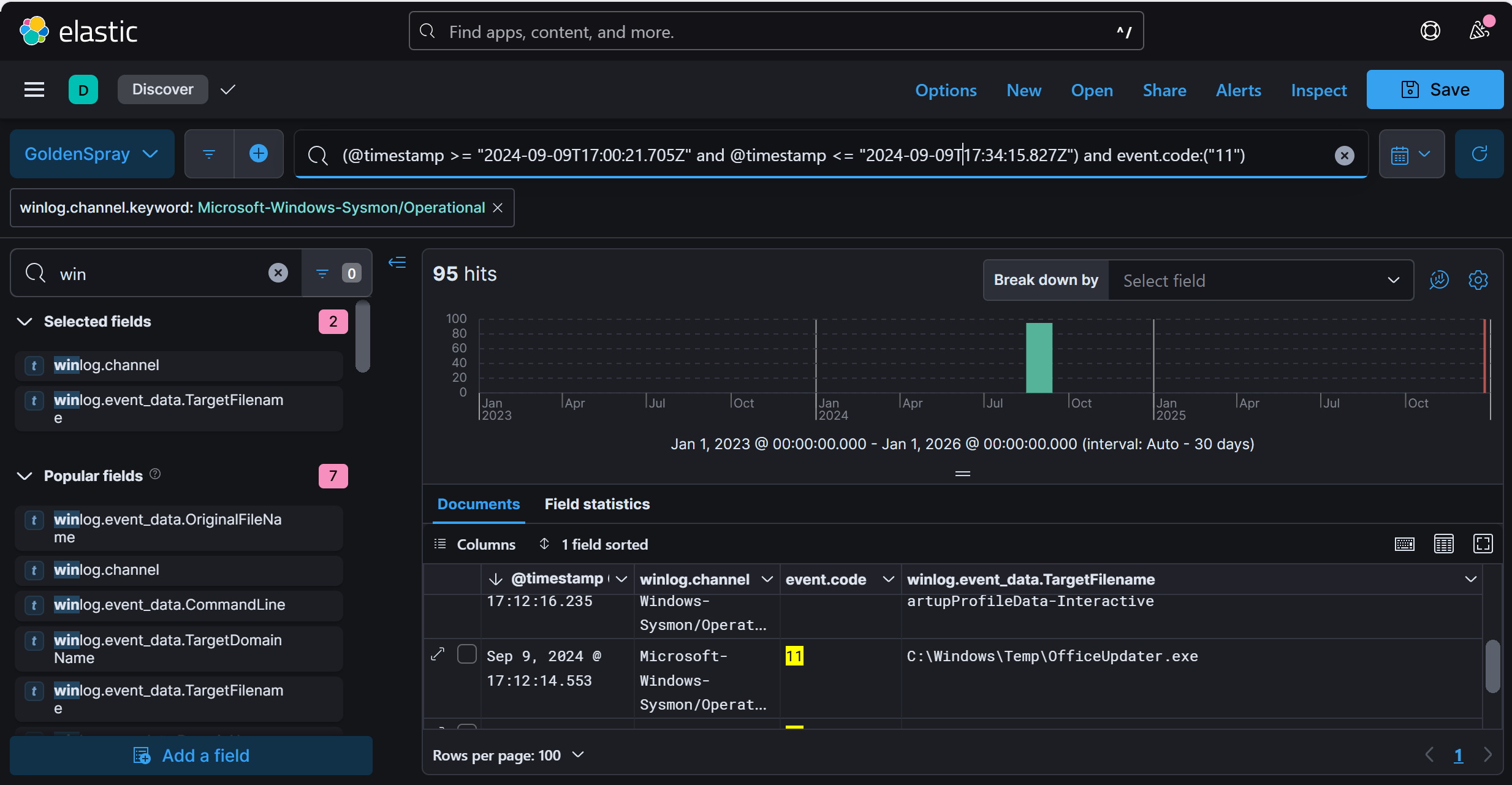




Answer: SECURETECH\mwilliams

Q4: What's the name of the malicious file utilized by the attacker for persistence on ST-WIN02?

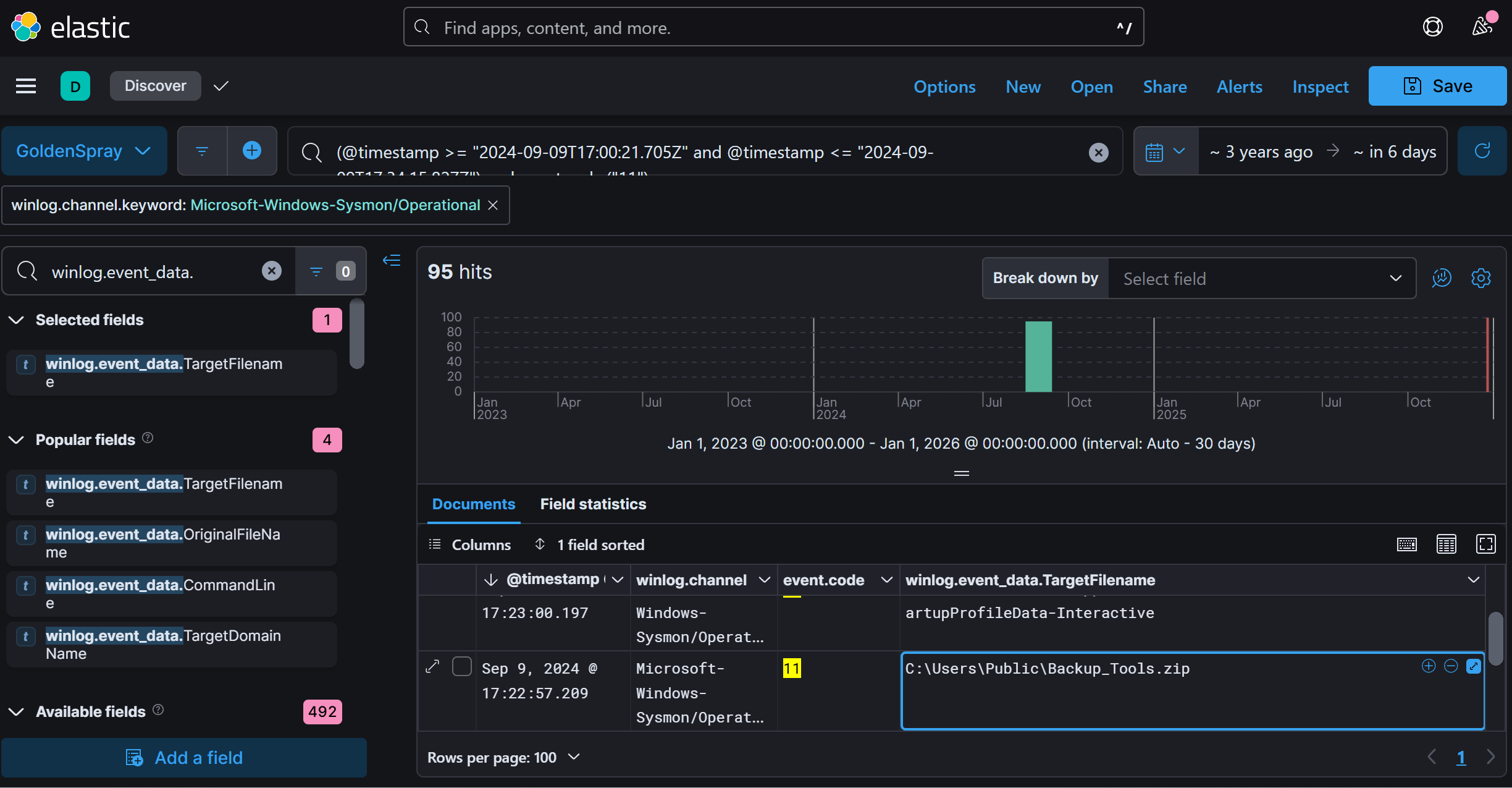
* Attackers often create malicious files in temporary or system directories for persistence.
* Look for Sysmon Event ID 11, which tracks file creation events. Investigate files created around the time of the attack.
* Query Elastic for event.code: 11 AND winlog.event\_data.TargetFilename:\*ST-WIN02\*. Look for suspicious files in C:\Windows\Temp.

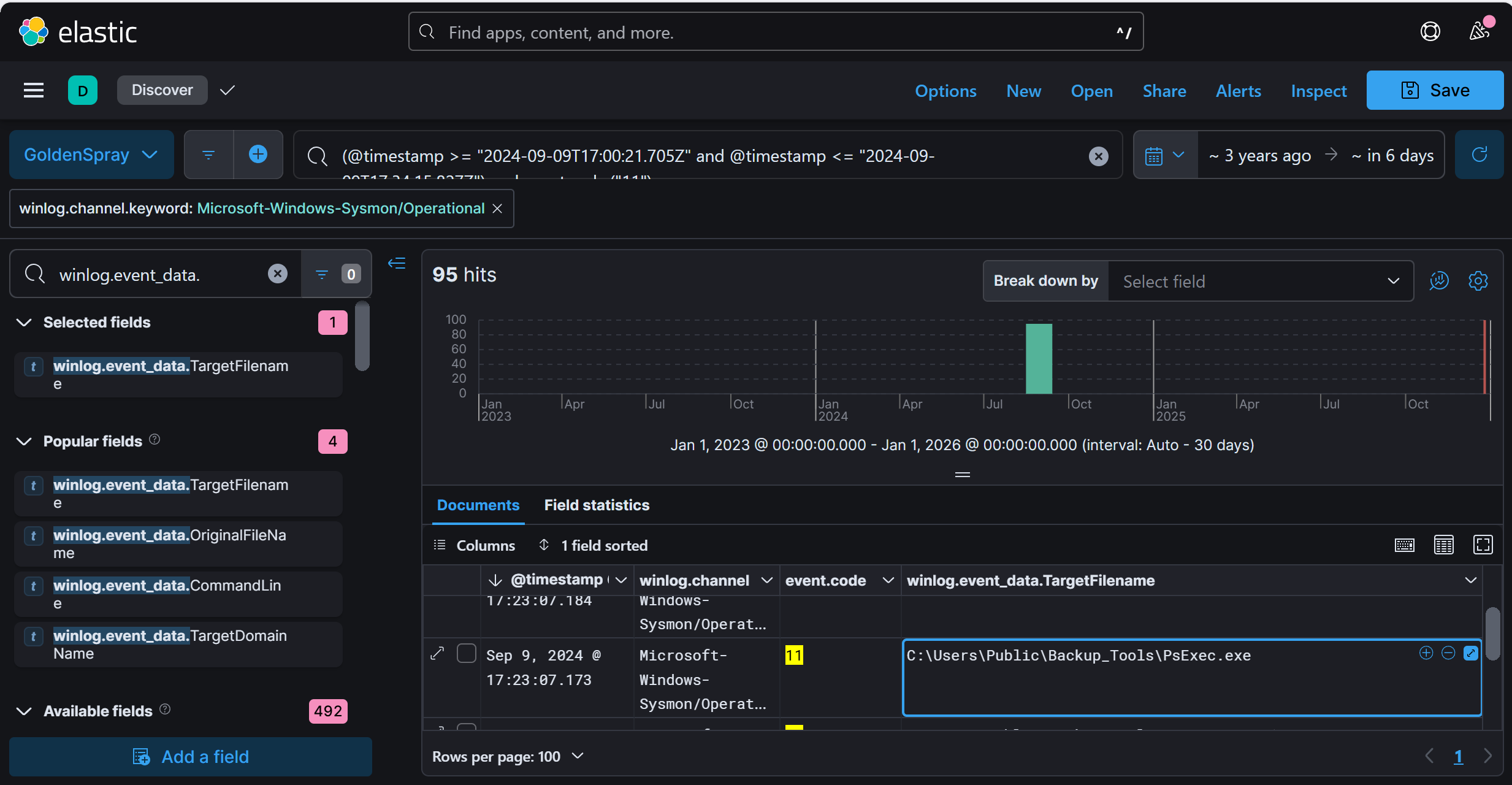


Answer: OfficeUpdater.exe

Q5: What is the complete path used by the attacker to store their tools?

* Attackers usually store tools in easily accessible directories like Public, Temp, or AppData. Top of Form
* Use Sysmon Event ID 11 to track file creation activity. Look for known attack tools.
* Query Elastic for event.code: 11 AND winlog.event\_data.TargetFilename:\*. Look for files associated with red-teaming/offensive security.

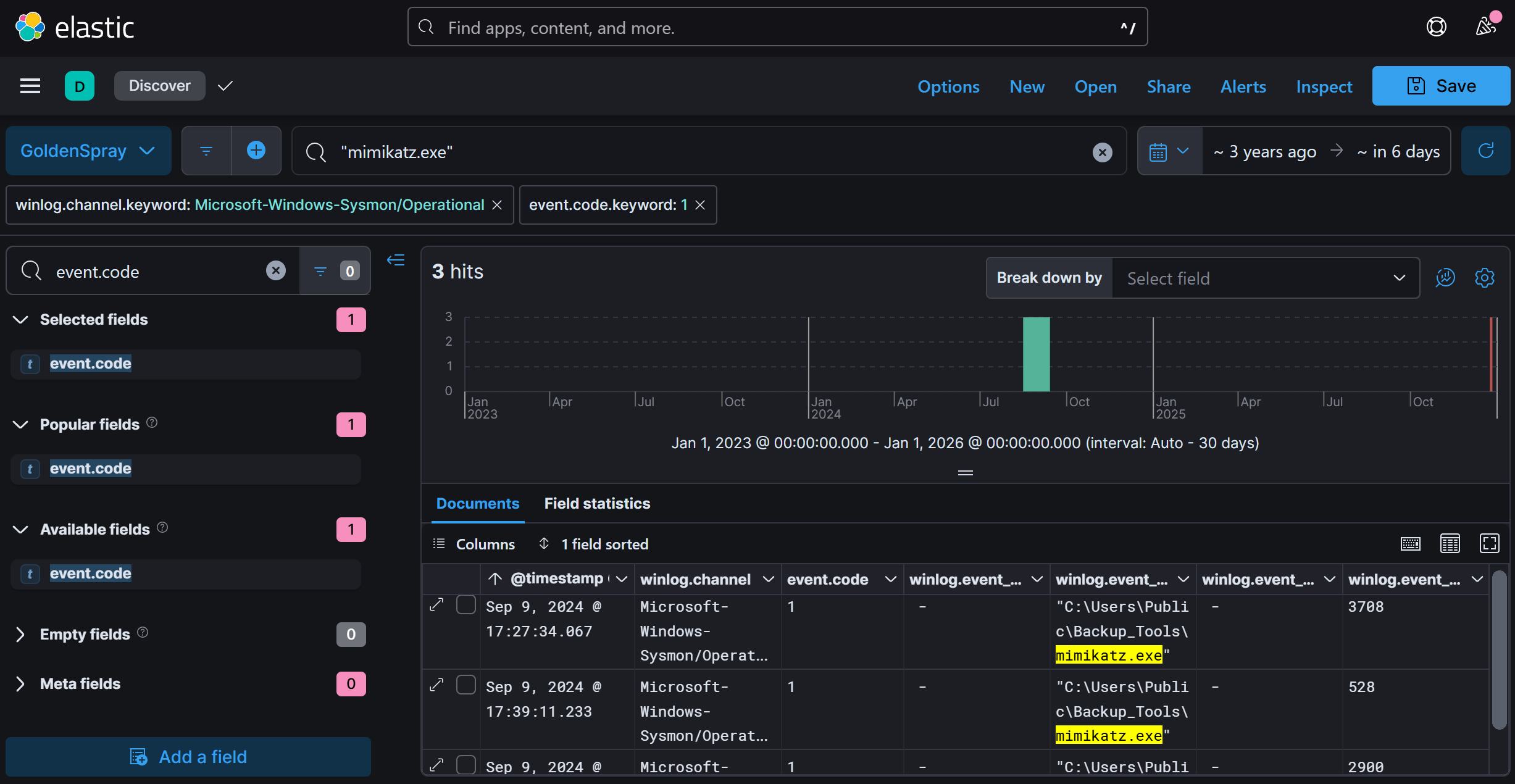




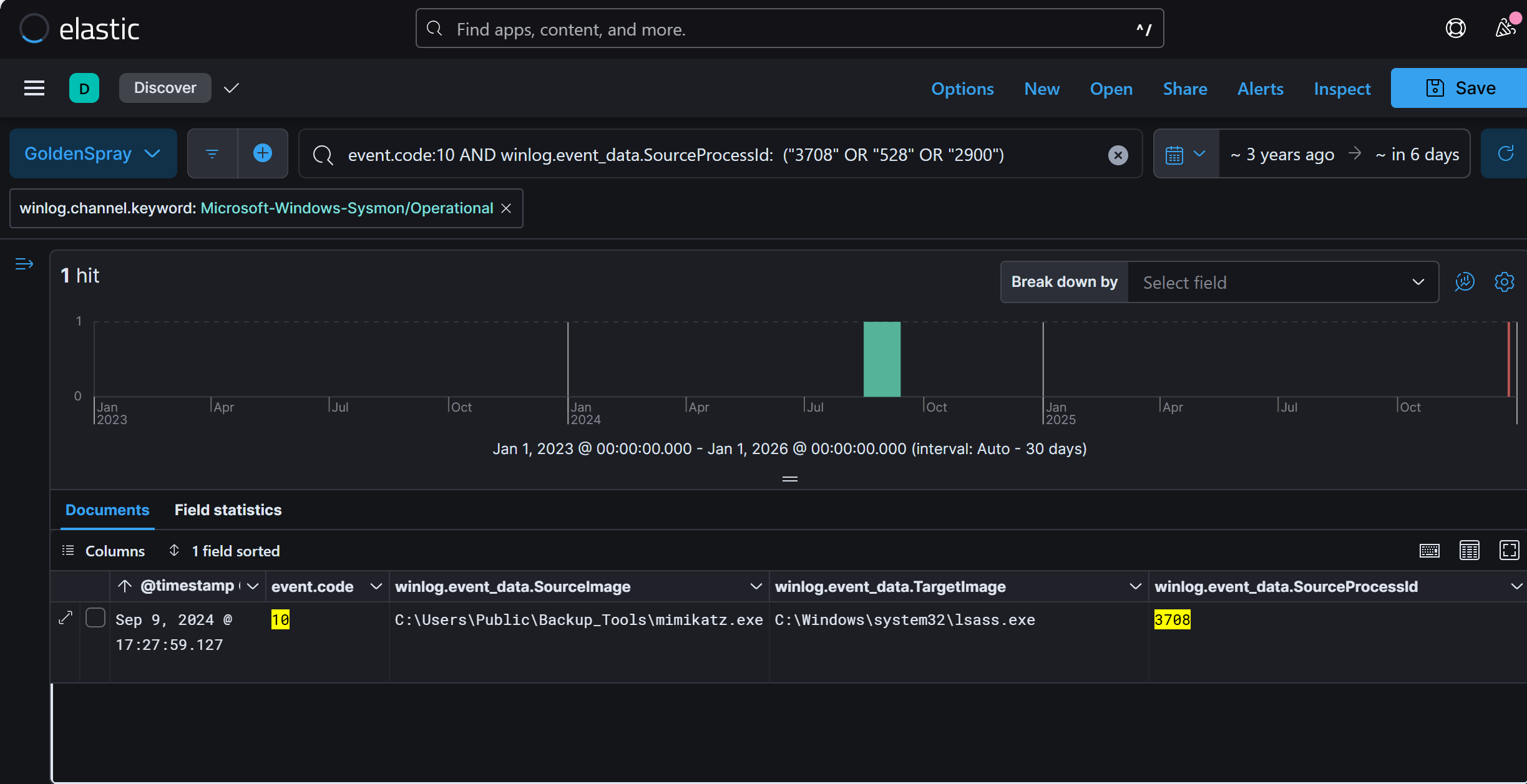
Answer: C:\Users\Public\Backup\_Tools\

Q6: What's the process ID of the tool responsible for dumping credentials on ST-WIN02?Top of Form

* Credential dumping tools often interact with the LSASS process.
* Look for Sysmon Event ID 10 (Process Access) and Event ID 1 (Process Creation) to detect Mimikatz or similar tools.



Query : event.code:10 AND winlog.event\_data.SourceProcessId: ("3708" OR "528" OR "2900")

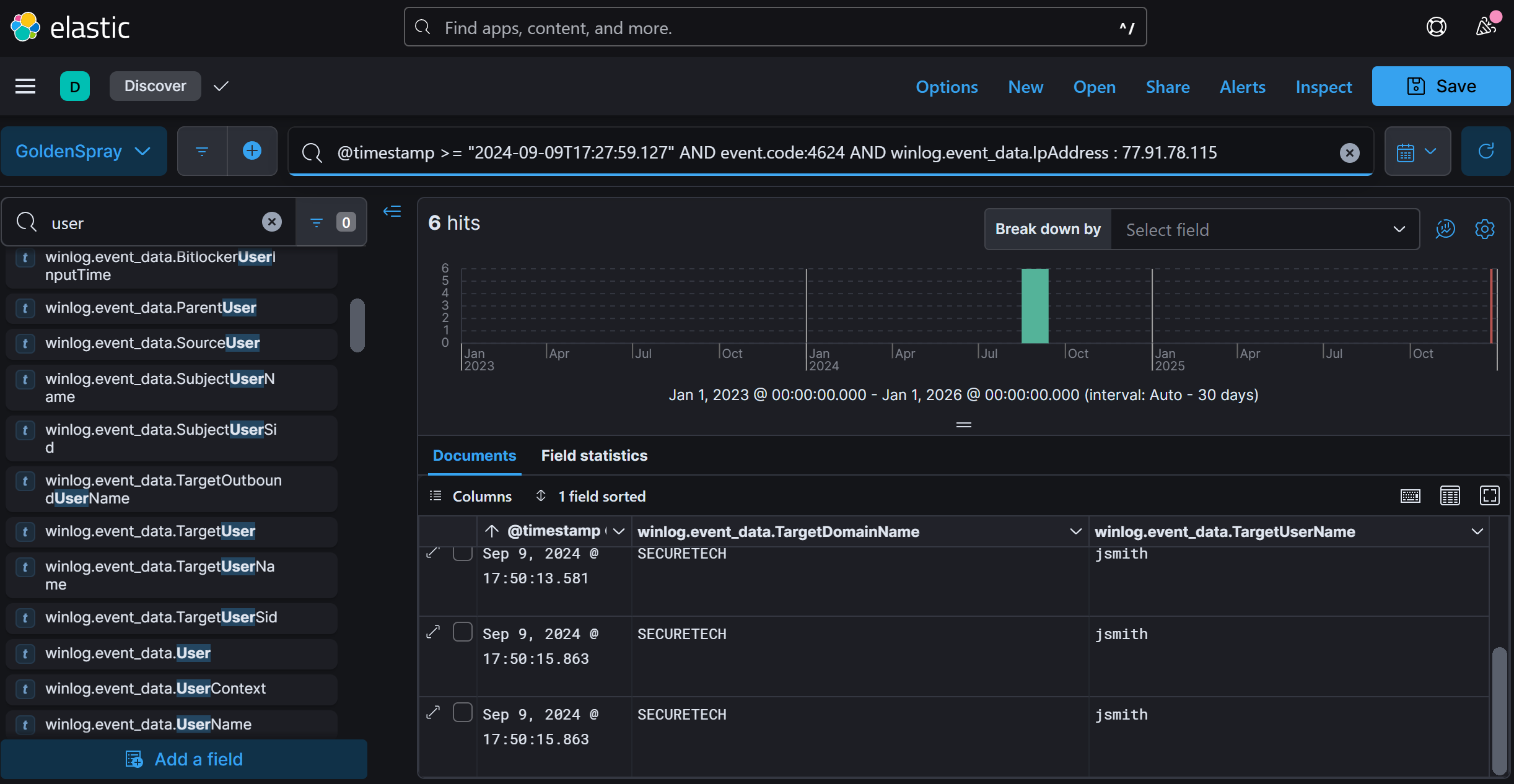


Answer: 3708

Q7: What's the second account username the attacker compromised and used for lateral movement?

Top of Form

* After gaining initial access, attackers usually escalate privileges or move laterally to another account.
* Look for successful logins (Event ID 4624) occurring after the credential dump.
* Query Elastic for event.code: "4624" AND winlog.event\_data.IpAddress: <attacker's IP> after the credential dump timestamp. Find the second compromised account.

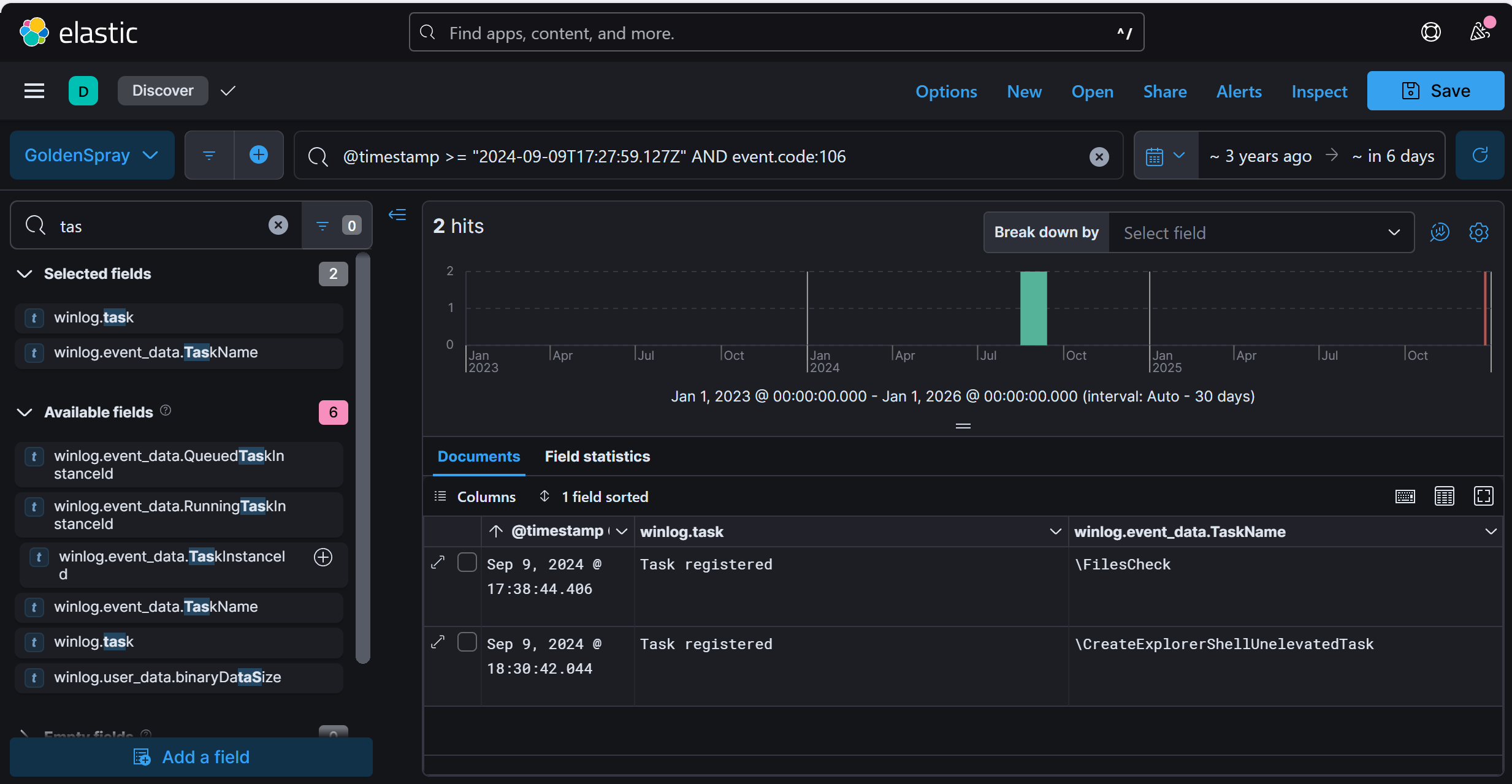


Answer: SECURETECH\jsmith

Q8: Can you provide the scheduled task created by the attacker for persistence on the domain controller?

* Attackers often use Scheduled Tasks to maintain persistence
* Look for Event ID 106, which logs the creation of scheduled tasks.
* Query Elastic for event.code: 106 and check for a suspicious task name. Look for PowerShell scripts or executables being scheduled.

Query: @timestamp >= "2024-09-09T17:27:59.127Z" AND event.code:106

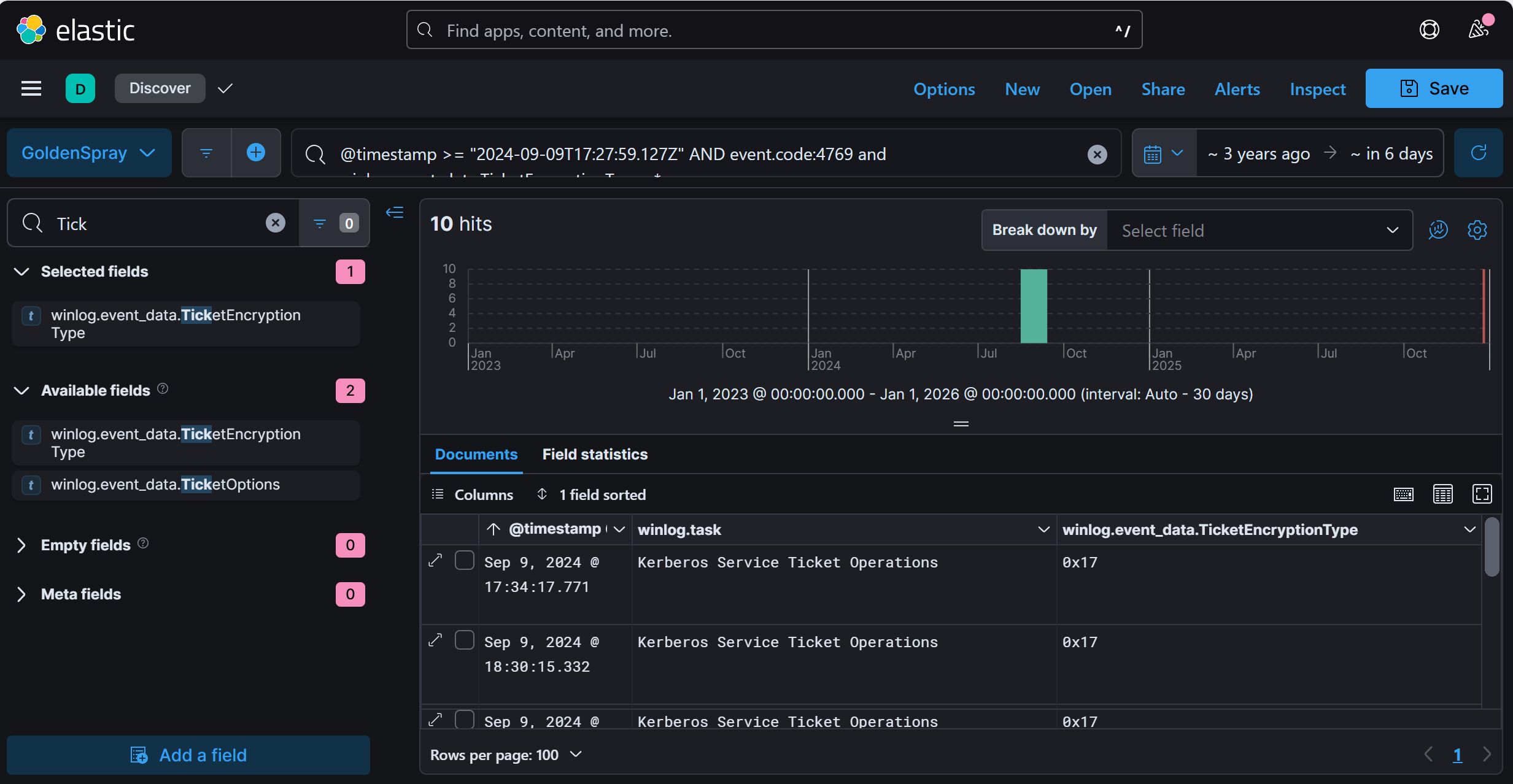


Answer: FilesCheck

Q9: What type of encryption is used for Kerberos tickets in the environment?

* Top of Form
* Kerberos tickets have different encryption types, which can indicate security weaknesses.
* Check Event ID 4769, which logs Kerberos ticket issuance.
* Query Elastic for event.code: 4769 AND winlog.event\_data.TicketEncryptionType:\*. Look for values like 0x17 or 0x12.

Query : @timestamp >= "2024-09-09T17:27:59.127Z" AND event.code:4769 and winlog.event\_data.TicketEncryptionType : \*

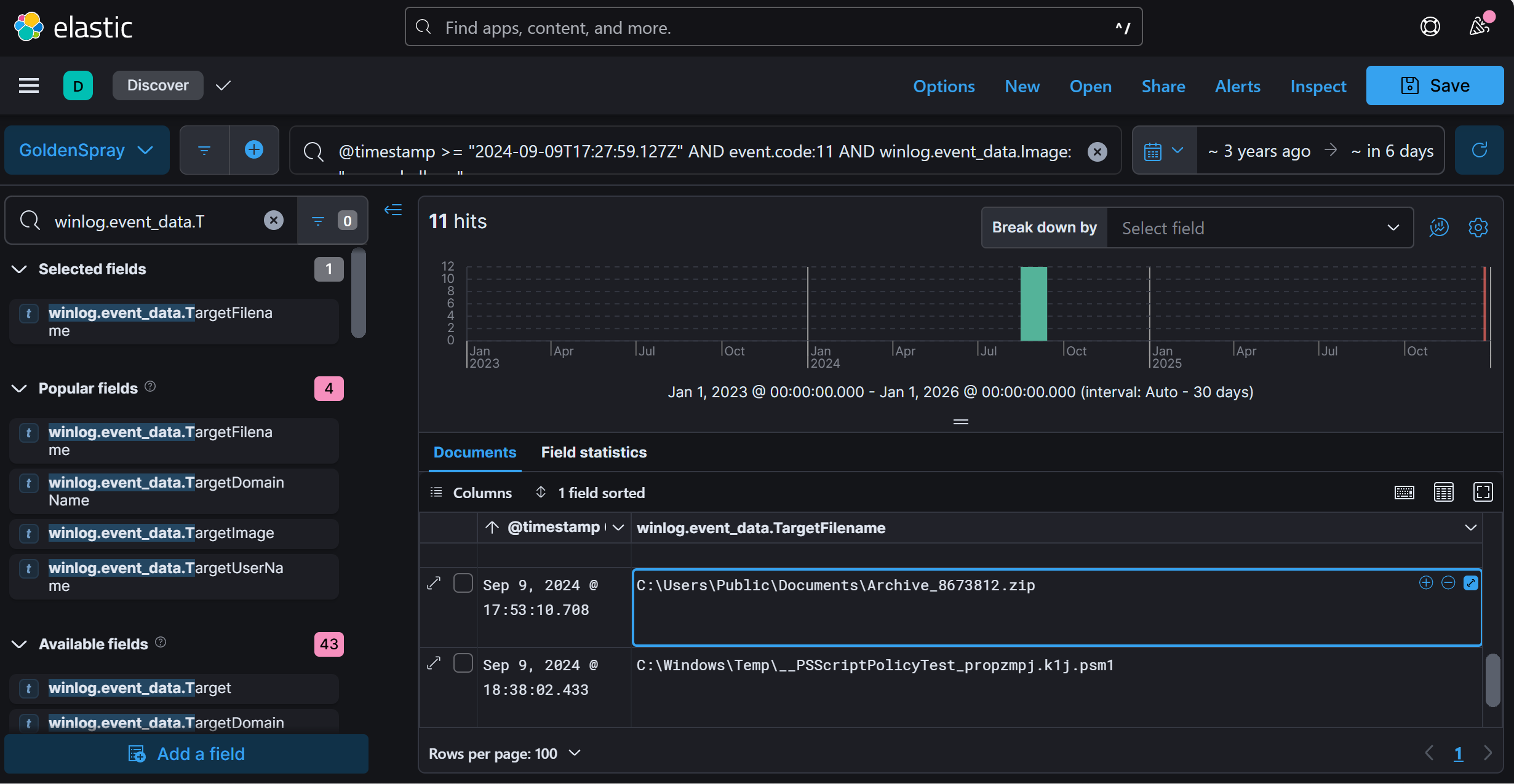


TicketEncryptionType:0x17 tương ứng với loại mã hóa: RC4-HMAC

Anwser: RC4-HMAC

Q10: Can you provide the full path of the output file in preparation for data exfiltration?

* Attackers often create ZIP or archive files before exfiltration.
* Look for Sysmon Event ID 11 (File Creation) around the time of suspected exfiltration.
* Query Elastic for event.code: 11 AND winlog.event\_data.TargetFilename:\*.zip\*. Identify the full file path.
* Query: @timestamp >= "2024-09-09T17:27:59.127Z" AND event.code:11 AND winlog.event\_data.Image: "powershell.exe"



Answer: C:\Users\Public\Documents\Archive\_8673812.zip